Vérifiez le CSR et la non-concordance de certificat pour l'UC

Contenu

Introduction

Ce document décrit comment identifier si le certificat signé d'Autorité de certification (CA) apparie la demande de signature de certificat existant (CSR) des serveurs d'applications de Cisco Unified.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de X.509/CSR.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified IM et présence
- Unity Connection de Cisco Unified

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

Informations générales

Une demande de certification se compose d'un nom unique, d'une clé publique, et d'un ensemble facultatif d'attributs collectivement signés par l'entité qui demandent la certification. Des demandes de certification sont envoyées à une autorité de certification qui transforme la demande en certificat de clé publique X.509. Dans quel formulaire l'autorité de certification renvoie le certificat nouvellement signé est hors de portée de ce document. Un message PKCS #7 est un possibility.(RFC:2986).

Gestion de certificat de Cisco Communications Manager

L'intention d'inclure un ensemble d'attributs est double :

- Afin de fournir d'autres informations sur une entité donnée, ou un mot de passe de défi par lequel l'entité peut plus tard demander la révocation de certificat.
- Afin de fournir des attributs pour l'intégration dans les Certificats X.509. Les serveurs des transmissions unifiés par courant (UC) ne prennent en charge pas un mot de passe de défi.

Les serveurs en cours de Cisco UC ont besoin de ces attributs dans un CSR suivant les indications de cette table :

Les informations	Description
orgunit	unité organisationnelle
orgname	nom organisationnel
localité	emplacement d'organisation
état	état d'organisation
pays	code de pays ne peut pas être changé
alternatehostname	nom d'hôte alternatif

Problème

Quand vous prenez en charge l'UC, vous pouvez rencontrer beaucoup de cas où le certificat signé CA ne le télécharge pas sur les serveurs UC. Vous ne pouvez pas toujours identifier ce qui s'est produit au moment de la création du certificat signé, puisque vous n'êtes pas la personne qui a utilisé le CSR afin de créer le certificat signé. Dans la plupart des scénarios, la re-signature d'un nouveau certificat prend plus de 24 heures. Les serveurs UC tels que CUCM n'ont pas détaillé le log/suivi afin d'aider à identifier pourquoi le téléchargement de certificat échoue mais ils donnent juste un message d'erreur. L'intention de cet article est de rétrécir vers le bas la question, si c'est un serveur UC ou une question CA.

Pratique générale pour les Certificats Ca-signés dans CUCM

CUCM prend en charge l'intégration avec la tierce partie CAs avec l'utilisation d'un mécanisme CSR PKCS#10 qui est accessible au GUI du système d'exploitation de gestionnaire de certificat de Cisco Unified Communications. Les clients, qui utilisent actuellement la tierce partie CAs doivent employer le mécanisme CSR afin de délivrer des Certificats pour le Cisco CallManager, le

CAPF, l'IPSec, et le Tomcat.

Étape 1. Changez l'identifier avant que vous génériez le CSR.

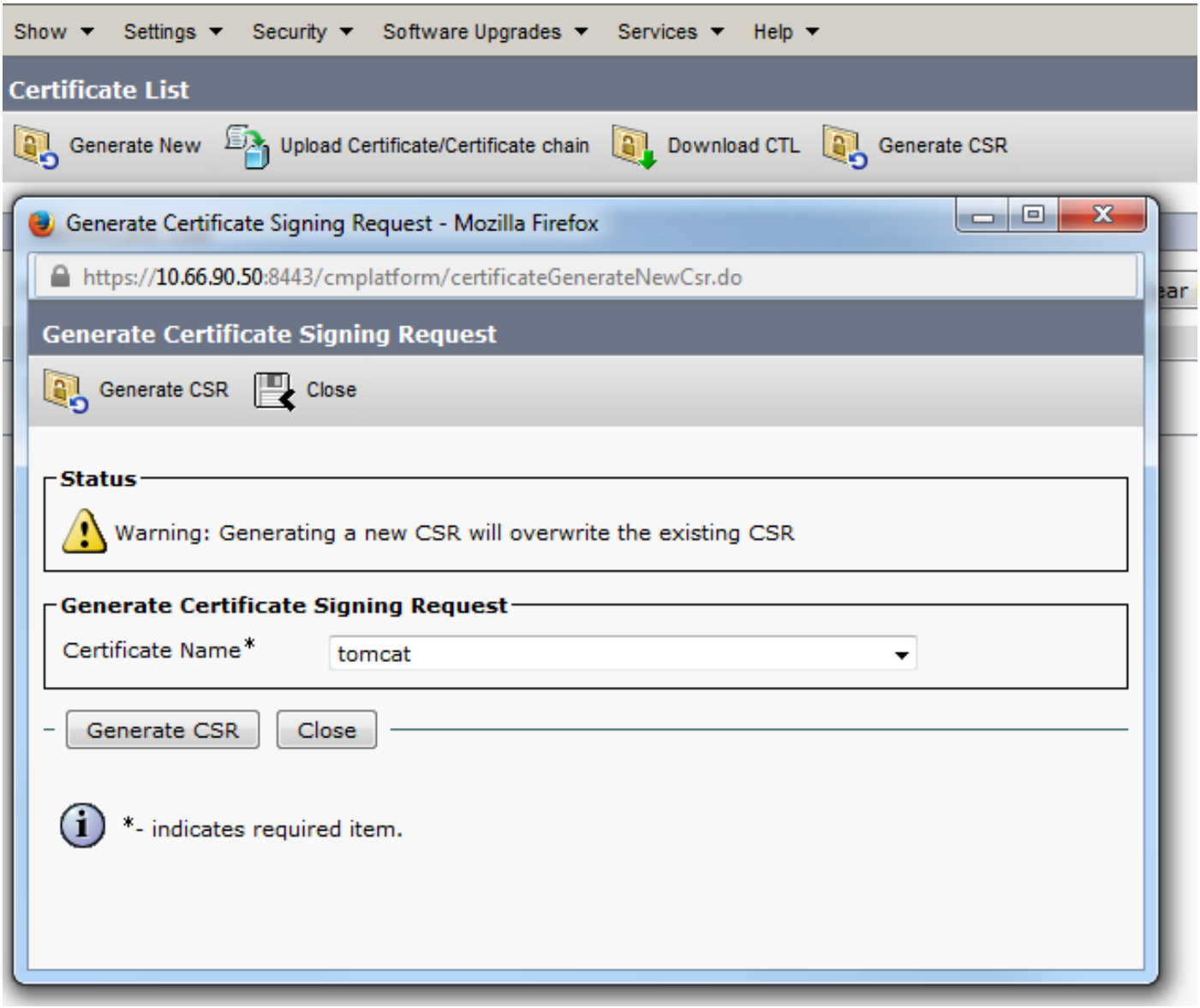
L'identité du serveur CUCM afin de générer un CSR peut être modifiée avec l'utilisation de la **sécurité Web réglée de** commande suivant les indications de cette image.

```
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
```

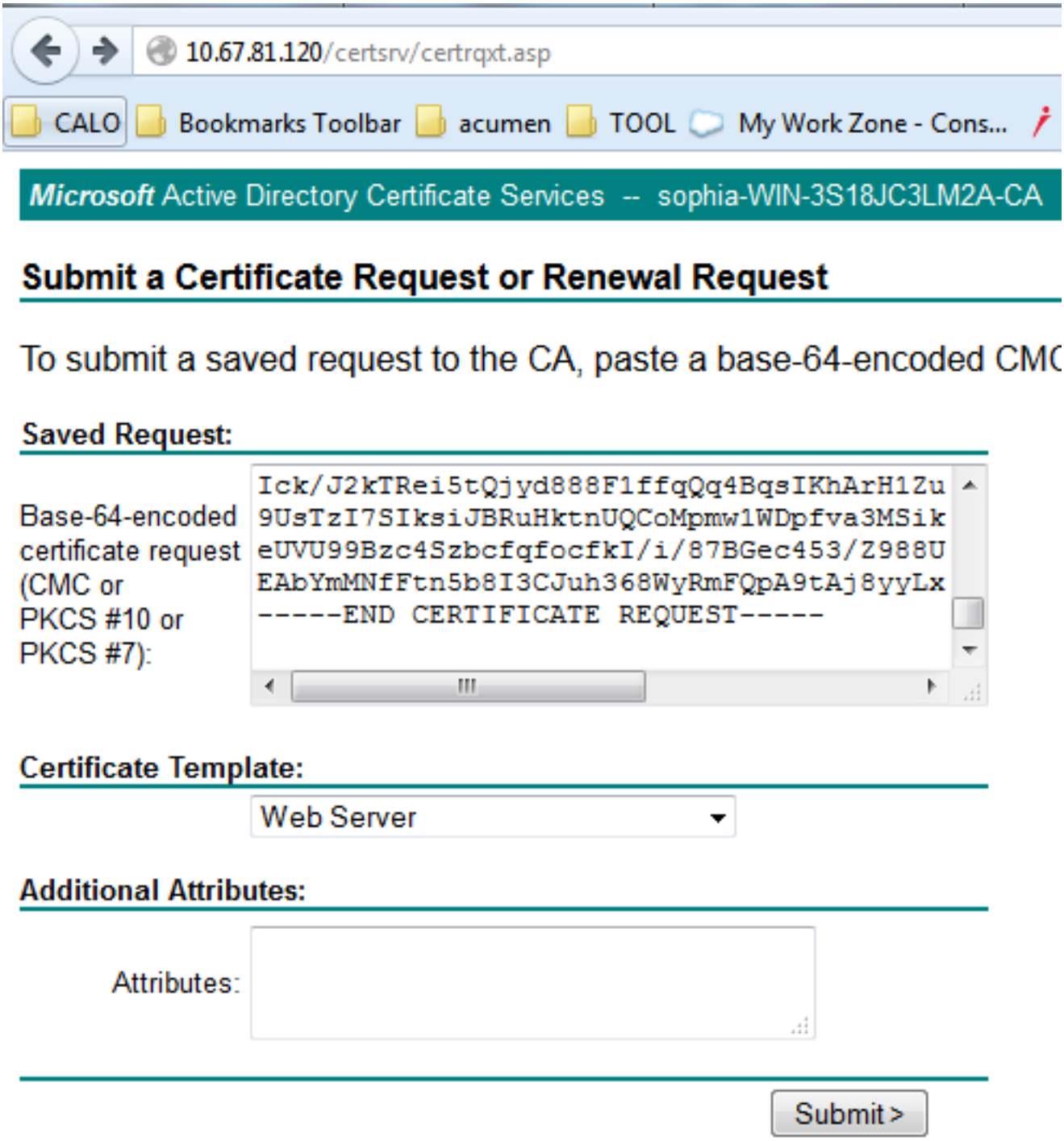
Si vous avez l'espace dans les domaines ci-dessus, l'utilisez **« »** afin de réaliser la commande suivant les indications de l'image.

```
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)?
```

Étape 2. Générez le CSR suivant les indications de l'image.

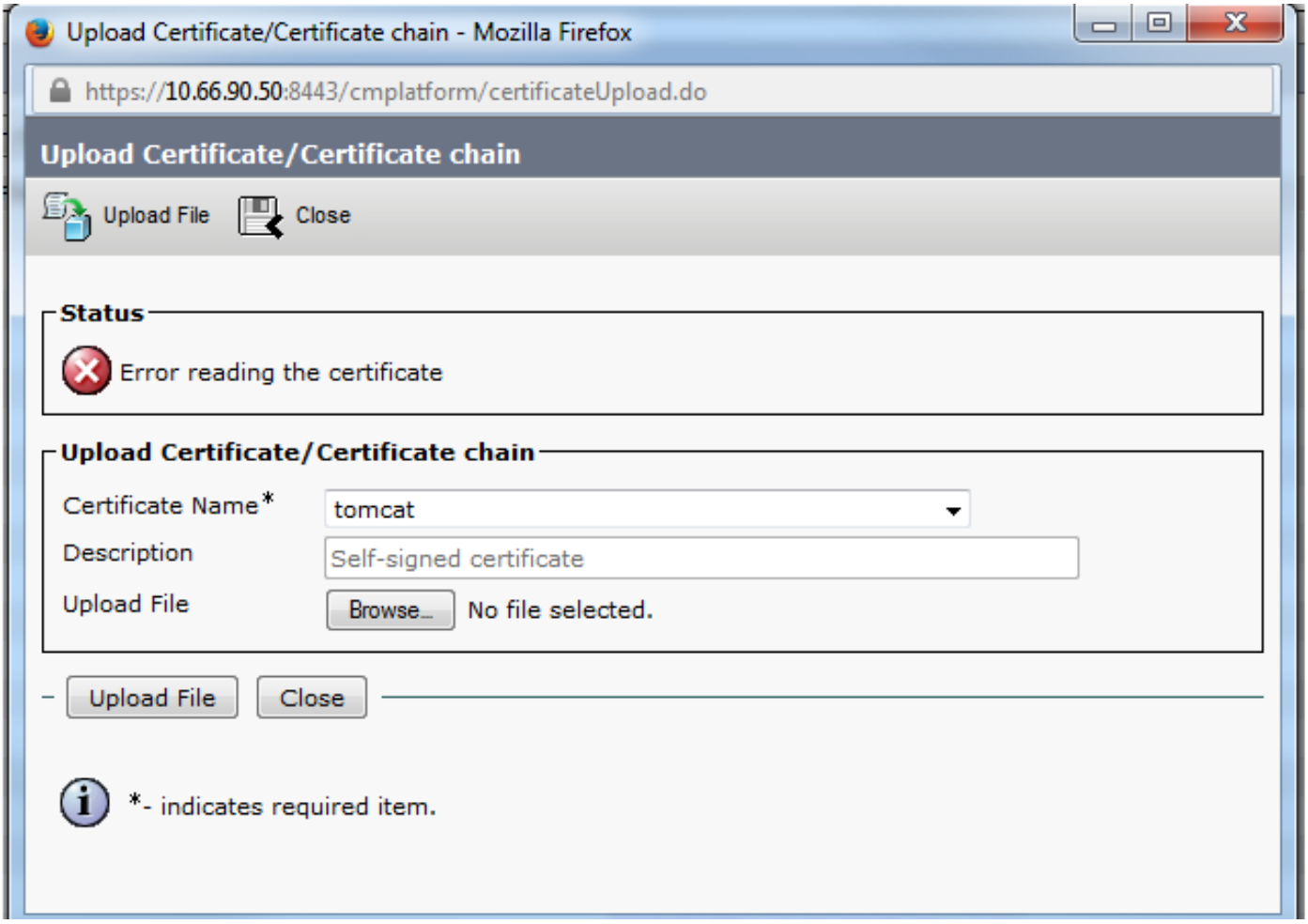


Étape 3. Téléchargez le CSR et obtenez-le a signé par le CA suivant les indications de l'image.



Étape 4. Téléchargez le certificat Ca-signé au serveur.

Une fois que le CSR est généré et le certificat est signé et si vous ne le téléchargez pas avec un message d'erreur « erreur de lecture le certificat » (suivant les indications de cette image), puis vous devez vérifier si le CSR est régénéré ou si le certificat signé lui-même est la cause de la question.



Il y a trois manières de vérifier si le CSR est régénéré ou le certificat signé lui-même est la cause de la question.

Solution 1. Commande d'OpenSSL d'utilisation dans la racine (ou le Linux)

Étape 1. Ouvrez une session à la racine et naviguez vers le répertoire suivant les indications de l'image.

```
[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]#
```

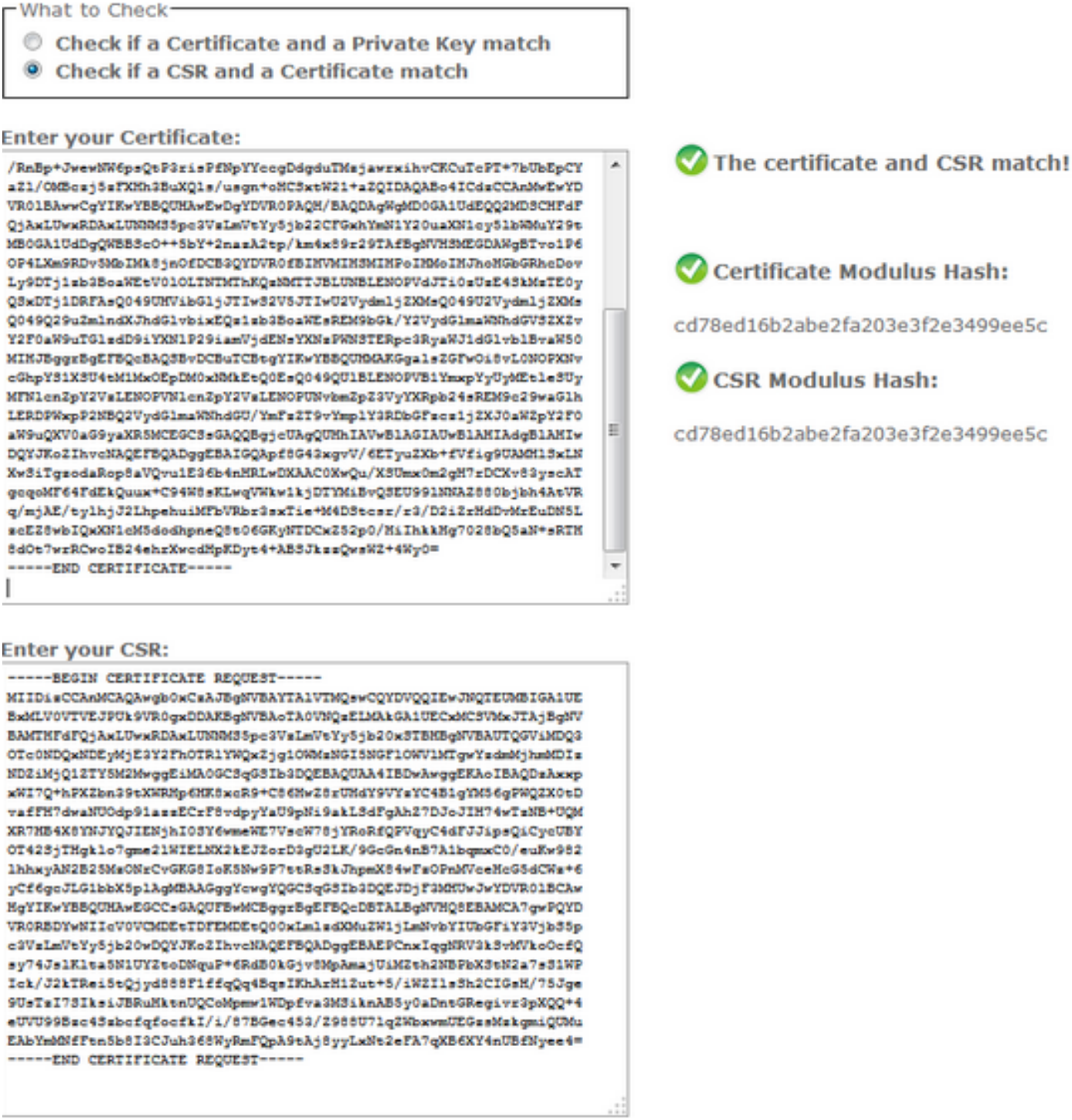
Étape 2. Copiez le certificat signé sur le même répertoire avec le FTP sécurisé (SFTP). Si vous ne pouvez pas installer un serveur de SFTP, alors le téléchargement sur le répertoire TFTP peut également obtenir le certificat sur le CUCM suivant les indications de l'image.

```
[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. Vérifiez le MD5 pour le CSR et le certificat signé suivant les indications de l'image.

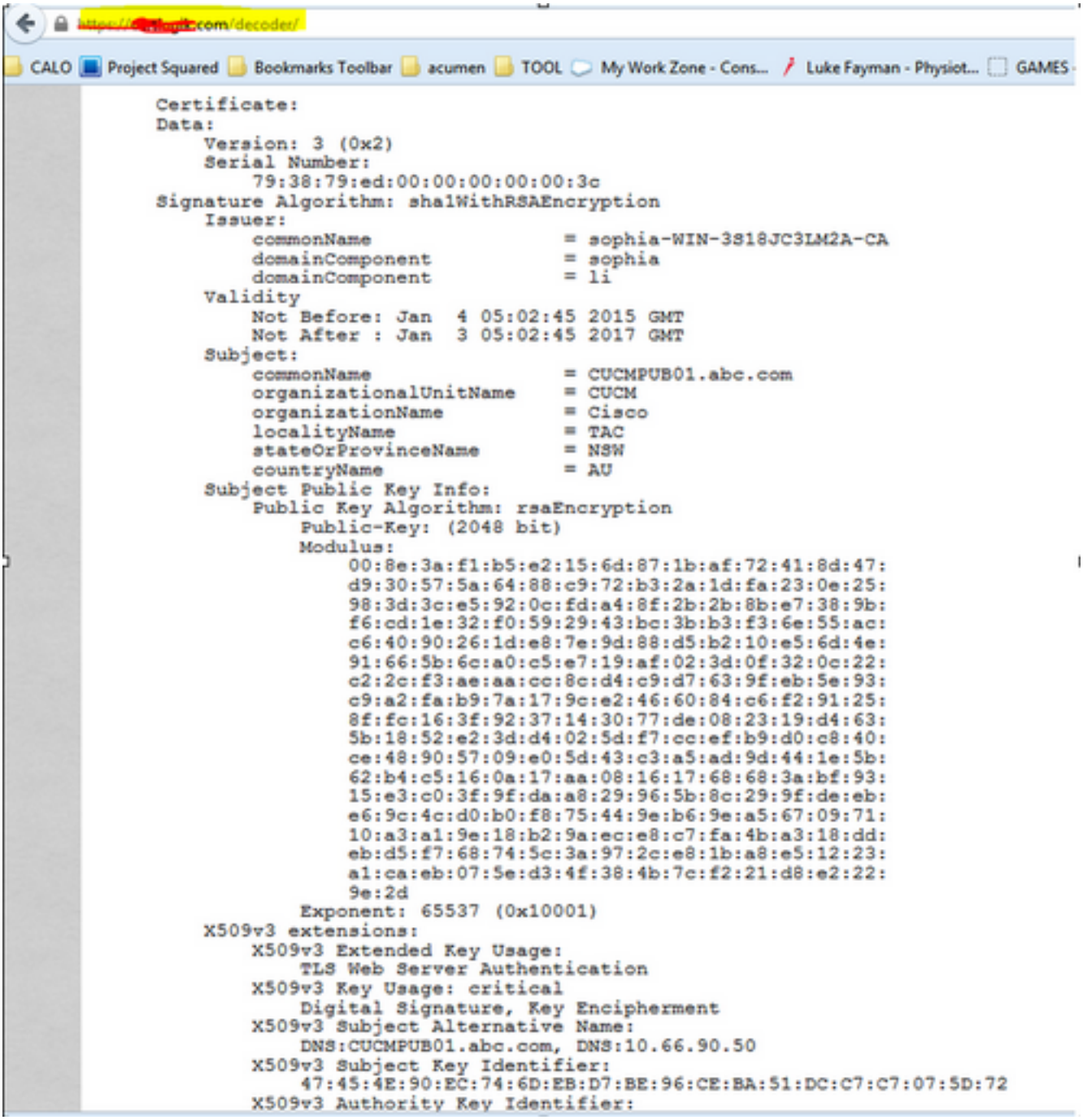
```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

Solution 2. Utilisez n'importe quelle bouveteuse de clé de certificat ssl d'Internet

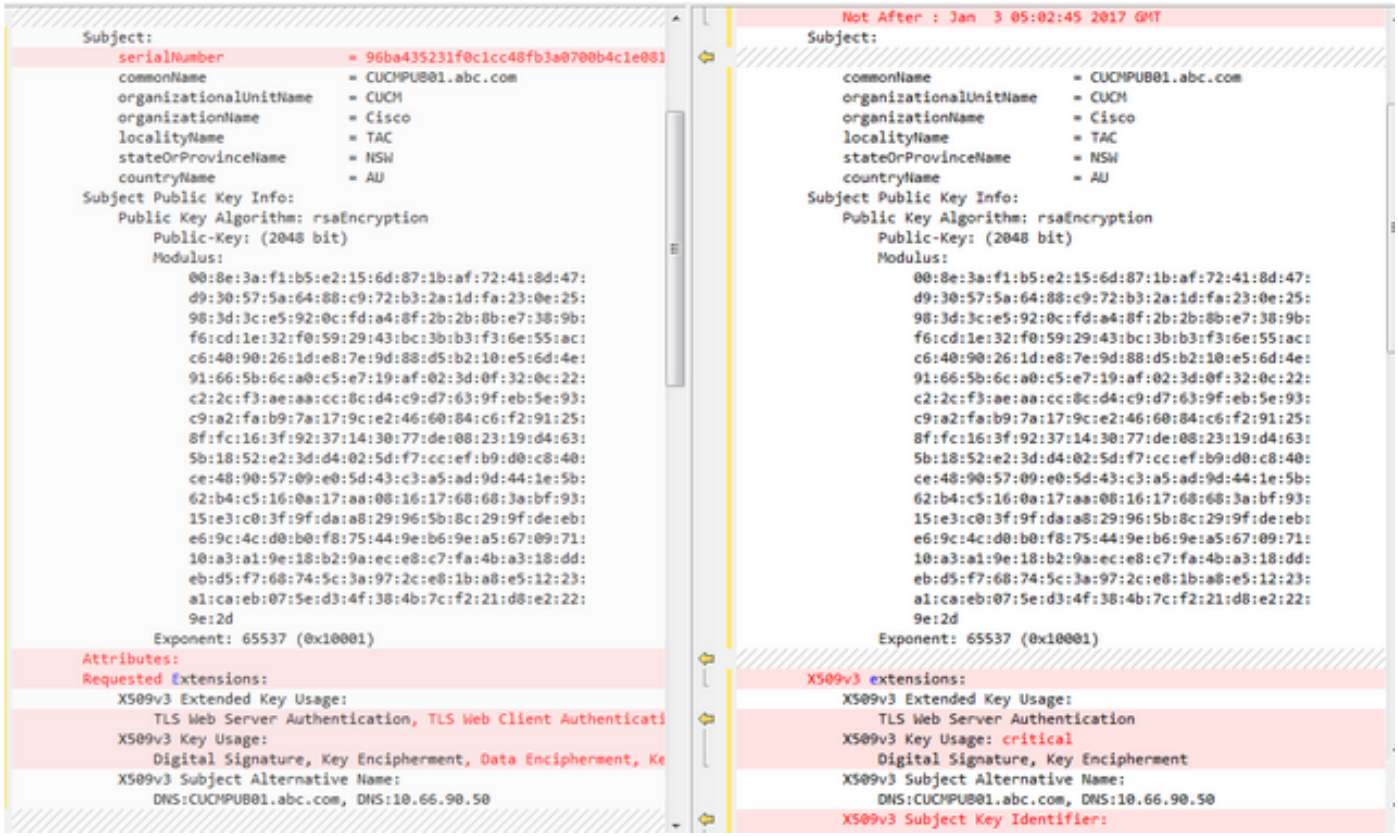


La solution 3. comparent le contenu de n'importe quel décodeur CSR d'Internet

Étape 1. Copiez les **informations détaillées de certificat de** session pour chacun suivant les indications de cette image.



Étape 2. Comparez-les dans un outil tel que Notepad++ au module d'extension de comparer suivant les indications de cette image.



```
        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:
```