Überprüfung der CSR- und Zertifikatsabweichung für UC

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie festgestellt werden kann, ob das signierte Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) mit dem vorhandenen CSR (Certificate Signing Request) für Cisco Unified Application Server übereinstimmt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über X.509/CSR zu verfügen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

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.

Zugehörige Produkte

Dieses Dokument kann auch mit den folgenden Hardware- und Softwareversionen verwendet werden:

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified IM und Presence

- Cisco Unified Unity Connection
- CUIS
- Cisco Meidasence
- Cisco Unified Contact Center Express (UCCX)

Hintergrundinformationen

Ein Zertifizierungsantrag besteht aus einem DN, einem öffentlichen Schlüssel und einem optionalen Satz von Attributen, die gemeinsam von der Stelle unterzeichnet werden, die die Zertifizierung anfordert. Zertifizierungsanfragen werden an eine Zertifizierungsstelle gesendet, die den Antrag in ein X.509-Zertifikat für den öffentlichen Schlüssel umwandelt. In welcher Form gibt die Zertifizierungsstelle das neu signierte Zertifikat zurück, das nicht in den Geltungsbereich dieses Dokuments fällt. Eine PKCS #7-Nachricht ist eine Möglichkeit. (RFC:2986).

Zertifikatsverwaltung von Cisco Communications Manager

Die Aufnahme eines Satzes von Attributen soll in zweifacher Hinsicht erfolgen:

- Um weitere Informationen über eine bestimmte Entität oder ein Anfechtungskennwort bereitzustellen, mit dem die Entität später den Widerruf eines Zertifikats beantragen kann.
- Um Attribute für die Aufnahme in X.509-Zertifikate bereitzustellen. Die aktuellen Unified Communications (UC)-Server unterstützen kein Challenge-Passwort.

Aktuelle Cisco UC-Server benötigen diese Attribute in einem CSR (siehe folgende Tabelle):

Informationen	Beschreibung
Orgie	Organisationseinheit
Orgname	Organisationsname
Ort	Sitz der Organisation
Staat	Organisationsstatus
Land	Ländercode kann nicht geändert werden.
alternatehostname	alternativer Hostname

Problem

Wenn Sie UC unterstützen, können Sie in vielen Fällen feststellen, dass das von der CA signierte Zertifikat nicht auf die UC-Server hochgeladen wird. Sie können nicht immer angeben, was bei der Erstellung des signierten Zertifikats geschehen ist, da Sie nicht die Person sind, die den CSR zum Erstellen des signierten Zertifikats verwendet hat. In den meisten Szenarien dauert das erneute Signieren eines neuen Zertifikats mehr als 24 Stunden. UC-Server wie CUCM verfügen nicht über detailliertes Log/Trace, um den Fehler beim Hochladen des Zertifikats zu identifizieren, sondern geben lediglich eine Fehlermeldung aus. Dieser Artikel soll das Problem eingrenzen, ob es sich um ein UC-Server- oder ein CA-Problem handelt.

Allgemeine Praxis für CA-signierte Zertifikate in CUCM

CUCM unterstützt die Integration mit CAs von Drittanbietern mithilfe eines PKCS#10 CSR-Mechanismus, auf den über die GUI des Cisco Unified Communications Operating System Certificate Manager zugegriffen werden kann. Kunden, die derzeit CAs von Drittanbietern verwenden, müssen den CSR-Mechanismus verwenden, um Zertifikate für Cisco CallManager,

CAPF, IPSec und Tomcat auszustellen.

Schritt 1: Ändern Sie die Identifikationsnummer, bevor Sie die CSR-Anfrage erstellen.

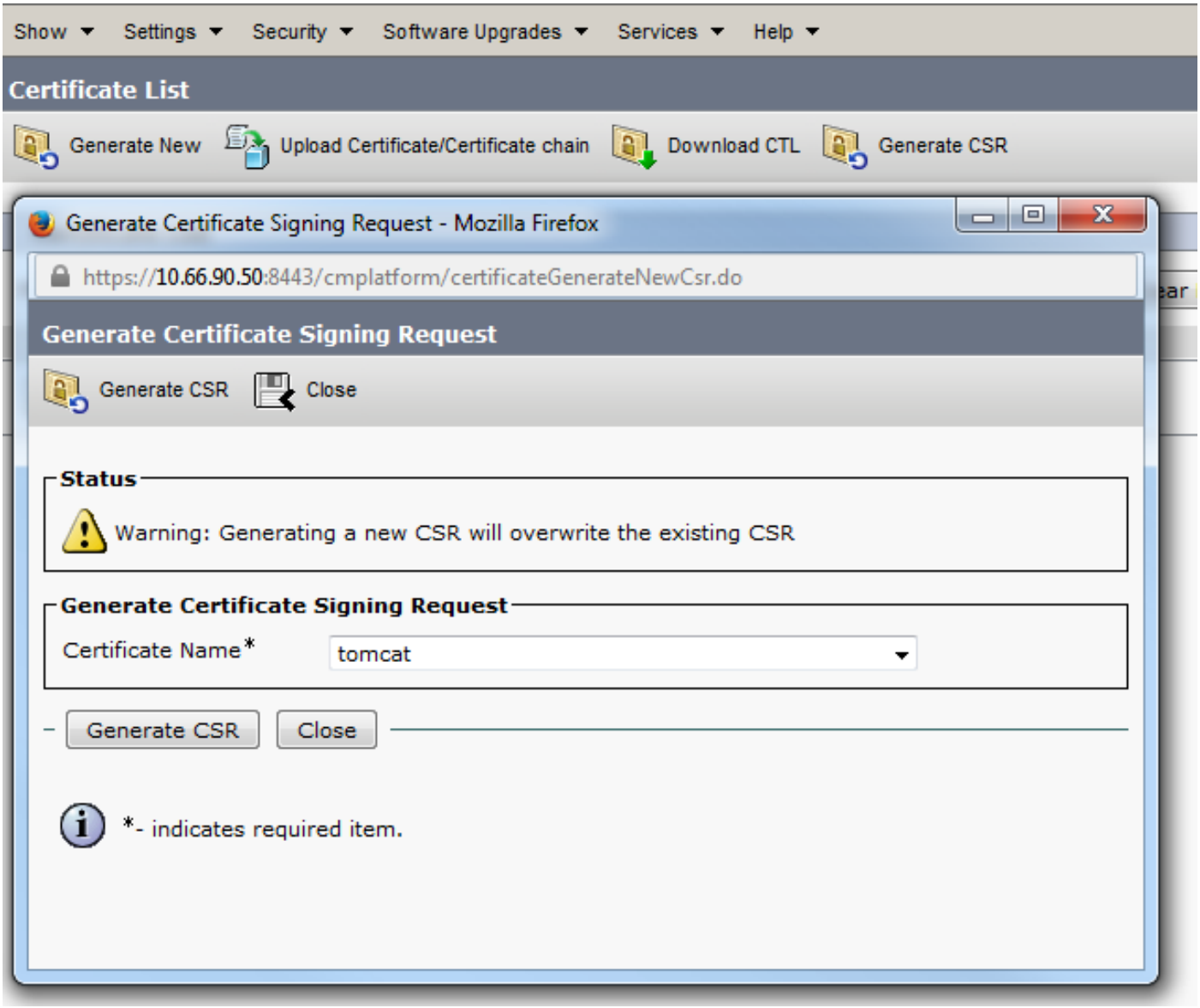
Die Identität des CUCM-Servers zur Generierung eines CSR kann mithilfe des Befehls **set web-security** geändert werden, wie in diesem Bild gezeigt.

```
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
```

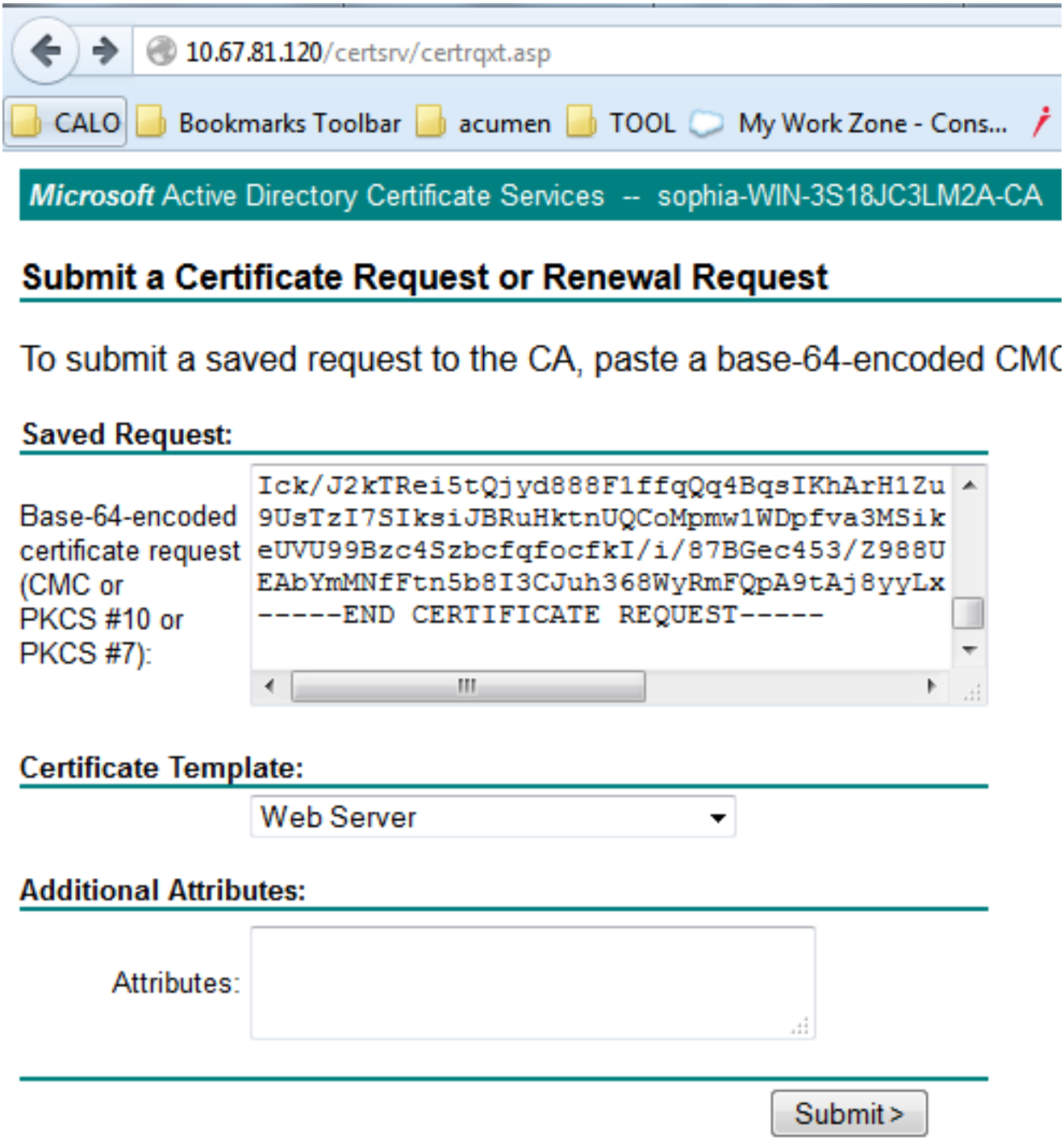
Wenn Sie in den obigen Feldern Speicherplatz haben, verwenden Sie **""**, um den Befehl wie im Bild gezeigt auszuführen.

```
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)?
```

Schritt 2: Erstellen Sie CSR, wie im Bild gezeigt.

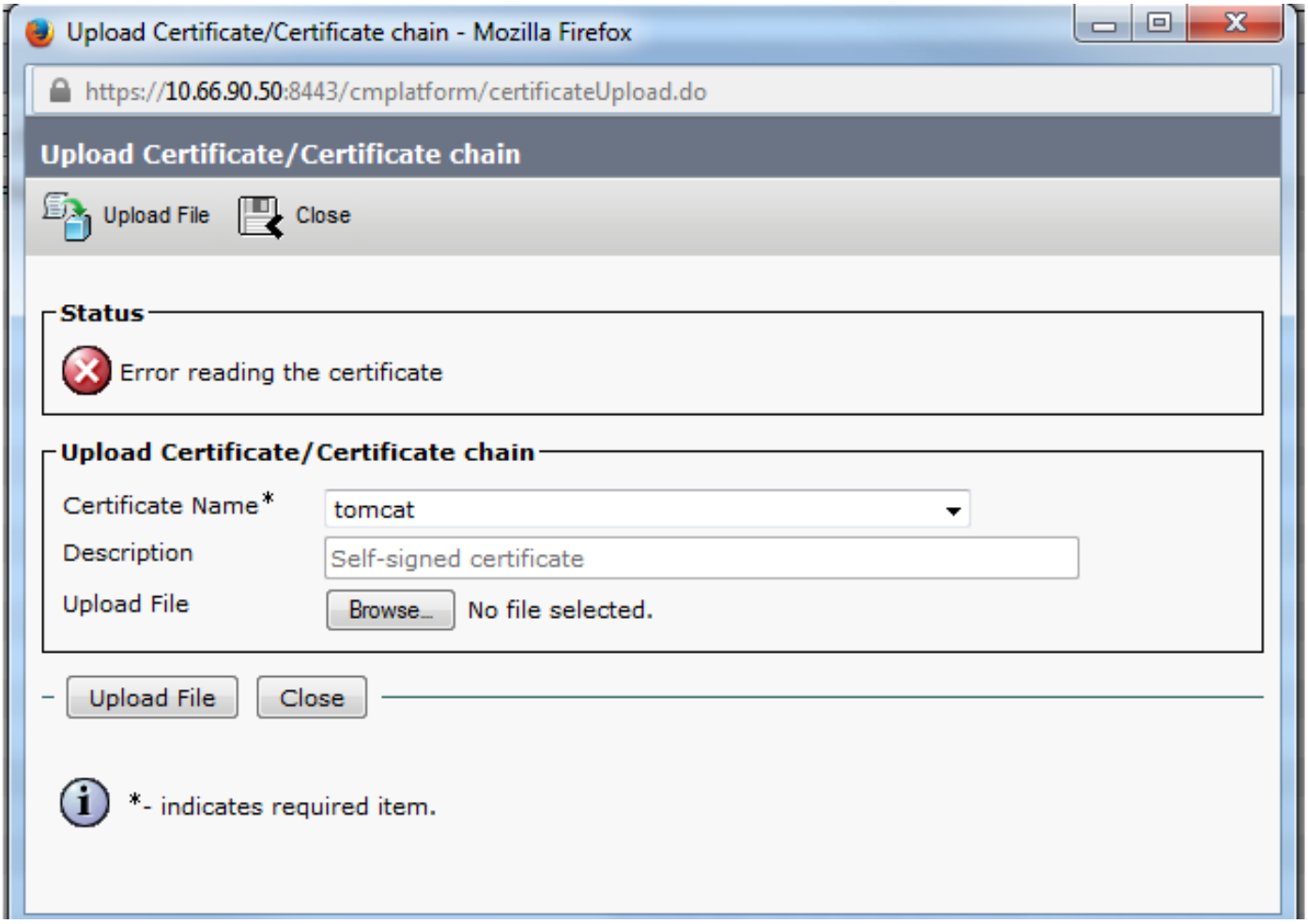


Schritt 3: Laden Sie den CSR herunter und lassen Sie ihn von der CA signieren, wie im Bild gezeigt.



Schritt 4: Laden Sie das Zertifikat mit CA-Signatur auf den Server hoch.

Wenn die CSR-Nummer erstellt und das Zertifikat signiert ist und Sie es nicht mit der Fehlermeldung "Fehler beim Lesen des Zertifikats" hochladen (wie in diesem Bild gezeigt), müssen Sie überprüfen, ob die CSR-Nummer erneut generiert wird oder ob das signierte Zertifikat selbst die Ursache des Problems ist.



Es gibt drei Möglichkeiten zu überprüfen, ob die CSR-Anfrage regeneriert wird oder das signierte Zertifikat selbst die Ursache für die Ausgabe ist.

Lösung 1. OpenSSL-Befehl in root (oder Linux) verwenden

Schritt 1: Melden Sie sich beim Stamm an, und navigieren Sie zum Ordner, wie im Bild gezeigt.

```
[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]#
```

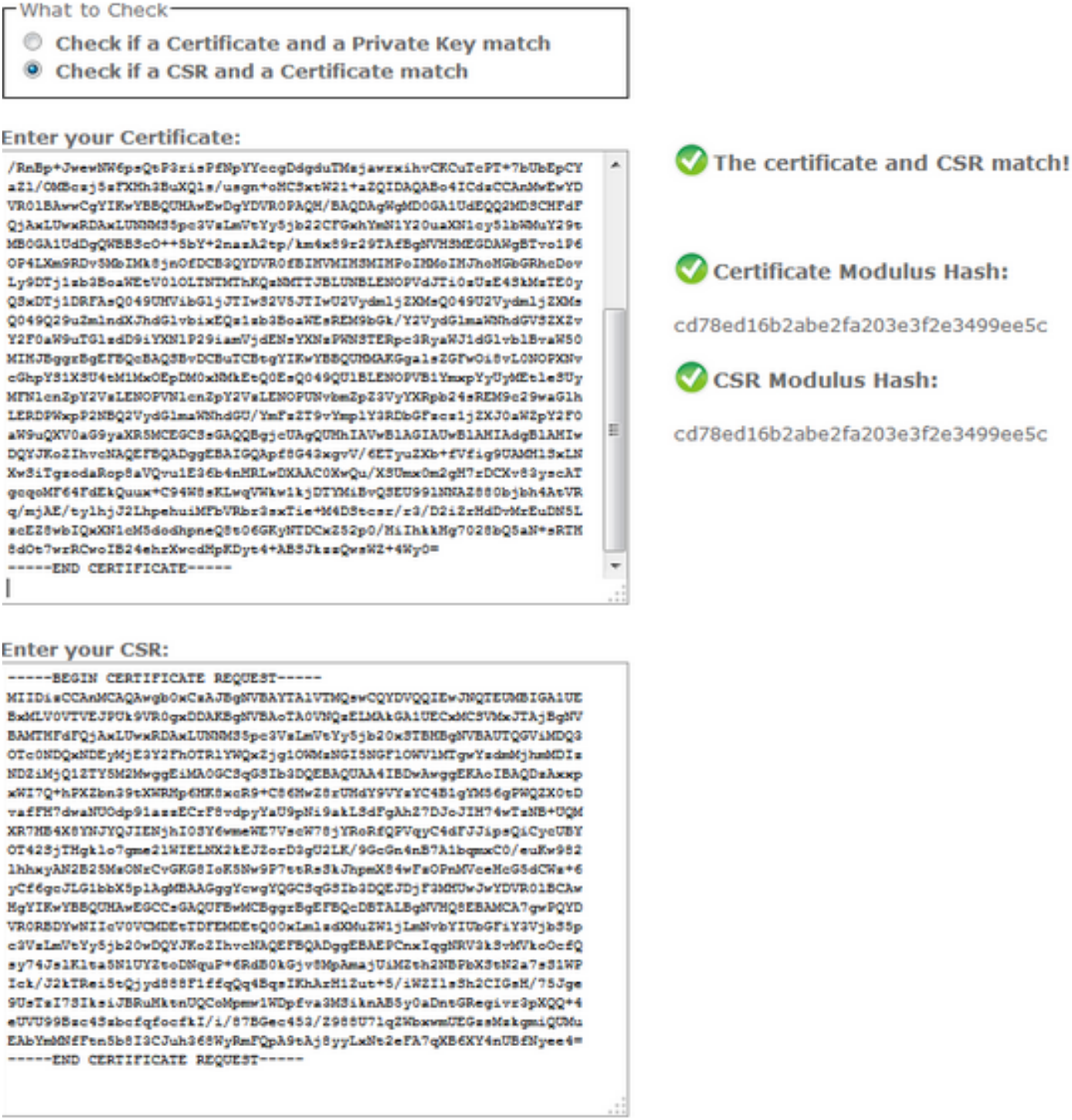
Schritt 2: Kopieren Sie das signierte Zertifikat in denselben Ordner mit Secure FTP (SFTP). Wenn Sie keinen SFTP-Server einrichten können, kann das Zertifikat auch vom Upload im TFTP-Ordner auf den CUCM übertragen werden, wie im Bild gezeigt.

```
[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. Überprüfen Sie MD5 auf die CSR-Nummer und das signierte Zertifikat, wie im Bild gezeigt.

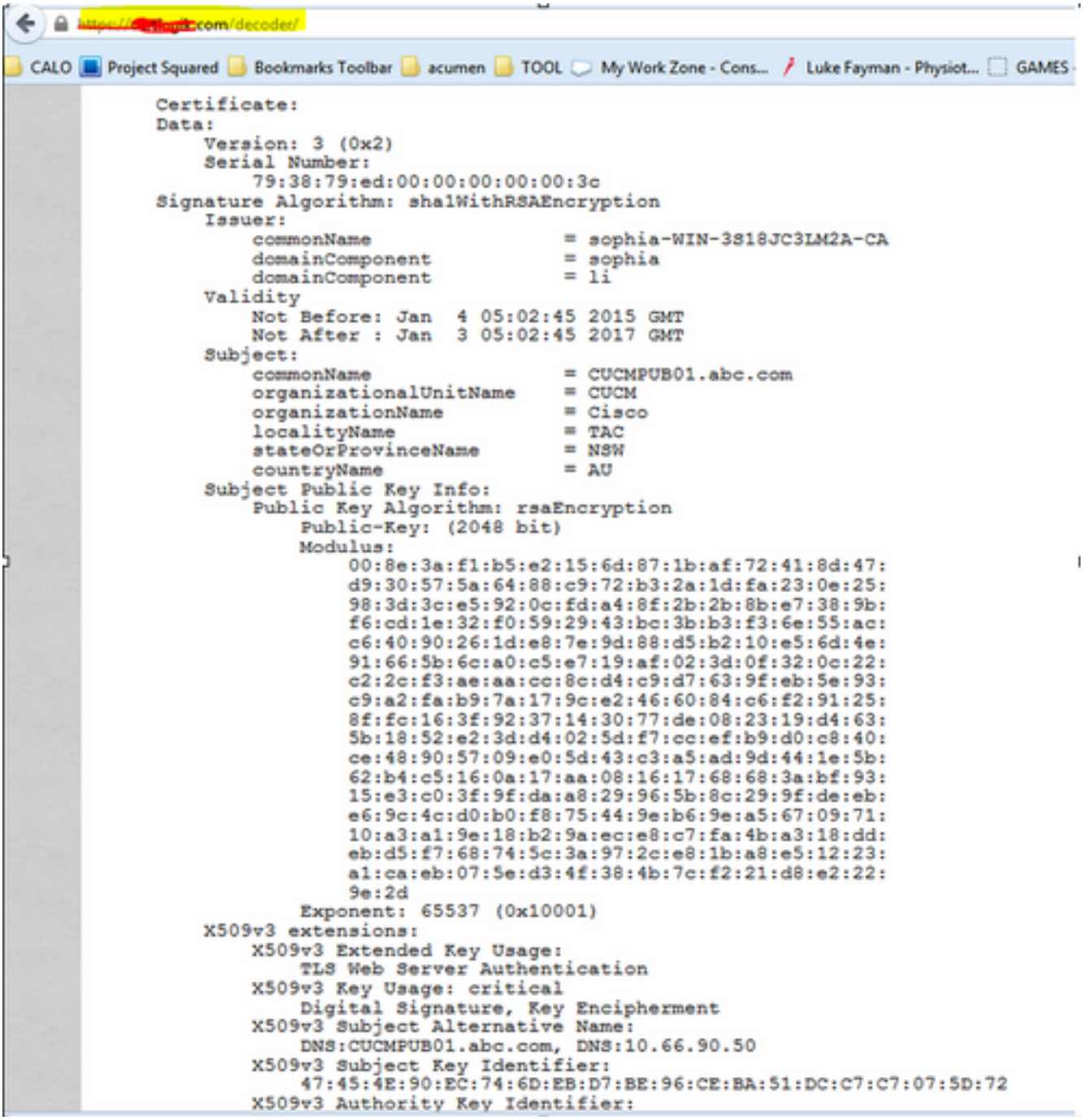
```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

Lösung 2. Beliebige SSL-Zertifikatsschlüsselzuordnung aus dem Internet verwenden

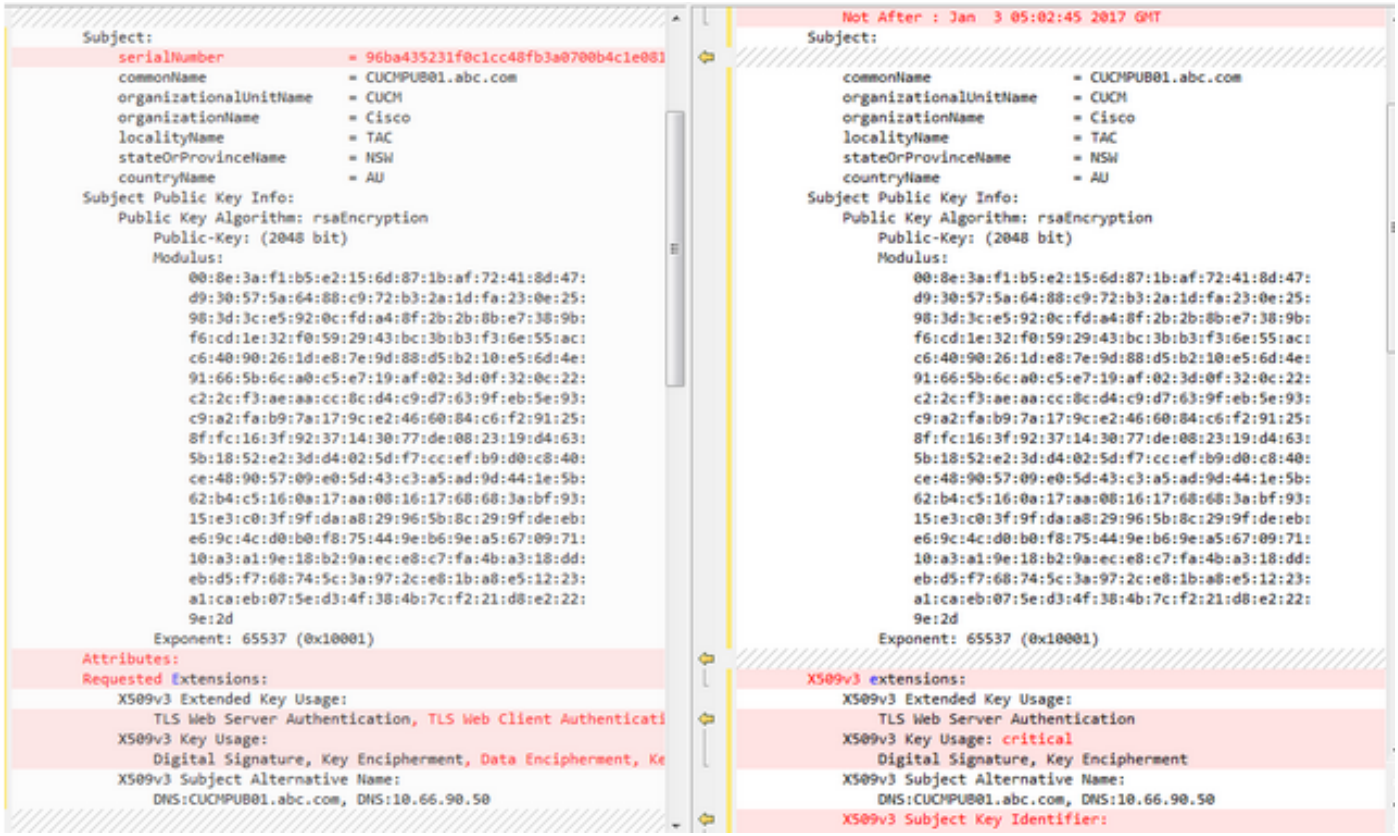


Lösung 3. Vergleichen von Inhalten aus jedem CSR-Decoder aus dem Internet

Schritt 1: Kopieren Sie die **Detailinformationen** des Sitzungszertifikats für jede Sitzung, wie in diesem Bild gezeigt.



Schritt 2: Vergleichen Sie sie in einem Tool wie Notepad+ mit dem Plugin Vergleichen, wie in diesem Bild gezeigt.



```
        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:
```