Controleer CSR- en certificaatwanverhouding voor UC

Inhoud

Inleiding

Dit document beschrijft hoe u kunt bepalen of het door de certificaatinstantie (CA) ondertekende certificaat overeenkomt met het bestaande certificaataanvraag (CSR) voor Cisco Unified Application Server.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van X.509/CSR.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Dit document kan ook met deze hardware- en softwareversies worden gebruikt:

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified IM and Presence
- Cisco Unified Unity Connection-software

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

Achtergrondinformatie

Een certificeringsaanvraag bestaat uit een vooraanstaande naam, een openbare sleutel en een optionele reeks eigenschappen die gezamenlijk ondertekend zijn door de entiteit die om de certificering verzoekt. Certificeringsverzoeken worden toegezonden aan een certificeringsinstantie die het verzoek in een X.509-certificaat omzet. In welke vorm heeft de certificeringsinstantie het nieuw ondertekende certificaat teruggegeven dat niet onder het toepassingsgebied van dit document valt. Een PKCS #7-bericht is één mogelijkheid.(RFC:2986).

Cisco Communications Manager-certificaatbeheer

Het voornemen om een reeks eigenschappen op te nemen is tweeledig:

- Om andere informatie over een bepaalde entiteit te verstrekken, of een aanspreekwachtwoord waarmee de entiteit later om intrekking van certificaten kan verzoeken.
- Om eigenschappen te verschaffen voor opname in X.509-certificaten. De huidige Unified Communications (UC)-servers ondersteunen geen uitdagingswachtwoord.

Huidige Cisco UC-servers vereisen deze eigenschappen in een CSR zoals weergegeven in deze tabel:

Informatie	Beschrijving
orka	organisatorische eenheid
oornaam	naam van de organisatie
plaats	plaats van de organisatie
toestand	organisatiestatus
land	landcode kan niet worden gewijzigd
alternatieve hostname	alternatieve naam

Probleem

Wanneer u UC ondersteunt, kunt u veel gevallen tegenkomen waarin het door CA ondertekende certificaat niet op de UC-servers wordt geüpload. U kunt niet altijd identificeren wat heeft plaatsgevonden op het moment van het creëren van het ondertekende certificaat, aangezien u niet de persoon bent die de CSR gebruikte om het ondertekende certificaat te maken. In de meeste scenario's duurt het opnieuw tekenen van een nieuw certificaat meer dan 24 uur. UC-servers zoals CUCM hebben geen gedetailleerd logbestand/spoor om te helpen identificeren waarom het uploaden van het certificaat mislukt, maar geven gewoon een foutmelding. De bedoeling van dit artikel is om de kwestie te vernauwen, of het nu een UC-server of een CA-kwestie is.

Algemene praktijk voor door CA ondertekende certificaten in CUCM

CUCM ondersteunt integratie met CA’s van derden met behulp van een PKCS#10 CSR-mechanisme dat toegankelijk is op de Cisco Unified Communications Operating System Manager GUI. Klanten, die momenteel CA's van derden gebruiken moeten het CSR-mechanisme gebruiken

om certificaten voor Cisco CallManager, CAPF, IPSec, en Tomcat uit te geven.

Stap 1. Verander het Identificeer voordat u de CSR genereert.

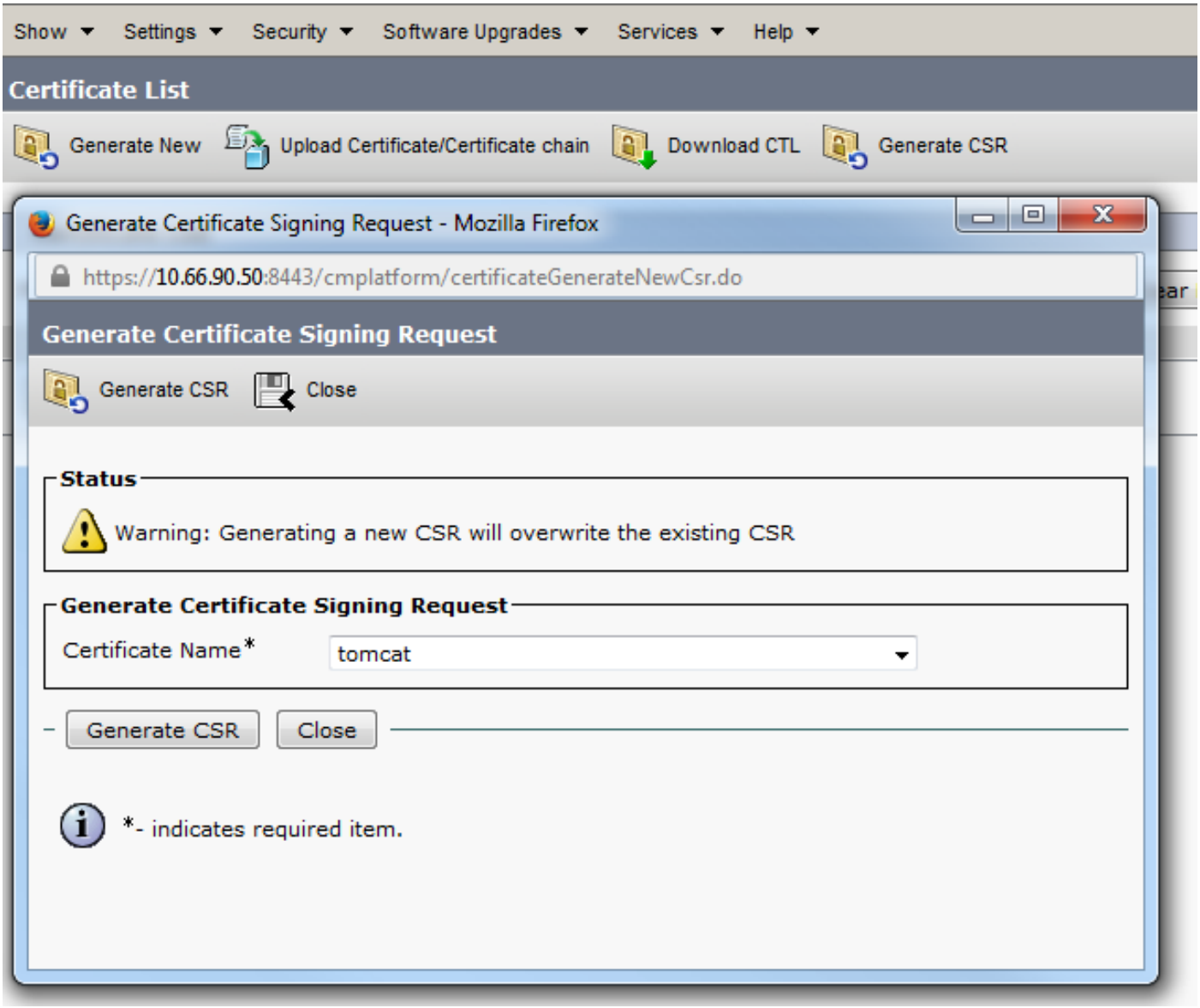
De identiteit van de CUCM-server om een CSR te genereren kan worden gewijzigd met behulp van de opdracht **ingesteld web-security** zoals in deze afbeelding wordt getoond.

```
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
```

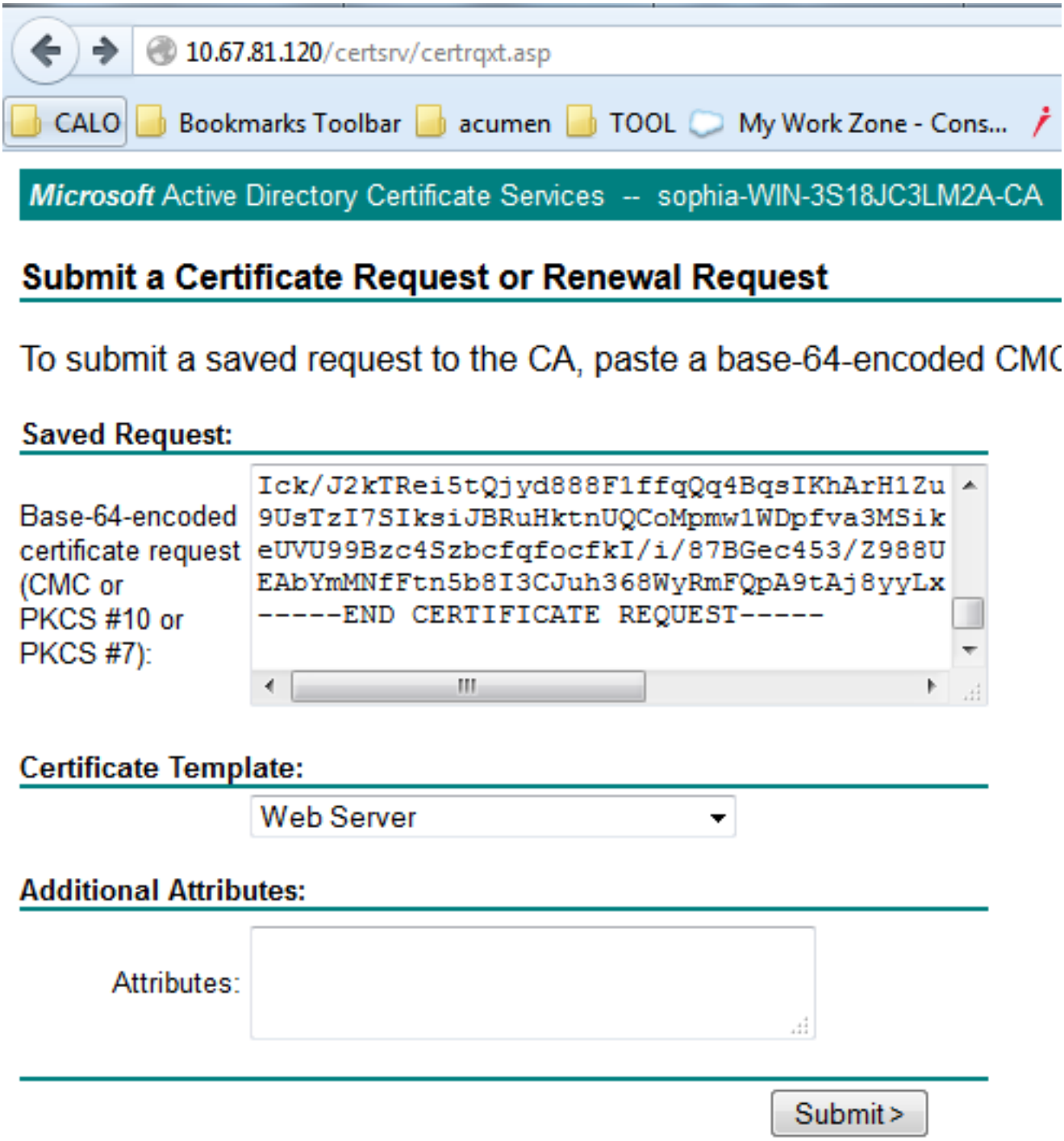
Als u in de bovengenoemde velden ruimte hebt, gebruikt u **"** om de opdracht zoals in de afbeelding te bereiken.

```
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)?
```

Stap 2. Generate CSR zoals getoond in de afbeelding.

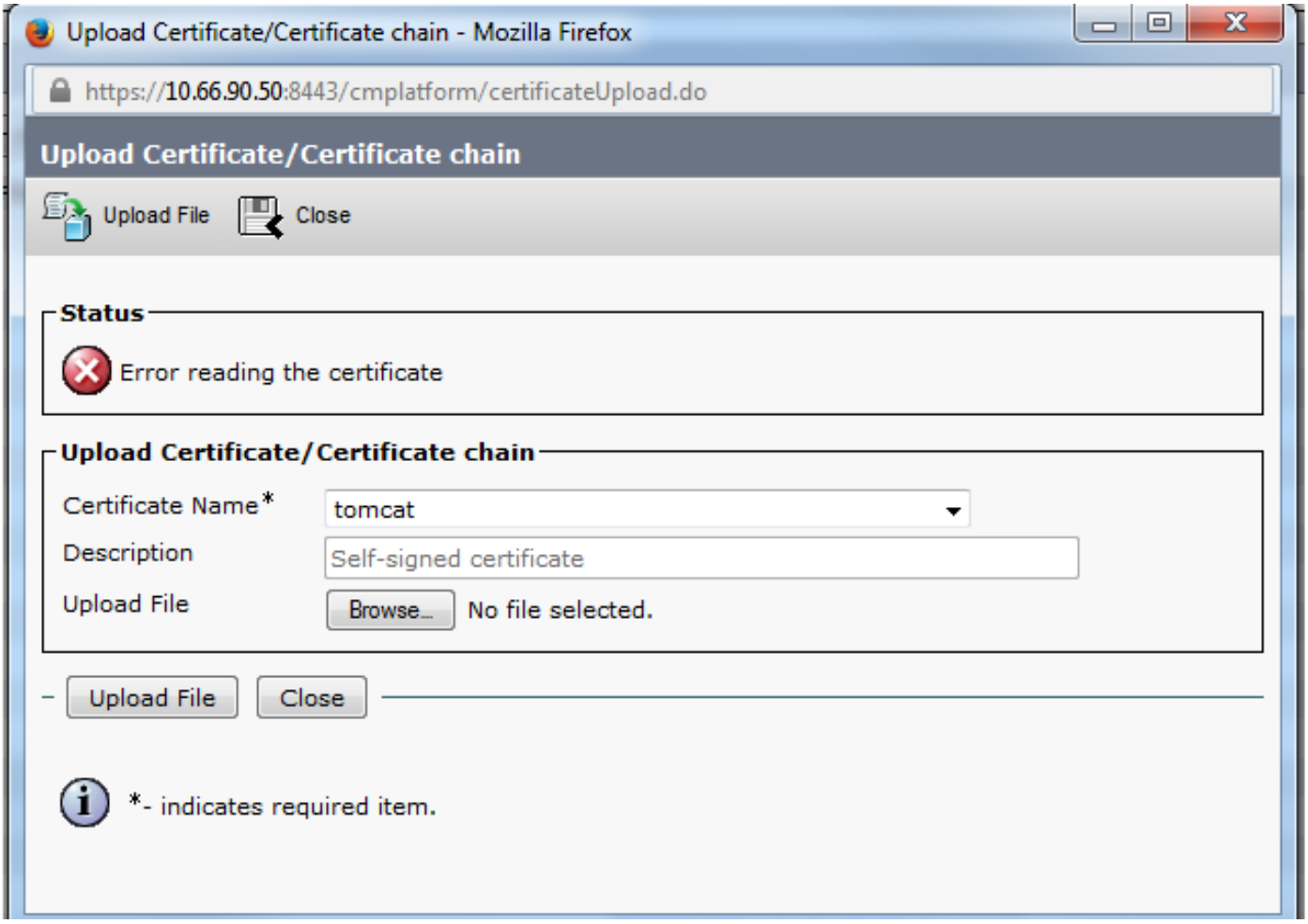


Stap 3. Download de CSR en laat het ondertekend door CA zoals in de afbeelding.



Stap 4. Upload het CA-ondertekend certificaat naar de server.

Wanneer de CSR gegenereerd is en het certificaat getekend is en u het niet uploadt met een foutbericht "Fout bij lezen van het certificaat" (zoals in deze afbeelding getoond), moet u controleren of de CSR opnieuw gegenereerd is of het ondertekende certificaat zelf de oorzaak van de afgifte is.



Er zijn drie manieren om te controleren of de CSR opnieuw wordt gegenereerd of het ondertekende certificaat zelf de oorzaak van de uitgifte is.

Oplossing 1. Gebruik OpenSSL-opdracht in root (of linux)

Stap 1. Meld u aan bij de wortel en navigeer naar de map zoals in de afbeelding.

```
[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]#
```

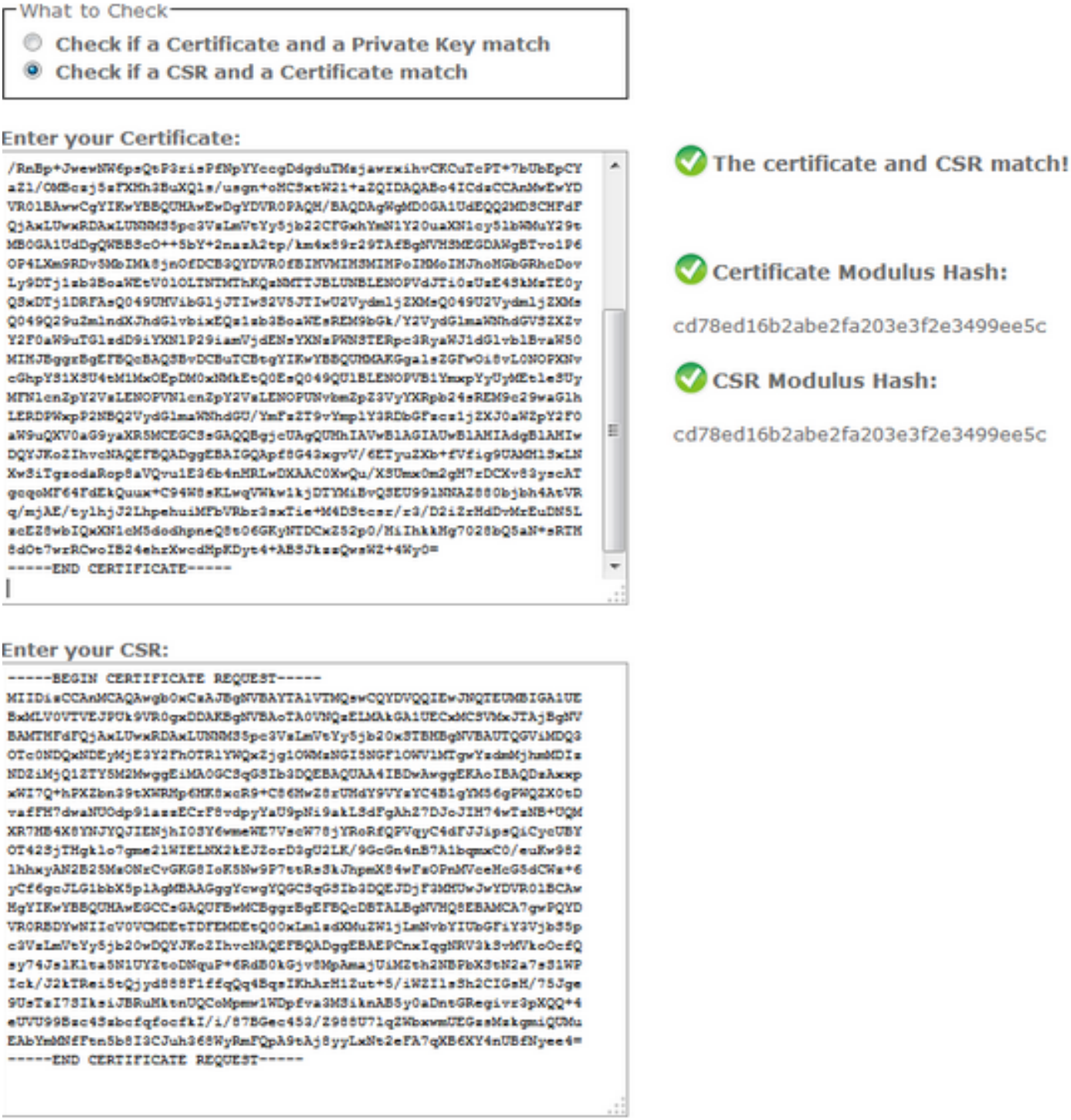
Stap 2. Kopieer het ondertekende certificaat naar dezelfde map met Secure FTP (SFTP). Als u geen SFTP-server kunt instellen, kan het uploaden in de TFTP-map ook het certificaat naar het CUCM verkrijgen zoals in de afbeelding wordt weergegeven.

```
[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. Controleer de MD5 op de CSR en het ondertekende certificaat zoals in de afbeelding weergegeven.

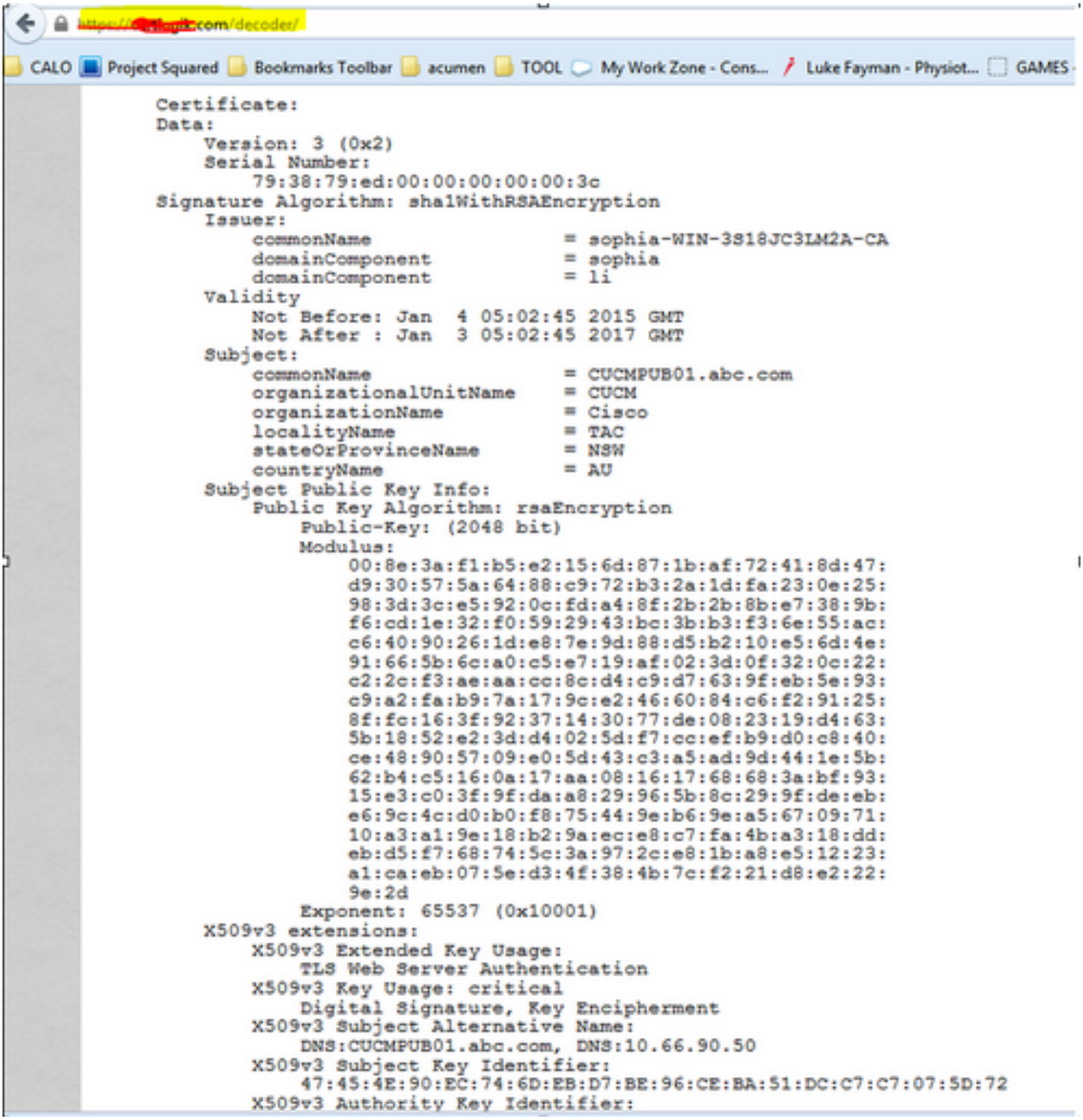
```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

Oplossing 2. Gebruik elke SSL-certificaattoetser van internet

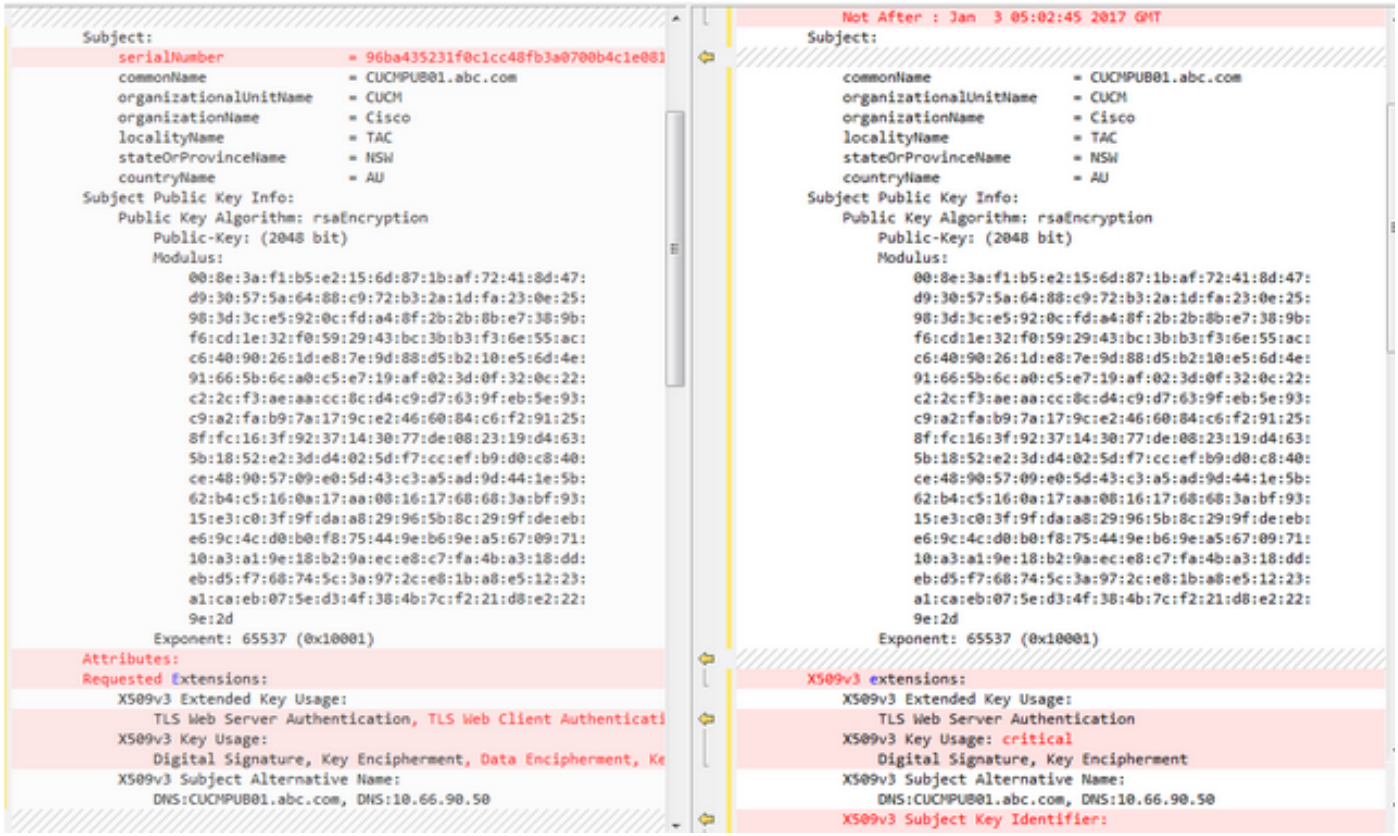


Oplossing 3. Vergelijk inhoud met elke CSR-decoder van internet

Stap 1. Kopieer de **gedetailleerde informatie** van het **sessiecertificaat** voor elke sessie zoals in deze afbeelding.



Stap 2. Vergelijk ze in een gereedschap zoals Kladblok+ met de stekker Vergelijken zoals in deze afbeelding.



```
        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:
```