验证CSR和认证不匹配UC的

目录

简介

本文描述如何识别Certificate Authority (CA)签名的证书是否匹配现有的证书署名请求(CSR) Cisco Unified应用服务器的。

先决条件

要求

Cisco建议您有X.509/CSR知识。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

本文可能也与这些一起使用硬件和软件版本：

- Cisco Unified通信管理器(CUCM)
- Cisco Unified IM和存在
- Cisco Unified Unity Connection
- CUIS
- Cisco Meidasence
- Cisco Unified Contact Center Express (UCCX)

背景信息

证明请求包括一个不同的名字、一个公共密钥和请求证明实体共同签字的可选的套属性。证明请求被发送到变换请求成X.509公钥证明的认证机构。在什么表认证机构返回在本文的范围之外，最近签名的证书是。 PKCS-7消息是一possibility.(RFC:2986)。

Cisco通信管理器证书管理

目的包括一套属性是二倍的：

- 为了提供关于一个特定实体的其他信息或者实体能以后请求认证吊销的质询密码。
- 为了为在X.509证书的包括提供属性。当前统一的通信(UC)服务器不支持质询密码。

如此表所显示，当前Cisco UC服务器要求在CSR的这些属性：

信息	说明
orgunit	组织单位
orgname	组织名字
现场	组织的位置
状态	组织状态
国家	不可能更改国家代码
alternatehostname	备选主机名

问题

当您支持UC时，您能遇到CA签名的证书在UC服务器不能被加载的很多案件。您不能总是识别什么在签名的证书的创建时发生了，因为您不是使用CSR为了创建签名的证书的人。在多种情况下，重签新证书耗费超过24小时。UC服务器例如CUCM没有详细日志/跟踪为了协助解决识别认证加载为什么发生故障，但是他们给予一个错误信息。此条款的目的将缩小问题，它是否是UC服务器或CA问题。

CA签发的证书的通例在CUCM

CUCM支持与第三方CAs的集成与是可访问的在Cisco Unified通信操作系统的认证管理器GUI的使用PKCS-10 CSR机制。用户，当前使用第三方CAs必须使用CSR机制为了发行Cisco CallManager、CAPF、IPSec和Tomcat的证书。

步骤1.，在您生成CSR前，请更改识别。

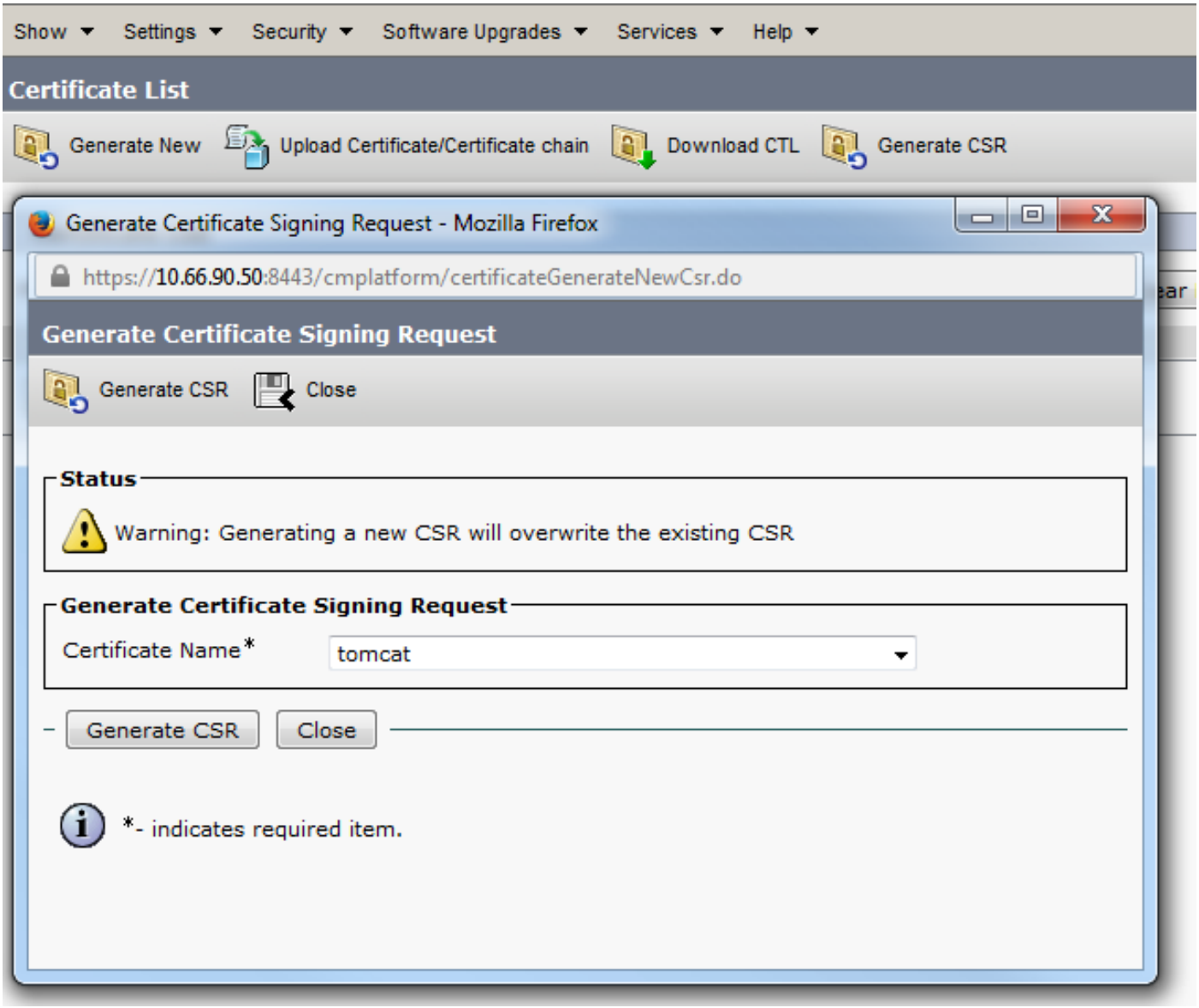
如此镜像所显示， CUCM服务器的身份为了生成CSR可以修改与使用set命令Web**安全**。

```
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
```

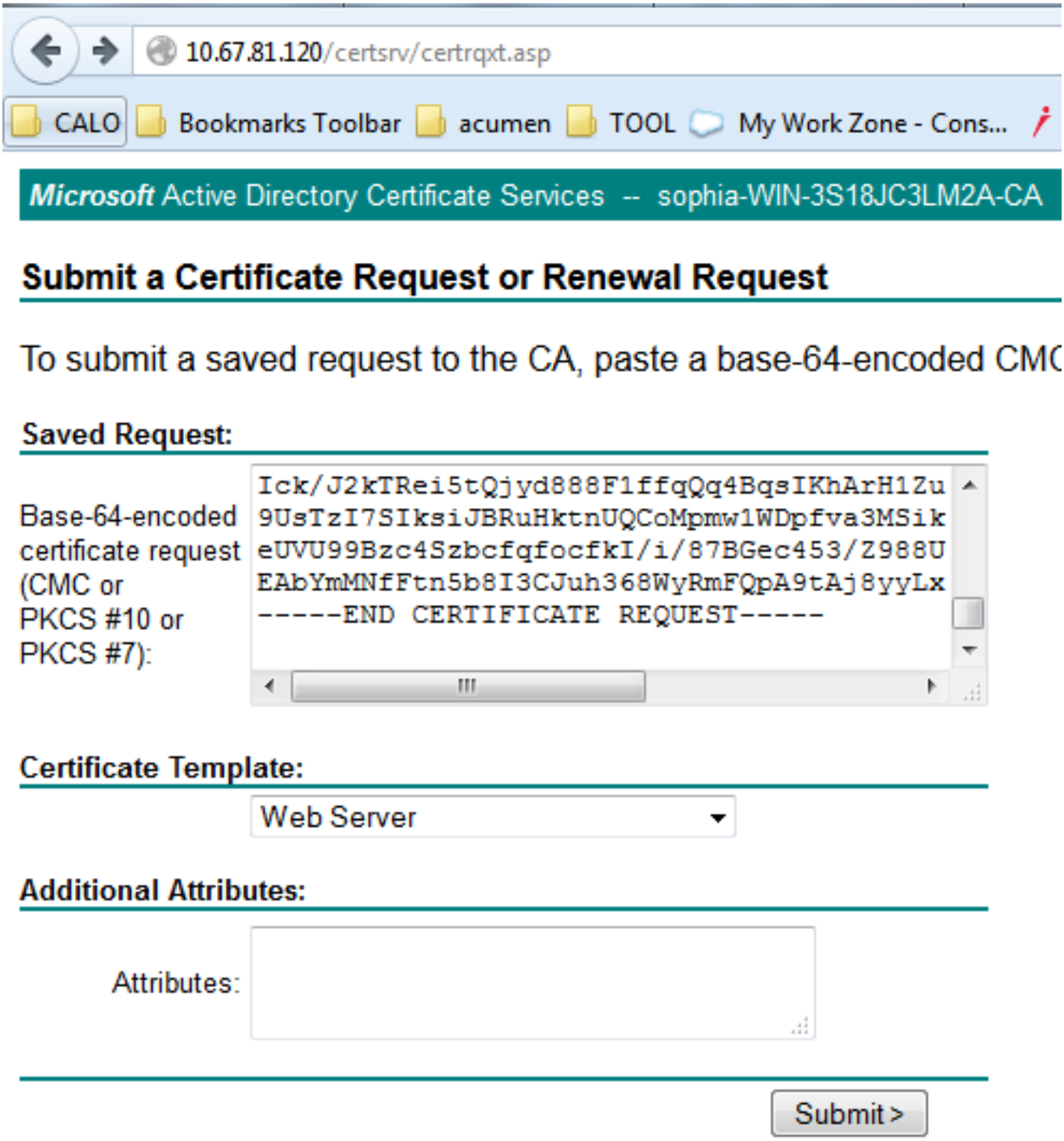
如果有空间在上述字段，如镜像所显示，请使用“”为了达到命令。

```
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)?
```

步骤2.如镜像所显示，生成CSR。

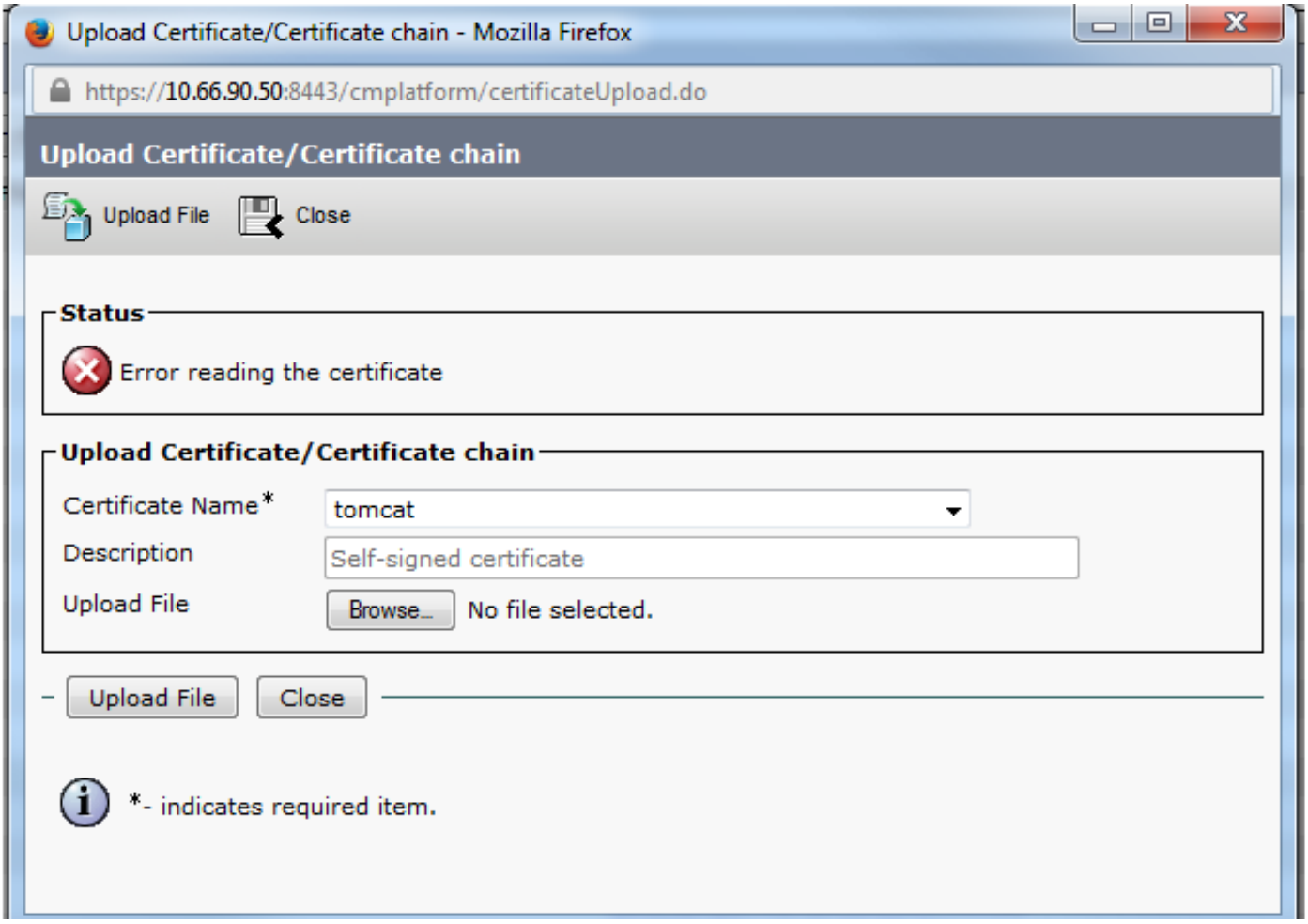


步骤3.下载CSR并且获得它签字由CA如镜像所显示。



步骤4.加载CA签发的证书到服务器。

一旦CSR生成，并且认证签字，并且，如果不能加载它与错误信息“错误读认证的” (如此镜像所显示)，然后您需要证实CSR是否被重新生成或签名的证书是否是问题的原因。



有三种方式证实CSR是否被重新生成或签名的证书是问题的原因。

解决方案1。请使用Openssl ln命令根(或Linux)

步骤1.如镜像所显示，登陆对根并且连接到文件夹。

```
[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]#
```

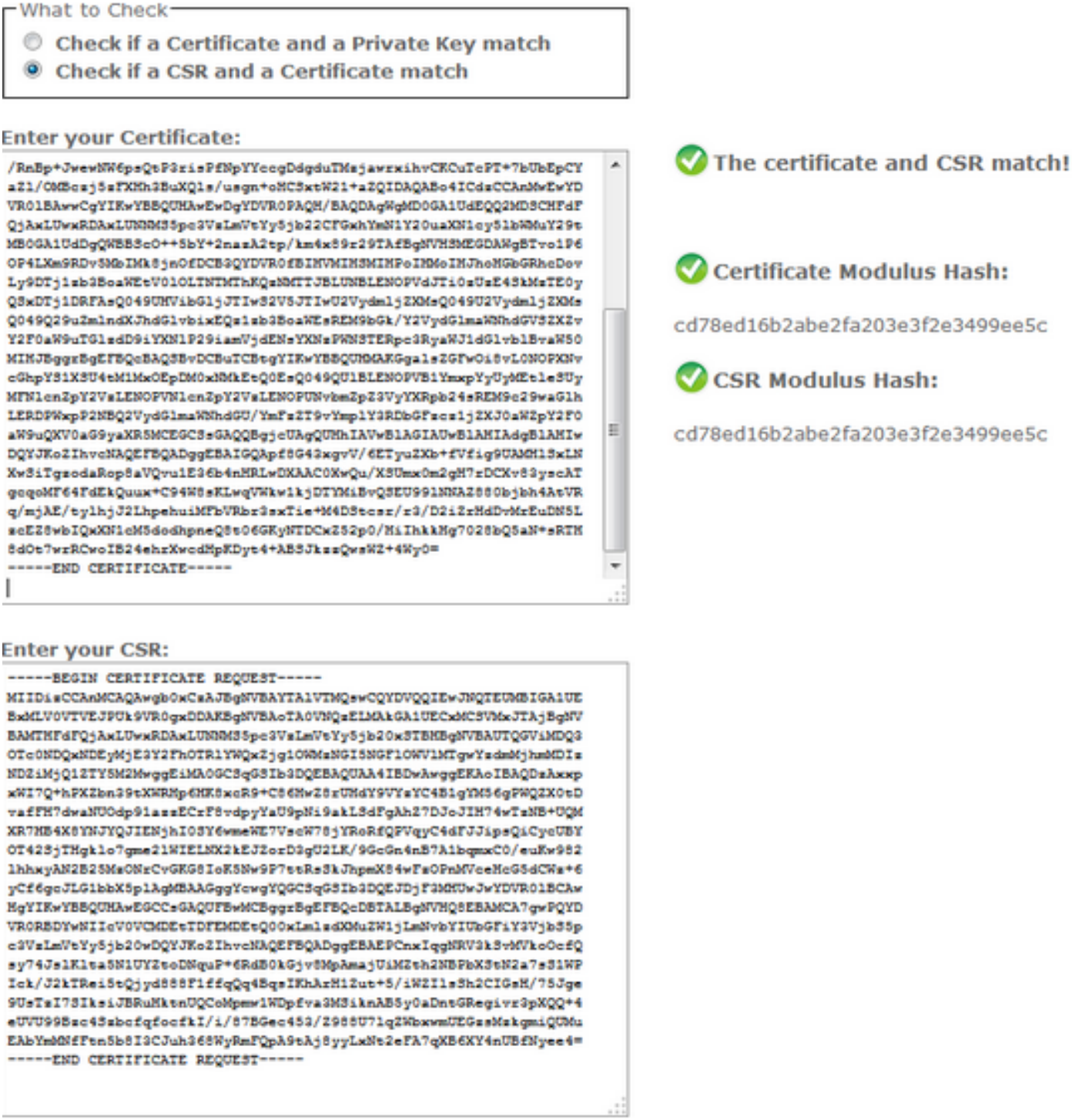
步骤2.复制签名的证书到有安全的FTP的(SFTP)同一个文件夹。如果无法设置SFTP服务器，如镜像所显示，则在TFTP文件夹的加载能也获得在CUCM上的认证。

```
[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. 如镜像所显示，检查MD5 CSR和签名的证书。

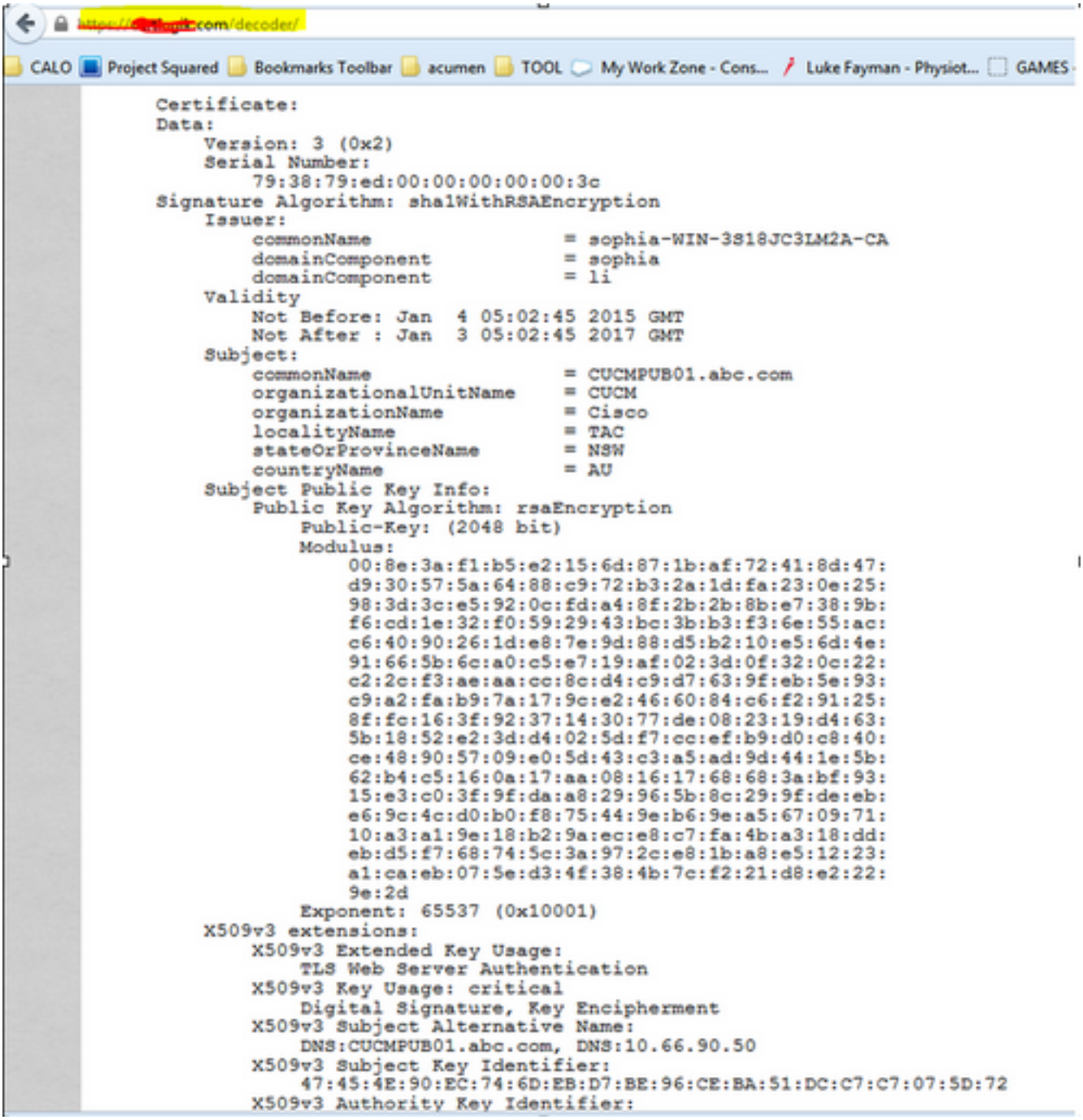
```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

解决方案2。请使用从互联网的所有SSL认证键分类员

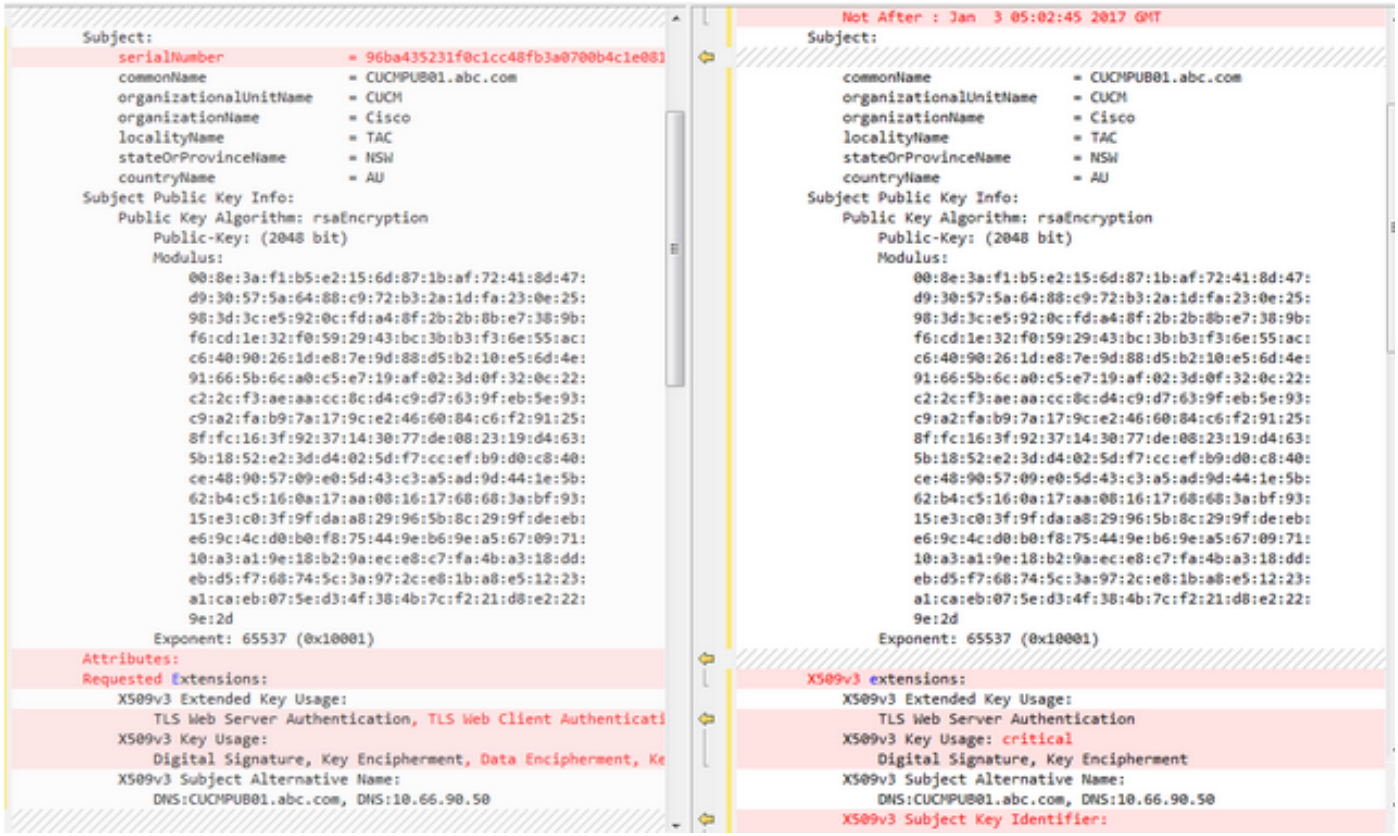


解决方案3.比较从所有CSR译码器的内容从互联网

步骤1.如此镜像所显示，复制其中每一会话**认证详细信息**。



步骤2.他们在一个工具例如Notepad++与比较比较插件如此镜像所显示。



```
        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:
```