サードパーティ証明書用のCSRの生成とCMXへのインストール

内容

概要

このドキュメントでは、サードパーティの証明書を取得するために証明書署名要求(CSR)を生成する方法、およびチェーン証明書をCisco Connected Mobile Experiences(CMX)にダウンロードする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Linuxの基礎知識
- 公開キー インフラストラクチャ（PKI）
- デジタル証明書

使用するコンポーネント

このドキュメントの情報は、CMXバージョン10.3に基づくものです

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

CSRの生成

ステップ1:CMXのCLIに接続し、ルートとしてアクセスし、証明書ディレクトリに移動し、CSRとキーファイルのフォルダを作成します。

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

注：CMXの証明書のデフォルトディレクトリは/opt/haproxy/ssl/です。

ステップ2:CSRとキーファイルを生成します。

```
[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
```

ステップ3：サードパーティによって署名されたCSRを取得します。

CMXから証明書を取得してサードパーティに送信するには、**catコマンドを実行**してCSRを開きます。出力を.txtファイルにコピーアンドペーストするか、サードパーティの要件に基づいて拡張子を変更できます。次に例を示します。

```
[root@cmx newcert]# cat cert.crt
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwgYsxCzAJBgNVBAYTAk1YMREwDwYDVQQIDAhUbGF4Y2FsYTER
MA8GA1UEBwwIVGxheGNhbGExDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANUQUMx
GDAWBgNVBAMMD2NteC5leGFtcGxlLmNvbTEeMBwGCSqGSIb3DQEJARYPY214QGV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2YybDkDR
vRSwD19EVaJehsNjG9Cyo3vQPOPcAAdgjFBpUHMt8QNgn6YFdHYZdpKaRTJXhztm
fa/7Nevb1IP/pSBgYRxHXQEhl9Gj4DT0gT2T+AZ8j3J9KMSe8Bakj4qY8Ua7GCdC
A62NzVcDxDM83gUD92oGbxOF9VFE2hiRvCQc+d6gBRuTOXxtyLBAtcL3hkiOEQx7
sDA55CwZU7ysMdWHUBn4AglzI1gPyzlmT3dwR0gfOSYN4j5+H0nrYtrPBZSUbZaa
8pGXVu7sFtV8bahgtnYiCUtiz9J+k5V9DBjqpSzYzb3+KxeAA+g0iV3J1VzsLNt7
mVocT9oPaOEI8wIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAI6Q/A4zTfrWP2uS
xtN8X6p6aP8guU0bTWhGEMBEgBQd0bBWYdhxaItGt1a1tdNcIGLACeMPuk7WpsiH
rUs5kiIjlAc2/ANBao6/nlv56vhGUx0dOq0fk/glbrKL+a8Lx9ixtee77aPZ1xVD
A/n3FdNdSIidWH0M4q8JunxbT33vM9h8H6oqe/JI3BDnw4tRnkYaGWJsyWUlPCuO
TWPMagMkntv0JaEOHLg4/JZyVSdDiTnmb/U8cEH2RrcUP8iwjykDpb/V4tb4VtgM
7+9HKxQRQHq5Qji8/QyMG6ctoD+B7k6UpzXvi5FpvqGQWwXJNC52suAt0QeeZj1J
rpudLUs=
-----END CERTIFICATE REQUEST-----
[root@cmx newcert]#
```

ステップ4:CMXへのインポート用の証明書チェーンを作成します。

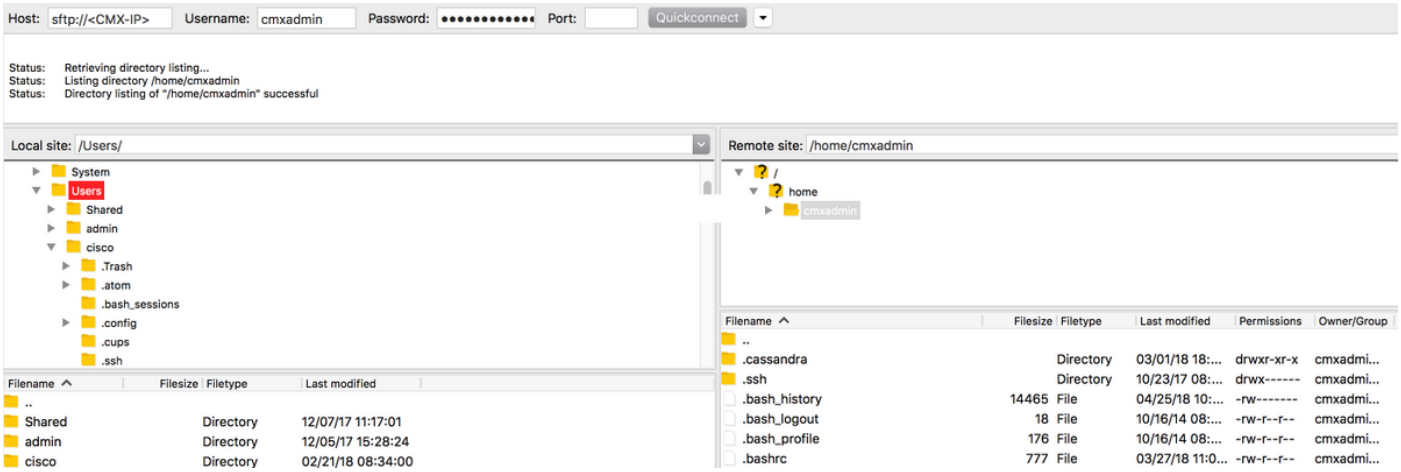
最終的な証明書を作成するには、秘密キー、中間証明書、およびルート証明書を含む.txtファイルに署名付き証明書をコピーアンドペーストします。必ず.pemファイルとして保存してください。

次の例は、最終的な証明書の形式を示しています。

```
-----BEGIN RSA PRIVATE KEY----- < Your Private Key
MIIEpAIBAAKCAQEA2gXgEo7ouyBfWwCktcYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- < Your CMX server signed certificate
MIIFEzCCAvugAwIBAgIBFzANBgkqhkiG9w0BAQsFADCBlDELMAkGA1UEBhMCVVMx
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < Your intermediate CA certificates
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < The root CA certificate that signed your certificate
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
...
-----END CERTIFICATE-----
```

ステップ5：最終証明書をCMXに転送します。

コンピュータからCMXに最終的な証明書を転送するには、SFTPアプリケーションを開き、管理者クレデンシャルを使用してCMXに接続します。図に示すように、CMXのフォルダを表示できる必要があります。



次に、チェーン証明書を/home/cmxadmin/フォルダにドラッグアンドドロップします。

注：CMXへのSFTP接続を開いた場合のデフォルトディレクトリは/home/cmxadmin/です。

ステップ6：最終証明書と所有者の権限を変更します。次に、秘密キーを含むフォルダに移動します。次に例を示します。

```
[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]#
```

ステップ7：すべてが正しく構築されていることを確認します。

```
[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
```

OKメッセージが表示されます。

ステップ8：最終的な証明書をインストールし、CMXをリブートします。

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

[root@cmx newcert]#reboot
```

ステップ 9 (オプション) ： CMX 10.3.1以降を実行している場合は、次のバグの影響を受ける可能性があります。

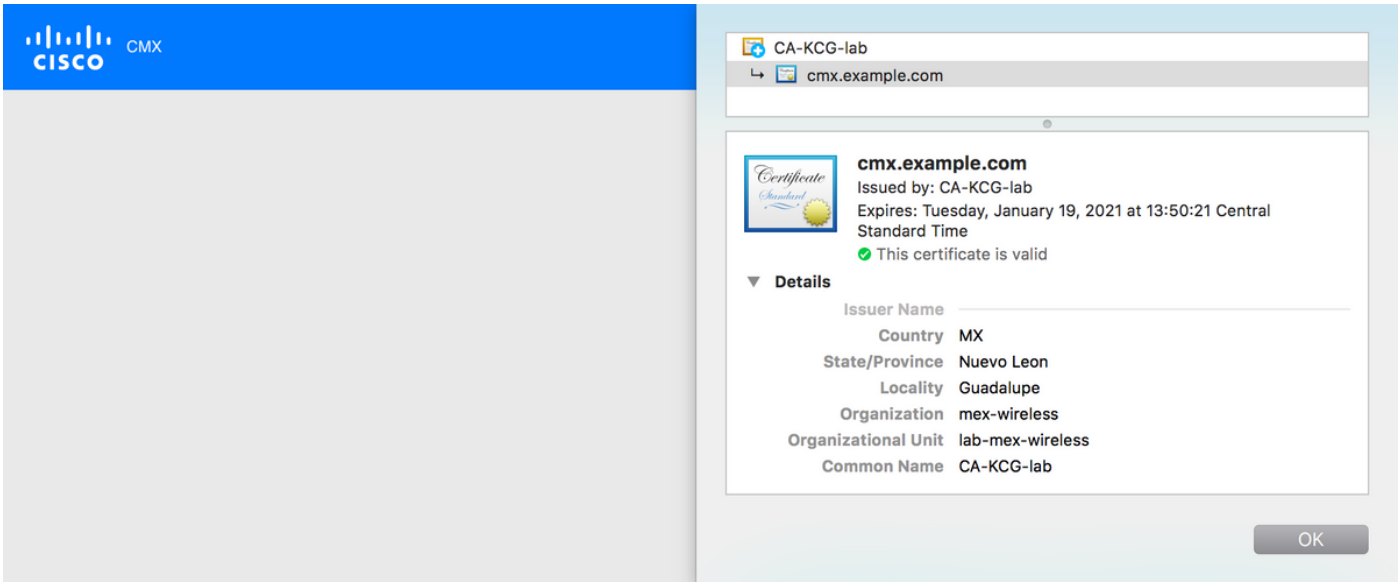
- CSCvh21464 :CMX WEBUIは、インストールされた自己署名またはサードパーティ証明書を使用しません

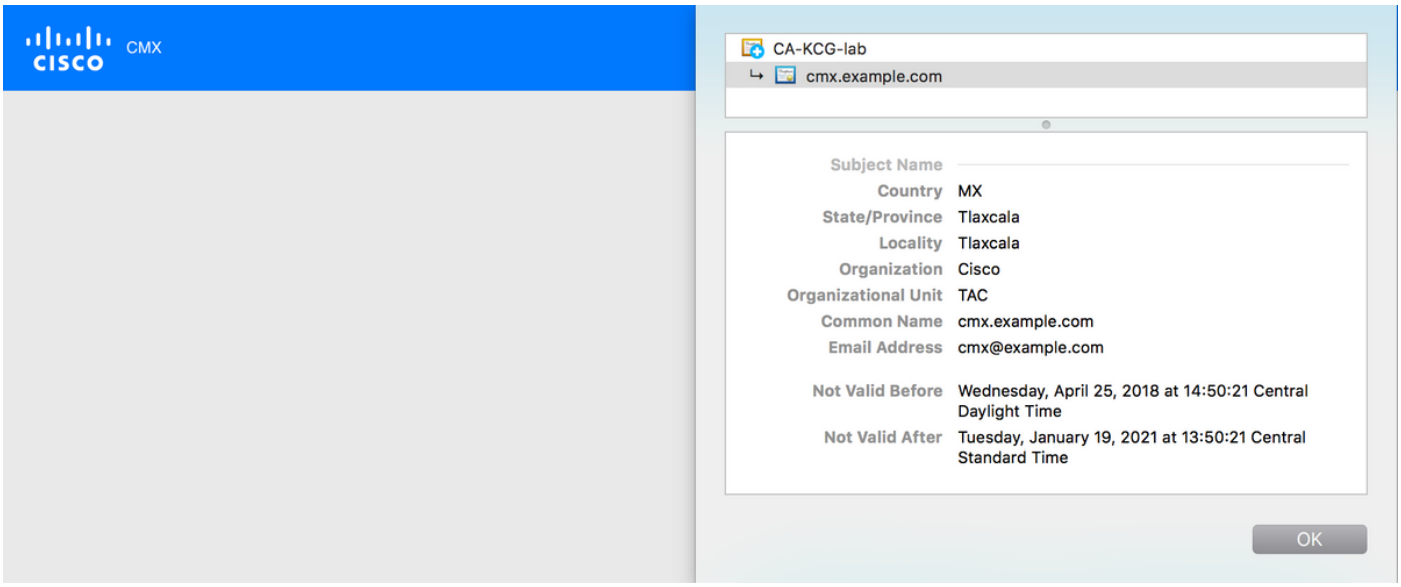
このバグにより、CMXは証明書パスを更新できません。この問題を解決する回避策は、新しい証明書と秘密キーをポイントする2つのソフトリンクを作成し、CMXをリロードすることです。以下が一例です。

```
[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
```

確認

CMXのGUIを開きます。この場合は、Google Chromeが使用されます。URLの横にある[Secure]タブをクリックして証明書を開き、図に示すように詳細を確認します。


CMX
CA-KCG-lab
cmx.example.com
cmx.example.com
Issued by: CA-KCG-lab
Expires: Tuesday, January 19, 2021 at 13:50:21 Central Standard Time
This certificate is valid
Details
Issuer Name
Country MX
State/Province Nuevo Leon
Locality Guadalupe
Organization mex-wireless
Organizational Unit lab-mex-wireless
Common Name CA-KCG-lab
OK


CMX
CA-KCG-lab
cmx.example.com
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
OK