

# Certificat CAPF signé par une autorité de certification pour CUCM

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Limite](#)

[Informations générales](#)

[Objectif de la CAPF avec signature de l'autorité de signature](#)

[Mécanisme pour cette infrastructure à clé publique](#)

[À quels égards la demande CSR de la CAPF est-elle différente des autres demandes de signature de certificat?](#)

[Configuration](#)

[Vérification](#)

[LSC lorsqu'il s'agit de CAPF avec autosignature](#)

[LSC lorsqu'il s'agit de CAPF avec signature d'une autorité de certification](#)

[Dépannage](#)

[Informations connexes](#)

## Introduction

Ce document explique comment faire en sorte qu'un certificat de CAPF (Certificate Authority Proxy Function) soit signé par une autorité de certification (CA) pour Cisco Unified Communications Manager (CUCM). Il y a toujours des demandes de signature de CAPF avec une autorité de certification externe. Ce document explique pourquoi il est aussi important de comprendre comment ça fonctionne que de connaître la procédure de configuration.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Infrastructure à clé publique (PKI)
- Configuration de la sécurité de CUCM

### Components Used

Les renseignements contenus dans le présent document sont fondés sur Cisco Unified Communications Manager version 8.6 ou ultérieure.

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Limite

Une autorité de certification différente peut présenter des exigences différentes pour ce qui concerne la demande de CSR. Il existe des rapports selon lesquels une version différente d'une autorité de certification OpenSSL entraîne une demande spécifique sur le plan de la demande CSR, mais l'autorité de certification Microsoft Windows fonctionne bien avec la demande CSR de Cisco CAPF jusqu'à présent. Cette question ne sera pas abordée dans le présent article.

## Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Microsoft Windows Server 2008 CA.
- Cisco Jabber pour Windows (différentes versions peuvent avoir un nom différent pour désigner le dossier de stockage de LSC).

## Informations générales

### Objectif de la CAPF avec signature de l'autorité de signature

Certains clients souhaitent s'aligner sur la politique de certificat mondial avec l'entreprise, de sorte qu'il soit nécessaire de signer le CAPF avec la même autorité de certification que les autres serveurs.

### Mécanisme pour cette infrastructure à clé publique

Par défaut, le certificat valable localement (LSC) est signé par la CAPF, donc la CAPF est l'autorité de certification pour les téléphones dans ce scénario. Toutefois, lorsque vous tentez d'obtenir la signature d'un certificat CAPF par l'autorité de certification externe, le CAPF dans ce scénario agit en tant qu'autorité de certification subordonnée ou intermédiaire.

Voici la différence entre CAPF avec autosignature et CAPF avec signature d'une autorité de certification est la suivante : le service de CAPF constitue l'autorité de certification racine pour le LSC lorsqu'il s'agit de CAPF avec autosignature et le service de CAPF constitue l'autorité de certification subordonnée (intermédiaire) pour le LSC lorsqu'il s'agit de CAPF avec signature de l'autorité de certification.

### À quels égards la demande CSR de la CAPF est-elle différente des autres demandes de signature de certificat?

En ce qui concerne [RFC5280](#), l'extension d'utilisation de la clé définit l'objectif (par exemple, le chiffrement, la signature, la signature de certificat) de la clé contenue dans le certificat. Le service de la CAPF est un proxy de certificat et une autorité de certification. Ce service peut signer le certificat des téléphones, mais les autres certificats, comme CallManager, Tomcat, IPSec agissent en tant que Leaf (identité de l'utilisateur). Lorsque vous les recherchez dans le CSR, vous pouvez

voir que le CSR CAPF a un rôle **de signature de certificat** mais pas les autres.

Demande de CSR de CAPF :

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

Demande de CSR de Tomcat :

```
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
```

Demande de CSR de CallManager :

```
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
```

Demande de CSR de IPsec :

Attributs : Extensions demandées : Utilisation de la clé étendue X509v3 : Authentification du serveur Web TLS, authentification du client Web TLS, utilisation de la clé X509v3 du système IPsec : Signature numérique, chiffrement des clés, chiffrement des données, accord de clé

## Configuration



Voici un scénario dans lequel l'autorité de certification racine externe est utilisée pour signer le certificat de CAPF : pour chiffrer le signal/support pour le client Jabber et le téléphone IP.

Étape 1. Faites de votre grappe CUCM la grappe de sécurité.

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

Étape 2. Comme l'illustre l'image, générez le CSR CAPF.

## Generate Certificate Signing Request

 Generate  Close

### Status



Warning: Generating a new CSR for a specific certificate type will overwrite type

### Generate Certificate Signing Request

Certificate Purpose*	CAPF
Distribution*	CCM105PUB.sophia.li
Common Name*	CCM105PUB.sophia.li
Key Length*	2048
Hash Algorithm*	SHA256

Generate

Close

Étape 3. Signé avec l'autorité de certification (à l'aide d'un modèle subordonné dans l'autorité de certification Windows 2008).

**Note:** Vous devez utiliser le modèle d'autorité de certification subordonnée de l'utilisateur pour signer ce certificat.

## 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  
J7Xot0WbkseyQVWsHBY17w==  
-----END CERTIFICATE REQUEST-----
```

### Certificate Template:

Subordinate Certification Authority

### Additional Attributes:

Attributes:

Submit >

10.67.81.120/certsrv/certifnsh.asp


Cisco Service Award OS X Yosemite 虚拟机... CALO Project Squared

Microsoft Active Directory Certificate Services -- sophia-WIN-3S18JC3LM2A-C

## Certificate Issued

The certificate you requested was issued to you.

DER encoded or 
  Base 64 encoded


[Download certificate](#)  
[Download certificate chain](#)

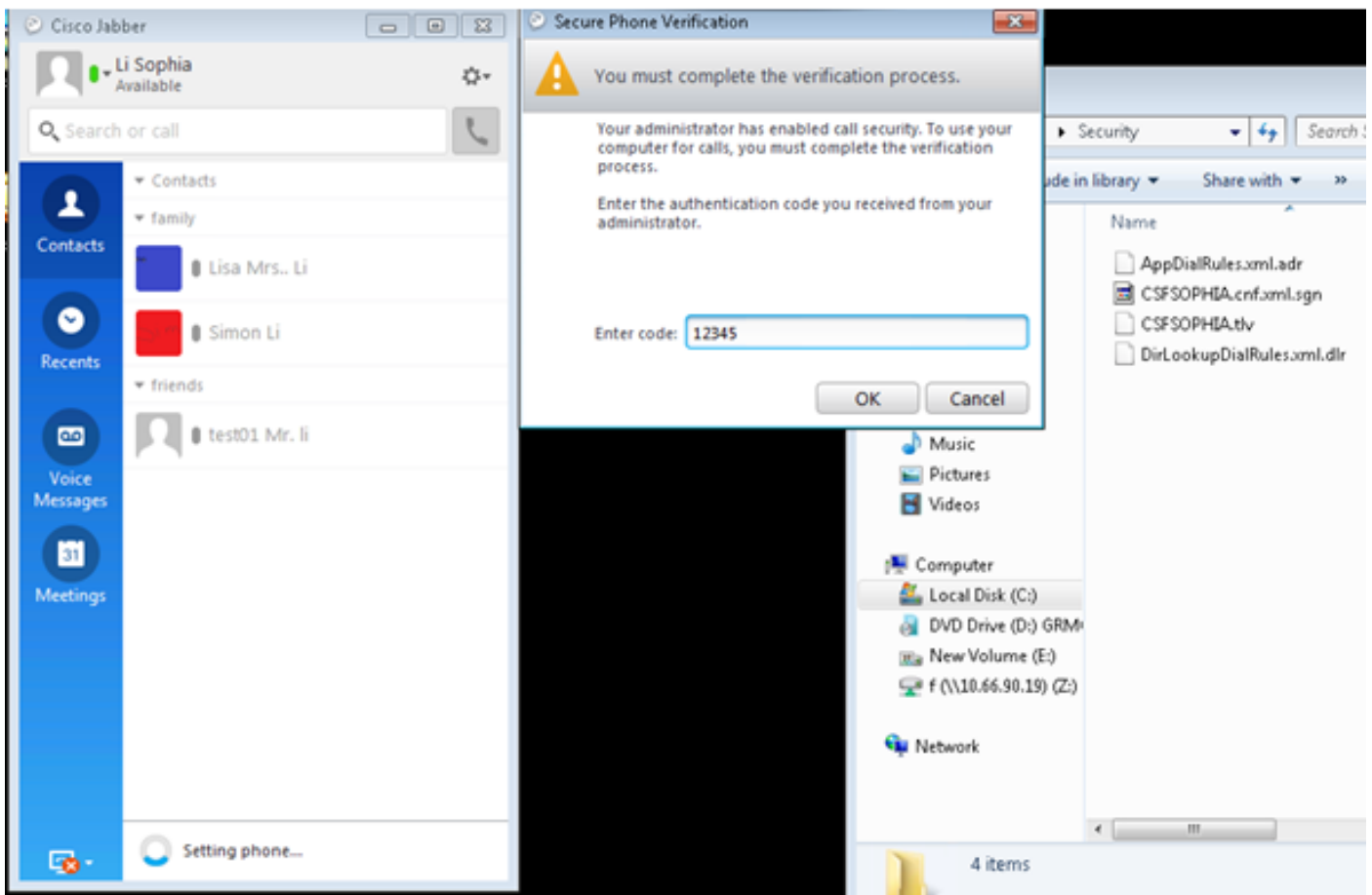
Étape 4. Téléchargez l'autorité de certification racine en tant que CAPF-trust et le certificat du serveur en tant que CAPF. Pour ce test, téléchargez également cette autorité de certification racine en tant que CallManager-trust pour établir une connexion TLS entre Jabber et le service CallManager, car le LSC signé doit aussi être approuvé par le service CallManager. Tel que mentionné au début de cet article, il est nécessaire d'harmoniser l'autorité de certification pour tous les serveurs, par conséquent, cette autorité de certification doit déjà avoir été chargée dans CallManager pour le chiffrement de signal/support. Pour le scénario de déploiement du téléphone IP 802.1x, vous n'êtes pas obligé de définir le CUCM en mode mixte ou de charger l'autorité de certification qui signe le certificat de CAPF comme CallManager-trust dans le serveur CUCM.

Étape 5. Redémarrez le service CAPF.

Étape 6. Redémarrez les services CallManager/TFTP dans toutes les notes.

Étape 7. Signé le LSC du téléphone logiciel Jabber.

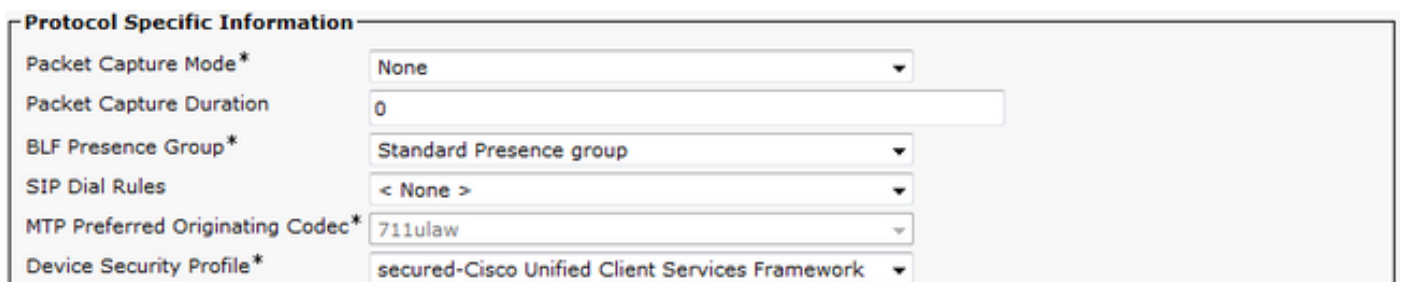
Certification Authority Proxy Function (CAPF) Information	
Certificate Operation*	Install/Upgrade
Authentication Mode*	By Authentication String
Authentication String	12345
<input type="button" value="Generate String"/>	
Key Size (Bits)*	1024
Operation Completes By	2015 12 27 12 (YYYY:MM:DD:HH)
Certificate Operation Status: Upgrade Success	
Note: Security Profile Contains Addition CAPF Settings.	



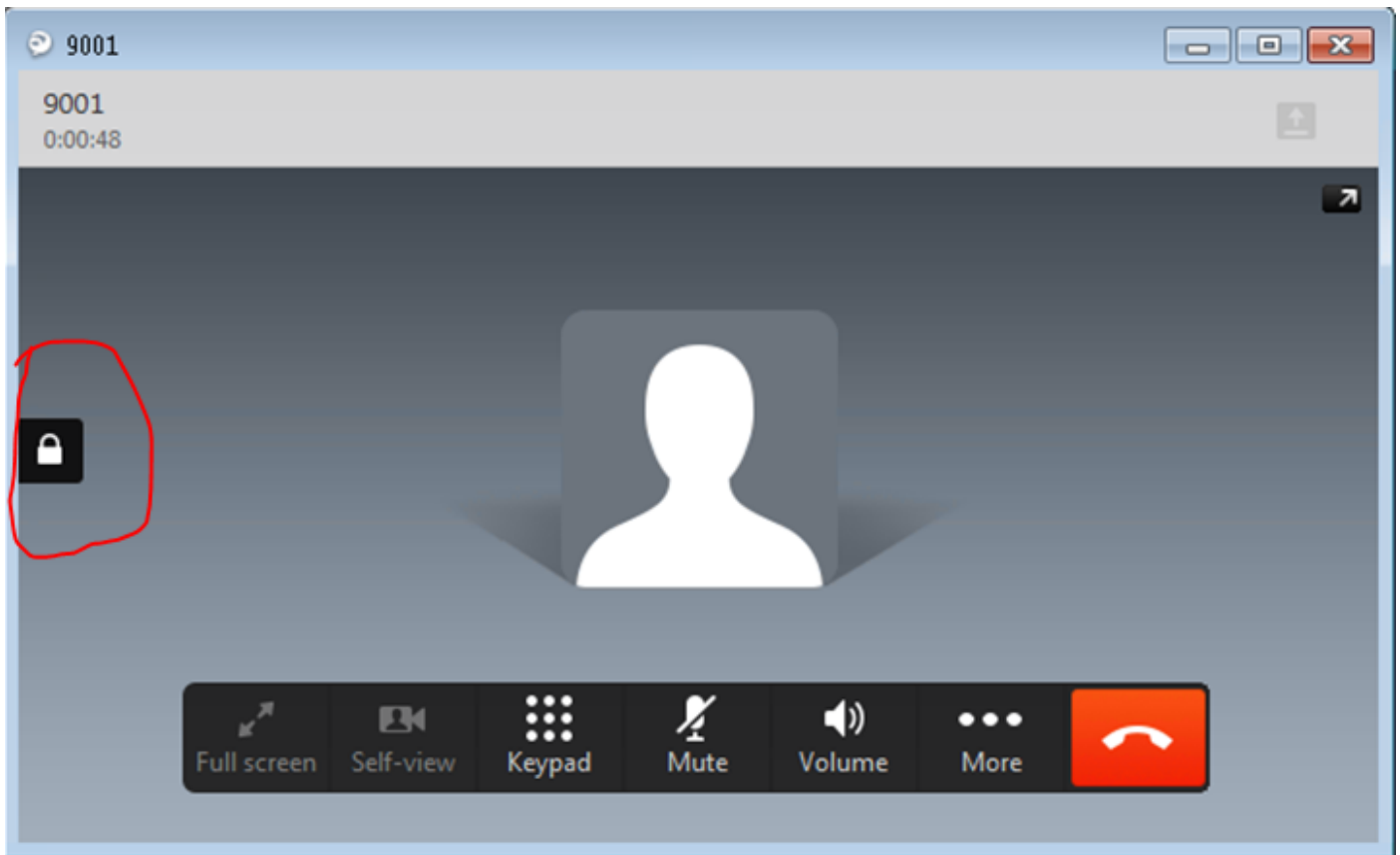
AppData ▶ Roaming ▶ Cisco ▶ Unified Communications ▶ Jabber ▶ CSF ▶ Security ▶

Name	Date modified	Type	Size
AppDialRules.xml.adr	20/03/2015 12:37 ...	ADR File	
CSFSOPHIA.cnf.xml.enc.sgn	20/03/2015 12:37 ...	XML Configuratio...	
CSFSOPHIA.cnf.xml.sgn	20/03/2015 12:37 ...	XML Configuratio...	
CSFSOPHIA.key	20/03/2015 10:42 ...	KEY File	
CSFSOPHIA.lsc	20/03/2015 10:42 ...	LSC File	
CSFSOPHIA.tlv	20/03/2015 12:37 ...	TLV File	
DirLookupDialRules.xml.dlr	20/03/2015 12:37 ...	DLR File	
Security	20/03/2015 2:20 PM	Compressed (zipp...	

Étape 8. Activez le profil de sécurité du téléphone logiciel Jabber.



Étape 9. Désormais, le protocole RTP sécurisé se déroule comme suit :



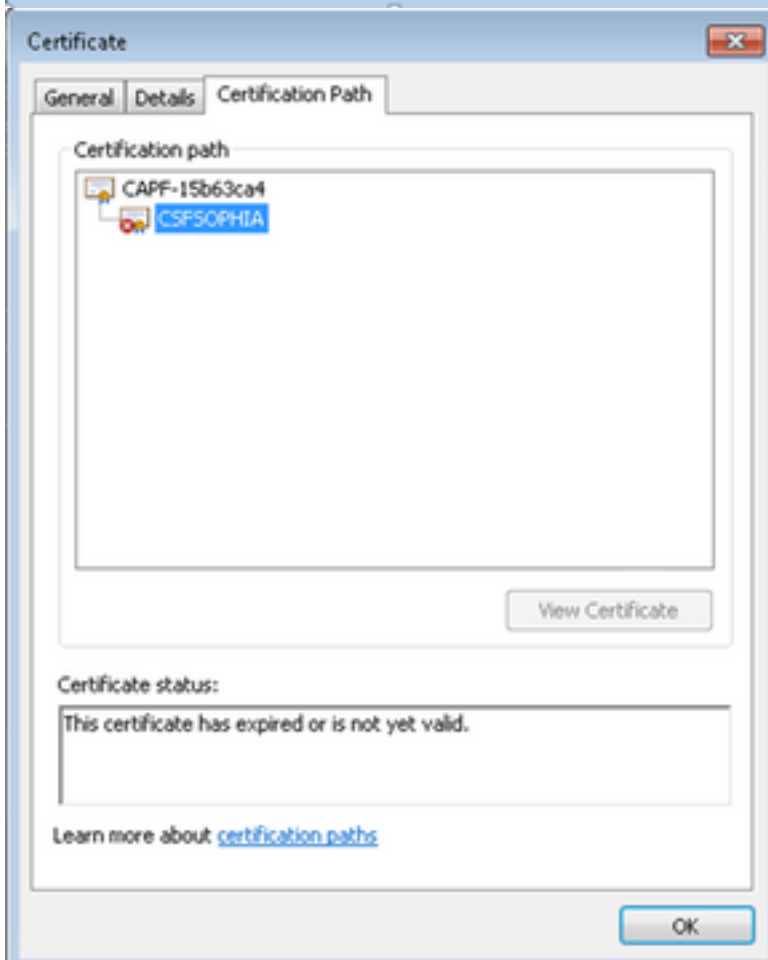
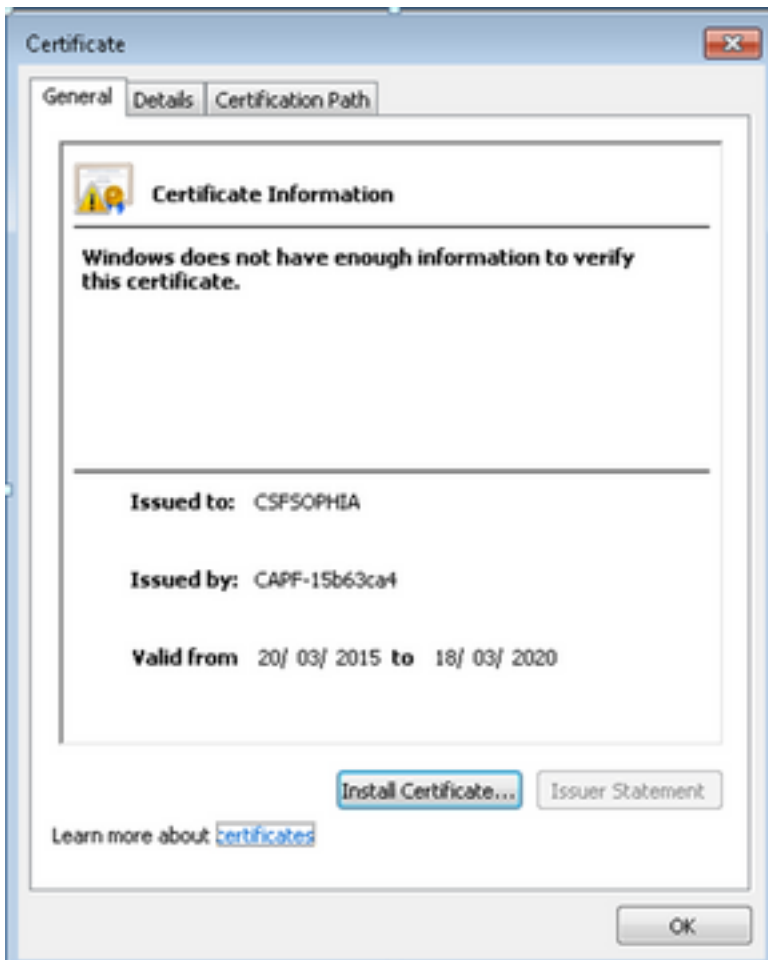
## Vérification

Comparez le LSC avec CAPF autosigné et le LSC avec CAPF signé par une autorité de certification :

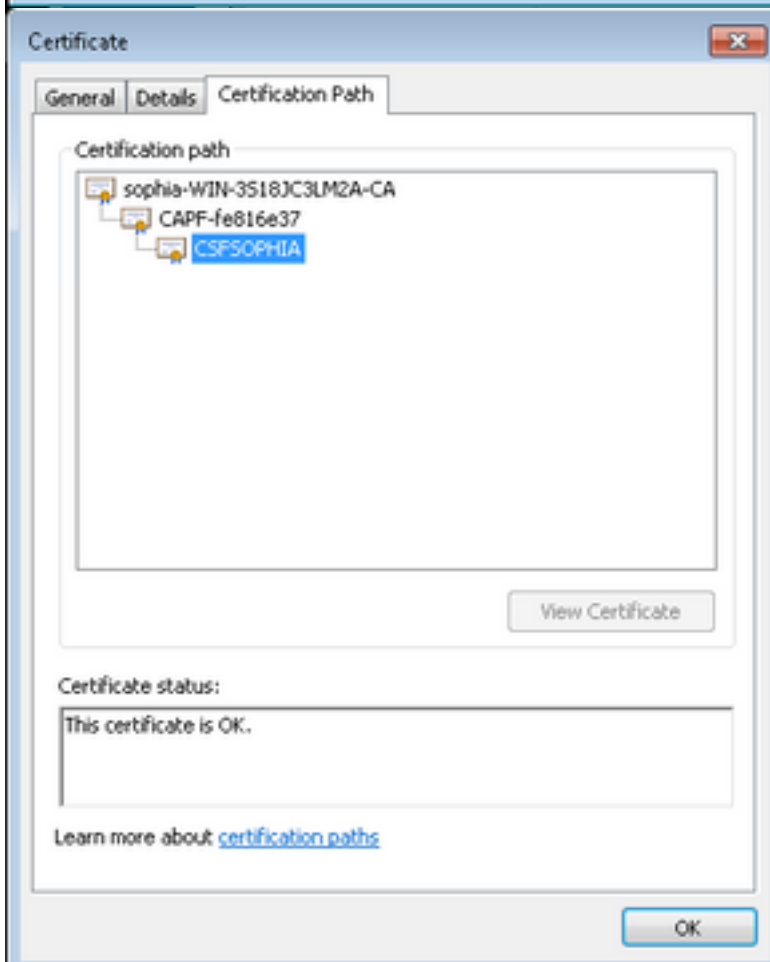
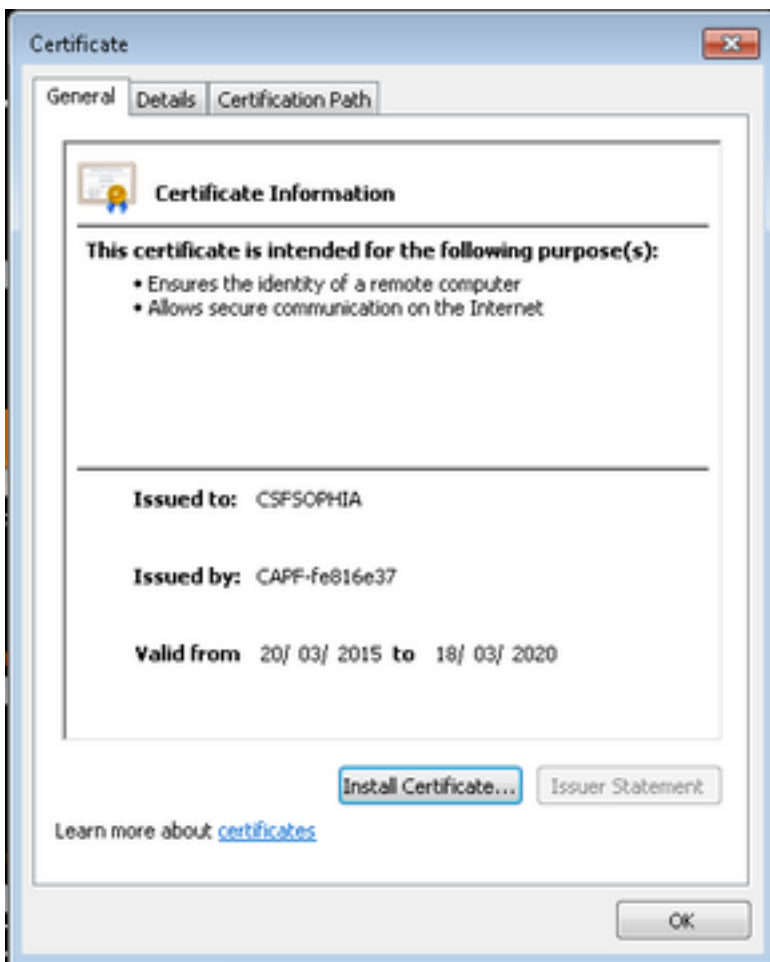
Comme vous pouvez le voir sur ces images du certificat valable localement (LSC), sous l'angle du LSC, le service CAPF est l'autorité de certification racine lorsque vous faites appel à un certificat de CAPF autosigné, mais CAPF est l'autorité de certification (intermédiaire) subordonnée lorsque vous faites appel à un certificat de CAPF signé par une autorité de certification.

**LSC lorsqu'il s'agit de CAPF avec autosignature**





LSC lorsqu'il s'agit de CAPF avec signature d'une autorité de certification



Alerte :

le LSC du client Jabber qui affiche toute la chaîne de certificats dans cet exemple est différent du téléphone IP. Les téléphones IP AS sont conçus sur la base du RFC 5280 (3.2. Chemins de certification et approbation) alors l'AKI (ID de clé d'autorité) est manquant, puis le CAPF et le certificat de l'autorité de certification racine ne sont pas présents dans la chaîne de certificats. Si le certificat CAPF/Root CA est manquant dans la chaîne de certificats, ISE aura un problème pour authentifier les téléphones IP lors de l'authentification 801.x sans télécharger les certificats CAPF et racine dans l'ISE. Il existe une autre option dans CUCM 12.5 avec LSC signé directement par CA hors connexion externe, de sorte que le certificat CAPF n'est pas nécessaire pour être téléchargé dans l'ISE pour l'authentification 802.1x du téléphone IP.

## Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

## Informations connexes

Défaut connu : Certificat CAPF signé par une autorité de certification, le certificat racine doit être chargé en tant que certificat de confiance CM-trust :

[https://bst.cloudapps.cisco.com/bugsearch/bug/CSCut87382/?referring\\_site=bugquickviewredir](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCut87382/?referring_site=bugquickviewredir)