UC에 대한 CSR 및 인증서 불일치 확인

목차

소개

이 문서에서는 CA(Certificate Authority) 서명 인증서가 Cisco Unified Application Server의 기존 CSR(Certificate Signing Request)과 일치하는지 여부를 식별하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

X.509/CSR에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 문서는 다음과 같은 하드웨어 및 소프트웨어 버전과 함께 사용할 수도 있습니다.

- Cisco CUCM(Unified Communications Manager)
- Cisco Unified IM and Presence
- Cisco Unified Unity Connection
- CUIS
- Cisco 환경
- Cisco UCCX(Unified Contact Center Express)

배경 정보

인증 요청은 인증을 요청하는 엔티티에서 총서명하는 고유 이름, 공개 키 및 선택적 특성 집합으로 구성됩니다.인증 요청은 요청을 X.509 공개 키 인증서로 변환하는 인증 기관에 전송됩니다.인증 기관에서 새로 서명된 인증서를 반환하는 형식은 이 문서의 범위를 벗어납니다. PKCS #7 메시지가 있을 수 있습니다(RFC:2986).

Cisco Communications Manager 인증서 관리

속성 집합을 포함하려는 의도는 두 가지입니다.

- 지정된 엔티티에 대한 다른 정보 또는 엔티티가 나중에 인증서 취소를 요청할 수 있는 챌린지 비밀번호를 제공하기 위해.
- X.509 인증서에 포함할 특성을 제공합니다.현재 UC(Unified Communications) 서버는 챌린지 비밀번호를 지원하지 않습니다.

현재 Cisco UC 서버에는 다음 표와 같이 CSR에서 이러한 특성이 필요합니다.

정보	설명
조직 단위	조직 단위
조직 이름	조직 이름
구	조직 위치
주	조직 상태
국가	국가 코드를 변경할 수 없습니다.
대체 호스트 이름	대체 호스트 이름

문제

UC를 지원할 때 CA 서명 인증서를 UC 서버에 업로드하지 못하는 경우가 많습니다.서명된 인증서를 생성하기 위해 CSR을 사용한 사용자가 아니므로 서명된 인증서를 생성할 때 발생한 사항을 항상 확인할 수는 없습니다.대부분의 경우 새 인증서를 다시 서명하는 데 24시간 이상이 걸립니다.CUCM과 같은 UC 서버에는 인증서 업로드가 실패하는 이유를 파악하는 데 도움이 되는 자세한 로그/추적이 없으며 오류 메시지만 제공합니다.이 문서는 UC 서버든 CA 문제든 문제를 좁히고자 합니다.

CUCM에서 CA 서명 인증서에 대한 일반 사례

CUCM은 Cisco Unified Communications Operating System Certificate Manager GUI에서 액세스할 수 있는 PKCS#10 CSR 메커니즘을 사용하여 서드파티 CA와의 통합을 지원합니다.현재 서드파티 CA를 사용하는 고객은 Cisco CallManager, CAPF, IPSec 및 Tomcat용 인증서를 발급하려면 CSR 메커니즘을 사용해야 합니다.

1단계. CSR을 생성하기 전에 ID를 변경합니다.

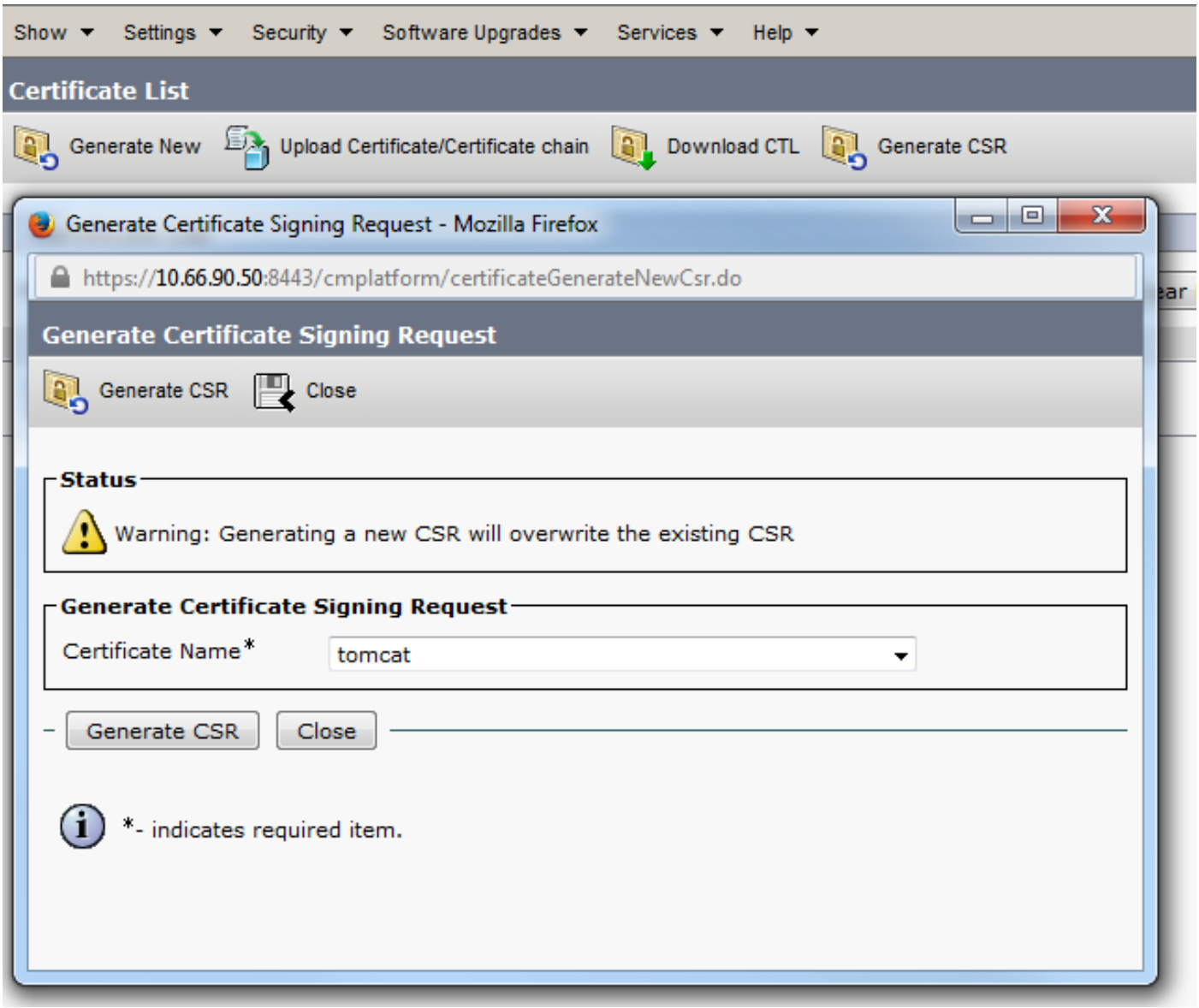
CSR을 생성하기 위해 CUCM 서버의 ID는 이 이미지에 표시된 대로 명령 **집합 웹 보안**을 사용하여 수정할 수 있습니다.

```
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
```

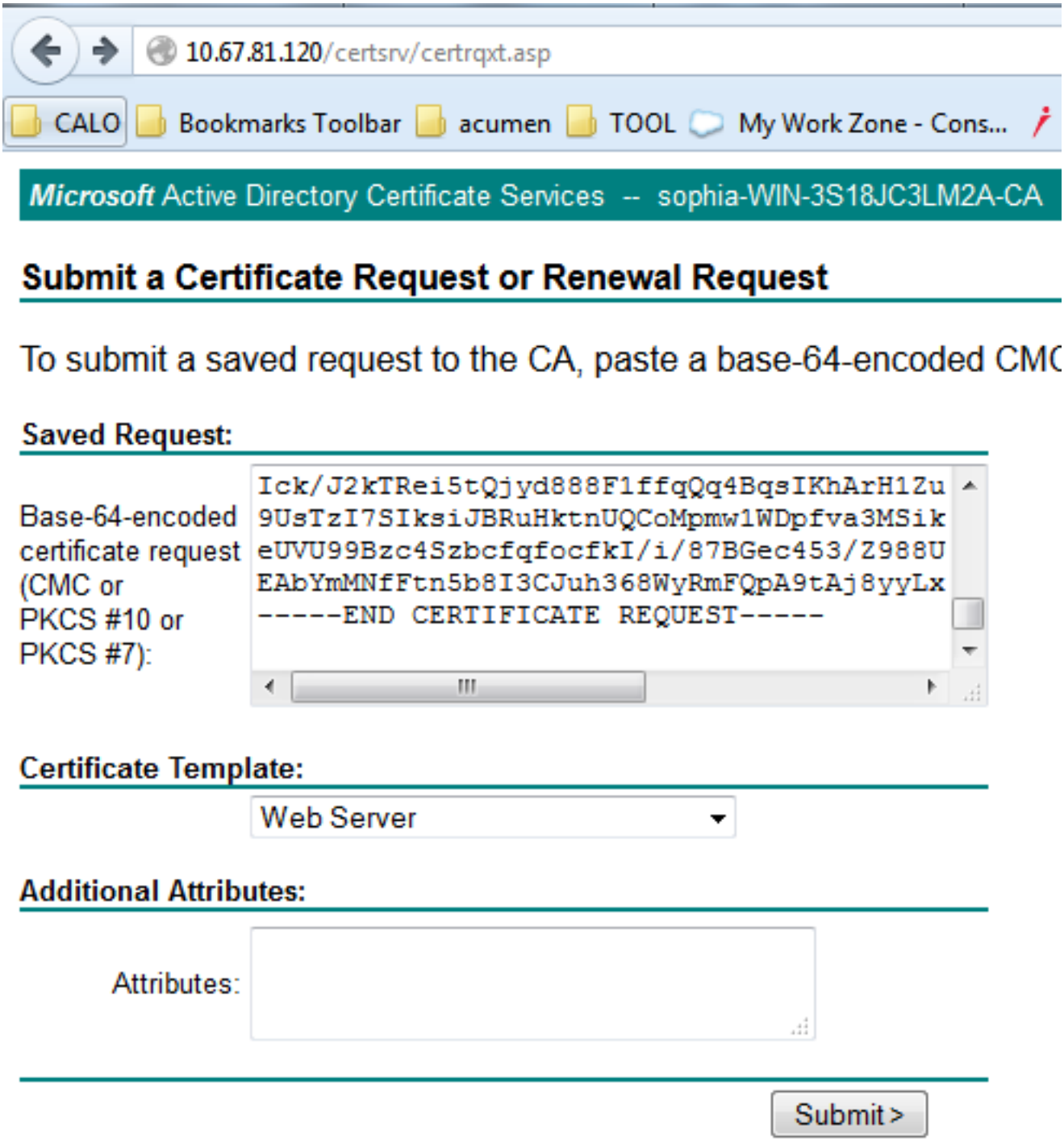
위 필드에 공간이 있는 경우 이미지에 표시된 대로 명령을 실행하려면 ""를 사용합니다.

```
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)?
```

2단계. 이미지에 표시된 대로 CSR을 생성합니다.

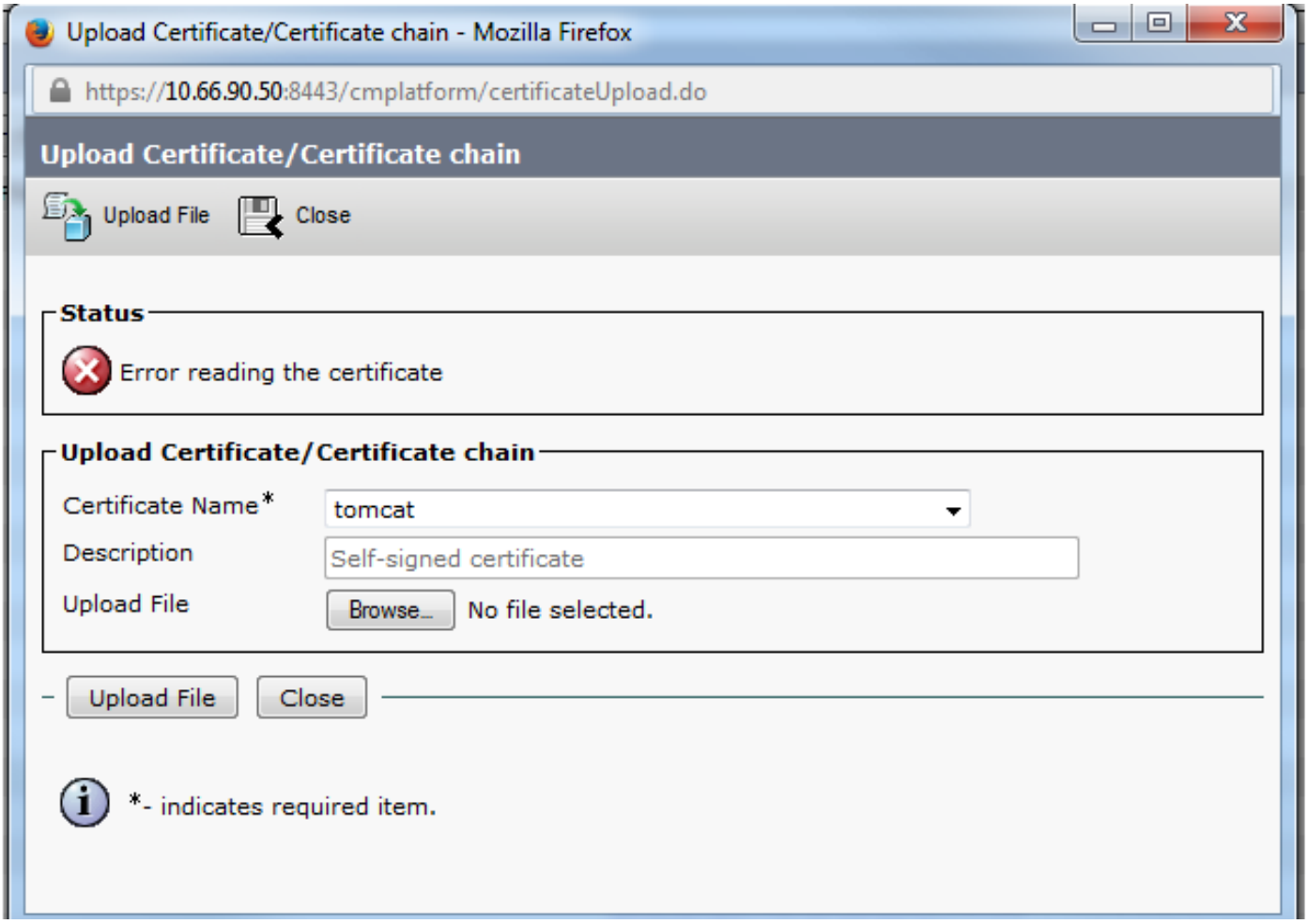


3단계. CSR을 다운로드하고 이미지에 표시된 대로 CA에서 서명합니다.



4단계. CA 서명 인증서를 서버에 업로드합니다.

CSR이 생성되고 인증서가 서명되고 "인증서 읽기 오류"(이 이미지에 표시됨)라는 오류 메시지와 함께 업로드하지 못한 경우 CSR이 재생성되었는지 또는 서명된 인증서 자체가 문제의 원인인지 확인해야 합니다.



CSR이 재생성되었는지 또는 서명된 인증서 자체가 문제의 원인인지 확인하는 세 가지 방법이 있습니다.

해결 방법 1. 루트(또는 linux)에서 OpenSSL 명령 사용

1단계. 루트에 로그인하고 이미지에 표시된 대로 폴더로 이동합니다.

```
[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]#
```

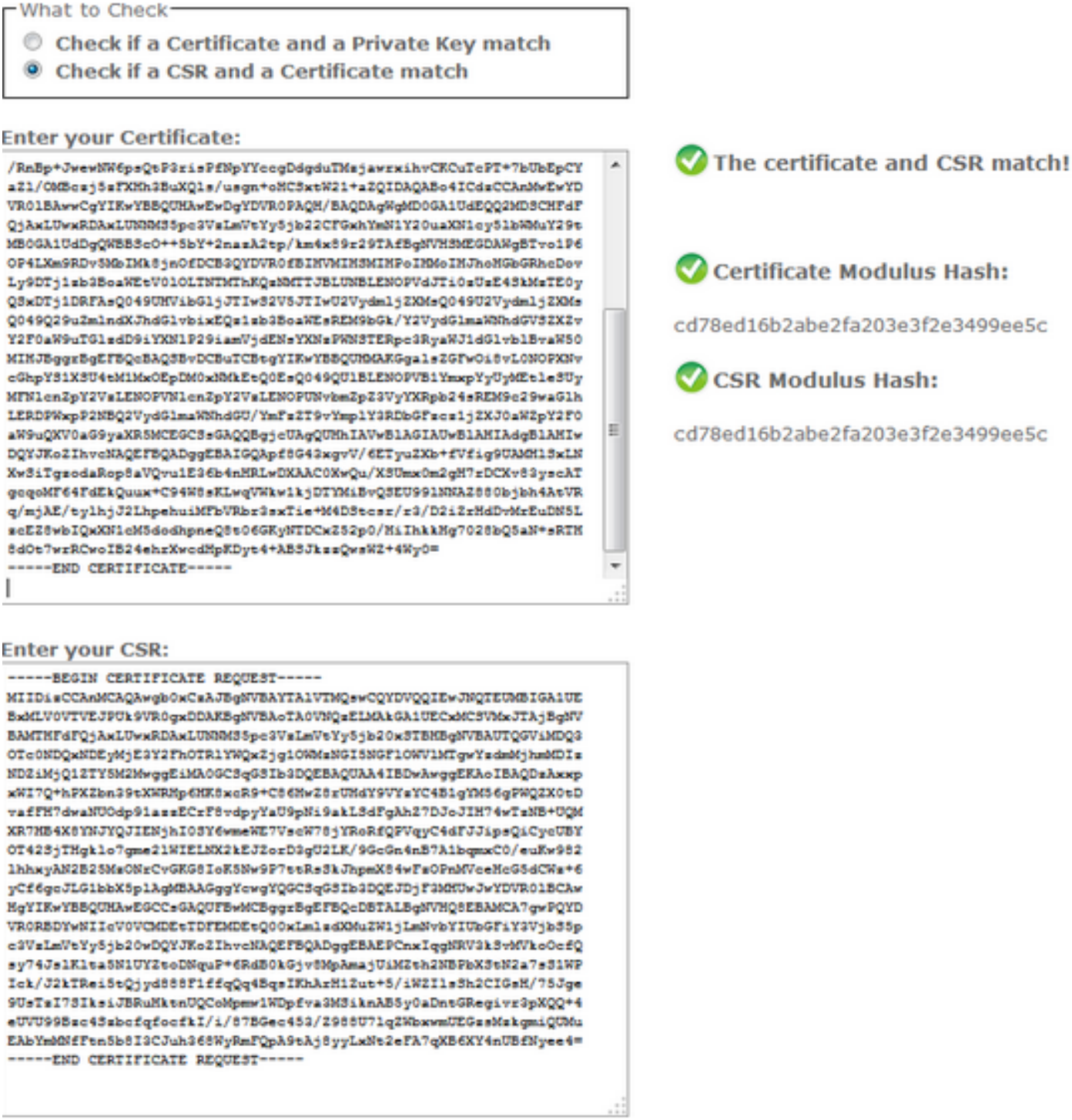
2단계. 서명된 인증서를 SFTP(Secure FTP)를 사용하여 동일한 폴더에 복사합니다. SFTP 서버를 설정할 수 없는 경우 TFTP 폴더의 업로드는 이미지에 표시된 대로 CUCM에 인증서를 가져올 수도 있습니다.

```
[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. 이미지에 표시된 대로 CSR의 MD5와 서명된 인증서를 확인합니다.

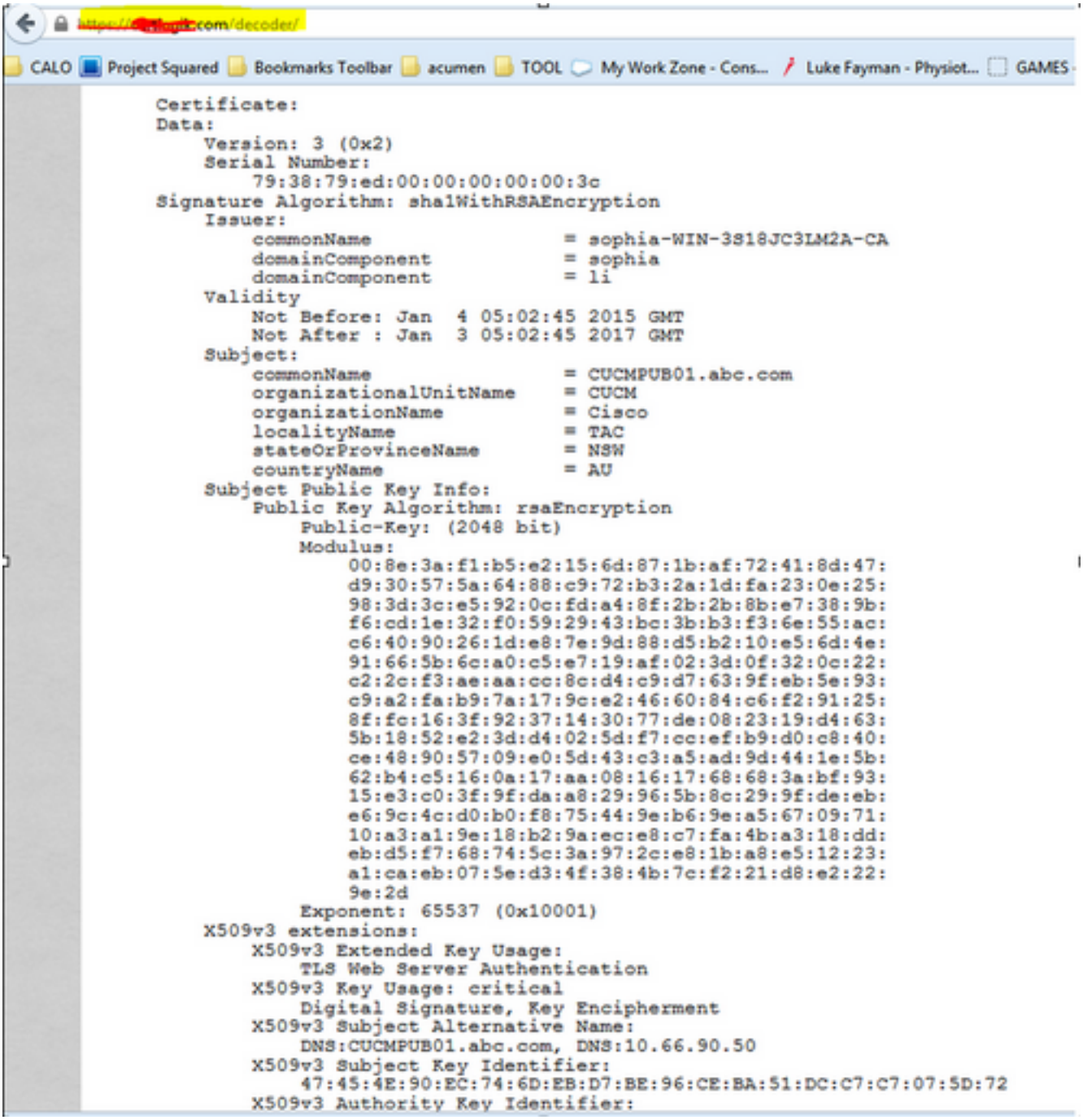
```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

해결 방법 2. 인터넷에서 SSL 인증서 키 매처 사용

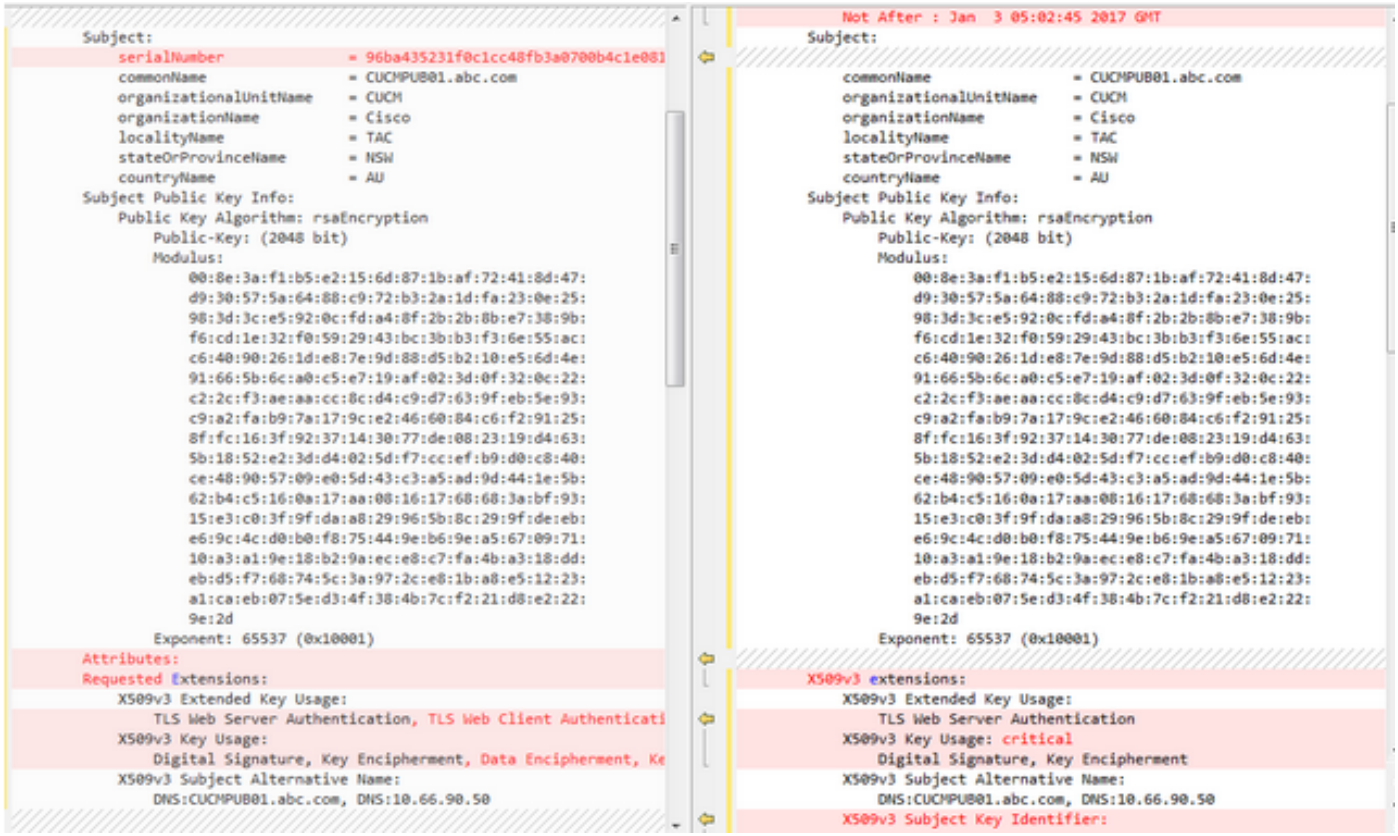


솔루션 3. 인터넷에서 CSR 디코더의 콘텐츠를 비교합니다.

1단계. 이 이미지에 표시된 대로 각각에 대한 세션 **인증서 세부 정보**를 복사합니다.



2단계. 이 이미지에 표시된 대로 Notepad++와 같은 도구에서 Compare 플러그인과 비교합니다.



```
        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:
```