EEM gebruiken om beveiligde e-mails aan gebruikers te automatiseren

Inhoud

Inleiding

Use case

Achtergrond

Gmail-account instellen

EEM-basisconfiguratie

Probleem gezien met alleen geïnstalleerde standaardcertificaten

Certificaten voor het beveiligen van SMTP

Een eenvoudiger manier om de certificaten te vinden

EEM opnieuw testen met beveiligde SMTP

Andere voorbehouden en overwegingen

- Gebruikersnamen met @-symbolen

Conclusie

Inleiding

Dit document beschrijft het proces dat nodig is om de "mailserver"-actie in Embedded Event Manager (EEM) binnen Cisco IOS® XE te gebruiken om beveiligde e-mails te verzenden naar een Simple Mail Transfer Protocol (SMTP)-server met behulp van Transport Layer Security (TLS) op poort 587.

Er zijn veel voorbehouden die u kunt tegenkomen tijdens dit proces, daarom is dit artikel geschreven om de stappen te documenteren die nodig zijn om dit te bereiken.

Use case

Veel klanten zien waarde in het automatisch ontvangen van een e-mailbericht na een bepaalde gebeurtenis. Het EEM-subsysteem is een krachtig hulpmiddel voor de detectie van netwerkgebeurtenissen en on-board automatisering en kan een efficiënte manier bieden om e-mailmeldingen op een Cisco IOS XE-apparaat te automatiseren. Bijvoorbeeld, zou u een spoor van IPSLA kunnen willen controleren, en in antwoord op een syslog die op een staatsverandering wijst, neemt één of ander soort actie en alarmeert de netwerkbeheerders van de gebeurtenis via e-mail. Dit idee van e-mailberichten kan worden toegepast op vele andere scenario's als een manier om de aandacht te vestigen op een bepaalde gebeurtenis die u wilt markeren.

Achtergrond

PEM staat voor "Privacy Enhanced Mail" en is een formaat dat vaak wordt gebruikt om certificaten

en sleutels weer te geven. Dit is de certificaatindeling die door Cisco IOS XE-apparaten wordt gebruikt. Beveiligde toepassingen (zoals HTTPS of beveiligde SMTP) hebben vaak een "stapelbare PEM", waarbij er meerdere certificaten bij betrokken zijn, waaronder:

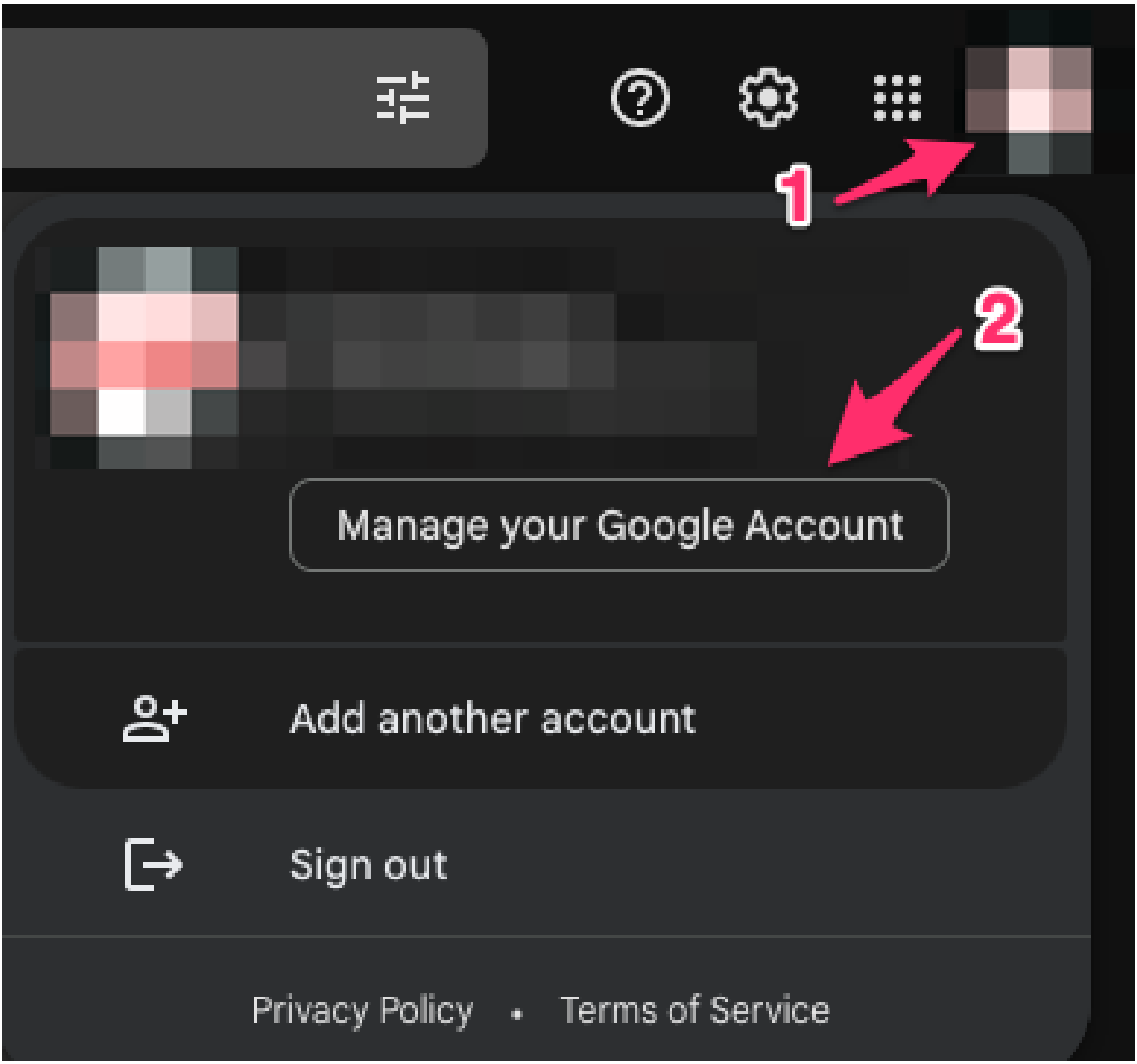
- basiscertificaat
- Certificaat van ondertekening (tussentijds)
- Certificaat van eindgebruiker (of server)

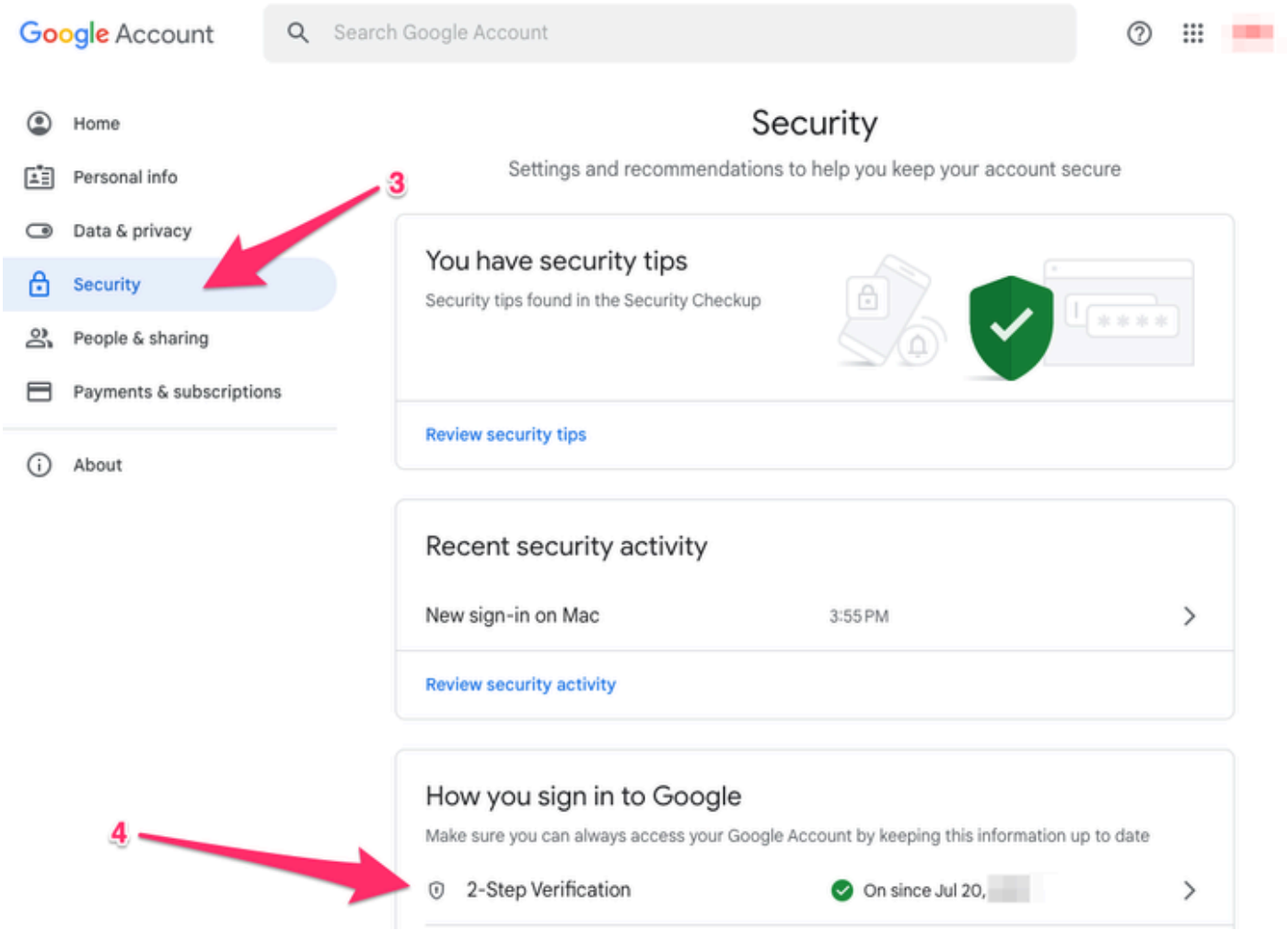
Gmail-account instellen

De SMTP-diensten van Google zullen in dit artikel als voorbeeld worden gebruikt. Voorwaarde is dat u een Gmail-account hebt ingesteld.

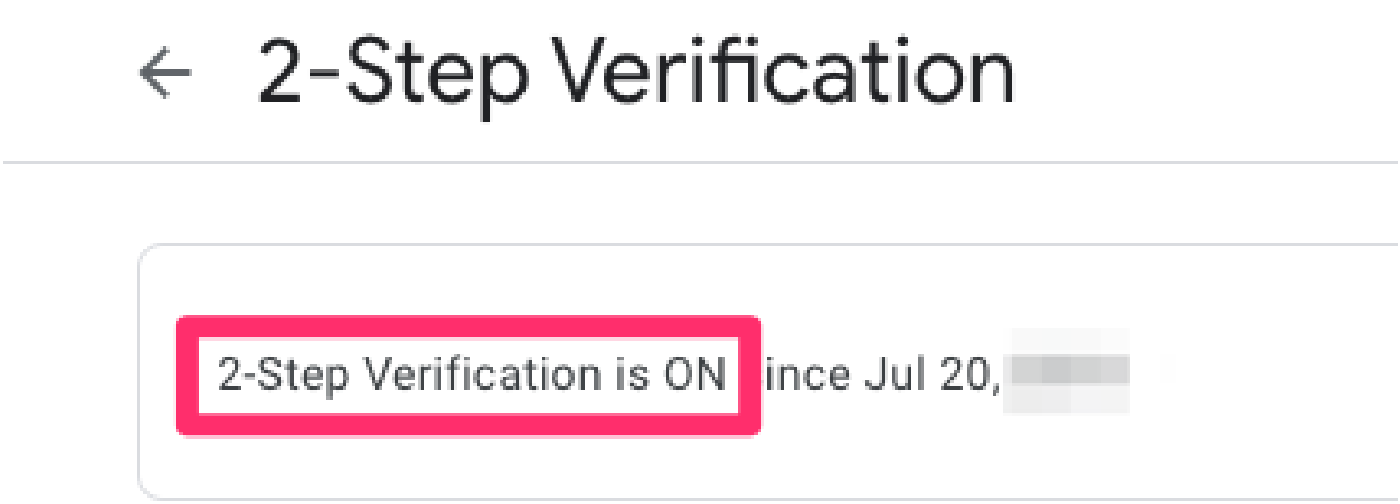
Google stelt u in staat e-mails van externe klanten naar Gmail te sturen. Vroeger was er een instelling in Gmail voor "onbeveiligde apps", en de toepassing zou een fout tegenkomen als deze instelling niet was toegestaan aan het einde van Google. Die instelling is verwijderd, en in zijn plaats is een "Secure Application" optie. die toegankelijk is via:

mail.google.com > Klik op Uw profiel (#1) > Uw Google-account beheren (#2) > Beveiliging (#3) > Inloggen bij Google > Verificatie in 2 stappen (#4)


1
2
Manage your Google Account
Add another account
Sign out
Privacy Policy • Terms of Service



Zorg ervoor dat vanaf deze pagina de tweestapsverificatie is ingeschakeld.



U kunt vervolgens naar beneden scrollen naar "App wachtwoorden" om Gmail een wachtwoord te laten genereren dat kan worden gebruikt om in te loggen op uw Google-account vanuit een toepassing die geen 2-staps verificatie ondersteunt.

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

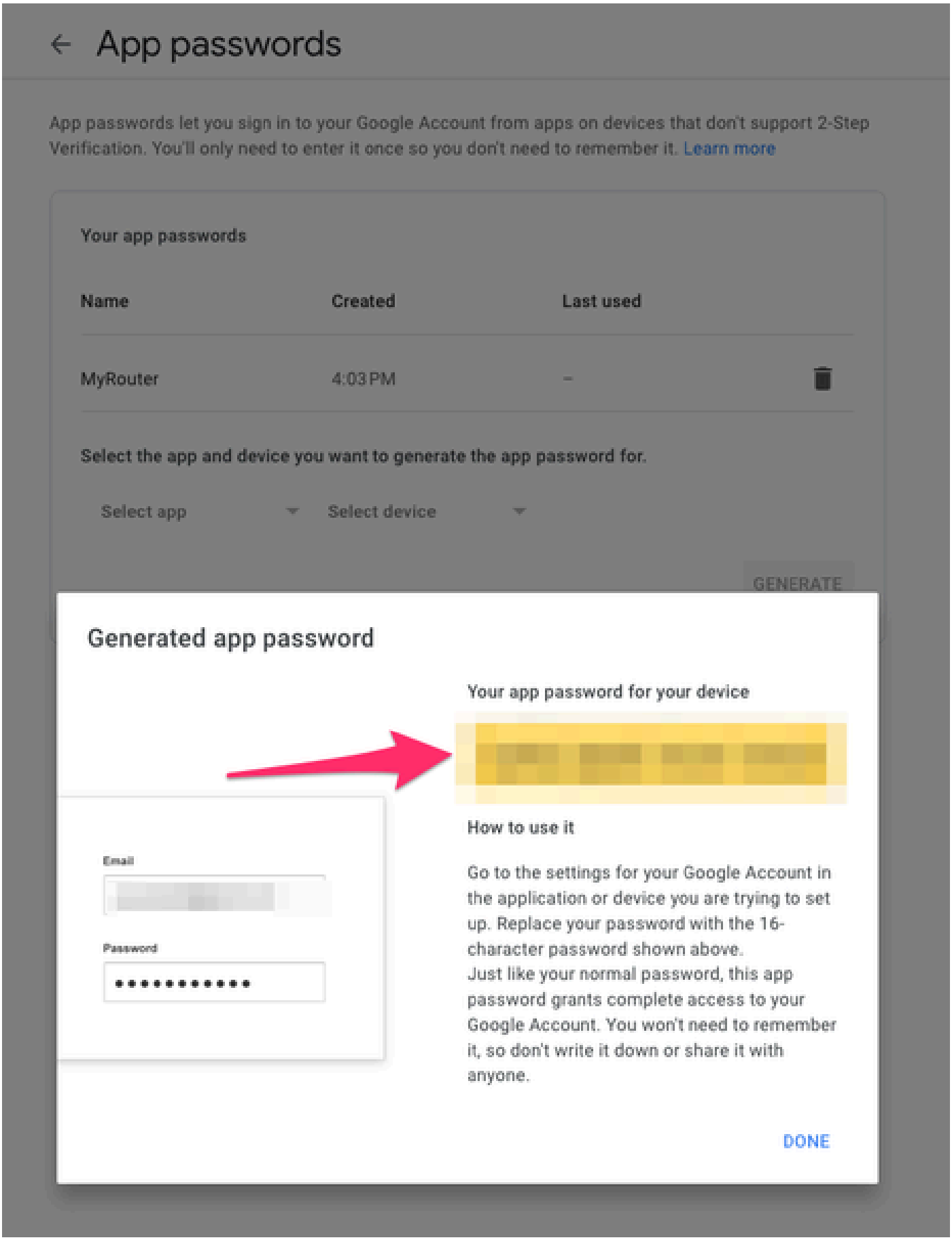
App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. Learn more

You don't have any app passwords.

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

MyRouter

GENERATE



Het wachtwoord van 16 tekens in deze screenshot is vervaagd omdat het is gekoppeld aan een persoonlijke Gmail-account.

Nu u een toepassingswachtwoord voor Gmail hebt, kunt u dit, samen met uw naam van de Gmail-account, gebruiken als de e-mailserver voor het doorsturen van de e-mail. De notatie voor het opgeven van de server is "gebruikersnaam:password@host".

EEM-basisconfiguratie

Er zijn vele manieren waarop u een EEM script kunt aanpassen aan uw exacte behoeften, maar dit voorbeeld is een basis EEM script om de beveiligde e-mail functionaliteit te laten werken:

```
(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 "$_email_from" cc "$_
```

De configuraties maken eerst drie EEM omgevingsvariabelen: _email_from, _email_to, en _email_server. Elke wordt gedefinieerd in een variabele om configuratieveranderingen gemakkelijker te maken. U maakt vervolgens het script SendSecureEmailEEM. De triggergebeurtenis hier is "none", zodat u het EEM script handmatig kunt uitvoeren op-will met "# event manager run SendSecureEmailEEM" (in plaats van te wachten op een specifieke gebeurtenis die moet worden geactiveerd). Vervolgens heb je slechts één actie "mailserver" die de e-mailgeneratie verzorgt. De "beveiligde tls" en "port 587" opties vertellen het apparaat om te onderhandelen over TLS op poort 587, die de Gmail servers zullen luisteren.

U moet er ook voor zorgen dat uw veld "van" geldig is. Als je authenticeert als "Alice" maar probeert om een e-mail te sturen van "Bob", dan zal het fout omdat Alice is het spoofing van iemand anders e-mailadres. Het veld "Van" moet worden afgestemd op de account die wordt gebruikt om de e-mail op de server te verzenden.

Probleem gezien met alleen geïnstalleerde standaardcertificaten

EEM gebruikt openssl om een verbinding te maken met de SMTP-server. Voor beveiligde communicatie stuurt de server een certificaat terug naar openssl die in Cisco IOSd wordt uitgevoerd. IOS zal dan op zoek gaan naar een trustpoint gekoppeld aan dat certificaat.

Op een Cisco IOS XE-apparaat worden de certificaten voor de Gmail SMTP-servers niet standaard geïnstalleerd. Ze moeten handmatig worden geïmporteerd om vertrouwen te wekken. Zonder de certificaten die zijn geïnstalleerd, zal de TLS-handdruk mislukken vanwege een "slecht certificaat".

Deze debugs zijn zeer nuttig voor het debuggen van eventuele certificaatproblemen:

```
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
```

U kunt een ingesloten pakketvastlegging (EPC) starten op de router om elk verkeer naar of van de e-mailserver op te nemen als de EM wordt geactiveerd:

```
! 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:
*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: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
```

Uiteindelijk kan openssl de beveiligde TLS-sessie niet met de SMTP-server instellen, zodat er een

fout met het 'slechte certificaat' wordt gegenereerd, die ervoor zorgt dat de EEM ophoudt met draaien:

```
*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
```

De pakketopname die vanaf deze uitwisseling is gedocumenteerd, is aangesloten als "NoCertificateInstall.pcap". Het laatste TLS-pakket van de router (10.122.x.x) naar de Gmail-SMTP-server (142.251.163.xx) toont aan dat de TLS-onderhandeling werd beëindigd vanwege hetzelfde bericht "Slecht certificaat" dat eerder in de debugs werd gezien.

```
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)
```

Certificaten voor het beveiligen van SMTP

Omdat de certificaten die het Cisco IOS XE-apparaat in staat stellen om de servers van Gmail te vertrouwen, ontbreken, is de oplossing om een/al die certificaten in een trustpoint op het apparaat te installeren.

Bijvoorbeeld, de volledige debugs van de vorige test tonen deze certificaat lookups die plaatsvonden:

```
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
```

Een certificaat voor elk van deze emittenten moet worden geïnstalleerd onder een trustpoint zodat het apparaat een beveiligde sessie kan instellen met de Gmail-SMTP-servers. U kunt een trustpoint maken voor elke emittent met behulp van deze configuraties:

```
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
```

U hebt nu een trustpoint voor elke emittent die is opgericht; er zijn echter nog geen daadwerkelijke certificaten die daarmee verband houden. Het zijn in wezen blanco vertrouwenspunten:

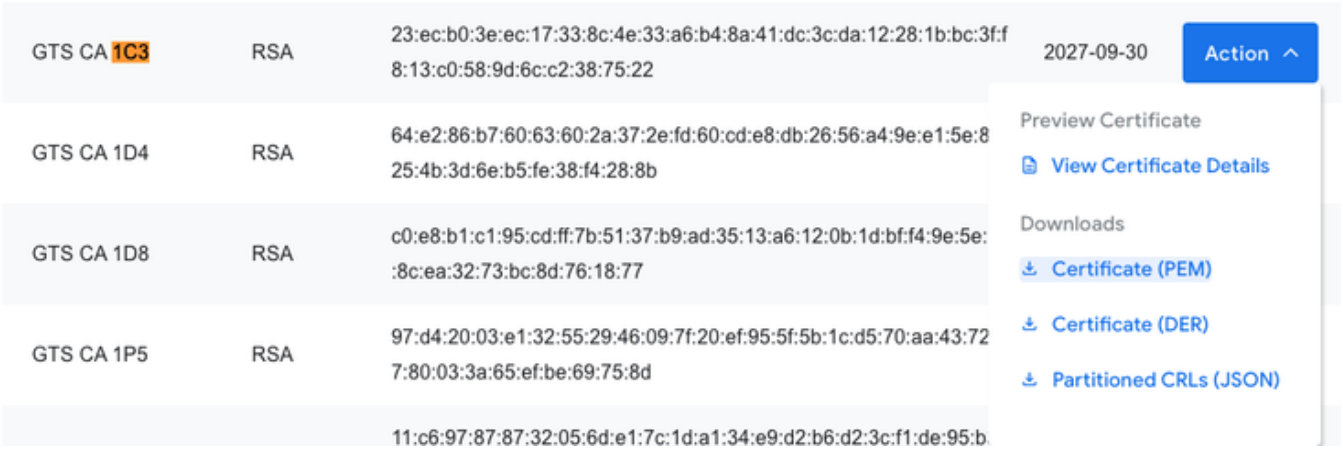
```
# show run | sec crypto pki certificate chain CA-
crypto pki certificate chain CA-GTS-1C3
crypto pki certificate chain CA-GTS-Root-R1
crypto pki certificate chain CA-GlobalSign-Root
crypto pki certificate chain CA-gmail-SMTP
```

U moet opsporen waar die certificaten zijn en ze dan op het apparaat installeren.

Op zoek naar "Google Trust Services 1C3", komen we snel de Google Trust Services Repository van certificaten tegen:

https://pki.goog/repository/

Na het uitbreiden van alle certificaten op die pagina, kunt u zoeken om "1C3" te vinden, op de "Actie" dropdown te klikken, en het PEM-certificaat te downloaden:



Wanneer u het gedownloade PEM-bestand met een teksteditor opent, blijkt dat dit slechts een certificaat is dat op het Cisco IOS XE-apparaat kan worden geïmporteerd onder het vertrouwde punt dat u eerder hebt gemaakt:

```
-----BEGIN CERTIFICATE-----
MIIFljCCA36gAwIBAgINAgO8U1lrNMcY9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU
<snip>
AJ2xDx8hcFH1mt0G/FX0Kw4zd8NLQsLxdxP8c4CU6x+7Nz/OAipmsHMdMqUybDKw
juDEI/9bfU1lcKwrmz3O2+BtjjKAvpafkmO8l7tdufThcV4q5O8DIrGKZTqPwJNl
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDBlHz4n/FsRC6UfTd
-----END CERTIFICATE-----
```

U kunt het onder "CA-GTS-1C3" trustpoint importeren met behulp van de configuratieopdrachten:

```
(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

MIIFljCCA36gAwIBAgINAgO8U1lrNMcY9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU
<snip>
juDEI/9bfU1lcKwrmz3O2+BtjjKAvpafkmO8l7tdufThcV4q5O8DIrGKZTqPwJNl
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDBlHz4n/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)#
```

En dan kunt u bevestigen dat het certificaat is geïnstalleerd:

```
# 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 B1108A51 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
```

Vervolgens kunt u de certificaten installeren voor de andere twee emittenten.

CA-GTS-Root-R1:

Configuratie:

Spoiler (Markeren om te lezen)

```
(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
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU
<snip>
2tIMPNuzjsmhDYAPexZ3FL//2wmUspO8IFgV6dtxQ/PeEMMA3KgqlbbC1j+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 authenticeren CA-GTS-Root-R1Voer het basis 64 gecodeerde CA-certificaat in.Einde met een lege regel of het woord "ophouden" op een regel zelfMIIFVzCCAz+gIBAgINAgPlk28xsBNJGuiFzANBgkqhkiG9w0BAQwFADBHMQCQYDVQQGEJVUzMC MZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU<snip>2tIMPNuzjsmhDYAPexZ3FL//2wmUspO8IFgV6dt VNguV/u3gm3cCertificaat heeft de volgende eigenschappen:Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40 Fingerprint SHA1: E58C1C4 913B3863 4BE9106E3AD8E6B 9DD9814A% Accepteer dit certificaat? [ja/nee]: jaTrustpoint CA-certificaat geaccepteerd.% certificaat met succes geïmporteerd (configuratie)# einde

Verificatie in actieve configuratie:

Spoiler (Markeren om te lezen)

```
# 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
  BFFFDB09 94B293BC 205815E9 DB7143F3 DE10C300 DCA82A95 B6C2D63F 906B76DB
  6CFE8CBC F270350C DC991935 DCD7C846 63D53671 AE57FBB7 826DDC
    quit
```

show run | sec crypto pki certificaatketen CA-GTS-Root-R1crypto pki certificaatketen CA-GTS-Root-R1 certificate ca 0203E5936F31B01349886BA217 30820557 3082033F A0030201 02020D02 03E5936F 31B01349 86BA217 300D0609 2A864886 F70D010C050030 B30 47310 09060355 <snip> 6775C119 3A2B474E D3428EFD 31C04061302 DAD20C3C DBB38EC9 A10D800F 7B55533122 BFDB09 94B293BC 30200603E9 DB7143F3 DE10C300 DCA82A95 B6C SF63F 906B76DB 6CFE8CBC F81666C DC167714 DCD7C846 63D205815 270350 991935 53671 AE57FBB7 826DDC afsluiten

Crypto verificatie tonen:

Spoiler (Markeren om te lezen)

```
# 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
```

toon crypto pki certificaten breedsprakig CA-GTS-Root-R1CA Certificaatstatus: Beschikbare versie: 3 Certificaat Serienummer (hex): 0203E5936F31B01349886BA217 Certificaatgebruik: Handtekening Afgever: cn=GTS Root R1 o=Google Trust Services LLC c=US Onderwerp: cn=GTS Root R1 o=Google Trust Services LLC c=US Geldigheid Datum: 00:00 UTC Jun 22016: 00:00:00 UTC Jun 22 2036 Onderwerp Key Info: Public Key Algoritme: rsaEncryption RSA Public Key: (4096 bit) Signature Algoritme: SHA384 met RSA Encryption Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40 Fingerprint SHA1: E58C1C4 913B 863 4BE9106E E3AD8E6B 9D9814A X509v3 uitbreidingen: X509v3 Key Usage: 86000000 Digital Signature Key Cert Sign CRL Signature X509v3 Onderwerp Key ID: E4AF2B26 711A2B48 27852F52 662CEFF0 8913713E X509v3 Basisbeperkingen: CA: TRUE Authority Access: Cert Info tijd installeren 4:39:38 UTC Mar 13 2023 Cert installeert tijd in nsec: 1678718378546968064 Associated Trustpoints: CA-GTS-Root-R1 Trustpool

CA-GlobalSign-Root:

Dit certificaat is gevonden op deze locatie:

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

Configuratie:

Spoiler (Markeren om te lezen)

```
(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

MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
<snip>
DKqC5JlR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyICh3WZlXi/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 authenticeren CA-GlobalSign-RootVoer het basis 64 gecodeerde CA-certificaat in.Einde met een lege regel of het woord "ophouden" op een regel zelfMIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYKoZIhvcNAQEFBQAwVzELMAkGA1UEBQUxGJhbFNpZ24gbnYTC2EXEDAOBgNVBAsTB1JV<snip>DKqC5JlR3XC321Y9YeRQ4VzW9v493kHMB65jUEjJKSZp4A==Certificate heeft de volgende kenmerken:Vingerafdruk MD5: 3E455215 095192E1 B75D379F B187298A Vingerafdruk SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C% Accepteert u dit certificaat? [ja/nee]: jaTrustpoint CA-certificaat geaccepteerd.% certificaat met succes geïmporteerd (configuratie)# einde

Verificatie in actieve configuratie:

Spoiler (Markeren om te lezen)

```
# 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 certificaatketen CA-GlobalSign-Rootcrypto pki certificaatketen CA-

GlobalSign-Root certificate ca 040000000001154B5AC394 30820375 3082025D A0030201 02020B04 00000000B5A C394300D 06092A86 <snip> 2AC45631 95D01154 852BF96C A65D469D 0CAA82E4 9951D70 B7D63D 61E 46AE1 5CD6F6FE 3D41CC 07AE6352 BF535F4 2BE9C7FD B6F7825F 85D06789 DB81B304 1C51FA4 806F1520 C9DE0C88 0A1D6655E2FC48 C24118 9292669 E0 quit

Crypto verificatie tonen:

Spoiler (Markeren om te lezen)

```
#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 certificaten verbose CA-GlobalSign-RootCA CertificateStatus: BeschikbaarVersie: 3Certificate Serial Number (hex): 040000000001154B5AC394Certificate Gebruik: SignatureIssuer: cn=GlobalSign Root CAou=Root CAo=GlobalSign nv-sac=BESubject: cn=GlobalSign Root CAou=Root CAo=GlobalSign nv-sac=BEValidity Datum: 12:00:00 UTC Sep199 einddatum: 12:00:00 UTC Jan 28 2028Onderwerp Belangrijke info:Public Key Algoritme: rsaEncryptionRSA Public Key: (2048 bit)Signature Algorithm: SHA1 met RSA EncryptionFingerprint MD5: 3E455215 095192E1 B75D379F B187298A Fingerprint SHA1: B1BC968B D4F49D62 2AA89A21501521 A41D829C X509v3 extensies:X509v3 Key Usage:

6000000Key Cert SignCRL SignatureX509v3 Onderwerp Key ID: 607B61A 450D97CA 89502F7D 04CD34A8 FCFD4B X509v3 Basic Constraints:CA: TRUEAuthority Info Access:Cert installatietijd: 03:01 Mar 16 2023 Cert installeer tijd in nsec: 1678935781942944000Associated Trustpoints: CA-GlobalSign-Root

CA-Gmail-SMTP:

Het TLS-certificaat voor Gmail's servers (CA-gmail-SMTP) is gevonden met behulp van de hier beschreven stappen: Gebruik TLS-certificaten voor veilig transport

Configuratie:

Spoiler (Markeren om te lezen)

```
(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
MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
<snip>
b1J2gZAyjyd4nfFRG1jeL5KrsfUR9hIXufqySvlPUoPuKSi3fvsIS21BYEXEe8uZ
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 authenticeren CA-gmail-SMTPEnteer de basis 64 gecodeerde CA-certificaat.Einde met een lege regel of het woord "ophouden" op een regel door zichzelfMIIEhjCCA26gIBAgIQUofgQKT+9wcSaLBP3d3w9DANBgkqhkiG9w0BAQsFADBGMQCQYDVQQ 1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM<snip>b1J2gZAyjyd4nfFRG1jeL5KrsfUR9hIXufqySvlPU 'CA-gmail -SMTP' is een ondergeschikte CA.but certificaat is geen CA certificaat.Handmatige verificatie vereistCertificaat heeft de volgende eigenschappen:Vingerafdruk MD5: 19651FBE 906A414D 6D57B783 946F30A2 Vingerafdruk SHA1: 4EF392CB EEB46D5E 47433953 AEF313F 4C6D2825% Accepteer dit certificaat? [ja/nee]: jaTrustpoint CA-certificaat geaccepteerd.% certificaat met succes geïmporteerd (configuratie)#

Verificatie in actieve configuratie:

Spoiler (Markeren om te lezen)

```
# 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 certificaatketen CA-gmail-SMTP crypto pki certificaatketen CA-gmail-SMTP certificaat ca 5287E040A4FEF7071268B04FDDDF0F4 30820486 3082036E A0030201 02021052 87E040A4 FEF70712 68B04FDD DDF0F430 0D06092A 864886F7 0D01010B 05003046 310B3009 06035504-06130255 <ABB> F5 11F53312230 B9FAB24A F94F5283 E2928B7 7EFB084B 6D61217 416045 C47BCB99 801C4969 E4D48E77 2FA3 stopcontact

Crypto verificatie tonen:

Spoiler (Markeren om te lezen)

```
# 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
```

toon crypto pki certificaten breedsprakig CA-gmail-SMTPCA CertificateStatus: BeschikbaarVersie: 3Certificate Serial Number (hex): 5287E040A4FEF7071268B04FDDDF0F4Certificate Gebruik: SignatureIssuer: cn=GTS CA 1C3o=Google Trust Services LLC=USSubject: cn=smtp.gmail.comCRL Distribution points: http://crls.pki.goog/gts1c3/moVDfISia2k.crlValidity Datum: start datum: 09:15:03 UTC Feb 20 20 23end date: 09:15:02 UTC Mei 15 2023Onderwerp Key Info:Public Key Algoritme: ecEncryptionEC Public Key: (256 bit)Signature Algoritme: SHA256 met RSA EncryptionFingerprint MD5: 19651FBE 906A414D 6D57B783 946F30A2 Fingerprint SHA1: 4EFEEB46CB5E 47433953 AEF313F 4C6D2825 X509v3 extensions:X509v3 Key Usage: 80000000Digital SignatureX509v3 Onderwerp Key ID: 5CC36972 D07FE97 510E1A67 8A8ECC23 E40CFB68 X509v3 Basic Constraints:CA: FALSEX509v3 Onderwerp Alternatieve naam: IP Adres: AndereNamen: X509v3 Instantie Key ID: 8A747FAF 85CDEE95 CD3D9CD0 E24614F3 71351D27 Instantie Info: OCSP URL: http://ocsp.pki.goog/gts1c3CA http://pki.goog/repo/certs/gts1c3.derX509v3 EMITTENTEN: smtp.gmail.com CertificatePolicies:Beleid: 2.23.140.1.2.1Uitgebreid sleutelgebruik:Server AuthCert installatietijd: 03:10:41 UTC Mar 16 2023 Cert installeert tijd in nsec: 1678936241822955008:::: CA-Gmail-SMTP

Een eenvoudiger manier om de certificaten te vinden

U kunt ook proberen om een openssl-gesprek van een server/laptop te gebruiken als een gemakkelijkere manier om de certificaten van een SMTP-server te krijgen zonder dat u debugs en zoekacties van Google hoeft te gebruiken om ze op te sporen:

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

U kunt ook use smtp.gmail.com:

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

De uitkomsten van die oproep zullen de daadwerkelijke certificaten zelf bevatten die kunnen worden gebruikt voor de configuraties "crypto pki authenticate <trustpoint>".

EEM opnieuw testen met beveiligde SMTP

Nu de certificaten worden toegepast op het Cisco IOS XE-apparaat, zal het EEM-script de

beveiligde SMTP-berichten verzenden zoals verwacht.

```
# event manager run SendSecureEmailEEM
```

Controleer de Spoiler voor de volledige crypto en ssl debug uitgangen:

Spoiler (Markeren om te lezen)

```
# 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:pri
*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 SendSecure EmailEEM*Mar 16 03:28:50.673: CRYPTO_OPSSL: Toegewezen geheugen voor OPSSLContext*Mar 16 03:28:50.673: CRYPTO_OPSSL: Stel algoritme specificaties in op masker 0x02FC000 voor versie 128*Mar 16 03:28:50.674: Stel de

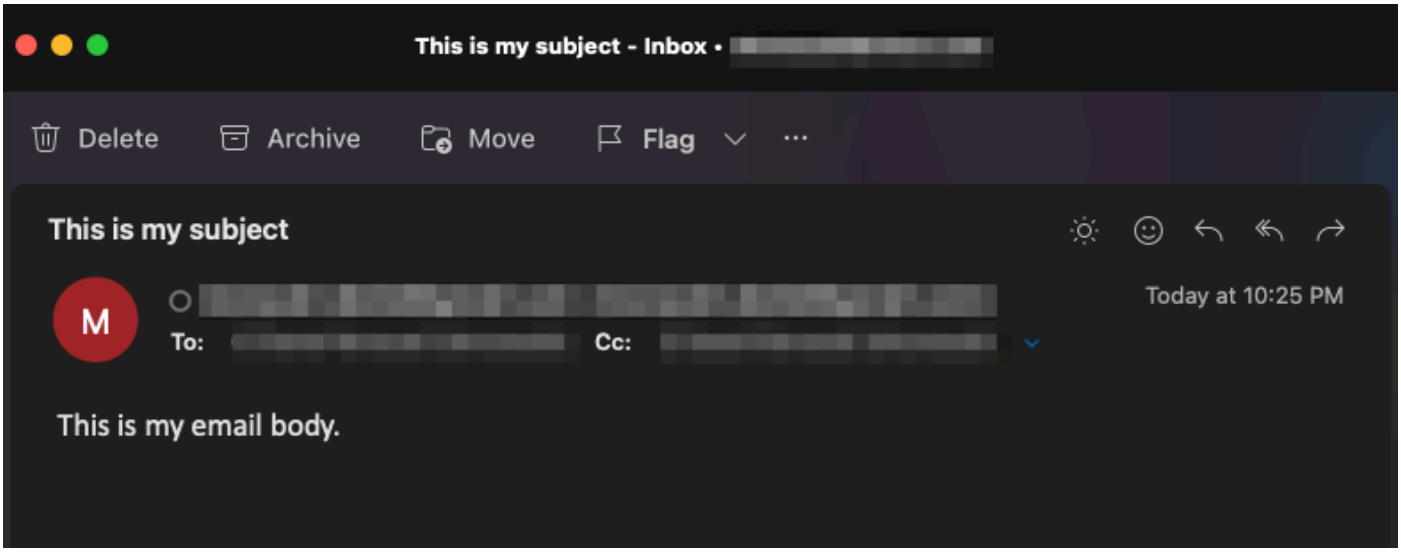
standaard EC Curve lijst in: 0x7 de EC curve list: secp521r1:secp384r1:prime256v1*Mar 16 03:28:50.674: opssl_SetPKIInfo entry*Mar 16 03:28:50.674: CRYPTO_PKI: (A069B) Session begonnen - identiteit geselecteerd (TP-self-signed-486541296-)xTP-self-signed-486541296:hercount na increment = 1Mar 03:28:50.674: CRYPTO_PKI: Begin met lokale cert ketting ophalen.*Mar 16 03:28:50.674: CRYPTO_PKI(Cert Lookup) issuer="cn=IOS-Self-Signed-Certificate-486541296" serienummer= 01*Mar 16 03:28:50.674: CRYPTO_PKI: op zoek naar cert in handle=7F41E53CE0, digest=1C0 F 3D 52 67 66 D5 59 E2 66 58 E7 8B E7 9B 8E*Mar 16 03:28:50.675: CRYPTO_PKI: Gereed met lokale cert ketting halen 0.*Mar 16 03:28:50.675: CRYPTO_PKI: Rcvd verzoek om beëindiging PKI sessie A069B.*Mar 16 03:28:50.675:_PKI: PKI-sessie A069B is beëindigd. Alle resources bevrijden.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 is uitgeschakeld op deze sessie.Schakel de functie Common Criteria in CiscoSSL op SSL CTX 0x7F28EAFF8*Mar:1603 uit 8:50.675: CRYPTO_OPSSL: ciphersuites ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA 256:AES256-GCM-SHA384:AES256-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-GCM-SHA 56:DHE-RSA-AES128-SHA256:AES128-GCM-SHA256:AES128-SHA256*Mar 16 03:28:50.676: Handshake start: voor SSL initialisatie*Mar 16 03:28:50.676: SSL_connect:voor SSL initialisatie*Mar 16 03:28:50.6 6: >> ??? [lengte 0005]*Maart 16 03:28:50.676: 16 03 01 00 95*Maart 16 03:28:50.676: *Maart 16 03:28:50.676: >> TLS 1.2 Handdruk [lengte 0095], ClientHello*Maart 16 03:28:50.676: 01 00 0 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 schrijf client hello*Mar 16 03:2 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 schrijfclient hello*Mar 16 03:28:50.692: < TLS 1.2 Handshake [F00], 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 44 4F*Mar 16 03:28:50.69 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-serverextensie "onbekend" (id=23)=0TLS server extensie "heronderhandelen" (id=65281), len=1*Mar 16 03:28:50.693: 00*Mar 16 03:28:50.693: TLS server extensie "EC point formats" (id=11), len=2*Mar 16 03:28:50.693: 01 00*Mar 16 03:28:50.693: TLS ticket server extensie "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 Certificate9A [0F] * Maart 16 03:28:50.702: 0B 00 0F 96 00 0F 93 00 04 8A 30 82 04 86 30 82*Mrt 16 03:28:50.702: 03 6E A0 03 02 01 02 10 52 87 E0 40 A4 FE7<snip>*Maart 16 03:28 82 35 CF 62 8B C9 24 8B A5 B7 39 0C B 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 functie terug * Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Sessie gestart - identiteit niet gespecificeerd*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Toevoeging peer certificate*Mar 16 03:28:50.767: CRYPTO_PKI: Toegevoegd x509 peer certificate - (1162)*Mar 16 28:50.767: CRYPTO_PKI: (A069C) Toevoeging peer certificate*Mar 16 03:28:50.768: CRYPTO_PKI: Toegevoegd x509 peer certificate - (1434) bytes*Mar 16 03:28:50.768: CRYPTO_PKI: (A069C) Toevoeging peer certificate*Mar 16 03:28:50.70.7 20: CRYPTO_PKI: Toegevoegd 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"

serienummer= 52 87 E0 40 A4 FE7 68 B0 4F DD F0 F4*Mar 16 03:28:50.770: CRYPTO_PKI: op zoek naar zekerheid in handle=7F41E523CE0, samenvatting=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) emittent="cn=Go Root1=Google Trust Services LLC,c=US" serienummer= 02 03 BC 53 59 6B 34 C7 18 F5 01 50 66*Mar 16 03:28:50.771: CRYPTO_PKI: op zoek naar cert in handle=7F41E523CE0, samenvatting=03 9F CF 59 82 EE 09 CC 4F 53 AE D8 02 7E 4B AF*Mar 16 03:28 20.771: CRYPTO_PKI (Cert Lookup) issuer="cn=GlobalSign Root CA, ou=Root CA, o=GlobalSign nv-sa, c=BE" serienummer= 77 BD 0D 6C DB 36 F9 1A EA 21 0F C4 F0 58 D3 0D*Mar 16 03:28:50.771: CRYPTO_PKI: Looking for cert in handle=7F41E523CE0, digest=9 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 niet gevonden voor emittentenserie.*Mar 16 03:28:50.772: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()*Mar 16 03:28:50.772:: Gevonden een onderwerp match*Mar 16 03:#28:50.772: CRYPTO_PKI: ip-ext-val: IP extensie validatie niet vereist:Verhogende refcount voor context id-35 to 1*Mar 16 03:28:50.773: CRYPTO_PKI: creeer nieuw ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 35*Mar 16 03:28:50.773: CRYPTO_PKI: (A06: 9C)validatiepad heeft 1 certs*Mar 16 03:28:50.773: CRYPTO_PKI: (A069C) Controleer op identieke certs*Mar 16 03:28:50.773: CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA, ou=Root CA, o=GlobalSign nv-sa,c=BE" serienummer= 77 BD 0D 6C DB 36 F9 1A2F F0 58 D3 0D*Mar 16 03:28:50.774: CRYPTO_PKI: op zoek naar zekerheid in handle=7F41E523CE0, samenvatting=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 niet gevonden voor emittent.*Mar 160 28:50.774: CRYPTO_PKI: (A069C) Validatie van niet-vertrouwde cert*Mar 16 03:28:50.774: CRYPTO_PKI: (A069C) Maak een lijst van geschikte trustpoints*Mar 16 03:28:50.774: CRYPTO_PKI: crypto_pki_get_cert_record_by_issuer()*Mar16 03:28:58:5 774: CRYPTO_PKI: Found a issuer match*Mar 16 03:28:50.774: CRYPTO_PKI: (A069C) Geschikte trustpoints zijn: CA-GlobalSign-Root,*Mar 16 03:28:50.775: CRYPTO_PKI: (A069C) Poging tot validatie van certificaat met behulp van CA-GlobalSign-Root beleid*Mar 16 03:28:50.70.7 5: CRYPTO_PKI: (A069C) Gebruik van CA-GlobalSign-Root om certificaat te valideren*Mar 16 03:28:50.775: CRYPTO_PKI(maak vertrouwde certs keten)*Mar 16 03:28:50.775: CRYPTO_PKI: Toegevoegd 1 certs aan vertrouwde keten.*Mar 16 03:28:50.775: CRYPTO_PKI: Voorbereiden sessie herroeping service providers*Mar*Mar*Mar 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 0E6 99 8D CE A3 4F1 8B FB 25 6B EA 48 1F F1 2A 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: Het verwijderen van cached sleutel met sleutel id 45*Mar 16 03:28:50.781: CRYPTO_PKI: Poging om de peer's openbare sleutel in cache op te nemen*Mar 16 03:28:50.781: CRYPTO_PKI:Peer's publiek succesvol ingevoegd met sleutel id 46*Mar 16 03:28:50.781: P11:C_CreateObject: 131118*Mar 16 03:28:5 1.781: P11:C_GetMechanismInfo slot 1 type 3 (ongeldig mechanisme)*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: P1:C_verifyMarRecover - 131118 16 03:28:50.781: P11:gevonden schotel in cache met index = 46*Mar 16 03:28:50.781: P11:openbare sleutel gevonden: 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 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 cached sleutel van de peer met sleutel id 46*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C) Certificaat is geverifieerd*Mar 16 03:28:50.788: CRYPTO_PKI: Verwijderen sessie herroeping service

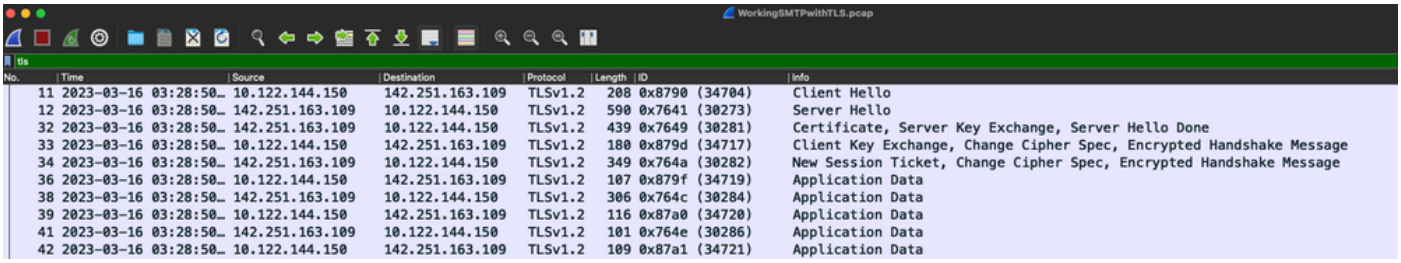
providers*Mar 16 03:28:50.788: CRYPTO_PKI: Verwijder sessie herroeping service providersCA-Global Sign-Root:validatie status - CRYPTO_PKI T_WITH_WARNING*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C) Certificaat gevalideerd zonder herroeping check:cert hertelling na toename = 1*Mar 16 03:28:50.790: CRYPTO_PKI: Populate AAA auth data*Mar 16 03:28:50.790: CRYPTO_PKI: Kan niet ingesteld worden voor primaire AAA-lijstautorisatie*Mar 16.:28:50.790: PKI: Cert-sleutelgebruik: Digital-Signature, Certificate-Signing, CRL-Signing*Mar 16:03:28:50.790: CRYPTO_PKI: (A069C)chain cert was verankerd aan trustpoint CA-GlobalSign-Root, en kettingvalidatieresultaat was: CRYPTO_GELDIG_CERT_WITH_WARNING*Mar 16 03:28:50.790: CRYPTO_PKI: (A0) 69C) Verwijderen verify context*Mar 16 03:28:50.790: CRYPTO_PKI: vernietigen ca_req_context type PKI_VERIFY_CHAIN_CONTEXT, ident 35, ref count 1:Decrementing refcount voor context id-35 to 0*Mar 16 03:28:50.790: CRYPTO_PKI: ca_req_context release*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Validatie TP is CA-GlobalSign-Root*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Certificaatvalidatie geslaagd*Mar 16 03:28:50.790: CRYPTO_OPSSL: Certificaatverificatie succesvol*Mar 16 03:28:50.790: CRYPTO_PKI: Rcvd verzoek om beëindiging PKI sessie*A069C. Mar 16 03:28:50.790: CRYPTO_PKI: PKI sessie A069C is beëindigd. Alle middelen vrijmaken.:bepaalde hertelling na decrement = 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 read server certificate*Mar 16 03:28:50.791: < TLS 1.2 Handshake [00] 3], 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: 0 D7 D5 9C 75 C0 7D 5B D6 B2 0A B5 C EA E1 4B*Mar 16 03:28:50.792: 4E E5 72 7B 54 5D 9B2 95 91 E0 C D6 A5 8E CE*Mar 16 03:28:50.792: 8D 36 C9 83 42 B0 4D AC 0C 03 00 46 304 2*mrt 16 03:28:50.792: 20 67 B3 F1 DA D1 BF 13 72 DD B6 B2 11 3B 6E 6F*mrt 16 03:28:50.793: 87 52 D9 00 F7 44 31 C3 C2 5E BE 2D FF 93 4E F0*mrt 16 03:28:50.793: A8 02 4 42 91 BE B7 10 1C D1 C0 12 28 FB 1F*mrt 16 03:28:50.793: E4 DE 81 0B AA 66 19 CD 28 5A A0 30 7D 3C 4A 56*mrt 16 03:28:50.793: 0D 94 E2*mrt 16 03:28:50.793: *Mar 16 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 6 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>*mrt 16 03:28:50.796: P11:C_FindObjectsFinal*mrt 16 03:28:50.796: p11:c_verifyverify - Sessie gevonden*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 004], 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: >> ??? [lengte 0005]*Maart 16 03:28:50.810: 16 03 03 00 46*Maart 16 03:28:50.811: *Maart 16 03:28:50.811: >> TLS 1.2 Handdruk [lengte 0046], ClientKeyExchange*Maart 16 03:28:50.810: 10 00 42 41 04 26 C3 EF 02 05 6C 82 D1 90 B3*Mar 16 03:28:50.811: 17 31 9A CD 8C 81 91 BA E8 C0 86 40 7B 2C E4*Mar 16 03:28:50.811: 9A 2C 18 9D1 6A C0 56 A0 98 2E B7 3B *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 TLS schrijven client key exchange*Mar 16 03:28:50.812: >> ??? [lengte 0005]*mrt 16 03:28:50.812: 14 03 03 00 01*mrt 16 03:28:50.812: *mrt 16 03:28:50.812: >> TLS 1.2 ChangeCyperSpec [lengte 0001]*mrt 16 03:28:51.16: > ???>>> [lengte 0005]*Maart 16 03:28:51.116: 17 03 03 00 35*Maart 16 03:28:51.116: *Maart 16 03:28:51.116: >> ??? [lengte

0005]*Maart 16 03:28:51.116: 17 03 03 00 1A*Maart 16 03:28:51.116: *Maart 16 03:28:51.116: >> ??? [lengte 0005]*Maart 16 03:28:51.116: 17 03 03 00 30*Maart 16 03:28:51.116: *Maart 16 03:28:51.116: >> ??? [lengte 0005]*Maart 16 03:28:51.116: 17 03 03 00 1B*Maart 16 03:28:51.117: *Maart 16 03:28:51.713: << ??? [lengte 0005]*Maart 16 03:28:51.713: 17 03 03 00 6D*Maart 16 03:28:51.713: *Maart 16 03:28:51.714: >> ??? [lengte 0005]*Maart 16 03:28:51.714: 17 03 03 00 1E*Maart 16 03:28:51.714: *Maart 16 03:28:51.732: << ??? [lengte 0005]*Maart 16 03:28:51.732: 17 03 03 00 71*Maart 16 03:28:51.732:

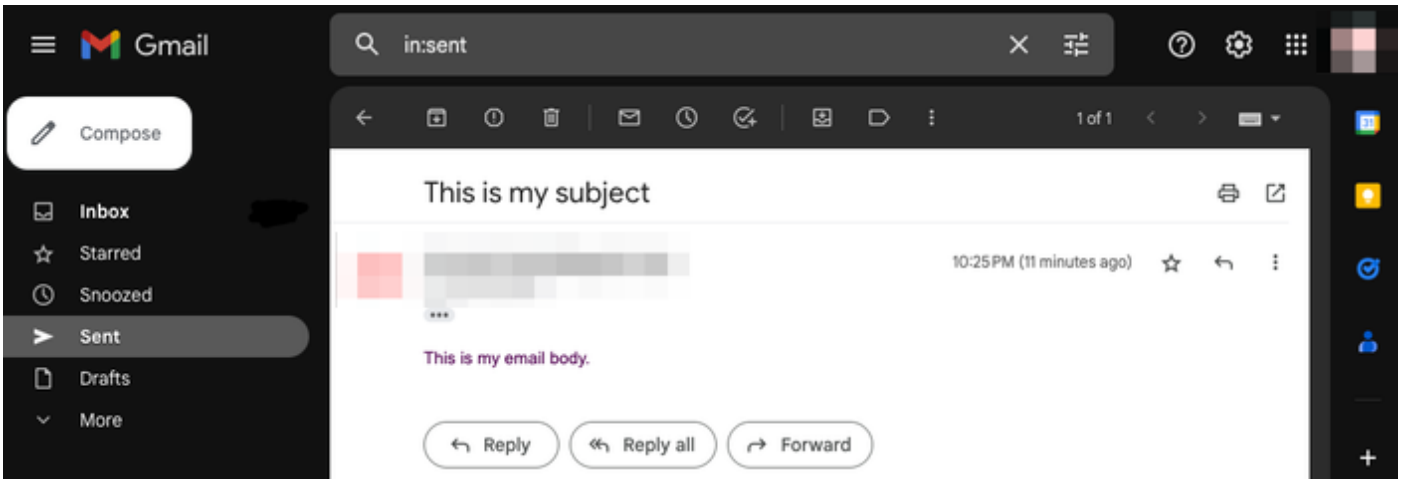
U kunt verifiëren dat de e-mail is ontvangen en dat alle velden (van, naar, van, cc, onderwerp, lichaam) correct zijn ingevuld:



U kunt ook controleren of de TLS-handdruk en sessie vanaf de pakketopname op het Cisco IOS XE-apparaat hebben plaatsgevonden (in bijlage als "WorkingSMTP met TLS.pcap"):



U kunt zelfs controleren of de e-mails worden weergegeven in de map "Verzonden" van de gebruikte e-mailaccount:



Andere voorbehouden en overwegingen

Gebruikersnamen met @-symbolen

Problemen kunnen worden gezien bij het gebruik van een SMTP-relay. Vanwege het SMTP-relay heeft de serverstring deze indeling (een "@" in de gebruikersnaam):

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

De code om de gebruikersnaam en het wachtwoord te parsen, splitst de string bij het eerste voorkomen van het "@" symbool. Dientengevolge denkt het systeem dat de server hostname begint onmiddellijk na het eerste "@" symbool door de rest van de string, en het interpreteert alles daarvoor als de "gebruikersnaam:wachtwoord".

De TCL-implementatie van SMTP maakt gebruik van een Regular Expression (regex) die deze gebruikersnaam/wachtwoord/server-informatie op verschillende wijze verwerkt. Wegens dat verschil, staat TCL gebruikersnamen met een "@"symbool toe; nochtans, steunt Cisco IOS XE TCL geen crypto, zodat is er geen optie om veilige e-mails over TLS te verzenden.

Kort samengevat:

- Als de e-mail beveiligd moet zijn, dan kunt u deze niet verzenden met TCL.
- Als er een '@' in uw gebruikersnaam staat, kunt u deze niet verzenden met een EEM.

Cisco bug-id CSCwe75439 is gedeponeerd om deze kans te grijpen om de EEM e-mailfunctie te verbeteren; er is momenteel echter geen routekaart voor dit verbeteringsverzoek.

Conclusie

Zoals hier getoond, is het mogelijk om beveiligde e-mails via SMTP te verzenden met TLS met behulp van de Embedded Event Manager (EEM) applet. Het vereist enige installatie aan de serverkant, evenals het configureren van de benodigde certificaten om vertrouwen toe te staan,

maar het is haalbaar als u geautomatiseerde, veilige, e-mail meldingen wilt genereren.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.