# Certificado CAPF firmado por CA para CUCM

## Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Limitación](#)
[Antecedentes](#)
[Propósito de CAPF firmado por CA](#)
[Mecanismo para esta PKI](#)
[¿En qué se diferencia CAPF CSR de otros CSR?](#)
[Configurar](#)
[Verificación](#)
[LSC en el caso de CAPF autofirmado](#)
[LSC en el caso de CAPF firmado por CA](#)
[Troubleshoot](#)
[Información Relacionada](#)

## Introducción

En este documento, se describe cómo obtener un certificado de Función de proxy de autoridad de certificación (CAPF) firmado por la Autoridad de certificación (CA) para Cisco Unified Communications Manager (CUCM). Siempre hay solicitudes para firmar el CAPF con la CA externa. En este documento, se muestra por qué comprender cómo funciona es tan importante como el procedimiento de configuración.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Public Key Infrastructure (PKI)
- Configuración de seguridad de CUCM

### Componentes Utilizados

La información que contiene este documento se basa en Cisco Unified Communications Manager versión 8.6 y superior.

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. Si tiene una red

en vivo, asegúrese de entender el posible impacto de cualquier comando.

### Limitación

Diferentes CA pueden tener diferentes requisitos para el CSR. Hay informes de que una versión diferente de OpenSSL CA tiene una tarea específica para el CSR; no obstante, hasta el momento, la CA de Microsoft Windows funcionó bien con el CSR de Cisco CAPF, aunque este tema no se abordará en este artículo.

## Productos Relacionados

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

- CA de Microsoft Windows Server 2008.
- Cisco Jabber para Windows (es posible que versiones diferentes tengan un nombre diferente de la carpeta para almacenar el LSC).

## Antecedentes

### Propósito de CAPF firmado por CA

Algunos clientes desean alinearse con la política de certificados global con la empresa, por lo que existe la necesidad de firmar el CAPF con la misma CA que la de otros servidores.

### Mecanismo para esta PKI

De manera predeterminada, el Certificado significativo localmente (LSC) está firmado por CAPF, por lo que CAPF es la CA para teléfonos en esta situación. Sin embargo, cuando intenta que la CA externa firme el CAPF, el CAPF en esta situación actúa como CA subordinada o CA intermedia.

La diferencia entre el CAPF autofirmado y el CAPF firmado por CA es: el CAPF es la CA de raíz a LSC cuando se realiza un CAPF autofirmado; el CAPF es la CA subordinada (intermedia) a LSC al realizar CAPF con firma de CA.

### ¿En qué se diferencia CAPF CSR de otros CSR?

En relación con RFC5280, la extensión de uso de claves define el propósito (por ej., el cifrado, la firma y la firma de certificados) de la clave incluida en el certificado. CAPF es un proxy de certificado y una CA, y puede firmar el certificado para los teléfonos, pero otro certificados, como CallManager, Tomcat e IPSec actúan como hoja (identidad del usuario). Cuando busca en el CSR para ellos, puede ver que el CSR de CAPF tiene el rol **Firma de certificado** pero no los otros.

CAPF CSR:

```
        Attributes:
        Requested Extensions:
            X509v3 Extended Key Usage:
```

```
            TLS Web Server Authentication, IPSec End System
        X509v3 Key Usage:
            Digital Signature, Certificate Sign
```

Tomcat CSR:

```
Attributes:
        Requested Extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
            X509v3 Key Usage:
                Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

CallManager CSR:

```
Attributes:
        Requested Extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
            X509v3 Key Usage:
                Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

IPSec CSR:

Atributos: Extensiones solicitadas: Uso extendido de la clave de X509v3: Autenticación del servidor Web TLS, autenticación de Cliente Web TLS, uso de claves X509v3 del sistema final de IPSec: Firma digital, Cifrado de clave, Cifrado de datos, Acuerdo de claves

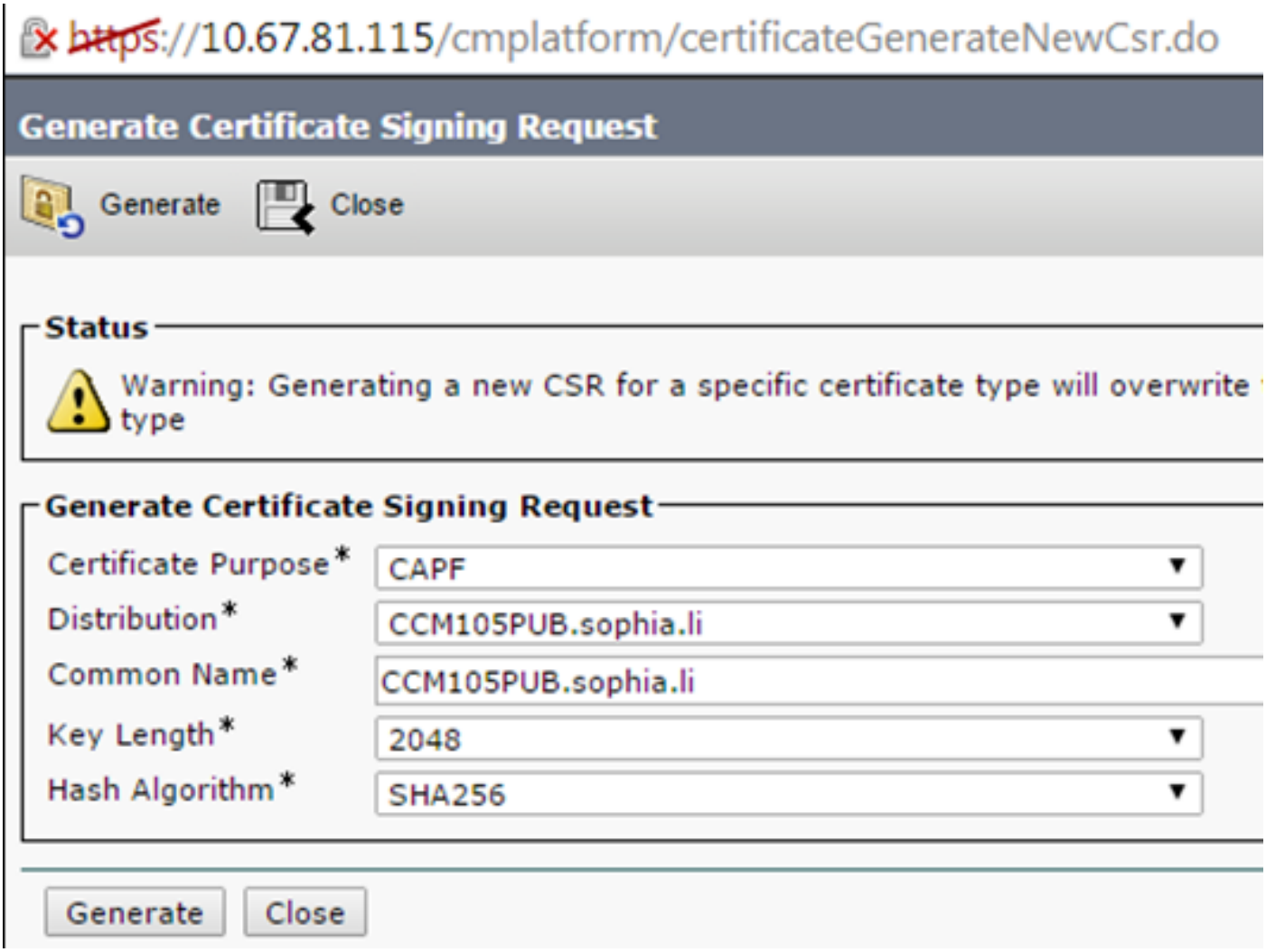
# Configurar

Considere la siguiente situación: la CA de raíz externa se utiliza para firmar el certificado de CAPF: para cifrar la señal/medio para el cliente de Jabber y el teléfono IP.

Paso 1. Convierta el clúster de CUCM en un clúster de seguridad.

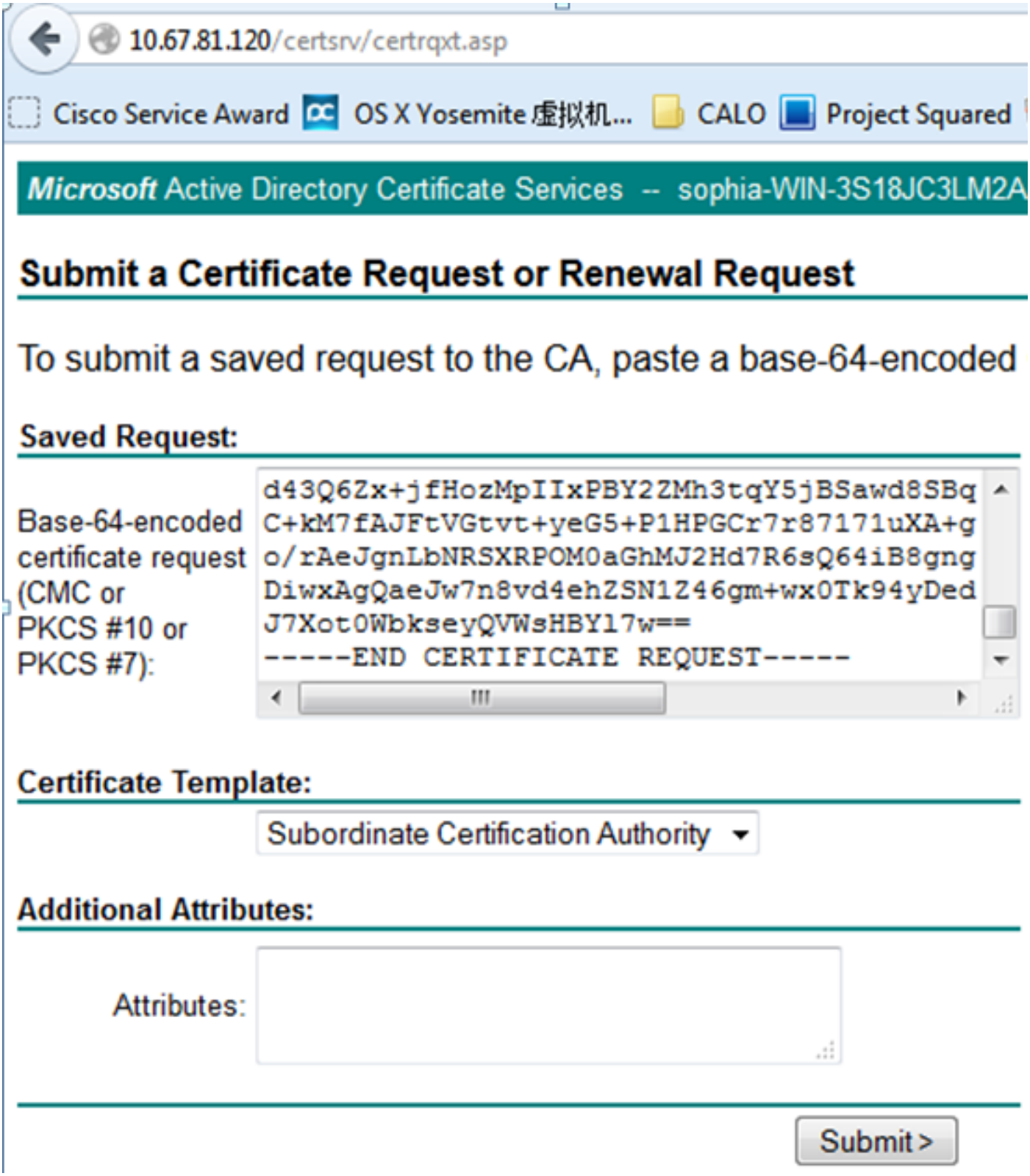
```
admin:utils ctl set-cluster mixed-mode
```

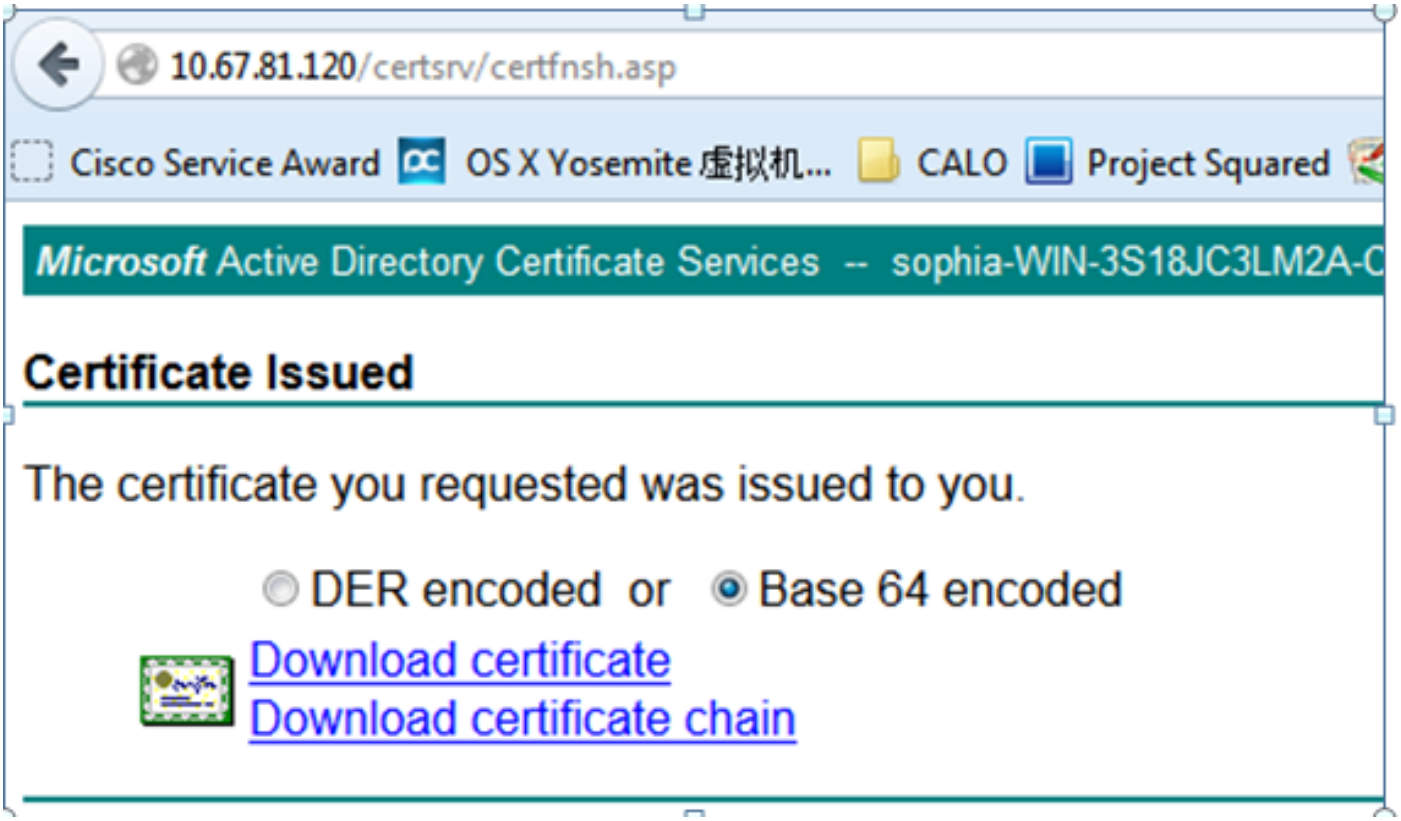
Paso 2. Como se muestra en la imagen, genere la CSR CAPF.




Paso 3. Firmó esto con la CA (utilizando una plantilla subordinada en Windows 2008 CA).

> **Nota:** Debe utilizar la plantilla **Autoridad de certificación de subordinado** para firmar este certificado.


10.67.81.120/certsrv/certrqxt.asp
Cisco Service Award
OS X Yosemite 虚拟机...
CALO
Project Squared
Microsoft Active Directory Certificate Services -- sophia-WIN-3S18JC3LM2A
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded
Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
d43Q6Zx+jfHozMpIIxPBY2ZMh3tqY5jBSawd8SBq
C+kM7fAJFtVGtvt+yeG5+P1HPGCr7r87171uXA+g
o/rAeJgnLbNRSXRPOM0aGhMJ2Hd7R6sQ64iB8gng
DiwxAgQaeJw7n8vd4ehZSN1Z46gm+wx0Tk94yDed
J7Xot0WbkseyQVWsHBYl7w==
-----END CERTIFICATE REQUEST-----
Certificate Template:
Subordinate Certification Authority
Additional Attributes:
Attributes:
Submit >

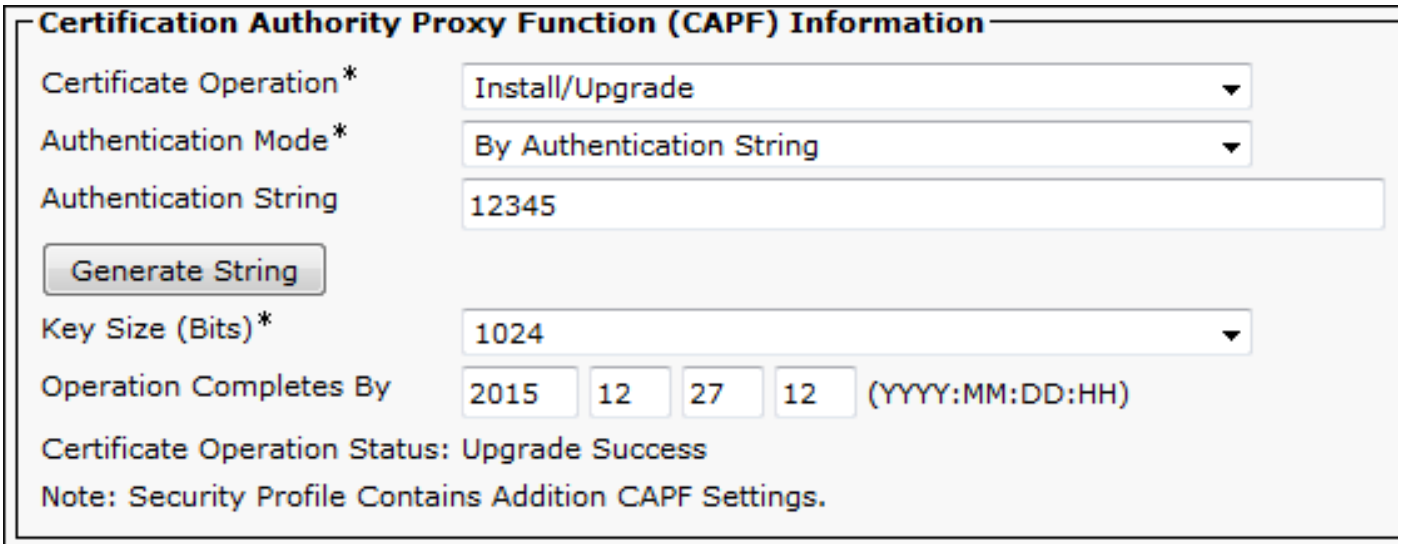


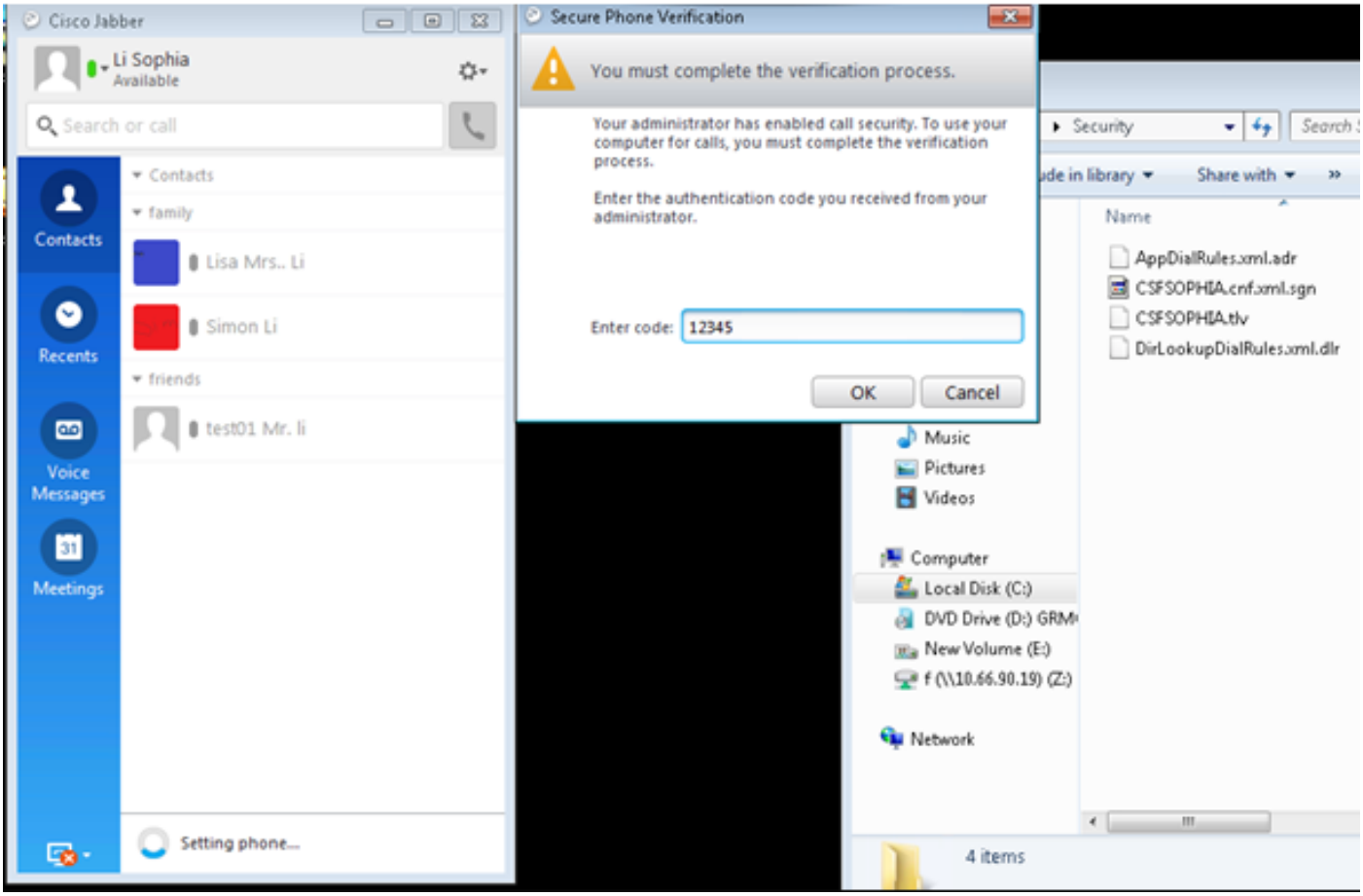

Paso 4. Cargue la CA raíz como CAPF-trust y el certificado de servidor como CAPF. Para esta prueba, también cargue esta CA de raíz como CallManager-trust para que haya conexión TLS entre los servicios Jabber y CallManager, ya que el LSC firmado también debe ser confiable para el servicio CallManager. Como se mencionó al comienzo de este artículo, es necesario alinear la CA para todos los servidores, de modo que esta CA ya debería haberse cargado en CallManager para el cifrado de señal/medios. Para la situación de implementar el teléfono IP 802.1x, no tiene que generar el CUCM como modo mixto ni cargar la CA que firma el CAPF como CallManager-trust en el servidor CUCM.

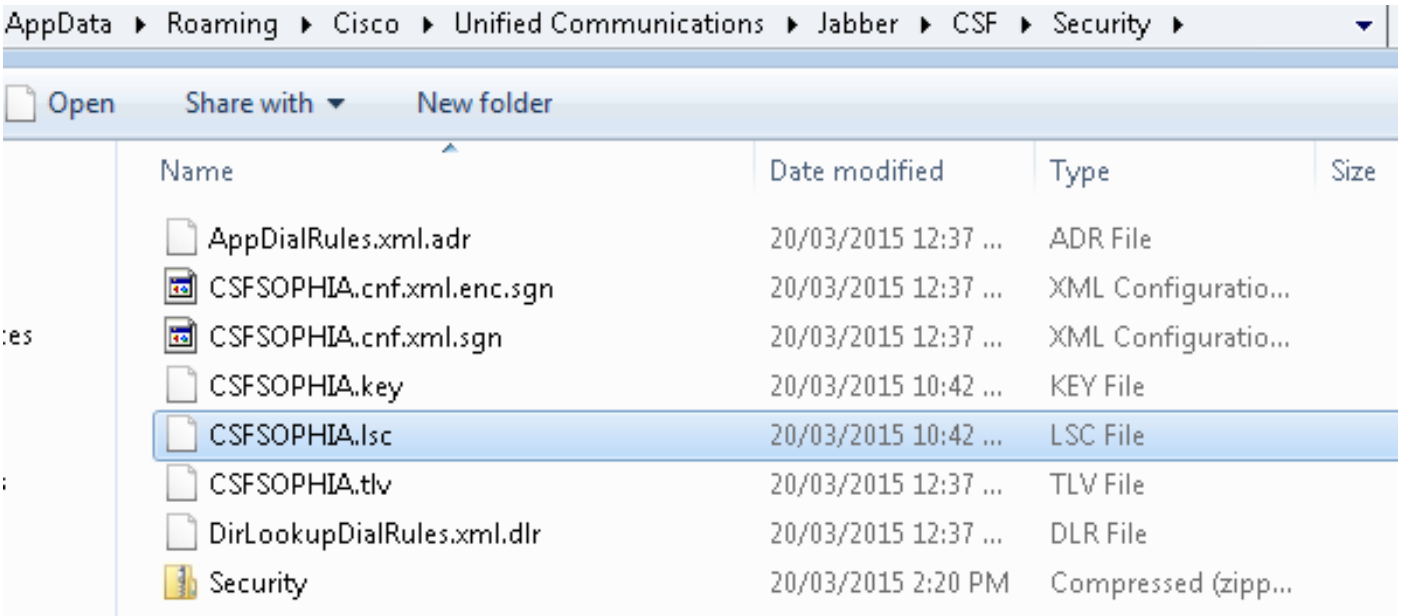
Paso 5. Reinicie el servicio CAPF.

Paso 6. Reinicie los servicios CallManager/TFTP en todas las notas.

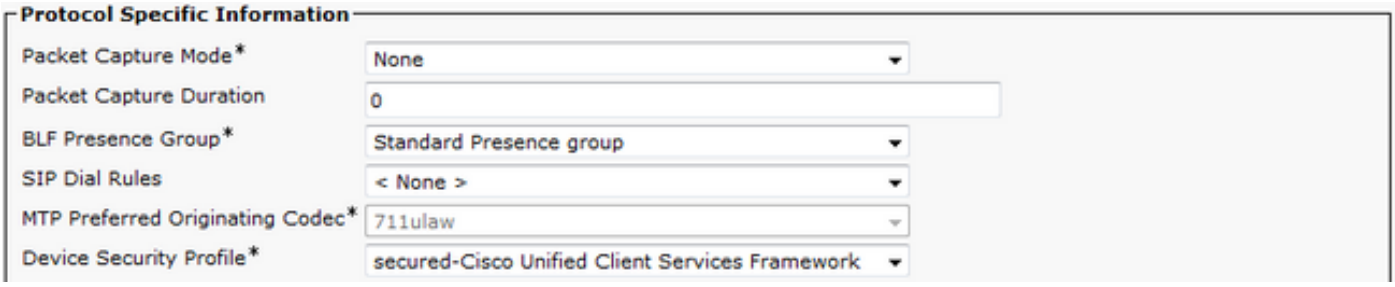
Paso 7. Firmó el LSC del teléfono basado en software Jabber.



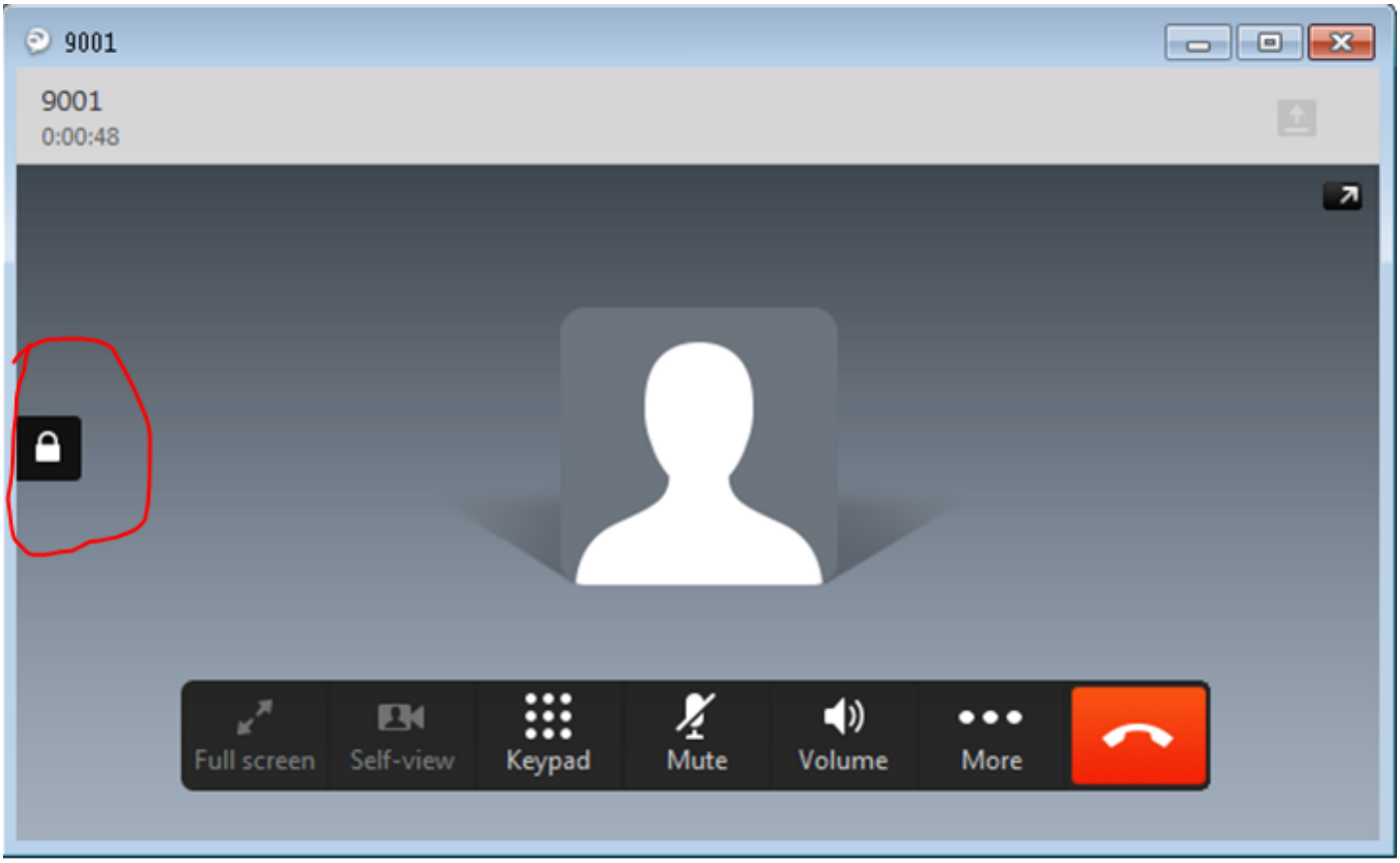



Paso 8. Active el perfil de seguridad del teléfono basado en software Jabber.




Paso 9. Ahora el RTP protegido se produce de la siguiente manera:

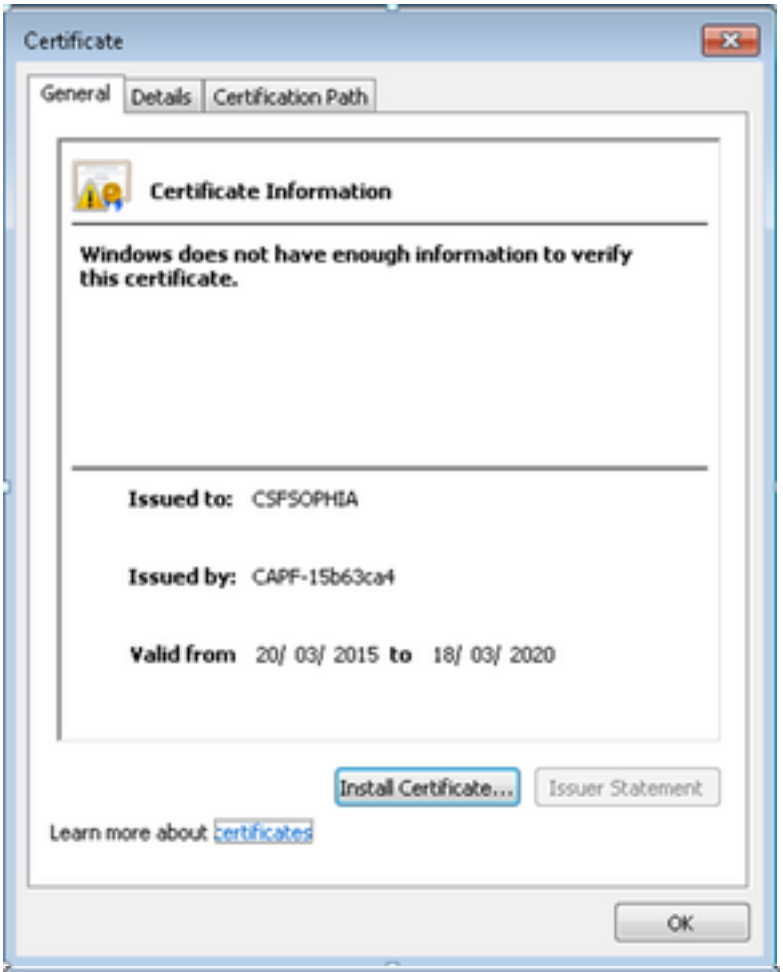



# Verificación

Compare la LSC en el caso de CAPF autofirmado y CAPF firmado por CA:

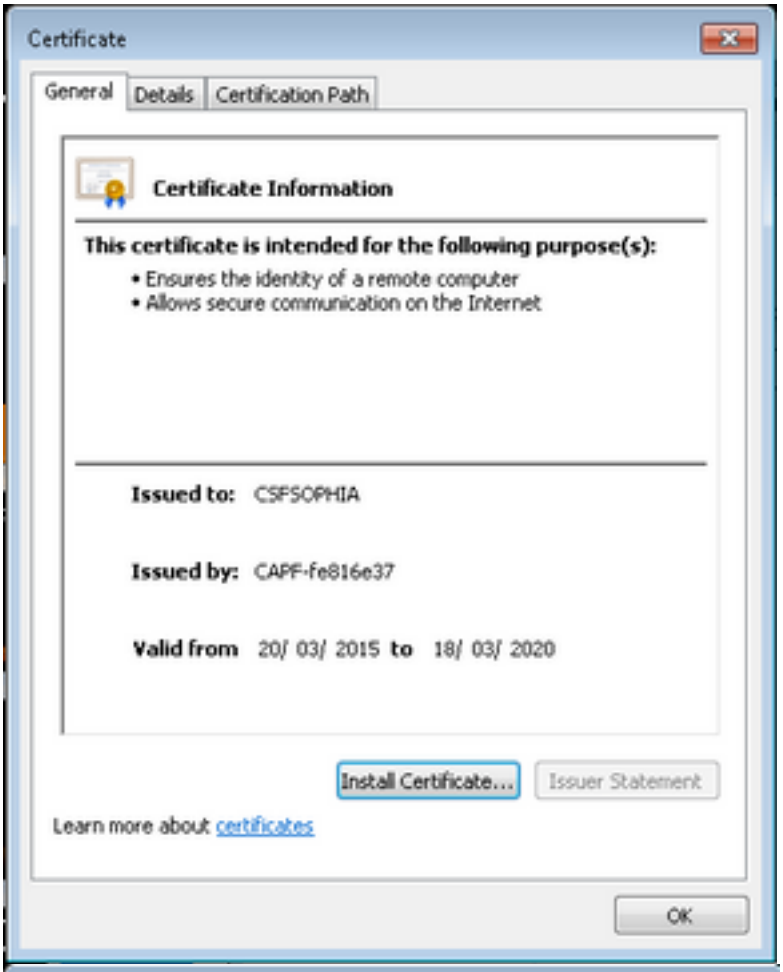
Como se puede ver en estas imágenes para LSC, desde el punto de vista de LSC, CAPF es la CA raíz cuando se utiliza el CAPF autofirmado, pero CAPF es la CA subordinada (intermedia) cuando se utiliza CAPF firmado por CA.

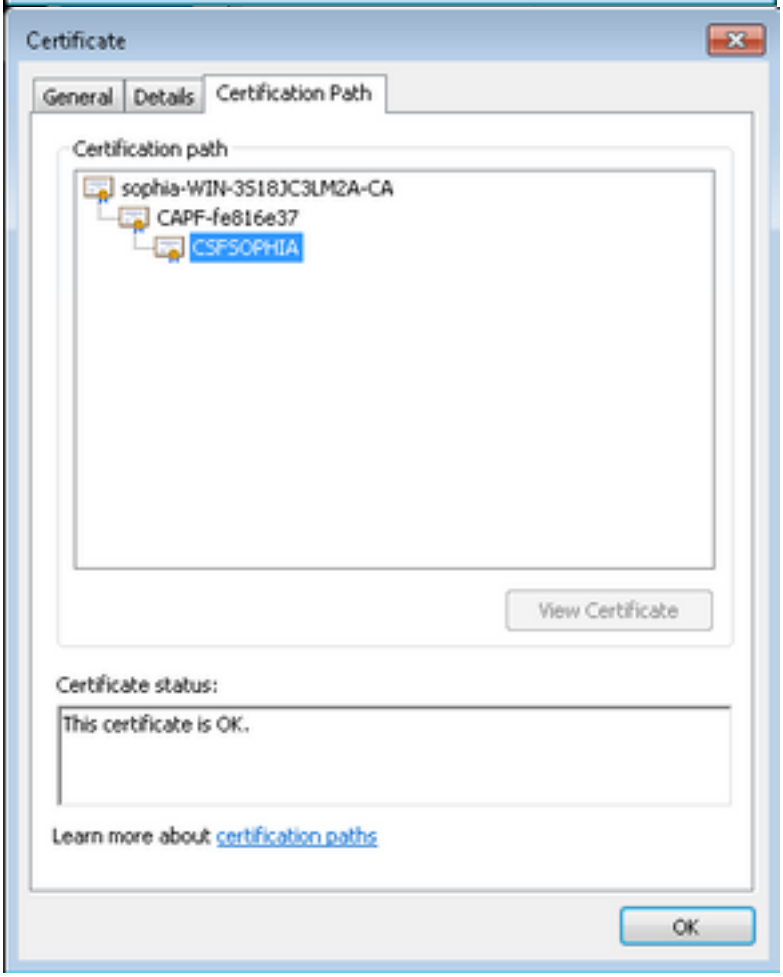
## LSC en el caso de CAPF autofirmado





## LSC en el caso de CAPF firmado por CA


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Allows secure communication on the Internet
Issued to: CSFSOPHIA
Issued by: CAPF-fe816e37
Valid from 20/ 03/ 2015 to 18/ 03/ 2020
Install Certificate...
Issuer Statement
Learn more about certificates
OK


Certificate
General
Details
Certification Path
Certification path
sophia-WIN-3S18JC3LM2A-CA
CAPF-fe816e37
CSFSOPHIA
View Certificate
Certificate status:
This certificate is OK.
Learn more about certification paths
OK

Alerta:

el LSC del cliente Jabber que muestra toda la cadena de certificados en este ejemplo es diferente del teléfono IP. Los teléfonos IP AS están diseñados según el RFC 5280 (3.2). Rutas de certificación y confianza), a continuación, falta el AKI (identificador de clave de autoridad) y, a continuación, el CAPF y el certificado de CA raíz no están presentes en la cadena de certificados. Si falta el certificado CAPF/CA raíz en la cadena de certificados, ISE producirá algún problema para autenticar los teléfonos IP durante la autenticación 801.x sin cargar el CAPF y los certificados raíz en el ISE.  Hay otra opción en CUCM 12.5 con LSC firmado por CA externa sin conexión directamente, por lo que no es necesario cargar el certificado CAPF en el ISE para la autenticación del teléfono IP 802.1x.

# Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

# Información Relacionada

Defectos conocidos: Certificado de CAPF firmado por CA; el certificado raíz debe cargarse como CM-trust:

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCut87382/?referring_site=bugquickviewredir