Como verificar o CSR e a má combinação do certificado para o UC

Índice

Introdução

Este documento descreve como identificar se o certificado assinado do Certificate Authority (CA) combina a requisição de assinatura do certificado existente (CSR) para Cisco unificou serveres de aplicativo.

Pré-requisitos

Requisitos

Reccommends de Cisco que você tem o conhecimento de X.509/CSR.

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Um pedido da certificação consiste em um nome destacado, em uma chave pública, e em um grupo opcional de atributos, assinado coletivamente pela entidade que pede a certificação. Os pedidos da certificação são enviados a uma autoridade de certificação que transforme o pedido em um certificado da chave pública X.509. Que formulário a autoridade de certificação retorna

recentemente no certificado assinado é fora do âmbito deste documento. Uma mensagem PKCS #7 é um possibility.(RFC:2986)

Gerenciamento certificado do Gerenciador de Comunicações de Cisco

A intenção de incluir um grupo de atributos é dupla:

- Para fornecer a outra informação sobre uma entidade dada, ou uma senha do desafio por que a entidade pode mais tarde pedir a revogação de certificado.
- Para fornecer atributos para a inclusão nos Certificados X.509. Os server atuais UC não apoiam uma senha do desafio.

Os server atuais de Cisco UC exigem estes atributos em um CSR segundo as indicações desta tabela:

Informações	Descrição
orgunit	unidade organizacional
orgname	nome de organização
localidade	lugar da organização
estado	estado de organização
país	o código de país não pode ser mudado
alternatehostname	nome de host alternativo

Produtos Relacionados

Este documento pode igualmente ser usado com estes versão de hardware e software:

- Gerente das comunicações unificadas de Cisco (CUCM)
- Cisco unificou IM e presença
- Cisco unificou a conexão de unidade
- CUIS
- Cisco Meidasence
- Cisco Unified Contact Center Express (UCCX)

Problema

Em apoiar o UC, você encontra muitos casos onde o certificado assinado de CA não transfere arquivos pela rede nos server UC. Você não pode sempre identificar o que ocorreu durante a criação do certificado assinado, desde que você não é a pessoa que usou o CSR para criar o certificado assinado. Na maioria de encenações, re-assinar um certificado novo toma mais de 24 horas. Os server UC tais como CUCM não detalharam o log/traço para ajudar em identificar porque a transferência de arquivo pela rede do certificado falha mas apenas dão um Mensagem de Erro. Este artigo é pretendido ajudar no redução abaixo da edição, se é um server UC ou uma edição de CA.

Prática geral para certificados assinados CA em CUCM

CUCM apoia a integração com os CA da terceira usando um mecanismo PKCS#10 CSR que seja acessível no gerenciador certificado GUI do sistema operacional das comunicações unificadas de Cisco. Os clientes, que usam atualmente CA da terceira devem usar o mecanismo CSR para emitir Certificados para o CallManager da Cisco, o CAPF, o IPsec, e o Tomcat.

Etapa 1. Mude a identificação antes de gerar o CSR

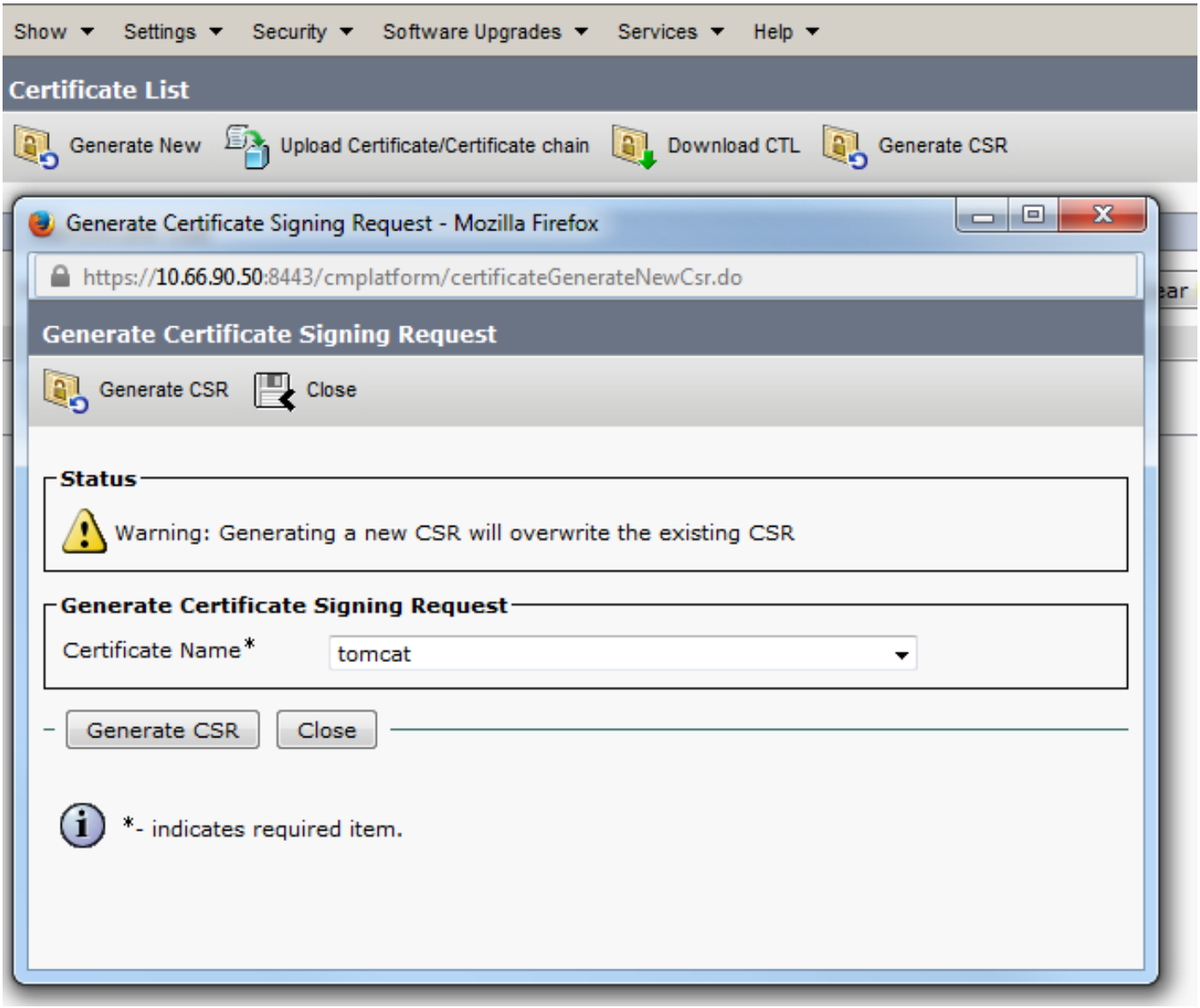
A identidade do server CUCM para gerar um CSR pode ser alterada usando a Web-**Segurança do** comando set segundo as indicações desta imagem.

```
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
```

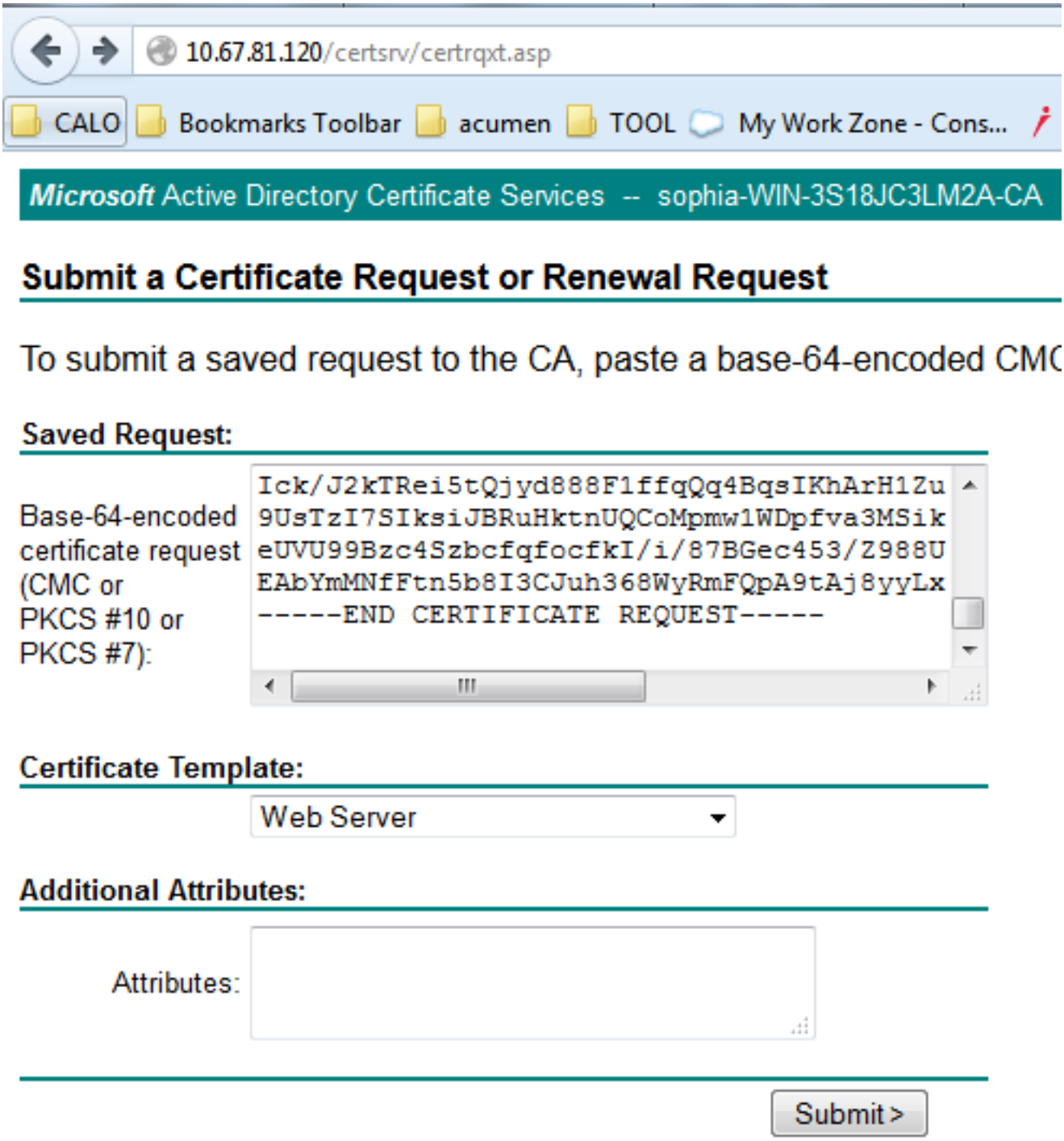
Se você tem o espaço nos campos acima, use por favor?? para conseguir o comando como:

```
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. Gerencia o CSR.

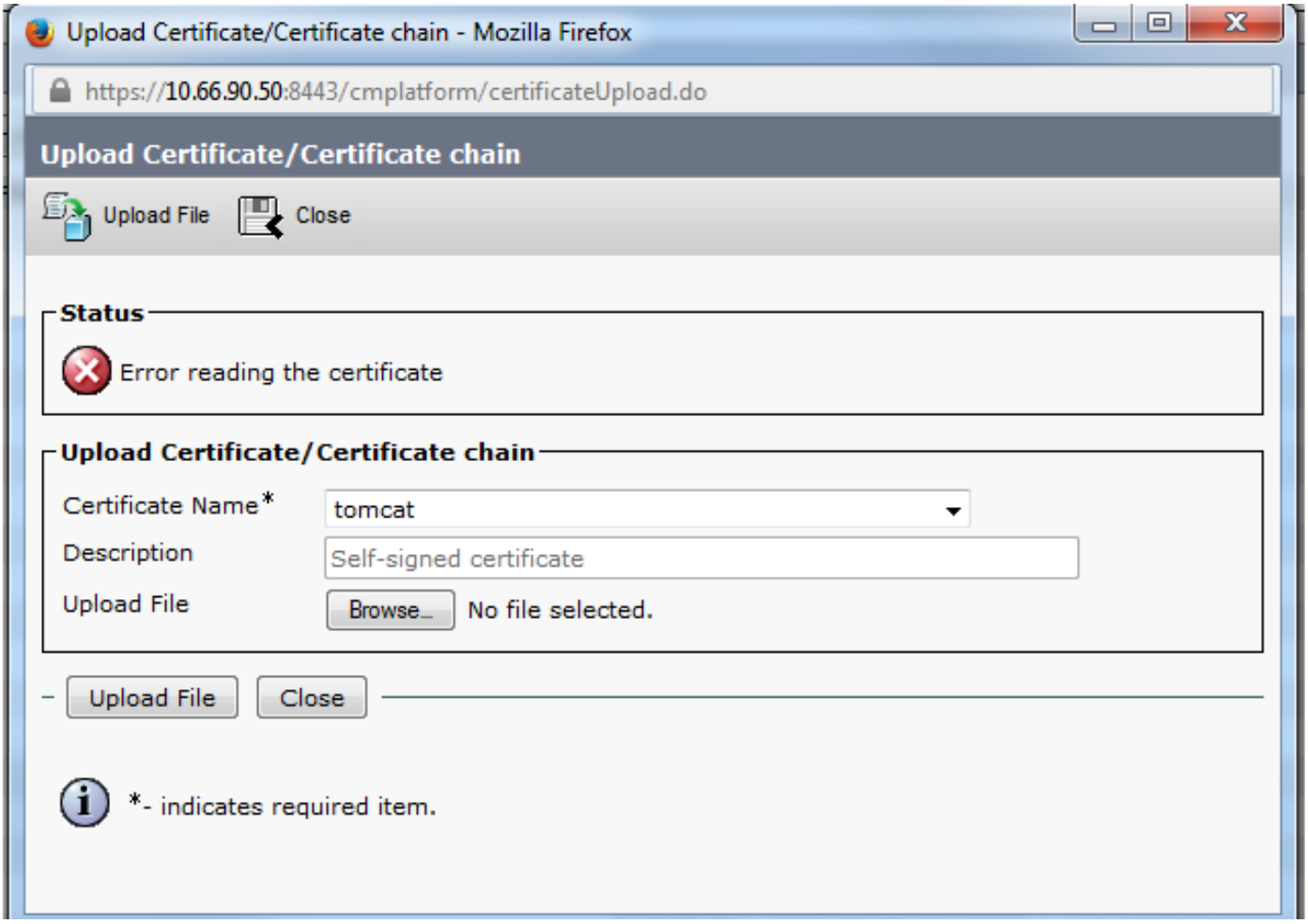


Etapa 3. Transfira o CSR e obtenha-o assinado por CA.



Etapa 4. Transfira arquivos pela rede o certificado assinado CA ao server.

Uma vez que o CSR está gerado e o certificado está assinado, se você não o transfere arquivos pela rede com uma **leitura de erro do** Mensagem de Erro o **certificado** (segundo as indicações desta imagem), a seguir você precisa de verificar se o CSR esteja regenerado ou se o certificado assinado próprio é a causa da edição.



Há três maneiras de verificar se o CSR esteja regenerado ou o certificado assinado próprio seja a causa da edição.

Solução 1. Use o comando do OpenSSL na raiz (ou no linux)

1. Entre à raiz e navegue ao dobrador.

```
[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]#
```

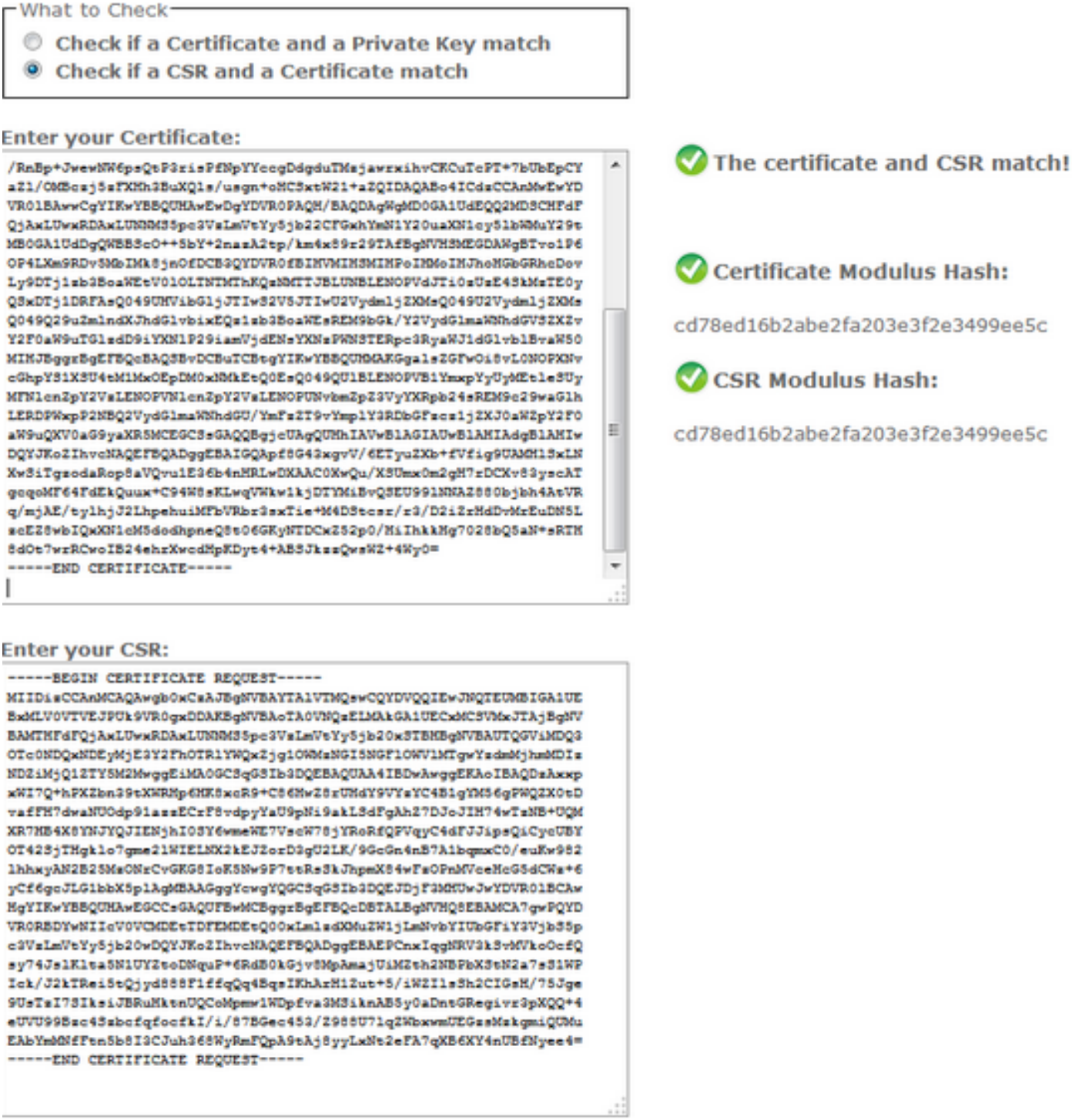
2. Copie o certificado assinado ao mesmo dobrador usando FTP seguro (SFTP). Se você é incapaz de estabelecer um servidor SFTP, a seguir transferi-lo arquivos pela rede ao dobrador TFTP igualmente obtém o certificado no CUCM.

```
[root@CCM105PUB keys]# sftpt cisco@10.66.90.19
bash: sftpt: 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 para ver se há o CSR e o certificado assinado.

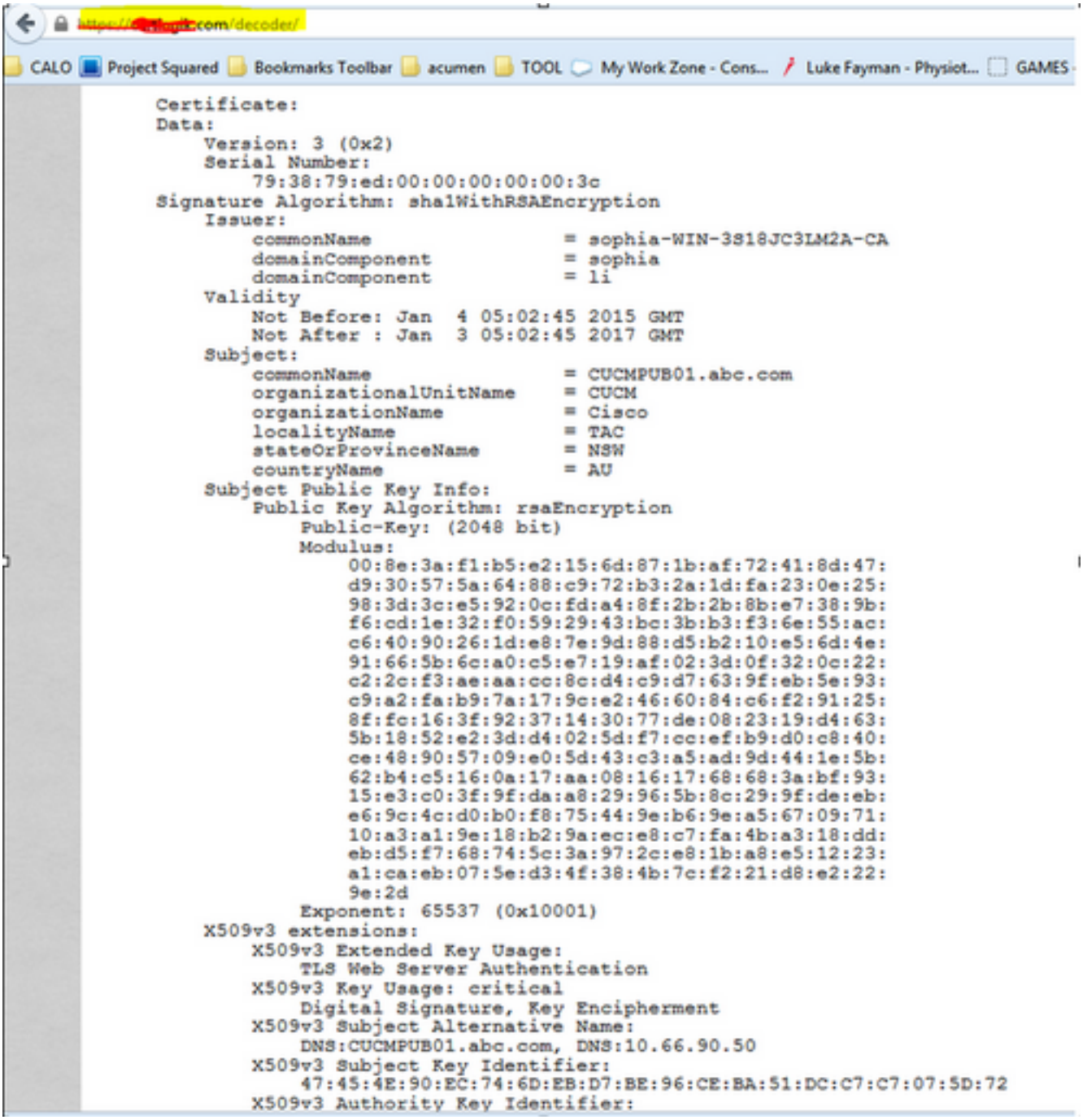
```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

Solução 2. Use todo o matcher da chave do certificado SSL do Internet

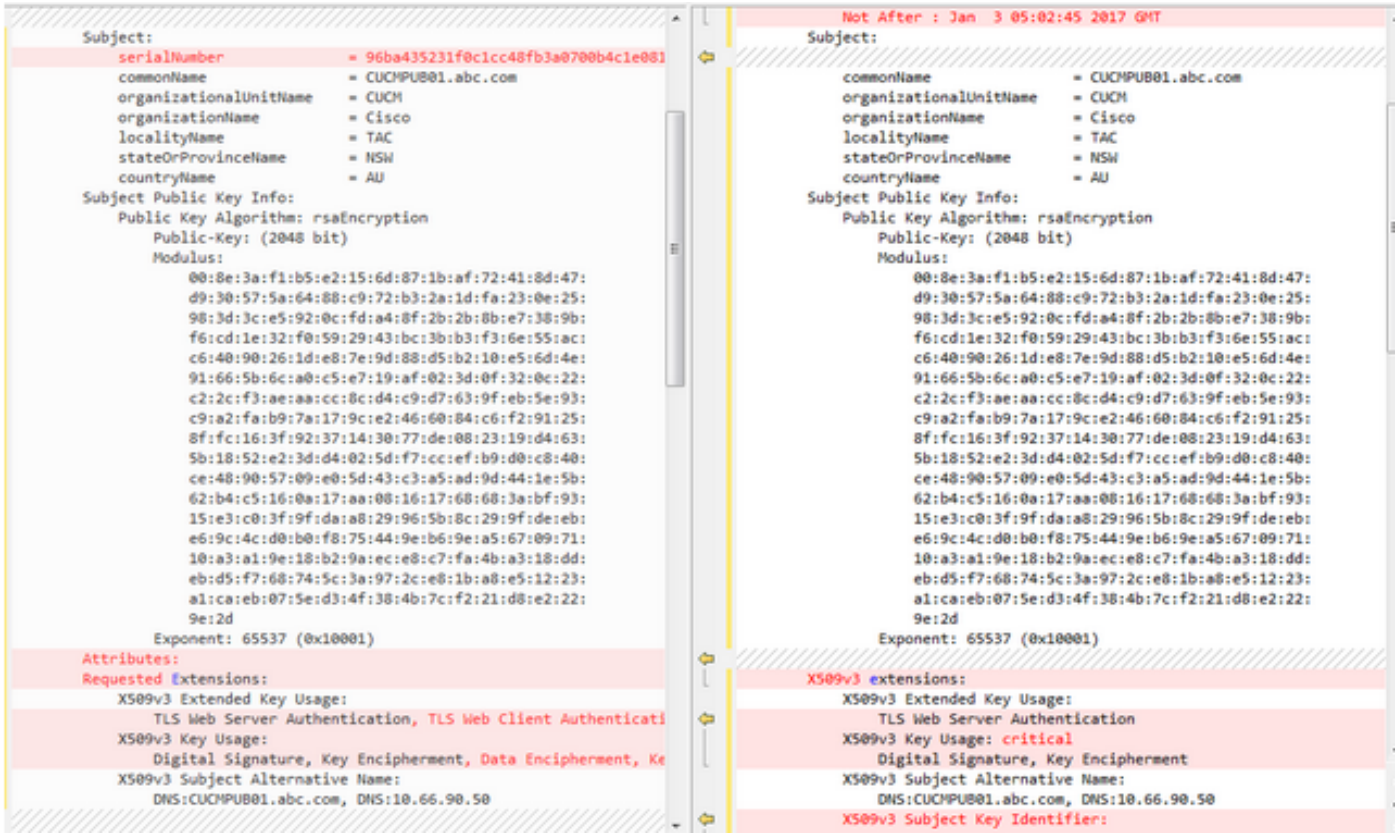


A solução 3. compara o índice de todo o decodificador CSR do Internet

1. Copie a **informação detalhada do certificado da** sessão para cada um segundo as indicações desta imagem.



2. Compare-os em uma ferramenta tal como Notepad++ com a comparação de encaixe segundo as indicações desta 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:
```