

Erstellen eines CSR für Drittanbieterzertifikate und Installation auf CMX

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfen](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Zertifikatsanforderung (Certificate Signing Request, CSR) für den Erhalt eines Zertifikats eines Drittanbieters generieren und ein verkettetes Zertifikat auf Cisco Connected Mobile Experiences (CMX) herunterladen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse von Linux
- Public Key Infrastructure (PKI)
- Digitale Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf CMX-Version 10.3.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

CSR erstellen

Schritt 1: Stellen Sie eine Verbindung zur CLI von CMX her, greifen Sie als Root zu, wechseln Sie in das Zertifikatsverzeichnis, und erstellen Sie einen Ordner für den CSR und die Schlüsseldatei.

```
[cmxadmin@cmx]$ su -
Password:
[root@cmx]# cd /opt/haproxy/ssl/
[root@cmx]# mkdir newcert
[root@cmx]# cd newcert
```

Hinweis: Das Standardverzeichnis für Zertifikate in CMX lautet /opt/haproxy/ssl/.

Schritt 2: Erstellen Sie die CSR- und Schlüsseldatei.

```
[root@cmx newcert]# openssl req -nodes -days 365 -newkey rsa:2048 -keyout
/opt/haproxy/ssl/newcert/private.key -out /opt/haproxy/ssl/newcert/cert.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/opt/haproxy/ssl/newcert/private.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:MX
State or Province Name (full name) []:Tlaxcala
Locality Name (eg, city) [Default City]:Tlaxcala
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (eg, your name or your server's hostname) []:cmx.example.com
Email Address []:cmx@example.com
```

Schritt 3: Lassen Sie den CSR von einem Drittanbieter unterzeichnen.

Um das Zertifikat von CMX abzurufen und an Dritte zu senden, führen Sie den Befehl **cat** aus, um den CSR zu öffnen. Sie können die Ausgabe in eine TXT-Datei kopieren und einfügen oder die Erweiterung entsprechend den Anforderungen des Drittanbieters ändern. Hier ein Beispiel.

```
[root@cmx newcert]# cat cert.crt
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwYsxCzAJBgNVBAYTAk1YMRUwDwYDVQQIDAhUbgGF4Y2FsYTER
MA8GA1UEBwwIVGxheGNhbGExDjAMBgNVBAoMBUNpc2NmMQwwCgYDVQQQLDANUQUx
GDAWBgNVBAMMD2NteC5leGFtcGxlLmNvbTEeMBwGCsGSIb3DQEJARYPY214QGV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA2YybDkDR
vRSwD19EvaJehsNjG9Cyo3vQPOPcAAAdjFBpUHMt8QNgn6YFdHYZdpKaRTJXhztm
fa/7Nevb1IP/pSBgYRxHXQEh19Gj4DT0gT2T+AZ8j3J9KMSe8Bakj4qY8Ua7GCdC
A62NzVcDxDM83gUD92oGbxOF9VFE2hiRvCQc+d6gBRuTOXxtyLBAtcL3hkiOEQx7
sDA55CwZU7ysMdWHUBn4AglzI1gPyzlmT3dwr0gfOSYN4j5+H0nrYtrPBZSUbZaa
8pGXVu7sFtV8bahgtnYiCUTiz9J+k5V9DBjqPszYzb3+KxAAA+g0iV3J1VzsLnt7
mVocT9oPaOEI8wIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAI6Q/A4zTfrWP2uS
xtN8X6p6aP8guU0bTWhGEMBEgBQd0bBWYdhxaItGt1a1tdNcIGLACeMPuk7WpsiH
rUs5kiIj1Ac2/ANBao6/nlv56vhGUx0d0q0fk/g1brKL+a8Lx9ixtee77aPZ1xVD
A/n3FdNdSiidWH0M4q8JunxbT33vM9h8H6oqe/JI3BDnw4tRnkYaGWJsyWU1PCuO
TWPMagMkntv0JaEOHLg4/JZyVsDdiTnmb/U8cEH2RrcUP8iwjykDpb/V4tb4VtgM
7+9HKxQRQhQ5Qji8/QyMG6ctoD+B7k6UpzXvi5FpvgQGWwXJNC52suAt0QeeZj1J
rpudLUs=
-----END CERTIFICATE REQUEST-----
[root@cmx newcert]#
```

Schritt 4: Erstellen Sie die Zertifikatskette für den Import in CMX.

Um das endgültige Zertifikat zu erstellen, kopieren Sie das signierte Zertifikat und fügen es in eine TXT-Datei ein. Dazu gehören der private Schlüssel, das Zwischenzertifikat und das Stammzertifikat. Stellen Sie sicher, dass Sie die Datei als **.pem**-Datei speichern.

Dieses Beispiel zeigt das Format des endgültigen Zertifikats.

```
-----BEGIN RSA PRIVATE KEY----- < Your Private Key
MIIEpAIBAAKCAQEAA2gXgEo7ouyBfWwCkctcYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- < Your CMX server signed certificate
MIIFEzCCAavugAwIBAgIBFzANBgkqhkiG9w0BAQsFADCB1DELMAkGA1UEBhMCMVVMx
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < Your intermediate CA certificates
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < The root CA certificate that signed your certificate
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
...
-----END CERTIFICATE-----
```

Schritt 5: Übertragen Sie das endgültige Zertifikat in CMX.

Um das endgültige Zertifikat von Ihrem Computer in CMX zu übertragen, öffnen Sie die SFTP-Anwendung, und stellen Sie mit den Administratoranmeldeinformationen eine Verbindung zu CMX her. Sie müssen in der Lage sein, die Ordner von CMX anzuzeigen, wie im Bild gezeigt.

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Group
..		Directory	03/01/18 18:...	drwxr-xr-x	cmxadmin...
..		Directory	10/23/17 08:...	drwx-----	cmxadmin...
.cassandra		Directory	04/25/18 10:...	-rw-----	cmxadmin...
.ssh	14465	File	10/16/14 08:...	-rw-r--r--	cmxadmin...
.bash_history	18	File	10/16/14 08:...	-rw-r--r--	cmxadmin...
.bash_logout	176	File	10/16/14 08:...	-rw-r--r--	cmxadmin...
.bash_profile	777	File	03/27/18 11:0...	-rw-r--r--	cmxadmin...
.bashrc		File			

Ziehen Sie das verkettete Zertifikat anschließend in den Ordner `/home/cmxadmin/`, und legen Sie es ab.

Hinweis: Das Standardverzeichnis beim Öffnen einer SFTP-Verbindung mit CMX ist `/home/cmxadmin/`.

Schritt 6: Ändern Sie die Berechtigung des endgültigen Zertifikats und des Besitzers. Verschieben Sie es dann in den Ordner, der den privaten Schlüssel enthält. Hier ein Beispiel.

```
[root@cmx ~]# cd /home/cmxadmin/
[root@cmx cmxadmin]# chmod 775 final.pem
```

```
[root@cmx cmxadmin]# chown cmx:cmx final.pem
[root@cmx cmxadmin]# mv final.pem /opt/haproxy/ssl/newcert/
[root@cmx cmxadmin]# cd /opt/haproxy/ssl/newcert/
[root@cmx newcert]# ls -la
total 16
drwxr-xr-x 2 root root 4096 Apr 25 12:30 .
drwxr-xr-x 4 cmx cmx 4096 Apr 25 09:25 ..
-rw-r--r-- 1 root root 1054 Apr 25 11:01 cert.crt
-rwxrwxr-x 1 cmx cmx 0 Apr 25 12:29 final.pem
-rw-r--r-- 1 root root 1708 Apr 25 11:01 private.key
[root@cmx newcert]#
```

Schritt 7: Stellen Sie sicher, dass alle Komponenten richtig gebaut sind.

```
[root@cmx newcert]#openssl verify -CAfile /opt/haproxy/ssl/newcert/final.pem
/opt/haproxy/ssl/newcert/final.pem
/opt/haproxy/ssl/newcert/final.pem: OK
```

Sie müssen eine OK-Meldung erhalten.

Schritt 8: Installieren Sie das letzte Zertifikat, und starten Sie CMX neu.

```
[root@cmx newcert]#cmxctl node sslmode enable --pem /opt/haproxy/ssl/newcert/final.pem
enabling ssl
ssl enabled
```

```
[root@cmx newcert]#reboot
```

Schritt 9 (optional). Wenn Sie CMX 10.3.1 oder höher ausführen, kann dieser Fehler folgende Auswirkungen haben:

- [CSCvh21464](#) : Die CMX-WEBUI verwendet das installierte selbstsignierte Zertifikat oder das Zertifikat eines Drittanbieters nicht.

Dieser Fehler verhindert, dass CMX den Zertifikatspfad aktualisiert. Die Problemumgehung zur Lösung dieses Problems besteht darin, zwei Soft-Links zu erstellen, um auf das neue Zertifikat und den neuen privaten Schlüssel zu verweisen, und CMX erneut zu laden. Hier ein Beispiel:

```
[root@cmx ~]# cd /opt/haproxy/ssl/
[root@cmx ssl]# mkdir backup
[root@cmx ssl]# mv host.pem backup/
[root@cmx ssl]# mv host.key backup/
[root@cmx ssl]# ln -s /opt/haproxy/ssl/newcert/final.pem host.pem
[root@cmx ssl]# ln -s /opt/haproxy/ssl/newcert/private.key host.key
[root@cmx ssl]#
[root@cmx ssl]# ls -la
total 16
drwxr-xr-x 4 cmx cmx 4096 Apr 25 12:59 .
drwxr-xr-x 6 cmx cmx 4096 Mar 31 2017 ..
lrwxrwxrwx 1 root root 36 Mar 26 09:58 host.key -> /opt/haproxy/ssl/newcert/private.key
lrwxrwxrwx 1 root root 38 Mar 26 09:58 host.pem -> /opt/haproxy/ssl/newcert/final.pem
drwxr-xr-x 2 root root 4096 Apr 25 12:30 newcert
[root@cmx ssl]#
[root@cmx ssl]# reboot
```

Überprüfen

Öffnen Sie die grafische Benutzeroberfläche von CMX, in diesem Fall wird Google Chrome verwendet. Öffnen Sie das Zertifikat, indem Sie auf die Registerkarte **Sicher** neben der URL

klicken und die Details wie im Bild gezeigt überprüfen.

The screenshot shows a Cisco CMX interface with a blue header. On the right, a certificate details window is open for 'CA-KCG-lab' at 'cmx.example.com'. The window displays a 'Certificate Standard' icon and the following information:

- cmx.example.com**
- Issued by: CA-KCG-lab
- Expires: Tuesday, January 19, 2021 at 13:50:21 Central Standard Time
- ✓ This certificate is valid

The 'Details' section is expanded, showing the following fields:

- Issuer Name
- Country: MX
- State/Province: Nuevo Leon
- Locality: Guadalupe
- Organization: mex-wireless
- Organizational Unit: lab-mex-wireless
- Common Name: CA-KCG-lab

An 'OK' button is located at the bottom right of the window.

The screenshot shows the same Cisco CMX interface. The certificate details window for 'CA-KCG-lab' at 'cmx.example.com' is open, displaying the following information:

- Subject Name
- Country: MX
- State/Province: Tlaxcala
- Locality: Tlaxcala
- Organization: Cisco
- Organizational Unit: TAC
- Common Name: cmx.example.com
- Email Address: cmx@example.com
- Not Valid Before: Wednesday, April 25, 2018 at 14:50:21 Central Daylight Time
- Not Valid After: Tuesday, January 19, 2021 at 13:50:21 Central Standard Time

An 'OK' button is located at the bottom right of the window.