CAPF-certificaat ondertekend door CA voor CUCM

Inhoud

Inleiding

Dit document beschrijft hoe u een certificaat van Licentie voor certificaatfunctie (CAPF) kunt verkrijgen die door de certificaatautoriteit (CA) is ondertekend voor Cisco Unified Communications Manager (CUCM). Er zijn altijd verzoeken om de CAPF met externe CA te ondertekenen. Dit document toont aan waarom om te begrijpen hoe het werkt zo belangrijk is als de configuratieprocedure.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- PKI-infrastructuur
- Configuratie van CUCM-beveiliging

Gebruikte componenten

De informatie in dit document is gebaseerd op versie 8.6 en hoger van Cisco Unified Communications Manager.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Beperking

Een andere CA kan verschillende eisen aan de CSR hebben. Er zijn meldingen dat de andere versie van OpenSSL CA een of andere specifieke vraag naar CSR heeft, maar Microsoft Windows CA werkt tot nu toe goed met CSR van Cisco CAPF, welke discussie niet in dit artikel zal worden behandeld.

Verwante producten

Dit document kan ook met deze hardware- en softwareversies worden gebruikt:

- Microsoft Windows Server 2008 CA.
- Cisco Jabber voor Windows (verschillende versies kunnen een andere naam voor map hebben om de LSC op te slaan).

Achtergrondinformatie

Doel van de door het CAPF ondertekende VK

Sommige klanten zouden zich willen aanpassen aan het mondiale certificatenbeleid van het bedrijf, zodat het nodig is de CAPF te ondertekenen met dezelfde CA als andere servers.

Mechanisme voor deze PKI

Standaard wordt plaatselijk aanzienlijk certificaat (LSC) getekend door de CAPF, zodat de CAPF de CA is voor telefoons in dit scenario. Wanneer u echter probeert de CAPF te laten ondertekenen door de externe CA, dan fungeert CAPF in dit scenario als ondergeschikte CA of tussenliggende CA.

Het verschil tussen zelfgetekende CAPF en CAPF is: CAPF de bron-CA aan LSC is bij het doen van zelfgetekende CAPF, de CAPF de ondergeschikte (intermediaire) CA aan LSC bij het doen van CA-ondertekende CAPF.

Hoe CSR van CAPF verschilt van andere CSR's?

Met betrekking tot RFC5280, definieert de belangrijkste gebruiksuitbreiding het doel (bv. aansluiting, ondertekening, ondertekening van certificaten) van de in het certificaat opgenomen sleutel. CAPF is een certificaat proxy en CA en kan certificaat voor de telefoons tekenen, maar het andere certificaat zoals CallManager, Tomcat en IPSec (gebruikersidentiteit). Wanneer u naar de CSR kijkt voor hen, kunt u zien dat CAPF CSR **certificaatfunctie** heeft maar niet de andere.

CSR CAPF:

```
        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:

Kenmerken: Vereiste uitbreidingen: X509v3 uitgebreid gebruik: TLS-webserververificatie, TLS-web-clientverificatie, IPSec End-systeem X509v3 toetsuitbreiding: Digitale handtekeningen, essentiële versterking, gegevensversterking, sleutelovereenkomst

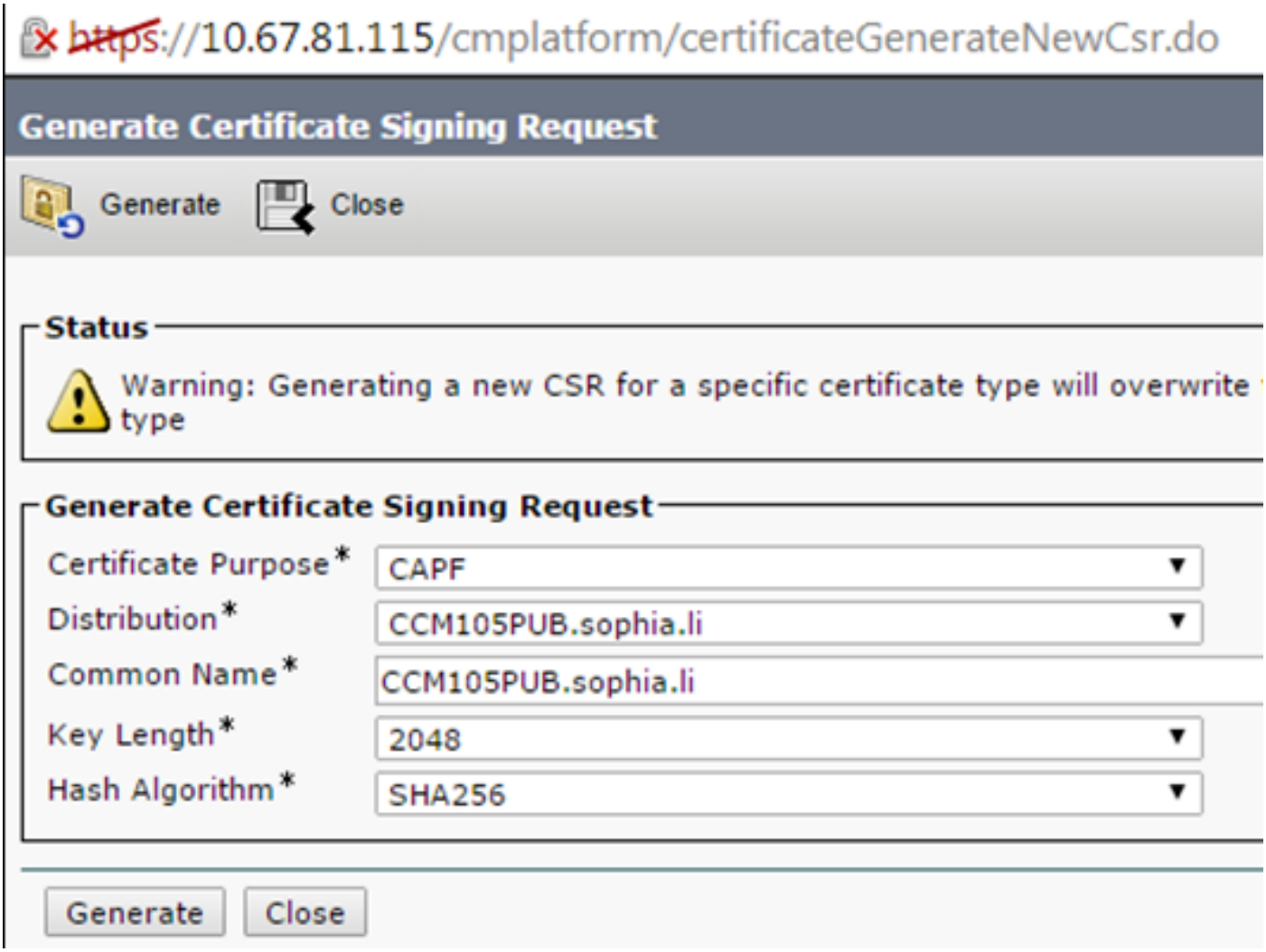
Configureren

Hier is één scenario, de externe wortel CA wordt gebruikt om CAPF certificaat te ondertekenen: versleutelen van het signaal/de media voor Jabber-client en IP-telefoon.

Stap 1. Maak uw CUCM-cluster als een beveiligingscluster.

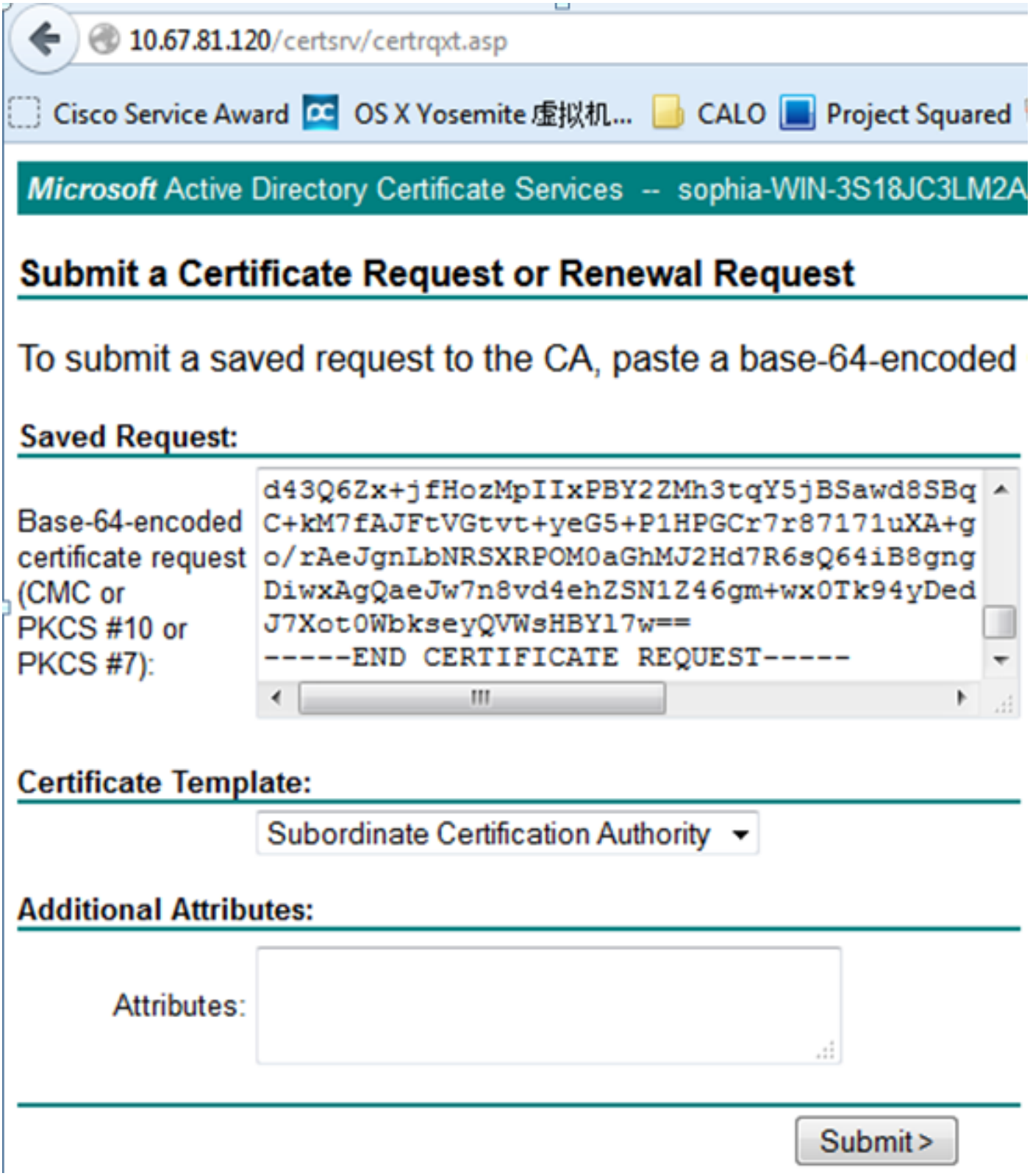
```
admin:utils ctl set-cluster mixed-mode
```

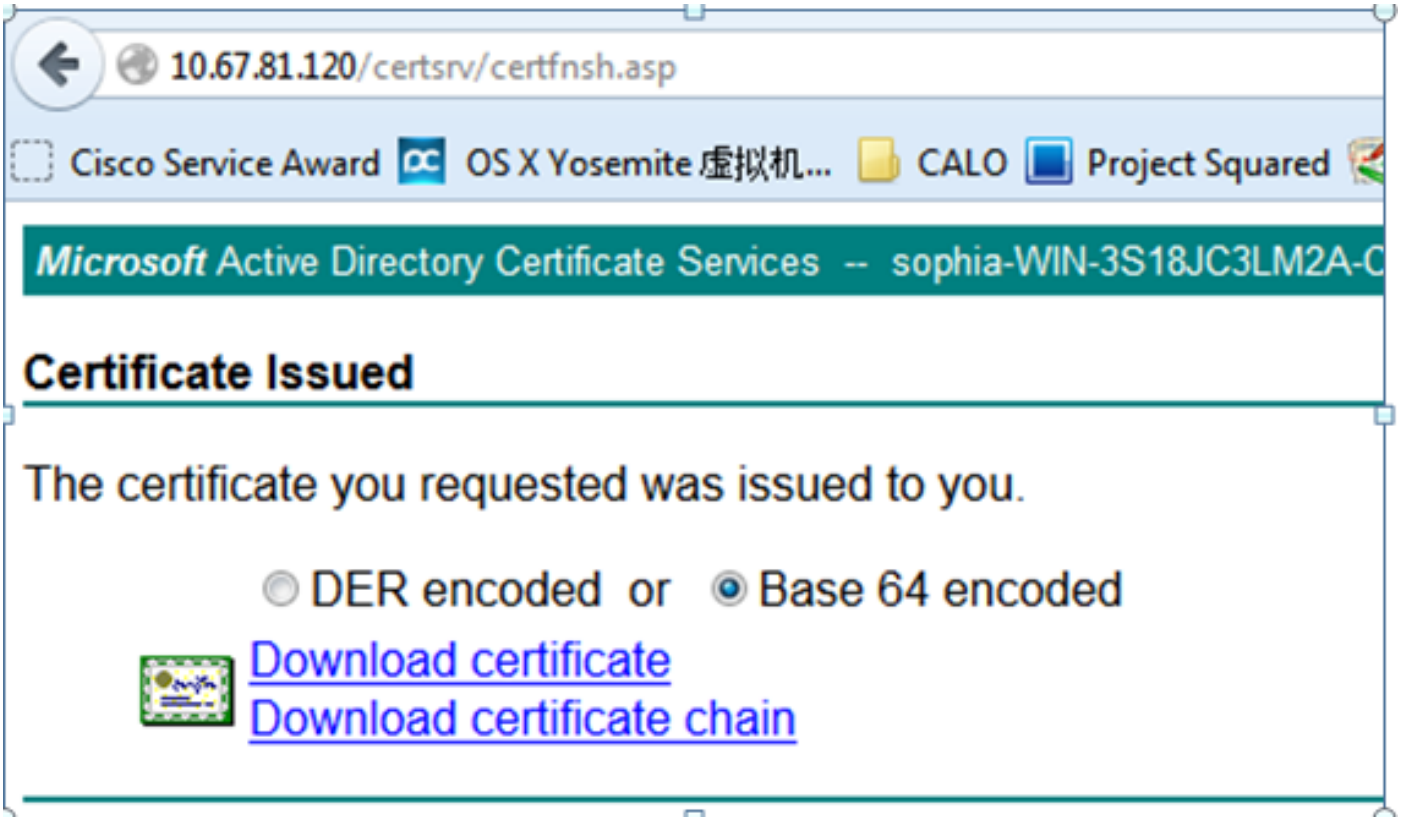
Stap 2. Zoals in de afbeelding, genereert u het CSR-bestand.



Stap 3. Ondertekend dit met de CA (gebruik makend van ondergeschikte sjabloon in Windows 2008 CA).

> **Opmerking:** U dient de sjabloon **voor certificeringsinstanties** te gebruiken om dit certificaat te ondertekenen.


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 >

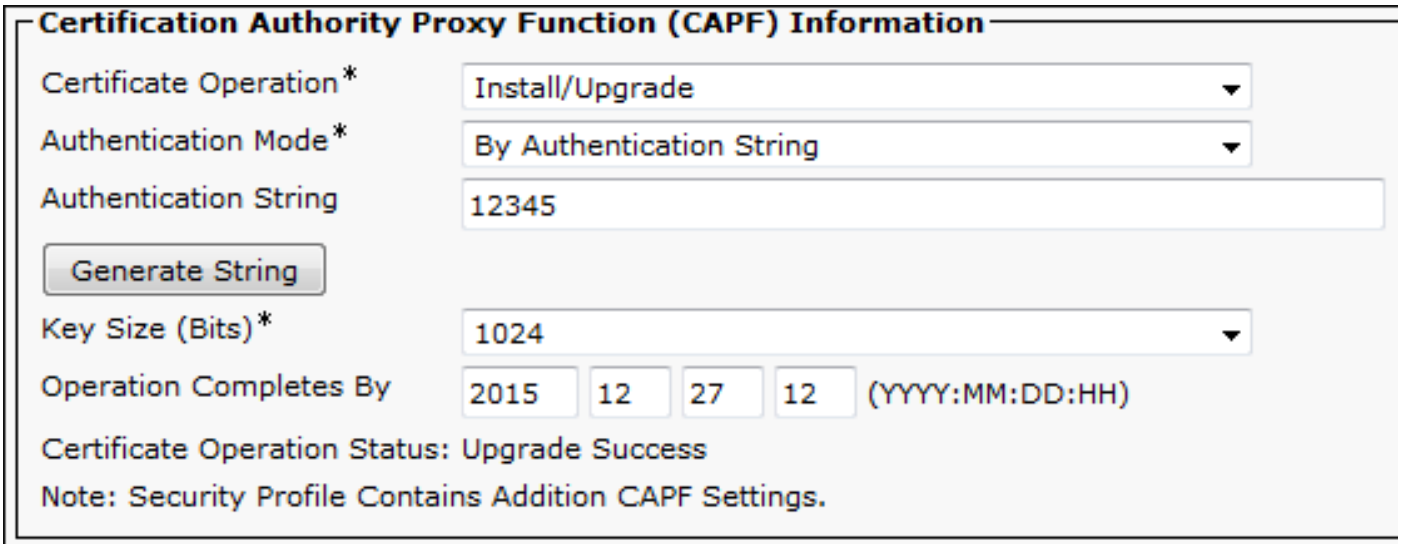


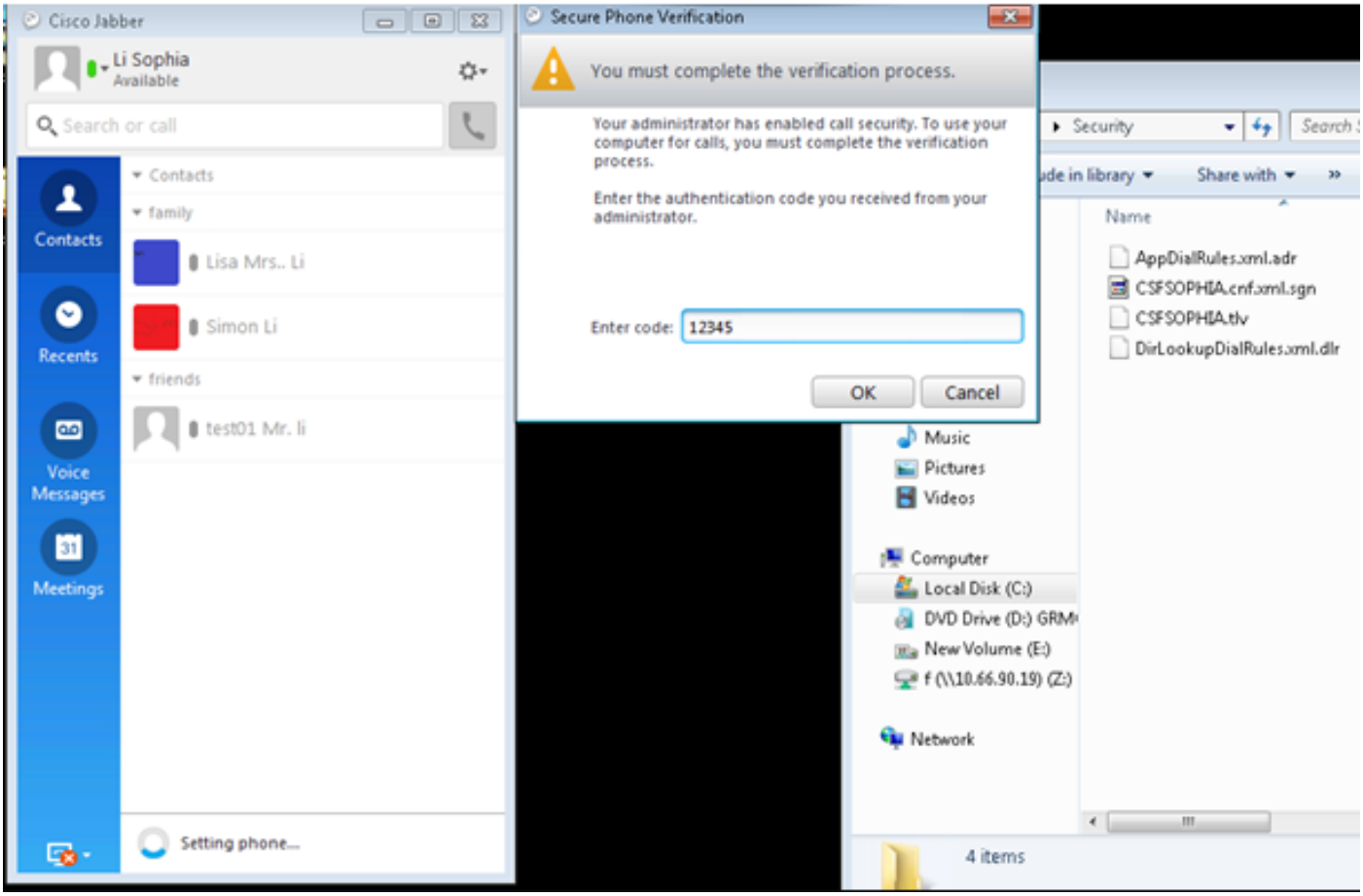
Stap 4. Upload de wortel CA als CAPF-trust en het servercertificaat als CAPF. Voor deze test kunt u deze Root CA als CallManager-trust ook uploaden om TLS-verbinding tussen Jabber en CallManager te hebben, aangezien de ondertekende LSC ook door CallManager moet worden vertrouwd. Zoals aan het begin van dit artikel is vermeld, moet de CA voor alle servers worden uitgelijnd, zodat deze CA al naar CallManager had moeten worden geüpload voor signaal-/mediaconcentratie. In het geval van het implementeren van IP-telefoon 802.1x, hoeft u geen CUCM als gemengde modus te maken of de CA te uploaden die de CAPF als CallManager-trust in de CUCM-server toont.

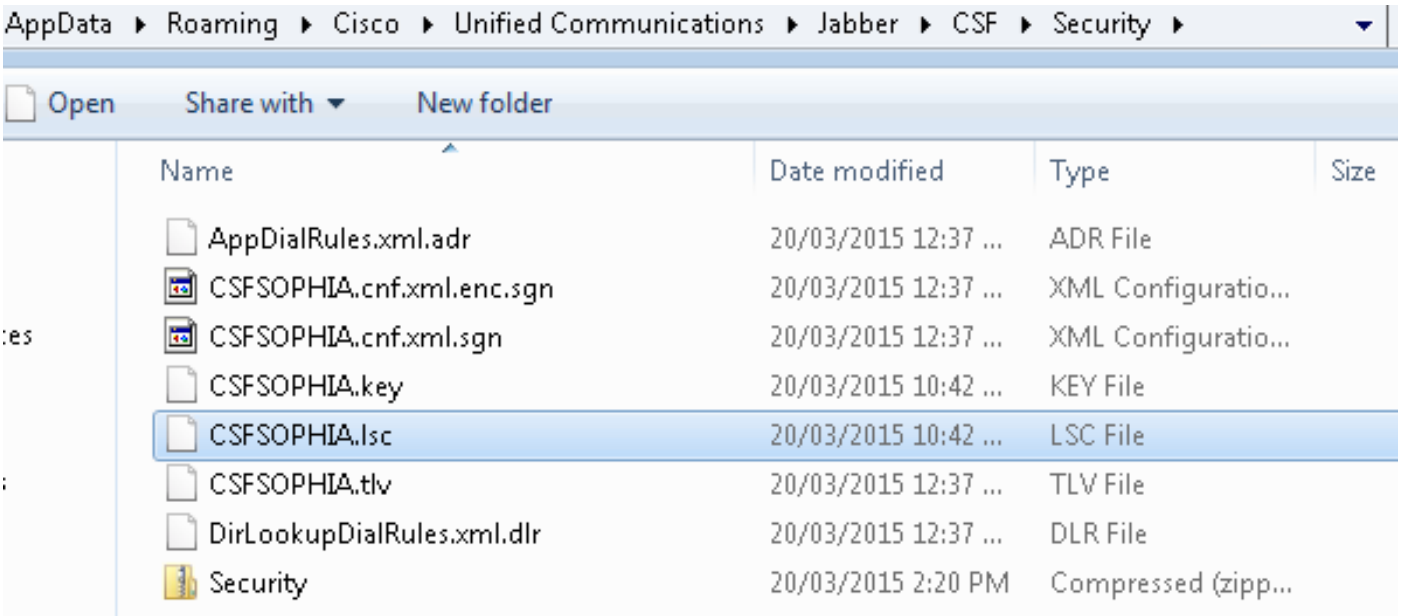
Stap 5. Start de CAPF-service opnieuw.

Stap 6. Start de CallManager/TFTP-services opnieuw in alle opmerkingen.

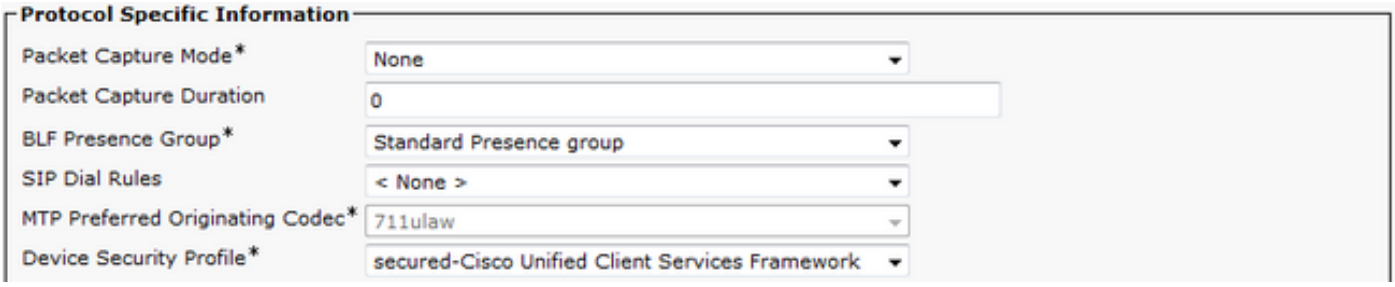
Stap 7. Ondertekend de Jabber softphone LSC.



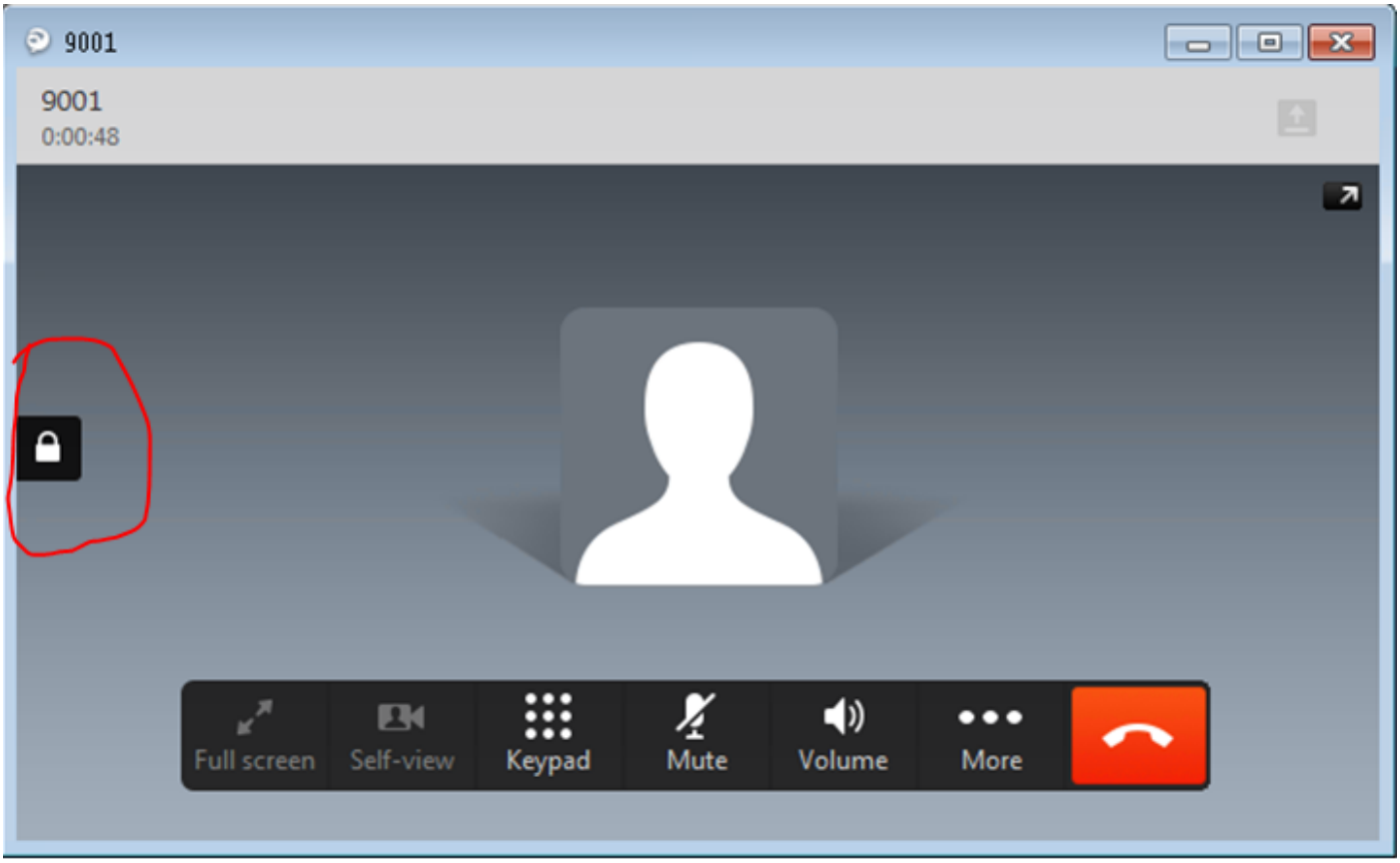




Stap 8. Schakel het beveiligingsprofiel voor Jabber-softphone in.



Stap 9. Nu wordt de beveiligde RTP uitgevoerd als:

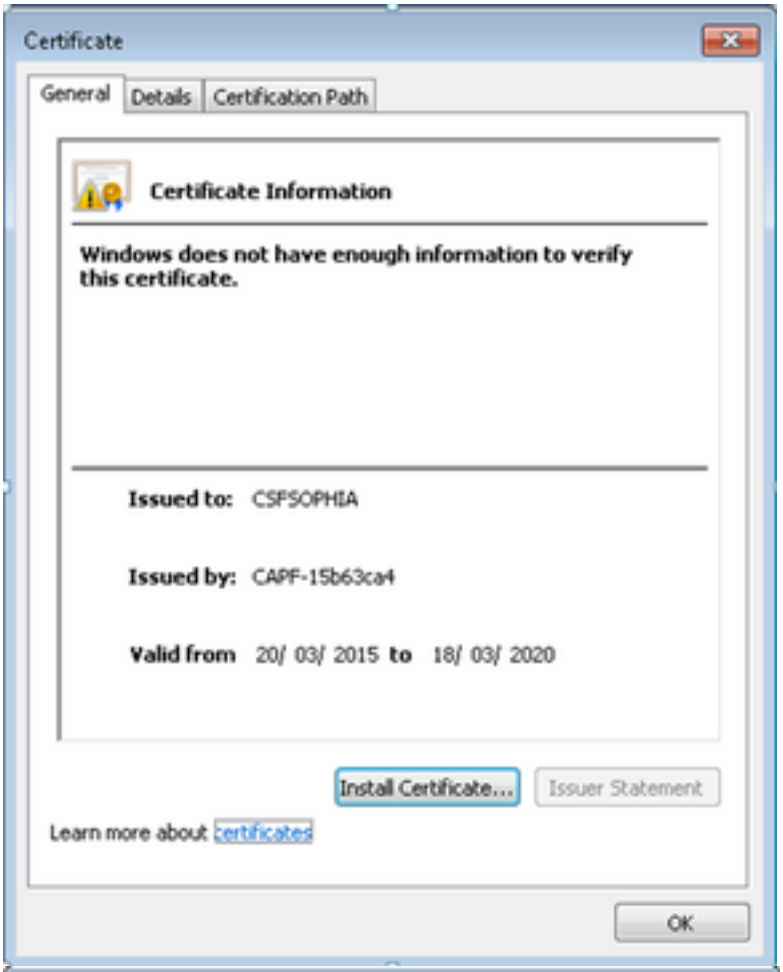


Verifiëren

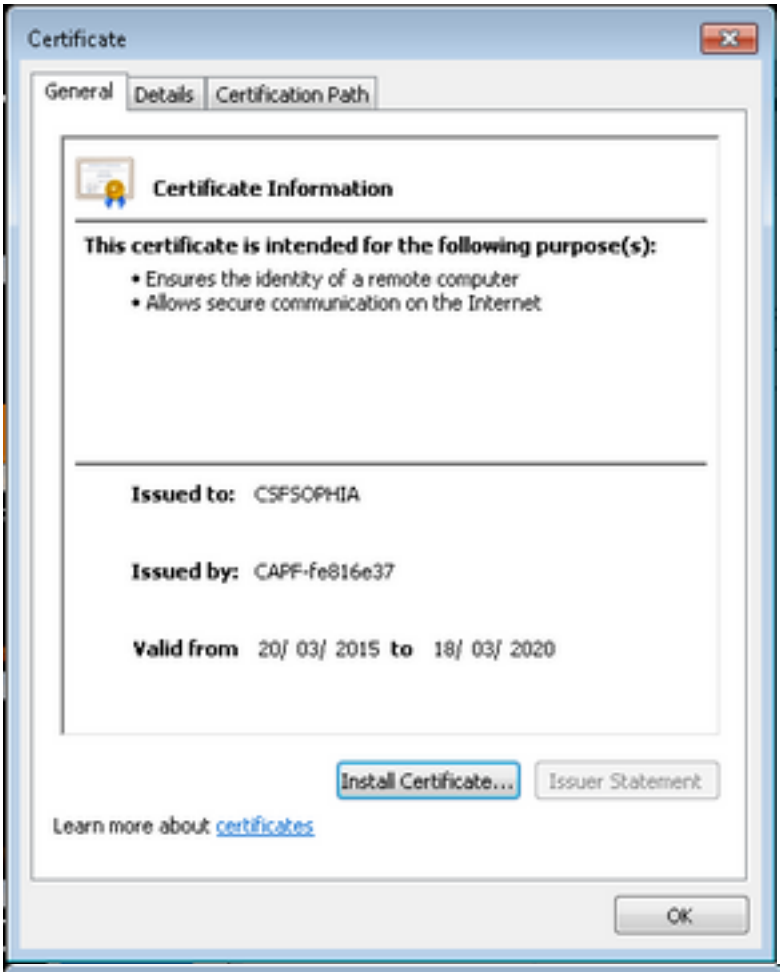
Vergelijk de LSC wanneer CAPF zelf en een CAPF met CA-handtekening worden ondertekend:

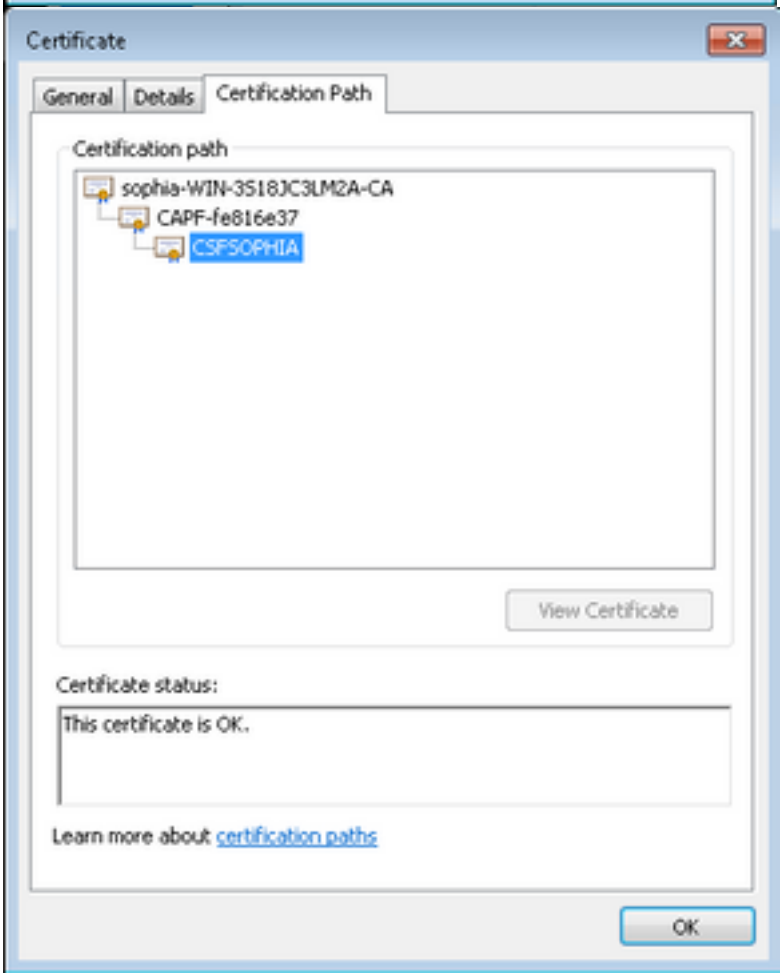
Zoals u aan deze beelden voor LSC kunt zien, is CAPF vanuit LSC gezichtspunt de wortel CA wanneer u zelfgetekende CAPF gebruikt maar CAPF is de ondergeschikte (tussenliggende) CA terwijl u CA-ondertekend CAPF gebruikt.

LSC bij zelfgetekende CAPF



LSC bij een CA-ondertekend CAPF





Waarschuwing:

De Jabber-client-LSC waarop de gehele certificeringsketen in dit voorbeeld wordt weergegeven, verschilt van de IP-telefoon. Aangezien IP-telefoons zijn ontworpen op basis van RFC 5280 (3.2. Certificatiepaden en vertrouwen), ontbreekt de AKI (Authority Key Identifier), en is CAPF en het basiscertificaat van CA niet aanwezig in de certificeringsketen. Het ontbreken van het CAPF/Root CA-certificaat in de certificeringsketen zal enige kwestie aan ISE veroorzaken om IP-telefoons tijdens 801.x-verificatie te certificeren zonder de CAPF- en Root-certificaten aan de ISE te uploaden. Er is een andere optie in CUCM 12.5 waarbij LSC rechtstreeks is ondertekend door externe offline CA, zodat het CAPF-certificaat niet naar ISE hoeft te worden geüpload voor IP-telefoon 802.1x-verificatie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

Bekend defect: CA-ondertekend CAPF-certificaat, basiscertificaat moet als CM-trust worden geüpload:

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