Contents

Introduction

This document describes how to identify whether the Certificate Authority (CA) signed certificate matches the existing Certificate Signing Request (CSR) for Cisco Unified Application Servers.

Prerequisites

Requirements

Cisco reccommends that you have the knowledge of X.509/CSR.

Components Used

This document is not restricted to specific software and hardware versions.

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.

Background Information

A certification request consists of a distinguished name, a public key, and an optional set of attributes, collectively signed by the entity requesting certification. Certification requests are sent to a certification authority that transforms the request into an X.509 public-key certificate.In what form the certification authority returns the newly signed certificate is outside the scope of this document. A PKCS #7 message is one possibility.(RFC:2986)

Cisco Communications Manager Certificate Management

The intention of including a set of attributes is twofold:

- To provide other information about a given entity, or a challenge password by which the entity may later request certificate revocation.
- To provide attributes for inclusion in X.509 certificates. The current UC servers do not support a challenge password.

Current Cisco UC servers require these attributes in a CSR as shown in this table:

Information	Description
orgunit	organizational unit
orgname	organizational name
locality	location of organization
state	state of organization
country	country code can not be changed
alternatehostname	alternate host name

Related Products

This document can also be used with these hardware and software versions:

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

Problem

In supporting UC, you encounter a lot of cases where the CA signed certificate fails to be uploaded on the UC servers. You cannot always identify what has occurred during the creation of the signed certificate, since you are not the person who used the CSR to create the signed certificate. In most scenarios, re-signing a new certificate takes more than 24 hours. UC servers such as CUCM do not have detailed log/trace to assist in identifying why the certificate upload fails but they just give an error message. This article is intended to assist in narrowing down the issue, whether it is a UC server or a CA issue.

General Practice for CA-signed certificates in CUCM

CUCM supports integration with third-party CAs by using a PKCS#10 CSR mechanism that is accessible at the Cisco Unified Communications Operating System Certificate Manager GUI. Customers, who currently use third-party CAs must use the CSR mechanism to issue certificates for Cisco CallManager, CAPF , IPSec, and Tomcat.

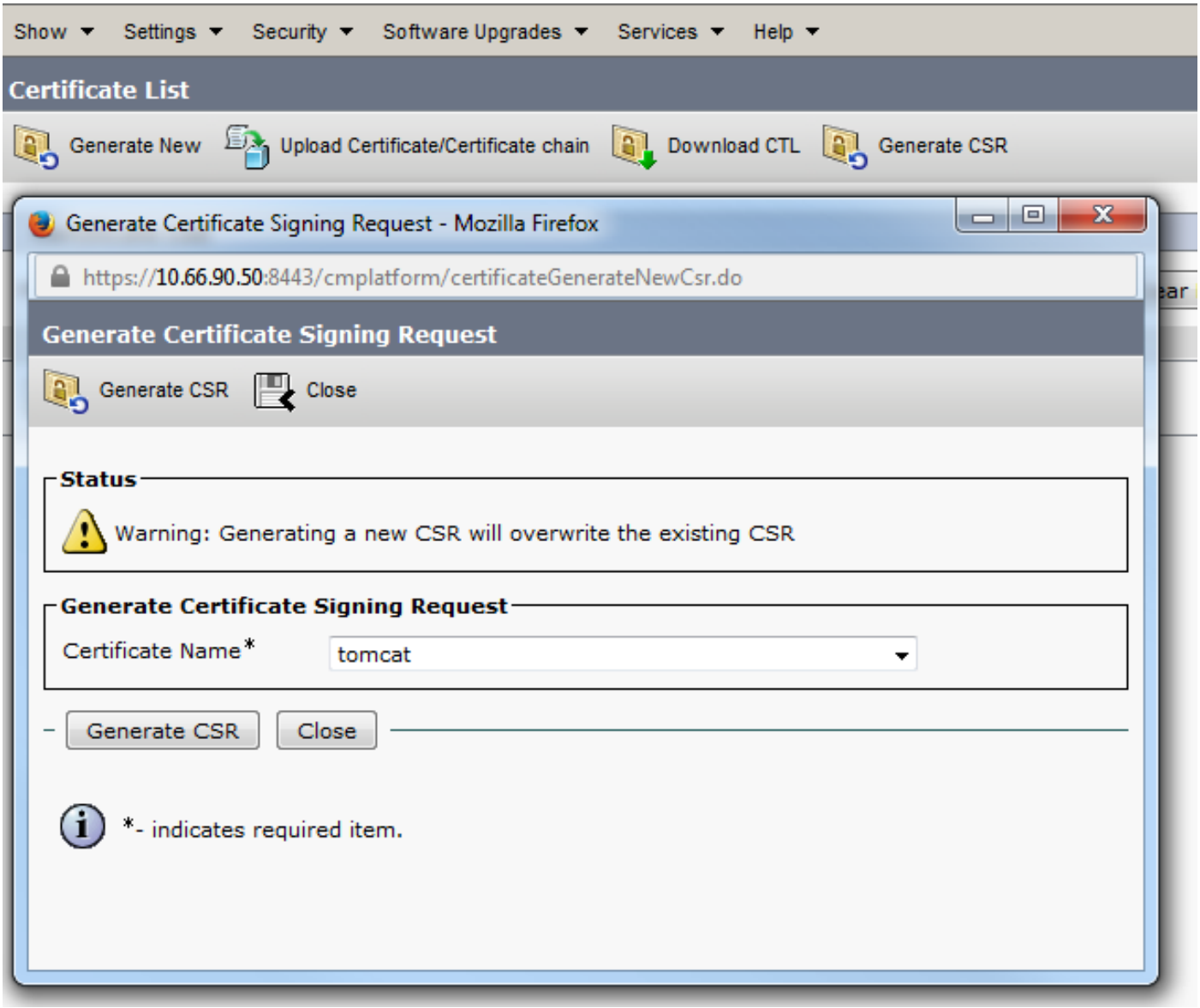
Step 1. Change the Identify before generating the CSR

The identity of the CUCM server to generate a CSR can be modified by using the command **set web-security** as shown in this image.

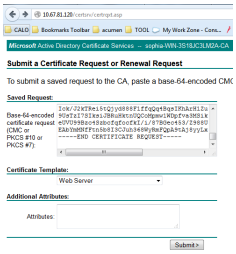
If you have space in the above fields, please use “” to achieve the command as:

```
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)?
```

Step 2. Generate the CSR.

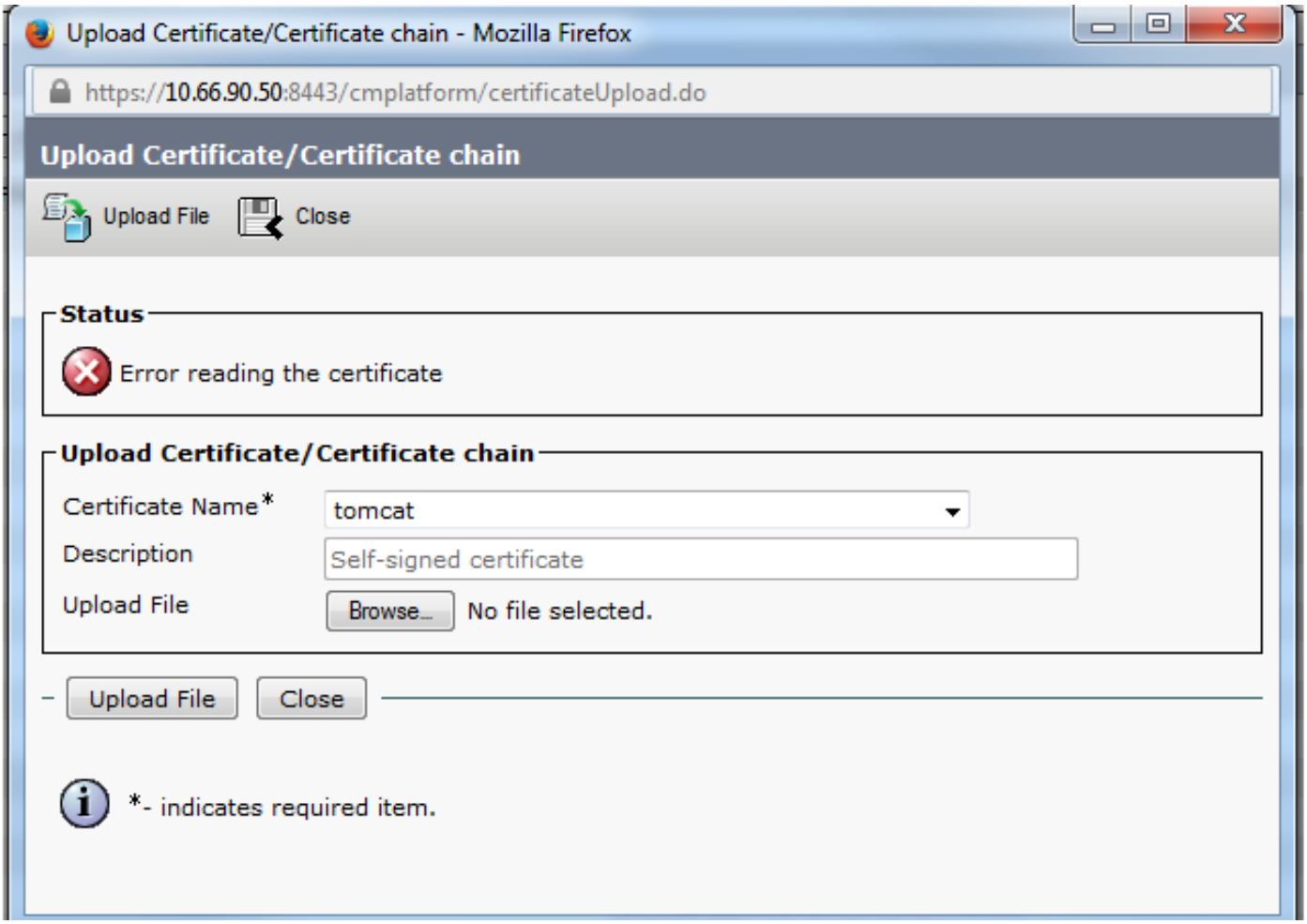


Step 3. Download the CSR and get it signed by the CA.



Step 4. Upload the CA-signed certificate to the server.

Once the CSR is generated and the certificate is signed, if you fail to upload it with an error message **Error reading the certificate** (as shown in this image), then you need to check whether the CSR is regenerated or whether the signed certificate itself is the cause of the issue.



There are three ways to check whether the CSR is regenerated or the signed certificate itself is the cause of the issue.

Solution 1. Use the OpenSSL Command in root (or linux)

1. Log in to the root and navigate to the folder.

```
[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. Copy the signed certificate to the same folder using Secure FTP (SFTP). If you are unable to set up an SFTP server, then uploading it to the TFTP folder also gets the certificate onto the

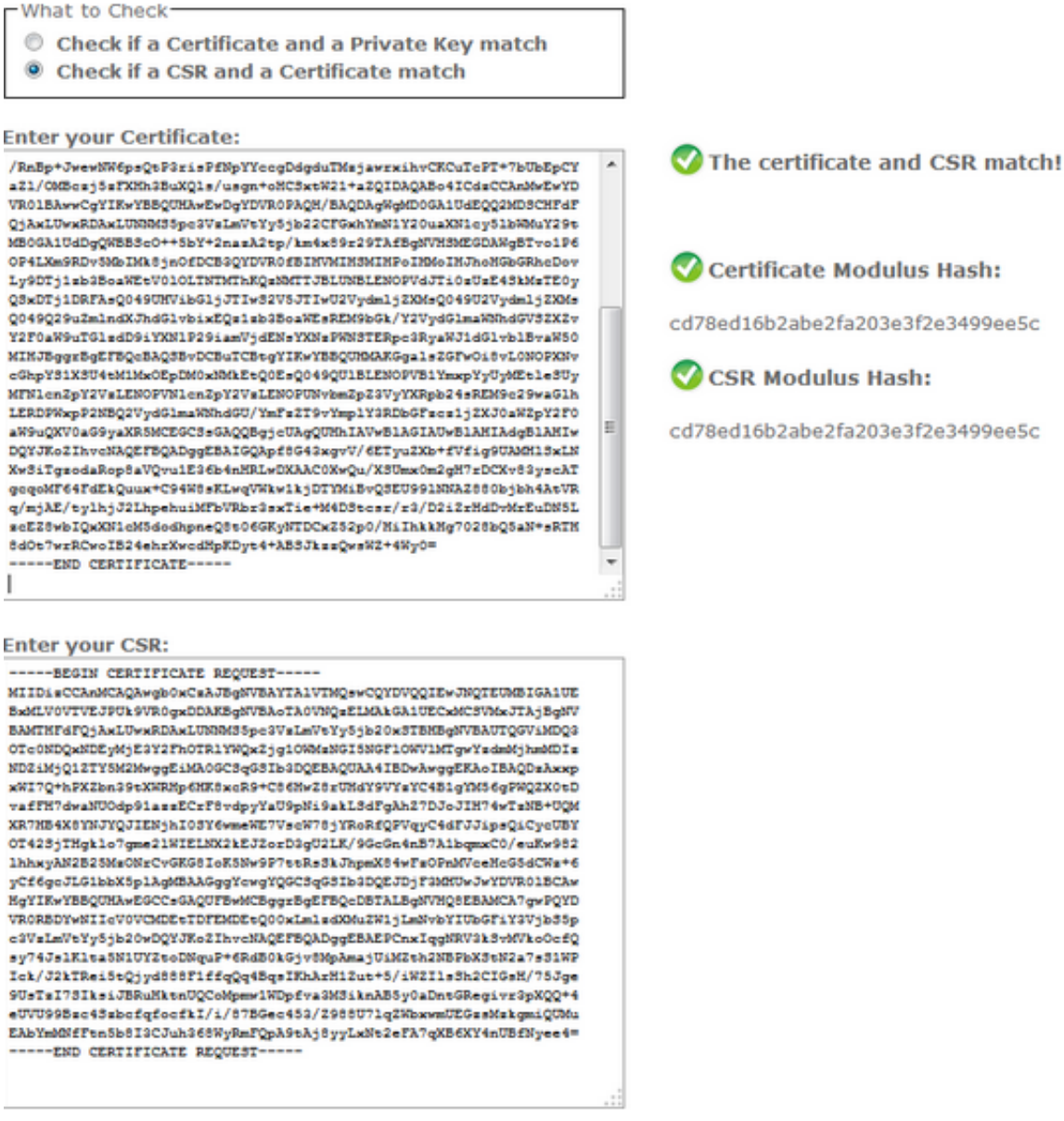
CUCM.

```
[root@CCM105PUB keys]# sftp cisco@10.66.90.19
bash: sftp: 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. Check the MD5 for the CSR and the signed certificate.

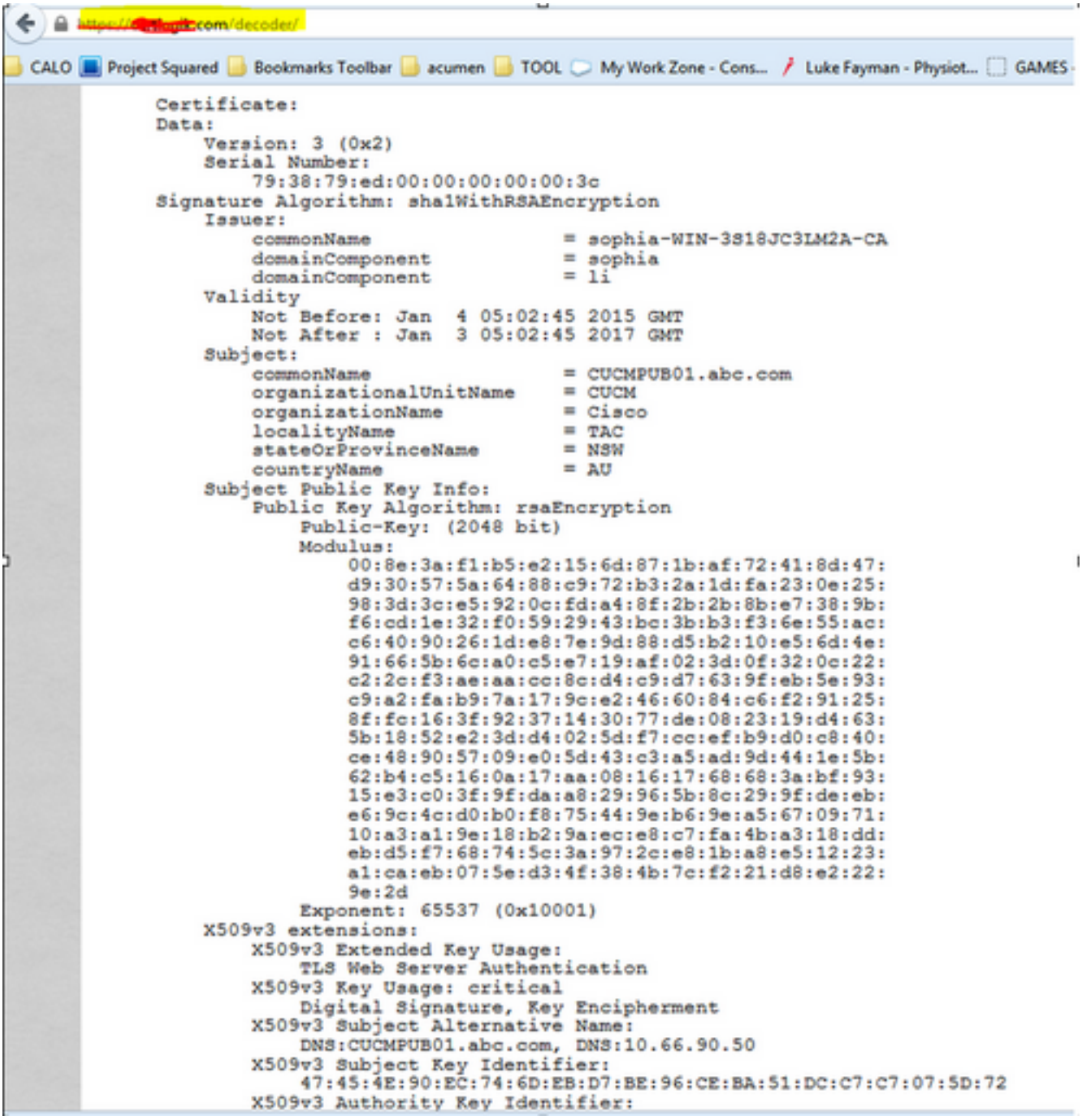
```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

Solution 2. Use any SSL certificate key matcher from the Internet



Solution 3. Compare the Content from any CSR decoder from the Internet

1. Copy the session **Certificate Detailed Information** for each as shown in this image.



2. Compare them in a tool such as Notepad++ with the Compare plugin as shown in this image.