Verificar a incompatibilidade de certificado e CSR para UC

Contents

Introduction

Este documento descreve como identificar se o certificado assinado pela Autoridade de Certificação (AC) corresponde à Solicitação de Assinatura de Certificado (CSR - Certificate Signing Request) existente para Cisco Unified Application Servers.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do X.509/CSR.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

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

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

Informações de Apoio

Uma solicitação de certificação consiste em um nome distinto, uma chave pública e um conjunto opcional de atributos coletivamente assinados pela entidade que solicita a certificação. As solicitações de certificação são enviadas a uma autoridade de certificação que transforma a solicitação em um certificado X.509 de chave pública. De que forma a autoridade de certificação retorna o certificado recém-assinado está fora do escopo deste documento. Uma mensagem PKCS #7 é uma possibilidade. (RFC:2986).

Gerenciamento de certificado do Cisco Communications Manager

A intenção de incluir um conjunto de atributos é dupla:

- A fim de fornecer outras informações sobre uma determinada entidade, ou uma senha de desafio pela qual a entidade pode posteriormente solicitar a revogação de certificado.
- A fim de fornecer atributos para inclusão em certificados X.509. Os atuais servidores de Unified Communications (UC) não suportam uma senha de desafio.

Os servidores Cisco UC atuais exigem estes atributos em um CSR, como mostrado nesta tabela:

Informações	Descrição
órgão	unidade organizacional
orgname	nome da organização
localidade	local da organização
estado	estado de organização
país	o código do país não pode ser alterado
nome de host alternativo	nome de host alternativo

Problema

Quando você oferece suporte a UC, você pode encontrar muitos casos em que o certificado assinado da CA não pode ser carregado nos servidores UC. Nem sempre é possível identificar o que ocorreu no momento da criação do certificado assinado, pois você não é a pessoa que usou o CSR para criar o certificado assinado. Na maioria dos cenários, assinar novamente um novo certificado leva mais de 24 horas. Os servidores UC, como o CUCM, não têm registro/rastreamento detalhado para ajudar a identificar por que o carregamento do certificado falha, mas apenas fornecem uma mensagem de erro. A intenção deste artigo é restringir o problema, seja um servidor UC ou um problema CA.

Prática geral para certificados assinados por CA no CUCM

O CUCM suporta a integração com CAs de terceiros com o uso de um mecanismo PKCS#10 CSR acessível na GUI do Cisco Unified Communications Operating System Certificate Manager. Os clientes que atualmente usam CAs de terceiros devem usar o mecanismo CSR para emitir certificados para Cisco CallManager, CAPF, IPSec e Tomcat.

Etapa 1. Altere o Identificador antes de gerar o CSR.

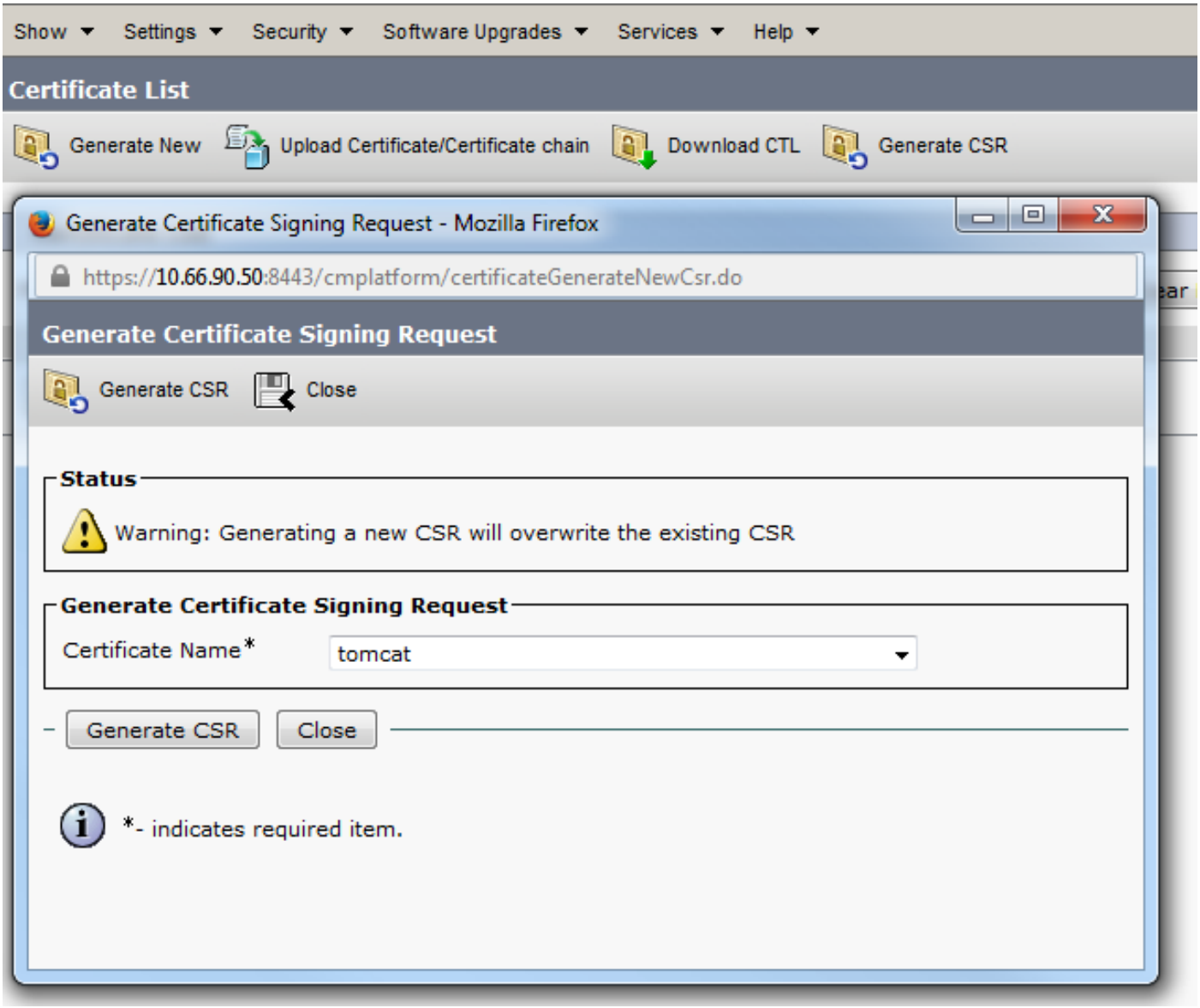
A identidade do servidor CUCM para gerar um CSR pode ser modificada com o uso do comando **set web-security** como mostrado nesta imagem.

```
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
```

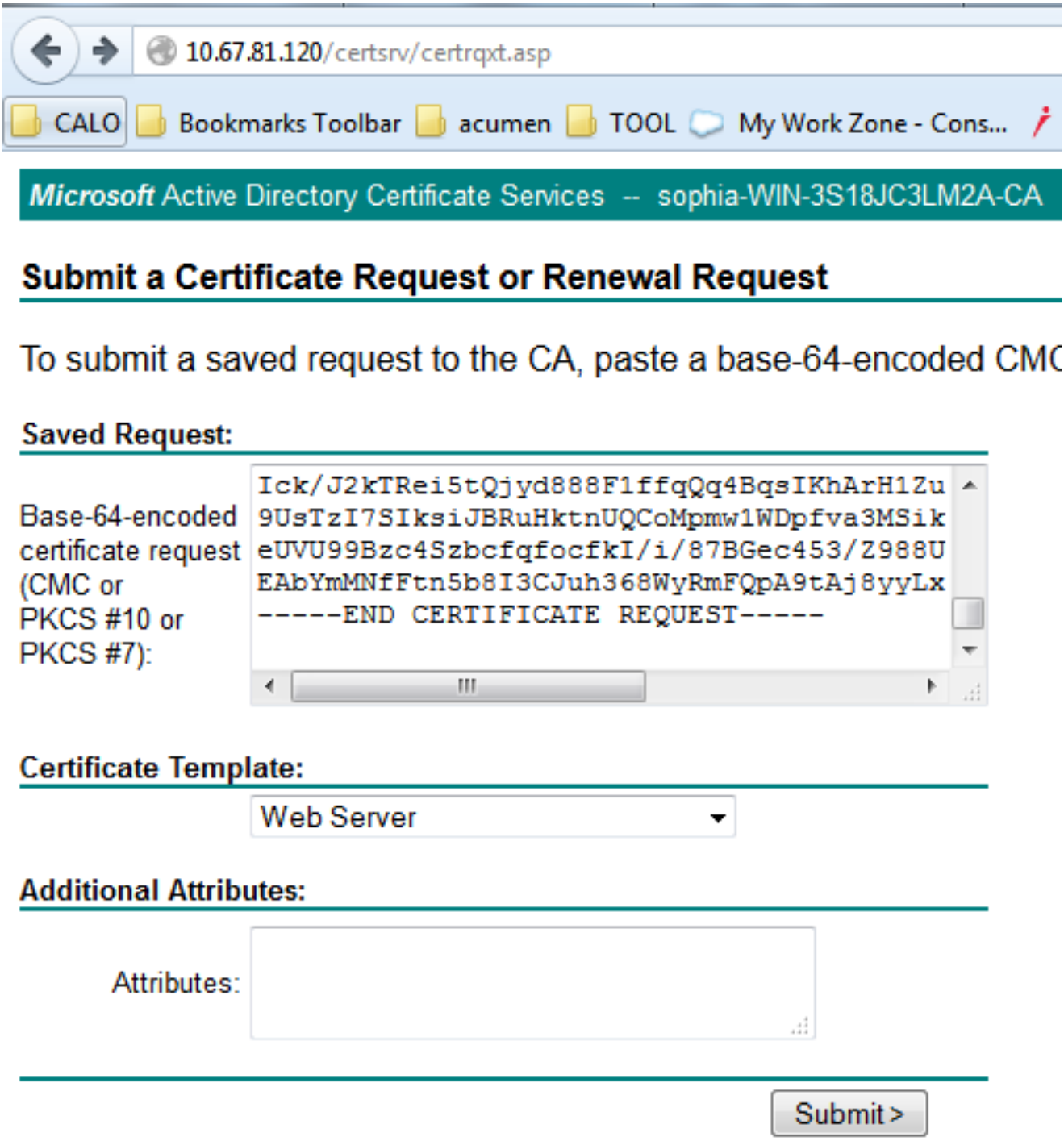
Se você tiver espaço nos campos acima, use **""** para obter o comando como mostrado na imagem.

```
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)?
```

Etapa 2. Gere CSR conforme mostrado na imagem.

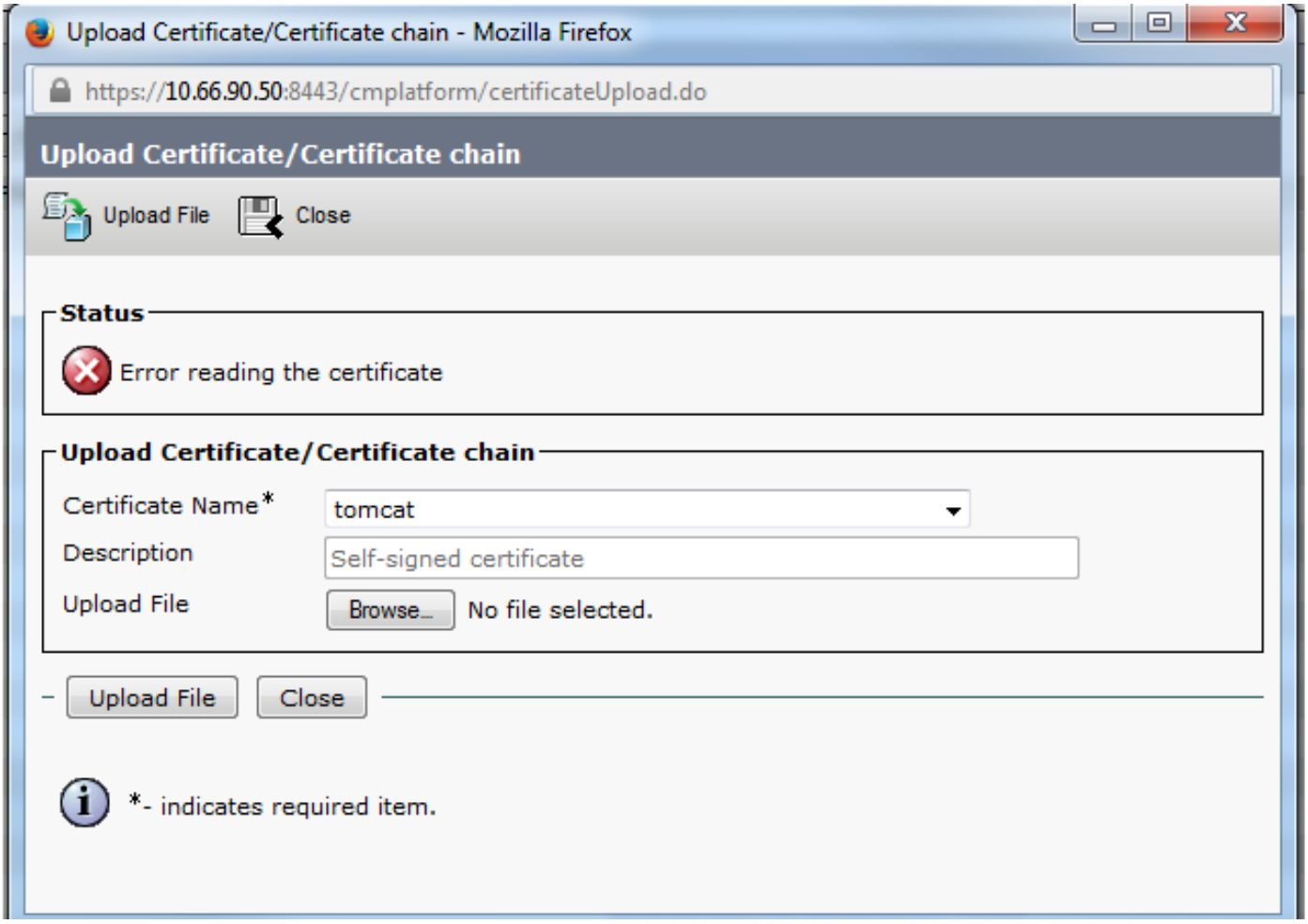


Etapa 3. Baixe o CSR e obtenha-o assinado pela CA, como mostrado na imagem.



Etapa 4. Carregue o certificado assinado pela AC no servidor.

Quando o CSR é gerado e o certificado é assinado e você não consegue carregá-lo com uma mensagem de erro "Error reading the certificate" (como mostrado nesta imagem), você precisa verificar se o CSR é regenerado ou se o certificado assinado em si é a causa do problema.



Há três maneiras de verificar se o CSR está regenerado ou se o certificado assinado em si é a causa do problema.

Solução 1. Usar o comando OpenSSL na raiz (ou linux)

Etapa 1. Faça login na raiz e navegue até a pasta como mostrado na imagem.

```
[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]#
```

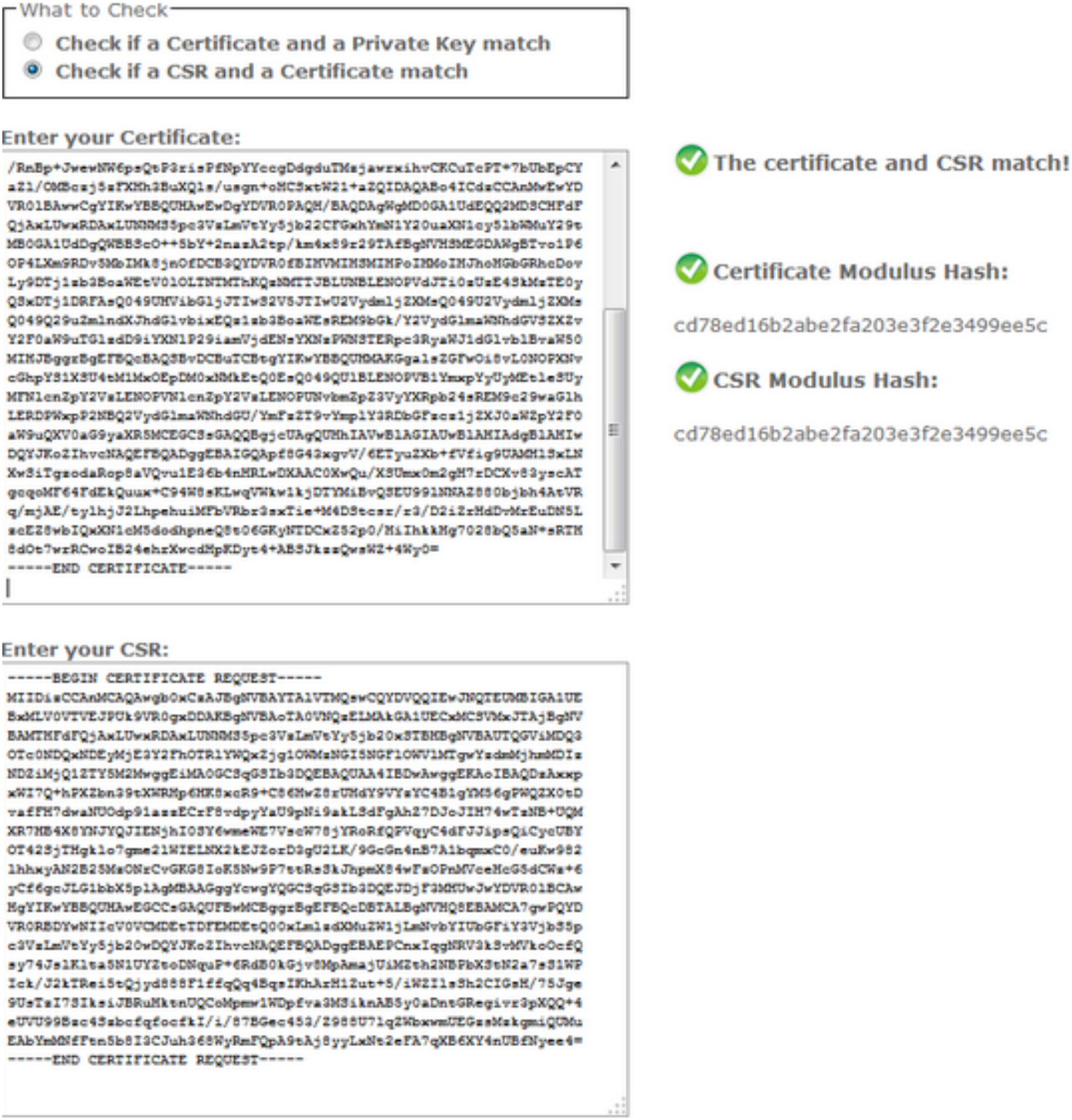
Etapa 2. Copie o certificado assinado para a mesma pasta com FTP seguro (SFTP). Se você não puder configurar um servidor SFTP, o carregamento na pasta TFTP também poderá obter o certificado no CUCM como mostrado na imagem.

```
[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. Verifique o MD5 do CSR e o certificado assinado conforme mostrado na imagem.

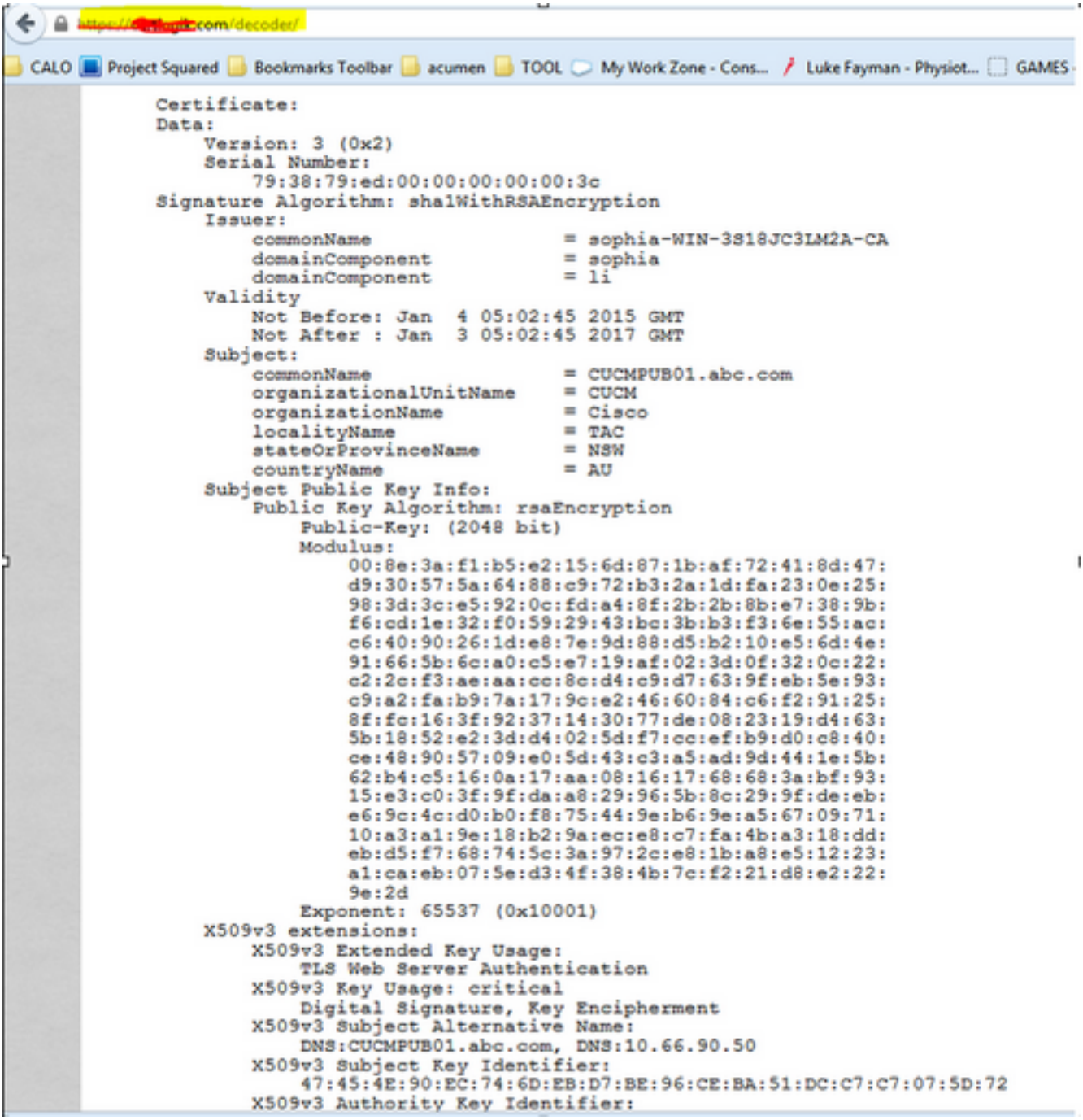
```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

Solução 2. Usar qualquer correspondência de chave de certificado SSL da Internet

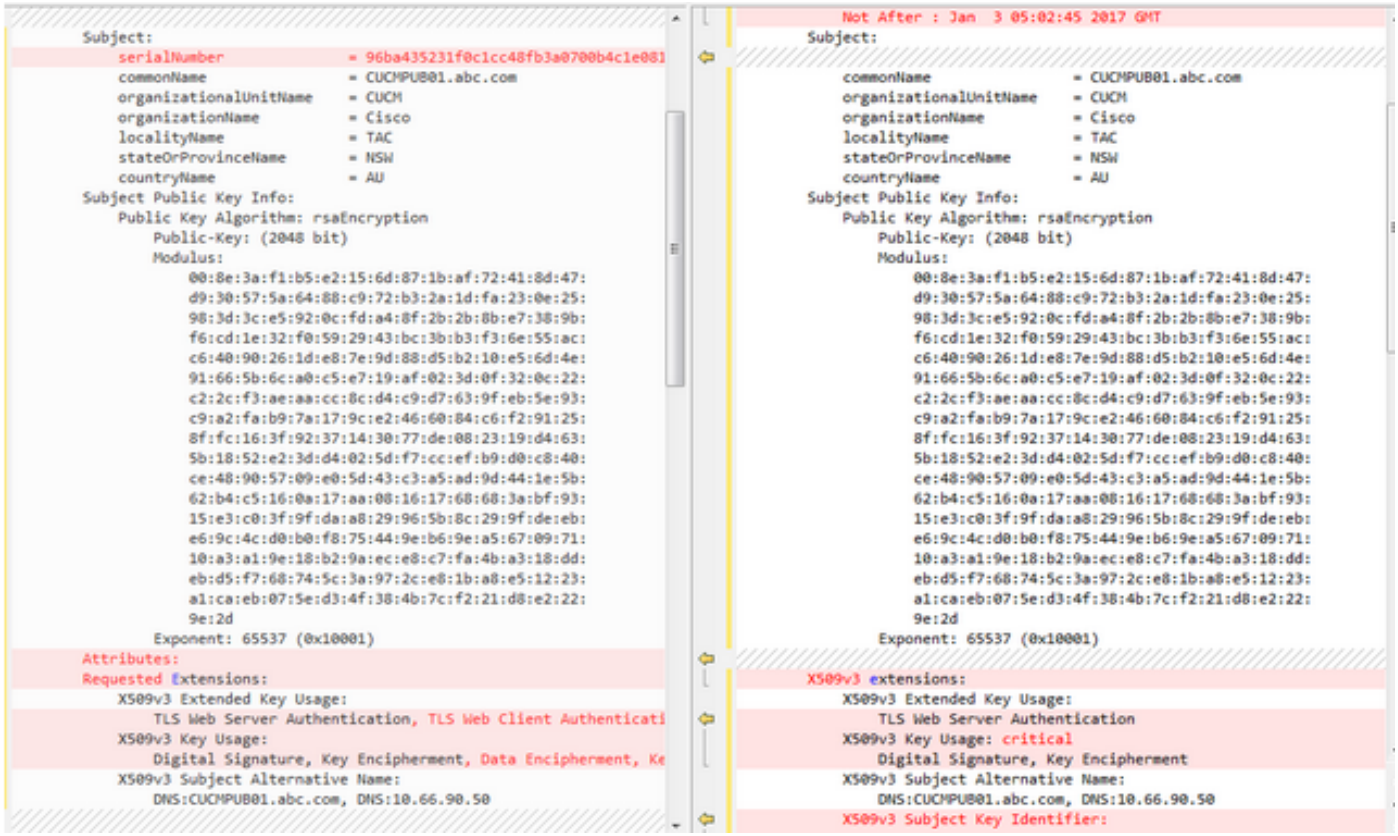


Solução 3. Comparar conteúdo de qualquer decodificador CSR da Internet

Etapa 1. Copie as **Informações Detalhadas do Certificado** da sessão para cada uma, conforme mostrado nesta imagem.



Etapa 2. Compare-os em uma ferramenta como o Notepad++ com o plug-in Comparar como mostrado nesta imagem.



```
        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:
```