

Verifica mancata corrispondenza di CSR e certificati per UC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Gestione certificati Cisco Communications Manager](#)

[Problema](#)

[Procedura generale per i certificati firmati CA in CUCM](#)

[Soluzione 1. Utilizzare il comando OpenSSL nella radice \(o linux\)](#)

[Soluzione 2. Utilizzare qualsiasi strumento di ricerca delle chiavi dei certificati SSL da Internet](#)

[Soluzione 3. Confronto dei contenuti da qualsiasi decoder CSR da Internet](#)

Introduzione

In questo documento viene descritto come identificare se il certificato firmato dall'Autorità di certificazione (CA) corrisponde alla richiesta di firma del certificato (CSR) esistente per i Cisco Unified Application Server.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di X.509/CSR.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified IM e Presence
- Cisco Unified Unity Connection

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

Premesse

Una richiesta di certificazione è costituita da un nome distinto, una chiave pubblica e un insieme facoltativo di attributi firmati collettivamente dall'entità che richiede la certificazione. Le richieste di certificazione vengono inviate a un'autorità di certificazione che le trasforma in un certificato a chiave pubblica X.509. In quale formato l'autorità di certificazione restituisce il certificato appena firmato non rientra nell'ambito del presente documento. Un messaggio PKCS #7 è una possibilità. (RFC:2986).

Gestione certificati Cisco Communications Manager

L'intenzione di includere una serie di attributi è duplice:

- Per fornire altre informazioni su una determinata entità o una password di richiesta con cui l'entità può in seguito richiedere la revoca del certificato.
- Per fornire attributi da includere nei certificati X.509. I server UC correnti non supportano una password di richiesta.

Gli attuali server Cisco UCS richiedono questi attributi in un CSR, come mostrato nella tabella seguente:

Informazioni	Descrizione
orgunit	unità organizzativa
nomeorganizzazione	nome organizzazione
località	sede dell'organizzazione
state	stato dell'organizzazione
paese	impossibile modificare il codice del paese
nomehostalternativo	nome host alternativo

Problema

Quando si supporta il certificato UC, è possibile che si verifichino molti casi in cui il certificato firmato dalla CA non può essere caricato sui server UC. Non è sempre possibile identificare ciò che si è verificato al momento della creazione del certificato firmato, poiché non si è la persona che ha utilizzato il CSR per creare il certificato firmato. Nella maggior parte dei casi, la rifirma di un nuovo certificato richiede più di 24 ore. I server UC, ad esempio CUCM, non dispongono di un log/trace dettagliato che consenta di identificare il motivo per cui il caricamento del certificato non riesce, ma forniscono semplicemente un messaggio di errore. L'intenzione di questo articolo è di limitare il problema, che si tratti di un server UC o di un problema di CA.

Procedura generale per i certificati firmati CA in CUCM

CUCM supporta l'integrazione con CA di terze parti tramite un meccanismo CSR PKCS#10 accessibile dall'interfaccia utente di Cisco Unified Communications Operating System Certificate Manager. I clienti che attualmente utilizzano CA di terze parti devono utilizzare il meccanismo CSR per rilasciare certificati per Cisco CallManager, CAPF, IPsec e Tomcat.

Passaggio 1. Modificare l'identificatore prima di generare il CSR.

L'identità del server CUCM per generare un CSR può essere modificata con il comando **set web-security** come mostrato nell'immagine.

```
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
```

Se nei campi sopra indicati è presente spazio, usare "" per ottenere il comando come mostrato nell'immagine.

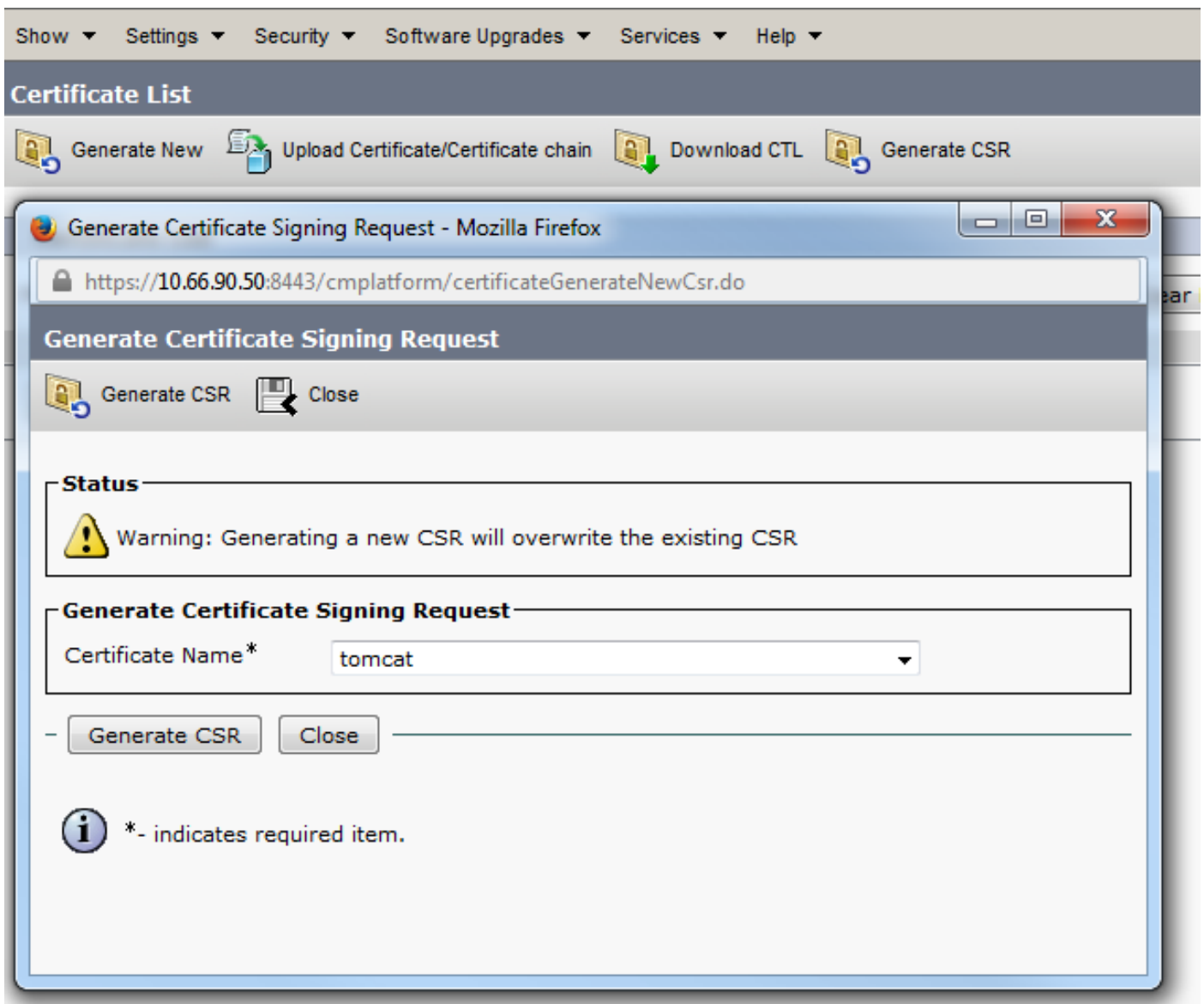
```
admin:set web-security "Cisco Systems" "Cisco TAC" "St Leonard" NSW AU CUCM105.sophia.11
WARNING: Country code can not be changed.
country code for existing web-security is : AU

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.

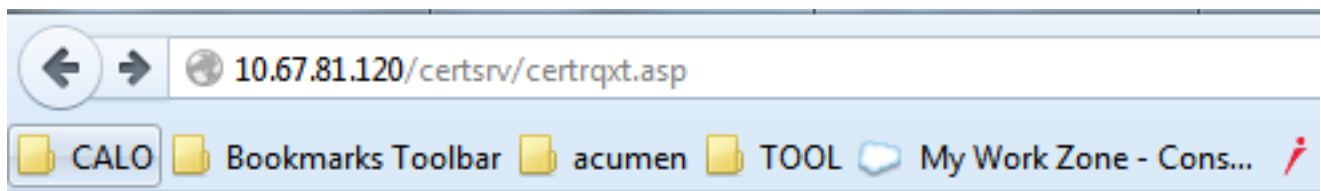
Regenerating web security certificates please wait ...

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

Passaggio 2. Generare il CSR come illustrato nell'immagine.



Passaggio 3. Scaricare il CSR e farlo firmare dall'autorità di certificazione, come mostrato nell'immagine.



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

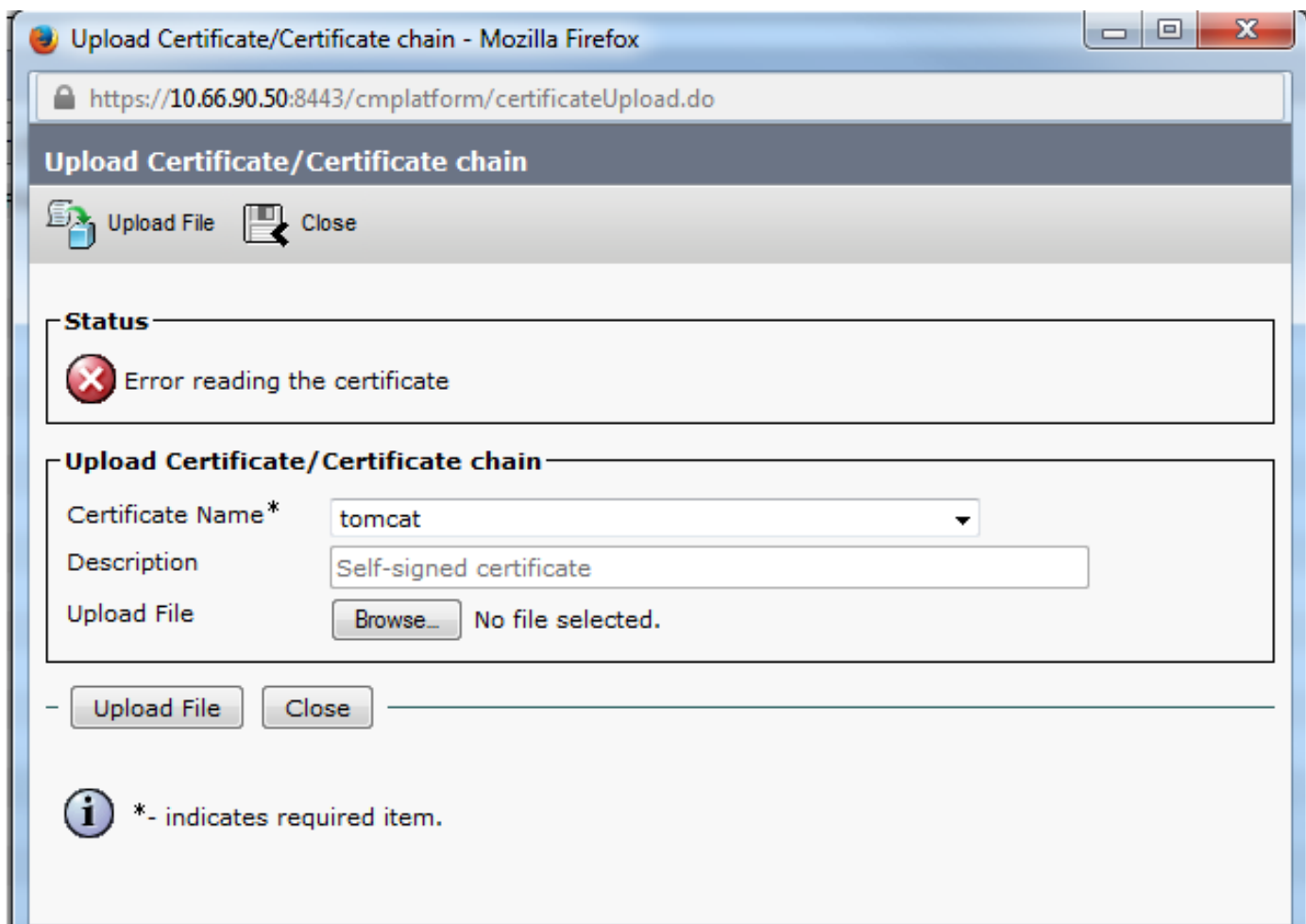
Additional Attributes:

Attributes:

Submit >

Passaggio 4. Caricare il certificato firmato dalla CA nel server.

Dopo aver generato il CSR e firmato il certificato e se non si riesce a caricarlo con il messaggio di errore "Error reading the certificate" (Errore durante la lettura del certificato), come mostrato nell'immagine, è necessario verificare se il CSR è stato rigenerato o se il certificato firmato è la causa del problema.



Esistono tre modi per verificare se il CSR viene rigenerato oppure se il certificato firmato è la causa del problema.

Soluzione 1. Utilizzare il comando OpenSSL nella radice (o linux)

Passaggio 1. Accedere alla directory principale e passare alla cartella come mostrato nell'immagine.

```
[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]#
```

Passaggio 2. Copiare il certificato firmato nella stessa cartella con SFTP (Secure FTP). Se non si riesce a configurare un server SFTP, il caricamento nella cartella TFTP può anche ottenere il certificato sul CUCM, come mostrato nell'immagine.

```
[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. Controllare il MD5 per il CSR e il certificato firmato, come mostrato nell'immagine.

```
[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]# █
```

Soluzione 2. Utilizzare qualsiasi strumento di ricerca delle chiavi dei certificati SSL da Internet

What to Check

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

Enter your Certificate:

```
/RnBp+JwewNw6peQcF2rieFENpYecgDdqdUmsjwvxihvCRKuTePT+7bUbEpCY
aZ1/OMBwaj5eFXHh3BuXQ1s/usgn+oHCSxtW21+aZQIDAQABo4ICdeCCAnMwEwYD
VR01BAAwCgYIKwYBBQUHAEwEwDgYDVROFAQM/BAQDAgWgMD0GA1UdEQQ2MDSCHFdF
QjAaLUwXRDAxLUNRMS5pe3VwLmVtYy5jb2ZCFGwhYeN1Y20uaXN1ey51bW9uY29t
MBOGA1UdDgQWBBSco++8bY+2naaA2ep/km4x89z29TAfBgNVHSMGDAWgSTvo1P6
OP4LXm9RDv5N6eIMk8jaoEDCB9QYDVROfBIMVMIN3MINFoIM6oIMJhoM6GRhoDev
Ly9DTj1ab2BoaWEtV01OLINTMTkRQeBM7TJBLUNBLENOFVdJTI0aUzE4SkmTE0y
QSkwDTj1DRFAeQ0490UHV1bG1jJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
Q049Q29uZmlndXhhdG1vbixEQe1ab2BoaWEtREM9bGk/Y2VydG1maW9hdGV5ZXZv
Y2F0aW9uTG1sdD9iYXN1P29iamVjdENeYXNzPWNSTERpc3RyaWJ1dG1vb1BvaW50
MINJBggrSgEFTBQeBAQSBvDCBuTCBtgYIKwYBBQUHGAAGgalsZGFwO18vLONOPXGv
cGhpYS1XSU4tM1MxOEpDM0xDMkEeQ0EzQ049Q1BLENOFVBIYmXpYyUyMTEleSUy
MFI1enZpY2V5LENOFVNI1enZpY2V5LENOFVNI1enZpY2V5YXRpb24eREM9c29waG1h
LERDPWxpP2NBQ2VydG1maW9hdGU/YmFzZi9vYm1Y3RD0GFccs1jZXJ0aWZpY2F0
aW9uQUV0aG9yaXRSMCEGCSsGAQQGbgJcUAQQUHhIAVvB1AGIAUvB1AHIAAgB1AHIAw
DQVJKoZIhvcNAQEFBQADggEBAIGQApE6G42xgvV/6ETyuZXb+fVfi9UAMH13xLN
Xw8iTGzodaRop8aVQvulE36b4nHRLwDCAAC0KwQu/XSUmX0m2qH7zDCXv83ycAT
gqoQMF64FdEkkQuux+C94W8eKLWqVWk1k1jDTYMiBvQSEU991NNAZ880bjbh4AeVR
q/mjAE/tylhjJ2LhpheuiMFbVRbr3axTie+M4DSccr/z0/D2i2xHdDvMrEuDN5L
seE28wbIQXN1cM3dodhpneQ8e06GRyNTDCxZ52p0/HiIhkkHg7028bQ5aN+eRTH
8d0t7wrRCwoIB24ehzXwcdHpkDyt4+ABSJkzQwvW2+4WY0=
-----END CERTIFICATE-----
```

✔ The certificate and CSR match!

✔ Certificate Modulus Hash:

cd78ed16b2abe2fa203e3f2e3499ee5c

✔ CSR Modulus Hash:

cd78ed16b2abe2fa203e3f2e3499ee5c

Enter your CSR:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDi1CCANMCAQAwgboXCAAJBgNVBAYTA1VMTQswCQYDVQQIEwVJNQEUMBIGA1UE
BxMLV0VVEJF0k9VR0gxDDAKBgNVBAoTA0VRQzEELGAKGA1UECmQCSV6xJTAjBgNV
BAMTFdFQjAaLUwXRDAxLUNRMS5pe3VwLmVtYy5jb20kSTBHBG9VBAUTQGVIMDQ3
OTc0NDQxNDUyMjE3Y2FhOTRlYWQxZjg1OHNMaNGI5NGF1OWV1MTgwYzdm6jhm6DIz
NDZiMjQ1ZTY5M2MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQAdeAxxp
xwITQ+hFXIbn39tXRRM6pHR8xcR9+C86HwZ8zUHdY9VYaYC4B1gYMS6gPWQ2X0tD
vafFH7dwaNU0dp91aazECrF8vdpYyaU9pNi9akL3dFgAh27DJoJIN74wTzNB+UQM
XR7HB4X0YNJYQJIEJhI0SY6wseWE7VscW78jYRoRfQPVgyC4dFJJipeQiCyoUBY
OT425jTHgk1o7gme21WIELMX2kEJZorD9gU2LR/9GcGn4nB7A1bqmxCO/euKw982
1hhxyAN2B2SMs0NrcCvGRG8IoK5Nw9P7tRr3kJhpeX84wFwOPnMVceHcG6dCNa+6
yCf6gcJLG1bbX5p1AgMBAAGggYcwYQGC5qG5Ib3DQEJJDjF3MNUvJwYDVRO1BCAw
HgYIKwYBBQUHAEwECCsGAQQFBSwMCSBgggrSgEFTBQeDBTALBgNVHSMGEBAMCA7gwPQYD
VRORBDYwNIIeV0VCKDEtTDfEMDEtQ00xLmls4X0uZW1jLmNvbYUuBGF1Y3Vjb35p
c3VwLmVtYy5jb20wDQVJKoZIhvcNAQEFBQADggEBAEPcXlqgNRV3kSvMvkoOcfQ
sy74JelK1ea5N1UYZtoDNquP+6Rd80kgjv8MpAmajU1Mzth2NBf6X3eN2a7e31WP
Ick/J2kTReiStQjy888F1ffqQ48qsIKhArH1Zut+S/iWZ1eSh2CIGeH/75Jge
9UeTeI7S1keiJBRuMktnUQC0Mpmw1Wdpfva3MSiknAB5y0aDntGRgivr3pXQQ+4
eUVU99Bsc4Szb0cfqocfk/i/87BGec452/2988U71qZWbxwMEGsaMkqmiQUMu
EAbYm8NFtc5b8I3Cjuh368WyRmFQpA9tAj8yyLxNt2eFA7qKB6KY4nUBfNye4=
-----END CERTIFICATE REQUEST-----
```

Soluzione 3. Confronto dei contenuti da qualsiasi decoder CSR da Internet

Passaggio 1. Copiare le informazioni dettagliate sul certificato della sessione per ciascuno di essi, come illustrato in questa immagine.


```
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:
```

Passaggio 2. Confrontarli in uno strumento quale Blocco note++ con il plug-in Confronta, come illustrato in questa immagine.

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: