

UCのCSRと証明書の不一致の確認

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[Cisco Communications Manager証明書管理](#)

[問題](#)

[CUCMでのCA署名付き証明書の一般的な方法](#)

[解決策1：ルート（またはlinux）でOpenSSLコマンドを使用する](#)

[解決策2.インターネットからの任意のSSL証明書キーマッチャの使用](#)

[ソリューション3.インターネットのAny CSR Decoderのコンテンツの比較](#)

概要

このドキュメントでは、認証局(CA)署名付き証明書がCisco Unified Application Serverの既存の証明書署名要求(CSR)と一致するかどうかを確認する方法について説明します。

前提条件

要件

X.509/CSRに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの内容は、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。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

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 and Presence
- Cisco Unified Unity Connection
- CUIS

- Cisco MediaEnce
- Cisco Unified Contact Center Express (UCCX)

背景説明

認証リクエストは、識別名、公開キー、および認証を要求するエンティティによって一括署名されたオプションの属性セットで構成されます。認証要求は、要求をX.509公開キー証明書に変換する認証局に送信されます。証明機関が新しく署名された証明書を返す形式は、このドキュメントの範囲外です。 PKCS #7メッセージが1つの可能性があります(RFC:2986)。

Cisco Communications Manager証明書管理

一連の属性を含めるという意図は、2つあります。

- 特定のエンティティに関するその他の情報、または後で証明書失効を要求できるチャレンジパスワードを提供するために。
- X.509証明書に含める属性を提供します。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ていません。

現在のCisco UCサーバでは、次の表に示すように、CSRに次の属性が必要です。

情報	説明
組織	組織単位
orgname	組織名
地域	組織所在地
state	組織状態
country	国番号は変更できません
代替ホスト名	代替ホスト名

問題

UCをサポートすると、CA署名付き証明書をUCサーバにアップロードできないケースが多く発生することがあります。署名付き証明書を作成するためにCSRを使用したユーザではないため、署名付き証明書の作成時に何が発生したかを常に特定することはできません。ほとんどのシナリオでは、新しい証明書の再署名に24時間以上かかります。CUCMなどのUCサーバには、証明書のアップロードが失敗した理由を特定するための詳細なログ/トレースはありませんが、エラーメッセージが表示されるだけです。この記事の目的は、UCサーバでもCAでも、問題を絞り込むことです。

CUCMでのCA署名付き証明書の一般的な方法

CUCMは、Cisco Unified Communicationsオペレーティングシステム(OS)証明書マネージャのGUIからアクセスできるPKCS#10 CSRメカニズムを使用して、サードパーティCAとの統合をサポートします。現在サードパーティCAを使用しているお客様は、Cisco CallManager、CAPF、IPSec、およびTomcat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[Identify]を変更します。

CSRを生成するためのCUCMサーバのIDは、次の図に示すようにset web-securityコマンドを使用して変更できます。

```
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
```

上記のフィールドにスペースがある場合は、図に示すようにコマンドを実行するために""を使用します。

```
admin:set web-security "Cisco Systems" "Cisco TAC" "St Leonard" NSW AU CUCM105.sophia.lf
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)? █
```

ステップ2：図に示すようにCSRを生成します。

Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate List

Generate New Upload Certificate/Certificate chain Download CTL Generate CSR

Generate Certificate Signing Request - Mozilla Firefox

https://10.66.90.50:8443/cmplatform/certificateGenerateNewCsr.do

Generate Certificate Signing Request

Generate CSR Close

Status

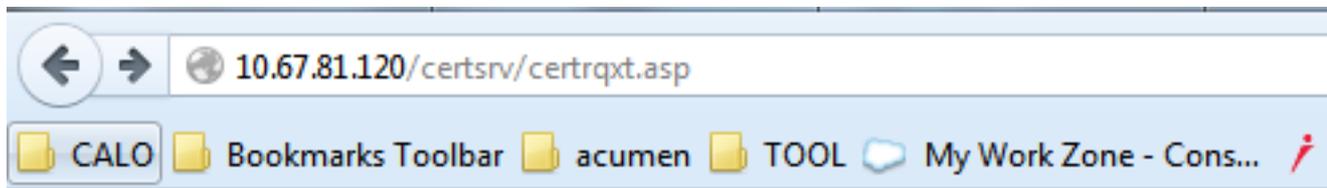
Warning: Generating a new CSR will overwrite the existing CSR

Generate Certificate Signing Request

Certificate Name*

*- indicates required item.

ステップ3:CSRをダウンロードし、図に示すようにCAによって署名されたCSRを取得します。



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  
eUVU99Bzc4SzbfcqfocfkI/i/87BGec453/Z988U  
EAbYmMNfFtn5b8I3CJuh368WyRmFQpA9tAj8yyLx  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

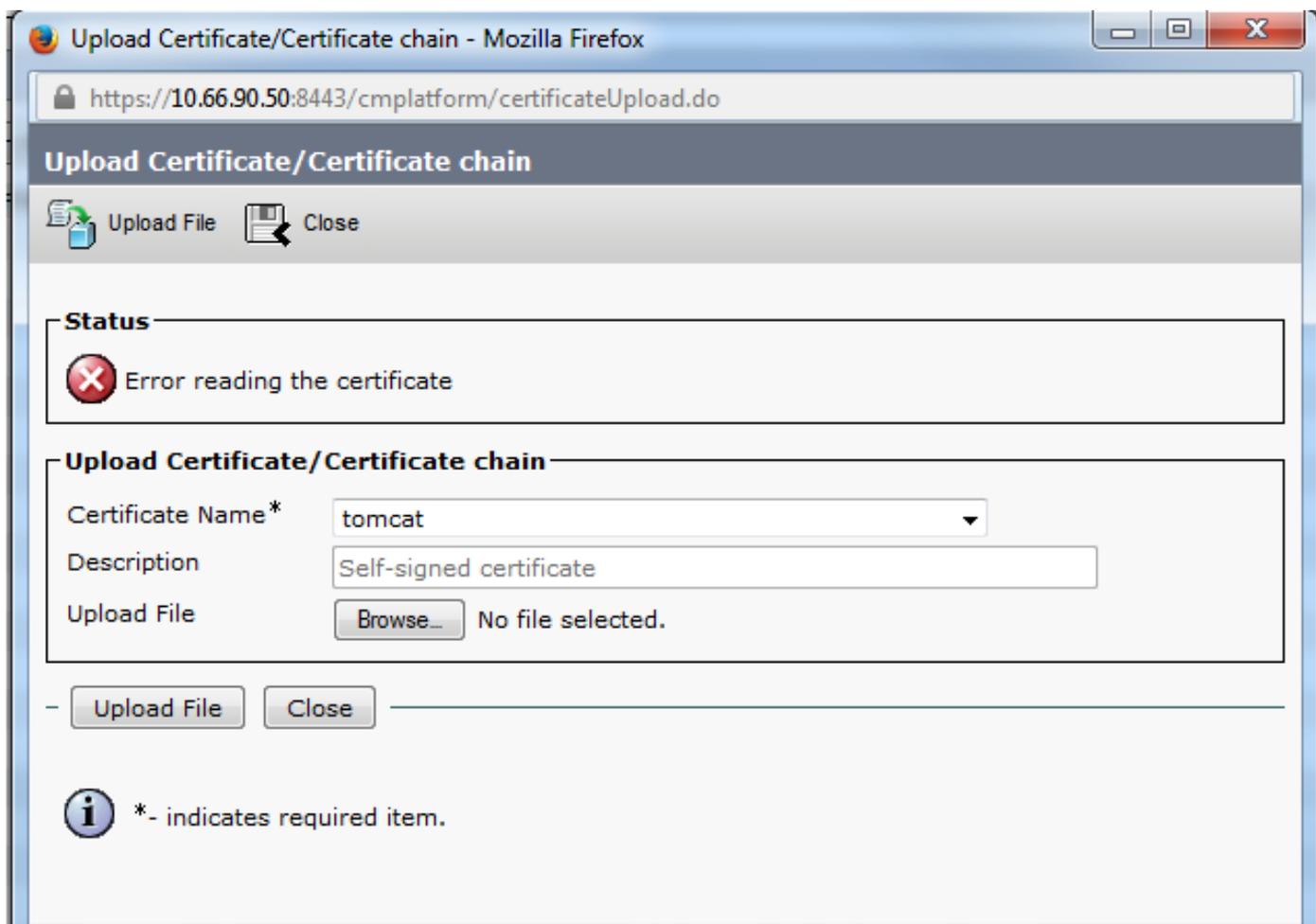
Additional Attributes:

Attributes:

Submit >

ステップ4:CA署名付き証明書をサーバにアップロードします。

CSRが生成され、証明書が署名された後、「Error reading the certificate」というエラーメッセージが表示されてアップロードに失敗した場合（次の図を参照）、CSRが再生成されたか、署名済み証明書自体が問題の原因であるかどうかを確認する必要があります。



CSRが再生成されたか、署名付き証明書自体が問題の原因であるかどうかを確認するには、3つの方法があります。

解決策1：ルート（またはlinux）でOpenSSLコマンドを使用する

ステップ1：ルートにログインし、図に示すようにフォルダに移動します。

```
[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：署名付き証明書をSecure FTP(SFTP)と同じフォルダにコピーします。SFTPサーバをセットアップできない場合は、図に示すように、TFTPフォルダのアップロードでもCUCMに証明書を取得できます。

```
[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.図に示すように、CSRのMD5と署名付き証明書を確認します。

```
[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]# █
```

解決策2.インターネットからの任意のSSL証明書キーマツチャの使用

What to Check

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

Enter your Certificate:

```
/RnBp+JwewNW6peQcF2riaFfNpYfYecgDdqdUmsjwvxihvCRKuTePT+7bUbEpCY
aZ1/OMBwaj5eFXHh3BuXQ1s/usgn+oHCSxtW21+aZQIDAQABo4ICDeCCAnMwEwYD
VR01BAAwCgYIKwYBBQUHAwEwDgYDVROFAQM/BAQDAgWgMD0GA1UdEQQ2MDSCHFdF
QjAaLWwRDAAxLUNRMS5pe3VwLmVtYy5jb22CFGwhYeN1Y20uaXN1ey51bW9uY29t
MBOGA1UdDgQWBBSScO++8bY+2naaA2ep/km4x89z29TAfBgNVHSMEGDAWgSTvo1P6
OP4LXm9RDv5N6eIMk8jnoFDCEB9QYDVROfBIMVMIN3MINFoIM6oIMJhoM6GRhoDev
Ly9DTj1ab2BoaWEtV010LINTMTbKQeSMITTJBLUNBLENOPVdJTI0zUzE4SkMaTE0y
QSkwDTj1DRFAzQ049UHV1bG1jJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
Q049Q29uZmlndXhhdG1vbixEQz1ab2BoaWEtREM9bGk/Y2VydG1maW9hdGV5ZXZv
Y2F0aW9uTG1sdD9iYXN1P29iamVjdENeYXNzPWNSTERpc3RyaWJ1dG1vb1BvaW50
MINJBggrSgEFTBQcBAQSBvDCBuTCBtgYIKwYBBQUIGARGGalsZGFwO18vLONOPXGv
cGhpYS1XSU4tMlMxOEpDM0xDMkEtQ0EzQ049Q1BLENOPVBIYmXpYyUyMzEt1eSUy
MfN1enZpY2V5LENOPVNIenZpY2V5LENOPUNvbmZpZ3V5YXRpb24eREM9c29waG1h
LERDPWxpP2NBQ2VydG1maW9hdGU/YmFzZTI9vYmplY3RDdGFzc1jZXJ0aWZpY2F0
aW9uQUV0aG9yaXRSMCEGCSzGAQQAQBgjcuAqQUHhIAVvB1AGIAUvB1AHIAAqB1AMIw
DQYJKoZIhvcNAQEFBQADggEBAIGQApf8G42xgvV/6ETyu2Xb+fvfi9UAMH13xLN
Xw81TgzodaRop8aVQvulE36b4nHRLwDAAAC0KwQu/XSUmX0m2qH7zDCXv83ycAT
gqoqMf64FdEkkQuux+C94W8sKLwqVWk1k1jDTYMiBvQSEU991NNAZ880bjbh4AeVR
q/mjAE/tylhjJ2LhpheuiMFbVRbr3axTie+M4DSccr/z0/D2i2xHdDvMrEuDN5L
seE28wbIQXN1cM3dodhpneQ8e06GRyNTDCxZ52p0/HiIhkkHg7028bQ5aN+rTH
8d0t7wrRCwoIB24ehzXwcdMpdYt4+ABSJkzQwvW2+4WY0=
-----END CERTIFICATE-----
```

✔ The certificate and CSR match!

✔ Certificate Modulus Hash:

cd78ed16b2abe2fa203e3f2e3499ee5c

✔ CSR Modulus Hash:

cd78ed16b2abe2fa203e3f2e3499ee5c

Enter your CSR:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDi1CCANMCAQAwgboXCAAJBgNVBAYTA1VMTQswCQYDVQQIEwVJNQEUMBIGA1UE
BxMLV0VVEJFUCk9VR0gxDDAKBgVBAoTA0VRQzEELGAKGA1UECmQCSVh6JTAjBgNV
BAMTFmFfQj1AbLWwRDAAxLUNRMS5pe3VwLmVtYy5jb20kSTBhBgVBAUTQGVIMDQ3
OTc0NDQxNDYyMjY2PhOTR1YWQxZjg1OHNMaNGI5NGF1OWV1MTgwYzdm6jhm6DIz
NDZiMjQ1ZTY5M2MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAAoIBAQAdeAxp
xWITQ+hFXIbn39tXMR6p6HR8xCR9+C86Wz8zUHDY9VYsYC4B1gYMS6gFWQ2X0tD
vafFH7dwaNU0dP91aazECrF8vdpYyaU9pMi9akL3dFgAh27DJoJIN74tZNB+UQM
XR7HB4X8YNJYQJIEJhI0SY6wseWE7VscW78jYRoRfQFVqyC4dFJJiPeQ1CyoUBV
OT425jTHgk1o7gme21WIELMX2kEJZorD9gU2LR/9GcGn4nB7A1bqmxCO/euKw982
1hhxyAN2B25Mz0NxCvGRG8IoK5Nw9P7tRz8kJhpeX84wFwOPnMVceHcG8dCNa+6
yCf6gcJLG1bbX5p1AgMBAAGggYcwgYQGC5qG5Ib3DQEJJDjF3M0UwJwYDVRO1BCAw
HgYIKwYBBQUHAwEGCCsGAQUFBwMCEBgggrSgEFTBQcDBTALBgNVHSEBAMCA7gwPQYD
VRORBDYwNIIeV0VCKDEtTDfEMDEtQ00xLmls4XMaZW1jLmNvbYUuBGF1Y3Vjb35p
c3VwLmVtYy5jb20wDQYJKoZIhvcNAQEFBQADggEBAEPcXlqgNRV3kSvMvkoCcfQ
sy74JelK1ea5N1UYZtoDNquP+6Rd80kGjv8MpAmajU1Mzth2NBf6X3tN2a7e31WP
Ick/J2kTReiStQjy888F1ffqQ48qsIKHArH1Zut+S/iWZ11eSh2CIGeH/75Jge
9UeTeI7S1keiJBRuMktnUQC0Mpmw1Wdpfva3MSiknAB5y0aDntGRgivr3pXQQ+4
eUVU99Bsc4SzbefqfoekI/i/87BGec452/2988U71qZWbxwMEGzsmkqmiQUMu
EAbYm8NfFtn5b8I3CJuh368WyRmFQpA9tAj8yyLxNt2eFA7qKB6KY4nUBfNyee4=
-----END CERTIFICATE REQUEST-----
```

ソリューション3.インターネットのAny CSR Decoderのコンテンツの比較

ステップ1: 次の図に示すように、それぞれのセッション証明書の詳細情報をコピーします。

```
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:
```

ステップ2：次の図に示すように、Notepad++などのツールでCompareプラグインと比較します。

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
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: