驗證UC的CSR和證書不匹配

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[Cisco Communications Manager Certificate Management](#)
[問題](#)
[CUCM中CA簽名證書的一般實踐](#)
[解決方案1.在root（或linux）環境中使用OpenSSL命令](#)
[解決方案2.使用來自Internet的任何SSL證書金鑰匹配程式](#)
[解決方案3.比較來自Internet的任何CSR解碼器的內容](#)

簡介

本檔案介紹如何識別憑證授權單位(CA)簽署的憑證是否與思科整合應用伺服器的現有憑證簽署請求(CSR)相符。

必要條件

需求

思科建議您瞭解X.509/CSR。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

本文件也適用於以下硬體和軟體版本：

- 思科整合通訊管理員(CUCM)
- Cisco Unified IM and Presence
- Cisco Unified Unity Connection
- CUIS
- Cisco Mediasence
- Cisco Unified Contact Center Express(UCCX)

背景資訊

認證請求由可分辨名稱、公鑰和由請求認證的實體共同簽名的一組可選屬性組成。證書請求被傳送到將請求轉換為X.509公鑰證書的證書頒發機構。證書頒發機構以何種形式返回新簽名的證書不屬於本文檔的範圍。 PKCS #7訊息是一種可能性。(RFC:2986)。

Cisco Communications Manager Certificate Management

包含一組屬性的意圖有兩方面：

- 為了提供有關給定實體的其他資訊，或者提供質詢密碼，實體以後可以通過該密碼請求證書撤銷。
- 以提供包含在X.509憑證中的屬性。當前的統一通訊(UC)伺服器不支援質詢密碼。

當前的Cisco UC伺服器需要在CSR中具備以下屬性，如下表所示：

資訊	說明
orgunit	組織單位
組織名稱	組織名稱
地區	組織地點
狀態	組織狀態
國家/地區	無法更改國家/地區代碼
備用主機名	備用主機名

問題

當您支援UC時，可能會遇到許多在UC伺服器上無法上傳CA簽名證書的情況。由於您並非使用CSR建立簽署憑證的使用者，因此您無法一律識別建立簽署憑證時發生的情況。在大多數情況下，重新簽名新證書需要超過24小時。CUCM等UC伺服器沒有詳細的日誌/跟蹤，以幫助確定證書上傳失敗的原因，但它們只給出錯誤消息。本文的目的是縮小問題範圍，無論是UC伺服器還是CA問題。

CUCM中CA簽名證書的一般實踐

CUCM支援使用可在Cisco Unified Communications Operating System Certificate Manager GUI上訪問的PKCS#10 CSR機制與第三方CA整合。目前使用第三方CA的客戶必須使用CSR機制來為Cisco CallManager、CAPF、IPSec和Tomcat頒發證書。

步驟1。在產生CSR之前變更識別。

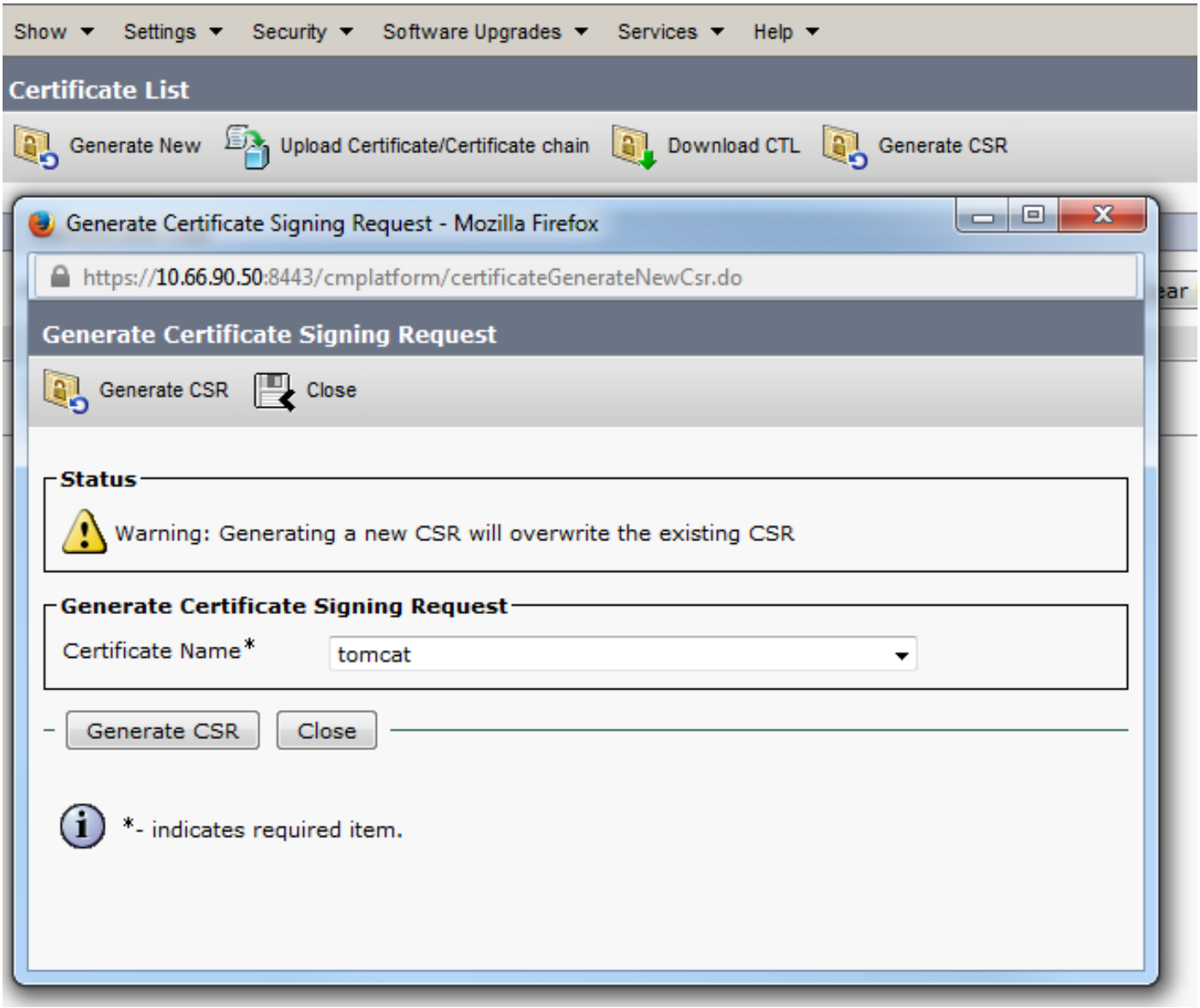
您可以使用**set web-security** 指令，修改CUCM伺服器的身分以產生CSR，如下圖所示。

```
admin:set web-security  ?
Syntax:
set web-security orgunit orgname locality state [country] [alternatehostname]
orgunit  mandatory   organizational unit
orgname  mandatory   organizational name
locality mandatory   location of organization
state    mandatory   state of organization
country  optional   country code can not be changed
alternatehostname  optional   alternate host name

admin:set web-security
```

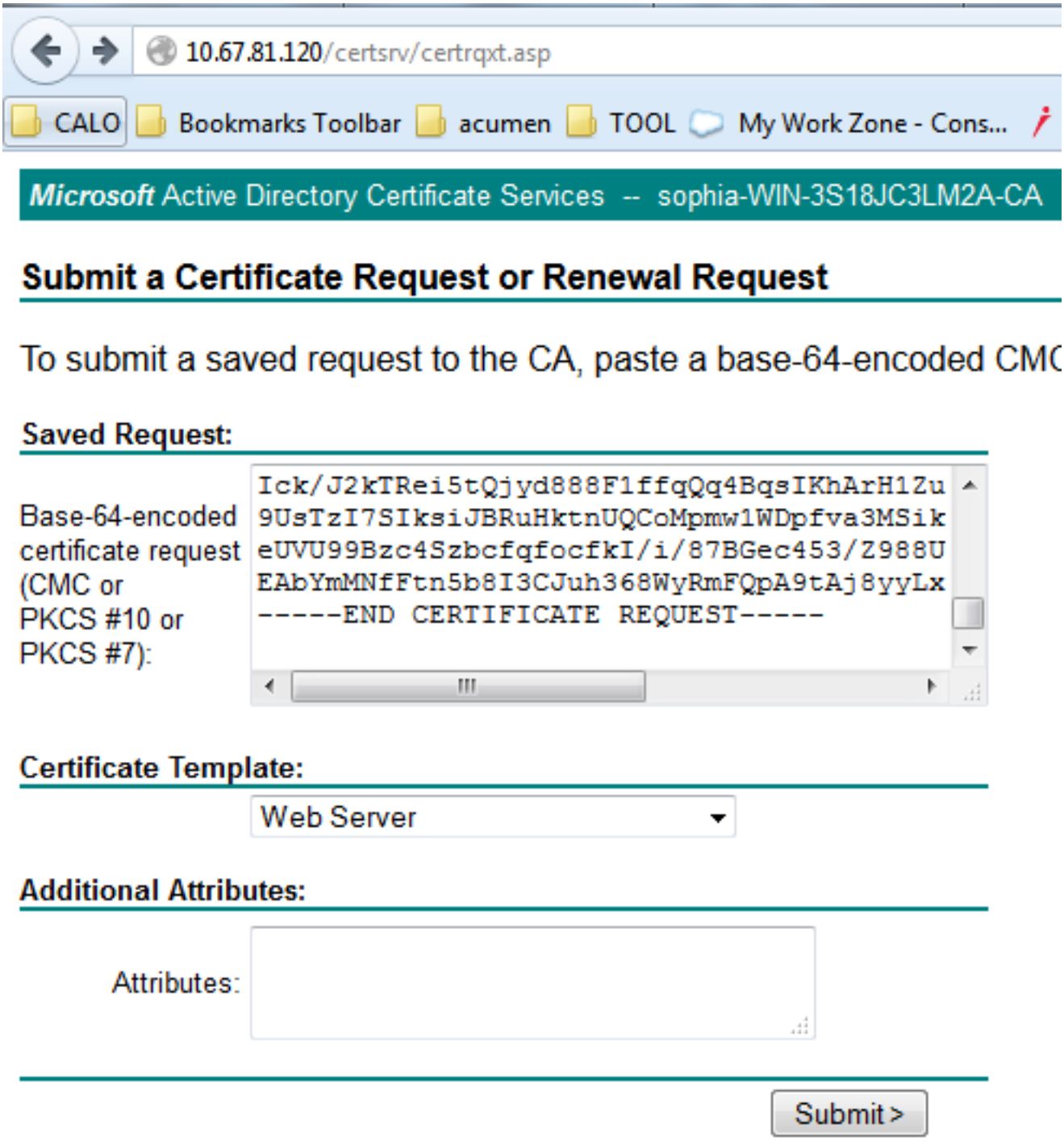
如果上述欄位中有空格，請使用""完成命令，如下圖所示。

```
admin:set web-security "Cisco Systems" "Cisco TAC" "St Leonard" NSW AU CUCM105.sophia.li

WARNING: Country code can not be changed.
Country code for existing web-security is : AU

WARNING: This operation creates self signed certificate for web access (tomcat) with the
r, certificates for other components (ipsec, callmanager, CAPF, etc.) still contain the o
erate these self-signed certificates to update them.

Regenerating web security certificates please wait ...

WARNING: This operation will overwrite any CA signed certificate previously imported for
Proceed with regeneration (yes|no)?
```

步驟2.產生CSR，如下圖所示。

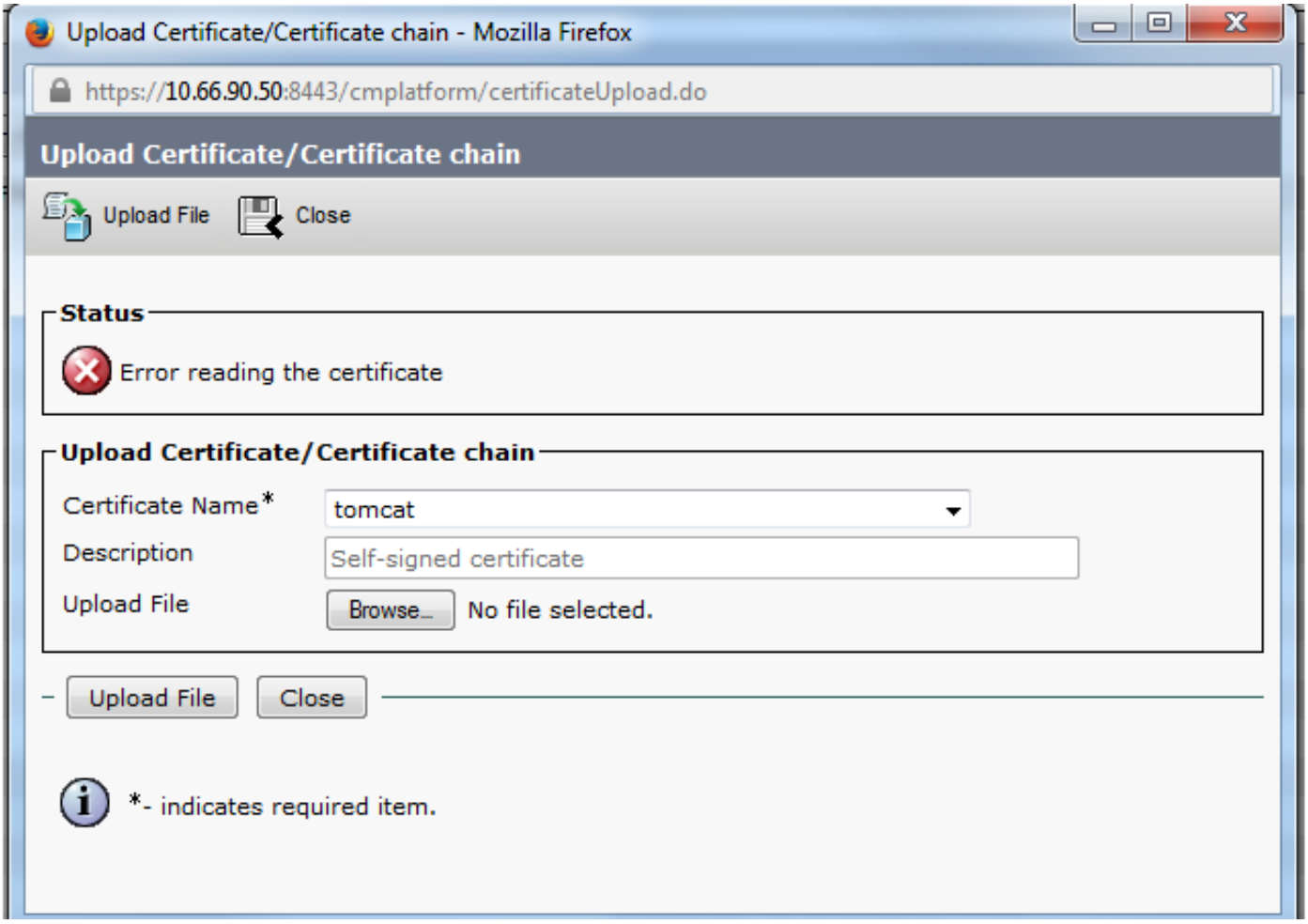


步驟3.下載CSR並由CA簽署，如下圖所示。



步驟4.將CA簽名的證書上傳到伺服器。

產生CSR並簽署憑證後，如果您無法上傳憑證，並顯示錯誤訊息「讀取憑證時出錯」（如本圖所示），則需要檢查是否已重新產生CSR，或是已簽署的憑證本身是否為問題的原因。



有三種方法可檢查CSR是否重新產生，或簽名的憑證本身是否為問題的原因。

解決方案1.在root（或linux）環境中使用OpenSSL命令

步驟1.登入根目錄，然後導覽至資料夾，如下圖所示。

```
[root@CCM105PUB keys]# pwd
/usr/local/platform/.security/tomcat/keys
[root@CCM105PUB keys]# ls -thl
total 28K
-rwxr-xr-x. 1 certbase ccmbase 1.7K Sep  1 23:22 tomcat_priv_csr.pem
-rwxr-xr-x. 1 certbase ccmbase 1.2K Sep  1 23:22 tomcat_priv_csr.der
-rwxr-xr-x. 1 certbase ccmbase 1.4K Sep  1 23:22 tomcat.csr
-rwxr-xr-x. 1 certbase ccmbase 1.2K Aug 13 16:11 tomcat_priv.der
-rwxr-xr-x. 1 certbase ccmbase 1.7K Aug 13 16:11 tomcat_priv.pem
-rwxr-xr-x. 1 certbase ccmbase   16 Apr 26 15:10 tomcat-trust.passphrase
-rwxr-xr-x. 1 certbase ccmbase   16 Apr 26 15:10 tomcat.passphrase
[root@CCM105PUB keys]#
```

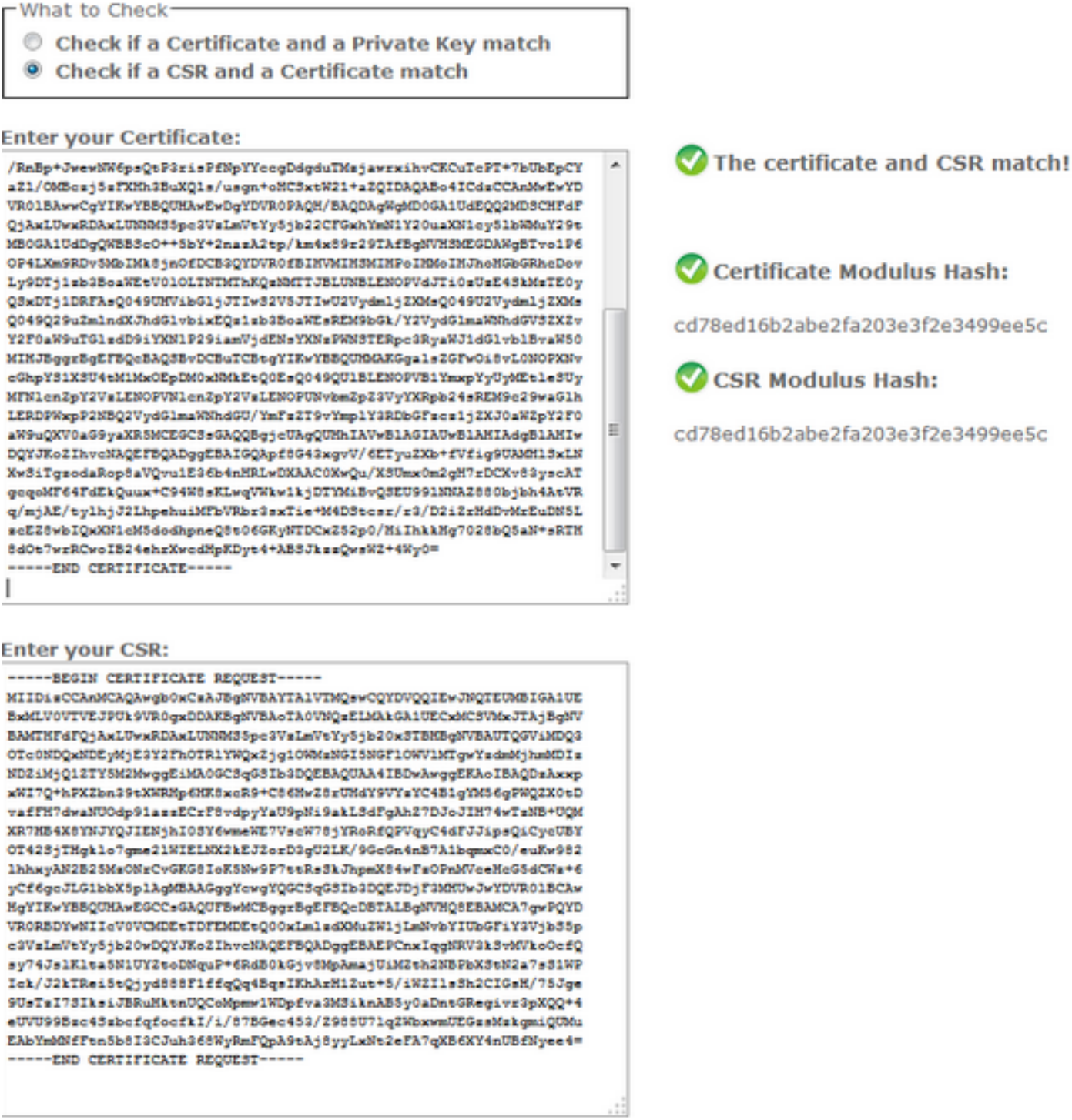
步驟2.使用安全FTP(SFTP)將簽署憑證複製到同一個資料夾中。 如果您無法設定SFTP伺服器，則TFTP資料夾上的上傳也能將憑證上傳到CUCM，如下圖所示。

```
[root@CCM105PUB keys]# sfpt cisco@10.66.90.19
bash: sfpt: command not found
[root@CCM105PUB keys]# sftp cisco@10.66.90.19
Connecting to 10.66.90.19...
Authenticated with partial success.
cisco@10.66.90.19's password:
Hello, I'm freeFTPd 1.0sftp> get tomcat.cer
Fetching /tomcat.cer to tomcat.cer
/tomcat.cer                                   100% 2140     2.1KB/s   00:00
sftp>
```

3.檢查MD5中的CSR和已簽名的證書，如下圖所示。

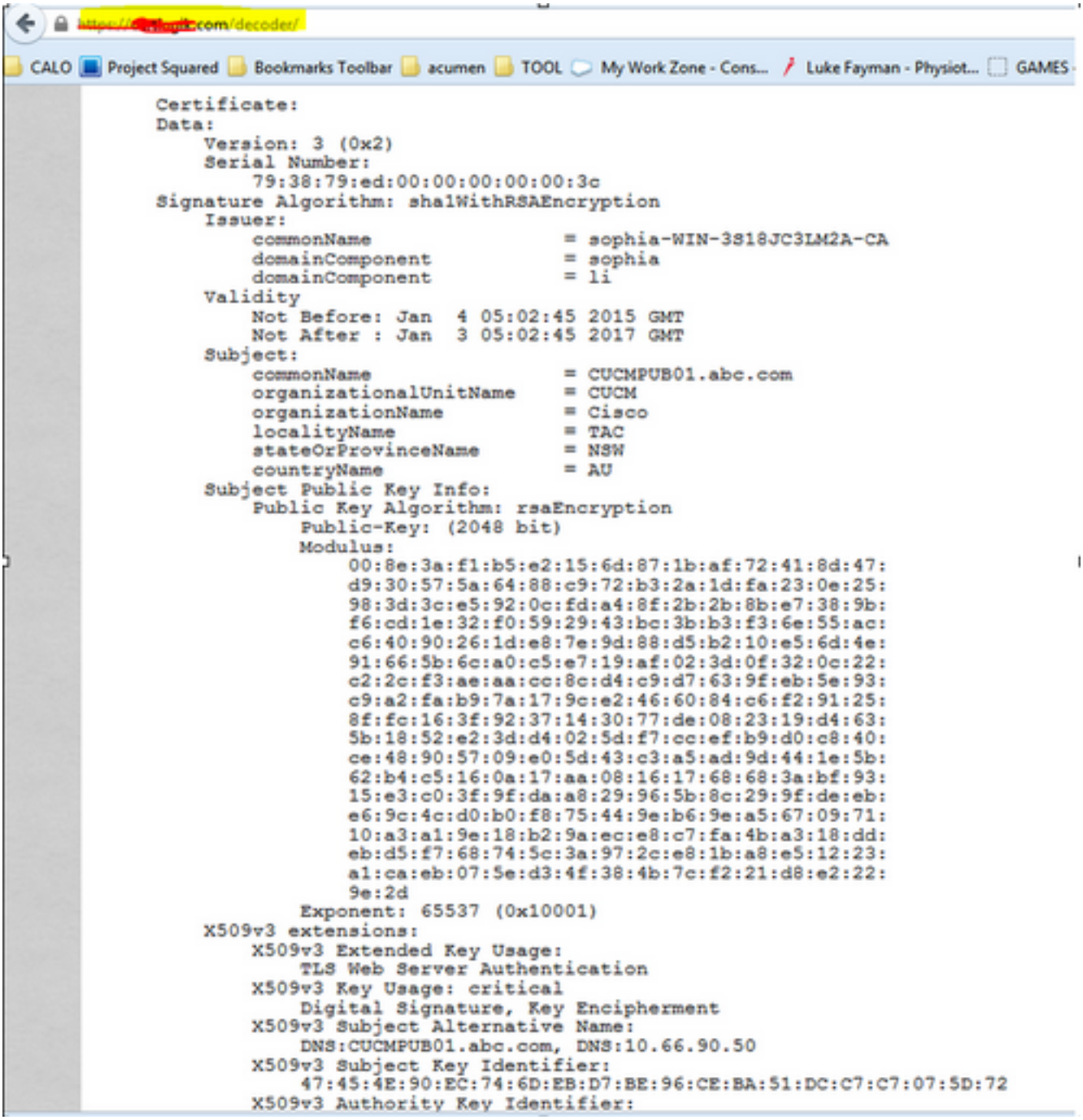
```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

解決方案2.使用來自Internet的任何SSL證書金鑰匹配程式

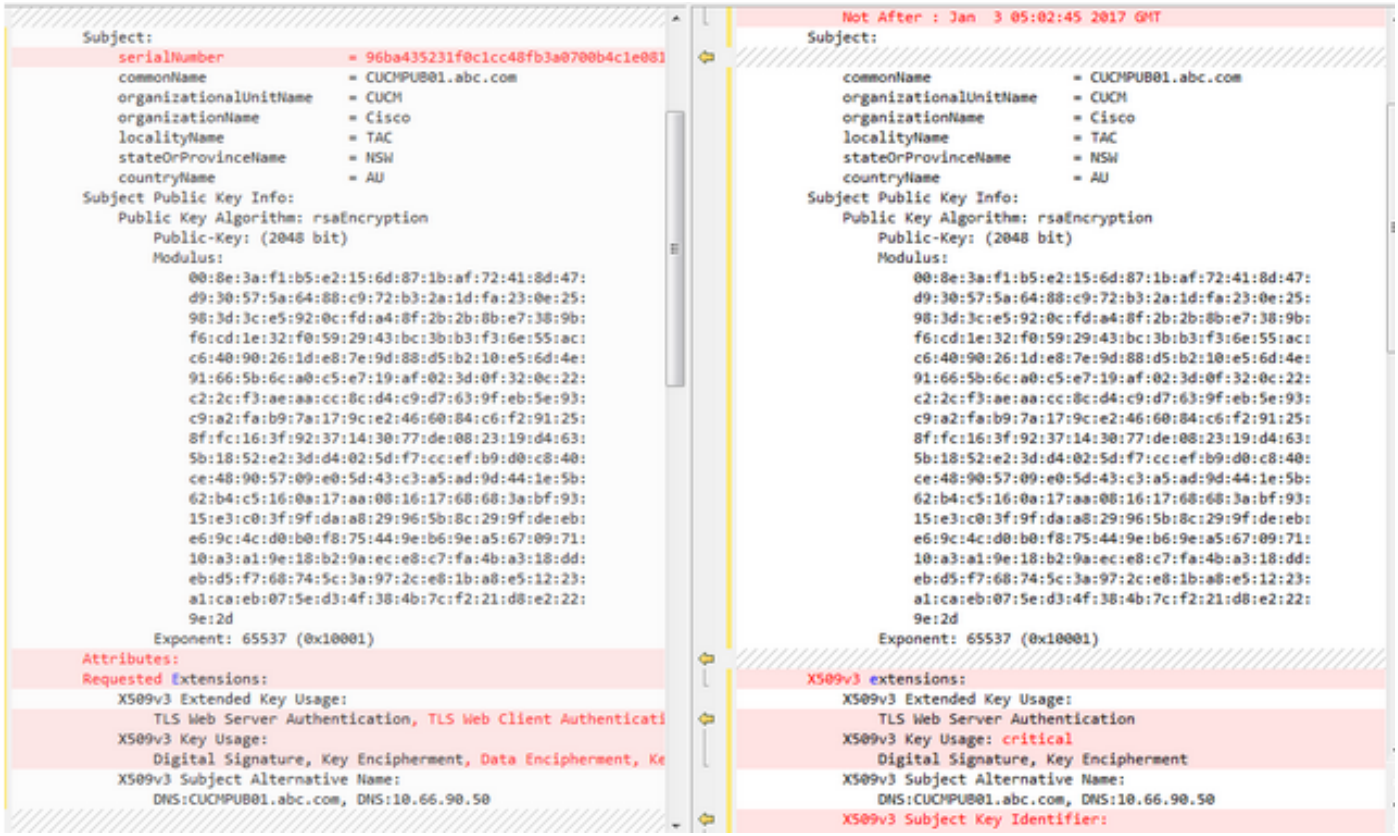


解決方案3.比較來自Internet的任何CSR解碼器的內容

步驟1.複製每個的**作業階段憑證**詳細資訊，如下圖所示。



步驟2.將這些產品在工具（如記事本）++Compare外掛中進行比較，如下圖所示。



```
        Subject:
            serialNumber               = 96ba435231f0c1cc48fb3a0700b4c1e081
            commonName                 = CUCMPUB01.abc.com
            organizationalUnitName     = CUCM
            organizationName           = Cisco
            localityName               = TAC
            stateOrProvinceName        = NSW
            countryName                = AU
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:8e:3a:f1:b5:e2:15:6d:87:1b:af:72:41:8d:47:
                    d9:30:57:5a:64:88:c9:72:b3:2a:1d:fa:23:0e:25:
                    98:3d:3c:e5:92:0c:fd:a4:8f:2b:2b:8b:e7:38:9b:
                    f6:cd:1e:32:f0:59:29:43:bc:3b:b3:f3:6e:55:ac:
                    c6:40:90:26:1d:e8:7e:9d:88:d5:b2:10:e5:6d:4e:
                    91:66:5b:6c:a0:c5:e7:19:af:02:3d:0f:32:0c:22:
                    c2:2c:f3:ae:aa:cc:8c:d4:c9:d7:63:9f:eb:5e:93:
                    c9:a2:fa:b9:7a:17:9c:e2:46:60:84:c6:f2:91:25:
                    8f:fc:16:3f:92:37:14:30:77:de:08:23:19:d4:63:
                    5b:18:52:e2:3d:d4:02:5d:f7:cc:ef:b9:d0:c8:40:
                    ce:48:90:57:09:e0:5d:43:c3:a5:ad:9d:44:1e:5b:
                    62:b4:c5:16:0a:17:aa:08:16:17:68:68:3a:bf:93:
                    15:e3:c0:3f:9f:da:a8:29:96:5b:8c:29:9f:de:eb:
                    e6:9c:4c:d0:b0:f8:75:44:9e:b6:9e:a5:67:09:71:
                    10:a3:a1:9e:18:b2:9a:ec:e8:c7:fa:4b:a3:18:dd:
                    eb:d5:f7:68:74:5c:3a:97:2c:e8:1b:a8:e5:12:23:
                    a1:ca:eb:07:5e:d3:4f:38:4b:7c:f2:21:d8:e2:22:
                    9e:2d
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authenticati
            X509v3 Key Usage:
                Digital Signature, Key Encipherment, Data Encipherment, Ke
            X509v3 Subject Alternative Name:
                DNS:CUCMPUB01.abc.com, DNS:10.66.90.50
```

```
            Not After : Jan  3 05:02:45 2017 GMT
        Subject:
            commonName                 = CUCMPUB01.abc.com
            organizationalUnitName     = CUCM
            organizationName           = Cisco
            localityName               = TAC
            stateOrProvinceName        = NSW
            countryName                = AU
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:8e:3a:f1:b5:e2:15:6d:87:1b:af:72:41:8d:47:
                    d9:30:57:5a:64:88:c9:72:b3:2a:1d:fa:23:0e:25:
                    98:3d:3c:e5:92:0c:fd:a4:8f:2b:2b:8b:e7:38:9b:
                    f6:cd:1e:32:f0:59:29:43:bc:3b:b3:f3:6e:55:ac:
                    c6:40:90:26:1d:e8:7e:9d:88:d5:b2:10:e5:6d:4e:
                    91:66:5b:6c:a0:c5:e7:19:af:02:3d:0f:32:0c:22:
                    c2:2c:f3:ae:aa:cc:8c:d4:c9:d7:63:9f:eb:5e:93:
                    c9:a2:fa:b9:7a:17:9c:e2:46:60:84:c6:f2:91:25:
                    8f:fc:16:3f:92:37:14:30:77:de:08:23:19:d4:63:
                    5b:18:52:e2:3d:d4:02:5d:f7:cc:ef:b9:d0:c8:40:
                    ce:48:90:57:09:e0:5d:43:c3:a5:ad:9d:44:1e:5b:
                    62:b4:c5:16:0a:17:aa:08:16:17:68:68:3a:bf:93:
                    15:e3:c0:3f:9f:da:a8:29:96:5b:8c:29:9f:de:eb:
                    e6:9c:4c:d0:b0:f8:75:44:9e:b6:9e:a5:67:09:71:
                    10:a3:a1:9e:18:b2:9a:ec:e8:c7:fa:4b:a3:18:dd:
                    eb:d5:f7:68:74:5c:3a:97:2c:e8:1b:a8:e5:12:23:
                    a1:ca:eb:07:5e:d3:4f:38:4b:7c:f2:21:d8:e2:22:
                    9e:2d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Subject Alternative Name:
                DNS:CUCMPUB01.abc.com, DNS:10.66.90.50
            X509v3 Subject Key Identifier:
```