

Nutzung von EEM zur Automatisierung sicherer E-Mails an Benutzer

Inhalt

[Einleitung](#)

[Anwendungsfall](#)

[Hintergrund](#)

[Einrichtung des Gmail-Kontos](#)

[EEM-Basiskonfiguration](#)

[Problem nur bei installierten Standardzertifikaten](#)

[Zertifikate zum Sichern von SMTP](#)

[Einfachere Suche nach Zertifikaten](#)

[EEM mit Secure SMTP erneut testen](#)

[Weitere Hinweise und Überlegungen](#)

[Benutzernamen mit @ Symbolen](#)

[Schlussfolgerung](#)

Einleitung

In diesem Dokument wird der Prozess beschrieben, der erforderlich ist, um mithilfe der Mailserver-Aktion im Embedded Event Manager (EEM) in Cisco IOS® XE sichere E-Mails an einen SMTP-Server (Simple Mail Transfer Protocol) mit Transport Layer Security (TLS) auf Port 587 zu senden.

Es gibt viele Vorbehalte, die Sie während dieses Prozesses begegnen können, weshalb dieser Artikel geschrieben wurde, um die Schritte zu dokumentieren, die notwendig sind, um dies zu erreichen.

Anwendungsfall

Für viele Kunden ist es sinnvoll, nach einem bestimmten Ereignis automatisch eine E-Mail-Benachrichtigung zu erhalten. Das EEM-Subsystem ist ein leistungsstarkes Tool für die Erkennung von Netzwerkereignissen und die integrierte Automatisierung und bietet eine effiziente Möglichkeit zur Automatisierung von E-Mail-Benachrichtigungen auf einem Cisco IOS XE-Gerät. Sie können z. B. eine IPSLA-Spur überwachen und als Reaktion auf ein Syslog, das eine Statusänderung anzeigt, eine Aktion durchführen und die Netzwerkadministratoren per E-Mail über das Ereignis informieren. Diese Idee der "E-Mail-Benachrichtigung" kann auf viele andere Szenarien angewendet werden, um die Aufmerksamkeit auf ein bestimmtes Ereignis zu lenken, das Sie hervorheben möchten.

Hintergrund

PEM steht für "Privacy Enhanced Mail" und ist ein Format, das häufig zur Darstellung von Zertifikaten und Schlüsseln verwendet wird. Dies ist das Zertifikatformat, das von Cisco IOS XE-Geräten verwendet wird. Sichere Anwendungen (wie HTTPS oder Secure SMTP) verfügen häufig über ein "Stacked PEM", bei dem mehrere Zertifikate involviert sind, darunter:

- Stammzertifikat
- Signaturzertifikat (Zwischenprodukt)
- Endbenutzer- (oder Serverzertifikat)

Einrichtung des Gmail-Kontos

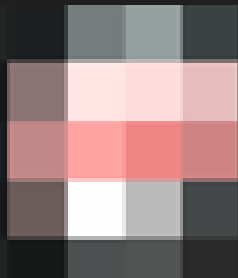
Die SMTP-Dienste von Google werden in diesem Artikel als Beispiel verwendet. Voraussetzung ist, dass Sie bereits ein Gmail-Konto eingerichtet haben.

Bei Google können Sie E-Mails von entfernten Clients an Gmail senden. In Gmail gab es früher eine Einstellung für "ungesicherte Apps", und die Anwendung würde einen Fehler bekommen, wenn diese Einstellung auf Googles Seite nicht erlaubt wäre. Diese Einstellung wurde entfernt. Stattdessen steht eine Option für "sichere Anwendungen" zur Verfügung, auf die über Folgendes zugegriffen werden kann:

mail.google.com > auf Ihr Profil klicken (#1) > Ihr Google-Konto verwalten (#2) > Sicherheit (#3) > Wie Sie sich bei Google anmelden > 2-Step Verification (#4)



1



Manage your Google Account

2



Add another account



Sign out

[Privacy Policy](#) • [Terms of Service](#)

- Home
- Personal info
- Data & privacy
- Security**
- People & sharing
- Payments & subscriptions
- About

Security

Settings and recommendations to help you keep your account secure

You have security tips

Security tips found in the Security Checkup



[Review security tips](#)

Recent security activity

New sign-in on Mac

3:55 PM



[Review security activity](#)

How you sign in to Google

Make sure you can always access your Google Account by keeping this information up to date

2-Step Verification



On since Jul 20, [blurred]



Stellen Sie auf dieser Seite sicher, dass die 2-Schritt-Überprüfung aktiviert ist.

← 2-Step Verification

2-Step Verification is ON since Jul 20, [blurred]

Sie können dann nach unten zu "App-Passwörter" scrollen, um Gmail ein Passwort generieren zu lassen, das verwendet werden kann, um sich bei Ihrem Google-Konto von einer Anwendung anzumelden, die keine 2-Schritt-Verifizierung unterstützt.

App passwords

App Passwords aren't recommended and are unnecessary in most cases. To help keep your account secure, use "Sign in with Google" to connect apps to your Google Account.

App passwords

None



← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)

You don't have any app passwords.

Select the app and device you want to generate the app password for.

Mail



Select device

iPhone

iPad

BlackBerry

Mac

Windows Phone

Windows Computer

Other *(Custom name)*

GENERATE

← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)

You don't have any app passwords.

Select the app and device you want to generate the app password for.


MyRouter ×

GENERATE

← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)

Your app passwords

Name	Created	Last used	
MyRouter	4:03 PM	-	

Select the app and device you want to generate the app password for.

Select app



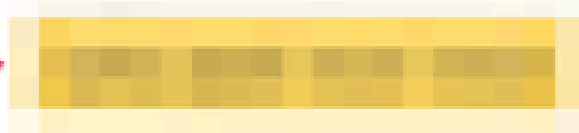
Select device



GENERATE

Generated app password

Your app password for your device



How to use it

Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above.

Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

DONE

Das 16-stellige Anwendungskennwort in diesem Screenshot wurde verschwommen, da es an ein persönliches Gmail-Konto gebunden ist.

Nachdem Sie nun ein Anwendungskennwort für Gmail haben, können Sie dieses zusammen mit Ihrem Gmail-Kontonamen als E-Mail-Server für die Weiterleitung der E-Mail verwenden. Das Format zur Angabe des Servers ist "username:password@host".

EEM-Basiskonfiguration

Es gibt viele Möglichkeiten, ein EEM-Skript genau an Ihre Anforderungen anzupassen. Dieses Beispiel ist jedoch ein einfaches EEM-Skript, mit dem die sichere E-Mail-Funktion ausgeführt werden kann:

```
(config)# event manager environment _email_from <username@gmail.com>
(config)# event manager environment _email_to <EMAIL@domain.com>
(config)# event manager environment _email_server <username>:<password>@smtp.gmail.com

(config)# event manager applet SendSecureEmailEEM
(config-applet)# event none
(config-applet)# action 0010 mail server "$_email_server" to "$_email_to" from "$_email_from" cc "$_
```

Bei den Konfigurationen werden zunächst drei EEM-Umgebungsvariablen erstellt: `_email_from`, `_email_to` und `_email_server`. Jede Variable wird definiert, um Konfigurationsänderungen zu vereinfachen. Anschließend erstellen Sie das `SendSecureEmailEEM`-Skript. Das auslösende Ereignis ist hier "none", d. h. Sie können das EEM-Skript beliebig manuell ausführen, indem Sie "# event manager run SendSecureEmailEEM" verwenden (anstatt darauf zu warten, dass ein bestimmtes Ereignis ausgelöst wird). Als Nächstes haben Sie nur eine einzige "Mail-Server" Aktion, die die E-Mail-Generierung übernimmt. Die Optionen "secure tls" (sicher) und "port 587" (Port 587) weisen das Gerät an, TLS auf Port 587 auszuhandeln, auf den die Gmail-Server zugreifen werden.

Sie müssen außerdem sicherstellen, dass Ihr Feld "von" gültig ist. Wenn Sie sich als "Alice" authentifizieren, aber versuchen, eine E-Mail von "Bob" zu senden, dann wird es fehlerhaft sein, weil Alice die E-Mail-Adresse eines anderen getäuscht hat. Das Feld "Von" muss mit dem Konto übereinstimmen, das zum Senden der E-Mail auf dem Server verwendet wird.

Problem nur bei installierten Standardzertifikaten

EEM verwendet openssl, um eine Verbindung mit dem SMTP-Server herzustellen. Zur sicheren Kommunikation sendet der Server ein Zertifikat zurück an openssl, das in Cisco IOSd ausgeführt wird. IOSd sucht dann nach einem Vertrauenspunkt, der mit diesem Zertifikat verknüpft ist.

Auf einem Cisco IOS XE-Gerät werden die Zertifikate für die Gmail SMTP-Server nicht standardmäßig installiert. Sie müssen manuell importiert werden, damit eine Vertrauensstellung hergestellt werden kann. Ohne die installierten Zertifikate schlägt der TLS-Handshake aufgrund eines "schlechten Zertifikats" fehl.

Diese Fehlerbehebungen sind äußerst hilfreich beim Debuggen von Zertifikatproblemen:


```
debug event manager action mail
debug crypto pki API
debug crypto pki callbacks
debug crypto pki messages
debug crypto pki scep
debug crypto pki server
debug crypto pki transactions
debug crypto pki validation
debug ssl openssl errors
debug ssl openssl ext
debug ssl openssl msg
debug ssl openssl states
```

Sie können eine Embedded Packet Capture (EPC) auf dem Router starten, um den Datenverkehr zum oder vom E-Mail-Server zu erfassen, wenn der EEM ausgelöst wird:

! Trigger the EEM:

```
# event manager run SendSecureEmailEEM
```

<SNIP>

```
*Mar 15 21:51:32.798: CRYPTO_PKI: (A0693) Check for identical certs
```

```
*Mar 15 21:51:32.798: CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-f
```

```
*Mar 15 21:51:32.798: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI: Cert record not found for issuer serial.
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI : (A0693) Validating non-trusted cert
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI: (A0693) Create a list of suitable trustpoints
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI: crypto_pki_get_cert_record_by_issuer()
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI: Unable to locate cert record by issuername
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI: No trust point for cert issuer, looking up cert chain
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI: (A0693) No suitable trustpoints found
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI: (A0693) Removing verify context
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI: destroying ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 32, ref
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI: ca_req_context released
```

```
*Mar 15 21:51:32.799: CRYPTO_OPSSL: Certificate verification has failed
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI: Rcvd request to end PKI session A0693.
```

```
*Mar 15 21:51:32.799: CRYPTO_PKI: PKI session A0693 has ended. Freeing all resources.
```

```
*Mar 15 21:51:32.800: >>> ??? [length 0005]
```

```
*Mar 15 21:51:32.800: 15 03 03 00 02
```

```
*Mar 15 21:51:32.800:
```

```
*Mar 15 21:51:32.800: >>> TLS 1.2 Alert [length 0002], fatal bad_certificate
```

```
*Mar 15 21:51:32.800: 02 2A
```

```
*Mar 15 21:51:32.800:
```

```
*Mar 15 21:51:32.800: SSL3 alert write:fatal:bad certificate
```

```
*Mar 15 21:51:32.801: P11:COpenSession slot 1 flags 6
```

```
*Mar 15 21:51:32.801: SSL_connect:error in error
```

```
*Mar 15 21:51:32.801: 0:error:1416F086:SSL routines:tls_process_server_certificate:certificate verify f
```

OpenSSL kann die sichere TLS-Sitzung mit dem SMTP-Server nicht herstellen und löst daher den Fehler "Bad Certificate" aus, wodurch der EEM nicht mehr ausgeführt wird:

```
*Mar 15 21:51:32.801: %HA_EM-3-FMPD_SMTP: Error occurred when sending mail to SMTP server: username:pas
*Mar 15 21:51:32.802: %HA_EM-3-FMPD_ERROR: Error executing applet SendSecureEmailEEM statement 0010
```

Die von diesem Austausch dokumentierte Paketerfassung ist als "NoCertificateInstalled.pcap" angehängt. Das endgültige TLS-Paket vom Router (10.122.x.x) zum Gmail SMTP-Server (142.251.163.xx) zeigt, dass die TLS-Aushandlung aufgrund derselben Meldung "Bad Certificate" (Ungültiges Zertifikat) beendet wurde, die zuvor bei den Debugs festgestellt wurde.

```
Frame 33: 61 bytes on wire (488 bits), 61 bytes captured (488 bits)
Ethernet II, Src: Cisco_a3:c5:f0 (74:86:0b:a3:c5:f0), Dst: Cisco_f0:44:45 (00:08:30:f0:44:45)
Internet Protocol Version 4, Src: 10.122.xx.xx, Dst: 142.251.163.xx
Transmission Control Protocol, Src Port: 13306, Dst Port: 587, Seq: 189, Ack: 4516, Len: 7
Transport Layer Security
TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Bad Certificate)
Content Type: Alert (21)
Version: TLS 1.2 (0x0303)
Length: 2
Alert Message
Level: Fatal (2)
Description: Bad Certificate (42)
```

Zertifikate zum Sichern von SMTP

Da die Zertifikate fehlen, die es dem Cisco IOS XE-Gerät ermöglichen, den Servern von Gmail zu vertrauen, besteht der Fix darin, eines oder alle dieser Zertifikate in einem Vertrauenspunkt auf dem Gerät zu installieren.

Die vollständigen Debugs des vorherigen Tests zeigen beispielsweise die folgenden Zertifikatsuchvorgänge:

```
CRYPTO_PKI(Cert Lookup) issuer="cn=GTS CA 1C3,o=Google Trust Services LLC,c=US" serial number= 52 87 E0
CRYPTO_PKI(Cert Lookup) issuer="cn=GTS Root R1,o=Google Trust Services LLC,c=US" serial number= 02 03 B
CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-sa,c=BE" serial number=
```

Ein Zertifikat für jeden dieser Aussteller muss unter einem Vertrauenspunkt installiert werden, damit das Gerät eine sichere Sitzung mit den Gmail SMTP-Servern herstellen kann. Mithilfe der folgenden Konfigurationen können Sie für jeden Aussteller einen Vertrauenspunkt erstellen:

```
crypto pki trustpoint CA-GTS-1C3
  enrollment terminal
  revocation-check none
  chain-validation stop
```

```
crypto pki trustpoint CA-GTS-Root-R1
  enrollment terminal
  revocation-check none
  chain-validation stop
```

```
crypto pki trustpoint CA-GlobalSign-Root
  enrollment terminal
  revocation-check none
  chain-validation stop
```

```
crypto pki trustpoint CA-gmail-SMTP
  enrollment terminal
  revocation-check none
  chain-validation stop
```

Sie haben jetzt für jeden eingerichteten Emittenten einen Vertrauenspunkt, mit dem jedoch noch keine Zertifikate verknüpft sind. Im Wesentlichen handelt es sich dabei um leere vertrauenswürdige Punkte:

```
# show run | sec crypto pki certificate chain CA-
crypto pki certificate chain CA-GTS-1C3
crypto pki certificate chain CA-GTS-Root-R1
crypto pki certificate chain CA-GlobalSign-Root
crypto pki certificate chain CA-gmail-SMTP
```

Sie müssen feststellen, wo sich diese Zertifikate befinden, und sie dann auf dem Gerät installieren.

Wir suchen online nach "Google Trust Services 1C3" und stoßen schnell auf das Google Trust Services Repository mit Zertifikaten:

<https://pki.goog/repository/>

Nachdem Sie alle Zertifikate auf dieser Seite erweitert haben, können Sie nach "1C3" suchen, auf das Dropdown-Menü "Action" klicken und das PEM-Zertifikat herunterladen:

GTS CA 1C3	RSA	23:ec:b0:3e:ec:17:33:8c:4e:33:a6:b4:8a:41:dc:3c:da:12:28:1b:bc:3f:8:13:c0:58:9d:6c:c2:38:75:22	2027-09-30	Action ^
GTS CA 1D4	RSA	64:e2:86:b7:60:63:60:2a:37:2e:fd:60:cd:e8:db:26:56:a4:9e:e1:5e:825:4b:3d:6e:b5:fe:38:f4:28:8b		Preview Certificate View Certificate Details
GTS CA 1D8	RSA	c0:e8:b1:c1:95:cd:ff:7b:51:37:b9:ad:35:13:a6:12:0b:1d:bf:f4:9e:5e:8:c:ea:32:73:bc:8d:76:18:77		Downloads Certificate (PEM) Certificate (DER) Partitioned CRLs (JSON)
GTS CA 1P5	RSA	97:d4:20:03:e1:32:55:29:46:09:7f:20:ef:95:5f:5b:1c:d5:70:aa:43:727:80:03:3a:65:ef:be:69:75:8d		
		11:c6:97:87:87:32:05:6d:e1:7c:1d:a1:34:e9:d2:b6:d2:3c:f1:de:95:b		

Das Öffnen der heruntergeladenen PEM-Datei mit einem Texteditor zeigt, dass es sich lediglich um ein Zertifikat handelt, das unter dem zuvor erstellten Vertrauenspunkt auf das Cisco IOS XE-Gerät importiert werden kann:

```
-----BEGIN CERTIFICATE-----
MIIF1jCCA36gAwIBAgINAg08U11rNMcy9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2x1IFRydXN0IFN1cnZpY2VzIEExMQZEU
<snip>
AJ2xDx8hcFH1mt0G/FX0Kw4zd8NLQsLxdxP8c4CU6x+7Nz/OAipmsHMDmQyubDKw
juDEI/9bfU11cKwrmz302+BtjjKAvpafkm0817tdufThcV4q508DIrGKZTqPwJN1
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDB1Hz4n/FsRC6UfTd
-----END CERTIFICATE-----
```

Sie können es mithilfe der folgenden Konfigurationsbefehle unter dem Vertrauenspunkt "CA-GTS-1C3" importieren:

```
(config)# crypto pki authenticate CA-GTS-1C3

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIF1jCCA36gAwIBAgINAg08U11rNMcy9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2x1IFRydXN0IFN1cnZpY2VzIEExMQZEU
<snip>
juDEI/9bfU11cKwrmz302+BtjjKAvpafkm0817tdufThcV4q508DIrGKZTqPwJN1
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDB1Hz4n/FsRC6UfTd

Certificate has the following attributes:
Fingerprint MD5: 178EF183 43CCC9E0 ECB0E38D 9DEA03D8
Fingerprint SHA1: 1E7EF647 CBA15028 1C608972 57102878 C4BD8CDC
Certificate validated - Signed by existing trustpoint CA certificate.

Trustpoint CA certificate accepted.
% Certificate successfully imported

(config)#
```

Anschließend können Sie bestätigen, dass das Zertifikat installiert wurde:

```
# show run | sec crypto pki certificate chain CA-GTS-1C3
crypto pki certificate chain CA-GTS-1C3
certificate ca 0203BC53596B34C718F5015066
 30820596 3082037E A0030201 02020D02 03BC5359 6B34C718 F5015066 300D0609
2A864886 F70D0101 0B050030 47310B30 09060355 04061302 55533122 30200603
55040A13 19476F6F 676C6520 54727573 74205365 72766963 6573204C 4C433114
<snip>
E1715E2A E4EF0322 B18A653A 8FC09365 D485CD0F 0F5B8359 1647162D 9C243AC8
80A62614 859BF637 9BAC6FF9 C5C30651 F3E27FC5 B110BA51 F4DD
quit
```

```
#show crypto pki certificates verbose CA-GTS-1C3
CA Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 0203BC53596B34C718F5015066
Certificate Usage: Signature
Issuer:
  cn=GTS Root R1
  o=Google Trust Services LLC
  c=US
Subject:
  cn=GTS CA 1C3
  o=Google Trust Services LLC
  c=US
CRL Distribution Points:
  http://crl.pki.goog/gtsr1/gtsr1.crl
Validity Date:
  start date: 00:00:42 UTC Aug 13 2020
  end date: 00:00:42 UTC Sep 30 2027
Subject Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (2048 bit)
Signature Algorithm: SHA256 with RSA Encryption
Fingerprint MD5: 178EF183 43CCC9E0 ECB0E38D 9DEA03D8
Fingerprint SHA1: 1E7EF647 CBA15028 1C608972 57102878 C4BD8CDC
X509v3 extensions:
  X509v3 Key Usage: 86000000
    Digital Signature
    Key Cert Sign
    CRL Signature
  X509v3 Subject Key ID: 8A747FAF 85CDEE95 CD3D9CD0 E24614F3 71351D27
  X509v3 Basic Constraints:
    CA: TRUE
  X509v3 Authority Key ID: E4AF2B26 711A2B48 27852F52 662CEFF0 8913713E
Authority Info Access:
  OCSP URL: http://ocsp.pki.goog/gtsr1
  CA ISSUERS: http://pki.goog/repo/certs/gtsr1.der
X509v3 CertificatePolicies:
  Policy: 2.23.140.1.2.2
  Policy: 2.23.140.1.2.1
  Policy: 1.3.6.1.4.1.11129.2.5.3
    Qualifier ID: 1.3.6.1.5.5.7.2.1
    Qualifier Info: https://pki.goog/repository/
```

Extended Key Usage:
Client Auth
Server Auth
Cert install time: 02:31:20 UTC Mar 16 2023
Cert install time in nsec: 1678933880873946880
Associated Trustpoints: CA-GTS-1C3

Als Nächstes können Sie die Zertifikate für die beiden anderen Emittenten installieren.

CA-GTS-Root-R1:

Konfiguration:

[Spoiler](#) (Zum Lesen markieren)

```
(config)# crypto pki authenticate CA-GTS-Root-R1

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIFVzCCAz+gAwIBAgINAgPlk28xsBNJiGuiFzANBgkqhkiG9w0BAQwFADBHMQsw
CQYDVQQGEwJVUzEiMCAgA1UEChMZR29vZ2x1IFRydXN0IFNlcnZpY2VzIExMQzEU
<snip>
2tIMPNuzj-smhDYAPexZ3FL//2wmUsp08IFgV6dtxQ/PeEMMA3Kgq1bbC1j+Qa3bb
bP6MvPJwNQzcmRk13NfIRmPVNnGuV/u3gm3c

Certificate has the following attributes:
Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40
Fingerprint SHA1: E58C1CC4 913B3863 4BE9106E E3AD8E6B 9DD9814A

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

(config)# end
```

```
(config)# crypto pki authentication CA-GTS-Root-R1Geben Sie das Base 64-codierte CA-Zertifikat
ein.Beenden Sie das Zertifikat mit einer leeren Zeile oder dem Wort "quit" auf einer eigenen
ZeileMIFVzCCAz+gAwIBAgINAgPlk28xsBNJiGuiFzANBgkqhkiG9w0BAQwFADBHMQswCQYDVQQGEwJVUzEiMCAgA1UEChMZR29vZ2x1IFRydXN0IFNlcnZpY2Vz
>2tIMPNuzj-smhDYAPexZ3FL//2wmUsp08IFgV6dtxQ/PeEMMA3Kgq1bbC1j+Qa3bbbP6MvPJwNQzcmRk13NfIRmPVNnGuV/u3gm3cCertificate hat die folgenden Attribute:Fingerprint MD5: 05FED0BF 71A8A376
63DA01E0 D852DC40 Fingerprint SHA1: E58C1CC4 913B3863 4BE9 106E E3AD8E6B
9DD9814A% Akzeptieren Sie dieses Zertifikat? [ja/nein]: jaZertifikat der Vertrauensstelle
akzeptiert.% Zertifikat erfolgreich importiert(config)# Ende
```

Running-config-Verifizierung:

[Spoiler](#) (Zum Lesen markieren)

```
# show run | sec crypto pki certificate chain CA-GTS-Root-R1
crypto pki certificate chain CA-GTS-Root-R1
```

```
certificate ca 0203E5936F31B01349886BA217
30820557 3082033F A0030201 02020D02 03E5936F 31B01349 886BA217 300D0609
2A864886 F70D0101 0C050030 47310B30 09060355 04061302 55533122 30200603
<snip>
6775C119 3A2B474E D3428EFD 31C81666 DAD20C3C DBB38EC9 A10D800F 7B167714
BFFFD0B9 94B293BC 205815E9 DB7143F3 DE10C300 DCA82A95 B6C2D63F 906B76DB
6CFE8CBC F270350C DC991935 DCD7C846 63D53671 AE57FBB7 826DDC
quit
```

```
# show run | sec crypto pki certificate chain CA-GTS-Root-R1crypto pki certificate chain CA-GTS-
Root-R1 certificate ca 0203E5936F31B01349886BA217 30820557 3082033F A0030201
02020D02 03E5936F 31B01349 886BA217 300D0609 2A864886 F70D0101 0C050030
47310B30 09060355 04061302 55533122 <snip> 6775C119 3A2B474E D3428EFD 3
1C30200603 DAD20C3C DBB38EC9 A10D800F 7B81666 BFDB09 94B293BC 167714E9
DB7143F3 DE10C300 DCA82A95 B6C2D63F 906B76DB 6CFE8CBC F205815C DC270350
DCD7C846 63D991935 53671 AE57FBB7 826DDC quit
```

Kryptografieverifizierung anzeigen:

[Spoiler](#) (Zum Lesen markieren)

```
# show crypto pki certificates verbose CA-GTS-Root-R1
CA Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 0203E5936F31B01349886BA217
Certificate Usage: Signature
Issuer:
  cn=GTS Root R1
  o=Google Trust Services LLC
  c=US
Subject:
  cn=GTS Root R1
  o=Google Trust Services LLC
  c=US
Validity Date:
  start date: 00:00:00 UTC Jun 22 2016
  end date: 00:00:00 UTC Jun 22 2036
Subject Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (4096 bit)
Signature Algorithm: SHA384 with RSA Encryption
Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40
Fingerprint SHA1: E58C1CC4 913B3863 4BE9106E E3AD8E6B 9DD9814A
X509v3 extensions:
  X509v3 Key Usage: 86000000
    Digital Signature
    Key Cert Sign
    CRL Signature
  X509v3 Subject Key ID: E4AF2B26 711A2B48 27852F52 662CEFF0 8913713E
  X509v3 Basic Constraints:
    CA: TRUE
  Authority Info Access:
    Cert install time: 14:39:38 UTC Mar 13 2023
    Cert install time in nsec: 1678718378546968064
    Associated Trustpoints: CA-GTS-Root-R1 Trustpool
```

show crypto pki Certificates verbose CA-GTS-Root-R1CA Certificate Status: Available Version: 3 Certificate Serial Number (hex): 0203E5936F31B01349886BA217 Certificate Usage: Signature Issuer: cn=GTS Root R1 o=Google Trust Services LLC=US Subject: cn=US GTS Root R1 o=Google Trust Services LLC c=US Gültigkeitsdatum: Startdatum: 00:00:00 UTC Jun 22 2016 Enddatum: 00:00:00 UTC Jun 22 2036 Betreff-Schlüsselinfo: Öffentlicher Schlüssel Algorithmus: rsaEncryption RSA Öffentlicher Schlüssel: (404) 96 Bit) Signatur-Algorithmus: SHA384 mit RSA-Verschlüsselung Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40 Fingerprint SHA1: E58C1CC4 913B3863 4BE9106E E3AD8E6B 9DD9814A X509v3-Erweiterungen: X509v3 Key Usage: 86000000 Digital Signature Key Cert Sign CRL Signature X509v3 Subject Key ID: E4AF2B26 711A2B48 27852 F52 662CEFF0 8913713E X509v3 Grundbedingungen: CA: TRUE Authority Info Zugriff: CERT-Installationszeit: 14:39:38 UTC 13. März 2023 CERT-Installationszeit in nsec: 1678718378546968064 Zugehörige Vertrauenspunkte: CA-GTS-Root-R1 Trustpool

CA-GlobalSign-Root:

Dieses Zertifikat wurde an folgendem Speicherort gefunden:

<https://support.globalsign.com/ca-certificates/root-certificates/globalsign-root-certificates>

Konfiguration:

[Spoiler](#) (Zum Lesen markieren)

```
(config)# crypto pki authenticate CA-GlobalSign-Root
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

```
MIIDdTCCA12gAwIBAgILBAAAAAABFUtaW5QwDQYJKoZIhvcNAQEFBQAwVzELMAKGA1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv<snip>DKqC5J1R3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbMEHMUfpIBvFSDJ3gyICh3WZ1Xi/EjJKSZp4A==
```

Certificate has the following attributes:

Fingerprint MD5: 3E455215 095192E1 B75D379F B187298A

Fingerprint SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

```
(config)# end
```

(config)# crypto pki authentication CA-GlobalSign-RootGeben Sie das Base 64-codierte CA-Zertifikat ein.Beenden Sie das Zertifikat mit einer leeren Zeile oder dem Wort "quit" in einer Zeile

für sichMIIDdTCCA12gAwIBAgILBAAAAAABFUtaW5QwDQYJKoZIhvcHVC

NAQEFBQAwVzELMAKGA1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv

qC5J1R3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbMEHMUfpIBvFSDJ3gyICh3

IXi/EjJKSZp4A==Certificate hat die folgenden Attribute:Fingerprint MD5: 3E455215 095192E1

B75D379F B187298A Fingerprint SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A

41D829C% Akzeptieren Sie dieses Zertifikat? [ja/nein]: jaZertifikat der Vertrauensstelle

akzeptiert.% Zertifikat erfolgreich importiert(config)# Ende

Running-config-Verifizierung:

[Spoiler](#) (Zum Lesen markieren)

```
# show run | sec crypto pki certificate chain CA-GlobalSign-Root
crypto pki certificate chain CA-GlobalSign-Root
certificate ca 040000000001154B5AC394
 30820375 3082025D A0030201 02020B04 00000000 01154B5A C394300D 06092A86
 <snip>
 2AC45631 95D06789 852BF96C A65D469D 0CAA82E4 9951DD70 B7DB563D 61E46AE1
 5CD6F6FE 3DDE41CC 07AE6352 BF5353F4 2BE9C7FD B6F7825F 85D24118 DB81B304
 1CC51FA4 806F1520 C9DE0C88 0A1DD666 55E2FC48 C9292669 E0
 quit
```

```
# show run | sec crypto pki certificate chain CA-GlobalSign-Rootcrypto pki certificate chain CA-
GlobalSign-Root certificate ca 040000000001154B5AC394 30820375 3082025D A0030201
02020B04 00000000 01154B5A C394300D 06092A86 <snip> 2AC45631 95D06789 852BF99 6C
A65D469D 0CAA82E4 9951DD70 B7DB563D 61E46AE1 5CD6F6FE 3DDE41CC 07AE6352
BF5353F4 2BE9C7FX D B6F7825F 85D24118 DB81B304 1CC51FA4 806F1520 C9DE0C88
0A1DD666 55E2FC48 C9292669 E0 quit
```

Kryptografieverification anzeigen:

[Spoiler](#) (Zum Lesen markieren)

```
#show crypto pki certificates verbose CA-GlobalSign-Root
CA Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 040000000001154B5AC394
Certificate Usage: Signature
Issuer:
cn=GlobalSign Root CA
ou=Root CA
o=GlobalSign nv-sa
c=BE
Subject:
cn=GlobalSign Root CA
ou=Root CA
o=GlobalSign nv-sa
c=BE
Validity Date:
start date: 12:00:00 UTC Sep 1 1998
end date: 12:00:00 UTC Jan 28 2028
Subject Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: 3E455215 095192E1 B75D379F B187298A
Fingerprint SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C
X509v3 extensions:
X509v3 Key Usage: 6000000
Key Cert Sign
CRL Signature
```

X509v3 Subject Key ID: 607B661A 450D97CA 89502F7D 04CD34A8 FFFCFD4B
X509v3 Basic Constraints:
CA: TRUE
Authority Info Access:
Cert install time: 03:03:01 UTC Mar 16 2023
Cert install time in nsec: 1678935781942944000
Associated Trustpoints: CA-GlobalSign-Root

```
#show crypto pki Certificates verbose CA-GlobalSign-RootCA CertificateStatus: AvailableVersion:
3Certificate Serial Number (hex): 04000000001154B5AC394Certificate Usage: SignatureIssuer:
cn=GlobalSign Root CAou=Root CAo=GlobalSign nv-sac=BESubjekt: cn=GlobalSign Root of
CAou=Root CAo=GlobalSign nv-sac=BEValidity Datum: Startdatum: 12:00:00 UTC 1. September
1998Enddatum: 12:00:00 UTC 28. Januar 2028Subject Key Info:Public Key Algorithm:
rsaEncryptionRSA Public Key (2048 Bit)Signatur-Algorithmus: SHA1 mit RSA-
VerschlüsselungFingerprint MD5: 3E455215 095192E1 B75D379F B187298A Fingerprint SHA1:
B1BC968B D4F49D62 2AA89A81 F2150152 A 41D829C X509v3-Erweiterungen:X509v3
Schlüsselverwendung: 6000000Key-ZertifikatzeichenCRL-SignaturX509v3 Betreffschlüssel-ID:
607B661A 450D97CA 89502F7D 04CD34A8 FFF FCFD4B X509v3 Grundbedingungen:CA:
TRUEAuthority Info Access:Cert install time: 03:03:01 UTC Mar 16 2023 Cert install time in nsec:
1678935781942944000Associated Trustpoints: CA-GlobalSign-Root
```

CA-gmail-SMTP:

Das TLS-Zertifikat für die Gmail-Server (CA-gmail-SMTP) wurde mithilfe der hier dokumentierten Schritte gefunden: [TLS-Zertifikate für sicheren Transport verwenden](#)

Konfiguration:

[Spoiler](#) (Zum Lesen markieren)

```
(ca-trustpoint)# crypto pki authenticate CA-gmail-SMTP
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

```
MIIEhjCCA26gAwIBAgIQUofgQKT+9wcSaLBP3d3w9DANBgkqhkiG9w0BAQsFADBG
MQswCQYDVQQGEWJlbnRlbnR1eEiMCAGA1UEChMZMjRvZ29vZ29vZ29vZ29vZ29v
<snip>
b1J2gZAYjyd4nfFRG1jeL5KrsfUR9hIXufqySv1PUoPuKSi3fvsIS21BYEXEe8uZ
gBxJaeTUjncvow==
```

```
Trustpoint 'CA-gmail-SMTP' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
```

```
Certificate has the following attributes:
Fingerprint MD5: 19651FBE 906A414D 6D57B783 946F30A2
Fingerprint SHA1: 4EF392CB EEB46D5E 47433953 AAEF313F 4C6D2825
```

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

```
(config)#
```

(ca-trustpoint)# crypto pki authentifizieren CA-gmail-SMTP
Egeben Sie die Basis 64 codierte CA-Zertifikat.
Ende mit einer leeren Zeile oder das Wort "quit" auf einer Linie durch sich selbst
MIEhJCCA26gAwIBAgIQUofgQKT+9wcSaLBP3d3w9DANBgkqhkiG9w0BAQsFADBGMQswCQYDV
'CA gmail-SMTP' ist eine untergeordnete CA. Das Zertifikat ist jedoch kein CA-Zertifikat.
Manuelle Überprüfung erforderlich
Zertifikat weist die folgenden Attribute auf:
Fingerprint MD5: 19651FBE906A414D 6D57B783 946F30A2
Fingerprint SHA1: 4EF392CB EEB46D5E 47433953 AAEF313F4C6D2825%
Akzeptieren Sie dieses Zertifikat? [ja/nein]: ja
Zertifikat der Vertrauensstelle akzeptiert.%
Zertifikat erfolgreich importiert(config)#

Running-config-Verifizierung:

[Spoiler](#) (Zum Lesen markieren)

```
# show run | sec crypto pki certificate chain CA-gmail-SMTP
crypto pki certificate chain CA-gmail-SMTP
certificate ca 5287E040A4FEF7071268B04FDDDDF0F4
30820486 3082036E A0030201 02021052 87E040A4 FEF70712 68B04FDD DDF0F430
0D06092A 864886F7 0D01010B 05003046 310B3009 06035504 06130255 53312230
<snip>
92ABB1F5 11F61217 B9FAB24A F94F5283 EE2928B7 7EFB084B 6D416045 C47BCB99
801C4969 E4D48E77 2FA3
quit
```

```
# show run | sec crypto pki certificate chain CA-gmail-SMTP crypto pki certificate chain CA-gmail-SMTP
certificate ca 5287E040A4FEF7071268B04FDDDDF0F4 30820486 3082036E A0030201
02021052 87E040A4 FEF70712 68B04FDD DDF0F430 0D06092A 864886F7 0D01010B
05003046 310B3009 06035504 06130255 <snip> 92ABB1F5 11F53312230 B9FAB24A
F94F5283 EE2928B7 7EFB00 84B 6D61217 416045 C47BCB99 801C4969 E4D48E77 2FA3 quit
```

Kryptografieverification anzeigen:

[Spoiler](#) (Zum Lesen markieren)

```
# show crypto pki certificates verbose CA-gmail-SMTP
CA Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 5287E040A4FEF7071268B04FDDDDF0F4
Certificate Usage: Signature
Issuer:
cn=GTS CA 1C3
o=Google Trust Services LLC
c=US
Subject:
cn=smtp.gmail.com
CRL Distribution Points:
http://crls.pki.goog/gts1c3/moVDfISia2k.crl
Validity Date:
start date: 09:15:03 UTC Feb 20 2023
end date: 09:15:02 UTC May 15 2023
Subject Key Info:
Public Key Algorithm: ecEncryption
EC Public Key: (256 bit)
Signature Algorithm: SHA256 with RSA Encryption
```

Fingerprint MD5: 19651FBE 906A414D 6D57B783 946F30A2
Fingerprint SHA1: 4EF392CB EEB46D5E 47433953 AAEF313F 4C6D2825
X509v3 extensions:
X509v3 Key Usage: 80000000
Digital Signature
X509v3 Subject Key ID: 5CC36972 D07FE997 510E1A67 8A8ECC23 E40CFB68
X509v3 Basic Constraints:
CA: FALSE
X509v3 Subject Alternative Name:
smtp.gmail.com
IP Address :
OtherNames :
X509v3 Authority Key ID: 8A747FAF 85CDEE95 CD3D9CD0 E24614F3 71351D27
Authority Info Access:
OCSP URL: http://ocsp.pki.goog/gts1c3
CA ISSUERS: http://pki.goog/repo/certs/gts1c3.der
X509v3 CertificatePolicies:
Policy: 2.23.140.1.2.1
Extended Key Usage:
Server Auth
Cert install time: 03:10:41 UTC Mar 16 2023
Cert install time in nsec: 1678936241822955008
Associated Trustpoints: CA-gmail-SMTP

```
# show crypto pki Certificates verbose CA-gmail-SMTPCA CertificateStatus: AvailableVersion:
3Certificate Serial Number (hex): 5287E040A4FEF7071268B04FDDDF0F4Certificate Usage:
SignatureIssuer: cn=GTS CA 1C3o=Google Trust Services LLCc=USS Betreff:
cn=smtp.gmail.comCRL Verteilungspunkte: http://crls.pki.goog/gts1c3/moVDfISia2k.crlValidity
Datum: Startdatum: 09:15:03 UTC Feb 20 2023Enddatum: 09:15:02 UTC May 15 2023Betreff-
Schlüsselinfo:Public Key Algorithm: ecEncryptionEC Public Key: (25) 6 Bit)Signatur-Algorithmus:
SHA256 mit RSA-VerschlüsselungFingerprint MD5: 19651FBE 906A414D 6D57B783 946F30A2
Fingerprint SHA1: 4EF392CB EEB46D5E 47433953 AAEF33 13F 4C6D2825 X509v3-
Erweiterungen:X509v3 Schlüsselverwendung: 80000000Digitale SignaturX509v3 Betreffschlüssel-
ID: 5CC36972 D07FE997 510E1A67 8A8ECC23 E40E CFB68 X509v3 Grundbedingungen:CA:
FALSEX509v3 Betreff Alternativer Name:smtp.gmail.com IP-Adresse: AndereNamen: X509v3
Autoritätsschlüssel-ID: 8A747FAF 85CDEE95 CD3D9CD0 E24614F3 71351D27 Autorität Info
Access:OCSP URL: http://ocsp.pki.goog/gts1c3CA ISSUERS:
http://pki.goog/repo/certs/gts1c3.derX509v3 CertificatePolicies:Policy: 2.23.140.1.2.1Extended
Key Usage:Server AuthCert install time: 03:10:41 UTC Mar 16 2023 Cert install time in nsec:
1678936241822955008Associated Trustpoints: CA-gmail-SMTP
```

Einfachere Suche nach Zertifikaten

Alternativ können Sie versuchen, einen openssl-Aufruf von einem Server/Laptop zu verwenden, um die Zertifikate von einem SMTP-Server zu erhalten, ohne Debugs verwenden und Google nach diesen suchen zu müssen:

```
openssl s_client -showcerts -verify 5 -connect gmail-smtp-in.l.google.com:25 -starttls smtp
```

Sie können auch use smtp.gmail.com:

```
openssl s_client -showcerts -verify 5 -connect smtp.gmail.com:25 -starttls smtp
```

Die Ergebnisse dieses Anrufs enthalten die eigentlichen Zertifikate, die für die "crypto pki authentication <trustpoint>"-Konfigurationen verwendet werden können.

EEM mit Secure SMTP erneut testen

Nachdem die Zertifikate auf das Cisco IOS XE-Gerät angewendet wurden, sendet das EEM-Skript die sicheren SMTP-Nachrichten wie erwartet.

```
# event manager run SendSecureEmailEEM
```

Überprüfen Sie den Spoiler auf die vollständigen Ausgaben für Crypto und SSL-Debugging:

[Spoiler](#) (Zum Lesen markieren)

```
# event manager run SendSecureEmailEEM
```

```
*Mar 16 03:28:50.673: CRYPTO_OPSSL: Allocated the memory for OPSSLContext
*Mar 16 03:28:50.673: CRYPTO_OPSSL: Set cipher specs to mask 0x02FC0000 for version 128
*Mar 16 03:28:50.674: Set the Default EC Curve list: 0x70Set the EC curve list: secp521r1:secp384r1:pr
*Mar 16 03:28:50.674: opssl_SetPKIInfo entry
*Mar 16 03:28:50.674: CRYPTO_PKI: (A069B) Session started - identity selected (TP-self-signed-486541296)
*Mar 16 03:28:50.674: CRYPTO_PKI: Begin local cert chain retrieval.
*Mar 16 03:28:50.674: CRYPTO_PKI(Cert Lookup) issuer="cn=IOS-Self-Signed-Certificate-486541296" serial
*Mar 16 03:28:50.674: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
1C 7F 3D 52 67 66 D5 59 E2 66 58 E7 8B E7 9B 8E
*Mar 16 03:28:50.675: CRYPTO_PKI: Done with local cert chain fetch 0.
*Mar 16 03:28:50.675: CRYPTO_PKI: Rcvd request to end PKI session A069B.
*Mar 16 03:28:50.675: CRYPTO_PKI: PKI session A069B has ended. Freeing all resources.TP-self-signed-486
*Mar 16 03:28:50.675: opssl_SetPKIInfo done.
*Mar 16 03:28:50.675: CRYPTO_OPSSL: Common Criteria is disabled on this session.Disabling Common Criter
*Mar 16 03:28:50.675: CRYPTO_OPSSL: ciphersuites ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA
*Mar 16 03:28:50.676: Handshake start: before SSL initialization
*Mar 16 03:28:50.676: SSL_connect:before SSL initialization
*Mar 16 03:28:50.676: >>> ??? [length 0005]
*Mar 16 03:28:50.676: 16 03 01 00 95
*Mar 16 03:28:50.676:
*Mar 16 03:28:50.676: >>> TLS 1.2 Handshake [length 0095], ClientHello
*Mar 16 03:28:50.676: 01 00 00 91 03 03 26 4B 9F B3 44 94 FD 5F FD A1
<snip>
*Mar 16 03:28:50.679: 03 03 01 02 01
*Mar 16 03:28:50.679:
*Mar 16 03:28:50.679: SSL_connect:SSLv3/TLS write client hello
```

```
*Mar 16 03:28:50.692: <<< ??? [length 0005]
*Mar 16 03:28:50.692: 16 03 03 00 3F
*Mar 16 03:28:50.692:
*Mar 16 03:28:50.692: SSL_connect:SSLv3/TLS write client hello
*Mar 16 03:28:50.692: <<< TLS 1.2 Handshake [length 003F], ServerHello
*Mar 16 03:28:50.692: 02 00 00 3B 03 03 64 12 7E 05 25 F6 7A BD A0 2E
*Mar 16 03:28:50.692: 58 83 12 7F 90 CD F4 AB E2 69 53 A8 C7 FC 44 4F
*Mar 16 03:28:50.692: 57 4E 47 52 44 01 00 C0 2B 00 00 13 00 17 00 00
*Mar 16 03:28:50.693: FF 01 00 01 00 00 0B 00 02 01 00 00 23 00 00
*Mar 16 03:28:50.693: TLS server extension "unknown" (id=23), len=0
TLS server extension "renegotiate" (id=65281), len=1

*Mar 16 03:28:50.693: 00
*Mar 16 03:28:50.693: TLS server extension "EC point formats" (id=11), len=2

*Mar 16 03:28:50.693: 01 00
*Mar 16 03:28:50.693: TLS server extension "session ticket" (id=35), len=0

*Mar 16 03:28:50.693: <<< ??? [length 0005]
*Mar 16 03:28:50.693: 16 03 03 0F 9A
*Mar 16 03:28:50.694:
*Mar 16 03:28:50.702: SSL_connect:SSLv3/TLS read server hello
*Mar 16 03:28:50.702: <<< TLS 1.2 Handshake [length 0F9A], Certificate
*Mar 16 03:28:50.702: 0B 00 0F 96 00 0F 93 00 04 8A 30 82 04 86 30 82
*Mar 16 03:28:50.702: 03 6E A0 03 02 01 02 02 10 52 87 E0 40 A4 FE F7
<snip>
*Mar 16 03:28:50.763: 82 35 CF 62 8B C9 24 8B A5 B7 39 0C BB 7E 2A 41
*Mar 16 03:28:50.763: BF 52 CF FC A2 96 B6 C2 82 3F
*Mar 16 03:28:50.763:
*Mar 16 03:28:50.765: CC_DEBUG: Entering shim layer app callback function
*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Session started - identity not specified
*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Adding peer certificate
*Mar 16 03:28:50.767: CRYPTO_PKI: Added x509 peer certificate - (1162) bytes
*Mar 16 03:28:50.767: CRYPTO_PKI: (A069C) Adding peer certificate
*Mar 16 03:28:50.768: CRYPTO_PKI: Added x509 peer certificate - (1434) bytes
*Mar 16 03:28:50.768: CRYPTO_PKI: (A069C) Adding peer certificate
*Mar 16 03:28:50.770: CRYPTO_PKI: Added x509 peer certificate - (1382) bytes
*Mar 16 03:28:50.770: CRYPTO_OPSSL: Validate Certificate Chain Callback
*Mar 16 03:28:50.770: CRYPTO_PKI(Cert Lookup) issuer="cn=GTS CA 1C3,o=Google Trust Services LLC,c=US" s

*Mar 16 03:28:50.770: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
A7 CC 4B 0F 36 C3 AC D1 2F 77 DD 1D 9A 37 DC FC

*Mar 16 03:28:50.770: CRYPTO_PKI(Cert Lookup) issuer="cn=GTS Root R1,o=Google Trust Services LLC,c=US"

*Mar 16 03:28:50.771: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
03 9F CF 59 82 EE 09 CC 4F 53 AE D8 02 7E 4B AF

*Mar 16 03:28:50.771: CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-

*Mar 16 03:28:50.771: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A

*Mar 16 03:28:50.771: CRYPTO_PKI: Cert record not found for issuer serial.
*Mar 16 03:28:50.772: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
*Mar 16 03:28:50.772: CRYPTO_PKI: Found a subject match
*Mar 16 03:
#28:50.772: CRYPTO_PKI: ip-ext-val: IP extension validation not required:Incrementing refcount for cont
*Mar 16 03:28:50.773: CRYPTO_PKI: create new ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 35
*Mar 16 03:28:50.773: CRYPTO_PKI: (A069C)validation path has 1 certs

*Mar 16 03:28:50.773: CRYPTO_PKI: (A069C) Check for identical certs
```

*Mar 16 03:28:50.773: CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-
*Mar 16 03:28:50.774: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A
*Mar 16 03:28:50.774: CRYPTO_PKI: Cert record not found for issuer serial.
*Mar 16 03:28:50.774: CRYPTO_PKI : (A069C) Validating non-trusted cert
*Mar 16 03:28:50.774: CRYPTO_PKI: (A069C) Create a list of suitable trustpoints
*Mar 16 03:28:50.774: CRYPTO_PKI: crypto_pki_get_cert_record_by_issuer()
*Mar 16 03:28:50.774: CRYPTO_PKI: Found a issuer match
*Mar 16 03:28:50.774: CRYPTO_PKI: (A069C) Suitable trustpoints are: CA-GlobalSign-Root,
*Mar 16 03:28:50.775: CRYPTO_PKI: (A069C) Attempting to validate certificate using CA-GlobalSign-Root p
*Mar 16 03:28:50.775: CRYPTO_PKI: (A069C) Using CA-GlobalSign-Root to validate certificate
*Mar 16 03:28:50.775: CRYPTO_PKI(make trusted certs chain)
*Mar 16 03:28:50.775: CRYPTO_PKI: Added 1 certs to trusted chain.
*Mar 16 03:28:50.775: CRYPTO_PKI: Prepare session revocation service providers
*Mar 16 03:28:50.776: P11:C_CreateObject:
*Mar 16 03:28:50.776: CKA_CLASS: PUBLIC KEY
*Mar 16 03:28:50.776: CKA_KEY_TYPE: RSA
*Mar 16 03:28:50.776: CKA_MODULUS:
DA 0E E6 99 8D CE A3 E3 4F 8A 7E FB F1 8B 83 25
6B EA 48 1F F1 2A B0 B9 95 11 04 BD F0 63 D1 E2
<snip>
*Mar 16 03:28:50.780: CKA_PUBLIC_EXPONENT: 01 00 01
*Mar 16 03:28:50.780: CKA_VERIFY_RECOVER: 01
*Mar 16 03:28:50.780: CRYPTO_PKI: Deleting cached key having key id 45
*Mar 16 03:28:50.781: CRYPTO_PKI: Attempting to insert the peer's public key into cache
*Mar 16 03:28:50.781: CRYPTO_PKI:Peer's public inserted successfully with key id 46
*Mar 16 03:28:50.781: P11:C_CreateObject: 131118
*Mar 16 03:28:50.781: P11:C_GetMechanismInfo slot 1 type 3 (invalid mechanism)
*Mar 16 03:28:50.781: P11:C_GetMechanismInfo slot 1 type 1
*Mar 16 03:28:50.781: P11:C_VerifyRecoverInit - 131118
*Mar 16 03:28:50.781: P11:C_VerifyRecover - 131118
*Mar 16 03:28:50.781: P11:found pubkey in cache using index = 46
*Mar 16 03:28:50.781: P11:public key found is :
30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01
01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01
<snip>
CF 02 03 01 00 01
*Mar 16 03:28:50.788: P11:CEAL:CRYPTO_NO_ERR
*Mar 16 03:28:50.788: P11:C_DestroyObject 2:2002E
*Mar 16 03:28:50.788: CRYPTO_PKI: Expiring peer's cached key with key id 46
*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C) Certificate is verified
*Mar 16 03:28:50.788: CRYPTO_PKI: Remove session revocation service providers
*Mar 16 03:28:50.788: CRYPTO_PKI: Remove session revocation service providersCA-GlobalSign-Root:validat
*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C) Certificate validated without revocation check:cert refcount
*Mar 16 03:28:50.790: CRYPTO_PKI: Populate AAA auth data
*Mar 16 03:28:50.790: CRYPTO_PKI: Unable to get configured attribute for primary AAA list authorization
*Mar 16 03:28:50.790: PKI: Cert key-usage: Digital-Signature , Certificate-Signing , CRL-Signing
*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C)chain cert was anchored to trustpoint CA-GlobalSign-Root, and
*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Removing verify context
*Mar 16 03:28:50.790: CRYPTO_PKI: destroying ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 35, ref
*Mar 16 03:28:50.790: CRYPTO_PKI: ca_req_context released
*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Validation TP is CA-GlobalSign-Root
*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Certificate validation succeeded
*Mar 16 03:28:50.790: CRYPTO_OPSSL: Certificate verification is successful
*Mar 16 03:28:50.790: CRYPTO_PKI: Rcvd request to end PKI session A069C.
*Mar 16 03:28:50.790: CRYPTO_PKI: PKI session A069C has ended. Freeing all resources.:cert refcount aft
*Mar 16 03:28:50.791: <<< ??? [length 0005]

```
*Mar 16 03:28:50.791: 16 03 03 00 93
*Mar 16 03:28:50.791:
*Mar 16 03:28:50.791: SSL_connect:SSLv3/TLS read server certificate
*Mar 16 03:28:50.791: <<< TLS 1.2 Handshake [length 0093], ServerKeyExchange
*Mar 16 03:28:50.791: 0C 00 00 8F 03 00 17 41 04 3D 49 34 A3 52 D4 EB
*Mar 16 03:28:50.791: DE A2 9E CC B0 91 AA CB 1B 39 D0 26 1B 7D FF 31
*Mar 16 03:28:50.792: E0 D7 D5 9C 75 C0 7D 5B D6 B2 0A B5 CC EA E1 4B
*Mar 16 03:28:50.792: 4E E5 72 7B 54 5D 9B B2 95 91 E0 CC D6 A5 8E CE
*Mar 16 03:28:50.792: 8D 36 C9 83 42 B0 4D AC 0C 04 03 00 46 30 44 02
*Mar 16 03:28:50.792: 20 67 B3 F1 DA D1 BF 13 72 DD B6 B2 11 3B 6E 6F
*Mar 16 03:28:50.793: 87 52 D9 00 F7 44 31 C3 C2 5E BE 2D FF 93 4E F0
*Mar 16 03:28:50.793: A8 02 20 24 42 91 BE B7 10 1C D1 C0 12 28 FB 1F
*Mar 16 03:28:50.793: E4 DE 81 0B AA 66 19 CD 28 5A A0 30 7D 3C 4A 56
*Mar 16 03:28:50.793: 0D 94 E2
*Mar 16 03:28:50.793:
*Mar 16 03:28:50.794: P11:C_FindObjectsInit:
*Mar 16 03:28:50.794: CKA_CLASS: PUBLIC KEY
*Mar 16 03:28:50.794: CKA_KEY_TYPE: : 00 00 00 03

*Mar 16 03:28:50.794: CKA_ECDSA_PARAMS:
30 59 30 13 06 07 2A 86 48 CE 3D 02 01 06 08 2A
86 48 CE 3D 03 01 07 03 42 00 04 63 B6 D3 1A 28
<snip>

*Mar 16 03:28:50.796: P11:C_FindObjectsFinal
*Mar 16 03:28:50.796: P11:C_VerifyInit - Session found
*Mar 16 03:28:50.796: P11:C_VerifyInit - key id = 131073
*Mar 16 03:28:50.796: P11:C_Verify
*Mar 16 03:28:50.800: P11:CEAL:CRYPTO_NO_ERR
*Mar 16 03:28:50.800: <<< ??? [length 0005]
*Mar 16 03:28:50.800: 16 03 03 00 04
*Mar 16 03:28:50.800:
*Mar 16 03:28:50.800: SSL_connect:SSLv3/TLS read server key exchange
*Mar 16 03:28:50.800: <<< TLS 1.2 Handshake [length 0004], ServerHelloDone
*Mar 16 03:28:50.801: 0E 00 00 00
*Mar 16 03:28:50.801:
*Mar 16 03:28:50.801: SSL_connect:SSLv3/TLS read server done
*Mar 16 03:28:50.810: >>> ??? [length 0005]
*Mar 16 03:28:50.810: 16 03 03 00 46
*Mar 16 03:28:50.811:
*Mar 16 03:28:50.811: >>> TLS 1.2 Handshake [length 0046], ClientKeyExchange
*Mar 16 03:28:50.811: 10 00 00 42 41 04 26 C3 EF 02 05 6C 82 D1 90 B3
*Mar 16 03:28:50.811: 17 31 9A CD DD 8C 81 91 BA E8 C0 86 40 7B 2C E4
*Mar 16 03:28:50.811: 9A 2C 18 9D D1 6A C0 56 A0 98 2E B7 3B AB B3 EB
*Mar 16 03:28:50.811: BB CD 5E 42 C5 76 C0 C4 BF 15 F4 87 F2 7C AD 74
*Mar 16 03:28:50.812: 97 0A 97 2B 06 B5
*Mar 16 03:28:50.812:
*Mar 16 03:28:50.812: SSL_connect:SSLv3/TLS write client key exchange
*Mar 16 03:28:50.812: >>> ??? [length 0005]
*Mar 16 03:28:50.812: 14 03 03 00 01
*Mar 16 03:28:50.812:
*Mar 16 03:28:50.812: >>> TLS 1.2 ChangeCipherSpec [length 0001]
*Mar 16 03:28:51.116: >>> ??? [length 0005]
*Mar 16 03:28:51.116: 17 03 03 00 35
*Mar 16 03:28:51.116:
*Mar 16 03:28:51.116: >>> ??? [length 0005]
*Mar 16 03:28:51.116: 17 03 03 00 1A
*Mar 16 03:28:51.116:
*Mar 16 03:28:51.116: >>> ??? [length 0005]
*Mar 16 03:28:51.116: 17 03 03 00 30
*Mar 16 03:28:51.116:
*Mar 16 03:28:51.116: >>> ??? [length 0005]
```


*Mar 16 03:28:51.116: 17 03 03 00 1B
*Mar 16 03:28:51.117:
*Mar 16 03:28:51.713: <<< ??? [length 0005]
*Mar 16 03:28:51.713: 17 03 03 00 6D
*Mar 16 03:28:51.713:
*Mar 16 03:28:51.714: >>> ??? [length 0005]
*Mar 16 03:28:51.714: 17 03 03 00 1E
*Mar 16 03:28:51.714:
*Mar 16 03:28:51.732: <<< ??? [length 0005]
*Mar 16 03:28:51.732: 17 03 03 00 71
*Mar 16 03:28:51.732:

event manager run SendSecureEmailEEM*Mar 16 03:28:50.673: CRYPTO_OPSSL:
Zugewiesener Speicher für OPSSLContext*Mar 16 03:28:50.673: CRYPTO_OPSSL:
Verschlüsselungsspezifikationen maskieren 0x0 2FC000 für Version 128*Mar 16 03:28:50.674:
EC-Standardkurvenliste festlegen: 0x70EC-Kurvenliste festlegen:
secp521r1:secp384r1:prime256v1*Mar 16 03:28:50.674: opssl_SetPKInfo entry*Mar 16
03:28:50.674: CRYPTO_PKI: (A069B) Sitzung gestartet - Identität ausgewählt (TP-selbst-signiert-
486541296)xTP-selbst-signiert-486541296:refcount after increment ment = 1*Mar 16
03:28:50.674: CRYPTO_PKI: Beginn des lokalen Abrufs der Zertifikatskette.*Mar 16 03:28:50.674:
CRYPTO_PKI(Zertifikatsuche) emitter="cn=IOS-Self-Signed-Certificate-486541296"
Seriennummer= 01*Mar 16 03:28:50.674: CRYPTO_PKI: Suche nach Zertifikat im
Griff=7F41EE523CE0, Digest=1C 7F 3D 52 67 66 D5 59 E2 66 58 E7 8B7 E7 B 8E*Mar 16
03:28:50.675: CRYPTO_PKI: Fertig mit lokalem Zert.-Abruf 0.*Mar 16 03:28:50.675:
CRYPTO_PKI: Anfrage zum Beenden der PKI-Sitzung A069B.*Mar 16 03:28:50.675:
CRYPTO_PKI: PKI-Sitzung A069B wurde beendet. Alle Ressourcen werden freigegeben.TP-self-
signed-486541296:unlocked trustpoint TP-self-signed-486541296, refcount is 0*Mar 16
03:28:50.675: opssl_SetPKInfo done.*Mar 16 03:28:50.675: CRYPTO_OPSSL: Common Criteria
ist in dieser Sitzung deaktiviert.Deaktivieren der Common Criteria-Modusfunktion in CiscoSSL
unter SSL CTX 0x7F41F28EAF8*Mar 16 03:28:50.675: CRYPTO_OPSSL: ciphersuites ECDHE-
RSA-AES256-GCM-SHA 384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-
SHA384:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA256:AES256-GCM-
SHA384:AES256-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-
SHA 256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-
SHA256:AES128-GCM-SHA256:AES128-SHA256*16.03:28:50.676: Handshake-Start: vor SSL-
Initialisierung*16.03:28:50.676: SSL_connect:vor SSL-Initialisierung*16.03:28:50,676: >>> ???
[length 0005]*Mär 16 03:28:50.676: 16 03 01 00 95*Mär 16 03:28:50.676: *Mär 16 03:28:50.676:
>>> TLS 1.2 Handshake [länge 0095], ClientHello*Mar 16 03:28:50.676: 01 00 00 91 03 03 26 4B
9F B3 44 94 FD 5F FD A1<snip>*Mar 16 03:28:50.679: 03 03 01 02 01*16.03:28:50.679:
*16.03:28:50.679: SSL_connect:SSLv3/TLS write client hello*Mar 16 03:28:50.692: <<< ???
[length 0005]*Mar 16 03:28:50.692: 16 03 03 00 3F*Mar 16 03:28:50.692: *Mar 16 03:28:50.692:
SSL_connect:SSLv3/TLS write client hello*Mar 16 03:28:50.692: << TLS 1.2 Handshake [length
003F], ServerHello*Mar 16 03:28:50.692: 02 00 00 3B 03 03 64 12 7E 05 25 F6 7A BD A0 2E*Mär
16 03:28:50.692: 58 83 12 7F 90 CD F4 AB E2 69 53 A8 C7 FC 44 4F*Mär 16 03:28:50.692: 57
4E 47 52 44 01 00 C0 2B 00 00 13 00 17 00 00*Mär 16 03:28:50.693: FF 01 00 01 00 00 0B 00 0
0 0 2 01 00 00 23 00 00*16. März 03:28:50.693: TLS-Servererweiterung "unbekannt" (id=23),
len=0TLS-Servererweiterung "neu verhandeln" (id=65281), len=1*16. März 03:28:50.693: 00*16.
März 03:28:50.693: TLS-Servererweiterung "EC point formats" (id=11), len=2*16. März
03:28:50.693: 01 00*16. März 03:28:50.693: TLS-Servererweiterung "session ticket" (id=35),

len=0*Mar 16 03:28:50.693: <<< ??? [length 0005]*Mar 16 03:28:50.693: 16 03 03 0F 9A*Mar 16 03:28:50.694: *Mar 16 03:28:50.702: SSL_connect:SSL v3/TLS Server lesen hello*Mar 16 03:28:50.702: << TLS 1.2 Handshake [length 0F9A], Certificate*Mar 16 03:28:50.702: 0B 00 0F 96 00 0F 93 00 0 0 4 8A 30 82 04 86 30 82*Mar 16 03:28:50.702: 03 6E A0 03 02 01 02 02 10 52 87 E0 40 A4 FE F7<snip>*Mar 16 03:28:50.763: 82 35 CF 62 8B C9 24 8B A5 B7 39 0C BB 7E 2A 41*Mar 16 03:28:50.763: BF 52 CF FC A2 96 B6 C2 82 3F*Mar 16 03:28:50.763: *16. März 03:28:50.765: CC_DEBUG: Rückruffunktion der Shim-Layer-App*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Sitzung gestartet - Identität nicht angegeben*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Peer-Zertifikat hinzufügen*Mar 16 03:28:50.767: CRYPTO_PKI: x509-Peer-Zertifikat hinzugefügt - (11) 162) Bytes*Mar 16 03:28:50.767: CRYPTO_PKI: (A069C) Hinzufügen eines Peer-Zertifikats*Mar 16 03:28:50.768: CRYPTO_PKI: x509-Peer-Zertifikat hinzugefügt - (116) 434) Bytes*Mar 16 03:28:50.768: CRYPTO_PKI: (A069C) Hinzufügen eines Peer-Zertifikats*Mar 16 03:28:50.770: CRYPTO_PKI: x509-Peer-Zertifikat hinzugefügt - (11) 382) Bytes*Mar 16 03:28:50.770: CRYPTO_OPSSL: Validate Certificate Chain Callback*Mar 16 03:28:50.770: CRYPTO_PKI(CERT Lookup) emittent="cn=GTS CA 1C3,o=Google Trust Services LLC,c=US" Seriennummer= 52 87 E0 40 A4 FE F7 07 12 68 B0 4F DD F0 F4*Mar 16 03:28:50.770: CRYPTO_PKI: such for cert in handle=7F41EE523CE0, digest=A7 CC 4B 0F 36 C3 AC D1 2F 77 DD 1D 9A 37 DC FC*Mär 16 03:28:50.770: CRYPTO_PKI(CERT-Suche) emittierende="cn=GTS Root R1,o=Google Trust Services LLC,c=US" Seriennummer = 02 03 BC 53 59 6B 34 C7 18 F5 01 50 66*Mar 16 03:28:50.771: CRYPTO_PKI: Suche nach Zertifikat im Handle=7F41EE523CE0, Digest=03 9F 59 82 EE 09 CC 4F 53 AE D8 02 7E 4B AF*Mar 16 03:28:50.771: CRYPTO_PKI(CERT-Suche) emittent="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-sa,c=BE Seriennummer= 77 BD 0D 6C DB 36 F9 1A EA 21 0F C4 F0 58 D3 0D*Mär 16 03:28:50.771: CRYPTO_PKI: Suche nach Zertifikat im Handle=7F41EE523CE0, digest=94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A*Mar 16 03:28:50.771: CRYPTO_PKI: Zertifikatseintrag nicht für Herausgeber gefunden (Serie).*Mar 16 03:28:50.772: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()*Mar 16 03:28:50.772: CRYPTO_PKI: Sucht eine Betreffübereinstimmung*Mar 16 03:28:50.772: CRYPTO_PKI: ip-ext-val: IP Verlängerungvalidierung nicht erforderlich:Erhöhung der Anzahl der Antworten für Kontext-ID-35 auf 1*Mär 16 03:28:50.773: CRYPTO_PKI: Neuer ca_req_context-Typ PKI_VERIFY_CHAIN_CONTEXT,ident 35*Mär 16 03:28:50.773: CRYPTO_PKI: (A069C)Validierungspfad hat 1 certs*Mar 16 03:28:50.773: CRYPTO_PKI: (A069C) Identische Zertifikate prüfen*Mar 16 03:28:50.773: CRYPTO_PKI(CERT Lookup) emittent="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-sa,c=BE" serial number= 77 BD 0D 6C DB 36 F9 1A EA 21 0F C4 F0 58 D3 0D*Mar 16 03:28:50.774: CRYPTO_PKI: sucht Zertifikat im Griff=7F41EE523CE0, Digest=94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A*Mar 16 03:28:50.774: CRYPTO_PKI: Zertifikatdatensatz für Herausgeber-Seriennummer nicht gefunden.*16.03:28:50.774: CRYPTO_PKI : (A069C) Validating non-trusted cert*16.03:28:50.774: CRYPTO_PKI I: (A069C) Erstellen Sie eine Liste geeigneter Vertrauenspunkte*Mar 16 03:28:50.774: CRYPTO_PKI: crypto_pki_get_cert_record_by_emittent()*Mar 16 03:28:50.774: CRYPTO_PKI I: Treffer gefunden*Mar 16 03:28:50.774: CRYPTO_PKI: (A069C) Geeignete Trustpoints sind: CA-GlobalSign-Root,*Mar 16 03:28:50.775: CRYPTO_PKI: (A 069C) Versuch, ein Zertifikat mithilfe der CA-GlobalSign-Root-Richtlinie zu validieren*Mär 16 03:28:50.775: CRYPTO_PKI: (A069C) Verwendung der CA-GlobalSign-Root zur Validierung eines Zertifikats*Mär 16 03:28:50.775: CRYPTO_PKI(make trusted certs chain)*16. März 03:28:50.775: CRYPTO_PKI: 1 Zertifikate zur vertrauenswürdigen Kette hinzugefügt.*16. März 03:28:50.775: CRYPTO_PKI: Sitzungsverweigerung vorbereiten service providers*Mar 16 03:28:50.776:

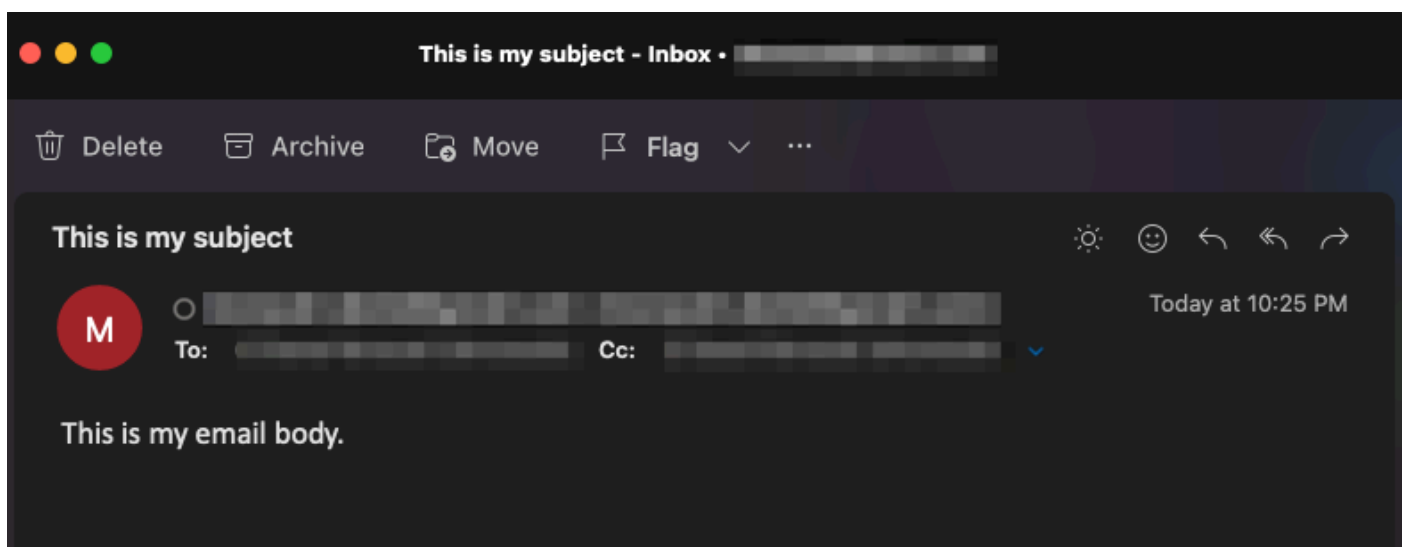
P11:C_CreateObject:*Mar 16 03:28:50.776: CKA_CLASS: PUBLIC KEY*Mar 16 03:28:50.776:
CKA_Mar KEY_TYPE: RSA*Mar 16 03:28:50.776: CKA_MODULUS: DA 0E E6 99 8D CE A3 E3
4F 8A 7E FB F1 8B 83 25 6B EA 48 1F F1 2A B0 B9 95 11 04 BD F0 63 D1 E2 <snip>*Mar 16
03:28:50.780: CKA_PUBLIC_EXPONENT: 01 00 01*Mar 16 03:28:50.780:
CKA_VERIFY_RECOVER: 01*Mar 16 03:28:50.780: CRYPTO_PKI: Cache-Schlüssel mit
Schlüssel-ID löschen 45*Mär 16 03:28:50.781: CRYPTO_PKI: Versuch, den öffentlichen Schlüssel
des Peers in den Cache einzufügen*Mär 16 03:28:50.781: CRYPTO_PKI:Peer's public insered
successfully with key id 46*Mar 16 03:28:50.781: P11:C_CreateObject: 131118*Mar 16
03:28:50.781: P11:C_GetMechanismInfo Steckplatz 1 Typ 3 (ungültiger Mechanismus)*Mar 16
03:28:50.781: P11:C_GetMechanismInfo Steckplatz 1 Typ 1*Mar 16 03:28:50.781:
P11:C_VerifyRecoverNit - 131118*Mar 16 03:28:50.781: P11:C_VerifyRecover - 131118*Mar 16
03:28:50.781: P11:found pubkey in cache using index = 46*Mar 16 03:28:50.781: P 11:öffentlicher
Schlüssel: 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 00 03 82 01 0F 00 30 82 01 0A
02 82 01 01 <snip>CF 02 03 01 00 01*Mar 16 03:28:50.788: P11:CEAL:CRYPTO_NO_ERR*Mar
16 03:28:50.788: P11:C_DestroyObject 2:2002E*Mar 16 03:28:50.788: CRYPTO_PKI:
Auslaufender zwischengespeicherter Peer-Schlüssel mit Schlüssel-ID 46*Mar 16 03:28:50.788:
CRYPTO_PKI: (A069C) Zertifikat ist verifiziert * Mär 16 03:28:50.788: CRYPTO_PKI: Remove
session revocation service providers*Mar 16 03:28:50.788: CRYPTO_PKI: Remove session
revocation service providersCA-GlobalSign-Root:validation status -
CRYPTO_VALID_CERT_WITH_WARNING*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C)
Zertifikat ohne Widerrufsprüfung validiert:cert refcount after increment = 1*Mar 16 03:28:50.790:
CRYPTO_PKI: AAA-Authentifizierungsdaten ausfüllen*Mar 16 03:28:50.790: CRYPTO_PKI:
Konfiguriertes Attribut für primäre AAA-Listenautorisierung kann nicht abgerufen werden.*Mar 16
03:28:50.790: PKI: Zertifikatschlüsselverwendung: Digitale Signatur , Zertifikatssignierung , CRL-
Signierung*16. März 03:28:50.790: CRYPTO_PKI: (A069C)chain cert was verankert to trustpoint
CA-GlobalSign-Root, and chain validation result was:
CRYPTO_VALID_CERT_WITH_WARNING*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Verify
context*Mar 16 03:28:50.790: CRYPTO_PKI: destroy ca_req_context type
PKI_VERIFY_CHAIN_CONTEXT,ident 35, ref count 1:Dekrementieren refcount for context id-35 to
0*Mar 16 03:28:50.790: CRYPTO_PKI: ca_req_context published*Mar 16 03:28:50.790:
CRYPTO_PKI: (A069C) Validierung TP ist CA-Global Sign-Root*Mar 16 03:28:50.790:
CRYPTO_PKI: (A069C) Zertifikatsvalidierung erfolgreich*Mar 16 03:28:50.790: CRYPTO_OPSSL:
Zertifikatsverifizierung erfolgreich*Mar 16 03:28:50.790: CRYPTO_PKI: Empf. Anfrage zum
Beenden der PKI-Sitzung A069C.*16. März 03:28:50.790: CRYPTO_PKI: PKI-Sitzung A069C
wurde beendet. Freigabe aller Ressourcen.:cert refcount after decment = 0*Mar 16 03:28:50.791:
<<< ??? [length 0005]*Mar 16 03:28:50.791: 16 03 03 00 93*Mar 16 03:28:50.791: *Mar 16
03:28:50.791: SSL_connect:SSLv3/TLS Serverzertifikat lesen*Mar 16 03:28:50.791: << TLS 1.2
Handshake [length 0093], ServerKeyExchange*Mar 16 03:28:50.791: 0C 00 00 8F 03 0 0 17 41
04 3D 49 34 A3 52 D4 EB*Mär 16 03:28:50.791: DE A2 9E CC B0 91 AA CB 1B 39 D0 26 1B 7D
FF 31*Mär 16 03:28:50.792: E0 D7 D5 9C 75 C0 7D 5B D6 B2 0A B5 CC EA E1 4B*Mär 16
03:28:50.792: 4E E5 72 7B 54 5D 9B2 95 91 E0 CC D6 A5 8E CE*Mar 16 03:28:50.792: 8D 36
C9 83 42 B0 4D AC 0C 04 03 00 46 30 44 02*Mar 16 03:28:50.792: 20 67 B3 F1 DA D1 BF 13 72
DD B6 B2 11 3B 6E 6F*Mär 16 03:28:50.793: 87 52 D9 00 F7 44 31 C3 C2 5E BE 2D FF 93 4E
F0*Mär 16 03:28:50.793: A8 02 20 24 42 91 BE B7 10 1C D1 C0 12 28 FB 1F*Mär 16
03:28:50.793: E4 DE 81 0B AA 66 19 CD 28 5A A0 30 7D 3C 4A 5 * Mär 16 03:28:50.793: 0D 94
E2 * Mär 16 03:28:50.793: *Mär 16 03:28:50.794: P11:C_FindObjectsInit:*Mar 16 03:28:50.794:
CKA_CLASS: PUBLIC KEY*Mar 16 03:28:50.794: CKA_KEY_TYPE: : 00 00 00 03*Mar 16

```

03:28:50.79 4: CKA_ECDSA_PARAMS: 30 59 30 13 06 07 2A 86 48 CE 3D 02 01 06 08 2A 86 48
CE 3D 03 01 07 03 42 00 04 63 B6 D3 1A 28 p>*Mär 16 03:28:50.796:
P11:C_FindObjectsFinal*Mär 16 03:28:50.796: P11:C_VerifyInit - Sitzung gefunden*Mär 16
03:28:50.79 6: P11:C_VerifyInit - Schlüssel-ID = 131073*Mar 16 03:28:50.796: P11:C_Verify*Mar
16 03:28:50.800: P11:CEAL:CRYPTO_NO_ERR*Mar 11 6.03:28:50.800: <<< ??? [length
0005]*Mar 16 03:28:50.800: 16 03 00 04*Mar 16 03:28:50.800: *Mar 16 03:28:50.800:
SSL_connect:SSLv3/TLS lesen server key exchange*Mar 16 03:28:50.800: << TLS 1.2
Handshake [length 0004], ServerHelloDone*Mar 16 03:28:50.801: 0E 00 00 0 00*Mar ar 16
03:28:50.801: *Mar 16 03:28:50.801: SSL_connect:SSLv3/TLS Read server done*Mar 16
03:28:50.810: >> ??? [length 0005]*Mar 16 03:28:50.810: 16 03 03 00 46*Mar 16 03:28:50.811:
*Mar 16 03:28:50.811: >>> TLS 1.2 Handshake [length 0046], ClientKeyExchange*Mar 16
03:28:50.811: 10 00 00 42 41 04 26 C3 EF 02 05 6C 82 D1 90 B3*Mar 16 03:28:50.811: 17:31 9A
CD DD 8C 81 91 BA E8 C0 86 40 7B 2C E4*Mär 16 03:28:50.811: 9A 2C 18 9D D1 6A C0 56 A0
98 2E B7 3B AB B3 EB*Mär 16 03:28:50.811: BB CD 5E 42 C5 76 C0 C4 BF 15 F4 87 F2 7C AD
74*Mär 16 03:28:50.812: 97 0A 97 2B 0 6 B5*Mar 16 03:28:50.812: *Mar 16 03:28:50.812:
SSL_connect:SSLv3/TLS write client key exchange*Mar 16 03:28:50.812: >>> ??? [length
0005]*Mar 16 03:28:50.812: 14 03 00 01*Mar 16 03:28:50.812: *Mar 16 03:28:50.812: >>> TLS
1.2 ChangeCipherSpec [length 0001]*Mar 16 03:28:51.116: >>> ??? [length 0005]*Mär 16
03:28:51.116: 17 03 03 00 35*Mär 16 03:28:51.116: *Mär 16 03:28:51.116: >>> ??? [length
0005]*Mär 16 03:28:51.116: 17 03 03 00 1A*Mär 16 03:28:51.116: *Mär 16 03:28:51.116: >>> ???
[length 0005]*Mär 16 03:28:51.116: 17 03 03 00 30*Mär 16 03:28:51.116: *Mär 16 03:28:51.116:
>>> ??? [length 0005]*Mar 16 03:28:51.116: 17 03 03 00 1B*Mar 16 03:28:51.117: *Mar 16
03:28:51.713: <<<< ??? [length 0005]*Mar 16 03:28:51.713: 17 03 03 00 6D*Mar 16
03:28:51.713: *Mar 16 03:28:51.714: >>> ??? [length 0005]*Mär 16 03:28:51.714: 17 03 03 00
1E*Mär 16 03:28:51.714: *Mär 16 03:28:51.732: <<< ??? [Länge 0005]*Mär 16 03:28:51.732: 17
03 03 00 71*Mär 16 03:28:51.732:

```

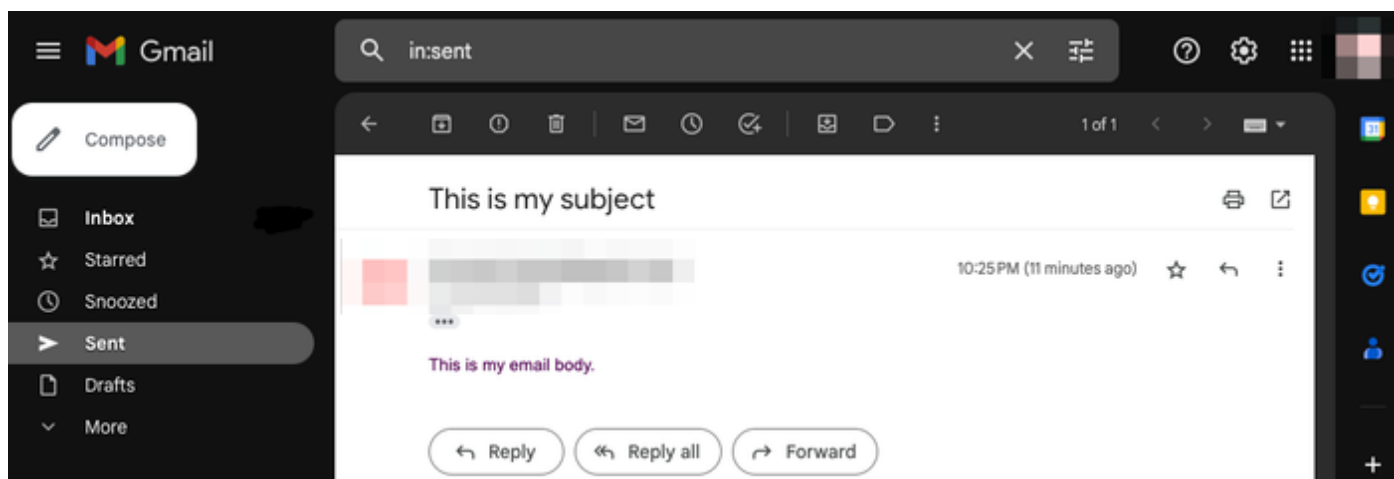
Sie können überprüfen, ob die E-Mail empfangen wurde und alle Felder (an, von, CC, Betreff, Text) korrekt ausgefüllt sind:



Sie können auch überprüfen, ob der TLS-Handshake und die TLS-Sitzung von der Paketerfassung auf dem Cisco IOS XE-Gerät (angehängt als "WorkingSMTPwithTLS.pcap") stattgefunden haben:

No.	Time	Source	Destination	Protocol	Length	ID	Info
11	2023-03-16 03:28:50...	10.122.144.150	142.251.163.109	TLSv1.2	208	0x8790 (34704)	Client Hello
12	2023-03-16 03:28:50...	142.251.163.109	10.122.144.150	TLSv1.2	590	0x7641 (30273)	Server Hello
32	2023-03-16 03:28:50...	142.251.163.109	10.122.144.150	TLSv1.2	439	0x7649 (30281)	Certificate, Server Key Exchange, Server Hello Done
33	2023-03-16 03:28:50...	10.122.144.150	142.251.163.109	TLSv1.2	180	0x879d (34717)	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
34	2023-03-16 03:28:50...	142.251.163.109	10.122.144.150	TLSv1.2	349	0x764a (30282)	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
36	2023-03-16 03:28:50...	10.122.144.150	142.251.163.109	TLSv1.2	107	0x879f (34719)	Application Data
38	2023-03-16 03:28:50...	142.251.163.109	10.122.144.150	TLSv1.2	306	0x764c (30284)	Application Data
39	2023-03-16 03:28:50...	10.122.144.150	142.251.163.109	TLSv1.2	116	0x87a0 (34720)	Application Data
41	2023-03-16 03:28:50...	142.251.163.109	10.122.144.150	TLSv1.2	101	0x764e (30286)	Application Data
42	2023-03-16 03:28:50...	10.122.144.150	142.251.163.109	TLSv1.2	109	0x87a1 (34721)	Application Data

Sie können sogar überprüfen, ob die E-Mails im Ordner "Gesendet" des verwendeten E-Mail-Kontos angezeigt werden:



Weitere Hinweise und Überlegungen

Benutzernamen mit @ Symbolen

Beim Versuch, einen SMTP-Relay zu verwenden, können Probleme auftreten. Aufgrund des SMTP-Relays hat die Serverzeichenfolge dieses Format (ein "@" im Benutzernamen):

```
event manager environment _email_server email.relay@My.Domain.Name:MyPasswordString@smtp-relay.gmail.com
```

Der Code zum Analysieren von Benutzername und Kennwort teilt die Zeichenfolge beim ersten Auftreten des "@"-Symbols auf. Das System geht davon aus, dass der Server-Hostname unmittelbar nach dem ersten "@"-Symbol durch den Rest der Zeichenfolge beginnt und interpretiert alles davor als "username:password".

Die TCL-Implementierung von SMTP verwendet einen regulären Ausdruck (Regex), der diese Benutzername/Kennwort/Serverinformationen unterschiedlich behandelt. Aufgrund dieses Unterschieds lässt TCL Benutzernamen mit dem Symbol "@" zu. Cisco IOS XE TCL unterstützt jedoch keine Krypto-Funktion, sodass es keine Option zum Senden sicherer E-Mails über TLS gibt.

Zusammenfassung:

- Wenn die E-Mail sicher sein muss, können Sie sie nicht mit TCL senden.
- Wenn Ihr Benutzername ein "@" enthält, können Sie dieses nicht mit einem EEM senden.

Die Cisco Bug-ID [CSCwe75439](#) wurde abgelegt, um diese Möglichkeit zur Verbesserung der EEM-E-Mail-Funktion zu adressieren. Es gibt derzeit jedoch keine Roadmap für diese Erweiterungsanfrage.

Schlussfolgerung

Wie hier gezeigt, ist es mithilfe des Embedded Event Manager (EEM)-Applets möglich, sichere E-Mails über SMTP mit TLS zu senden. Es erfordert eine gewisse Einrichtung auf Serverseite sowie die Konfiguration der erforderlichen Zertifikate, um Vertrauenswürdigkeit zu ermöglichen. Es ist jedoch machbar, wenn Sie automatisierte, sichere E-Mail-Benachrichtigungen generieren möchten.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.