

验证UC的CSR和证书不匹配

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[思科通信管理器证书管理](#)

[问题](#)

[CUCM中CA签名证书的一般实践](#)

[解决方案1.在根 \(或linux \) 中使用OpenSSL命令](#)

[解决方案2.使用来自Internet的任何SSL证书密钥匹配程序](#)

[解决方案3.比较来自Internet的任何CSR解码器的内容](#)

简介

本文档介绍如何确定证书颁发机构(CA)签名的证书是否与思科统一应用服务器的现有证书签名请求(CSR)匹配。

先决条件

要求

思科建议您了解X.509/CSR。

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

本文档也可用于以下硬件和软件版本：

- 思科统一通信管理器 (CUCM)
- 思科统一即时消息和在线状态
- 思科统一Unity Connection
- CUIS
- 思科媒体
- 思科统一联系中心快捷版(UCCX)

背景信息

认证请求由可分辨名称、公钥和由请求认证的实体共同签名的一组可选属性组成。认证请求被发送到将请求转换为X.509公钥证书的认证机构。证书颁发机构以何种形式返回新签名的证书不属于本文档的范围。 PKCS #7消息是一种可能。(RFC:2986)。

思科通信管理器证书管理

包含一组属性的意图是双重的：

- 为了提供关于给定实体的其他信息，或者提供挑战密码，该实体随后可以通过该密码请求证书撤销。
- 为了提供要包含在X.509证书中的属性。当前的统一通信(UC)服务器不支持质询密码。

当前Cisco UC服务器需要CSR中的以下属性，如下表所示：

信息	描述
组织	组织单位
组织名称	组织名称
位置	组织位置
状态	组织状态
国家	国家/地区代码无法更改
替代主机名	备用主机名

问题

当您支持UC时，可能会遇到许多CA签名证书无法上传到UC服务器的情况。由于您不是使用CSR创建签名证书的人，因此您无法始终确定在创建签名证书时发生了什么。在大多数情况下，重新签名新证书需要24小时以上。CUCM等UC服务器没有详细的日志/跟踪，无法帮助确定证书上传失败的原因，但它们只会提供错误消息。本文的目的是缩小问题范围，无论是UC服务器问题还是CA问题。

CUCM中CA签名证书的一般实践

CUCM支持使用PKCS#10 CSR机制与第三方CA集成，该机制可在思科统一通信操作系统证书管理器GUI中访问。当前使用第三方CA的客户必须使用CSR机制为Cisco CallManager、CAPF、IPSec和Tomcat颁发证书。

步骤1.在生成CSR之前更改标识。

使用如下图所示的命令set web-security可修改CUCM服务器的身份以生成CSR。

```
admin:set web-security ?
Syntax:
set web-security orgunit orgname locality state [country] [alternatename]
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
alternatename optional alternate host name
admin:set web-security
```

如果上述字段中有空格，请使用“”以实现如图所示的命令。

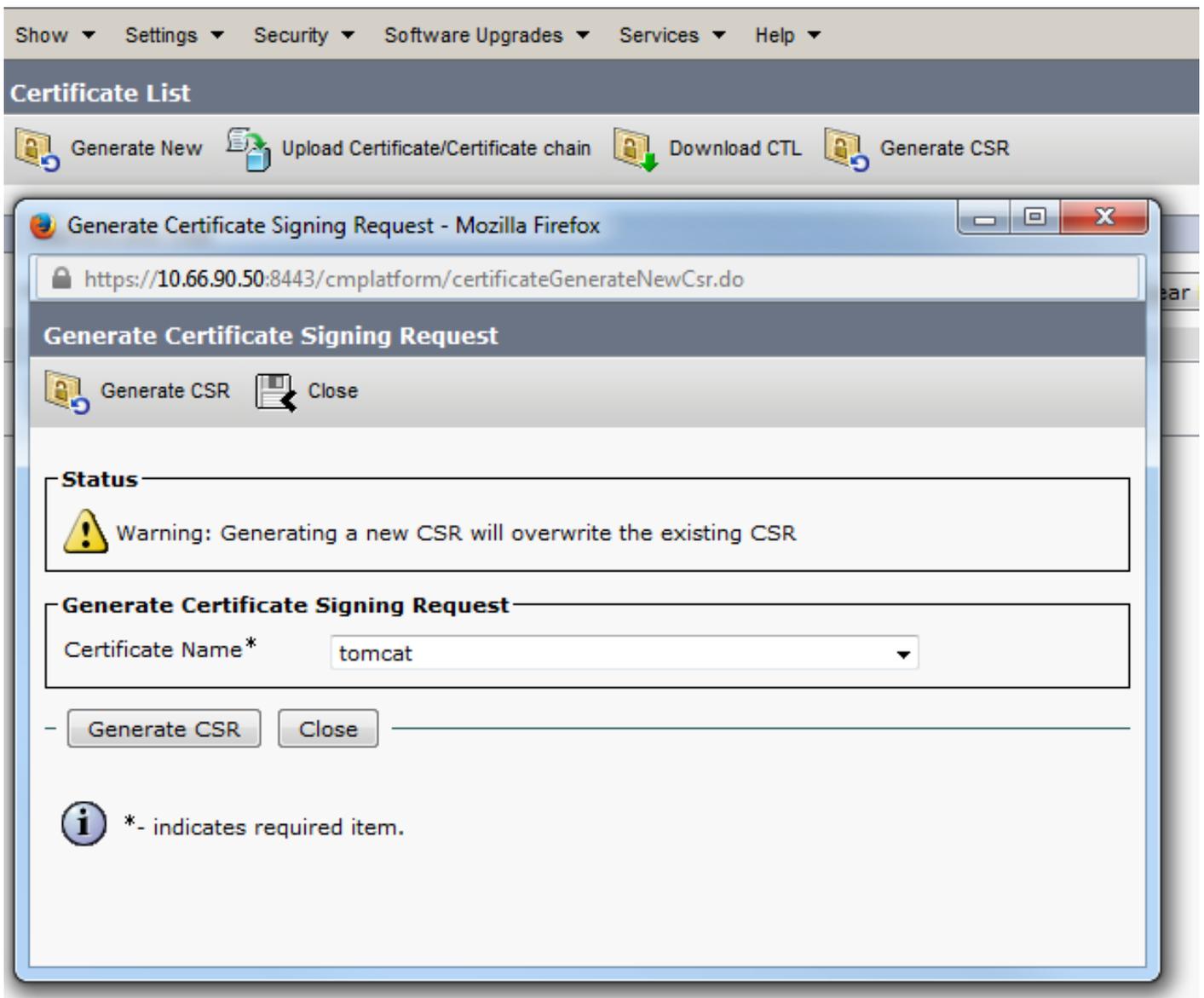
```
admin:set web-security "Cisco Systems" "Cisco TAC" "St Leonard" NSW AU CUCM105.sophia.li
WARNING: Country code can not be changed.
Country code for existing web-security is : AU

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
enerate these self-signed certificates to update them.

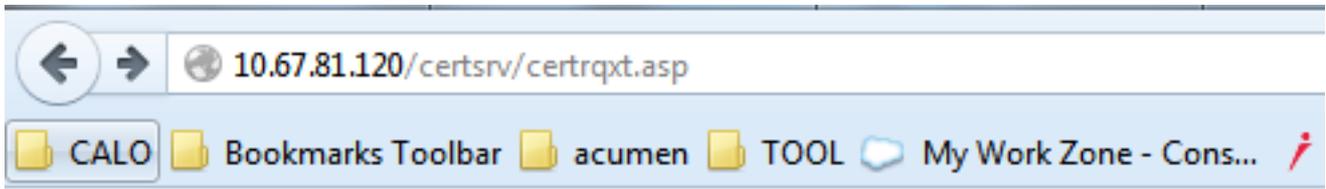
Regenerating web security certificates please wait ...

WARNING: This operation will overwrite any CA signed certificate previously imported for
Proceed with regeneration (yes/no)? █
```

步骤2.生成CSR，如图所示。



步骤3.下载CSR，并使其由CA签名，如图所示。



Microsoft Active Directory Certificate Services -- sophia-WIN-3S18JC3LM2A-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
Ick/J2kTRei5tQjyd888F1ffqQq4BqsIKhArH1Zu
9UsTzI7SIksiJBRuHktnUQCoMpmw1WDpfva3MSik
eUVU99Bzc4SzbcfqfocfkI/i/87BGec453/Z988U
EAbYmMNfFtn5b8I3CJuh368WyRmFQpA9tAj8yyLx
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

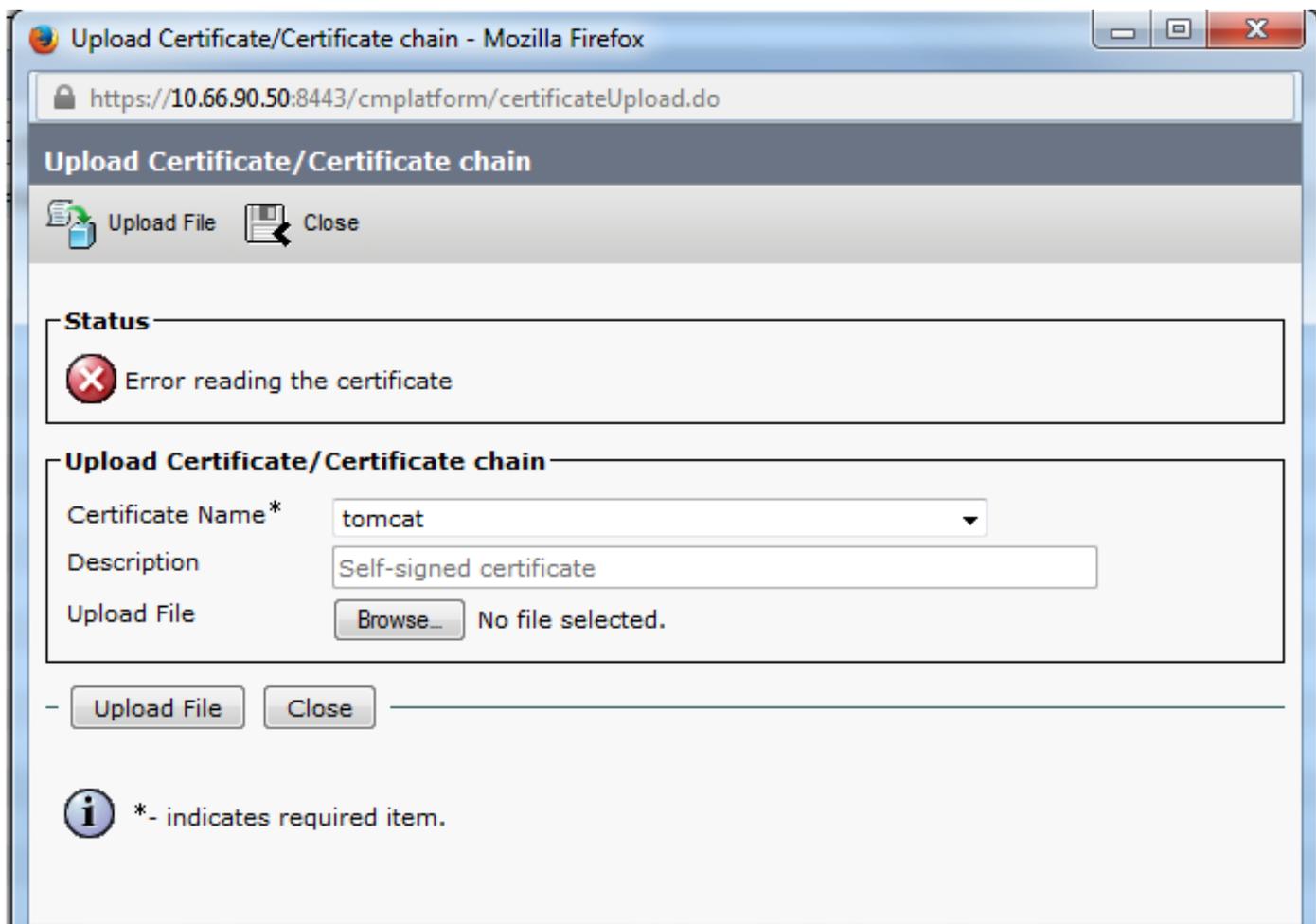
Additional Attributes:

Attributes:

Submit >

步骤4.将CA签名的证书上传到服务器。

生成CSR并签名证书后，如果您上传时未显示错误消息“读取证书时出错”（如此图所示），则您需要检查CSR是否重新生成或签名的证书本身是否是问题的原因。



有三种方法可检查CSR是否重新生成或签名证书本身是问题的原因。

解决方案1.在根 (或linux) 中使用OpenSSL命令

步骤1.登录到根目录并导航至文件夹，如图所示。

```
[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.将签名证书复制到使用Secure FTP(SFTP)的同一文件夹。 如果无法设置SFTP服务器，则TFTP文件夹上的上传也可以将证书上传到CUCM，如图所示。

```
[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.检查MD5中的CSR和签名证书，如图所示。

```
[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.使用来自Internet的任何SSL证书密钥匹配程序

What to Check

- Check if a Certificate and a Private Key match
- Check if a CSR and a Certificate match

Enter your Certificate:

```
/RnBp+JwewNw6peQcF2riaFfNpYfEcqDdqdUtmajawxihvCRKuTePT+7bUbEpCY
aZ1/OMBwaj5eFXHh3BuXQ1s/usgn+oHC9xtW21+aZQIDAQABo4ICDeCCAmMwEwYD
VR01BAAwCgYIKwYBBQUHAEwDgYDVROFAQM/BAQDAgWgMD0GA1UdEQQ2MDSCHFdF
QjAaLUwXRDAxLUNRMS5pe3VzLmVtYy5jb22CFGwhYmN1Y20uaXN1eY51bW8uY29t
MBOGA1UdDgQWBBSco++8bY+2naaA2ep/km4x89z29TAfBgNVHSMEGDAWgSTvo1P6
OP4LXm9RDv5hGeIMk8jaoEDCB9QYDVROfBIBVMIN3MINFoIMMoIMJhoMGRhoDev
Ly9DTj1ab2BoaWEtV010LINTMTkRQzBM7TJBLUNBLENOPVdJTI0zUzE4SkMaTE0y
QSkxDTj1DRFAzQ049UHV1bG1jJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
Q049Q29uZmlndXhhdG1vbixEQz1ab2BoaWEtREM9bGk/Y2VydG1maW9hdGV5ZXZv
Y2F0aW9uTG1sdD9iYXN1P29iamVjdENzYXNzPWNSTERpc3RyaWJ1dG1vb1BvaW50
MINJBggrBgEFBQcBAQSBvDCBuTCBtYIKwYBBQUIGARAGga1zGFvO18vLONOPXGv
cGhpYS1XSU4tM1MxOEpDM0xDMkEtQ0EzQ049Q1BLENOPVBIYmXpYyUyMzEt1eSUy
MfN1enZpY2VzLENOPVNIenZpY2VzLENOPUNvbmZpZ3V5YXRpb24zREM9c29waG1h
LERDPWxpP2NBQ2VydG1maW9hdGU/YmFzZi9vYm1Y3RD0GFcc1jZXJ0aWZpY2F0
aW9uQUV0aG9yaXRSMCEGCSzGAQQAQBgjCUAqQUHhIAVwBlAGIAUwBlAHIAAqBlAHIAw
DQYJKoZIhvcNAQEFBQADggEBAIGQApf8G42xgvV/6ETyu2Xb+fvfi9UAMH13xLN
Xw8iTGzodaRop8aVQvuiE36b4nHRLwDCAAC0KwQu/XSUmX0m2qH7zDCXv83ycAT
gqoqMf64FdEkkQuux+C94W8sKLwqVWk1k1jDTYMiBvQSEU991NNAZ880bjbh4AeVR
q/mjAE/tylhjJ2LhphehuimFbVRbr3axTie+M4DScczr/z0/D2izxHdDvMrEuDN5L
scE28wbIQXN1cM3dodhpneQ8t06GRyNTDCxZ52p0/HiIhkkHg7028bQ5aN+sRTN
8d0t7wrRCwoIB24ehzXwcdMpdKdyt4+ABSJkzQwzW2+4WY0=
-----END CERTIFICATE-----
```

✔ The certificate and CSR match!

✔ Certificate Modulus Hash:

cd78ed16b2abe2fa203e3f2e3499ee5c

✔ CSR Modulus Hash:

cd78ed16b2abe2fa203e3f2e3499ee5c

Enter your CSR:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDi1CCANMCAQAwgboXCAAJBgNVBAYTA1VMTQswCQYDVQQIEwVJNQEUMBIGA1UE
BxMLV0VVEJFUCk9VR0gxDDAKBgNVBAs0TAA0VRQzEELGAKGA1UECmQCSVh6eJTAjBgNV
BAMTFmFfQj1kLmVtYy5jb20kSTBhBgNVBAUTQGV1MDQ3
OTc0NDQxNDUyMjY2PhOTR1YWQxZjg1OHNMaNGI5NGF1OWV1MTgwYzdm6jhm8DIz
NDZiMjQ1ZTY5M2MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQAdeAxxp
xwITQ+hFXIbn39tXMRp6hR8xwR9+C86HwZ8zUHdY9VYsYC4B1gYMS6gFWQ2X0tD
vafFH7dwaNU0dp91aazECrF8vdpYyaU9pNi9akL3dFgAh27DJoJIN74wTzNB+UQM
XR7HB4X0YNJYQJIEJhI0SY6vseWE7VscW78jYRoRfQPVgyC4dFJJipeQiCyoUBY
OT425jTHgk1o7gme21WIELNX2kEJZozD9qU2LR/9GcGn4nB7A1bqmxCO/euKw982
1hhxyAN2B2SMs0RxCvGK8IoK5Nw9P7tRz3kJhpeX84wFwOPnMVveHcG8dCwa+6
yCf6gcJLG1bbX5p1AgMBAAGggYcwYQGC5qG5Ib3DQEJJDjF3M0UwJwYDVRO1BCAw
HgYIKwYBBQUHAEwDCCzGAQQAQBgjCUAqQUHhIAVwBlAGIAUwBlAHIAAqBlAHIAw
VRORBDYwNIIeV0VCKDEtDFEMDEtQ00xLmls4XMuZW1jLmNvbYU0bGF1Y3Vjb35p
c3VzLmVtYy5jb20wDQYJKoZIhvcNAQEFBQADggEBAEPcXlqgNRV3k38wVkoOcfQ
sy74JelK1ta5N1UYZtoDNquP+6Rd80kgjv8MpAmajU1M2th2NBfBk3eN2a7s31WP
Ick/J2kTReiStQjy888F1ffqQ48qsIKhArH1Zut+S/iWZ11eSh2CIGeH/75Jge
9UeTeI7S1keiJBRuMktnUQC0Mpmw1Wdpfva3MSiknAB5y0aDntGRgivr3pXQQ+4
eUVU99Bsc4Szb0cfqocfk/i/87BGec452/2988U71qZWbxwMEGzsMkqmiQUMu
EAbYm8NfFtn5b8I3CJuh368WyRmFQpA9tAj8yyLxNt2eFA7qKB6KY4nUBfNye4=
-----END CERTIFICATE REQUEST-----
```

解决方案3.比较来自Internet的任何CSR解码器的内容

步骤1.复制每个会话的证书详细信息，如下图所示。

```
http://www.mcafee.com/decoder/
CALO Project Squared Bookmarks Toolbar acumen TOOL My Work Zone - Cons... Luke Fayman - Physiot... GAMES

Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    79:38:79:ed:00:00:00:00:3c
  Signature Algorithm: sha1WithRSAEncryption
  Issuer:
    commonName           = sophia-WIN-3818JC3LM2A-CA
    domainComponent      = sophia
    domainComponent      = li
  Validity
    Not Before: Jan  4 05:02:45 2015 GMT
    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:
      47:45:4E:90:EC:74:6D:EB:D7:BE:96:CE:BA:51:DC:C7:C7:07:5D:72
    X509v3 Authority Key Identifier:
```

步骤2.在Notepad++等工具中将它们与此图中所示的“比较”插件进行比较。

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 Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
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: