

Verificar la discordancia de CSR y de certificado para UC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Administración de certificados de Cisco Communications Manager](#)

[Problema](#)

[Práctica general para certificados firmados por CA en CUCM](#)

[Solución 1. Utilice el comando OpenSSL en root \(o linux\)](#)

[Solución 2. Utilizar cualquier coincidencia de clave de certificado SSL desde Internet](#)

[Solución 3. Comparar contenido de cualquier descodificador CSR desde Internet](#)

Introducción

Este documento describe cómo identificar si el certificado firmado por la Autoridad de Certificación (CA) coincide con la solicitud de firma de certificado (CSR) existente para los servidores de aplicaciones de Cisco Unified.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de X.509/CSR.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified IM and Presence
- Conexión de Cisco Unified Unity

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

Antecedentes

Una solicitud de certificación consta de un nombre distinguido, una clave pública y un conjunto opcional de atributos firmados colectivamente por la entidad que solicita la certificación. Las solicitudes de certificación se envían a una entidad certificadora que transforma la solicitud en un certificado de clave pública X.509. En qué forma devuelve la autoridad de certificación el certificado recién firmado está fuera del alcance de este documento. Un mensaje PKCS #7 es una posibilidad.(RFC:2986).

Administración de certificados de Cisco Communications Manager

La intención de incluir un conjunto de atributos es doble:

- Para proporcionar otra información sobre una entidad dada, o una contraseña de impugnación por la cual la entidad pueda solicitar posteriormente la revocación del certificado.
- Para proporcionar atributos para su inclusión en certificados X.509. Los servidores de Unified Communications (UC) actuales no admiten una contraseña de desafío.

Los servidores Cisco UC actuales requieren estos atributos en un CSR, como se muestra en esta tabla:

Información	Descripción
orgunit	unidad organizativa
orgname	nombre de la organización
localidad	ubicación de la organización
estado	estado de organización
país	no se puede cambiar el código del país
nombre de host alternativo	nombre de host alternativo

Problema

Cuando admite UC, puede encontrar muchos casos en los que el certificado firmado por la CA no se puede cargar en los servidores de UC. No siempre puede identificar qué ha ocurrido en el momento de la creación del certificado firmado, ya que no es usted la persona que utilizó el CSR para crear el certificado firmado. En la mayoría de los casos, la refirma de un nuevo certificado tarda más de 24 horas. Los servidores de UC como CUCM no tienen registro/seguimiento detallado para ayudar a identificar por qué falla la carga del certificado, pero simplemente dan un mensaje de error. La intención de este artículo es reducir el problema, ya sea un servidor de UC o un problema de CA.

Práctica general para certificados firmados por CA en CUCM

CUCM admite la integración con CA de terceros mediante el uso de un mecanismo CSR PKCS#10 al que se puede acceder desde la GUI del administrador de certificados del sistema operativo Cisco Unified Communications. Los clientes que actualmente utilizan CA de terceros

deben utilizar el mecanismo CSR para emitir certificados para Cisco CallManager, CAPF , IPsec y Tomcat.

Paso 1. Cambie la ID antes de generar el CSR.

La identidad del servidor CUCM para generar una CSR puede ser modificada con el uso del comando **set web-security** como se muestra en esta imagen.

```
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
```

Si tiene espacio en los campos anteriores, utilice "" para alcanzar el comando como se muestra en la imagen.

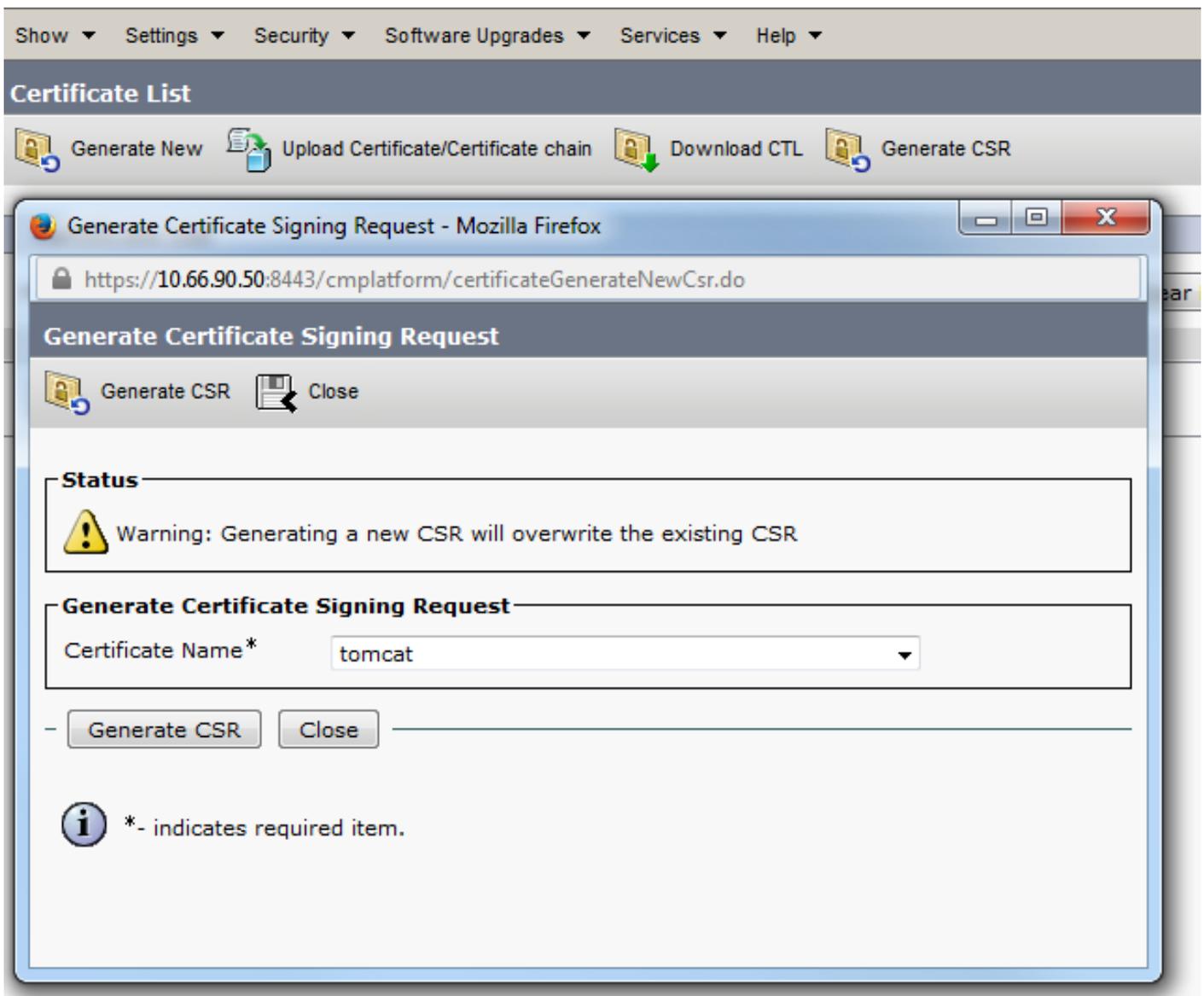
```
admin:set web-security "Cisco Systems" "Cisco TAC" "St Leonard" NSW AU CUCM105.sophia.lf
WARNING: Country code can not be changed.
Country code for existing web-security is : AU

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 o
enerate these self-signed certificates to update them.

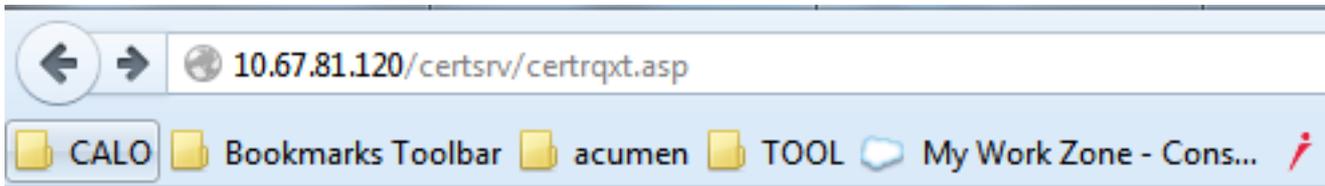
Regenerating web security certificates please wait ...

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

Paso 2. Genere CSR como se muestra en la imagen.



Paso 3. Descargue el CSR y consiga que lo firme la CA como se muestra en la imagen.



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

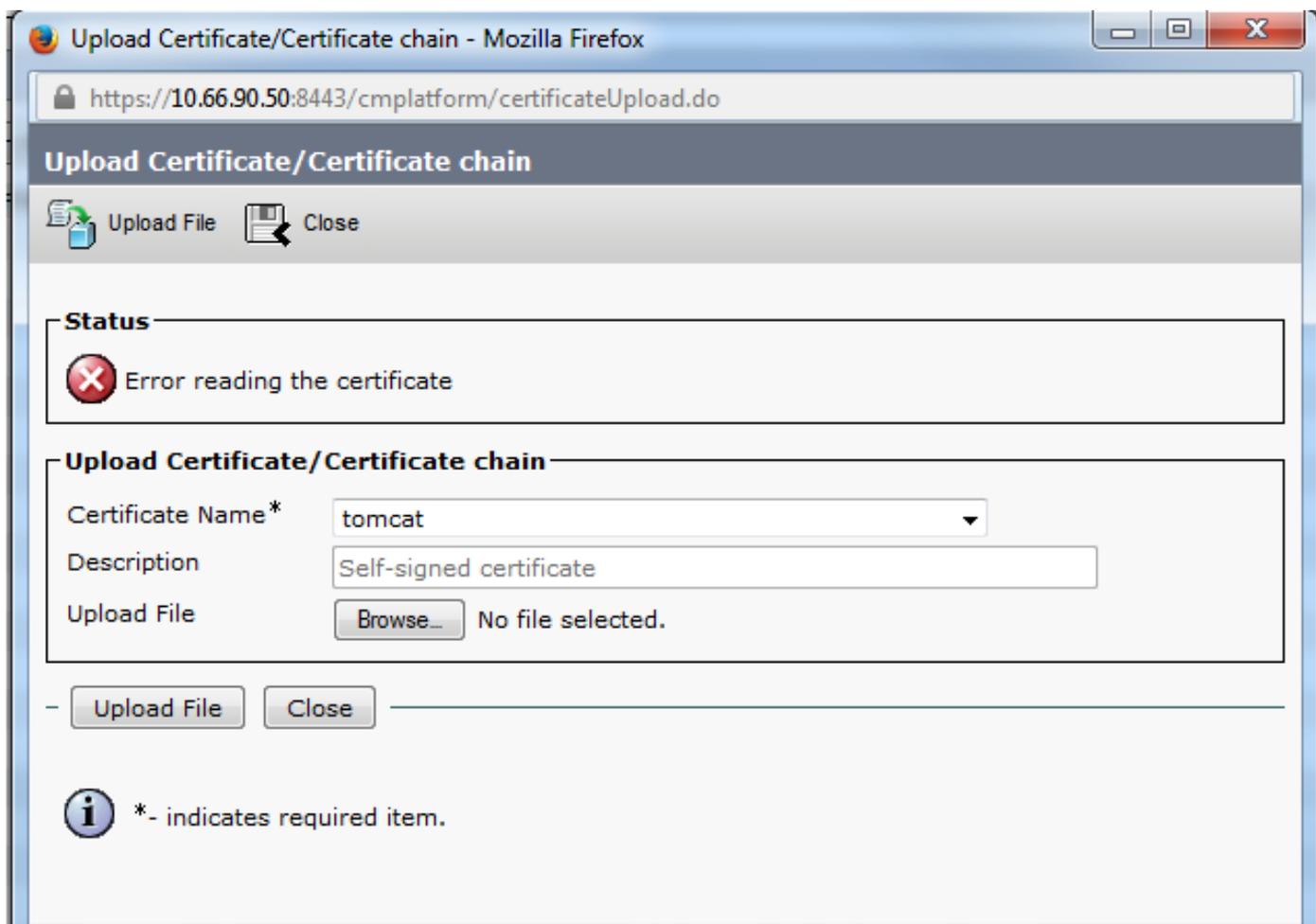
Additional Attributes:

Attributes:

Submit >

Paso 4. Cargue el certificado firmado por CA en el servidor.

Una vez que se genera el CSR y se firma el certificado y si no se lo carga con un mensaje de error "Error al leer el certificado" (como se muestra en esta imagen), debe verificar si el CSR se regenera o si el certificado firmado es la causa del problema.



Hay tres maneras de verificar si el CSR se regenera o el certificado firmado en sí es la causa del problema.

Solución 1. Utilice el comando OpenSSL en root (o linux)

Paso 1. Inicie sesión en la raíz y desplácese a la carpeta como se muestra en la imagen.

```
[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]#
```

Paso 2. Copie el certificado firmado en la misma carpeta con Secure FTP (SFTP). Si no puede configurar un servidor SFTP, entonces la carga en la carpeta TFTP también puede obtener el certificado en el CUCM como se muestra en la imagen.

```
[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. Verifique el MD5 para el CSR y el certificado firmado como se muestra en la imagen.

```
[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]# █
```

Solución 2. Utilizar cualquier coincidencia de clave de certificado SSL desde 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+JwewNw6peQcF2riaFENpYecgDdqdUmsjwvxihvCRKuTePT+7bUbEpCY
aZ1/OMBwaj5eFXHh3BuXQ1s/usgn+oHCSxtW21+aZQIDAQABo4ICDeCCAnMwEwYD
VR01BAAwCgYIKwYBBQUHAEwDgYDVROFAQM/BAQDAgWgMD0GA1UdEQQ2MDSCHFdF
QjAaLUwXRDAxLUNRMS5pe3VwLmVtYy5jb22CFGwhYeN1Y20uaXN1ey51bW9uY29t
MBOGA1UdDgQWBBSco++8bY+2naaA2ep/km4x89z29TAfBgNVHSMEGDAWgSTvo1P6
OP4LXm9RDv5N6eIMk8jaoEDCB9QYDVROfBIBVMIN3MINFoIM6oIMJhoMGRhoDev
Ly9DTj1ab2BoaWEtV010LINTMTkRQeMNTTJBLUNBLENOFVdJTI0aUzE4SkmTE0y
QSkwDTj1DRFAaQ049UHV1bG1jJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
Q049Q29uZmlndXhhdG1vbixEQe1ab2BoaWEtREM9bGk/Y2VydG1maW9hdGV5ZXZv
Y2F0aW9uTG1sdD9iYXN1P29iamVjdENaYXNzPWNSTERpc3RyaWJ1dG1vb1BvaW50
MINJBggrSgEFTBQcBAQSBvDCBuTCBtgYIKwYBBQUHGAHgga1eZGFwO18vLONOPXGv
cGhpYS1XSU4tM1MxOEppDM0xDMkEeQ0EzQ049Q1BLENOFVBIYmXpYyUyMTEleSUy
MFI1enZpY2V5LENOFVNI1enZpY2V5LENOFVNI1enZpY2V5YXRpb24eREM9c29waG1h
LERDPWxpP2NBQ2VydG1maW9hdGU/YmFzZTI9vYm1Y3RD0GFcc1jZXJ0aWZpY2F0
aW9uQUV0aG9yaXRSMCEGCSzGAQQAQBgjcuAqQUHhIAVvB1AGIAUvB1AHIAAqB1AHIAw
DQYJKoZIhvcNAQEFBQADggEBAIGQApE6G42xgvV/6ETyuZXb+fVfi9UAMH13xLN
Xw8iTGzodaRop8aVQvulE36h4nHRLwDCAAC0KwQu/XSUmX0m2qH7zDCXv83ycAT
gqoQMF64FdEkkQuux+C94W8sKLwqVWk1k1jDTYMiBvQSEU991NNAZ880bjbh4AeVR
q/mjAE/tylhjJ2LhpehuimFbVRbr3axTie+M4DScczr/z0/D2i2xHdDvMrEuDN5L
seE28wbIQXN1cM3dodhpneQ8e06GKyNTDCxZ52p0/HiIhkkHg7028bQ5aN+sRTN
8d0t7wrRCwoIB24ehzXwcdHpkDyt4+ABSJkzQwvW2+4WY0=
-----END CERTIFICATE-----
```

✔ The certificate and CSR match!

✔ Certificate Modulus Hash:

cd78ed16b2abe2fa203e3f2e3499ee5c

✔ CSR Modulus Hash:

cd78ed16b2abe2fa203e3f2e3499ee5c

Enter your CSR:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDiAICCAnMCAQAwgboXCAAJBgNVBAYTA1VMTQswCQYDVQQIEwVJNQEUMBIGA1UE
BxMLV0VVEJF0k9VR0gxDDAKBgNVBAoTA0VRQzEELzA1UECmQCSV6xJTAjBgNV
BAMTFdFQjAaLUwXRDAxLUNRMS5pe3VwLmVtYy5jb20kSTBHBG9VBAUTQGVIMDQ3
OTc0NDQxNDUyMjY2PhOTR1YWQxZjg1OHNMaNGI5NGF1OWV1MTgwYzdm6jhm8DIz
NDZiMjQ1ZTY5M2MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQAeAaxp
xWITQ+hFXIbn39tXRRM6pHR8xwR9+C86HwZ8zUHdY9VYaYC4B1gYMS6gPWQ2X0tD
vafFH7dwaNUodp91aazECrF8vdpYyaU9pNi9akL3dFgAh27DJoJIN74wTzNB+UQM
XR7HB4X0YNJYQJIEJhI0SY6vseWE7VwecW78jYRoRfQPVqyC4dFJJipeQiCyoUBY
OT425jTHgk1o7gme21WIELMX2kEJZorD9gU2LK/9GcGn4nB7A1bqmxCO/euKw982
1hhxyAN2B25MzONrCvGRG8IoK5Nw9P7tRtR3kJhpX84wFwOPnMVceHcG5dCNa+6
yCf6gcJLG1bbX5p1AgMBAAGggYcwYQGC5qG5Ib3DQEJJDjF3MNUwJwYDVRO1BCAw
HgYIKwYBBQUHAEwGCCsGAQUFBwMCEBgggrSgEFTBQcDBTALBgNVHQ8EBAMCA7gwPQYD
VRORBDYwNIIeV0VCMDEtTDIEMDEtQ00xLmls4X0uZW1jLmNvbYUuBGF1Y3Vjb35p
c3VwLmVtYy5jb20wDQYJKoZIhvcNAQEFBQADggEBAEPcXlqgNRV3kSvM/k0cFQ
sy74JelK1ea5N1UYZtoDNquP+6Rd80kGjv8MpAmajU1M2th2NBfBk3eN2a7s31WP
Ick/J2kTReiStQjy888F1ffqQq48qsIKhArH1Zut+S/iWZ1eSh2CIGeH/75Jge
9UeTeI7S1keiJBRuMktnUQC0Mpmw1Wdpfva3MSiknAB5y0aDntGRgivr3pXQQ+4
eUVU99Bc4Szb0cfqocfk/i/87BGec452/2988U71qZWbxwMEGzsmkqmiQUMu
EAbYm8NFtc5b8I3Cjuh368WYRmFQpA9tAj8yyLxNt2eFA7qKB6XY4nUBfNyee4=
-----END CERTIFICATE REQUEST-----
```

Solución 3. Comparar contenido de cualquier descodificador CSR desde Internet

Paso 1. Copie la sesión Información detallada del certificado para cada uno como se muestra en esta imagen.

```
http://www.itsm.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:
```

Paso 2. Compárelos en una herramienta como Notepad++ con el complemento Comparar como se muestra en esta imagen.

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: