

Verifique el CSR y la discordancia del certificado para el UC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requisitos](#)

[Componentes usados](#)

[Antecedentes](#)

[Administración de certificado del administrador de comunicaciones de Cisco](#)

[Problema](#)

[Práctica general para los Certificados Ca-firmados en CUCM](#)

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

[Solución 2. Utilice cualquier unidad emparejadora de la clave del certificado SSL de Internet](#)

[La solución 3. compara el contenido de cualquier decodificador CSR de Internet](#)

Introducción

Este documento describe cómo identificar si el certificado firmado del Certificate Authority (CA) hace juego la solicitud de firma del certificado existente (CSR) para Cisco unificó los servidores de aplicaciones.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de X.509/CSR.

Componentes usados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos relacionados

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

- Encargado de las Comunicaciones unificadas de Cisco (CUCM)
- Cisco unificó IM y la presencia

- Cisco unificó la conexión del Unity
- CUIS
- Cisco Meidasence
- Cisco Unified Contact Center Express (UCCX)

Antecedentes

Una petición de la certificación consiste en un nombre distinguido, una clave pública, y un conjunto opcional de los atributos firmados colectivamente por la entidad que piden la certificación. Las peticiones de la certificación se envían a las autoridades de certificación que transforman la petición en un certificado de la clave pública X.509. En qué forma las autoridades de certificación vuelven nuevamente el certificado firmado está fuera del ámbito de este documento. PKCS-7 un mensaje es un possibility.(RFC:2986).

Administración de certificado del administrador de comunicaciones de Cisco

La intención de incluir un conjunto de los atributos es doble:

- Para proporcionar a la otra información sobre una entidad dada, o a una contraseña del desafío por la cual la entidad puede pedir más adelante la revocación de certificado.
- Para proporcionar a los atributos para la inclusión en los Certificados X.509. Los servidores actuales de las Comunicaciones unificadas (UC) no utilizan una contraseña del desafío.

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

Información	Descripción
orgunit	unidad organizativa
orgname	nombre de organización
lugar	ubicación de la organización
estado	estado de la organización
país	el código del país no puede ser cambiado
alternatename	nombre de host alterno

Problema

Cuando usted utiliza el UC, usted puede encontrar muchos casos donde el certificado firmado CA no puede ser cargado por teletratamiento en los servidores UC. Usted no puede identificar siempre qué ha ocurrido a la hora de la creación del certificado firmado, puesto que usted no es la persona que utilizó el CSR para crear el certificado firmado. En la mayoría de los decorados, la re-firma de un nuevo certificado tarda más de 24 horas. Los servidores UC tales como CUCM no han detallado el registro/el rastro para ayudar a identificar porqué la carga por teletratamiento del certificado falla pero apenas dan un mensaje de error. La intención de este artículo es estrechar abajo el problema, si es un servidor UC o un problema CA.

Práctica general para los Certificados Ca-firmados en CUCM

CUCM utiliza la integración con el CAs de tercera persona con el uso de un mecanismo CSR PKCS#10 que sea accesible en el GUI del Certificate Manager del sistema operativo de las Comunicaciones unificadas de Cisco. Los clientes, que utilizan actualmente el CAs de tercera

persona deben utilizar el mecanismo CSR para publicar los Certificados para Cisco CallManager, CAPF, IPsec, y Tomcat.

Paso 1. Cambie la identificación antes de que usted genere el CSR.

La identidad del servidor CUCM para generar un CSR se puede modificar con el uso de la red-**Seguridad del** comando set tal y como se muestra en de 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 usted tiene espacio en los campos antedichos, utilice "" para alcanzar el comando tal y como se muestra en de la imagen.

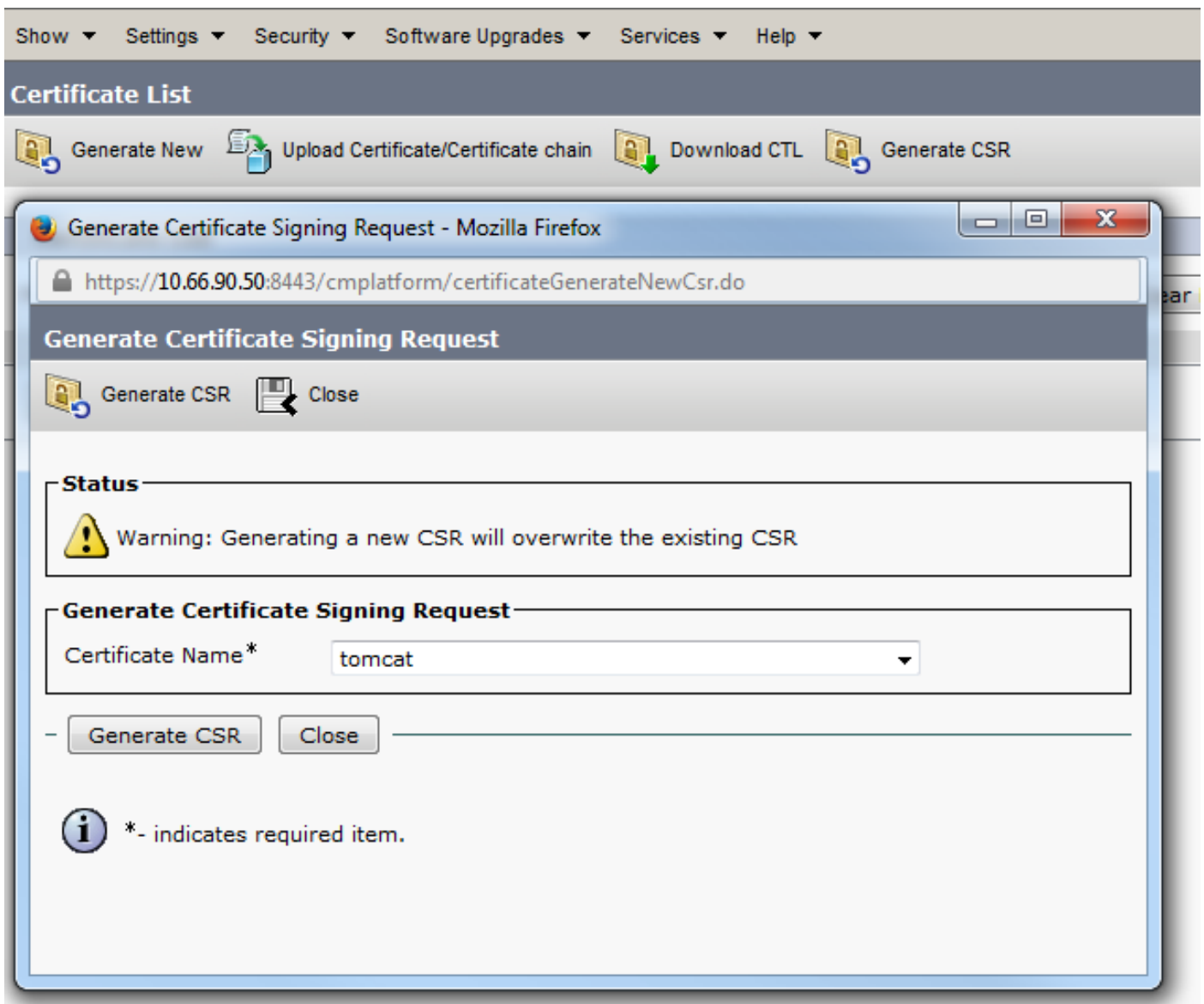
```
admin:set web-security "Cisco Systems" "Cisco TAC" "St Leonard" NSW AU CUCM105.sophia.lf
WARNING: Country code can not be changed.
Country code for existing web-security is : AU

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.

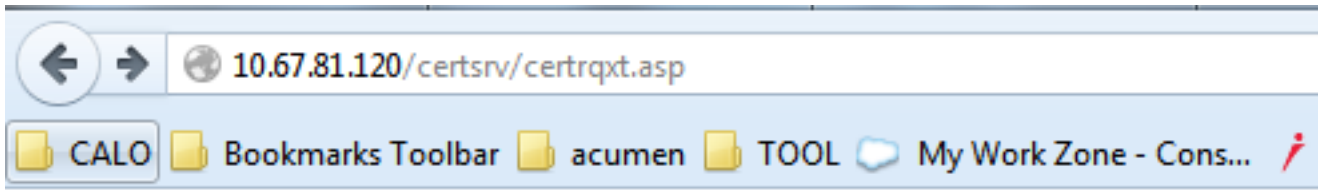
Regenerating web security certificates please wait ...

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

Paso 2. Genere el CSR tal y como se muestra en de la imagen.



Paso 3. Descargue el CSR y consígalo firmado por el CA tal y como se muestra en de 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
eUVU99Bzc4SzbcfqfocfkI/i/87BGec453/Z988U
EAbYmMNfFtn5b8I3CJuh368WyRmFQpA9tAj8yyLx
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

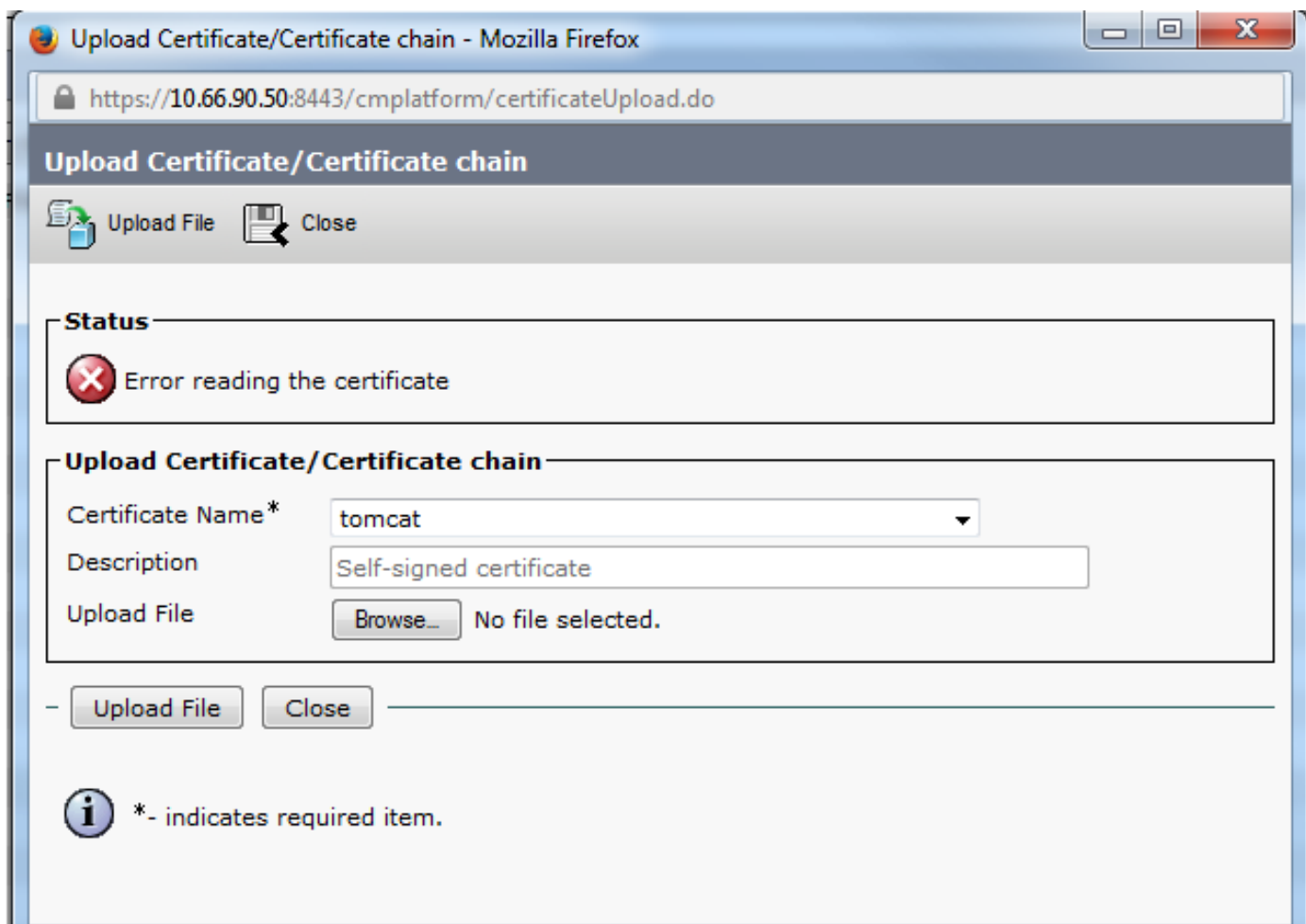
Additional Attributes:

Attributes:

Submit >

Paso 4. Cargue por teletratamiento certificado firmado por CA al servidor.

Una vez que se genera el CSR y se firma el certificado y si usted no puede cargarlo por teletratamiento con un mensaje de error "error de lectura el certificado" (tal y como se muestra en de esta imagen), después usted necesita controlar si el CSR esté regenerado o si el certificado firmado sí mismo es la causa del problema.



Hay tres maneras de controlar si el CSR está regenerado o el certificado firmado sí mismo es la causa del problema.

Solución 1. Utilice el comando de OpenSSL en la raíz (o el linux)

Paso 1. Ábrase una sesión a la raíz y navegue a la carpeta tal y como se muestra en de 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 a la misma carpeta con FTP seguro (SFTP). Si usted no puede poner a un servidor SFTP, después la carga por teletratamiento en la carpeta TFTP puede también conseguir el certificado sobre el CUCM tal y como se muestra en de 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. Controle el MD5 para saber si hay el CSR y el certificado firmado tal y como se muestra en de 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. Utilice cualquier unidad emparejadora de la clave del certificado SSL de 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
QjAaLUwRDAxLUNRMS5pe3VaLmVtYy5jb2ZCFGwhYmNlY20uaXNleY51bW9uY29t
MBOGA1UdDgQWBBSScO++SbY+2naaA2ep/km4x89z29TAfBgNVHSMEGDAWgSTvo1P6
OP4LXm9RDv5N6eIMk8jaoEDCB9QYDVROfBIMVMIN3MINFoIMMoIMJhoMGRhoDev
Ly9DTj1ab2BoaWEtV010LINTMTbRQe3MATTJBLUNBLENOPVdJTI0aUaE49kMaTE0y
QSkwDTj1DRFAaQ049UHV1abG1jJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
Q049Q29uZmlndXhhdG1vbixEQe1ab2BoaWEtREM9bGk/Y2VydG1maW9hdGV5ZXZv
Y2F0aW9uTG1sdD9iYXNlP29iamVjdENaYXNzPWNSTERpc3RyaWJ1dG1vb1BvaW50
MINJBggrSgEFTBQcBAQSBvDCBuTCBtgYIKwYBBQUHGAHgga1sZGFwO18vLONOPXGv
cGhpYS1XSU4tM1MxOEpDM0x3MkEtEQEaQ049Q1BLENOPVBIYmXpYyUyMzE1eSUY
MFI1enZpY2V5LENOPVNI1enZpY2V5LENOPUNvbmZpZ3V5YXRpb24eREM9c29waG1h
LERDPWxpP2NBQ2VydG1maW9hdGU/YmFzZTI9vYmplY3RDdGFcc1jZXJ0aWZpY2F0
aW9uQUV0aG9yaXRSMCEGCSsGAQQGbgg1UAQgQUHhIAVvB1AGIAUvB1AHIAAgB1AMiW
DQYJKoZIhvcNAQEFBQADggEBAIGQApE6G42xgvV/6ETyu2Xb+fVfiq9UAMH13xLN
Xw81TgzodaRop8aVQvuiE36b4nHRLwDCAAC0KwQu/XSUmX0m2qH7zDCXv83ycAT
gqoqMf64FdEkkQuux+C94W8sKLwqVWk1k1jDTYMiBvQSEU991NNAZ880bjbh4AeVR
q/mjAE/tylhjJ2LhpehuimFbVRbr3axTie+M4DSccr/z0/D2i2xHdDvMrEuDN5L
seE28wbIQXN1cM3dodhpneQ8e06GKyNTDCxZ52p0/MiIhkkHg7028bQ5aN+sRTH
8d0t7wrRCwoIB24ehzXwcdHpkDyt4+ABSJkzaQwaW2+4WY0=
-----END CERTIFICATE-----
```

✔ The certificate and CSR match!

✔ Certificate Modulus Hash:

cd78ed16b2abe2fa203e3f2e3499ee5c

✔ CSR Modulus Hash:

cd78ed16b2abe2fa203e3f2e3499ee5c

Enter your CSR:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDi1CCANMCAQAwgboxCSAJSgNVBAYTA1VMTQswCQYDVQQIEwVJNQEUMBIGA1UE
BxMxLUV0VVEJPCk9VR0gxDDAKBgNVBAs0TAA0VW9QaE1MGAkGA1UECm8CSVh6JTAjBgNV
BAMTFmF0Yy5jb2ZCFGwhYmNlY20uaXNleY51bW9uY29tMBOGA1UdEQQ2MDSCHFdF
QjAaLUwRDAxLUNRMS5pe3VaLmVtYy5jb2ZCFGwhYmNlY20uaXNleY51bW9uY29t
OTc0NDQxNDUyMjY2PhOTR1YWQxZjg1OHNMaNGI5NGF1OWV1MTgwYadmb6jhm8DIa
NDZiMjQ1ZTY5M2MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQAeAaxp
xwITQ+hFXIbn39tXRRM6p6HR8xCR9+C86HwZ8zUHdY9VYaYC4B1gYMS6gPWQ2X0tD
vafFH7dwaNUodp91aazECrF8vdpYyAu9pM19akL3dFgAh27DJoJIN74wTzNB+UQM
XR7HB4X0YNJYQJIEJhI0SY6wseWE7VseW78jYRoRfQPVgyC4dFJJiPeQiCyoUBY
OT425jTHgk1o7gme21WIELMX2kEJZorD9gU2LK/9GcGn4nB7A1bqmxCO/euKw982
1hhxyAN2B25MzONrCvGRG8IoK5Nw9P7tRr3kJhpeX84wFwOPnMVceHcG8dCNa+6
yCf6gcJLG1bbX5p1AgMBAAGggYcwYQGC5qG5Ib3DQEJJDjF3MNUwJwYDVRO1BCAw
HgYIKwYBBQUHAEwDgYDVROFAQM/BAQDAgWgMD0GA1UdEQQ2MDSCHFdFQjAaLUwR
DAxLUNRMS5pe3VaLmVtYy5jb2ZCFGwhYmNlY20uaXNleY51bW9uY29tMBOGA1Ud
VR0RBDYwNIIeV0VCMDEtTDFFEMDEtQ00xLmls4X0uZW1jLmNvbYUuBGF1Y3Vjb35p
c3VaLmVtYy5jb2ZCFGwhYmNlY20uaXNleY51bW9uY29tMBOGA1UdEQQ2MDSCHFdF
QjAaLUwRDAxLUNRMS5pe3VaLmVtYy5jb2ZCFGwhYmNlY20uaXNleY51bW9uY29t
sy74Jse1K1ta5N1UYZteDNquP+6Rd80kGjv8MpAmajU1M2th2NBf6X3eN2a7s31WP
Ick/J2kTReiStQjy888F1ffqQ48qsIKhArH1Zut+S/iWZ11eSh2CIGeH/75Jge
9UaTeI78IkeiJBRuMktnUQC0Mpmw1Wdpfva3MSiknAB5y0aDntGRgivr3pXQQ+4
eUVU99Bsc4Szbefqfoefki/i/87BGec452/2988U71qZWbxwMEGsaMkqmiQUMu
EAbYm8NfFen5b8I3CJuh368WYRmFQpA9taJj8yyLxNt2eFA7qKB6XY4nUBfNyee4=
-----END CERTIFICATE REQUEST-----
```

La solución 3. compara el contenido de cualquier decodificador CSR de Internet

Paso 1. Copie la información detallada del certificado de la sesión para cada uno tal y como se muestra en de esta imagen.


```
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 tal como Notepad++ con el comparar plug-in tal y como se muestra en de 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
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: