UC のための CSR および証明書 ミスマッチを確認して下さい

目次

概要

この資料に認証局（CA）署名入り認証が Cisco Unified アプリケ- ションサーバのための既存の証明書署名要求（CSR）と一致するかどうか識別する方法を記述されています。

前提条件

要件

Cisco は X.509/CSR のナレッジがあることを推奨します。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- Cisco Unified Communications Manager（CUCM）
- Cisco Unified IM および存在
- Cisco Unified Unity Connection

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

背景説明

認証 要求は識別名、公開キーおよび属性の一まとめにエンティティによって署名する認証を要求する設定 される オプションので構成されています。 認証 要求は X.509 公開鍵証明に要求をトランスフォームする認証局（CA）に送信 されます。 署名入り認証でどんな形式認証局（CA）が最近戻すかこの資料の範囲外にあります。 PKCS #7 メッセージは 1 possibility.(RFC:2986) です。

Cisco コミュニケーション マネージャ証明書管理

一組の属性を含む意図は二重です:

- ある特定のエンティティについての他の情報を、かエンティティがより遅い要求 証明書の失効できるチャレンジ パスワードを提供するため。
- 属性を X.509 証明書の包含に提供するため。 現在のユニファイド コミュニケーション（UC）サーバはチャレンジ パスワードをサポートしません。

Cisco 現在の UC サーバはこの表に示すように CSR のこれらの属性を必要とします:

情報	説明
orgunit	組織ユニット
orgname	組織名前
局所性	組織の場所
状態	組織の状態
国	国別コードは変更することができません
alternatehostname	代替ホスト名

問題

UC をサポートするとき、CA 署名入り認証が UC サーバでアップ ロードしない多くのケースに出会うことができます。 署名入り認証を作成するために CSR を使用した人ではないので発生したものが署名入り認証の作成の時に常に識別できません。 ほとんどのシナリオでは、新しい証明書を再契約して 24 時間以上かかります。 CUCM のような UC サーバは証明書アップ ロードがなぜの失敗するが、ちょうど エラー メッセージを伝えるか識別で助けるためにログ/トレースを詳述しませんでした。 この技術情報の意図はそれが UC サーバまたは CA 問題であるかどうか問題の範囲を絞ることです。

CUCM の CA 署名付き証明書のための一般診療

CUCM は Cisco Unified Communications オペレーティング システム認証マネージャ GUI でアクセス可能である PKCS#10 CSR メカニズムの使用のサード パーティ CA の統合をサポートします。 現在 サード パーティ CA を使用する顧客は、Cisco CallManager、CAPF、IPSec および Tomcat のための証明書を発行するために CSR メカニズムを使用する必要があります。

ステップ 1. CSR を生成する前に識別を変更して下さい。

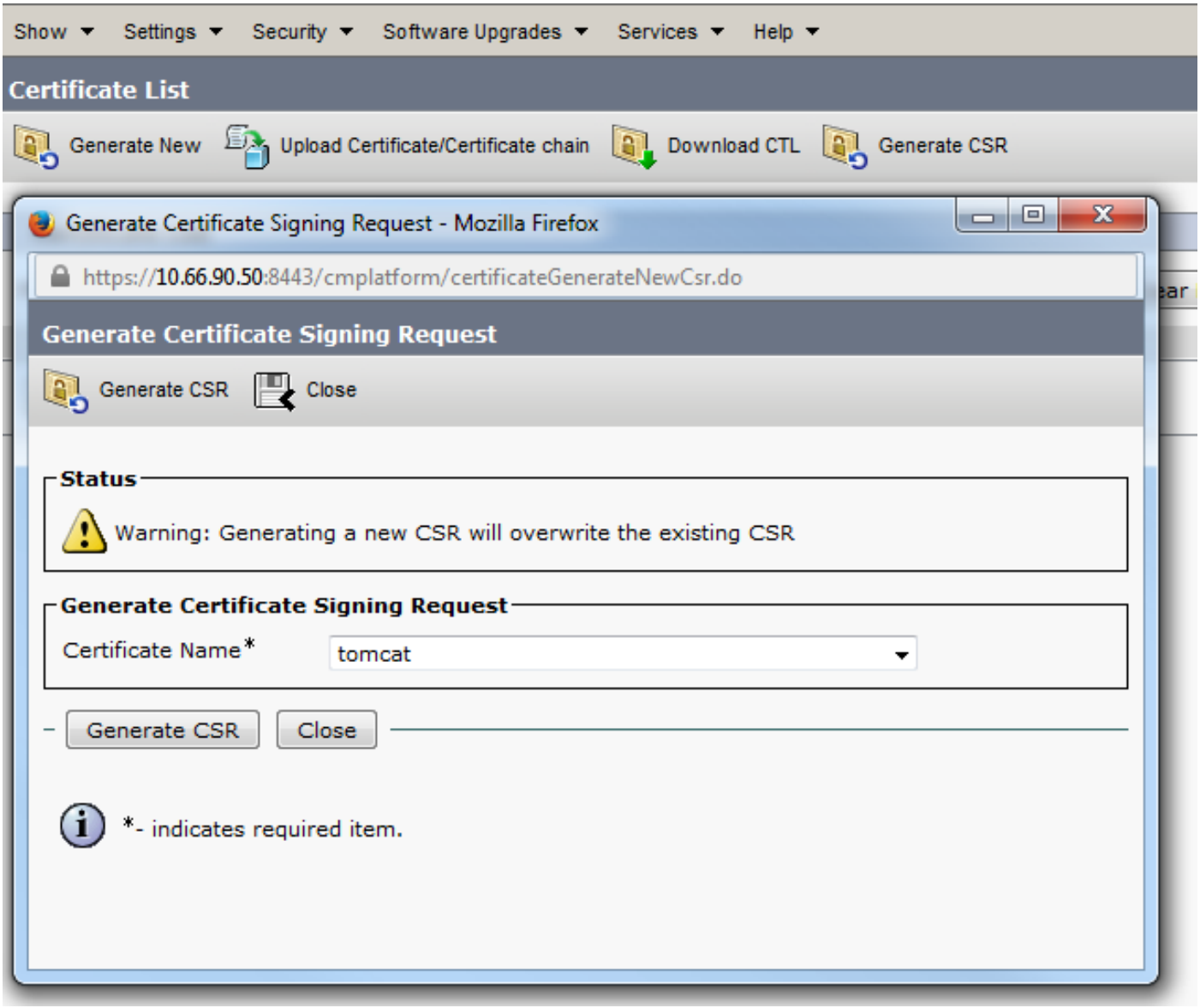
CUCM サーバの識別はこのイメージに示すようにコマンドによって**設定 される Web セキュリティ**の使用と CSR を生成するために修正することができます。

```
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
```

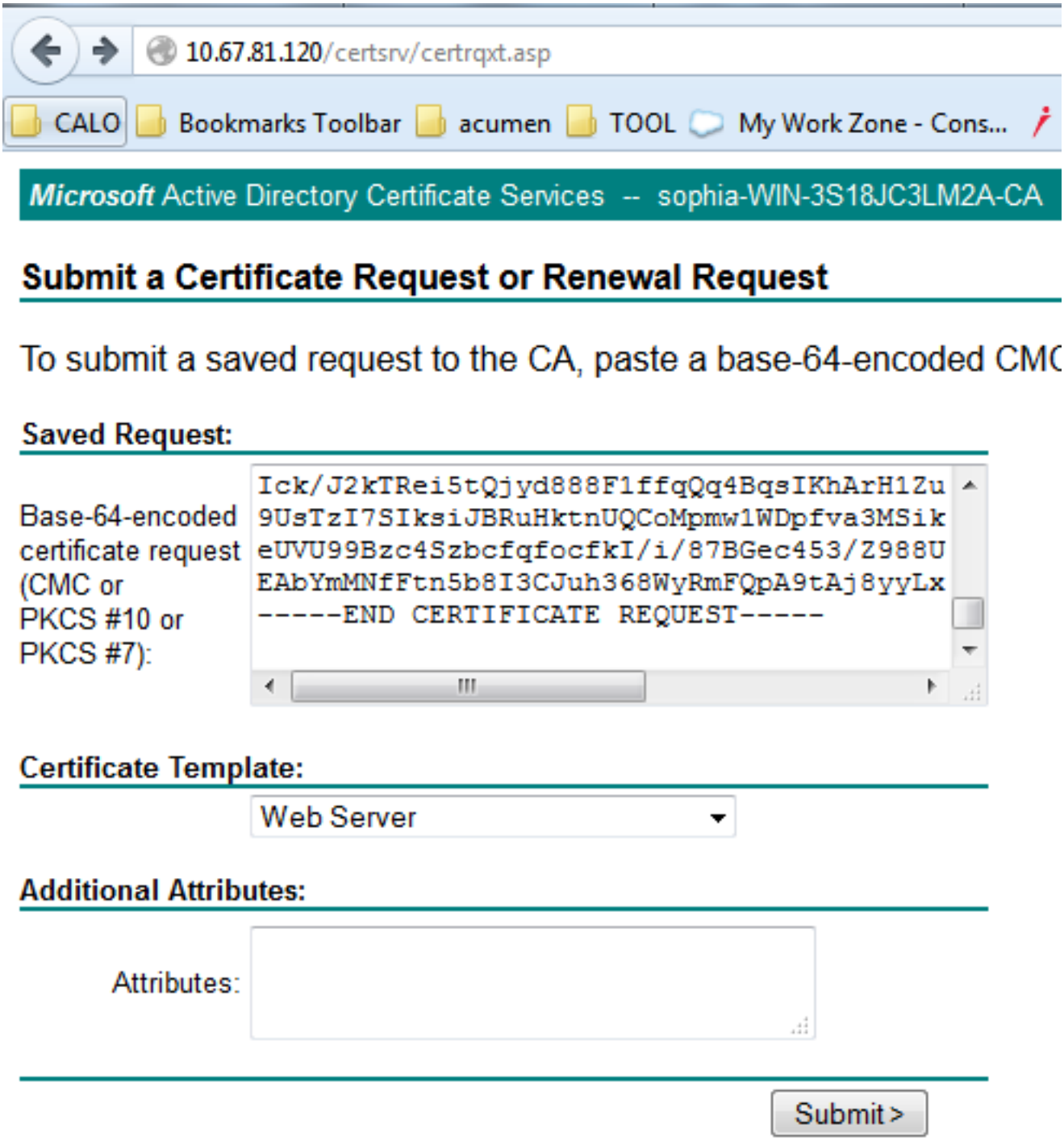
上記のフィールドで領域がある場合、イメージに示すようにコマンドを実現させるために「」使用して下さい。

```
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)?
```

ステップ 2.イメージに示すように生成する CSR。

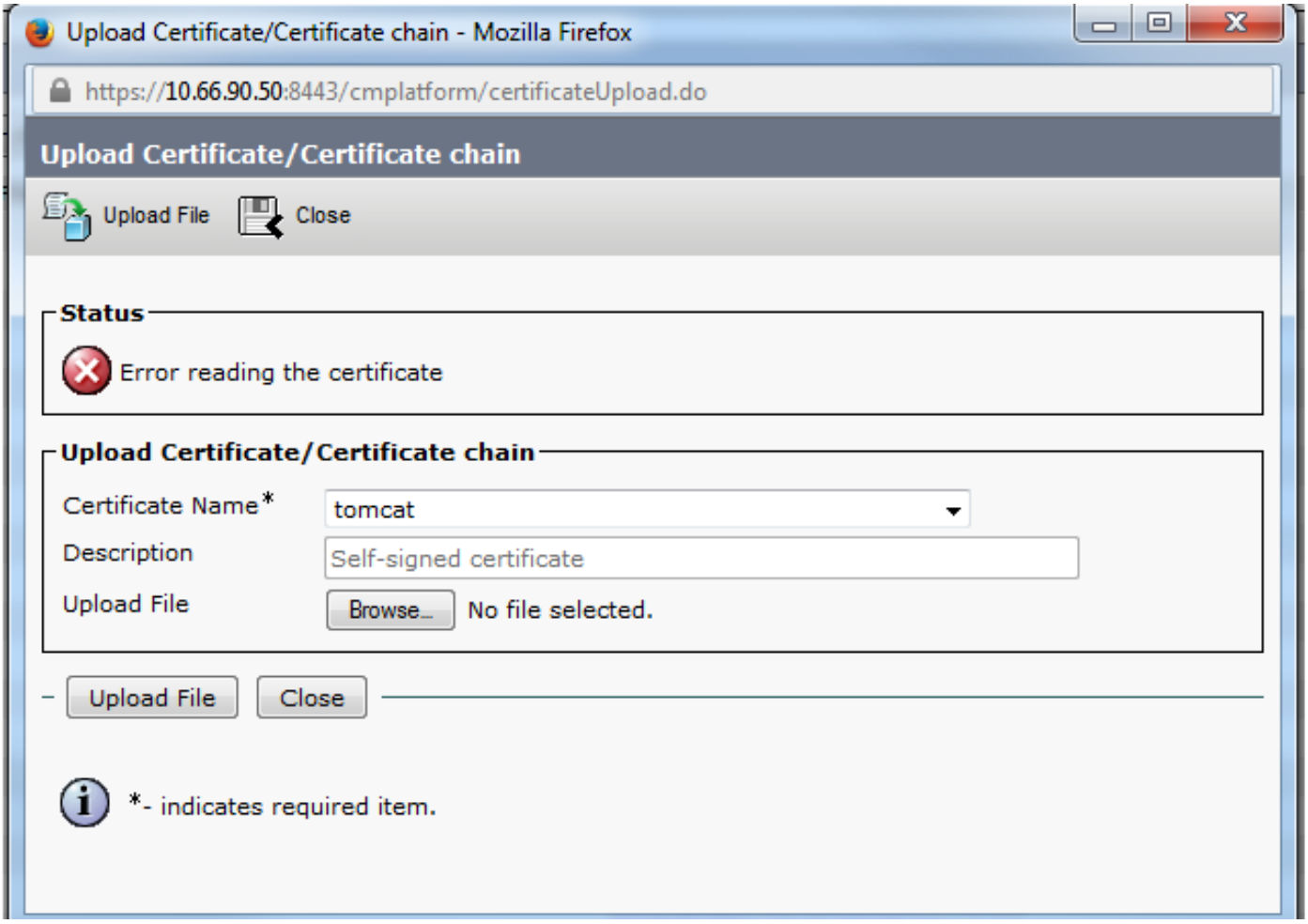


ステップ 3. CSR をダウンロードし、イメージに示すように CA によって署名されて得て下さい。



ステップ 4.サーバに CA署名付き証明書をアップ ロードして下さい。

、そして証明書が生成されれば、そして証明書」を読んでいれば (このイメージに示すように) 署名すれば CSR が エラー メッセージ「エラーとそれをアップ ロードし損えば、そして CSR が再生するか、または署名入り認証自体が問題の原因であるかどうか確認する必要があります。



CSR が再生するか、または署名入り認証自体が問題の原因であるかどうか確認する 3 つの方法があります。

ソリューション 1。 ルート使用して下さい（ または Linux ）で OpenSSL コマンドを

ステップ 1.ルートへのログインおよびイメージに示すようにフォルダへの移動。

```
[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]#
```

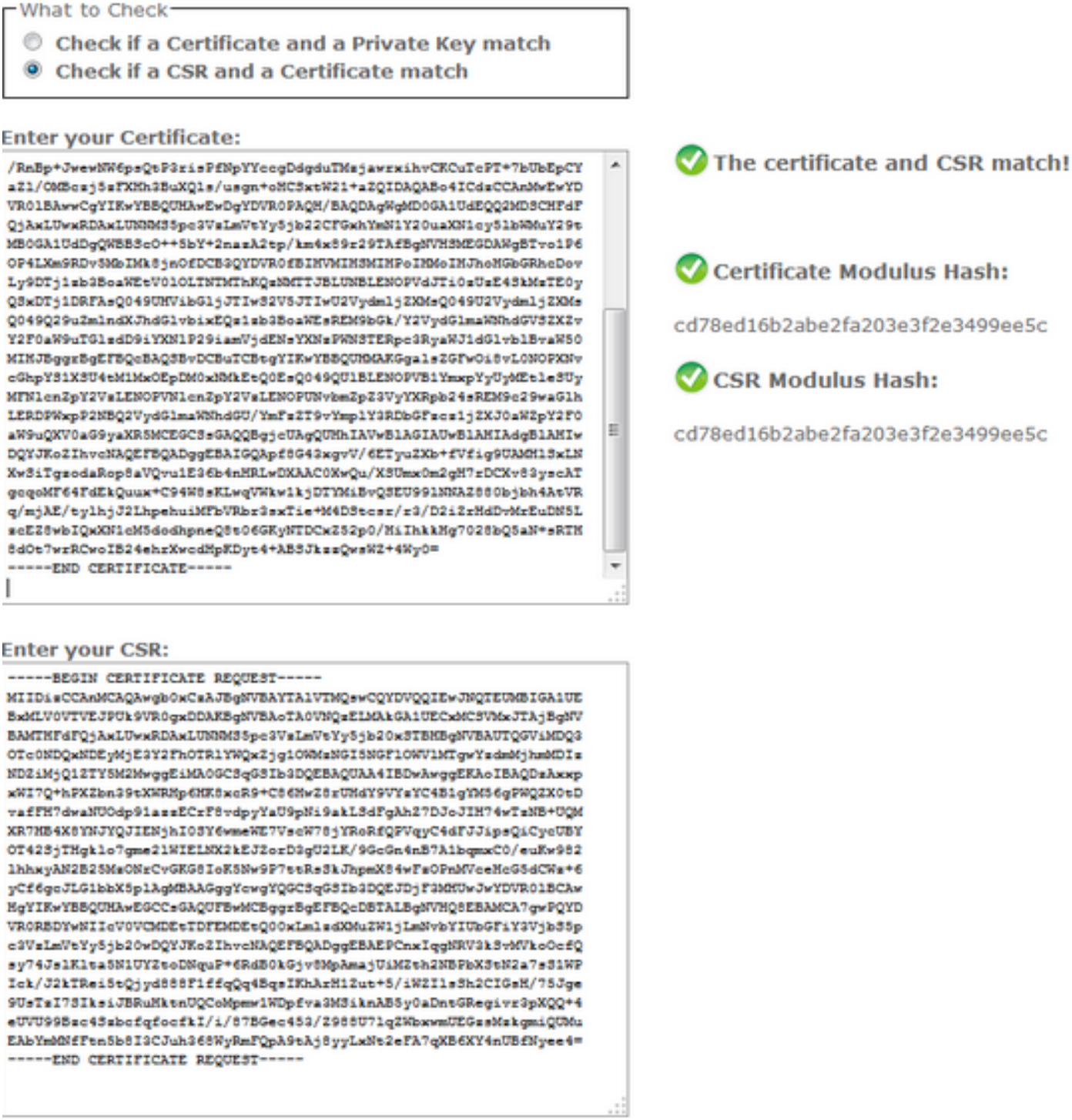
ステップ 2.セキュア FTP （ SFTP ）が付いている同じフォルダに署名入り認証をコピーして下さい。 SFTP サーバを設定することができない場合 TFTP フォルダのアップ ロードはまたイメージに示すように CUCM に証明書を得ることができます。

```
[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. イメージに示すように CSR および署名入り認証があるように MD5 を確認して下さい。

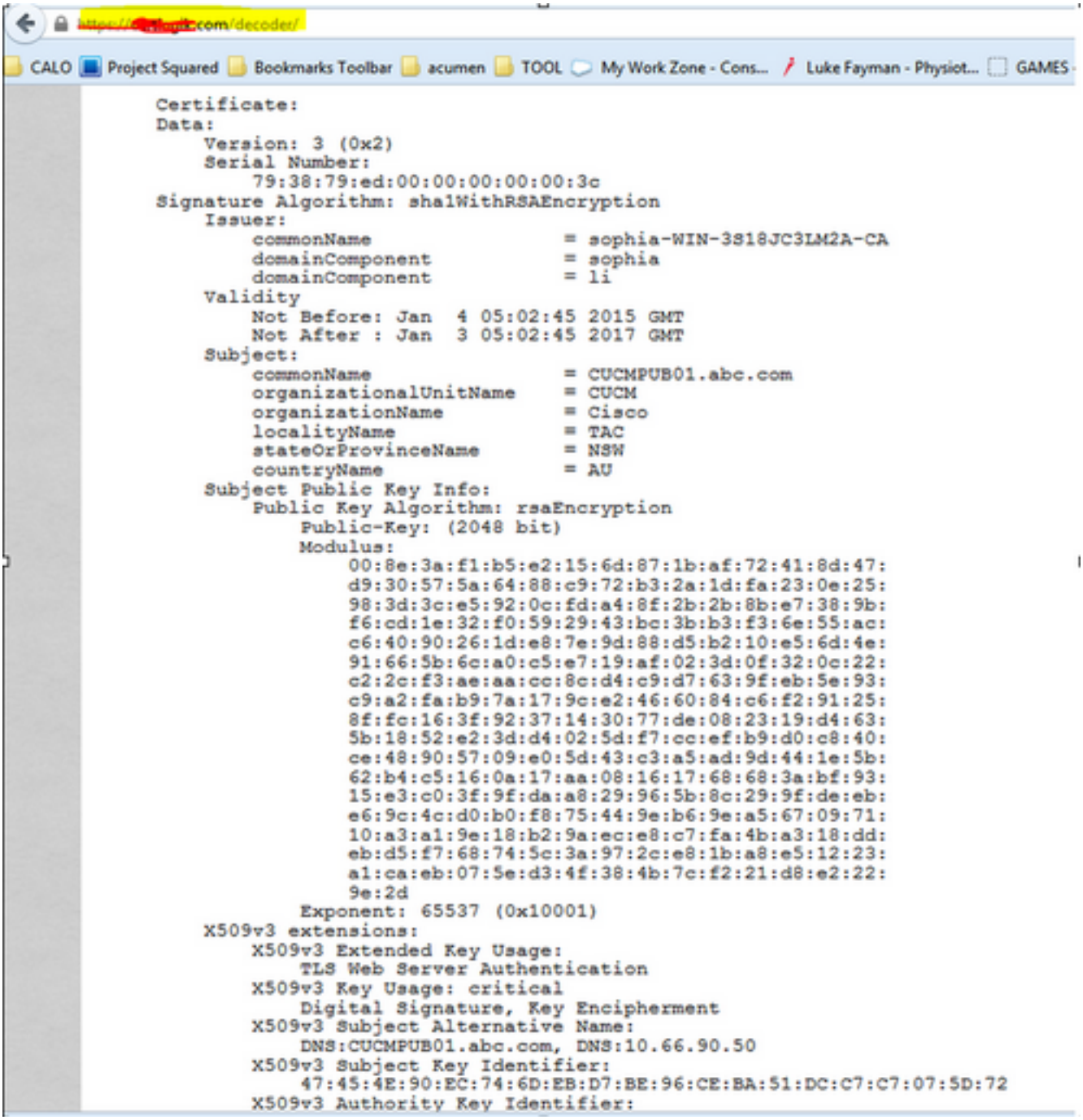
```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

ソリューション 2。 インターネットからの SSL Certificate 鍵さねはぎ機を使用して下さい

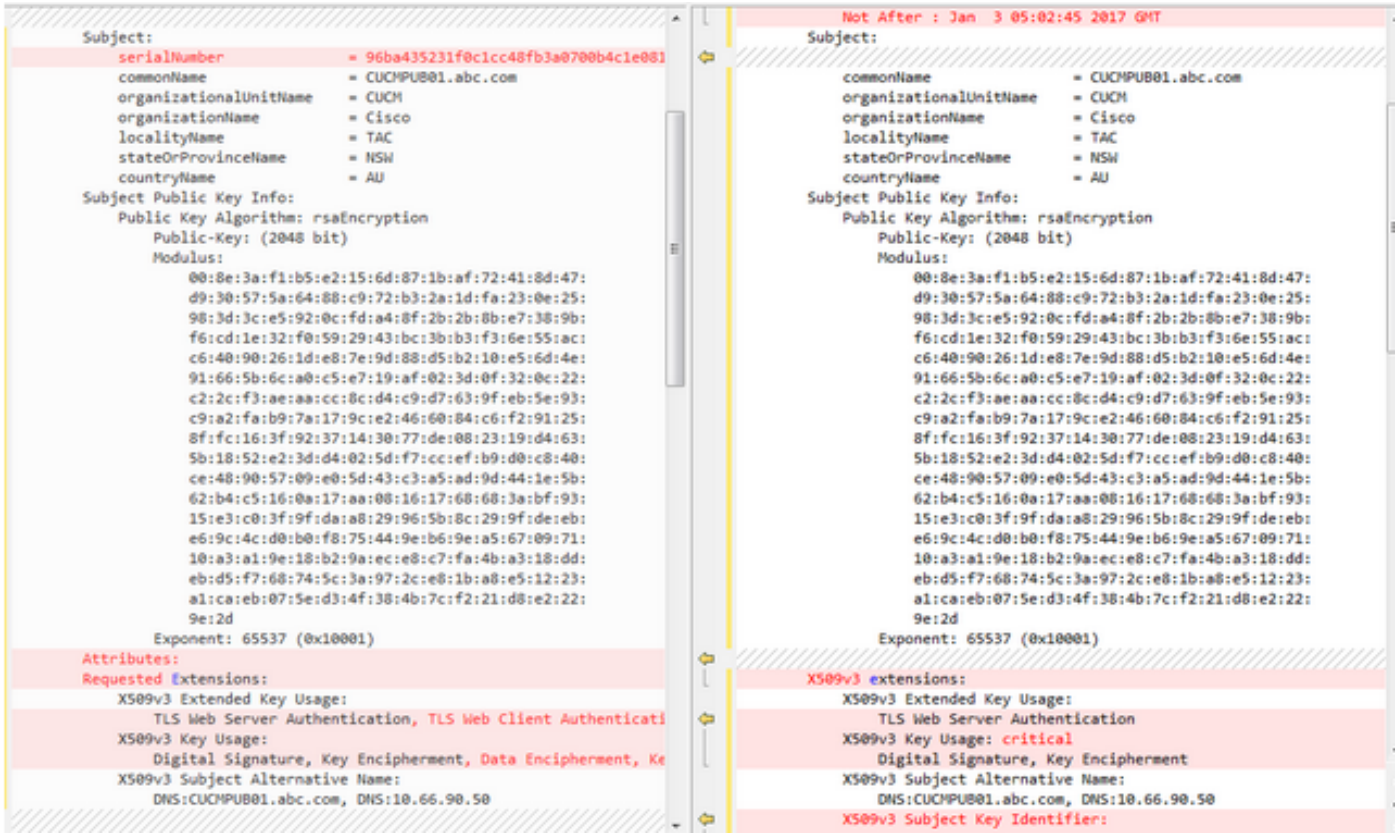


ソリューション 3.はインターネットからのあらゆる CSR デコーダからの内容を比較します

ステップ 1.このイメージに示すようにそれぞれのためのセッション **証明書詳細情報**をコピーして下さい。



ステップ 2.このイメージに示すように比較プラグインと Notepad++ のようなツールでそれらを比較して下さい。



```
        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:
```