

EEM을 활용하여 사용자에게 보내는 보안 이메일 자동화

목차

- [소개](#)
 - [사용 사례](#)
 - [배경](#)
 - [Gmail 계정 설정](#)
 - [기본 EEM 컨피그레이션](#)
 - [기본 인증서만 설치된 상태에서 문제가 발견됨](#)
 - [SMTP 보안을 위한 인증서](#)
 - [인증서를 찾는 더 쉬운 방법](#)
 - [Secure SMTP로 EEM 다시 테스트](#)
 - [기타 주의 사항 및 고려 사항](#)
 - [기호@사용자 이름](#)
 - [결론](#)
-

소개

이 문서에서는 Cisco IOS® XE 내의 EEM(Embedded Event Manager)에서 "메일 서버" 작업을 사용하여 포트 587에서 TLS(Transport Layer Security)를 사용하여 SMTP(Simple Mail Transfer Protocol) 서버로 보안 이메일을 보내는 데 필요한 프로세스에 대해 설명합니다.

이 과정에서 발생할 수 있는 많은 주의 사항이 있으며, 이것이 이 문서를 작성하는 이유는 이 작업을 수행하는 데 필요한 단계를 문서화하기 위해서입니다.

사용 사례

많은 고객이 특정 이벤트가 발생한 후 자동으로 이메일 알림을 받을 수 있는 가치를 알고 있습니다. EEM 하위 시스템은 네트워크 이벤트 감지 및 온보드 자동화를 위한 강력한 도구이며 Cisco IOS XE 디바이스에서 이메일 알림을 자동화하는 효율적인 방법을 제공할 수 있습니다. 예를 들어, IPSLA 트랙을 모니터링하고, 상태 변경을 나타내는 syslog에 대한 응답으로 일종의 작업을 수행하고 네트워크 관리자에게 이메일을 통해 이벤트를 알릴 수 있습니다. 이 "이메일 알림" 아이디어는 강조하고 싶은 특정 이벤트에 주의를 환기시키는 수단으로 다른 여러 시나리오에 적용될 수 있습니다.

배경

PEM은 "Privacy Enhanced Mail"의 약자로, 인증서 및 키를 나타내는 데 자주 사용되는 형식입니다. Cisco IOS XE 디바이스에서 사용하는 인증서 형식입니다. 보안 애플리케이션(예: HTTPS 또는 보안 SMTP)에는 "Stacked PEM"이 있는 경우가 많습니다. 여기에는 다음과 같은 여러 인증서가 포

합됩니다.

- 루트 인증서
- 서명(중간) 인증서
- 최종 사용자(또는 서버) 인증서

Gmail 계정 설정

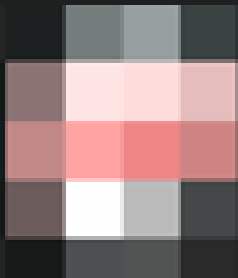
이 글에서는 구글의 SMTP 서비스가 예시로 사용될 것이다. 사전 요구 사항은 이전에 설정된 Gmail 계정을 가지고 있는 것입니다.

Google은 원격 클라이언트에서 Gmail로 이메일을 보낼 수 있습니다. 예전에는 Gmail에 "안전하지 않은 앱"에 대한 설정이 있었고, Google의 쪽에서 이 설정을 허용하지 않으면 응용 프로그램에서 오류가 발생합니다. 이 설정이 제거되었으며 그 자리에 "보안 응용 프로그램" 옵션이 있습니다. 이 옵션은 다음을 통해 액세스할 수 있습니다.

mail.google.com > 프로필(#1) > Google 계정 관리(#2) > 보안(#3) > Google 로그인 방법 > 2단계 인증(#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]



이 페이지에서 2단계 검증이 켜져 있는지 확인합니다.

← 2-Step Verification



그런 다음 "앱 암호"로 스크롤하면 Gmail에서 2단계 확인을 지원하지 않는 응용 프로그램에서 Google 계정에 로그인하는 데 사용할 수 있는 암호를 생성하도록 할 수 있습니다.

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.

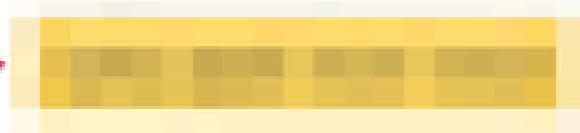
Select app

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

이 스크린샷의 16글자 애플리케이션 비밀번호는 개인 지메일 계정과 연동돼 흐릿하게 지워졌다. 이제 Gmail에 대한 응용 프로그램 암호가 있으므로 Gmail 계정 이름과 함께 이 암호를 전자 메일 전

달에 사용할 전자 메일 서버로 사용할 수 있습니다. 서버를 지정하는 형식은 "username:password@host"입니다.

기본 EEM 컨피그레이션

정확한 요구 사항에 맞게 EEM 스크립트를 사용자 지정할 수 있는 여러 방법이 있지만, 이 예는 보안 이메일 기능을 실행하기 위한 기본 EEM 스크립트입니다.

```
(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 "$_email_from" cc "$_email_cc"
```

컨피그레이션에서는 먼저 _email_from, _email_to 및 _email_server의 세 가지 EEM 환경 변수를 생성합니다. 컨피그레이션 변경을 더 쉽게 하기 위해 각 컨피그레이션을 변수에 정의합니다. 그런 다음 SendSecureEmailEEM 스크립트를 만듭니다. 여기서 트리거링 이벤트는 "none"이므로 특정 이벤트가 트리거될 때까지 기다리는 대신 "# event manager run SendSecureEmailEEM"을 사용하여 EEM 스크립트를 원하는 대로 수동으로 실행할 수 있습니다. 다음으로, 이메일 생성을 처리하는 단일 "메일 서버" 작업만 수행할 수 있습니다. "secure tls" 및 "port 587" 옵션은 디바이스에서 Gmail 서버가 수신할 포트 587의 TLS를 협상하도록 지정합니다.

또한 "from" 필드가 유효한지 확인해야 합니다. "Alice"로 인증하지만 "Bob"에서 보낸 전자 메일을 보내려고 하면 Alice가 다른 사람의 전자 메일 주소를 스푸핑하기 때문에 오류가 발생합니다. "보낸 사람" 필드는 서버에서 이메일을 보내는 데 사용되는 계정과 일치해야 합니다.

기본 인증서만 설치된 상태에서 문제가 발견됨

EEM은 openssl을 사용하여 SMTP 서버에 연결합니다. 안전한 통신을 위해 서버는 Cisco IOSd에서 실행 중인 openssl에 인증서를 다시 전송합니다. 그러면 IOSd에서 해당 인증서와 연결된 신뢰 지점을 찾습니다.

Cisco IOS XE 디바이스에서는 Gmail SMTP 서버의 인증서가 기본적으로 설치되지 않습니다. 신뢰를 설정하려면 수동으로 가져와야 합니다. 인증서가 설치되지 않은 경우 "불량 인증서"로 인해 TLS 핸드셰이크가 실패합니다.

이러한 디버깅은 인증서 문제를 디버깅하는 데 매우 유용합니다.

```
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
```

EEM이 트리거될 때 라우터에서 EPC(Embedded Packet Capture)를 시작하여 이메일 서버를 오가는 트래픽을 캡처할 수 있습니다.

```
! 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-
*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: >>> TLS 1.2 Alert [length 0002], fatal bad_certificate
*Mar 15 21:51:32.800: 02 2A
*Mar 15 21:51:32.800: SSL3 alert write:fatal:bad certificate
*Mar 15 21:51:32.801: P11:C_OpenSession 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
```

궁극적으로 openssl은 SMTP 서버와의 보안 TLS 세션을 설정할 수 없으므로 EEM 실행을 중지하는 "불량 인증서" 오류가 발생합니다.

```
*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
```

이 교환에서 문서화된 패킷 캡처는 "NoCertificateInstalled.pcap"로 연결됩니다. 라우터 (10.122.x.x)에서 Gmail SMTP 서버(142.251.163.xx)로의 최종 TLS 패킷에서는 이전에 디버그에 표시된 것과 동일한 "Bad Certificate" 메시지로 인해 TLS 협상이 종료되었음을 보여 줍니다.

```
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
TLV1.2 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)
```

SMTP 보안을 위한 인증서

Cisco IOS XE 디바이스에서 Gmail의 서버를 신뢰하도록 하는 인증서가 없으므로, 이 중 하나/모든 인증서를 디바이스의 신뢰 지점에 설치하는 것이 해결책입니다.

예를 들어, 이전 테스트의 전체 디버그는 수행된 다음 인증서 조회를 보여줍니다.

```
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=
```

디바이스에서 Gmail SMTP 서버와의 보안 세션을 설정할 수 있도록 이러한 발급자 각각에 대한 인증서를 신뢰 지점 아래에 설치해야 합니다. 다음 컨피그레이션을 사용하여 각 발급자에 대한 신뢰 지점을 생성할 수 있습니다.

```
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
```

이제 설정된 각 발급자에 대한 신뢰 지점이 있지만 아직 연결된 실제 인증서가 없습니다. 기본적으로 다음과 같은 빈 신뢰 지점입니다.

```
# 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
```

이러한 인증서의 위치를 추적한 다음 디바이스에 설치해야 합니다.

온라인에서 "Google Trust Services 1C3"를 검색하면 Google Trust Services Repository of certificates를 빠르게 볼 수 있습니다.

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

해당 페이지에서 모든 인증서를 확장한 후 "1C3"를 검색하고 "Action" 드롭다운을 클릭한 다음 PEM 인증서를 다운로드할 수 있습니다.

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:f8:13: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:8c: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		

다운로드한 PEM 파일을 텍스트 편집기로 열면 이전에 생성한 신뢰 지점 아래의 Cisco IOS XE 디바이스로 가져올 수 있는 인증서일 뿐입니다.

```
-----BEGIN CERTIFICATE-----
MIIF1jCCA36gAwIBAgINAg08U11rNmCY9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2x1IFRydXN0IFN1cnZpY2VzIEExMQzEU
<snip>
AJ2xDx8hcFH1mt0G/FX0Kw4zd8NLQsLxdxP8c4CU6x+7Nz/OAipmsHMDmQybdKw
juDEI/9bfU11cKwrmz302+BtjjKAvpafkm0817tdufThcV4q508DIrGKZTqPwJN1
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDB1Hz4n/FsRC6UfTd
```

-----END CERTIFICATE-----

"CA-GTS-1C3" 신뢰 지점 아래에서 컨피그레이션 명령을 사용하여 가져올 수 있습니다.

```
(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

```
MIIFljCCA36gAwIBAgINAg08U1lrNMcy9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw  
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2x1IFRydXN0IFN1cnZpY2VzIExMQzEU  
<snip>  
juDEI/9bfU1lcKwrmz302+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)#
```

그런 다음 인증서가 설치되었는지 확인할 수 있습니다.

```
# 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 ECBOE38D 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

다음으로 다른 두 발급자에 대한 인증서를 설치할 수 있습니다.

CA-GTS-Root-R1:

설정:

[스포일러](#) (읽으려면 강조 표시)

```
(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+gAwIBAgINAgP1k28xsBNJiGuiFzANBgkqhkiG9w0BAQwFADBHMQsw  
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2x1IFRydXN0IFN1cnZpY2VzIEExMQzEU  
<snip>  
2tIMPNUzjSmhDYAPexZ3FL//2wmUsp08IFgV6dtxQ/PeEMMA3Kgg1bbC1j+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 authenticate CA-GTS-Root-R1Base 64 encoded CA 인증서를 입력합니다. 빈 줄 또는 "quit"이라는 단어를 스스로 줄로 종료합니다

.MIIFVzCCAz+gAwIBAgINAgPlk28xsBNJiGuiFzANBgkqhkiG9w0BAQwFADBHMQswCQYDVQGEwJVUz29vZ2XLifr

ydXN0IFNlcnZpY2VzIExMQzEU<snip>2tIMPNuzjsmhDYAPexZ3FL//2wmUspO8IFgV6dtxQ/PeEMMA3KQ

has the attribute: Fingerprint MD5: 05FED0FED 0FED 0MD 0FED 0FED 0FEDFED 0Z3 1A8A376 63DA01E0 D852DC40 지문 SHA1: E58C1CC4 913B3863 4BE9106E3AD8E6B 9DD9814A% 이 인증서를 수락하십니까? [yes/no]: yesTrustpoint CA 인증서가 수락되었습니다.% 인증서를 성공적으로 가져왔습니다(config)# 끝

Running-config 확인:

[스포일러](#) (읽으려면 강조 표시)

```
# 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(실행 표시) | sec crypto pki 인증서 체인 CA-GTS-Root-R1crypto pki 인증서 체인 CA-
GTS-Root-R1 인증서 ca 0203E5936F31B01349886BA217 30820557 3082033F A0030201
02020D02 03E5936F 31B01349 886BA217 300D0609 2A864886 F70D0101C05003047310B30
09060355 <snip> 6755 c119 3A2B474E D3428EFD 31C04061302 DAD20C3C DBB38EC9
A10D800F 7B55533122 BFDB09 94B293BC 30200603E9 DB7143F3 DE10C300 DCA82A95
B6C2D63F 906B76DB 6CFE8CBC 81666C DC167714 DCD7C846 63D205815 270350 991935
53671 AE57FBB7 826DDC 종료
```

암호화 확인 표시:

[스포일러](#) (읽으려면 강조 표시)

```
# 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 c=US Subject: cn=GTS Root R1 o=Google
Trust Services LLC c=US Validity Date: start date:
0000:000:000:000:00:00:00:0:0:00:0:0:0:0:0:0:0:0:0:0:00:0:0:00 UTC
2036년 6월 22일 주체 키 정보: 공개 키 알고리즘: RSAEnCRYPTION RSA 공개 키: (4096비트) 서
명 알고리즘: SHA384 with RSA Encryption Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0
D852DC40 Fingerprint SHA1: E58C1CC4 913B3863 4BE9106E3AD8E6B 9DD99841 X509v3 확
장: X509v3 키 사용: 86000000 디지털 서명 키 인증서 서명 CRL 서명 X509v3 주체 키 ID:
E4AF2B26 711A2B48 27852F52 662CEFF0 8913713E X509v3 기본 제약 조건: CA: TRUE
Authority Info Access: Cert 설치 시간: 14:39:38 UTC Mar 132023 nsec의 인증서 설치 시간:
1678718378546968064 관련 신뢰 지점: CA-GTS root-Root R1 신뢰 풀

CA-GlobalSign-Root:

이 인증서가 다음 위치에서 발견되었습니다.

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

설정:

[스포일러](#) (읽으려면 강조 표시)

```
(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

```
MIIDdTCCA12gAwIBAgILBAAAAAABFUtaW5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
<snip>
DKqC5JIR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyIch3WZ1Xi/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
```

455215 (config)# crypto pki authenticate CA-GlobalSign-RootBase 64 인코딩 CA 인증서를 입력합
니다. 빈 줄 또는 "quit"이라는 단어를 스스로 줄로 끝냅니다

```
.MIIDdTCCA12gAwIBAgILBAAAAAABFUtaW5QwDQYJKoZIhvcNAQEFBQAwVzELMAkGA1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
```

```
dsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv<snip>DKqC5JIR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
```

는 다음 특성이 있습니다. Fingerprint MD5: 3E095192E1 E1 5B7 D379F B187298A 지문 SHA1:

B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C% 이 인증서를 수락하십니까? [yes/no]:

yesTrustpoint CA 인증서가 수락되었습니다.% 인증서를 성공적으로 가져왔습니다(config)# 끝

Running-config 확인:

[스포일러](#) (읽으려면 강조 표시)

```
# 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(실행 표시) | sec crypto pki 인증서 체인 CA-GlobalSign-Rootcrypto pki 인증서 체인 CA-
```

```
GlobalSign-Root 인증서 ca 040000000001154B5AC394 30820375 3082025D A0030201
```

```
02020B04 00000000 01154B5A C394300D 06092A86 <snip> 2AC45631 95D06789 852BF96C
```

```
A65D469D 0CAA82E4 9951DD70 B7DB563D 61E46AE1 5CD1 6F6FE 3DDE41CC 07AE6352
```

```
BF5353F4 2BE9C7FD B6F7825F 85D24118 DB81B304 1CC51FA4 806F1520 C9DE0C88
```

```
0A1DD6655E2FC48 C9292669 E0 quit
```

암호화 확인 표시:

스포일러 (읽으려면 강조 표시)

```
#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 인증서 verbose CA-GlobalSign-RootCA CertificateStatus: AvailableVersion: 3인
증서 일련 번호(16진수): 040000000001154B5AC394인증서 사용법: SignatureIssuer:
cn=GlobalSign Root CAou=Root CAo=GlobalSign nv-sac=BESubject: cn=GlobalSign Root
CAou=Root CAo=GlobalSign-sac=BEValidity 날짜: start date: 12:00:00 UTC Sep 1998end date:
12:00:00:0 UTC 8 2028제목 키 정보: 공개 키 알고리즘: RSAEnCRYPTIONRSA 공개 키: (2048비
트)서명 알고리즘: SHA1 with RSA EncryptionFingerprint MD5: 3E455215 095192E1 B75D379F
B187298A 지문 SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C X509v3 확장:
X509v3 키 사용 6000000: 키 인증서 서명CRL 서명X509v3 주체 키 ID: 607B661A 450D97CA
89502F7D 04CD34A8 FFFCFD4B X509v3 기본 제약 조건:CA: TRUEAuthority Info Access:인증서
설치 시간: 03:03:01 UTC Mar 16 2023 Cert install time in nsec: 1678935781942944000Associated
Trustpoints: CA-GlobalSign-Root
```

CA-gmail-SMTP:

Gmail 서버(CA-gmail-SMTP)용 TLS 인증서가 다음 단계에 따라 발견되었습니다. [보안 전송에 TLS 인증서 사용](#)

설정:

[스포일러](#) (읽으려면 강조 표시)

```
(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

```
MIIEnhjCCA26gAwIBAgIQUofgQKT+9wcSaLBP3d3w9DANBgkqhkiG9w0BAQsFADBG  
MQswCQYDVQQGEwJVVzEiMCAgA1UEChMZR29vZ2x1IFRydXN0IFN1cnZpY2VzIEExM  
<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 authenticate CA-gmail-SMTP Ebase 64 encoded CA certificate. End with  
a blank line or the word "quit" on a line by  
self MIIEnhjCCA26gAwIBAgIQUofgQKT+9wcSaLBP3d3d3w9DANBgkqhkiG9w0BAQsFADBG MQswCQYD  
'CA-gmail-SMTP'는 하위 CA이지만 인증서는 CA 인증서가 아닙니다. 수동 확인 필수 인증서는 다음  
특성을 갖습니다. Fingerprint MD5: 19651FFEE 906A414D 6D57B783 946F30A2 지문 SHA1:  
4EF392CB EEB46D5E 47433953 AAEF313F 4C6D2825 % 이 인증서를 수락하십니까? [yes/no]:  
yes Trustpoint CA 인증서가 수락되었습니다. % 인증서를 가져왔습니다 (config)#.
```

Running-config 확인:

[스포일러](#) (읽으려면 강조 표시)

```
# show run | sec crypto pki certificate chain CA-gmail-SMTP  
crypto pki certificate chain CA-gmail-SMTP  
certificate ca 5287E040A4FEF7071268B04FDDDF0F4  
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(실행 표시) | sec crypto pki 인증서 체인 CA-gmail-SMTP crypto pki 인증서 체인 CA-  
gmail-SMTP certificate chain CA 5287E040A4FEF7071268B04FDDDF0F4 30820486 3082036E  
A0030201 02021052 87E040A4 FEF70712 68B04FDD DDF0F430 0D06092A 864886F7
```

OD01010B 05003046 310B3009 06035504 06130255<snip> 92ABB1F5 11F53312230B9B F24A
F94F5283 EE2928B7 7EFB084B 6D61217 416045 C47BCB99 801C4969 E4D48E77 2FA3 quit

암호화 확인 표시:

[스포일러](#) (읽으려면 강조 표시)

```
# 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): 5287E040A4FEF7071268B04FDDDDF0F4Certificate Usage:
SignatureIssuer: cn=GTS CA 1C3o=Google Trust Services LLCc=USSubject:
cn=smtp.gmail.comCRL 배포 지점: http://crls.pki.goog/gts1c3/moVdfISia2k.crlValidity 날짜: 시작
날짜: 09:15:03 UTC 12 May 15 2023제목 키 정보: 공개 키 알고리즘: ecEncryptionEC 공개 키:
(256비트)서명 알고리즘: SHA256 with RSA EncryptionFingerprint MD5: 19651FBE 906A414D
```

6D57B783 946F30A2 지문 SHA1: 4EF392CB EIB46D5E 47433953 AAEF313F 4C6D2825
X509v3:X509v3 키 사용: 80000000디지털 서명X509v3 주체 키 ID: 5CC36972 D07FE997
510E1A67 8A8ECC23 E40CFB68 X509v3 기본 제약 조건:CA: FALSEX509v3 주체 대체 이름
:smtp.gmail.com IP 주소: 기타 이름: X509v3 권한 키 ID: 8A747FAF 85CDEE95 CD3D9CD0 E
24614F3 71351D27 Authority 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 설치 시간: 03:10:41 UTC Mar 16 2023 Cert 설치 시간(nsec):
1678936241822955008Associated Trustpoints: CA-gmail-SMTP

인증서를 찾는 더 쉬운 방법

또는 디버그를 사용하고 Google을 검색하여 추적하지 않고도 SMTP 서버에서 인증서를 가져오는 더 쉬운 방법으로 서버/랩톱의 openssl 호출을 사용할 수 있습니다.

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

use smtp.gmail.com에서도 확인할 수 있습니다.

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

해당 호출의 출력에는 "crypto pki authenticate <trustpoint>" 컨피그레이션에 사용할 수 있는 실제 인증서 자체가 포함됩니다.

Secure SMTP로 EEM 다시 테스트

이제 인증서가 Cisco IOS XE 디바이스에 적용되었으므로 EEM 스크립트는 보안 SMTP 메시지를 예상대로 전송합니다.

```
# event manager run SendSecureEmailEEM
```

스플러에서 전체 암호화 및 ssl 디버그 출력을 확인합니다.

[스포일러](#) (읽으려면 강조 표시)

```
# 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" s

*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 FO
*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:

```

```

# 이벤트 관리자 실행 SendSecureEmailEEM*3월 16일 03:28:50.673: CRYPTO_OPSSL:
OPSSLContext*3월 16일에 메모리를 할당함 03:28:50.673: CRYPTO_OPSSL: 버전 128에 대해
0x02FC0000을 마스킹하도록 암호 사양 설정*3월 16일 03:28:50.674: 기본 EC 곡선 목록 설정:
0x70EC 곡선 목록 설정: secp521r1:secp348 r1:prime256v1*3월 16일 03:28:50.674:
opssl_SetPKInfo entry*3월 16일 03:28:50.674: CRYPTO_PKI: (A069B) 세션 시작됨 - ID 선택됨
(TP-self-signed-486541296)xTP-self-signed-486541296:refcount after increment = 1*3월 16일
03:28:50.674: CRYPTO_PKI: Begin local chain cert retrieval.*3월 1003:28:50.60.674:
crypto_PKI(Cert Lookup) issuer="cn=IOS-Self-Signed-Certificate-486541296" serial number=
01*Mar 16 03:28:50.674: CRYPTO_PKI: handle=7F41EE523CE0, digest=1C 7D 52 67 6 D5 59
E2 66 58 E7 8B E7 9B 8E*Mar 16 03:28:50.675: CRYPTO_PKI: Done with local cert chain Fetch.
16 03:28:50.675: CRYPTO_PKI: PKI 세션 A069B.*3월 16일 03:28:50.675: CRYPTO_PKI: PKI 세
션 A069B가 종료되었습니다. 모든 리소스 비우기.TP-self-signed-486541296:unlocked trustpoint
TP-self-signed-486541296, refcount는 0*3월 16일 03:28:50.675: opssl_SetPKInfo done.*3월 16일
03:28:50.675: CRYPTO_OPSSL: 이 세션에서 공통 기준이 비활성화됩니다.SSL CTX
0x7F41F28EAF8*3월 1603:28:50.675: CRYPTO_OPSSL ciphersuites에서 공통 기준 모드 기능
비활성화: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-
RSA-AES256-SHA384:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:AES256-
GCM-SHA384:AES256 ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-

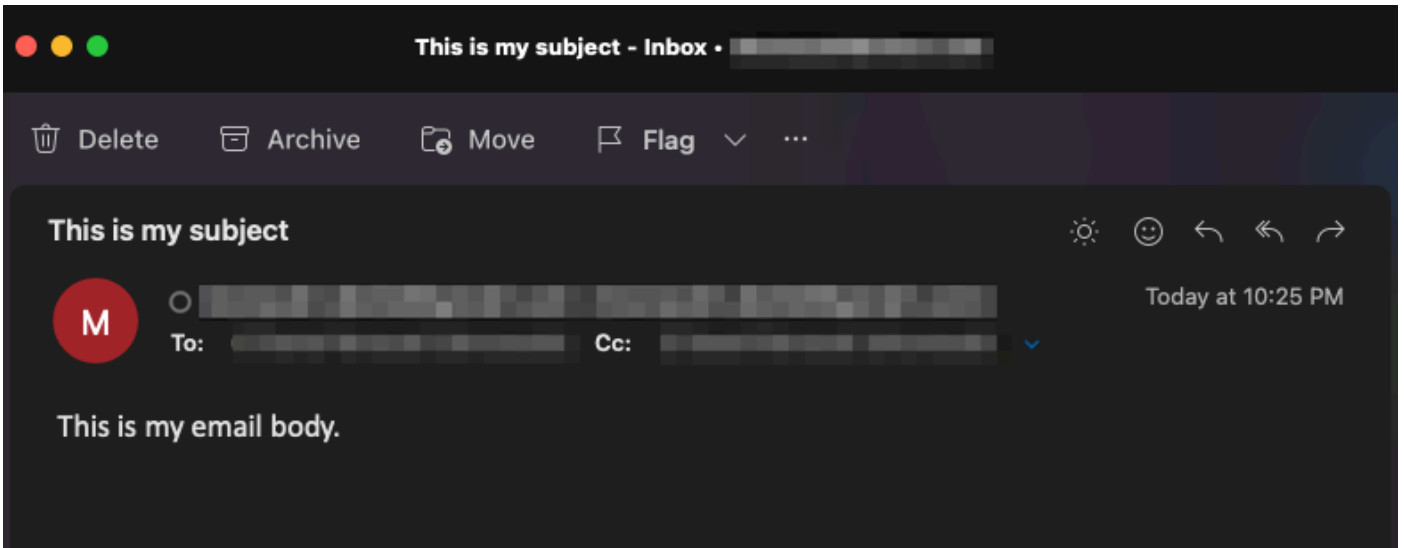
```


SHA256: AES128-GCM-SHA256: AES 128-SHA256*3월 16일 03:28:50.676: 핸드셰이크 시작: SSL 초기화 전*3월 16일 03:28:50.676: SSL_connect: SSL 초기화 전*3월 16일 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 핸드셰이크 [length 0095], ClientHello*Mar 16 03:28:50.676: 01 000 91 03 026 4B 9B3 4494 FD 5F FD A1<snip1> *3월 16일 03:28:50.679: 03 03 01 02 01*3월 16일 03:28:50.679: *3월 16일 03:28:50.679: SSL_connect: SSLv3/TLS write client hello*3월 16일 03:28:50.692: << ??? [length 0005]*3월 16 03:28:50.692: 16 03:03 00 3F*3월 16 03:28:50.692: *3월 16 03:28:50.692: SSL_connect: SSLv3/TLS 쓰기 클라이언트 hello*3월 16 03:28:50.692: <<< TLS 1.2 핸드셰이크 [length 003F], ServerHello*3월 1603:28:50.692: 00 3B 03 03 03 64 12 7E 05 25 F6 7A BD A0 2E*3월 16 03:28:50.692: 58 83 12 7F 90 CD F4 AB E2 69 53 A8 C7 FC 44 4F*3월 16 03:28:50.692: 57 4E 47 52 4 01 00 C0 2B 000 10 1000*3월 1603:28:5 .693: FF 01 00 01 00 00 00 0B 00 02 01 00 00 23 00 00*3월 16 03:28:50.693: TLS 서버 확장 "알 수 없음"(id=23), len=0 TLS 서버 확장 "재협상"(id=65281), len=1*3월 16 03:28:50.693: 00*3월 16 03:28:50.693: TLS 서버 확장 "EC point formats"(id=11), len=2*3월 1603:82:50.693: 01 00*3월 16일 03:28:50.693: TLS 서버 확장 "세션 티켓"(id=35), len=0*3월 16일 03:28:50.693: << ??? [length 0005]*3월 16 03:28:50.693: 16 03:03 0F 9A*3월 16 03:28:50.694: *3월 16 03:28:50.702: SSL_connect: SSLv3/TLS 읽기 서버 hello*3월 16 03:28:50.702: << TLS 1.2 핸드셰이크 [length 0F9A], Certificate*3월 16 03:28:50.702: 0B00F 90 0 0F 93 00 04 8A 30 82 04 86 30 82*3월 16 03:28:50.702: 03 6E A0 03 02 01 02 02 10 52 87 E0 40 A4 FE F7<snip>*3월 16 03:28:50.763: 82 35 CF 62 8B C9 24 8B A5 B7 39 0C BB 7E 2A 41*3월 1603:28:05 7.763: BF 52 CF FC A2 96 B6 C2 82 3F*3월 16일 03:28:50.763: *3월 16일 03:28:50.765: CC_DEBUG: shim layer app callback function 입력*3월 16일 03:28:50.765: CRYPTO_PKI: (A069C) 세션 시작됨 - identity not specified*3월 16 03:28:50.765: CRYPTO_PKI: (A069C) 1) 피어 인증서 추가*3월 16일 03:28:50.767: CRYPTO_PKI: 추가된 x509 피어 인증서 - (1162) 바이트*3월 16일 03:28:50.767: CRYPTO_PKI: (A069C) 피어 인증서 추가*3월 16일 03:28:50.768: CRYPTO_PKI: 추가된 x509 피어 인증서 - (1434 바이트)*3월 16 03:28:50.768: CRYPTO PKI: (A069C) 피어 인증서 추가*3월 16일 03:28:50.770: CRYPTO_PKI: 추가된 x509 피어 인증서 - (1382) 바이트*3월 16일 03:28:50.770: CRYPTO_OPSSL: 인증서 체인 콜백 확인*3월 16일 03:28:50.770: CRYPTO_PKI(Cert Lookup) issuer="cn=GTS CA 1C3,o=Google Trust Services LLC,c=US=US serial number= 5 2 87 E0 40 A4 FE F7 07 12 68 B0 4F DD F0 F4*Mar 16 03:28:50.770: CRYPTO_PKI: 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=) "cn=GTS Root R1,o=Google Trust Services LLC,c=US" serial number= 02 03 BC 53 59 6B 34 C7 18 F5 01 50 66*Mar 16 03:28:50.771: CRYPTO_PKI: handle=7F41EE523CE0, digest=03 9F CF 59 82 EE 09 CC 4F 53 AE D8 02 7E 4B AF*Mar 1603:28:5 0.771: CRYPTO_PKI(Cert Lookup) issuer="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*3월 16 03:28:50.771: CRYPTO_PKI: handle=7F41EE523CE0, digest=940 D1 90 A0 A3 d 47 E5 B5 31 F6 63 AD 1B 0A*3월 16일 03:28:50.771: CRYPTO_PKI: 발급자 직렬에 대한 인증서 레코드를 찾을 수 없습니다.*3월 16일 03:28:50.772: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()*3월 16일 03:28:50.772: CRYPTO_PKI: 주체 일치 발견*3월 1603:#28:50.772: CRYPTO_PKI-PIP: ext-val: IP 확장 검증이 필요하지 않음: 컨텍스트 id-35에 대한 refcount를 1*3월 16일 03:28:50.773으로 증가: CRYPTO_PKI: 새 ca_req_context 유형 PKI_VERIFY_CHAIN_CONTEXT 생성, ident 35*3월 16일 03:28:50.773: CRYPTO_PKI: (A069C) 검증 경로에 1개의 certs*3월 16일 03:28:50.773: CRYPTO_PKI: (A069C) 동일한 certs*에 대한 검사 16 03:28:50.773: CRYPTO_PKI(Cert Lookup) issuer="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*3월 16 03:28:50.774: CRYPTO_PKI: 핸들에서 인증서 찾기=7F41EE523CE0, digest=940 d1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A*3월 16일

03:28:50.774: CRYPTO_PKI: 발급자 직렬에 대한 인증서 레코드를 찾을 수 없습니다.*3월 16일
03:28:50.774: CRYPTO_PKI : (A069C) 신뢰할 수 없는 인증서 검증*3월 16일 03:28:50.774:
CRYPTO_PKI: (A069C) 적합한 신뢰 지점 목록 만들기*6월 1 03:28:50.774: CRYPTO_PKI:
crypto_pki_get_cert_record_by_issuer()*3월 16일 03:28:50.774: CRYPTO_PKI: 발급자 일치 검색
*3월 16일 03:28:50.774: CRYPTO_PKI: (A069C) 적합한 신뢰 지점: CA-GlobalSign-Root,*3월 16
03:28:50.775: CRYPTO_PKI: (A069C) 1) CA-GlobalSign-Root 정책을 사용하여 인증서의 유효성을
검사하려고 합니다.*3월 16일 03:28:50.775: CRYPTO_PKI: (A069C) CA-GlobalSign-Root를 사용
하여 인증서의 유효성을 검사합니다.*3월 16일 03:28:50.775: CRYPTO_PKI(신뢰할 수 있는 인증서
체인 만들기)*3월 16일 03:28:50.775: CRYPTO_PKI: 신뢰할 수 있는 체인에 인증서 1개 추가됨
.*3월 16 03:28:50.775: CRYPTO_PKI: 세션 해지 서비스 공급자 준비*3월 16일
03:28:50.776: P11:C_CreateObject:*3월 16일 03:28:50.776: CKA_CLASS: PUBLIC KEY*3월 16일
03:28:50.776: CKA_KEY_TYPE: RSA*3월 16일 03:28:50.776: CKA_MODULUS: DA 0E6 99 8D
CE E3 4F 8A 7E FB 1 8B 83 25 6B EA 48 1F1 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 has key
id 45*Mar 16 03:28:50.781: CRYPTO_PKI: 피어의 공개 키를 캐시에 삽입하려고 시도*3월 16일
03:28:50.781: CRYPTO_PKI:Peer's inserted successfully with key id 46*3월 16 03:28:50.781:
P11:C_CreateObject: 131118*3월 16 03:28:50.781: P11:C_GetMechanismInfo slot 1 type 3
(invalid mechanism)*3월 16 03:28:50.781: P11:C_GetMechanismInfo 슬롯 1 유형 1*3월 16일
03:28:50.781: P11:C_VerifyRecoverInit - 131118*3월 16일 03:28:50.781: P11:C_VerifyRecover -
131118*3월 16일 03:28:50.781: P11:found pubkey in cache using index = 46*3월 16
03:28:50.781: P1:public key found : 08220 2 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*3월 16 03:28:50.788:
P11:CEAL:CRYPTO_NO_ERR*3월 16 03:28:50.788: P1:C_DestroyObject 2 002E*3월 16일
03:28:50.788: CRYPTO_PKI: 만료되는 피어의 캐시된 키(키 ID: 46*3월 16일 03:28:50.788:
CRYPTO_PKI: (A069C) 인증서 확인*3월 16일 03:28:50.788: CRYPTO_PKI: 세션 해지 서비스 공
급자 제거*3월 16일 03:28:50.788: CRYPTO_PKI: 세션 해지 서비스 공급자 제거CA-GlobalSign
Root:validation status - CRYPTO_VALID_CERT_WITH_WARNING*3월 16일 03:28:50.788:
CRYPTO_PKI: (A069C) Certificate validated without revocation check:cert refcount after
increment = 1*3월 16일 03:28:50.790: CRYPTO_PKI: Populate AAA auth data*3월 16일
03:28:50.790: CRYPTO_PKI: Unable to get configured attribute for primary AAA list
authorization.*Mar 16 03:28:59:50.7 0: PKI: Cert key-usage: Digital-Signature , Certificate-Signing ,
CRL-Signing*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C)chain cert가 신뢰 지점 CA-GlobalSign-
Root에 고정되었으며, 체인 유효성 검사 결과: CRYPTO_VALID_CERT_WITH_WARNING*Mar 16
03:28:50.790: CRYPTO_PKI: (A069C) Verify context*Mar 16 03:28:50.79 0: CRYPTO_PKI:
destroying ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 35, ref count
1:Decrementing refcount for context id-35를 0*3월 16일 03:28:50.790: CRYPTO_PKI:
ca_req_context released*3월 16일 03:28:50.790: CRYPTO_PKI: (A069C) Validation TP is CA-
GlobalSign-Root*3월 16 03:28:50.790.790: CRYPTO_PKI (A069C) 인증서 유효성 검사에 성공했습
니다.*3월 16일 03:28:50.790: CRYPTO_OPSSL: 인증서 유효성 검사에 성공했습니다.*3월 16일
03:28:50.790: CRYPTO_PKI: PKI 세션 A069C를 종료하기 위한 요청 수신.*3월 16일 03:28:50.790:
CRYPTO_PKI: PKI 세션 A069C 종료 모든 리소스 비우기.:cert refcount after decrement = 0*Mar
16 03:28:50.791: << ??? [length 0005]*3월 16 03:28:50.791: 16 03:03 00 93*3월 16 03:28:50.791:
*3월 16 03:28:50.791: SSL_connect:SSLv3/TLS 읽기 서버 인증서*3월 16 03:28:50.791: <<< TLS
1.2 핸드셰이크 [length 0093], ServerKeyExchange*3월 16 03:28:50.791: 0C0 00 8F 03 00 17 41
04 3D 49 34 A3 52 D4 EB*3월 16 03:28:50.791: DE A2 9E CC B0 91 AA CB 1B 39 D0 26 1B 7D
FF 31*3월 16 03:28:50.792: E0 D5 9C 75 C0 7D 5B6 B2 0A B5 CC EA E1 4B*3월 16 03:28:50.792:

4E5 72 7B 54 5D 9B2 95 91 E0 CC D6 A5 8E CE*3월 16일 03:28:50.792: 8D 36 C9 83 42 B0 4D
AC 0C 04 03 00 46 30 44 02*3월 16일 03:28:50.792: 20 67 B3 F1 DA D1 BF 1372 DD B6 B2 111
3B 6E F*3월 16일 03:28:50.793: 87 52 D9 00 F7 44 31 C3 C2 5E BE 2D FF 93 4E F0*3월 16일
03:28:50.793: A8 02 20 24 42 91 BE B7 10 1C D1 C0 12 28 FB 1F*3월 16 03:28:50.793: E4 DE
81 0B AA 6619 CD 25A 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: 0 0 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 42 004 63 B6 D3 1A 28 <snip>*Mar 16 03:28:50.796: P11:C_FindObjectsFinal*Mar 1603:2
8:50.796: P11:C_VerifyInit - 세션 처음*3월 16일 03:28:50.796: P11:C_VerifyInit - 키 id =
131073*3월 16일 03:28:50.796: P11:C_Verify*3월 16일 03:28:50.800:
P11:CEAL:CRYPTO_NO_ERR*3월 1603:28:50.800: << ??? [length 0005]*Mar 16 03:28:50.800:
16 03:03 00 00 04*Mar 16 03:28:50.800: *Mar 16 03:28:50.800: SSL_connect:SSLv3/TLS 읽기 서
버 키 교환*Mar 16 03:28:50.800: <<< TLS 1.2 핸드셰이크 [length 004], ServerHelloDone*Mar
160:28:50 0 00 00*Mar 16 03:28:50.801: *Mar 16 03:28:50.801: SSL_connect:SSLv3/TLS 읽기 서
버 완료*Mar 16 03:28:50.810: >> ??? [length 0005]*3월 16일 03:28:50.810: 16 03 03 00 46*3월
16 03:28:50.811: *3월 16일 03:28:50.811: >>> TLS 1.2 핸드셰이크 [length 0046],
ClientKeyExchange*3월 16일 03:28:50.811: 10000 42 4 426 C3 EF 0205 6C 82 D1 90 B3 3월
16일 03:28:50.811: 17 31 9A CD DD 8C 81 91 BA E8 C0 86 40 7B 2C E4*3월 16일 03:28:50.811:
9A 2C 18 9D D1 6A C0 56 A0 98 2E B7 3B AB3 EB*3Mar 16 03:28:50.811: BB CD 5E 42 C5 76
C0 C4 BF4 15 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 쓰기 클라이언트 키 교환*Mar 16 03:28:50.812:
>> ??? [length 0005]*Mar 16 03:28:50.812: 14 03 03 00 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]*3월 16일 03:28:51.116: 17 03 03 00 35*3월 16 03:28:51.116: *3월 16일 03:28:51.116: >>
??? [length 0005]*3월 16일 03:28:51.116: 17 03 03 00 1A*3월 16일 03:28:51.116: *3월 16일
03:28:51.116: >> ??? [length 0005]*3월 16일 03:28:51.116: 17 03 03 00 30*3월 16일
03:28:51.116: *3월 16일 03:28:51.116: >> ??? [length 0005]*3월 16일 03:28:51.116: 17 03 03 00
1B*3월 16 03:28:51.117: *3월 16일 03:28:51.713: << ??? [length 0005]*3월 16일 03:28:51.713: 17
03 03 00 6D*3월 16일 03:28:51.713: *3월 16일 03:28:51.714: >> ??? [length 0005]*3월 16일
03:28:51.714: 17 03 03 00 1E*3월 16 03:28:51.714: *3월 16일 03:28:51.732: << ??? [length
0005]*3월 16일 03:28:51.732: 17 03 03 00 71*3월 16일 03:28:51.732:

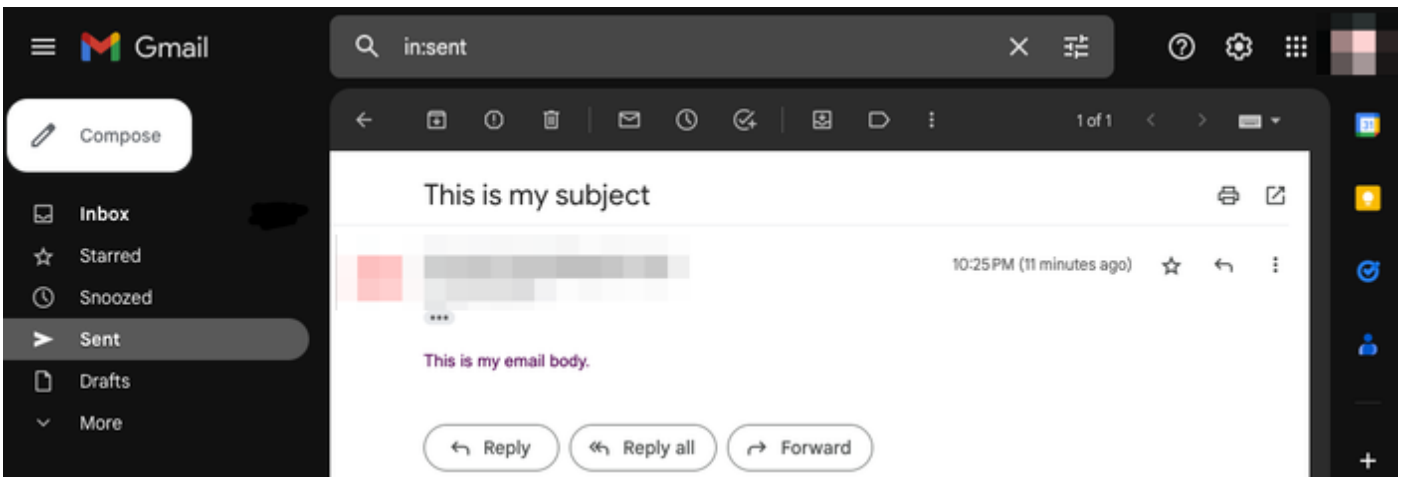
이메일이 수신되었고 모든 필드(받는 사람, 받는 사람, 참조, 제목, 본문)가 올바르게 입력되었는지
확인할 수 있습니다.



또한 Cisco IOS XE 디바이스의 패킷 캡처에서 TLS 핸드셰이크와 세션이 발생했는지 확인할 수 있습니다("WorkingSMTPwithTLS.pcap"로 첨부).

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

이메일이 사용된 이메일 계정의 "Sent(보냄)" 폴더에 반영되었는지 확인할 수도 있습니다.



기타 주의 사항 및 고려 사항

@ 기호가 있는 사용자 이름

SMTP 릴레이 사용을 시도할 때 문제가 나타날 수 있습니다. SMTP 릴레이 때문에 서버 문자열의 형식은 다음과 같습니다(사용자 이름에서 "@").

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

사용자 이름과 비밀번호를 구문 분석하는 코드는 "@" 기호의 첫 번째 발생 시 문자열을 분할합니다. 그 결과 시스템은 나머지 문자열에서 첫 번째 "@" 기호 바로 다음에 서버 호스트 이름이 시작된다고 생각하고 그 이전의 모든 항목을 "username:password"로 해석합니다.

SMTP의 TCL 구현에서는 이 사용자 이름/비밀번호/서버 정보를 다르게 처리하는 정규식(regex)을 사용합니다. 이러한 차이 때문에 TCL은 "@" 기호의 사용자 이름을 허용합니다. 그러나 Cisco IOS XE TCL은 암호화를 지원하지 않으므로 TLS를 통해 보안 이메일을 전송할 수 있는 옵션이 없습니다.

요약하자면,

- 이메일의 보안이 필요한 경우 TCL로 보낼 수 없습니다.
- 사용자 이름에 "@"이 있으면 EEM으로 보낼 수 없습니다.

Cisco 버그 ID [CSCwe75439](#)는 EEM 이메일 기능을 개선할 수 있는 이 기회를 해결하기 위해 제출되었지만 현재 이 개선 요청에 대한 로드맵은 없습니다.

결론

여기에 표시된 것처럼 EEM(Embedded Event Manager) 애플릿을 사용하여 TLS를 통해 SMTP를 통해 보안 이메일을 전송할 수 있습니다. 신뢰를 허용하도록 필요한 인증서를 구성할 뿐만 아니라 서버 측에서 일부 설정을 필요로 하지만, 자동화된 보안 이메일 알림을 생성하려는 경우 가능합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.