Configuratievoorbeeld van CUCM door derden voor CA-ondertekende LSC's

Inhoud

Inleiding

Lokaal significante certificaten (LSC's) van de certificaatinstantie Proxy-functie (CAPF) worden lokaal ondertekend. Mogelijk hebt u echter telefoons nodig om met de door derden ondertekende LSC's (certificaatautoriteit (CA) van derden te gebruiken. Dit document beschrijft een procedure die u hierbij helpt.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Cisco Unified Communications Manager (CUCM).

Gebruikte componenten

De informatie in dit document is gebaseerd op CUCM versie 10.5(2); deze optie werkt echter vanaf versie 10.0 en hoger.

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 live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Hier volgen de stappen die bij deze procedure betrokken zijn, die elk in de eigen sectie worden beschreven:

1. Het CA-wortelcertificaat uploaden
2. Offline CA instellen voor certificaatafgifte op endpoint
3. Genereert een CSR-aanvraag (certificaatsignalering) voor de telefoons
4. Verkrijg de gegenereerde CSR van Cisco Unified Communications Manager (CUCM) naar de FTP-server
5. Ontvang het telefooncertificaat via CA
6. .cer converteren naar .der Format
7. Comprimeer de certificaten (.der) tot .tgz formaat
8. Transfer het .tgz-bestand naar de Secure Shell FTP-server (SFTP)
9. Het .tgz-bestand naar de CUCM-server importeren
10. Teken de CSR met Microsoft Windows 2003 certificaatinstantie
11. Ontvang het wortelcertificaat van de CA

Het CA-wortelcertificaat uploaden

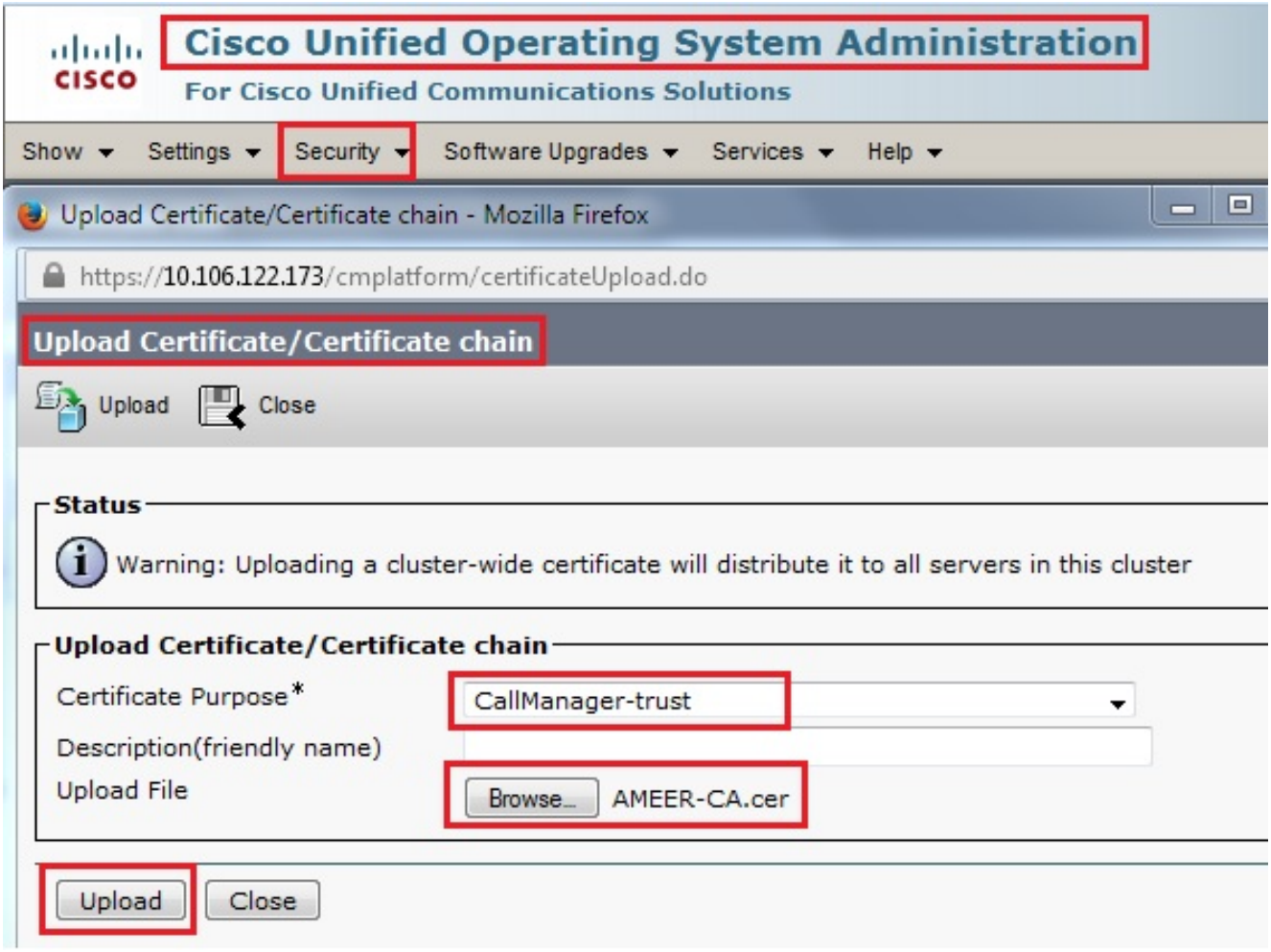
1. Meld u aan in de Cisco Unified Operating System (OS) Administration Web GUI.

2. Navigeer in op **Security certificaatbeheer**.

3. Klik op **Certificaat uploaden/certificaatketen**.

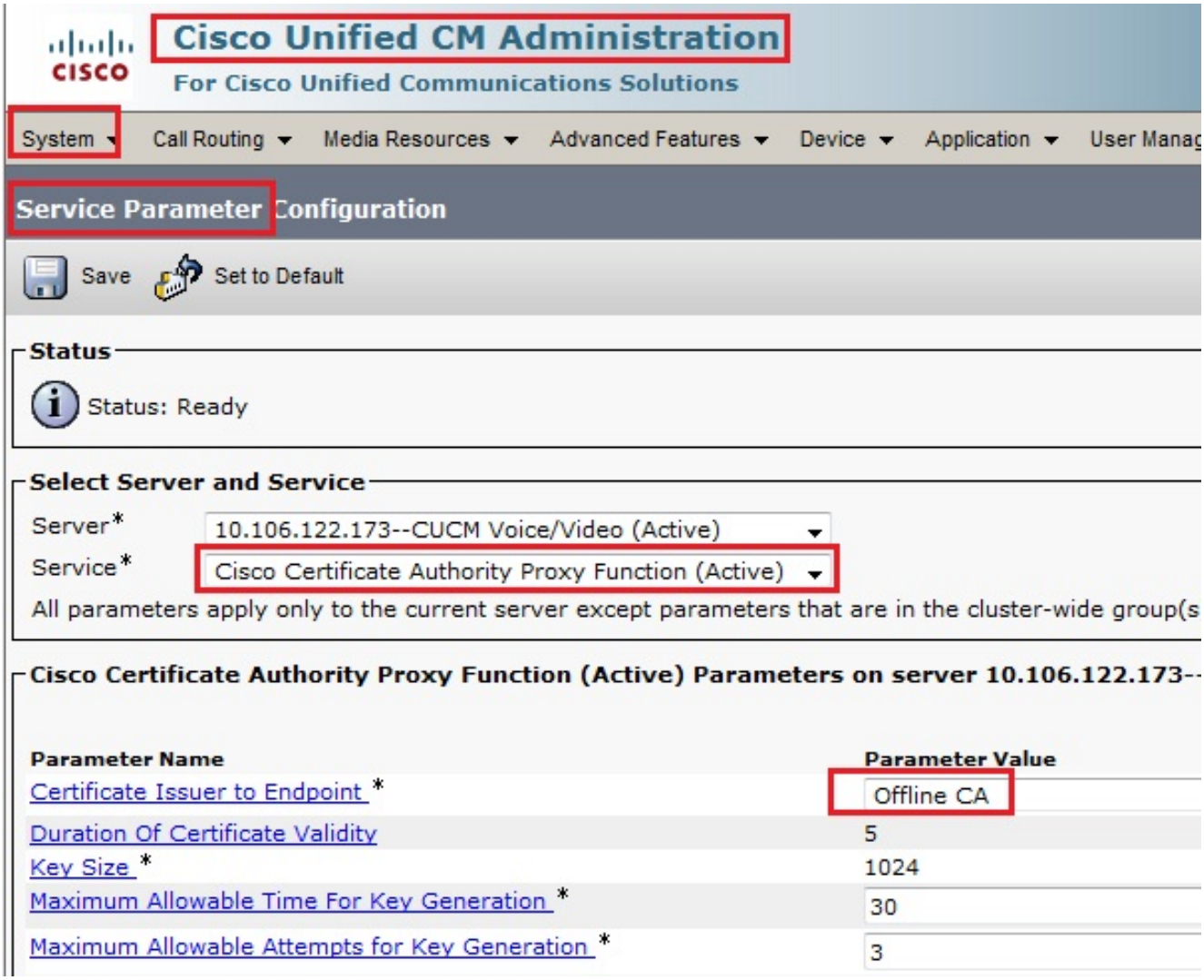
4. Kies **CallManager-**trust onder certificaatdoel.

5. Bladeren naar het basiscertificaat van de CA en klik op **Upload**.



Offline CA instellen voor certificaatafgifte op endpoint

1. Log in op de CUCM Administration web GUI.
2. Navigeer naar **System > Service Parameter**.
3. Kies de CUCM Server en selecteer de optie **Cisco Certificate Authority Proxy** voor de Service.
4. Selecteer **Offline CA** voor certificaatuitgifte aan endpoint.



Genereert een CSR-aanvraag (certificaatsignalering) voor de telefoons

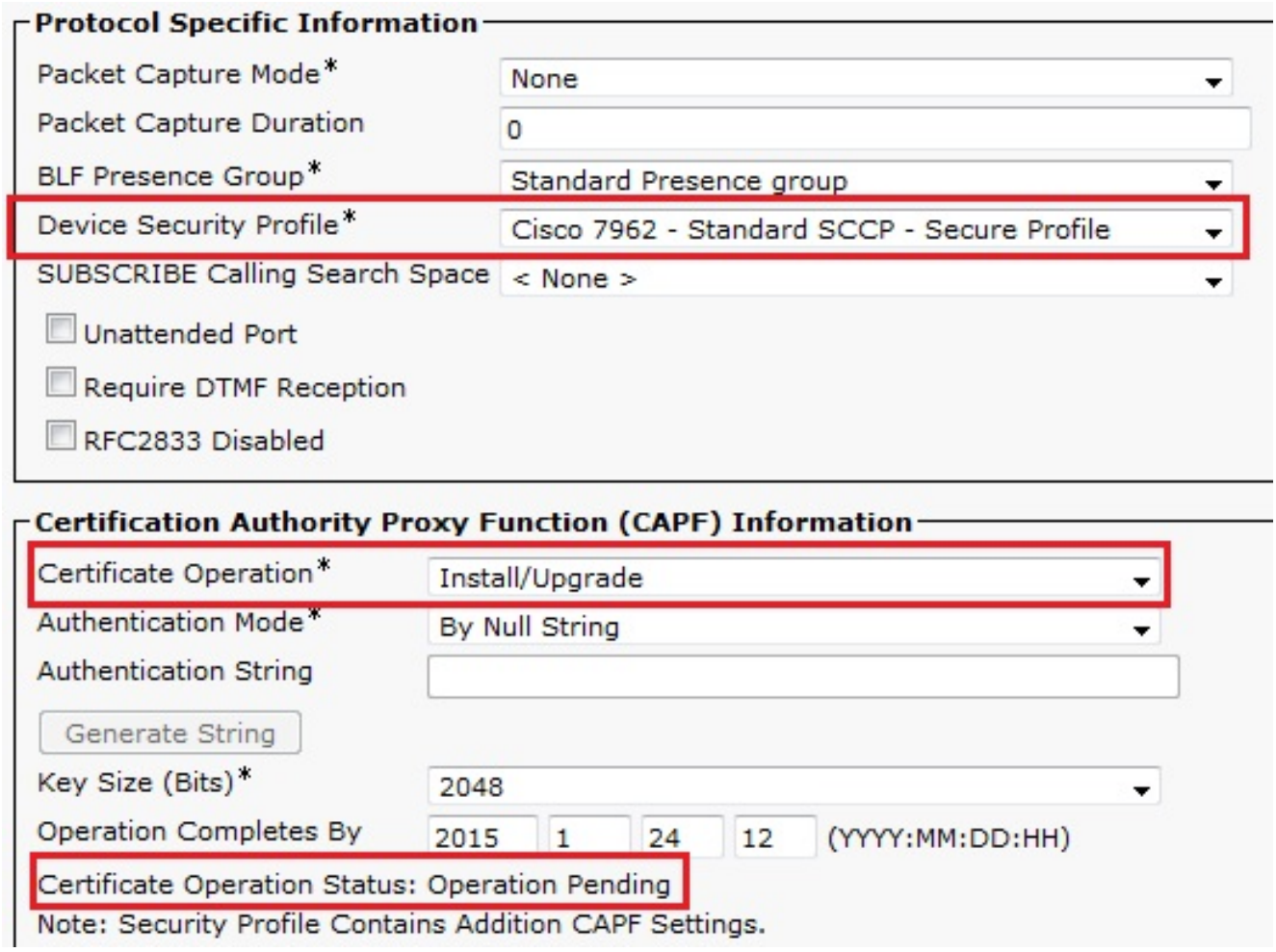
1. Log in op de CUCM Administration web GUI.

2. Navigeren naar **apparaattelefoons**.

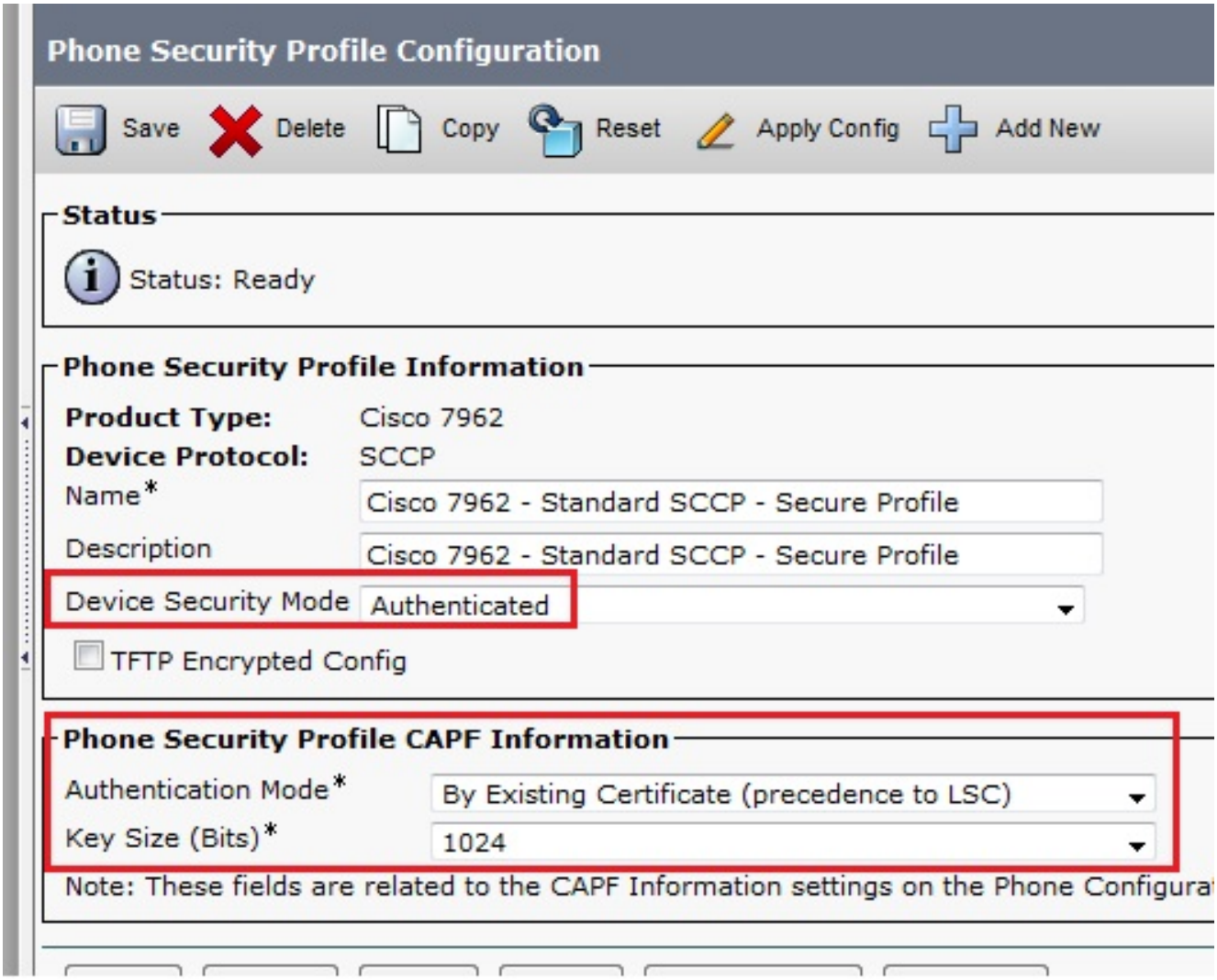
3. Kies de telefoon waarvan LSC door de externe CA moet worden ondertekend.

4. Verander het veiligheidsprofiel van het apparaat in een beveiligd (indien niet aanwezig, voeg één systeem aan het veiligheidsprofiel van de telefoon toe).

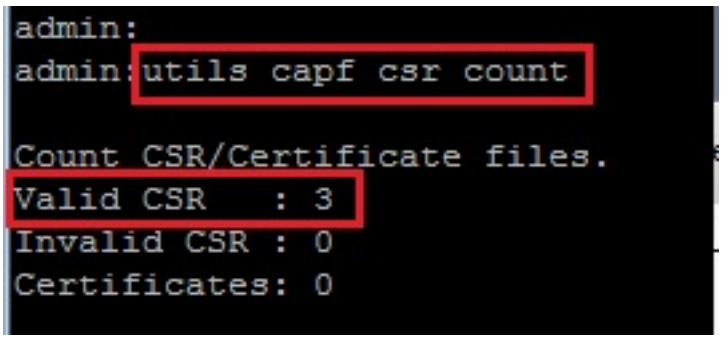
5. Kies op de pagina met de telefoonconfiguratie, onder het gedeelte CAPF, **Installatie/upgrade** voor de certificeringshandeling. Voltooi deze stap voor alle telefoons waarvan de LSC door de externe CA moet worden ondertekend. U dient de **werking** te **wachten** tot aan de besturingsstatus van het certificaat.



Telefonisch beveiligingsprofiel (7962-model).



Voer het opdracht **utils capf csr-telling** in in de SSH-sessie (Secure Shell) om te bevestigen dat er een CSR wordt gegenereerd. (Deze screenshot laat zien dat er een CSR is gegenereerd voor drie telefoons.)



Opmerking: De status van de certificaatbediening onder de sectie CAPF van de telefoon blijft in de **Handeling in afwachting van** staat.

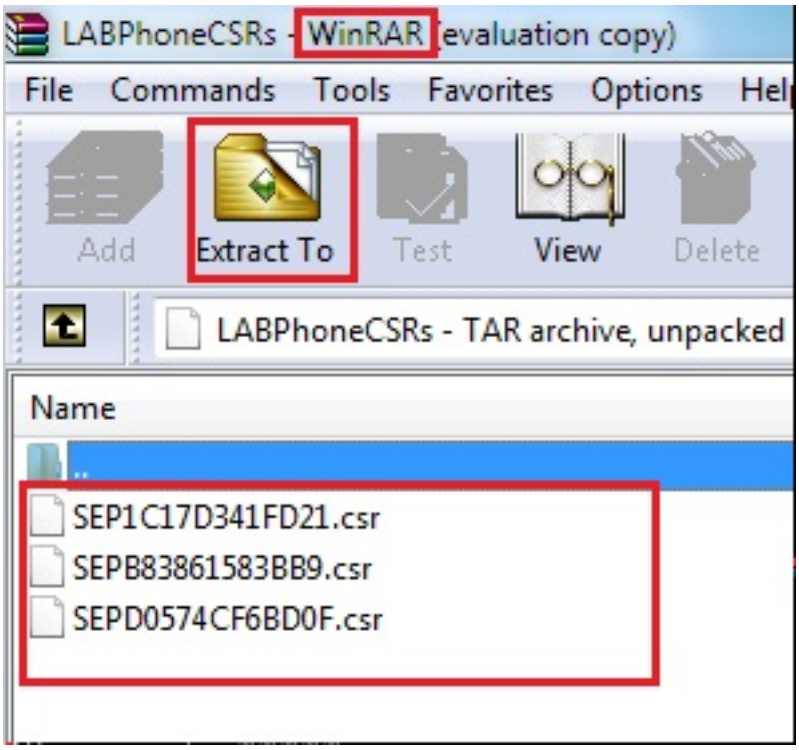
Ontvang de gegenereerde CSR van CUCM naar de FTP- (of TFTP-server)

1. SSH in de CUCM-server.

2. Voer de **utils capf csr stortbuis uit**. In deze screenshot is te zien hoe het dumpen naar het FTP wordt overgebracht.

```
admin:
admin:utils capf csr dump

Dump CSR files.
CSR File tarred successfully...

Destination:

 1) Remote Filesystem via FTP
 2) Remote Filesystem via TFTP
 3) Local Download Directory
 q) quit

Please select an option (1 - 3 or "q" ): 1
File Path: LABPhoneCSRs
Server: 10.65.43.173
User Name: cisco
Password: *****
File exported successfully
```

3. Open het vuilbestand met WinRAR en haal de CSR naar uw lokale machine.



Telefonisch certificaat verkrijgen

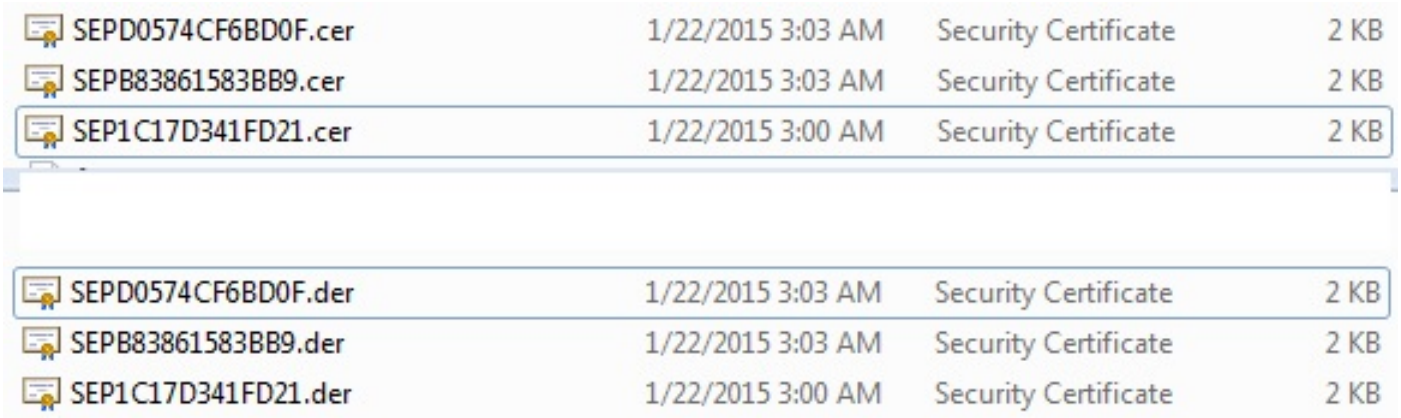
1. Stuur de CSR's van de telefoon naar de CA.

2. De CA biedt u een ondertekend certificaat.

Opmerking: U kunt een Microsoft Windows 2003-server als CA gebruiken. De procedure om de CSR te ondertekenen met een Microsoft Windows 2003 CA wordt later in dit document uitgelegd.

.cer converteren naar .der Format

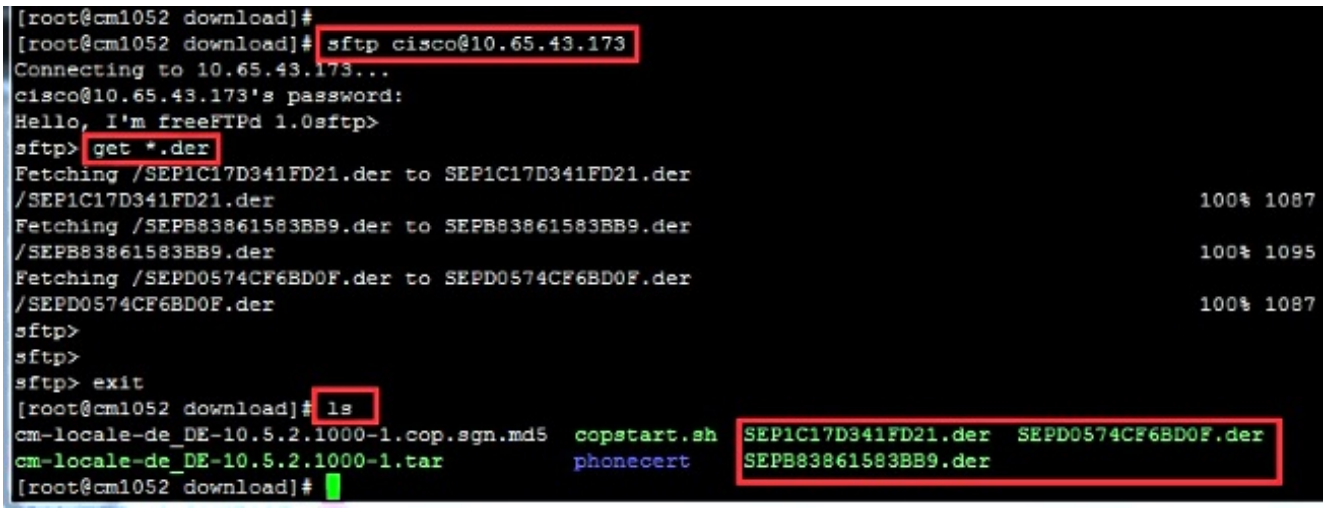
Als de ontvangen certificaten in .cer formaat zijn, dan hernoemen ze deze door .der.



Comprimeer de certificaten (.der) tot .tgz formaat

U kunt de root (Linux) van de CUCM-server gebruiken om de certificaatindeling te comprimeren. Je kunt dit ook doen in een normaal Linux systeem.

1. Breng alle ondertekende certificaten met de SFTP-server over aan het Linux-systeem.



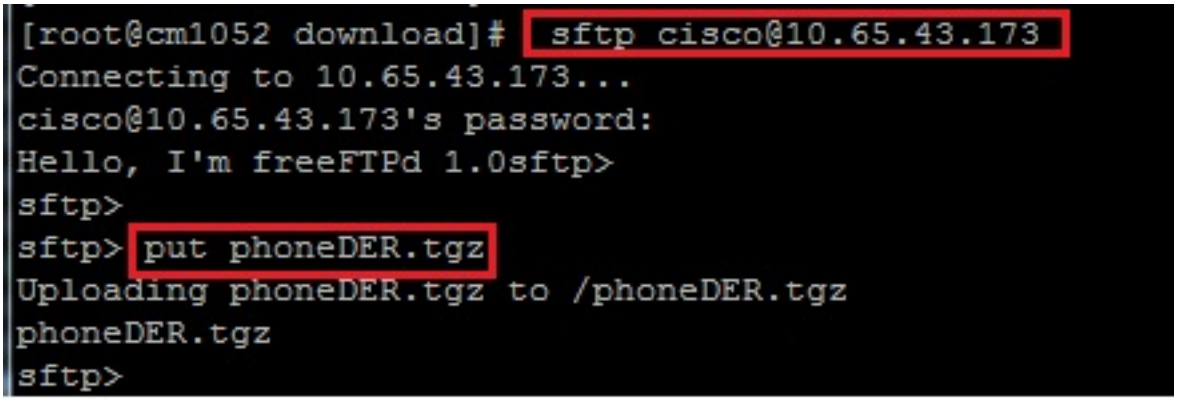
2. Typ deze opdracht om alle .der certificaten in een .tgz-bestand te comprimeren.

```
tar -zcvf
```

```
[root@cm1052 download]#
[root@cm1052 download]# tar -zcvf phoneDER.tgz *.der
SEP1C17D341FD21.der
SEPB83861583BB9.der
SEPD0574CF6BD0F.der
[root@cm1052 download]# ls
cm-locale-de_DE-10.5.2.1000-1.cop.sgn.md5  copstart.sh  phoneDER.tgz          SEPB83861583BB9.der
cm-locale-de_DE-10.5.2.1000-1.tar          phonecert    SEP1C17D341FD21.der   SEPD0574CF6BD0F.der
[root@cm1052 download]#
```

Het .tgz-bestand naar de SFTP-server overbrengen

Voltooi de stappen in de schermopname om het .tgz-bestand naar de SFTP-server over te brengen.



Het .tgz-bestand naar de CUCM-server importeren

1. SSH in de CUCM-server.

2. Voer de **utils capf cert import-**opdracht uit.

```
admin:
admin utils capf cert import

Importing files.

Source:

 1) Remote Filesystem via FTP
 2) Remote Filesystem via TFTP
 q) quit

Please select an option (1 - 2 or "q" ): 1
File Path: phoneDER.tgz
Server: 10.65.43.173
User Name: cisco
Password: *****
Certificate file imported successfully
Certificate files extracted successfully.
Please wait. Processing 3 files
```

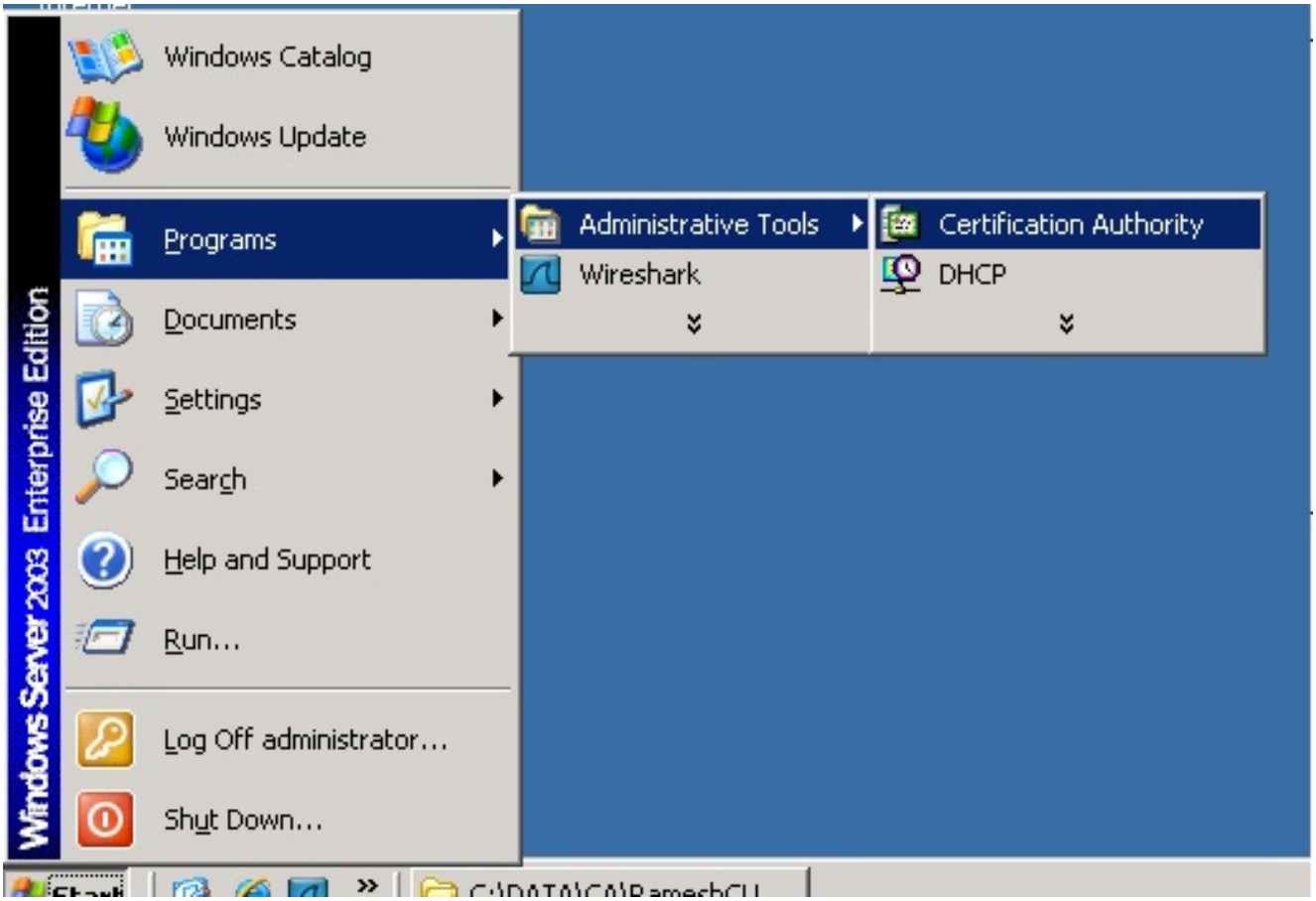
Zodra de certificaten met succes zijn geïmporteerd, kunt u zien dat de CSR-telling nul is.

```
admin:
admin:utils capf csr count

Count CSR/Certificate files.
Valid CSR   : 0
Invalid CSR : 0
Certificates: 0
```

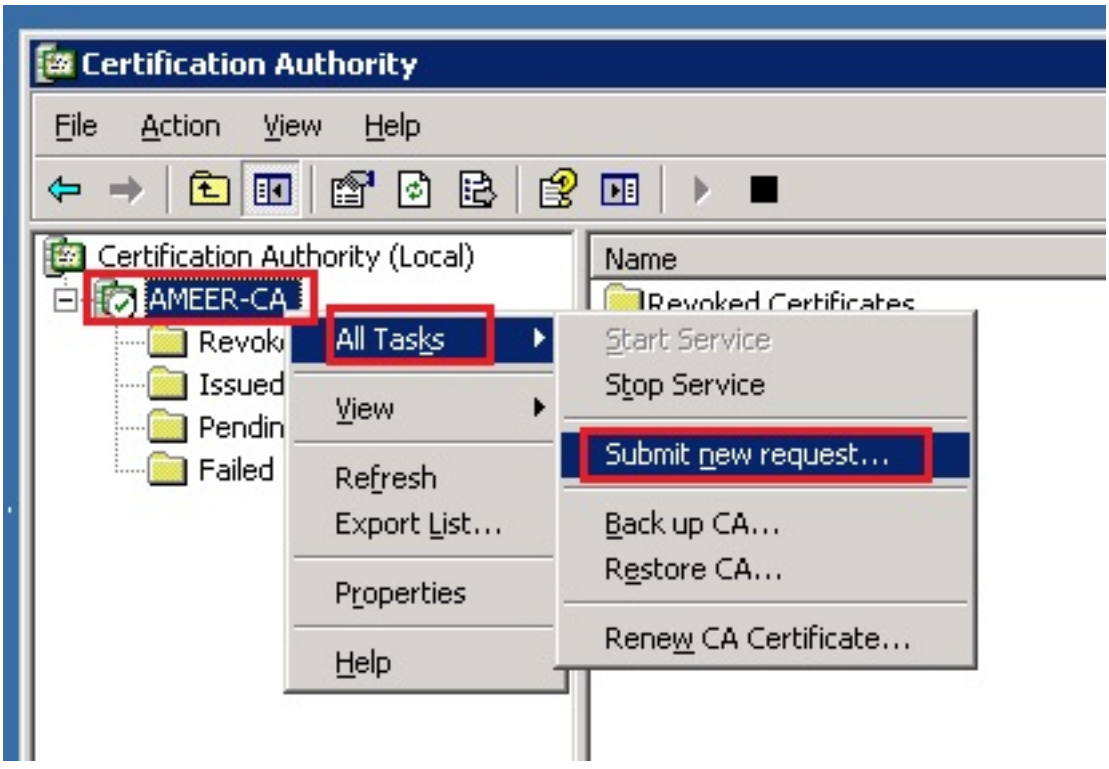
Teken de CSR met Microsoft Windows 2003 certificaatinstantie

Dit is optionele informatie voor Microsoft Windows 2003 - CA.

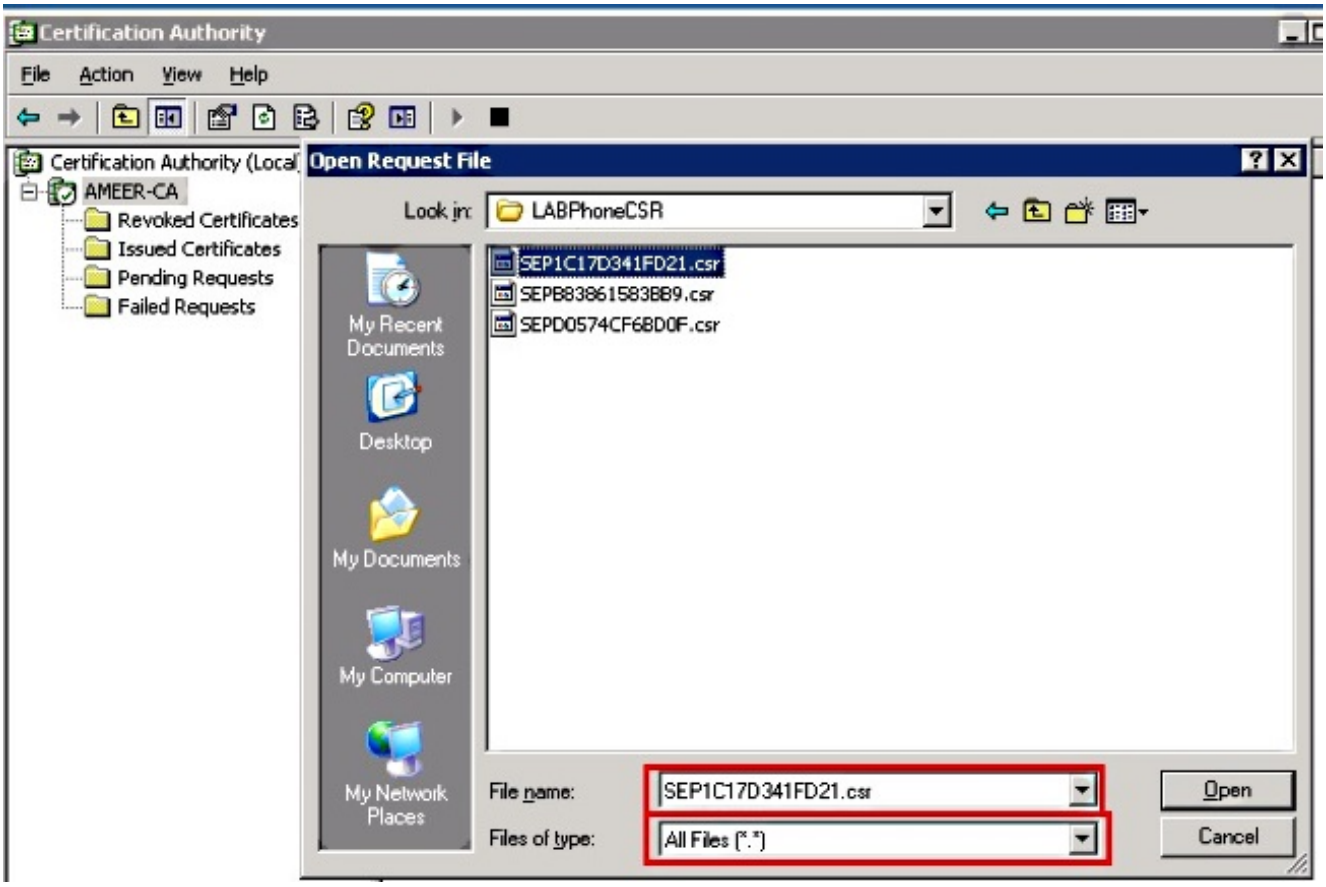
1. Open certificeringsinstantie.



2. Klik met de rechtermuisknop op CA en navigeer naar **Alle taken > Een nieuw verzoek indienen...**

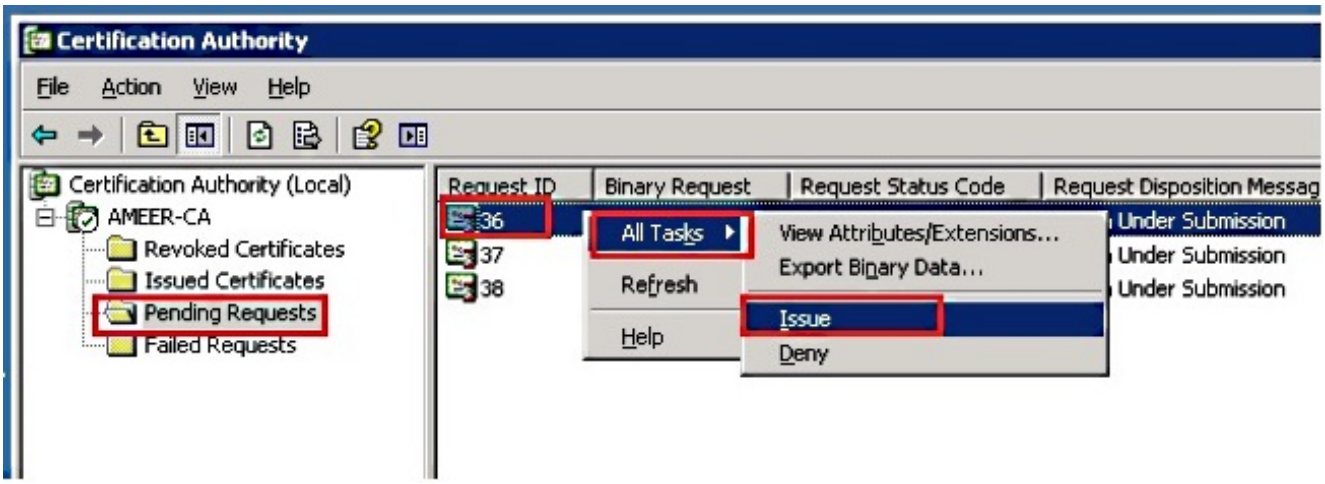


3. Selecteer de CSR en klik op **Openen**. Doe dit voor alle CSR's.



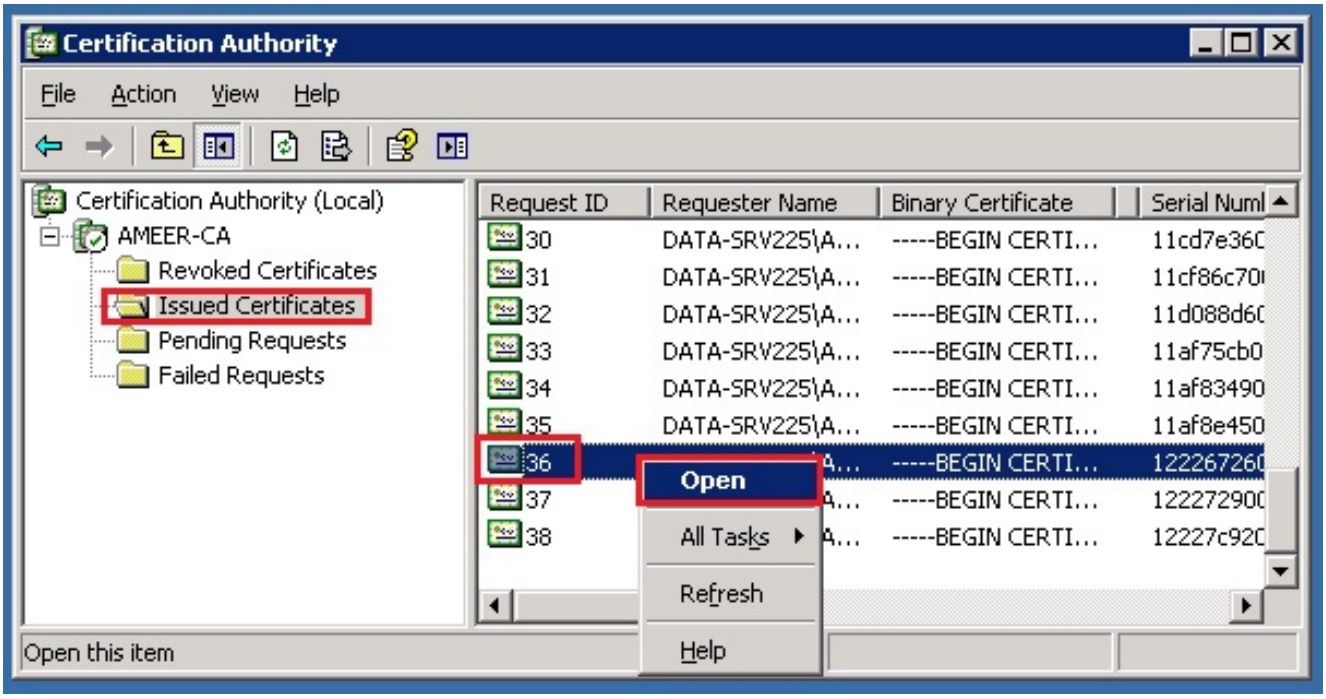
Alle geopende CSR-weergave in de map Verzoeken in behandeling.

4. Klik met de rechtermuisknop op elk en navigeer naar **Alle taken > Uitgeven** om certificaten uit te geven. Doe dit voor alle aanhangige verzoeken.

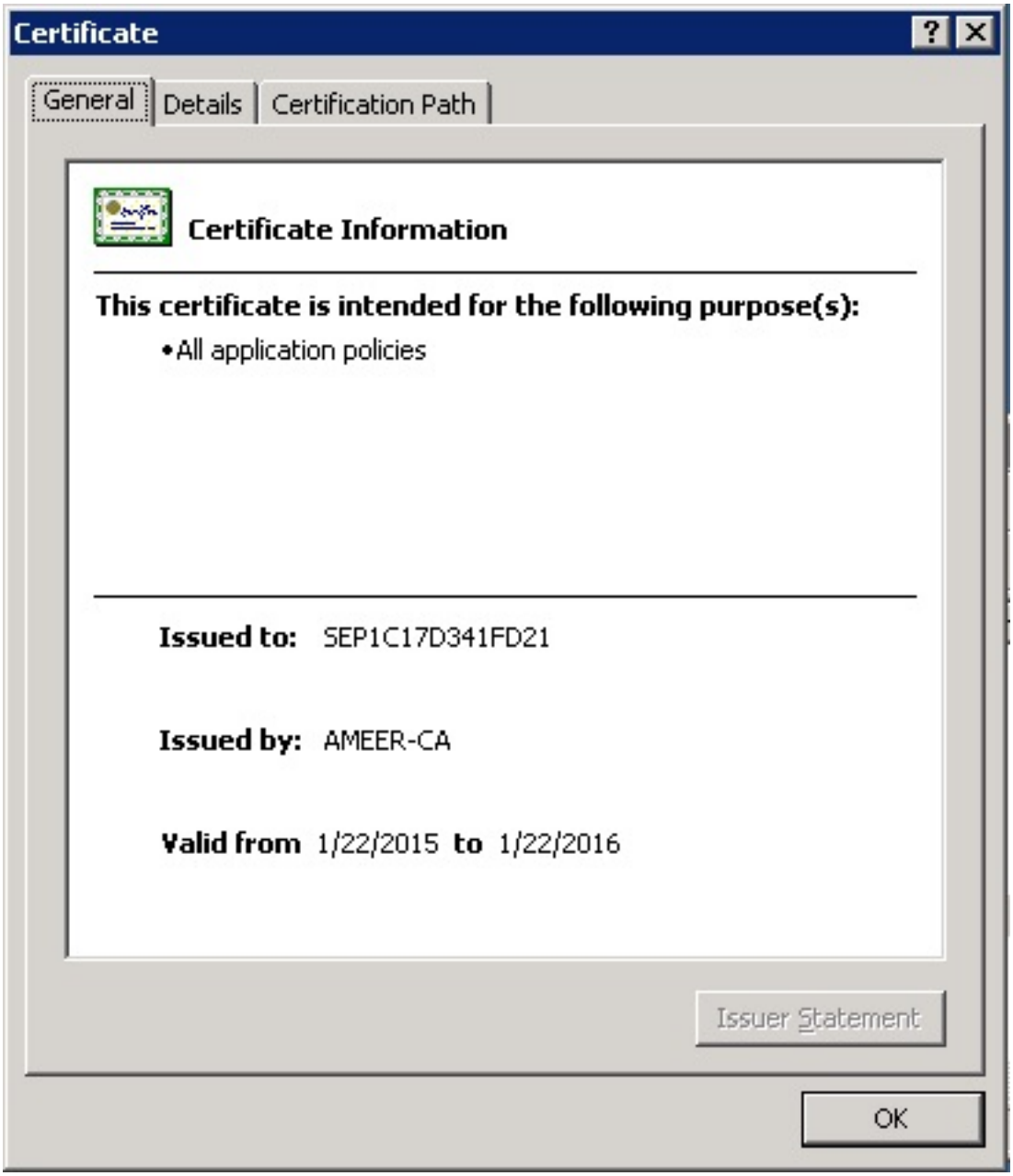


5. Kies een **afgegeven certificaat** om het certificaat te kunnen downloaden.

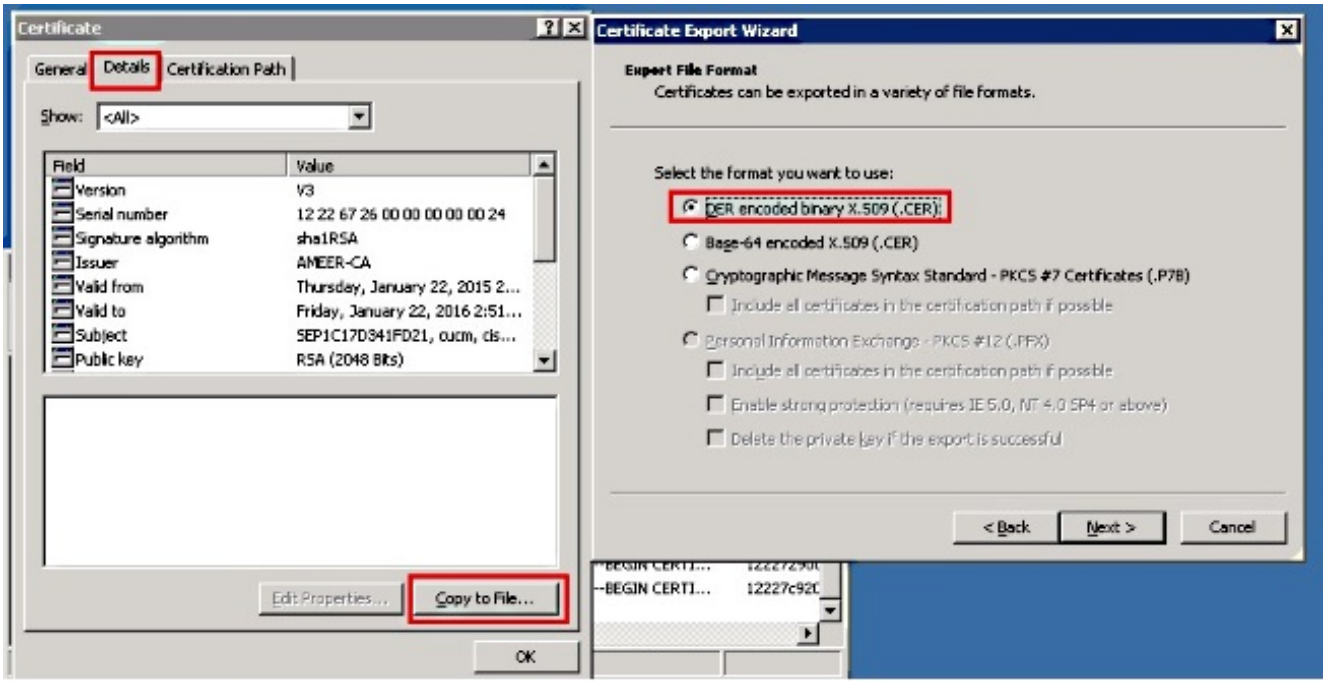
6. Klik met de rechtermuisknop op het certificaat en klik op **Openen**.



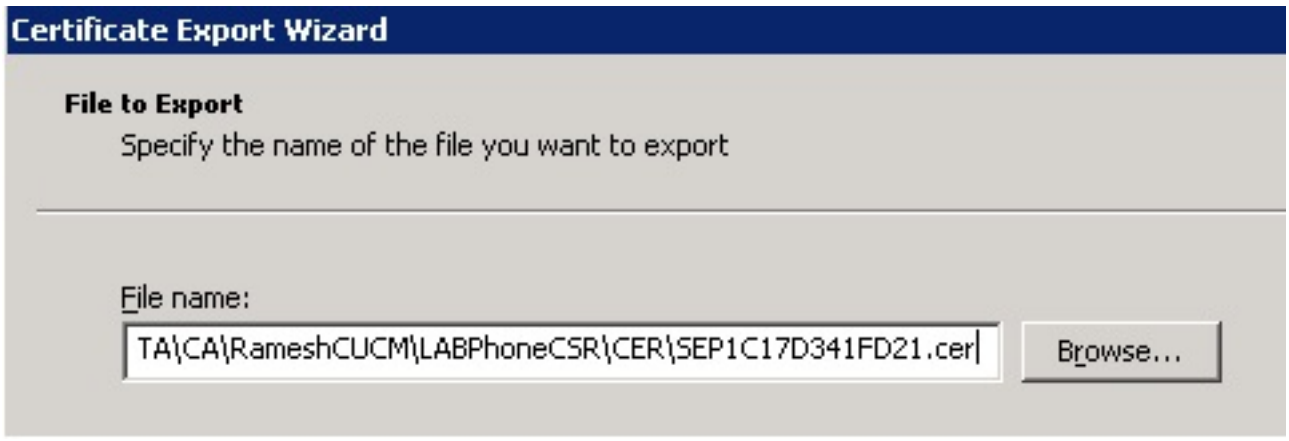
7. U kunt de certificeringsgegevens zien. Selecteer het tabblad Details en kies **Kopie naar bestand...**



8. Kies in de wizard Certificaat exporteren de optie **gecodeerde binaire X.509 (.CER)**.



9. Geef het bestand een geschikte naam. Dit voorbeeld gebruikt <MAC>.cer formaat.

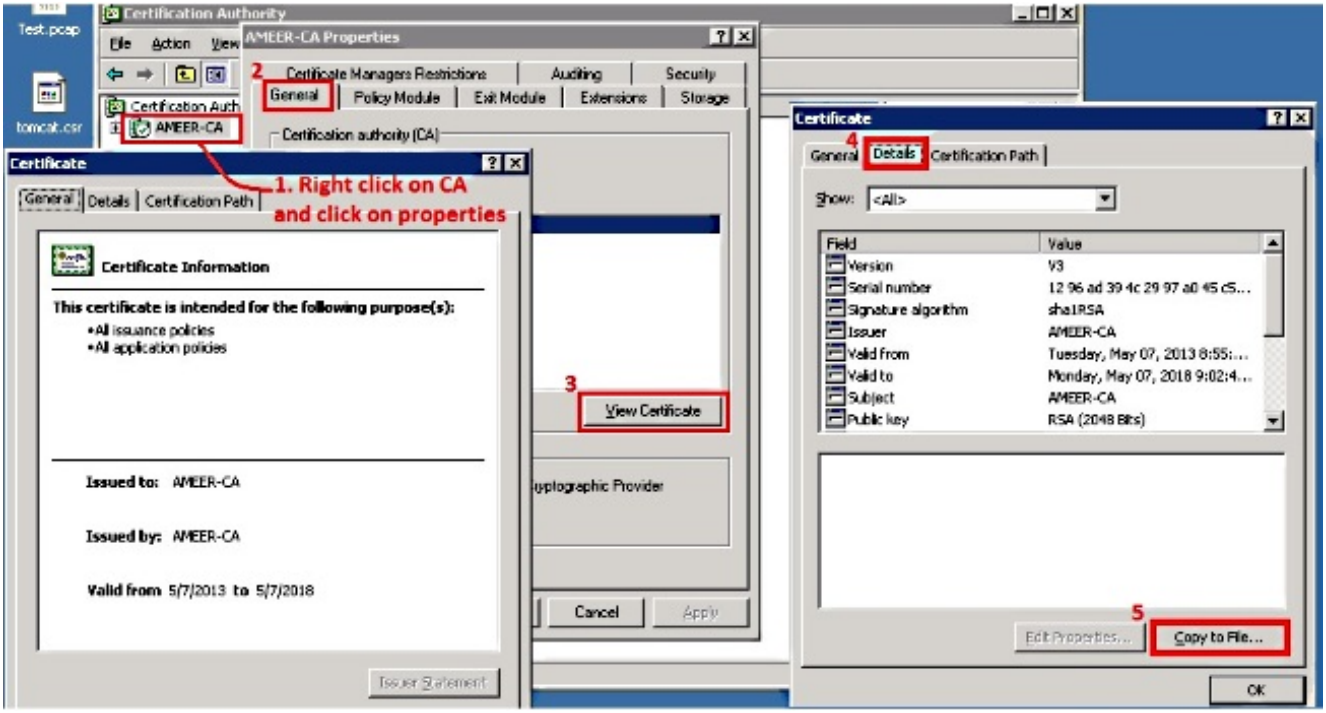


10. Ontvang de certificaten voor andere telefoons onder de Gegeven certificaatsectie met deze procedure.

Ontvang het wortelcertificaat van de CA

1. Open **certificeringsinstantie**.

2. Voltooi de stappen in dit schermshot om de root-CA te downloaden.

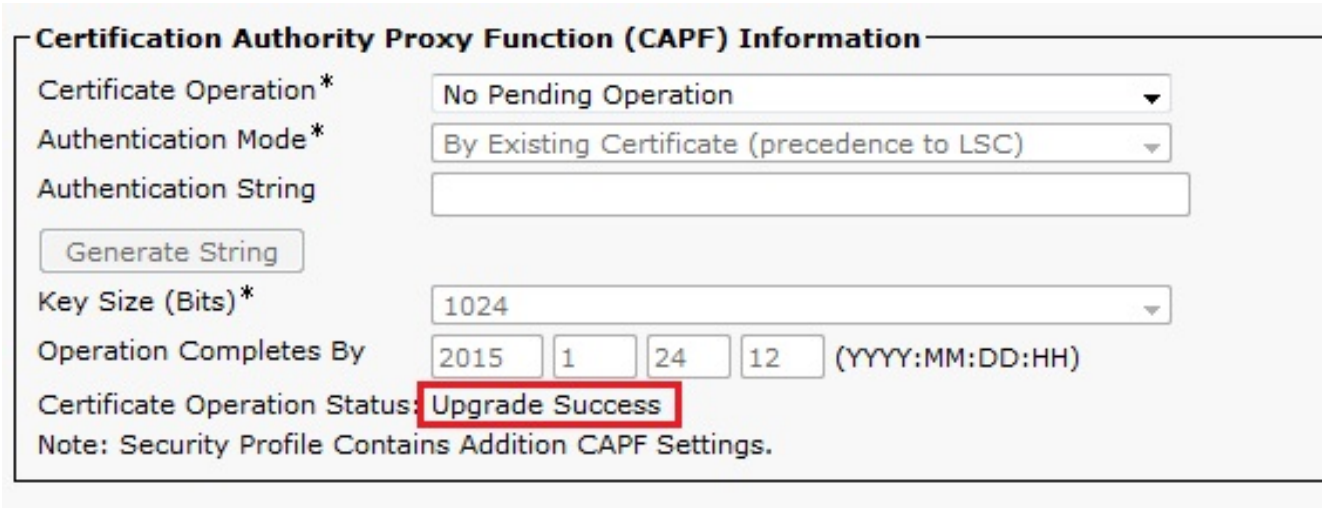


Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

1. Ga naar de pagina voor telefoonconfiguratie.

2. Onder het gedeelte CAPF, zou de status van de Certificaatbediening als **succes van de upgrade** moeten tonen.



Opmerking: Raadpleeg LSC's die door derden zijn ondertekend, genereren en importeren voor meer informatie.

Problemen oplossen

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