Utilizzo di EEM per automatizzare la protezione dei messaggi di posta elettronica inviati all'utente

Sommario

Introduzione

Questo documento descrive il processo necessario per utilizzare l'azione "server di posta" in Embedded Event Manager (EEM) in Cisco IOS® XE per inviare e-mail sicure a un server SMTP (Simple Mail Transfer Protocol) con TLS (Transport Layer Security) sulla porta 587.

Durante questo processo è possibile incontrare molte avvertenze, motivo per cui questo articolo è stato redatto per documentare i passaggi necessari a tale scopo.

Scenario d'uso

Molti clienti apprezzano la possibilità di ricevere automaticamente una notifica via e-mail dopo che si verifica un determinato evento. Il sottosistema EEM è un potente strumento per il rilevamento di eventi di rete e l'automazione integrata e può fornire un modo efficiente per automatizzare le notifiche e-mail su un dispositivo Cisco IOS XE. Ad esempio, è possibile monitorare una traccia IPSLA e, in risposta a un syslog che indica una modifica dello stato, eseguire un'azione e avvisare gli amministratori di rete dell'evento via e-mail. Questa idea di "notifica via e-mail" potrebbe essere applicata a molti altri scenari come mezzo per portare l'attenzione su qualsiasi evento particolare che si desidera evidenziare.

Introduzione

PEM è l'acronimo di Privacy Enhanced Mail ed è un formato spesso utilizzato per rappresentare certificati e chiavi. Questo è il formato del certificato utilizzato dai dispositivi Cisco IOS XE. Le

applicazioni sicure (come HTTPS o SMTP sicuro) hanno spesso un "PEM in pila", in cui sono coinvolti più certificati, tra cui:

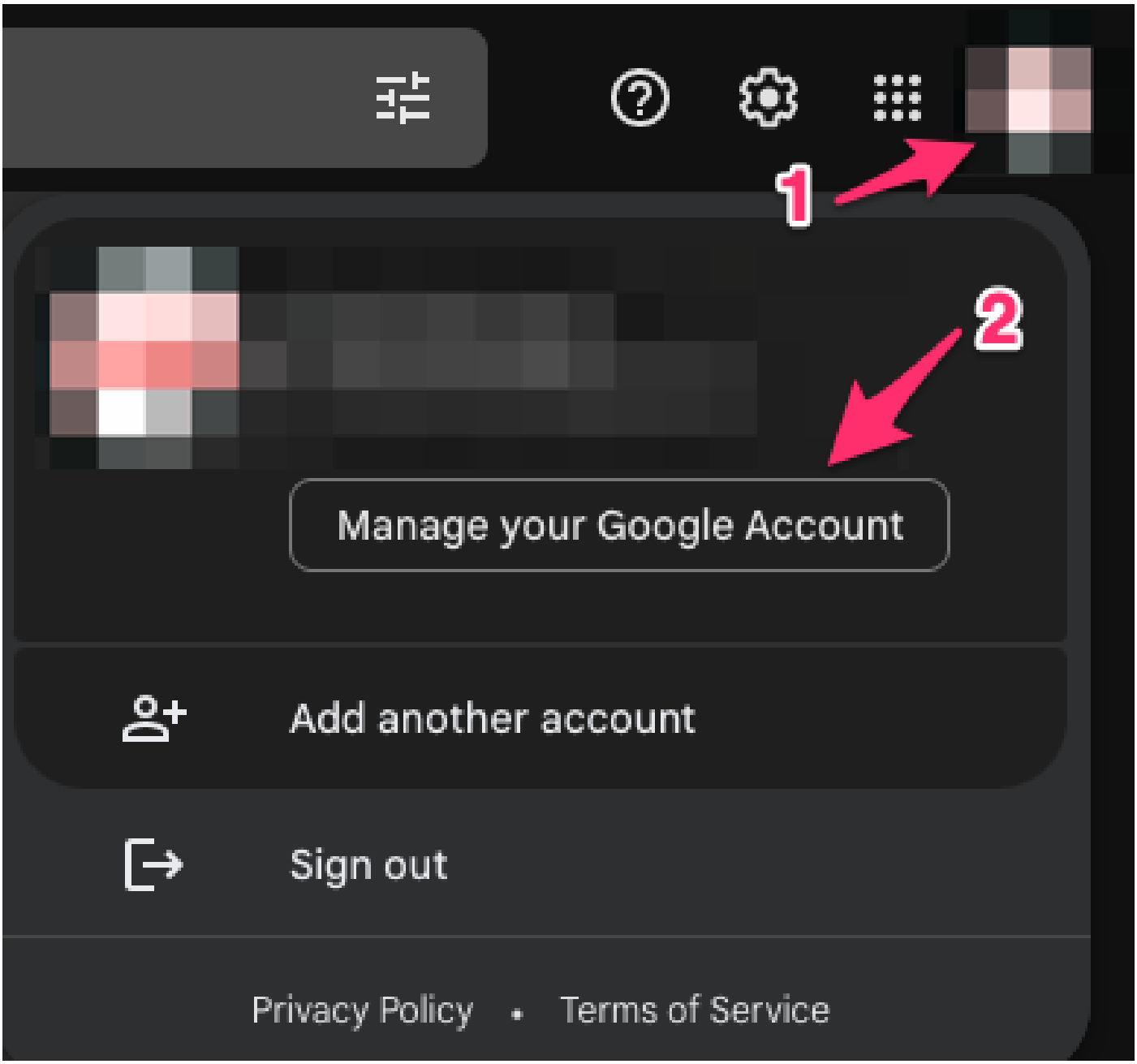
- Certificato radice
- Certificato di firma (intermedio)
- Certificato utente finale (o server)

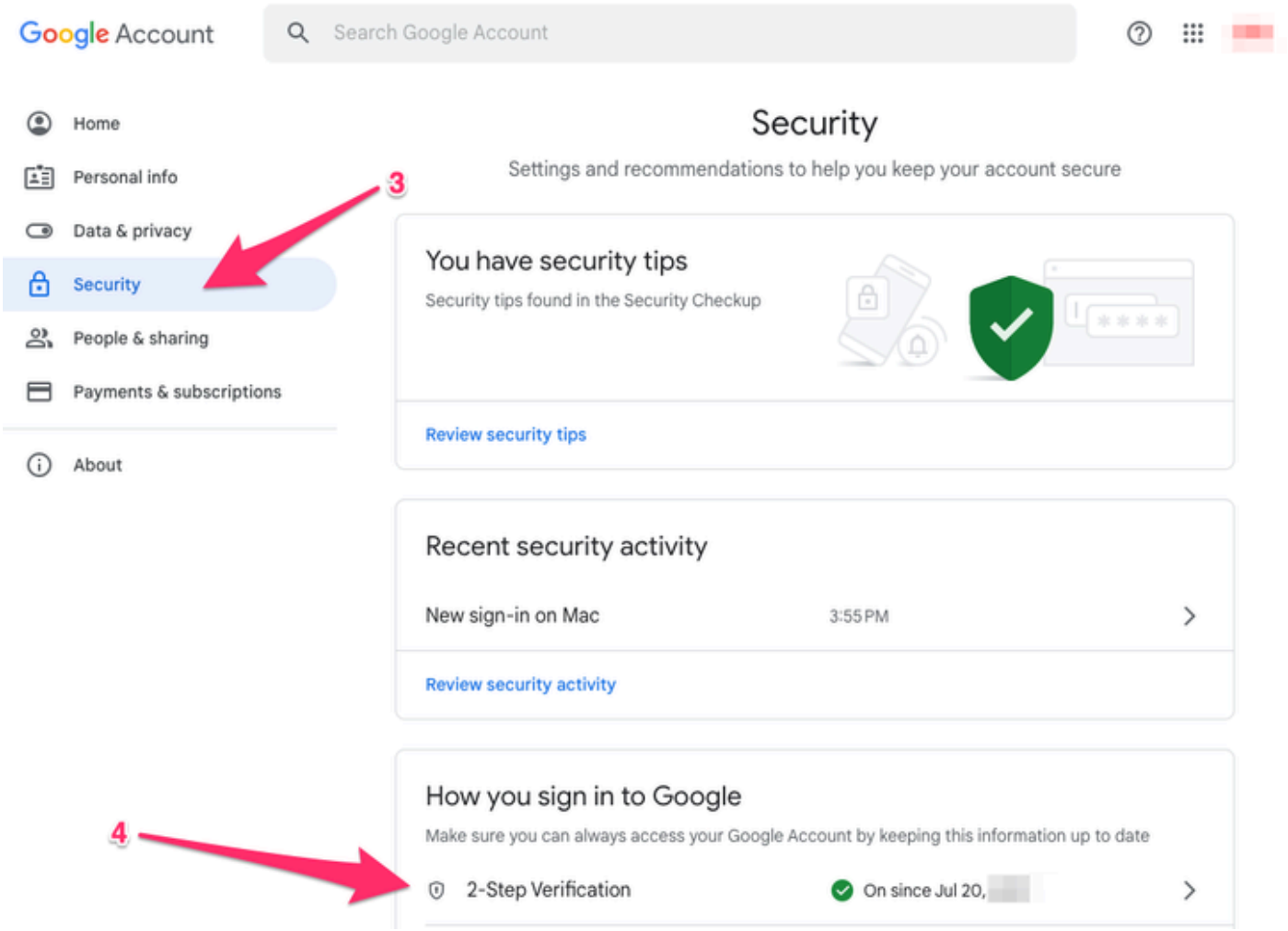
Impostazione account Gmail

I servizi SMTP di Google verranno utilizzati come esempio in questo articolo. I prerequisiti sono l'utilizzo di un account Gmail impostato in precedenza.

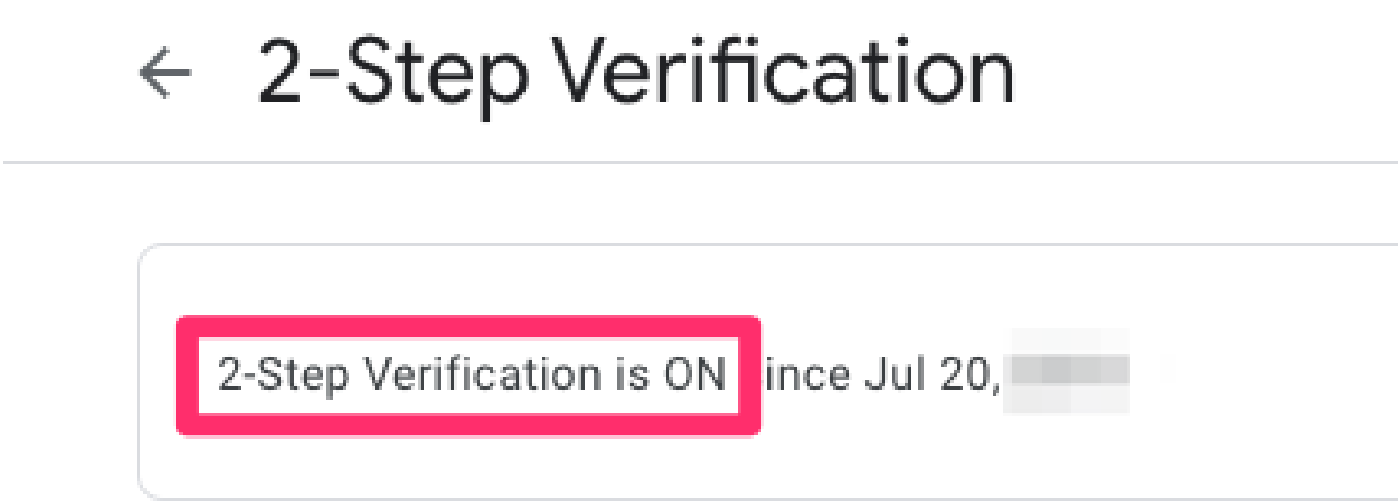
Google consente di inviare e-mail da client remoti a Gmail. C'era un'impostazione in Gmail per "app non protette", e l'applicazione avrebbe dovuto affrontare un errore se questa impostazione non fosse stata consentita alla fine di Google. L'impostazione è stata rimossa e al suo posto è disponibile l'opzione "Applicazioni sicure", accessibile tramite:

mail.google.com > Fai clic sul tuo profilo (#1) > Gestisci il tuo account Google (#2) > Sicurezza (#3) > Come accedi a Google > Verifica in due passaggi (#4)


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



Da questa pagina, verificare che la verifica in due passaggi sia attivata.



Puoi quindi scorrere verso il basso fino a "Password dell'app" per fare in modo che Gmail generi una password che possa essere utilizzata per accedere al tuo account Google da un'applicazione che non supporta la verifica in due passaggi.

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

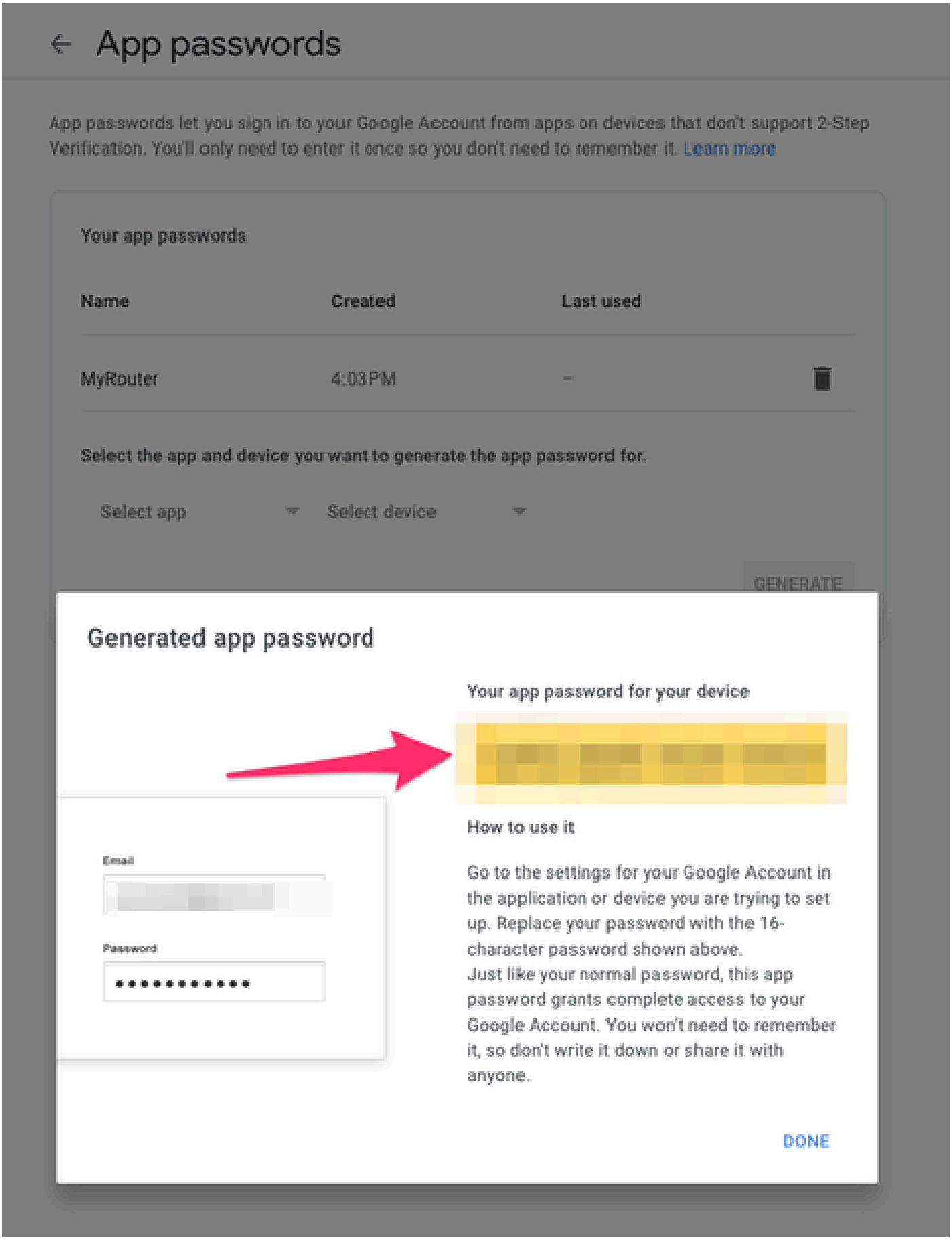
App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. Learn more

You don't have any app passwords.

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

MyRouter

GENERATE



La password dell'applicazione di 16 caratteri in questa schermata è stata sfocata in quanto è legata a un account Gmail personale.

Ora che si dispone di una password dell'applicazione per Gmail, è possibile utilizzarla, insieme al nome dell'account Gmail, come server di posta elettronica da utilizzare per l'inoltro del messaggio. Il formato per specificare il server è "nomeutente:password@host".

Configurazione EEM di base

Esistono molti modi per personalizzare uno script EEM in base alle proprie esigenze specifiche, ma questo esempio è uno script EEM di base per l'esecuzione della funzionalità di protezione della posta elettronica:

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

Le configurazioni creano innanzitutto tre variabili di ambiente EEM: _email_from, _email_to e _email_server. Ciascuna variabile viene definita in modo da semplificare le modifiche alla configurazione. È quindi possibile creare lo script SendSecureEmailEM. L'evento di attivazione è "none", pertanto è possibile eseguire manualmente lo script EEM in qualsiasi momento utilizzando "# event manager run SendSecureEmailEEM" (anziché attendere l'attivazione di un evento specifico). In seguito, si dispone di un'unica azione "server di posta" che si occupa della generazione dell'e-mail. Le opzioni "secure tls" e "port 587" indicano al dispositivo di negoziare TLS sulla porta 587, su cui i server Gmail saranno in ascolto.

È inoltre necessario verificare che il campo "Da" sia valido. Se si sta eseguendo l'autenticazione come "Alice" ma si sta tentando di inviare un messaggio di posta elettronica da "Bob", si verificherà un errore perché Alice sta falsificando l'indirizzo di posta elettronica di qualcun altro. Il campo "Da" deve essere allineato con l'account utilizzato per inviare l'e-mail sul server.

Problema rilevato solo con i certificati predefiniti installati

EEM utilizza openssl per stabilire una connessione con il server SMTP. Per una comunicazione sicura, il server invia un certificato a openssl in esecuzione in Cisco IOSd. IOSd cercherà quindi un trust point associato a tale certificato.

In un dispositivo Cisco IOS XE, i certificati per i server SMTP Gmail non vengono installati per impostazione predefinita. Per stabilire l'attendibilità, è necessario importarle manualmente. Senza i certificati installati, l'handshake TLS non riuscirà a causa di un "certificato errato".

Questi debug sono estremamente utili per il debug dei problemi relativi ai certificati:

```
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
```

È possibile avviare Embedded Packet Capture (EPC) sul router per acquisire qualsiasi traffico da o verso il server e-mail quando viene attivato EEM:

```
! 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
```

In ultima analisi, openssl non è in grado di stabilire una sessione TLS sicura con il server SMTP,

quindi viene generato un errore di "certificato errato" che determina l'interruzione dell'esecuzione di EEM:

```
*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
```

L'acquisizione dei pacchetti documentata da questo scambio viene allegata come "NoCertificateInstalled.pcap". Il pacchetto TLS finale inviato dal router (10.122.x.x) al server SMTP Gmail (142.251.163.xx) mostra che la negoziazione TLS è stata terminata a causa dello stesso messaggio "Bad Certificate" (Certificato non valido) visualizzato nei debug precedenti.

```
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)
```

Certificati per la protezione di SMTP

Poiché mancano i certificati che consentono al dispositivo Cisco IOS XE di considerare attendibili i server Gmail, è possibile installare uno o tutti i certificati in un trust point sul dispositivo.

Ad esempio, i debug completi del test precedente mostrano le seguenti ricerche di certificati eseguite:

```
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
```

Per consentire al dispositivo di stabilire una sessione protetta con i server Gmail SMTP, è necessario installare un certificato per ognuna di queste autorità in un trust point. È possibile creare un trust point per ogni autorità emittente utilizzando le configurazioni seguenti:

```
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
```

A questo punto si dispone di un trust point per ogni emittente impostato, tuttavia non sono ancora presenti certificati effettivi associati. Si tratta essenzialmente di trust vuoti:

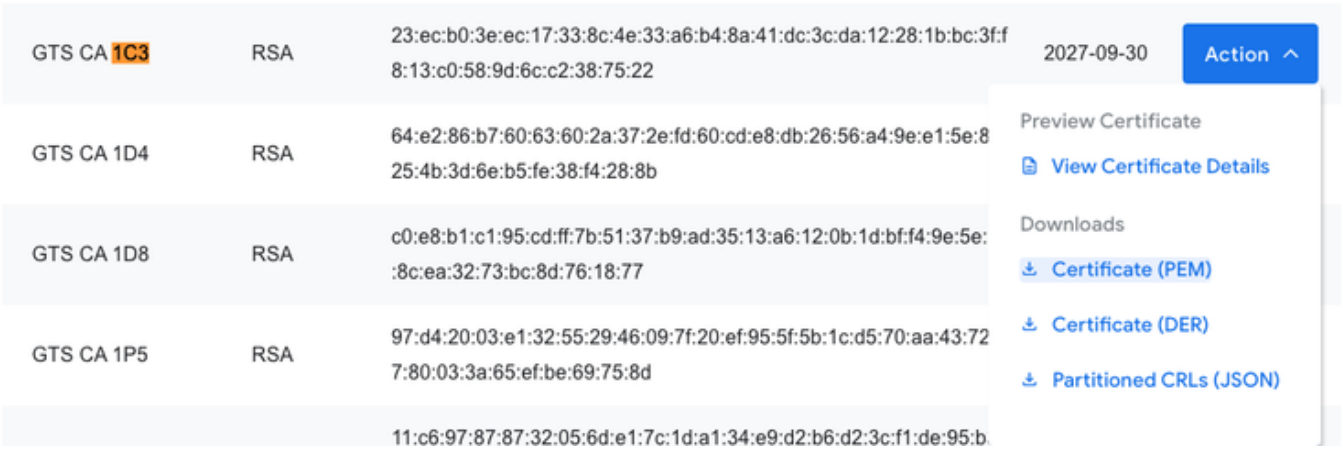
```
# show run | sec crypto pki certificate chain CA-
crypto pki certificate chain CA-GTS-1C3
crypto pki certificate chain CA-GTS-Root-R1
crypto pki certificate chain CA-GlobalSign-Root
crypto pki certificate chain CA-gmail-SMTP
```

È necessario individuare la posizione di tali certificati e quindi installarli nel dispositivo.

Cercando online "Google Trust Services 1C3", ci imbattiamo rapidamente nel Google Trust Services Repository dei certificati:

https://pki.goog/repository/

Dopo aver espanso tutti i certificati presenti nella pagina, è possibile cercare "1C3", fare clic sull'elenco a discesa "Azione" e scaricare il certificato PEM:



Se si apre il file PEM scaricato con un editor di testo, viene mostrato che si tratta solo di un certificato che può essere importato nel dispositivo Cisco IOS XE sotto il trust point creato in precedenza:

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

È possibile importarlo nel trust point "CA-GTS-1C3" utilizzando i comandi di configurazione riportati di seguito.

```
(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)#
```

È quindi possibile verificare che il certificato sia stato installato:

```
# 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 B1100BA51 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
```

Successivamente, è possibile installare i certificati per gli altri due emittenti.

CA-GTS-Root-R1:

Configurazione:

Spoiler (Evidenziato da leggere)

```
(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 autentica CA-GTS-Root-R1Immettere il certificato CA codificato in base 64.Terminare con una riga vuota o la parola "quit" su una riga a parte MIIFVzCCAz+gAwIBAgINAgPlk28xsBNJiGuiFzANBgkqhkiG9w0BAQwFADBHMQswCQYDVQQGEwJVUzI MZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU<snip>2tIMPNuzjsmhDYAPexZ3FL//2wmUspO8IFgV6dt ha i seguenti attributi:Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40 Fingerprint SHA1: E58C1C4 913B3863 4BE9106E E3AD8E6B 9DD9814A% Accettare questo certificato? [yes/no]: sìCertificato CA Trustpoint accettato.% Certificato importato correttamente(config)# fine

Verifica configurazione in esecuzione:

Spoiler (Evidenziato da leggere)

```
# 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 catena di certificati CA-GTS-Root-R1crypto pki catena di certificati CA-GTS-Root-R1 ca 0203E5936F31B01349886BA217 30820557 3082033F A0030201 02020D0203E593 F 31B01349 886BA217 300D0609 2A864886 F70D0101 0C050030 47310B30 09060355 04061302 5553122 3020 0603 <snip> 6775C119 3A2B474E D3428EFD 31C81666 DAD20C3C DBB38EC9 A10D800F 7B167714 BFDB09 94B293BC 205815E9 DB7143F3 DE3 0C300 DCA82A95 B6C2D63F 906B76DB 6CFE8CBC F270350C DC991935 DCD7C846 63D53671 AE57FBB7 826DDC quit

Mostra verifica della crittografia:

Spoiler (Evidenziato da leggere)

```
# 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 Stato del certificato: Disponibile Versione: 3 Certificato Numero di serie (hex): 0203E5936F31B01349886BA217 Uso del certificato: Signature Issuer: cn=GTS Root R1 o=Google Trust Services LLC=US Oggetto: cn=GTS Root R1 o=Google Trust Services LLC=US Data di inizio: 00:00:0 C Jun 22 2016 data di fine: 00:00:00 UTC Jun 22 2036 Informazioni sulla chiave del soggetto: Chiave pubblica Algoritmo: rsaEncryption RSA Chiave pubblica: (4096 bit) Algoritmo della firma: SHA384 con RSA Encryption Fingerprint MD5: 05FED0BF 71A8A376 6 63DA01E0 D852DC40 Fingerprint SHA1: 58C1C4 913B3863 4BE9106E E3AD8E6B 9DD9814A X509v3 estensioni: X509v3 Utilizzo chiave: 86000000 Digital Signature Signature Signature CRL Signature X509v3 ID chiave oggetto: E4AF2B26 711A2B48 27852F62 62CEFF0 8913713E X509v3 Vincoli di base: CA: TRUE Informazioni sull'autorità Accesso: Ora di installazione del certificato: 14:39:38 UTC Mar 13 2023 Ora di installazione del certificato in nsec: 1678718378546968064 Trust point associati: CA-GTS-Root-R1 Trust pool

CA-GlobalSign-Root:

Il certificato è stato trovato nel seguente percorso:

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

Configurazione:

Spoiler (Evidenziato da leggere)

```
(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>
DKqC5Jl R3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/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 autentica CA-GlobalSign-RootImmettere il certificato CA codificato in base 64.Terminare con una riga vuota o la parola "quit" su una riga da solaMIIDdTCCAl2gAwIBAgILBAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkGA1UEBhMCQ
jJKSZp4A==Il certificato ha i seguenti attributi:Impronta digitale MD5: 3E455215 095192E1 B75D379F B187298A Impronta digitale SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C% accetti questo certificato? [yes/no]: sìCertificato CA Trustpoint accettato.% Certificato importato correttamente(config)# fine

Verifica configurazione in esecuzione:

Spoiler (Evidenziato da leggere)

```
# 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 catena di certificati CA-GlobalSign-Rootcrypto pki catena di certificati CA-GlobalSign-Root certificato ca 040000000001154B5AC394 30820375 3082025D A0030201 02020B04 000000015 4B5A C394300D 06092A86 <snip> 2AC45631 95D06789 852BF96C A65D469D 0CAA82E4 9951DD70 B7DB563D 61E46AE1 5CD6F6FE 3DDE41CC 07AE66 52 BF5353F4 2BE9C7FD B6F7825F 85D24118 DB81B304 1CC51FA4 806F1520 C9DE0C88 0A1DD6655E2FC48 C9292669 E0 quit

Mostra verifica della crittografia:

Spoiler (Evidenziato da leggere)

```
#show crypto pki certificates verbose CA-GlobalSign-Root
CA Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 040000000001154B5AC394
Certificate Usage: Signature
Issuer:
cn=GlobalSign Root CA
ou=Root CA
o=GlobalSign nv-sa
c=BE
Subject:
cn=GlobalSign Root CA
ou=Root CA
o=GlobalSign nv-sa
c=BE
Validity Date:
start date: 12:00:00 UTC Sep 1 1998
end date: 12:00:00 UTC Jan 28 2028
Subject Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: 3E455215 095192E1 B75D379F B187298A
Fingerprint SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C
X509v3 extensions:
X509v3 Key Usage: 6000000
Key Cert Sign
CRL Signature
X509v3 Subject Key ID: 607B661A 450D97CA 89502F7D 04CD34A8 FFFCFD4B
X509v3 Basic Constraints:
CA: TRUE
Authority Info Access:
Cert install time: 03:03:01 UTC Mar 16 2023
Cert install time in nsec: 1678935781942944000
Associated Trustpoints: CA-GlobalSign-Root
```

#show crypto pki certificates verbose CA-GlobalSign-RootCA CertificateStatus: AvailableVersion: 3Certificate Serial Number (hex): 040000000001154B5AC394Certificate Usage: SignatureIssuer: cn=GlobalSign Root CAou=Root CAo=GlobalSign nv-sac=BESobject: cn=GlobalSign Root CAou=Root CAo=GlobalSign nv-sac=BEValidity Data: data di inizio: 12:00:00 UTC set 1 1998data di fine: 12:00:00 UTC gen 28 2028Informazioni sulla chiave del soggetto:Algoritmo a chiave pubblica: rsaEncryptionRSA Chiave pubblica: (2048 bit)Algoritmo di firma: SHA1 con crittografia RSAFingerprint MD5: 3E455215 095192E1 B75D377 B187298A Impronta digitale SHA1:

B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C X509v3 estensioni:X509v3 Utilizzo chiave: 6000000Key Cert SignCRL SignatureX509v3 ID chiave oggetto: 607B6 61A 450D97CA 89502F7D 04CD34A8 FFFCFD4B X509v3 Vincoli di base:CA: TRUEA Informazioni sull'autorità Accesso:Ora installazione certificato: 03:03:01 UTC Mar 16 2023 Ora installazione certificato in nsec: 1678935781942944000CA Trustpoints associati: GlobalSign-Root

CA-gmail-SMTP:

Il certificato TLS per i server Gmail (CA-gmail-SMTP) è stato trovato seguendo la procedura descritta di seguito: Utilizzare i certificati TLS per un trasporto sicuro

Configurazione:

Spoiler (Evidenziato da leggere)

```
(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)# autenticazione crypto-pki CA-gmail-SMTPEntere il certificato CA codificato in base 64.Terminare con una riga vuota o la parola "quit" su una riga da solaMIIEhjCCA26gAwIBAgIQUofgQKT+9wcSaLBP3d3w9DANBgkqhkiG9w0BAQsFADBGMQswCQYDVQ
EChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM<snip>b1J2gZAyjyd4nfFRG1jeL5KrsfUR9hIXufqySvlPUoP
'CA-gmail-SMTP' è Il certificato CA subordinato non è un certificato CA.Verifica manuale richiestaIl certificato ha i seguenti attributi:Impronta digitale MD5: 19651FBE 906A414D 6D57B783 946F30A2 Impronta digitale SHA1: 4EF392CB EEB46D5E 4743953 AAEF313F 4C6D2825% Accettare il certificato? [sì/no]: sìCertificato CA Trustpoint accettato.% Certificato importato correttamente(config)#

Verifica configurazione in esecuzione:

Spoiler (Evidenziato da leggere)

```
# 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 catena di certificati crypto pki CA-gmail-SMTP catena di certificati crypto pki CA-gmail-SMTP ca 5287E040A4FEF7071268B04FDDDF0F4 30820486 3082036E A0030201 02021052 87E040A4 FEF70 12 68B04FDD DDF0F430 0D06092A 864886F7 0D01010B 05003046 310B3009 06035504 06130255 5 53312230 <snip> 92ABB1F5 1F61217 B9FAB24A F94F5283 EE2928B7 7EFB084B 6D416045 C47BCB99 801C4969 E4D48E77 2FA3 quit

Mostra verifica della crittografia:

Spoiler (Evidenziato da leggere)

```
# 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: AvailableVersione: 3Certificate Serial Number (hex): 5287E040A4FEF7071268B04FDDDF0F4Certificate Utilizzo: SignatureIssuer: cn=GTS CA 1C3o=Google Trust Services LLCc=USSObject: cn=smtp.gmail.comCRL Distribution Points: http://crls.pki.goog/gts1c3/moVDfISia2k.crlValidity Data: data di inizio: 09:35:00 UTC 20 feb 2023data di fine: 09:15:02 UTC 15 maggio 2023Informazioni sulla chiave del soggetto:Algoritmo a chiave pubblica: ecEncryptionEC Chiave pubblica: (256 bit)Algoritmo della firma: SHA256 con crittografia RSAFingerprint MD5: 19651FBE 906A414D 6D57B783 946F30A2 Fingprint SHA1: 4EF392CB EEB46D5E 47433953 AAEF313F 4C6D2825 X509v3 estensioni:X509v3 Utilizzo chiave: 8000000Digital SignatureX509v3 ID chiave oggetto: 5CC36972 D07FE97510E1A60 8A8ECC23 E40CFB68 X509v3 Limitazioni di base:CA: FALSEX509v3 Nome alternativo soggetto:smtp.gmail.com Indirizzo IP: Altri nomi: X509v3 ID chiave autorità: 8A747FAF 85CDEE95 CD3D9CD0 E24614F3 71351D27 Informazioni autorità: http://ocsp.pki.goog/gts1c3CA ISSUERS: http://pki.goog/repo/certs/gts1c3.derX509v3 CertificatePolicies:Policy: 2.27 1.140.1.2.1Utilizzo chiave esteso:Auth serverOra di installazione del certificato: 03:10:41 UTC Mar 16 2023 Ora di installazione del certificato in nsec: 1678936241822955008Trust point associati: CA-gmail-SMTP

Un modo più semplice per trovare i certificati

In alternativa, è possibile provare a utilizzare una chiamata openssl da un server/laptop per ottenere più facilmente i certificati da un server SMTP senza dover utilizzare i debug e cercare in Google per rintracciarli:

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

Potresti anche use smtp.gmail.com:

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

Gli output di tale chiamata includeranno i certificati effettivi che possono essere utilizzati per le configurazioni "crypto pki authentication <trustpoint>".

Nuovo test di EEM con SMTP protetto

Dopo aver applicato i certificati al dispositivo Cisco IOS XE, lo script EEM invierà i messaggi

SMTP sicuri come previsto.

```
# event manager run SendSecureEmailEEM
```

Controllare lo spoiler per gli output completi di crittografia e debug SSL:

Spoiler (Evidenziato da leggere)

```
# 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 SendSecureEmailEM*Mar 16 03:28:50.673: CRYPTO_OPSSL: Allocata la memoria per OPSSLContext*Mar 16 03:28:50.673: CRYPTO_OPSSL: imposta le specifiche del cifrario sulla maschera 0x02FC000 per la versione 128*Mar 16 03:28:50.674: imposta l'elenco di

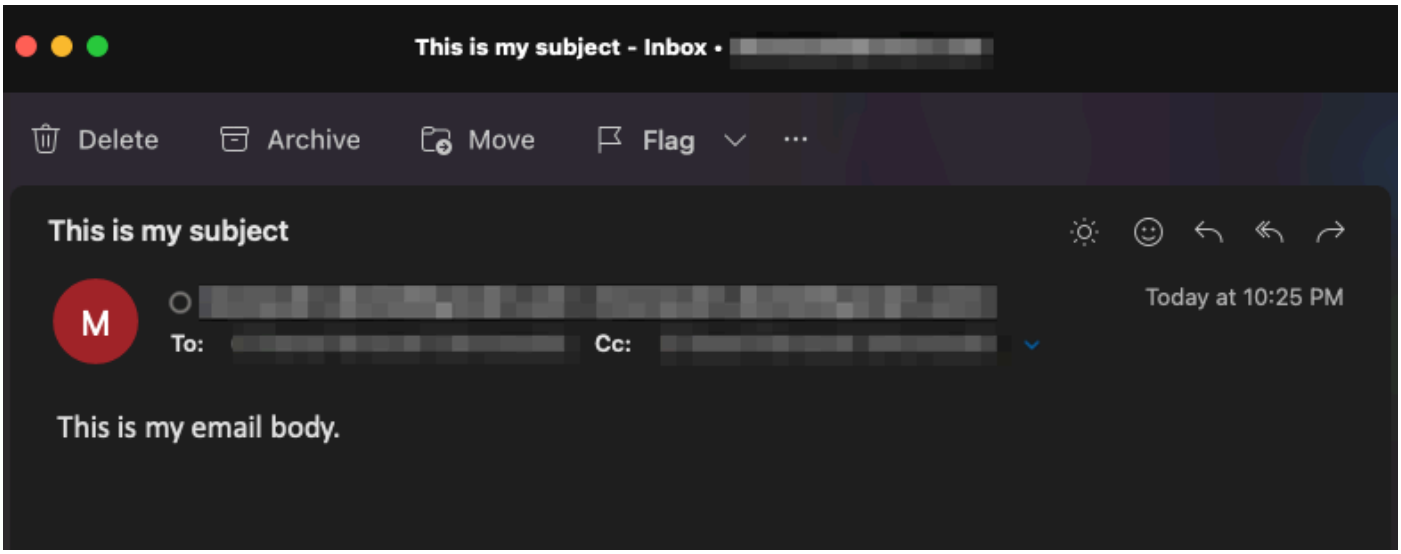
curve EC predefinite: 0x77 Impostare l'elenco di curve EC: secp521r1:secp384r1:prime256v1*Mar 16 03:28:50.674: voce opssl_SetPKIInfo*Mar 16 03:28:50.674: CRYPTO_PKI: (A069B) sessione avviata - identità selezionata (TP-self-signed-486541296)xTP-self -486541296:refcount dopo incremento = 1*Mar 16 03:28:50.674: CRYPTO_PKI: inizio recupero catena di certificati locale.*Mar 16 03:28:50.674: CRYPTO_PKI(Cert Lookup) issuer="cn=IOS-Self-Signed-Certificate-486541296" serial number= 01*Mar 1603 28:50.674: CRYPTO_PKI: ricerca del certificato nel 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: operazione completata con recupero catena di certificati locale 0.*Mar 16 03:28:50.675: TO_PKI: ricevuta richiesta di terminare la sessione PKI A069B.*Mar 16 03:28:50.675: CRYPTO_PKI: sessione PKI A069B terminata. Liberazione di tutte le risorse.TP-self-signed-486541296:unlocked trustpoint TP-self-signed-486541296, refcount è 0*Mar 16 03:28:50.675: opssl_SetPKIInfo fatto.*Mar 16 03:28:50.675: CRYPTO_OPSSL: Common Criteria è disabilitato in questa sessione.Disabilitazione della funzionalità della modalità Common Criteria in CiscoSSL SSL CTX 0x7F41F28EAFF8*Mar 16 03:28:50.675: CRYPTO_OPSSL: cifrsuiti ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES25 6-GCM-SHA384:DHE-RSA-AES256-SHA256:AES256-GCM-SHA384:AES256-SHA256: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:AES128-SHA256*Mar 16 03:28:50,676: inizio dell'handshake: prima dell'inizializzazione SSL*16 03:28:50,66 6: SSL_connect:prima dell'inizializzazione SSL*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: >> Handshake TLS 1.2 [length 0095], ClientHello*Mar 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 write client hello*Mar 16 03:28 0.692: <<< ??? [lunghezza 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 [lunghezza F0002], 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: estensione server TLS "sconosciuta" (id=23), ll=0TLS estensione server "renegotiate" (id=65281), len=1*Mar 16 03:28:50.693: 00*Mar 16 03:28:50.693: estensione server TLS "EC point formats" (id=11), len=2*Mar 16 03:28:50.693: 01 00*16 03:28:50.69 3: estensione server TLS "session ticket" (id=35), len=0*Mar 16 03:28:50.693: << ??? [lunghezza 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: <<< Certificato di handshake TLS 1.2 [lunghezza 0F9A], *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 03:28:5 0.763: 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 A2 96 B6 C2 82 3F*Mar 16 03:28:50.763: *16 03:28:50.765: CC_DEBUG: accesso alla funzione di richiamata dello strato shim Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) sessione avviata - identità non specificata*Mar 16:03:50.765: CRYPTO_PKI: (A069C) aggiunta certificato peer*Mar 16:03:28:50.767: CRYPTO_PKI: aggiunto certificato peer x509 - (1162) byte*3 Mar 160 16:28:50.767: CRYPTO_PKI: (A069C) Aggiunta di un certificato peer*Mar 16 03:28:50.768: CRYPTO_PKI: Aggiunta di un certificato peer x509 - (1434) byte*Mar 16 03:28:50.768: CRYPTO_PKI: (A069C) Aggiunta di un certificato peer*Mar 16 03:28:50 770: CRYPTO_PKI: aggiunto certificato peer x509 - (1382) byte*Mar 16 03:28:50.770: CRYPTO_OPSSL: convalida richiamata catena certificati*Mar

16 03:28:50.770: CRYPTO_PKI(Cert Lookup) issuer="cn=GTS CA 1C3,o=Google Trust Services LLC,c=US" serial number= 52 87 E0 40 A4 F7 07 12 68 B0 4F DD F0 F4*Mar 16 03:28:50.770: CRYPTO_PKI: ricerca del certificato nella maniglia=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 TS 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: cerca certificato in handle=7F41EE523CE0, digest=03 9F CF 59 82 EE 09 CC 4F 53 AE D8 02 7E 4B AF*16 3:28:50.771: 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*Mar 16 03:28:50.771: CRYPTO_PKI: ricerca del certificato nell'handle=7F41EE522 0, 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: record del certificato non trovato per il numero di serie dell'emittente.*Mar 16 03:28:50.772: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()*16 03:28:50.7 2: CRYPTO_PKI: Rilevata corrispondenza oggetto*Mar 16 03:#28:50.772: CRYPTO_PKI: ip-ext-val: Convalida estensione IP non richiesta:Incrementare il conteggio per il contesto da id-35 a 1*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: PTO_PKI: (A069C)il percorso di convalida ha 1 certificato*Mar 16 03:28:50.773: CRYPTO_PKI: (A069C) Verifica certificati identici*Mar 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= 7BD 0D 6C DB 3 6 F9 1A EA 21 0F C4 F0 58 D3 0D*Mar 16 03:28:50.774: CRYPTO_PKI: ricerca del certificato nella maniglia=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: Record del certificato non trovato per il numero di serie dell'emittente.*Mar 16 03:28:50.774: CRYPTO_PKI : (A069C) Convalida del certificato non attendibile*Mar 16 03:28:50.774: CRYPTO_PKI: (A069C) Creazione di un elenco di trust appropriati*Mar 16 03:28:50.774: CRYPTO_PKI: crypto_pki_get_cert_record_by_issuer() 16:03:28:50.774: CRYPTO_PKI: trovato un'autorità emittente corrispondente*Mar 16:03:28:50.774: CRYPTO_PKI: (A069C) I trust appropriati sono: CA-GlobalSign-Root,*Mar 16:03:28:50.775: CRYPTO_PKI: (A069C) Tentativo di convalida del certificato utilizzando la policy CA-GlobalSign-Root*1 6 03:28:50.775: CRYPTO_PKI: (A069C) Utilizzo di CA-GlobalSign-Root per convalidare il certificato*Mar 16 03:28:50.775: CRYPTO_PKI (rendere attendibile la catena di certificati)*Mar 16 03:28:50.775: CRYPTO_PKI: aggiunto 1 certificato a una catena attendibile.*Mar 16 03:28:50.775: CRYPKI_PKI: Preparazione provider servizio di revoca sessione*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 0E6 99 CE 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 03:28:5 0.780: CRYPTO_PKI: eliminazione della chiave memorizzata nella cache con ID chiave 45*Mar 16 03:28:50.781: CRYPTO_PKI: tentativo di inserimento della chiave pubblica del peer nella 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: 1 1118*Mar 16 03:28:50.781: P11:C_GetMechanismInfo slot 1 tipo 3 (meccanismo non valido)*Mar 16 03:28:50.781: P11:C_GetMechanismInfo slot 1 tipo 1*Mar 16 03:28:50.781: P11:C_VerifyRecoverInit - 131118*Mar 16 3:28:50.781: P11:C_VerifyRecover - 131118*Mar 16 03:28:50.781: P11:pubkey trovata nella cache utilizzando l'indice = 46*Mar 16 03:28:50.781: P11:public key trovata : 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 D 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_Destroy 2:2002E*Mar 16

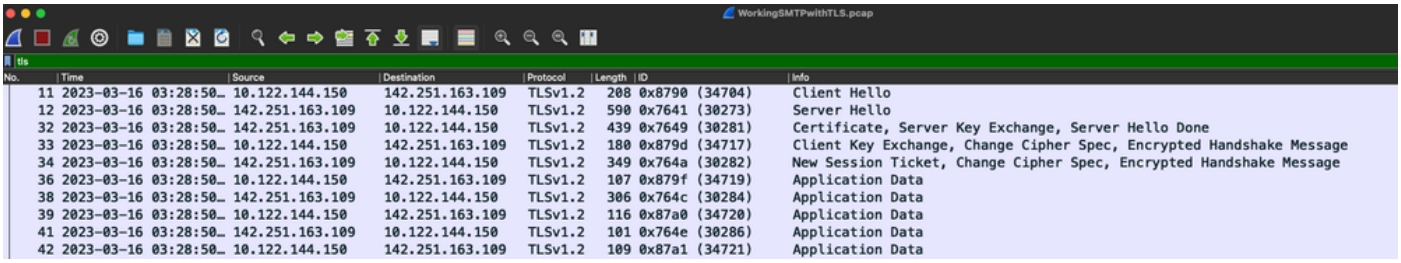
03:28:50.788: CRYPTO_PKI: chiave memorizzata nella cache del peer in scadenza con ID chiave 46*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C) Il certificato è verificato*Mar 16 03:28:50.788: CRYPTO_PKI: rimuove i provider del servizio di revoca della sessione*Mar 16 03:28:58 0.788: CRYPTO_PKI: rimuove i provider del servizio di revoca della sessioneCA-GlobalSign-Root:stato di convalida - CRYPTO_VALID_CERT_WITH_WARNING*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C) Certificato convalidato senza controllo di revoca:riconteggio certificato dopo incremento = 1*Mar 16 03:28:50.790: CRYPTO_PKI: popola dati di autenticazione AAA*Mar 162 03 8:50.790: CRYPTO_PKI: impossibile ottenere l'attributo configurato per l'autorizzazione dell'elenco AAA primario.*Mar 16 03:28:50.790: PKI: utilizzo chiave certificato: firma digitale, firma certificato, firma CRL*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C)il certificato concatenato è stato ancorato al trust CA-GlobalSign-Root e il risultato della convalida della catena è: CRYPTO_VALID_CERT T_WITH_WARNING*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Rimozione del contesto di verifica*Mar 16 03:28:50.790: CRYPTO_PKI: distruzione di ca_req_context tipo PKI_VERIFY_CHAIN_CONTEXT,ident 35, conteggio riferimenti 1:Decrementing refcount for context id-35 to 0*Mar 16 03:28:50.790: TO_PKI: ca_req_context rilasciato*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Convalida TP è CA-GlobalSign-Root*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Convalida del certificato riuscita*Mar 16 03:28:50.790: CRYPTO_OPSSL: verifica del certificato riuscita*Mar 16 03 28:50.790: CRYPTO_PKI: ricevuta richiesta di terminare la sessione PKI A069C.*Mar 16 03:28:50.790: CRYPTO_PKI: sessione PKI A069C terminata. Liberazione di tutte le risorse.:cert refcount dopo decremento = 0*Mar 16 03:28:50.791: <<< ??? [lunghezza 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 [lunghezza 0091 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 C0 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 9B2 95 91 E0 CC D6 8E CE*Mar 16 03:28:50.792: 8D 36 C9 83 42 B0 4D AC 0C 04 03 00 46 30 44 2*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 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: *3 Mar 16 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 10 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>*Mar 16 03:28:50.796: P11:C_FindObjectsFinal*Mar 16 03:28:50.796: P11:C_VerifyInit - Sessione trovata Mar 16 03:28:50,796: P11:C_VerifyInit - ID chiave = 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: <<< Handshake TLS 1.2 [length 000 4], 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: >> ??? [lunghezza 0005]*Mar 16 03:28:50.810: 16 03 03 00 46*Mar 16 03:28:50.811: *Mar 16 03:28:50.811: >> Handshake TLS 1.2 [lunghezza 0046], ClientKeyExchange*Mar 16 03:28:50.811: 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 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 B*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:SSL /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: >> ?? [lunghezza 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: >> ?? [lunghezza 0005]*Mar 16 03:28:51,714: 17 03 03 00 1E*Mar 16 03:28:51,714: *Mar 16 03:28:51,732: << ??? [lunghezza 0005]*Mar 16 03:28:51,732: 17 03 03 00 71*Mar 16 03:28:51,732:

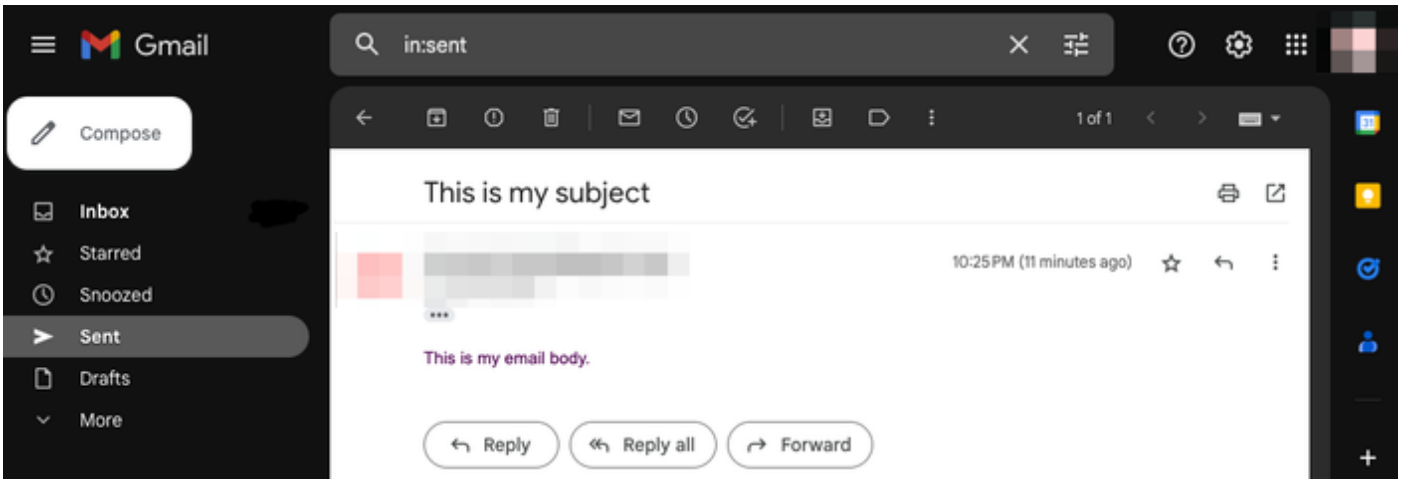
È possibile verificare che l'e-mail sia stata ricevuta e che tutti i campi (a, da, cc, oggetto, corpo) siano compilati correttamente:



È inoltre possibile verificare che l'handshake TLS e la sessione siano stati eseguiti dall'acquisizione del pacchetto sul dispositivo Cisco IOS XE (collegato come "WorkingSMTPwithTLS.pcap"):



È anche possibile verificare che i messaggi e-mail siano visualizzati nella cartella "Inviati" dell'account e-mail utilizzato:



Altre avvertenze e considerazioni

Nomi utente con simboli @

È possibile rilevare problemi quando si tenta di utilizzare un inoltro SMTP. A causa dell'inoltro SMTP, la stringa del server ha questo formato (un "@" nel nome utente):

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

Il codice per l'analisi del nome utente e della password divide la stringa sulla prima occorrenza del simbolo "@". Di conseguenza, il sistema ritiene che il nome host del server inizi immediatamente dopo il primo simbolo "@" attraverso il resto della stringa e interpreta tutti gli elementi precedenti come "nome utente:password".

L'implementazione TCL di SMTP utilizza un'espressione regolare (regex) che gestisce le informazioni relative a nome utente/password/server in modo diverso. A causa di questa differenza, TCL consente ai nomi utente di usare il simbolo "@"; tuttavia, Cisco IOS XE TCL non supporta la crittografia, quindi non vi è alcuna opzione per inviare e-mail sicure tramite TLS.

Per riepilogare:

- Se l'e-mail deve essere sicura, non puoi inviarla con TCL.
- Se il nome utente contiene una "@", non è possibile inviarla con un modulo EEM.

Per risolvere questo problema, consultare l'ID bug Cisco CSCwe75439 per migliorare la funzionalità e-mail di EEM. Non è tuttavia disponibile una roadmap per questa richiesta di miglioramento.

Conclusioni

Come mostrato di seguito, è possibile inviare e-mail sicure tramite SMTP con TLS utilizzando l'applet Embedded Event Manager (EEM). Richiede alcune impostazioni sul lato server, nonché la

configurazione dei certificati necessari per consentire l'attendibilità, ma è fattibile se si desidera generare notifiche e-mail automatizzate e sicure.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).