

UC のための CSR および認証 ミスマッチを確認する方法

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[Cisco 通信マネージャ証明書管理](#)

[問題](#)

[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](#)

[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 デコーダからのコンテンツを比較しま](#)
[す](#)

[Cisco サポート コミュニティ - 特集対話](#)

概要

この資料に認証局 (CA) 署名入り認証が Cisco Unified アプリケーションサーバのための既存の認証 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

X.509/CSR のナレッジがあること Cisco recommends。

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。

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、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

認証 要求は識別名、公開キーおよび認証を要求するエンティティによって属性の、一まとめに署名されて設定される 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 通信マネージャ証明書管理

一組の属性が含まれている意図は二重です:

- 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 証明書の失効かもしれないチャレンジ パスワードを提供するため。
- 属性を X.509 認証の包含に提供するため。 電流 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 | 組織の位置 |
| 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 |

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
- Unity Cisco Unified 接続
- CUIS
- Cisco Meidasence
- [Cisco Unified Contact Center Express \(UCCX \)](#)

問題

UC のサポートで、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います。 署名入り認証を作成するのに 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間に常に識別できません。 ほとんどのシナリオでは、新しい認証を再契約して 24 時間以上かかります。 CUCM のような UC サーバは認証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助けるように意図されています。

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 メカニズムの使用によってサードパーティ 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 Unified CallManager、CAPF、IPSec および Tomcat のための認証を発行するのに 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

CSR を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によって生成する CUCM サーバの識別は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、使用して下さいか。か。コマンドをとって実現させるため:

```
admin:set web-security "Cisco Systems" "Cisco TAC" "St Leonard" NSW AU CUCM105.sophia.11
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
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. CSR を生成して下さい。

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

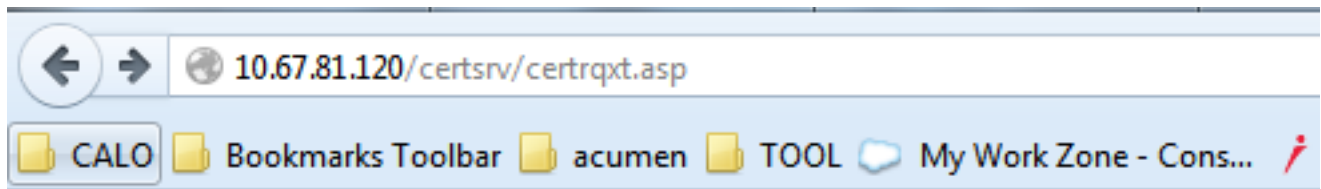
 Warning: Generating a new CSR will overwrite the existing CSR

Generate Certificate Signing Request

Certificate Name*

 *- indicates required item.

ステップ 3. CSR をダウンロードし、CA によって署名されて得て下さい。



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

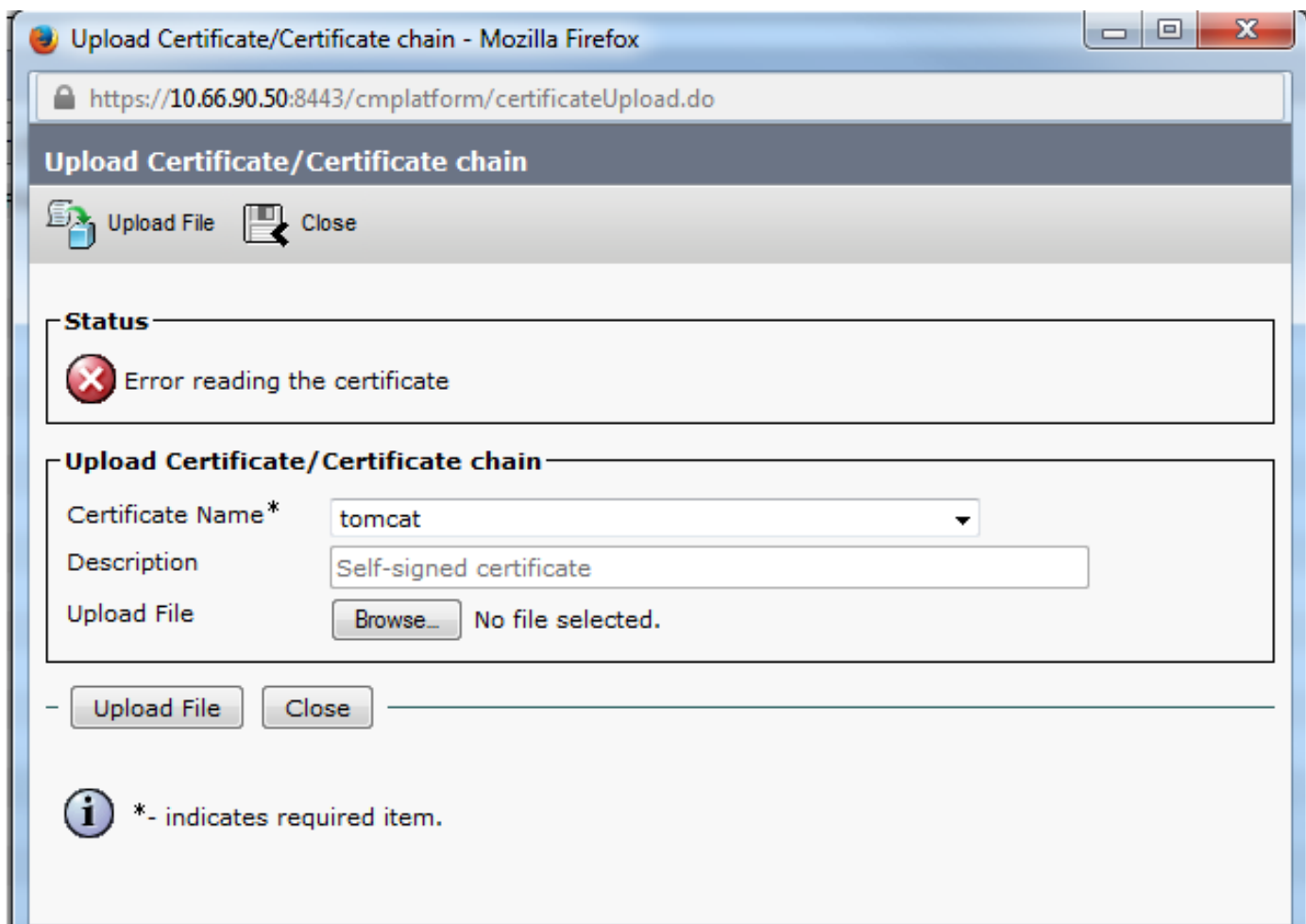
Additional Attributes:

Attributes:

Submit >

ステップ 4. サーバに CA署名付き証明書をアップロードして下さい。

CSR が生成されればおよび認証が署名すれば、エラーメッセージ エラーとそれをアップロードし認証を読んでいれば (このイメージに示すように) 損う場合、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

1. ルートへのログインおよびフォルダへのナビゲート。

```
[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. セキュア FTP (SFTP) を使用して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 フォルダへそれをアップロードすることはまた CUCM に認証を得ます。

```
[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. 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

What to Check

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

Enter your Certificate:

```
/RnBp+JwewNW6peQcF2riaFfNpYyccgDdqdUmsjwvxihvCRKuTePT+7bUbEpCY
aZ1/OMBwaj5eFXHh3BuXQ1s/usgn+oHC9xtW21+aZQIDAQABo4ICDeCCAnMwEwYD
VR01BAAwCgYIKwYBBQUHAwEwDgYDVROFAQM/BAQDAgWgMD0GA1UdEQQ2MDSCHFdF
QjAaLUwRDAxLUNRMS5pe3VwLmVtYy5jb22CFGwhYeN1Y20uaXN1ey51bW9uY29t
MBOGA1UdDgQWBBSco++8bY+2naaA2ep/km4x89z29TAfBgNVHSMEGDAWgSTvo1P6
OP4LXm9RDv5N6eIMk8jnoFDCEB9QYDVROfBIMVMIN3MINFoIM6oIMJhoM6GRhoDev
Ly9DTj1ab2BoaWEtV010LINTMTkRQeBM7TJBLUNBLENOPVdJTi0aUaE49kMaTE0y
QSkxDTj1DRFAaQ0490UHV1bG1jJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
Q049Q29uZmlndXhhdG1vbixEQe1ab2BoaWEtREM9bGk/Y2VydG1maW9hdGV5ZXZv
Y2F0aW9uTG1sdD9iYXN1P29iamVjdENaYXNzPWNSTERpc3RyaWJ1dG1vb1BvaW50
MINJBggr5gEFTBQcBAQSBvDCBvICBtYIKwYBBQUIGARAGga1zGFvO18vLONOPXGv
cGhpYS1X3U4tM1MxOEppDM0xDMkEtEQEaQ049Q1BLENOPVBiYmXpYyUyMzE1e3Uy
MfN1enZpY2VtLENOPVNi1enZpY2VtLENOPVNi1enZpY2VtYXRpb24eREM9c29waG1h
LERDPWxpP2NBQ2VydG1maW9hdGU/YmFzZTI9vYm1Y3RD0GFcc1jZXJ0aWZpY2F0
aW9uQUV0aG9yaXRSMCEGCS8GAQQBgjcuUAgQUHhIAVvB1AGIAUvB1AHIAAgB1AHIAw
DQYJKoZIhvcNAQEFBQADggEBAIGQApE6G42xgvV/6ETyu2Xb+fVfi9UAMH13xLN
Xw81TgzodaRop8aVQvulE36b4nHRLvDCAAC0KwQu/XSUmX0m2qH7zDCXv83ycAT
gqoqMf64FdEkkQuux+C94W8eKLwqVWk1k1jDTYMiBvQSEU991NNAZ880bjbh4AeVR
q/mjAE/tylhjJ2LhpheuiMFbVRbr3axTie+M4DSccr/z0/D2i2xHdDvMrEuDN5L
seE28wb1QxKHicM3dodhpneQ8e06GRyNTDCxZ52p0/HiIhkkHg7028bQ5aN+sRTH
8d0t7wrRCwoIB24ehzXwcdMpkDyt4+ABSJkzQwvW2+4WY0=
-----END CERTIFICATE-----
```

✔ The certificate and CSR match!

✔ Certificate Modulus Hash:

cd78ed16b2abe2fa203e3f2e3499ee5c

✔ CSR Modulus Hash:

cd78ed16b2abe2fa203e3f2e3499ee5c

Enter your CSR:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDi1CCANMCAQAwgboXCAAJBgNVBAYTA1VMTQswCQYDVQQIEwJNQTUUMBIGA1UE
BxMLV0VUVEJFUCk9VR0gxDDAKBgNVBAs0TAA0VW9QaE1MAkGA1UECmMCSTV6eXJhYjEg
BAMHMFdFQjAaLUwRDAxLUNRMS5pe3VwLmVtYy5jb20kSTBhBgNVBAUTQGV1MDQ3
OTc0NDQxNDUyMjY2PhOTR1YWQxZjg1OHNMaNGI5NGF1OWV1MTgwYzdm6jhm6DIa
NDZiMjQ1ZTY5M2MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAAIBAQDzAaxp
xWITQ+hFXIbn39tXMR6p6HR8xCR9+C86HwZ8zUHdY9VYaYC4B1gYMS6gFWQ2X0tD
vafFH7dwaNU0dp91aazECrF8vdpYyaU9pNi9akL3dFgAh27DJoJIN74wTzNB+UQM
XR7HB4X0YNJYQJIEJhI03Y6vseWE7VseW78jYRoRfQPVgyC4dFJJ1pQ1CyoUBV
OT425jTHgk1o7gme21WIELMX2kEJZorD9gU2LK/9Gc6n4nB7A1bqmxCO/euKw982
1hhxyAN2B25M8ONrCvGRG8IoK5Nw9P7tRz3kJhpeX84wFwOPnMvceHcG5dCwA+6
yCf6gcJLG1bbX5p1AgMBAAGggYcwYQGC5qG5Ib3DQEJDjF3M0UwJwYDVRO1BCAw
HgYIKwYBBQUHAwEGCC8GAQQFBSwMCEBgggrBgEFBQcDBTALBgNVHSEBAMCA7gwPQYD
VRORBDYwNIIeV0V0KDEtDFEMDEtQ00xLmls4X0uZW1jLmNvbYU1U0GF1Y3Vjb35p
c3VwLmVtYy5jb20wDQYJKoZIhvcNAQEFBQADggEBAEPcXlqgNRV3kSvMvkoCcfQ
sy74JelK1ta5N1UYZtoDNquP+6Rd80kGjv8MpAmajU1M2th2NBf6X3eN2a7e31WP
Ick/J2kTReiStQjy888F1ffqQ48qsIKHArH1Zut+S/iWZ11eSh2CIGeR/75Jge
9UeTeI73IkeiJBRuMktenUQC0Mpmw1WDPfva3MSiknAB5y0aDntGRgivr3pXQQ+4
eUVU99Bc4Szbefqfoefki/i/87BGec452/2988U71qZWbxwMEGsaMkqmiQUMu
EAbYm8NfFen5b8I3Cjuh368WyRmFQpA9tAj8yyLxNt2eFA7qKB6XY4nUBfNyee4=
-----END CERTIFICATE REQUEST-----
```

ソリューション 3.はインターネットからのあらゆる CSR デコーダからのコンテンツを比較します

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 認証 詳細な情報をコピーして下さい。


```
https://www.ssl.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:
```

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 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: