Unified CM-oplossing: Procedure voor het verkrijgen en uploaden van CA-certificaten van derden (versie 11.x)

Inhoud

Inleiding

Dit document heeft tot doel gedetailleerd uit te leggen welke stappen zijn ondernomen om een certificaat van certificeringsinstantie (CA) te verkrijgen en te installeren, dat is gegenereerd door een verkoper van derden, om een HTTPS-verbinding op te zetten tussen Finse, Cisco Unified Intelligence Center (CUIC) en Live Data (LD)-servers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Contact Center Enterprise (UCCE)
- Cisco Live Data (LD)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Finesse
- CA-certificering

Gebruikte componenten

De in het document gebruikte informatie is gebaseerd op de versie van UCCE-oplossing 11.0(1).

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 leeft, zorg ervoor dat u de potentiële impact van om het even welke stap begrijpt.

Achtergrondinformatie

Om HTTPS te kunnen gebruiken voor veilige communicatie tussen Finesse, CUIC en Live Data servers, zijn beveiligingscertificaten nodig. Deze servers bieden standaard zelfgetekende certificaten die worden gebruikt of klanten kunnen certificaten van de certificeringsinstantie (CA) aanschaffen en installeren. Deze CA-certs kunnen worden verkregen bij een derde verkoper zoals VeriSign, Thawte, GeoTrust of kunnen worden geproduceerd in het buitenland.

Configureren

Voor het instellen van een certificaat voor HTTPS-communicatie in Finesse-, CUIC- en Live-gegevensservers moeten de volgende stappen worden gezet:

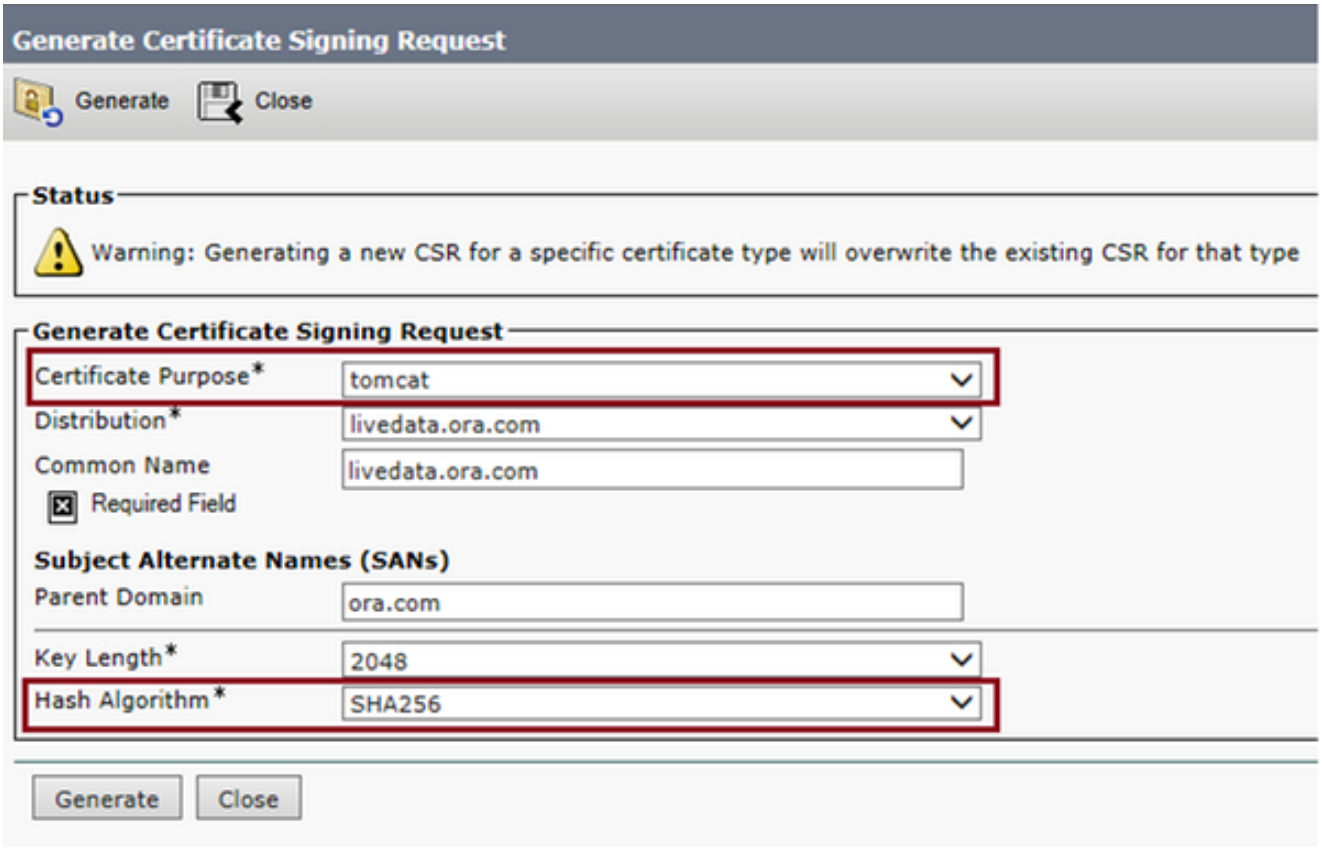
1. certificaataanvraag genereren en downloaden (CSR).
2. Aanvragen van wortel, tussenproduct (indien van toepassing) en aanvraagcertificaat van de certificeringsinstantie met behulp van CSR.
3. Certificaten uploaden naar de servers.

Stap 1. Generate en download certificaataanvraag (CSR).

1. De hier beschreven stappen voor het genereren en downloaden van CSR zijn dezelfde voor Finesse-, CUIC- en Live-gegevensservers.

2. Open de pagina **Cisco Unified Communications Operating System** Management met de aangegeven URL en teken in met de OS-beheeraccount die tijdens het installatieproces is gemaakt
   https://FQDN:8443/cmplatform

3. Genereert de certificaataanvraag (CSR) zoals in de afbeelding getoond:

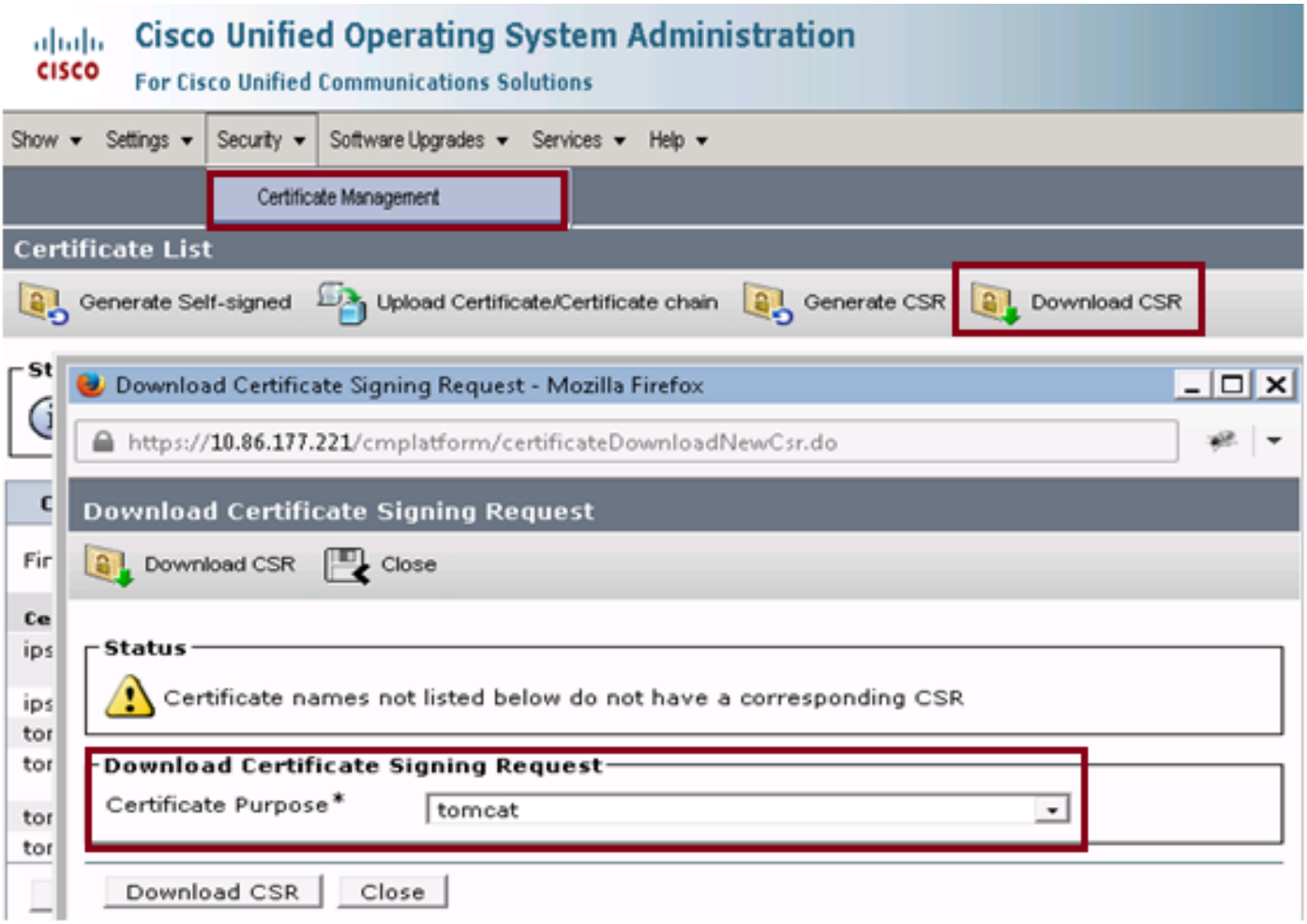


Stap 1. Navigeer naar **security > certificaatbeheer > Generate CSR**.Stap 2. Selecteer de gewenste naam in de vervolgkeuzelijst certificaatdoel.Stap 3. Selecteer Hash Algorithm en key length, afhankelijk van de zakelijke behoeften.

- Sleutellengte: 2048 voor \ Hash Algoritme SHA256 wordt aanbevolen

Stap 4. Klik op **Generate CSR**.**Opmerking**: Als voor het bedrijf is vereist dat het veld Land Alternate Name (SAN's) van het moederdomein wordt ingevuld met de domeinnaam, dan is u op de hoogte van de uitgifteadressen in het document "SAN's"-kwestie met een door derden ondertekend certificaat in finesse."

4. Download de certificaataanvraag (CSR) zoals weergegeven in de afbeelding:



Stap 1. Navigeer naar **Security > certificaatbeheer > Download CSR**.
Stap 2. Selecteer de gewenste optie in de vervolgkeuzelijst certificaatnaam.
Stap 3. Klik op **CSR downloaden**.

Opmerking:

> Opmerking: Voer de bovengenoemde stappen op de secundaire server uit met behulp van de URL **https://FQDN:8443/cmplatform** om CSR's voor certificaatinstantie te verkrijgen

Stap 2. Neem Opslag, Intermediate (indien van toepassing) en Toepassingscertificaat van de certificaatinstantie.

1. Verstrek de informatie over de primaire en secundaire servers certificaataanvraag (CSR) aan de certificeringsinstantie van derden zoals VeriSign, Thawte, GeoTrust, enz.

2. Van de certificeringsinstantie dient de volgende certificeringsketen voor de primaire en de secundaire servers te worden ontvangen.

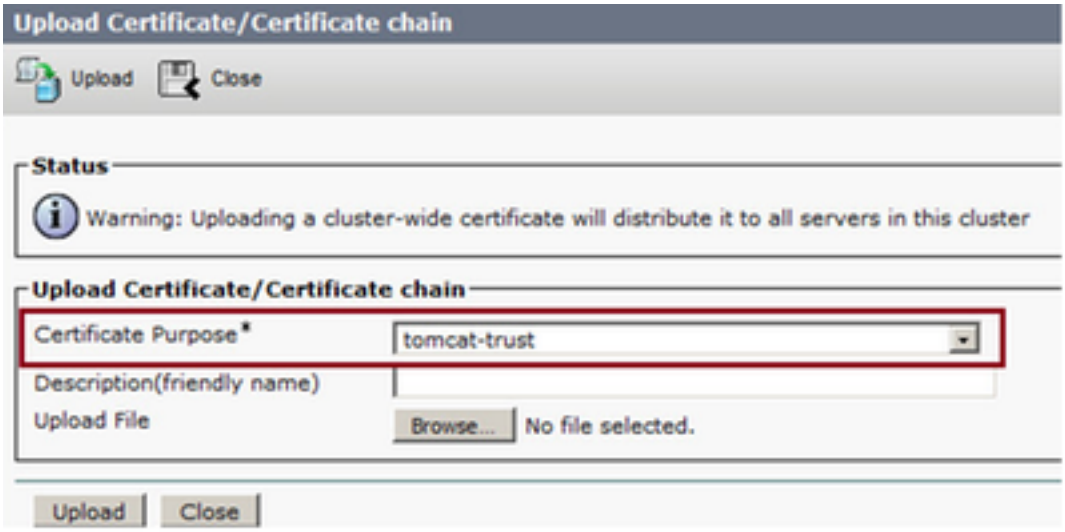
- **Finse servers: Opstarten, middelgroot (optioneel) en toepassingscertificaat**
- **CUIC-servers: Opstarten, middelgroot (optioneel) en toepassingscertificaat**
- **Live-gegevens dienen: Opstarten, middelgroot (optioneel) en toepassingscertificaat**

Stap 3. Uploadcertificaten aan de servers.

In dit gedeelte wordt beschreven hoe de certificeringsketen op Finse, CUIC- en Live-

gegevensservers correct kan worden geüpload.

Eindservers

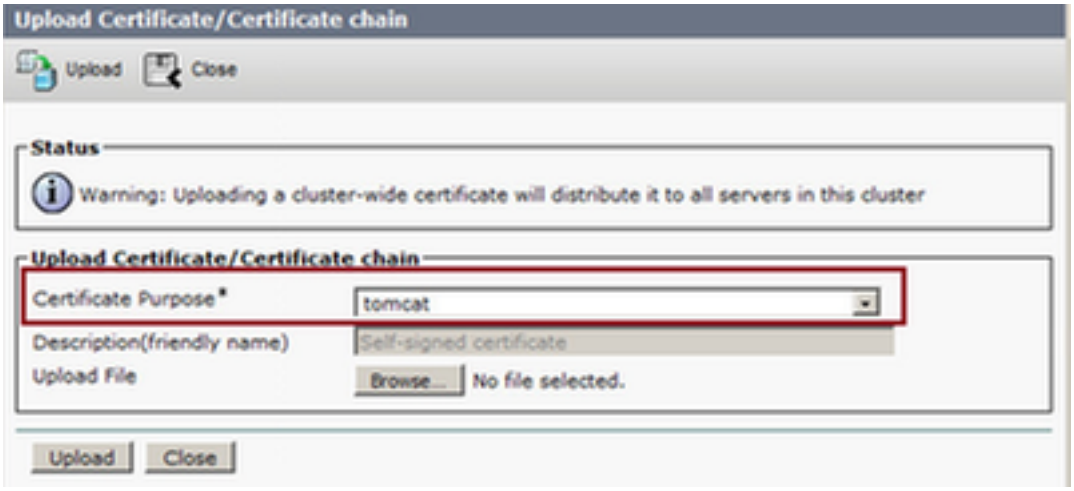


1. Upload het certificaat van Opstarten op Primaire Server met behulp van deze stappen:

   Stap 1. Ga op de primaire server naar Cisco Unified Communications Operating System Management-pagina **Beveiliging > certificaatbeheer > Uploadcertificaat.**
   Stap 2. Selecteer de optie Vertrouwen in de vervolgkeuzelijst certificaatnaam.
   Stap 3. Klik in het veld Upload File op Bladeren en blader naar het broncertificeringsbestand.
   Stap 4. Klik op Upload File.

2. Upload het intermediaire certificaat op Primaire Finse server met behulp van deze stappen:

   Stap 1. Stappen bij het uploaden van het tussentijdse certificaat zijn gelijk aan het basiscertificaat zoals in stap 1 is weergegeven.
   Stap 2. Ga op de primaire server van Cisco Unified Communications Operating System Management-pagina naar **Security > certificaatbeheer > Upload Certificate.**
   Stap 3. Selecteer de optie Eigennaam in de vervolgkeuzelijst certificaatnaam.
   Stap 4. Klik in het veld Upload File op Bladeren en blader naar het middelbare certificeringsbestand.
   Stap 5. Klik op **Upload**.Opmerking: Aangezien de Tomcat-trust-winkel tussen de primaire en secundaire servers wordt gerepliceerd, is het niet nodig om de wortel- of Intermediate-certificaat te uploaden naar de secondaire finesse server.
3. Upload het certificaat van de Primaire Finse server zoals in de afbeelding getoond:



Stap 1. Selecteer de gewenste optie in de vervolgkeuzelijst certificaatnaam.Stap 2. In het veld Upload File klikt u op **Bladeren** en vervolgens bladert u naar het toepassingscertificaatbestand.
Stap 3. Klik op **Upload** om het bestand te uploaden.

4. Upload het Secundaire FineReader Server-toepassingscertificaat.
   In deze stap fVolg hetzelfde proces als vermeld in Stap 3 op de secundaire server voor het eigen toepassingscertificaat.

5. U kunt de servers nu opnieuw opstarten.
   Toegang tot de CLI op de primaire en secundaire Finesse-servers en **start** het **systeem** van het commando-**utils opnieuw** om de servers opnieuw te starten.

CUIC-servers (aangenomen dat er geen intermediaire certificaten aanwezig zijn in de certificeringsketen)

1. Upload Root certificaat op primaire CUIC server.

   Stap 1. Ga op de primaire server van Cisco Unified Communications Operating System Management-pagina naar **Security > certificaatbeheer > Upload certificaatketen**.
   Stap 2. Selecteer de optie Vertrouwen in de vervolgkeuzelijst certificaatnaam.
   Stap 3. Klik in het veld Upload File op Bladeren en blader naar het broncertificeringsbestand.
   Stap 4. Klik op Upload File.Opmerking: Aangezien de tomcat-trust-winkel tussen de primaire en secundaire servers wordt gerepliceerd, hoeft het wortelcertificaat niet te worden geüpload naar de Secundaire CUIC-server.

2. Primair CUIC-servertoepassingscertificaat uploaden.

   Stap 1. Selecteer de gewenste optie in de vervolgkeuzelijst certificaatnaam.
   Stap 2. Klik in het veld Upload File op Bladeren en blader naar het toepassingscertificaatbestand.
   Stap 3. Klik op Upload File.
3. Upload secondair CUIC server Application Certificate.
   Volg het zelfde proces zoals vermeld in stap (2) op de secundaire server voor zijn eigen toepassingscertificaat

4. Herstart servers
   Toegang tot de CLI op de primaire en secundaire CUIC-servers en voer de opdracht **"utils system start"** in om de servers opnieuw te starten.
   Opmerking: Als de CA-autoriteit de certificeringsketen biedt die intermediaire certificaten omvat, dan zijn ook de stappen die in de sectie Finse servers zijn vermeld van toepassing op CUIC-servers.

Live-datacservers

1. De stappen die op Live-Data-servers worden ondernomen om de certificaten te uploaden, zijn identiek aan Finse of CUIC-servers, afhankelijk van de certificeringsketen.

2. Opslagcertificaat uploaden op Primaire Live-Data server.

   Stap 1. Ga op de primaire server van Cisco Unified Communications Operating System Management-pagina naar **Security > certificaatbeheer > Upload Certificate**.
   Stap 2. Selecteer de optie Vertrouwen in de vervolgkeuzelijst certificaatnaam.
   Stap 3. Klik in het veld Upload File op **browsen** en blader naar het broncertificeringsbestand.
   Stap 4. Klik op **Upload**.

3. Tussencertificaat uploaden op Primaire Live-Data server.

   Stap 1. Stappen bij het uploaden van het tussentijdse certificaat zijn gelijk aan het basiscertificaat zoals in stap 1 is weergegeven.
   Stap 2. Ga op de primaire server van Cisco Unified Communications Operating System Management-pagina naar **Security > certificaatbeheer > Upload Certificate**.
   Stap 3. Selecteer de optie Eigennaam in de vervolgkeuzelijst certificaatnaam.
   Stap 4. Klik in het veld Upload File op **browsen** en blader naar het middelbare certificeringsbestand.
   Stap 5. Klik op **Upload**.
   Opmerking: Aangezien de Tomcat-trust-winkel tussen de primaire en de secundaire servers wordt gerepliceerd, hoeft de wortel- of Intermediate-certificaat niet te worden geüpload naar de secundaire Live-Data-server.
4. Toepassingscertificaat voor primaire Live-gegevensserver uploaden.

   Stap 1. Selecteer de gewenste optie in de vervolgkeuzelijst certificaatnaam.
   Stap 2. In het veld Upload File klikt u op **Bladeren** en vervolgens bladert u naar het toepassingscertificaatbestand.
   Stap 3. Klik op **Upload**.

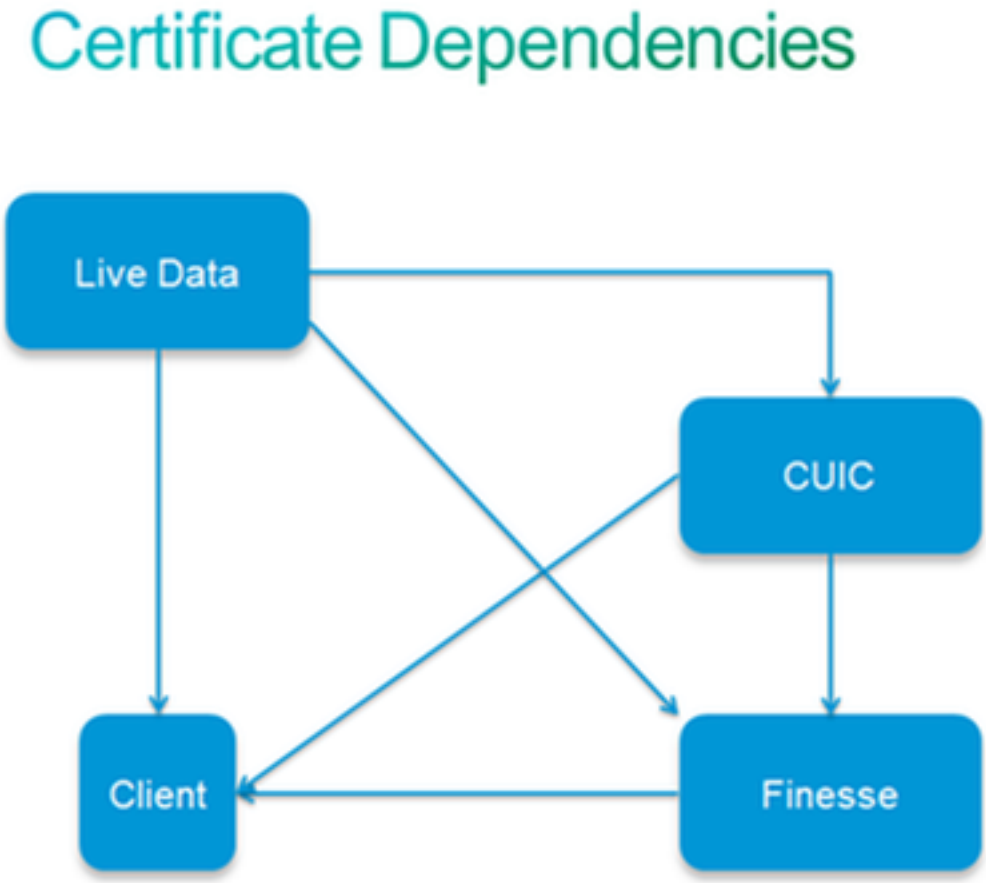
5. Certificaat voor secundaire Live-Data-server uploaden.
   Volg de stappen die hierboven in (4) zijn beschreven op de secundaire server voor het eigen aanvraagcertificaat.

6. Herstart servers
   Toegang tot de CLI op de primaire en secundaire Finse servers en voer de opdracht **"utils**

system start" in om de servers opnieuw te starten.

Licentie voor live-datacenterservers

Aangezien levende gegevensservers met CUIC- en Finse-servers samenwerken, zijn er certificeringsafhankelijkheden tussen deze servers zoals in de afbeelding te zien is:



Wat de certificatieketen van derden betreft, zijn de certificaten Root en Intermediate voor alle servers in de organisatie gelijk. Als resultaat voor een Live-gegevensserver om goed te kunnen werken, moet u ervoor zorgen dat de Fins- en CUIC-servers de Root- en intermediaire certificaten hebben die correct in de Tomcat-Trust-containers zijn geladen.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.