Navigeer door Client EKU Sunset met Expressway x15.5

Inleiding

In dit document wordt beschreven hoe u met Cisco Expressway x15.5 door de EKU-zonsondergang van de client navigeert.

Achtergrondinformatie

Digitale certificaten zijn elektronische referenties die worden uitgegeven door vertrouwde certificeringsinstanties (CA's) die de communicatie tussen servers en clients beveiligen door authenticatie, gegevensintegriteit en vertrouwelijkheid te waarborgen. Deze certificaten bevatten EKU-velden (Extended Key Usage) die hun doel definiëren:

- Serververificatie EKU (id-kp-serverAuth) wordt gebruikt wanneer een server zijn certificaat presenteert om zijn identiteit te bewijzen.
- Client Authentication EKU (id-kp-clientAuth) wordt gebruikt in wederzijdse TLS (mTLS) verbindingen waar beide partijen elkaar authenticeren.

Traditioneel kan een enkel certificaat zowel server- als clientverificatie-EKU's bevatten, waardoor het voor twee doeleinden kan worden gebruikt. Dit is vooral belangrijk voor producten zoals Cisco Expressway die zowel als server als client fungeren in verschillende verbindingsscenario's.

probleemdefinitie

Wijziging van het rootprogramma van Chrome

Met ingang van juni 2026 beperkt het Chrome Root Program Policy Root Certificate Authority (CA) -certificaten die zijn opgenomen in de Chrome Root Store, waardoor multifunctionele roots worden uitgefaseerd om alle public-key infrastructure (PKI) -hiërarchieën uit te lijnen om alleen TLS-serverauthenticatie te gebruiken.

Belangrijkste beleidsvereisten

- Public Root CA's moeten EKU (Extended Key Usage) ALLEEN voor serververificatie (id-kp-serverAuth) bevestigen.
- Het opnemen van Client Authentication EKU in deze certificaten is verboden.
- Geen root-CA's voor gemengd gebruik meer voor TLS-certificaten voor openbare servers.
- Tijdschema voor handhaving: juni 2026

Openbare CA-responstijdlijn

- Oktober 2025: Veel publieke CA's (DigiCert, Sectigo, SSL) begonnen standaard met het uitgeven van alleen-servercertificaten.
- Mei 2026: Openbare CA-servers geven geen EKU-certificeringen voor clientverificatie meer uit
- Juni 2026: Chrome Root Program Policy wordt volledig effectief

---

Opmerking: dit beleid is alleen van toepassing op certificaten die zijn uitgegeven door openbare CA's. Particuliere PKI en zelf ondertekende certificaten worden niet beïnvloed door dit beleid.

Als u geïnteresseerd bent in het lezen over de impact van zonsondergang van client EKU op Expressways, raadpleeg dan Prepare Expressway for Client Auth EKU Sunset in Public CA Certificates.

Expressway Release x15.5 met oplossing

Expressway x15.5

Expressway x15.5 wordt geleverd met een voorgestelde oplossing voor een probleem dat zich voordoet als gevolg van het niet instellen van client-EKU door alle openbare certificeringsinstanties. Dit is een wereldwijd probleem en treft alle leveranciers/implementaties die ervoor kiezen om openbare PKI-certificaten te gebruiken.

x15.4, een eerdere release, had een CLI-opdrachtcertificaat waarmee de beheerder alleen het EKU-servercertificaat (geen client-EKU aanwezig) kon uploaden op Expressway E.

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload: On

---

Opmerking: deze opdracht is uitgeschakeld op x15.5.

Toevoeging X15.5 Certificate Store

X15.5 heeft twee certificaatstores:

1. Servercertificaatarchief

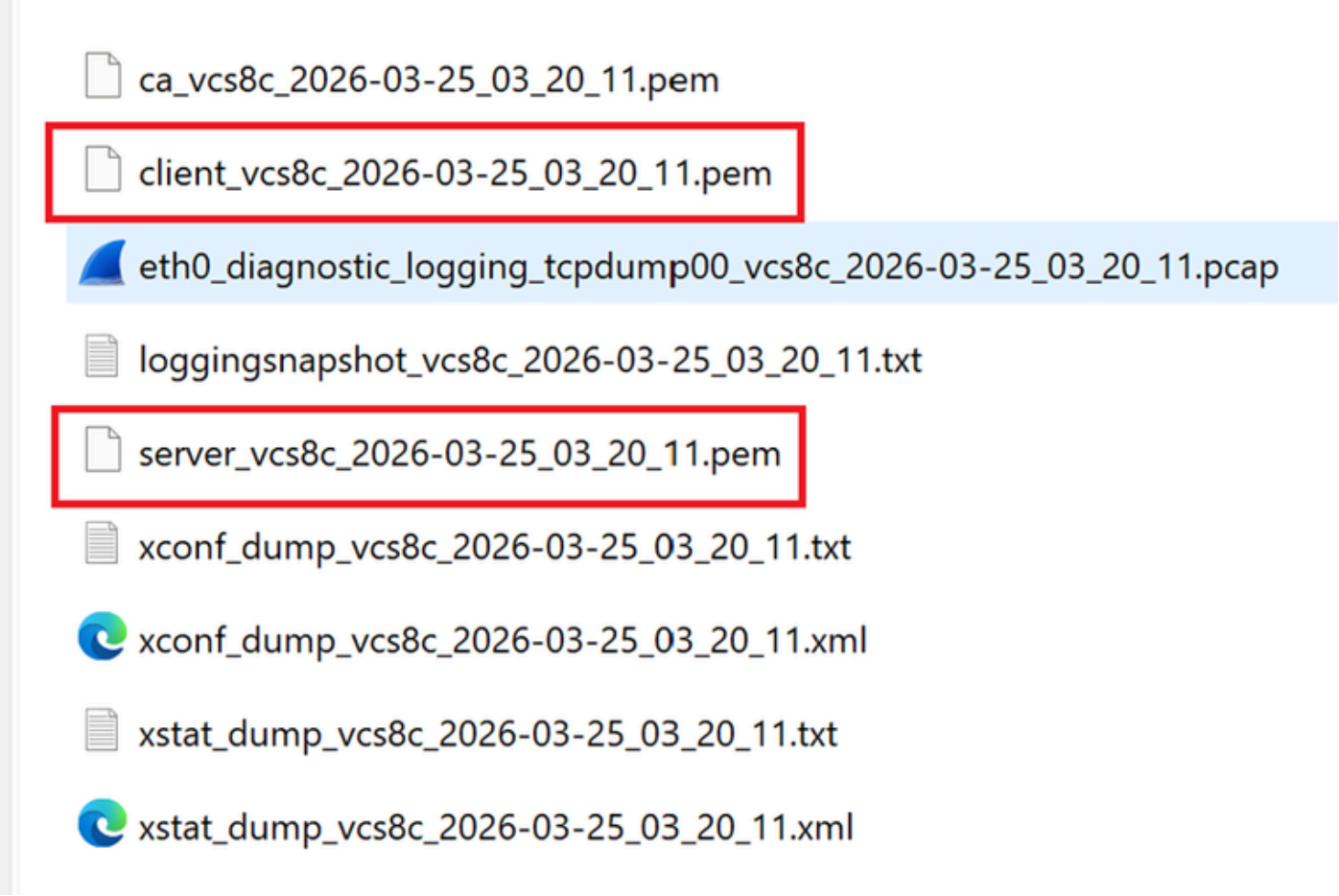
2. Clientcertificaatarchief

Expressways (één NIC of twee NIC's): beide Expressway-interfaces kunnen naar behoefte gebruikmaken van twee certificaatstores.

Voorbeeld:

- Wanneer de expressway als client fungeert tijdens de TLS-handshake, wordt het clientcertificaat weergegeven.
- Wanneer de expressway tijdens de TLS-handshake als server fungeert, wordt het servercertificaat weergegeven.

Opmerking: beide certificaatstores (client en server) gebruiken dezelfde vertrouwde CA-bibliotheek. Zorg ervoor dat de CA die server- en clientcertificaten heeft ondertekend, correct wordt geüpload in de Trust-opslag. Diagnostische logboeken bevatten nu een servercertificaat en een clientcertificaat in PEM-bestandsindeling.



Upgrade van X15.4 of eerdere versie naar X15.5

Wanneer een upgrade wordt uitgevoerd, wordt het servercertificaat van x15.4 of een eerdere versie, de ExpressWay-servercertificaatopslag gekopieerd naar de clientcertificaatopslag op x15.5. Client- en servercertificaatstores op x15.5 hebben hetzelfde certificaat.

Voorbeeld met screenshots

Expressway-server op 15.4, huidig servercertificaat Serienummer 46:df:76:aa:00:00:00:00:00:29

Certificaat:

Versie: 3 (0x2)

Serienummer:

46:DF:76:AA:00:00:00:00:00:29

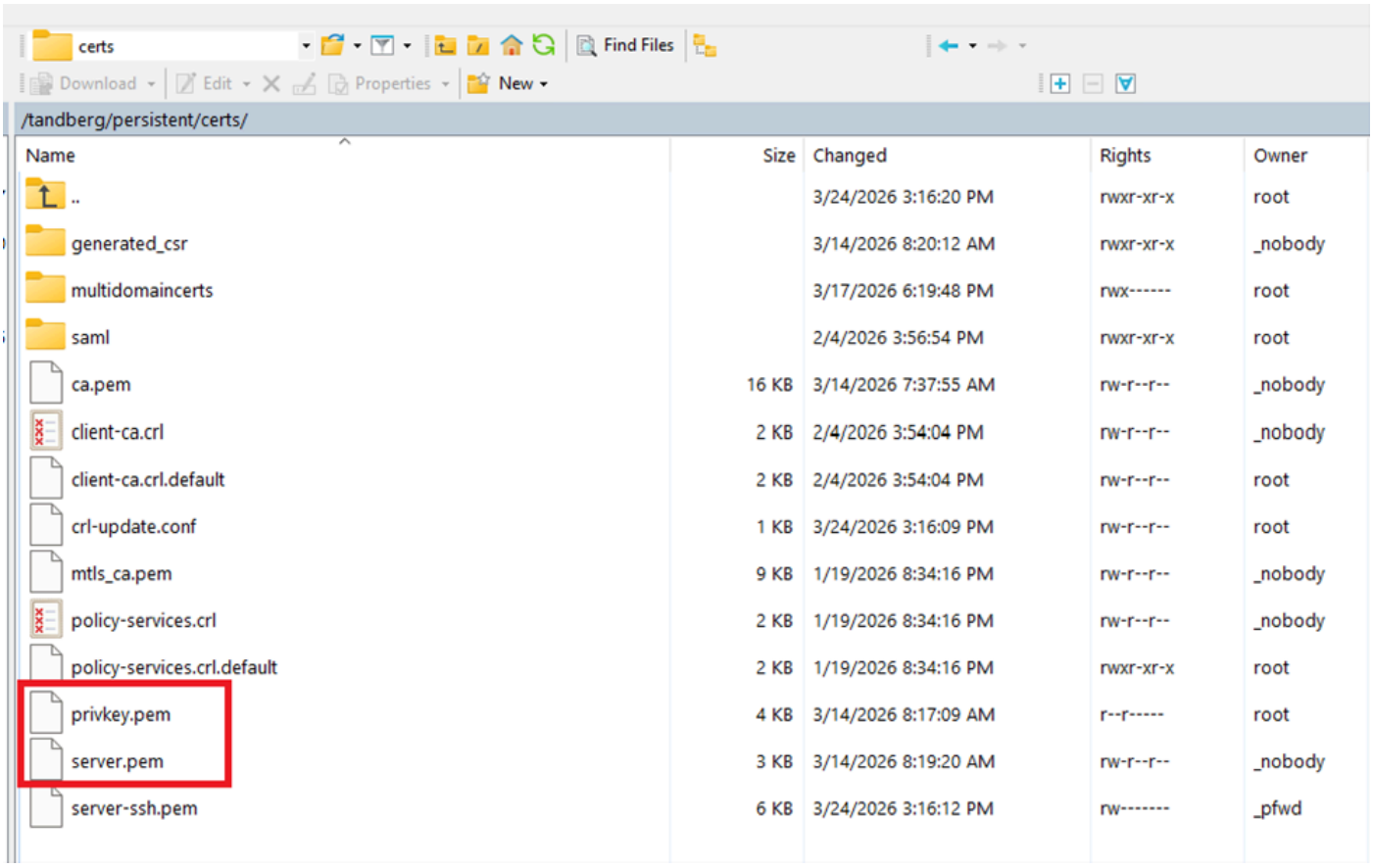
geldigheid

Niet eerder: Mrt 14 02:37:40 2026 GMT

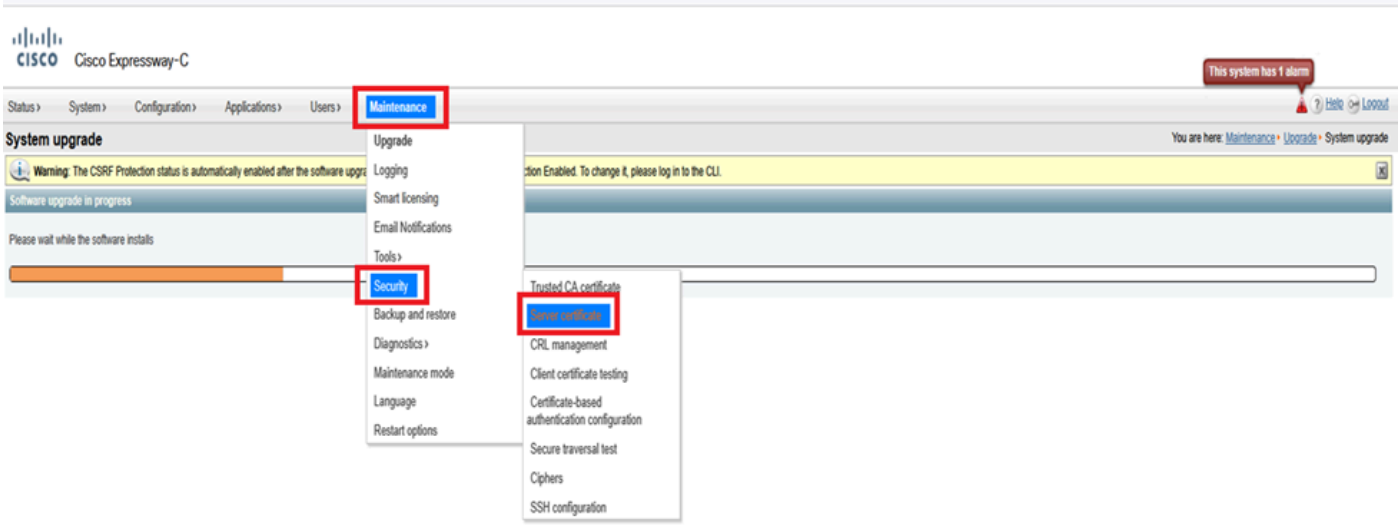
Niet na: Mrt 14 02:47:40 2028 GMT

Onderwerp: C = IN, ST = KA, L = KA, O = Cisco, OU = TAc, CN = cluster.s.com

Expressway-bestandssysteempersistente/cert-directory op x15.4:

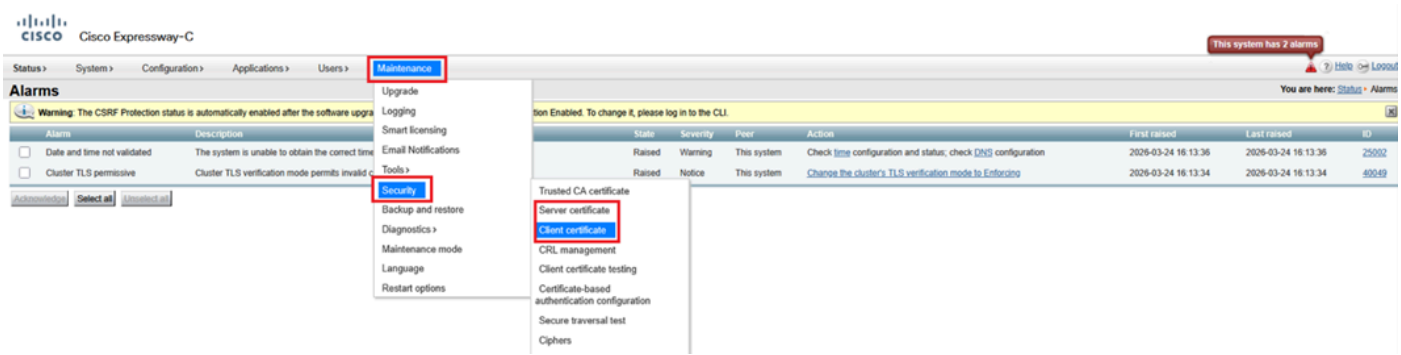


Expressway-menu (Onderhoud > Beveiliging > Servercertificaat) op x15.4 (alleen veld Servercertificaat aanwezig):



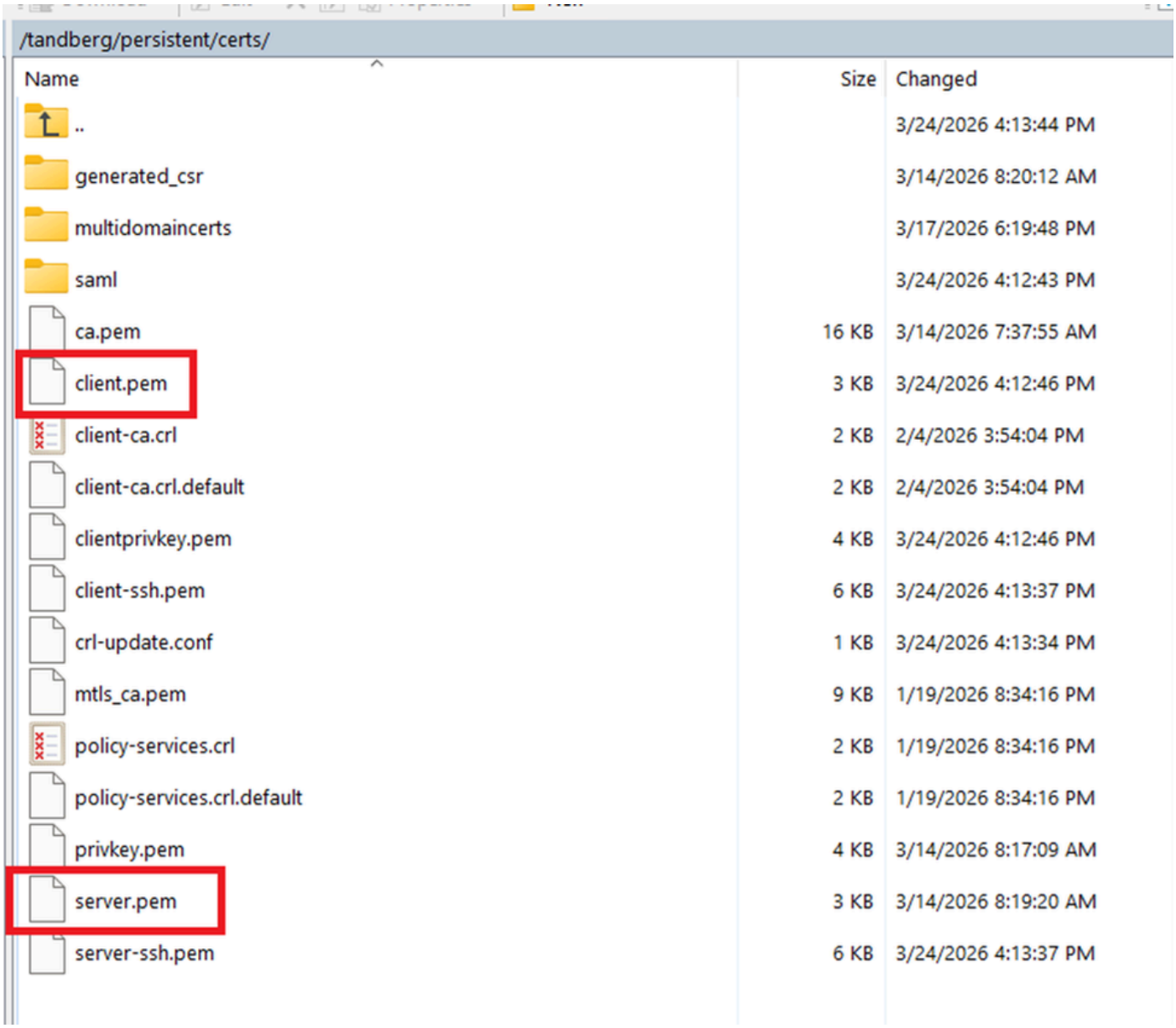
Na succesvolle upgrade naar x15.5

Hier ziet u 2 certificaatopties onder Onderhoud > Beveiliging > clientcertificaat en servercertificaten. Na het upgraden naar x15.5 wordt hetzelfde certificaat weergegeven op zowel de server- als de clientcertificaatportals op webbeheer, omdat het servercertificaat van x15.4 is gekopieerd naar de clientcertificaatopslag op x15.5.



Na de upgrade naar x15.5 zijn het bestaande certificaat en de privésleutel gekopieerd naar het clientcertificaatarchief.

Expressway-bestandssysteempersistente/cert-directory op x15.5:



X15.5 EKU-controle tijdens TLS-handshake

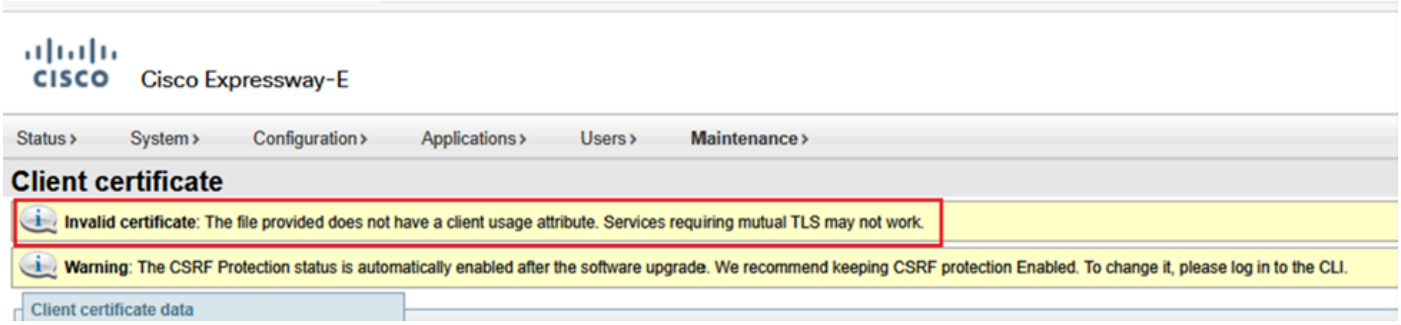
Op x15.5 is een nieuwe CLI-opdracht geïntroduceerd om Extended key use (EKU) tijdens TLS-handshake te controleren. De standaardwaarde is "ON". De opdrachtset is geldig op Expressway Core en Edge.

De opdrachtset activeert een controle voor alle INBOUND SIP TLS-verbindingen naar Expressway. (Inkomende client-HELLO's/certificaat gepresenteerd). Wanneer deze optie is ingeschakeld, wordt gecontroleerd of het certificaat dat door de TLS-initiator wordt gepresenteerd, client-EKU in certificaat bevat. ALS DEZE OPTIE IS UITGESCHAKELD, wordt de controle overgeslagen; de server-EKU wordt echter gecontroleerd als deze aanwezig is op het certificaat.

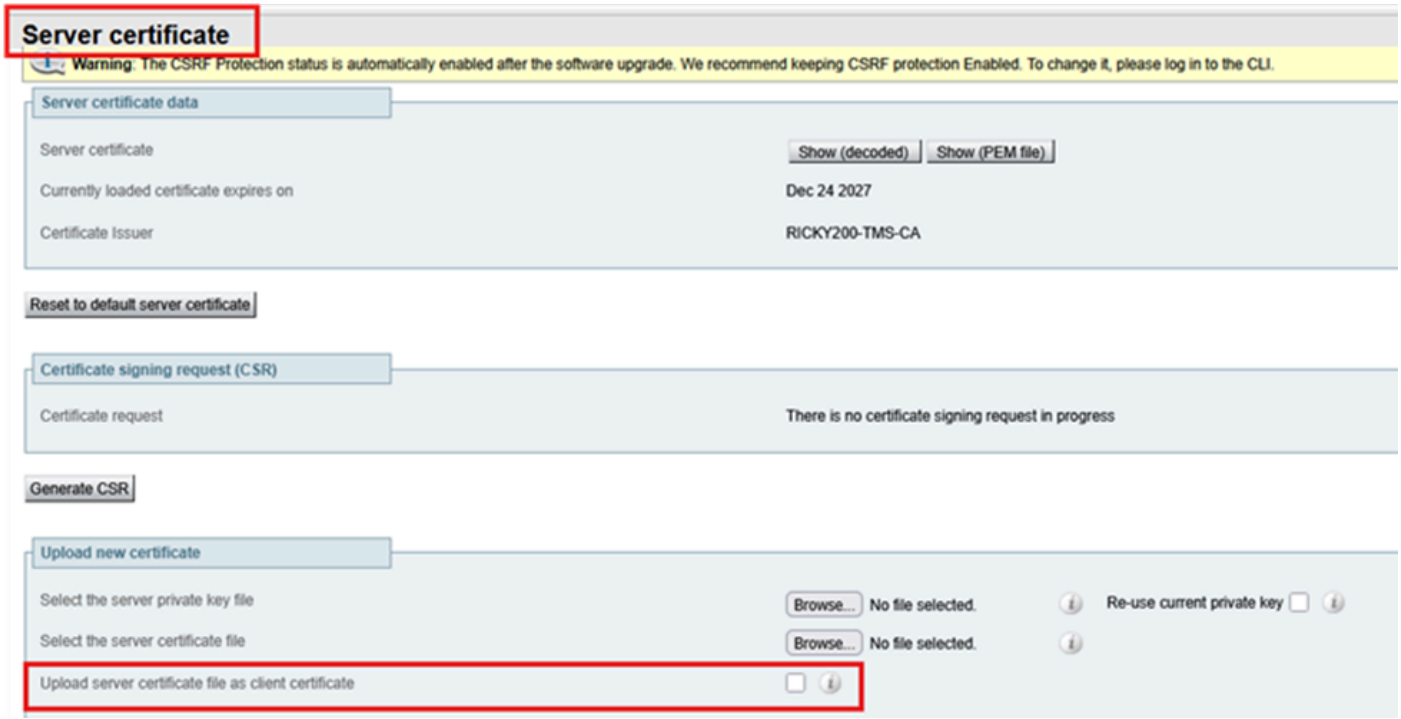
xconfiguration SIP TLS Certificate ExtendedKeyUse Checking Mode: AAN/UIT:

Opmerking: als u een clientcertificaat genereert en een CSR ondertekent die geen client-EKU bevat (een voorbeeld van een openbaar CA-ondertekend certificaat), kunt u dit certificaat niet handmatig uploaden in het clientcertificaatarchief. U moet er dus voor zorgen dat certificaten die worden gegenereerd door het ondertekenen van een CSR altijd de EKU van de klant bevatten (een particuliere CA kan worden gebruikt om de EKU van de klant in te voegen).

Tip: deze fout wordt duidelijk wanneer u probeert een certificaat met een CSR-handtekening te uploaden, dat de EKU van de client mist, in de certificaatopslag van de client.



Als u er echter voor kiest om een certificaat met alleen een server-EKU (geen client-EKU) te uploaden via de servercertificaatopslag en Servercertificaatbestand uploaden als clientcertificaat selecteert, wordt het certificaat gekopieerd naar de clientcertificaatopslag. Beheerders die geen door een particuliere certificeringsinstantie ondertekend certificaat op Expressway-Edge willen gebruiken, kunnen ervoor kiezen de EKU-server alleen te kopiëren van het servercertificaatarchief naar het clientcertificaatarchief.

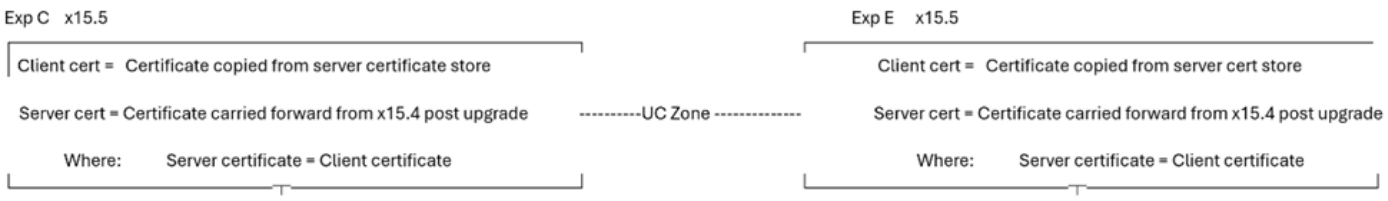


Meerdere certificaatwinkels, meerdere implementatiescenario's

Omdat er nu twee certificaatwinkels op Expressway zijn, zijn er meerdere scenario's van certificaatwinkels.

Voorwaarde 1: Upgrade

Wanneer de Expressway wordt bijgewerkt van x15.4 of eerder dan x15.5, is deze voorwaarde waar. Bestaande certificaten uit de x15.4-versie worden gekopieerd naar twee (2) certificaatstores. Op de x15.5-client en -server zijn de te-certificaten hetzelfde.

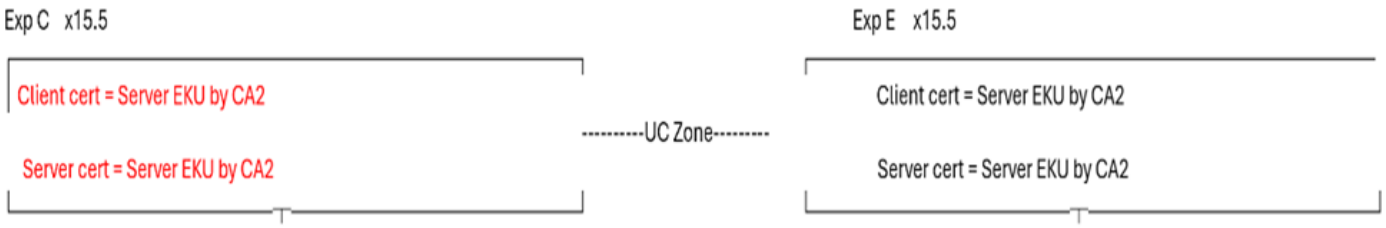


Voorwaarde 2: wanneer de beheerder een nieuw certificaat installeert op x15.5 (bestaande certificaten verlopen)

CA 1 = Interne CA

CA 2 = Openbare CA

In de volgende afbeelding heeft Expressway Core een clientcertificaat met server-EKU dat alleen is ondertekend door CA 2 (Public CA) en een servercertificaat met server-EKU dat alleen is ondertekend door CA 2 (Public CA). Op dezelfde manier heeft Expressway E een clientcertificaat met de server EKU ondertekend door CA2 (openbare CA) en een servercertificaat met server EKU alleen ondertekend door CA 2 (openbare CA).



Als het Expressway-kernservercertificaat geen client-EKU, Unified communications traversal zone, MRA heeft, werkt de WebRTC-proxy niet. Zorg ervoor dat het Expressway Core-servercertificaat een client-EKU heeft. Dit is een veel voorkomend geval waarbij gebruikers ervoor kiezen om alle certificaten van openbare CA te ondertekenen. Aangezien de openbare CA Client EKU niet in certificaten opneemt, wordt de zone Unified communications traversal wel actief.

Als u de UC-zone actief wilt maken, kunt u de EKU-controle op Expressway E uitschakelen. Dit brengt de UC-zone naar voren. SSH-tunnels blijven echter inactief. Vanaf vandaag vereist de SSH-tunnelcommunicatie op 2222 validatie van de klant-EKU.

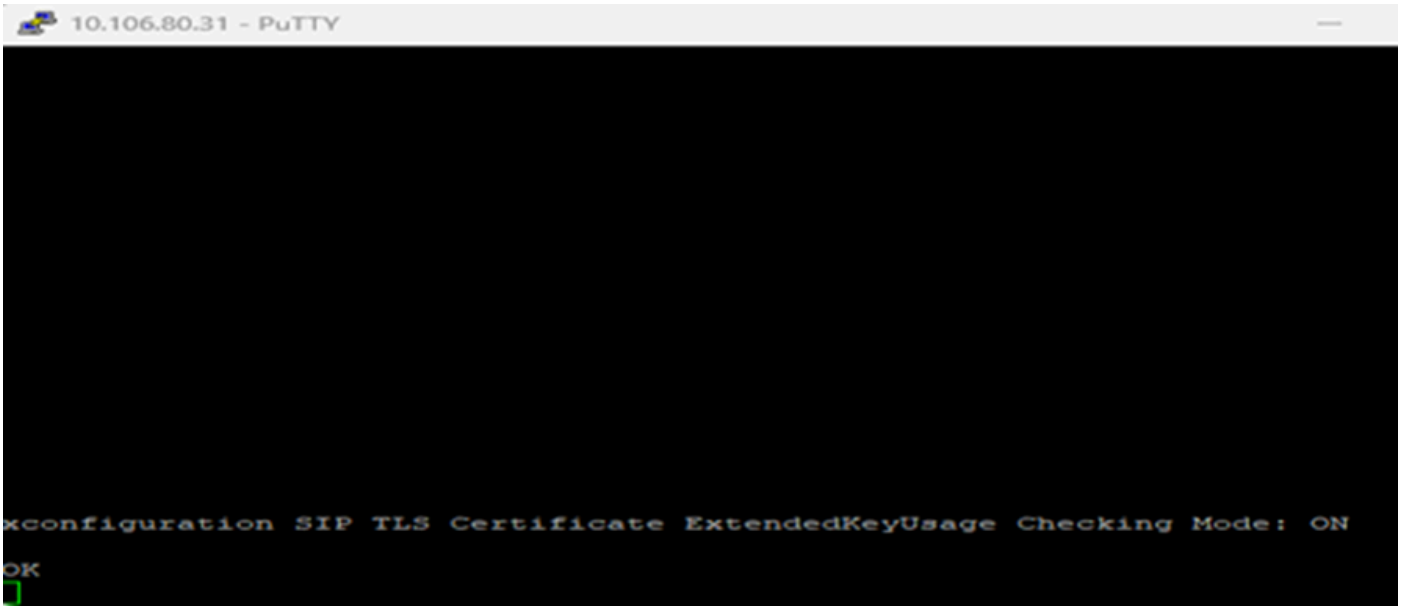
MRA-clientaanmelding en WebRTC-proxyfuncties werken niet. Je zou je toevlucht kunnen nemen tot een privé-CA.

Testcase 1

- Wanneer EKU-controle "ON" is op Expressway E
- Wanneer client- en servercertificaat op Expressway core Server alleen EKU heeft
- UC-zonestatus is MISLUKT

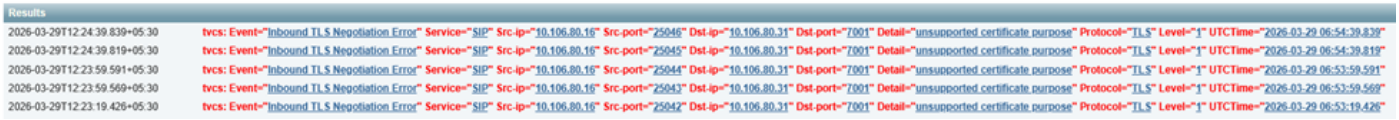
On Expressway-Edge ExtendedKeyUsage controleren ON.

xconfiguration SIP TLS Certificate ExtendedKeyUse Checking Mode: Aan:



Mislukte Unified Communication Zone:

Expressway E-logs tonen waar 10.106.80.16 = Expressway Core, 10.106.80.31 = Expressway Edge:

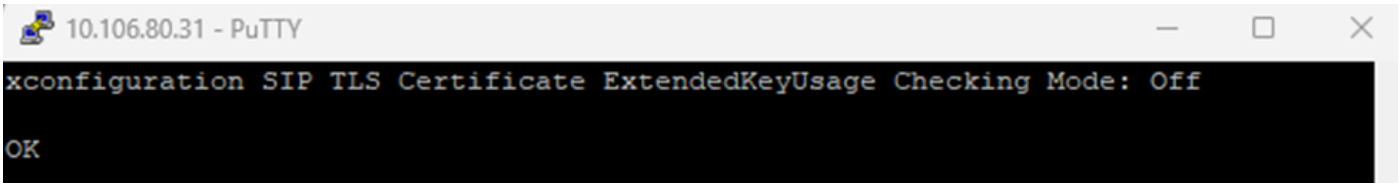


Testcase 2

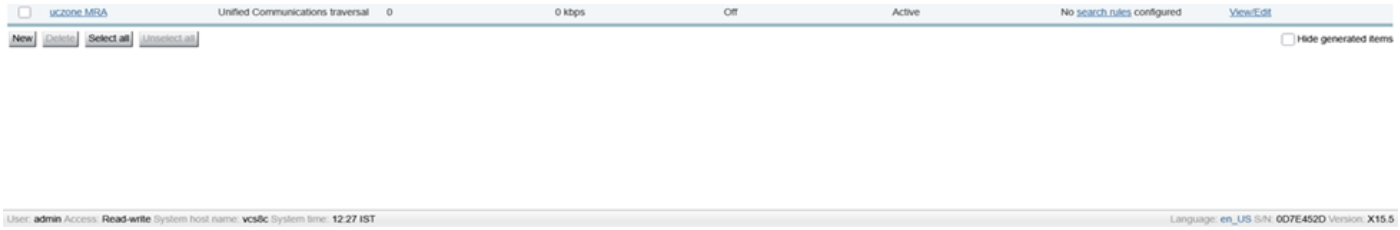
- Wanneer EKU-controle is UITGESCHAKELD op Expressway E
- Wanneer client- en servercertificaat op Expressway Core-server alleen EKU heeft
- UC-zonestatus is ACTIEF

Schakel de EKU-controle uit op Expressway E.

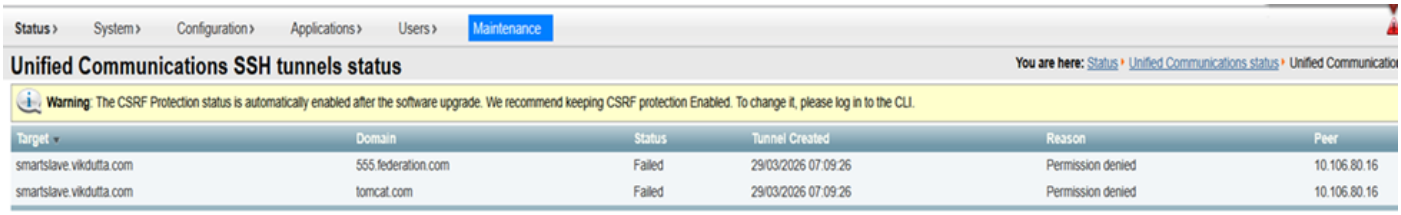
xconfiguration SIP TLS Certificate ExtendedKeyUse Checking Mode: Uit



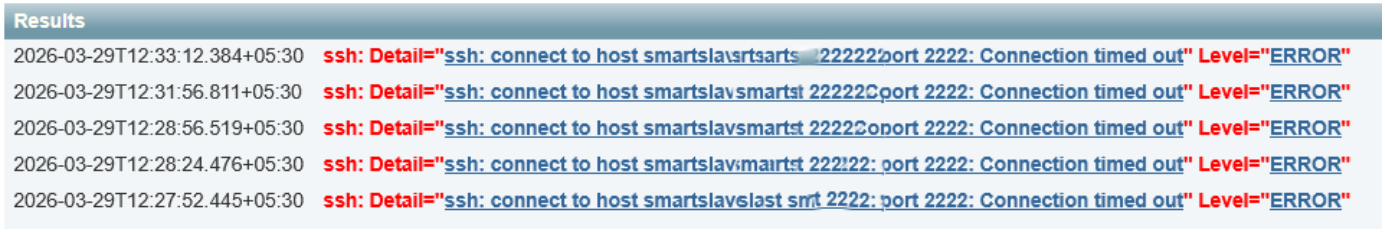
Unified communication zone Actief:



De ssh-tunnels mislukten echter nog steeds:



Expressway-gebeurtenislogboeken:



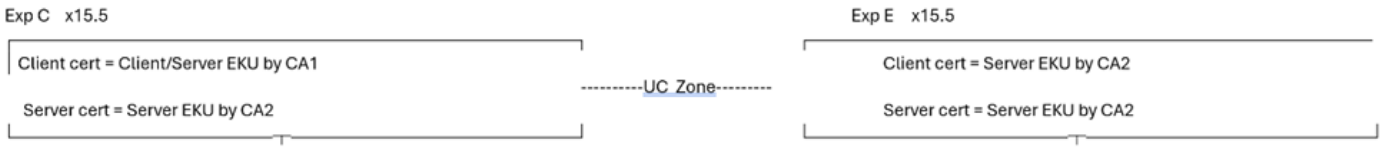
Voorwaarde 2.1: Succesgeval

CA 1 = Interne CA

CA 2 = Openbare CA

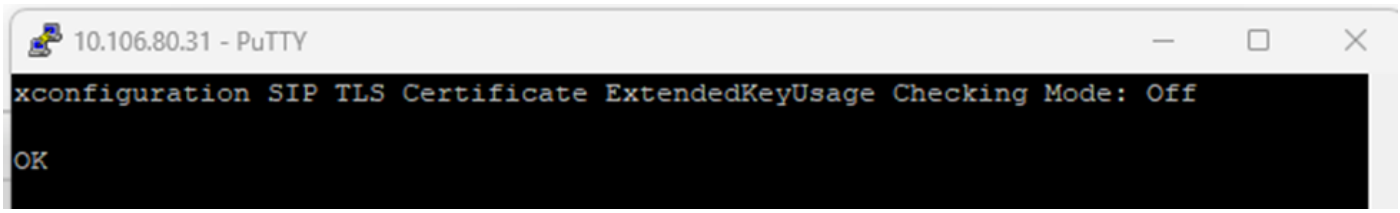
- Waar het Expressway-kernclientcertificaat is ondertekend door CA 1 (interne CA) en waarin Client/Server-EKU is opgenomen, worden beide ondertekend.
- Het Expressway-kernservercertificaat is ondertekend door CA 2 public CA en bevat alleen Server EKU.

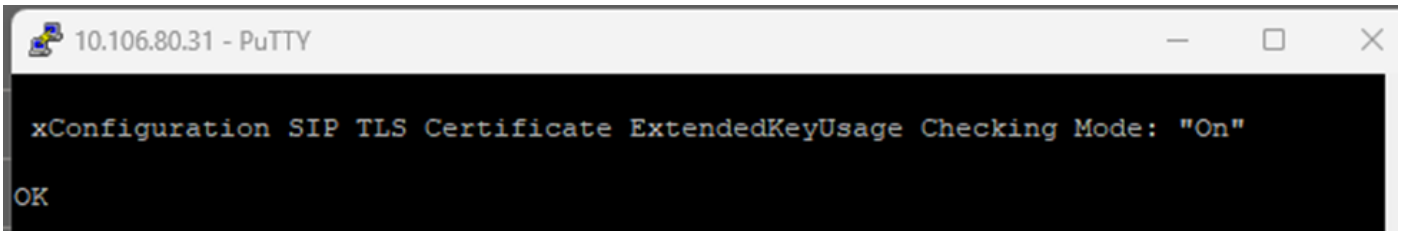
- Het Expressway Edge-servercertificaat is ondertekend door CA 2 public CA en bevat alleen Server EKU.
- Het Expressway Edge-clientcertificaat is ondertekend door CA 2 public CA en bevat alleen server-EKU.



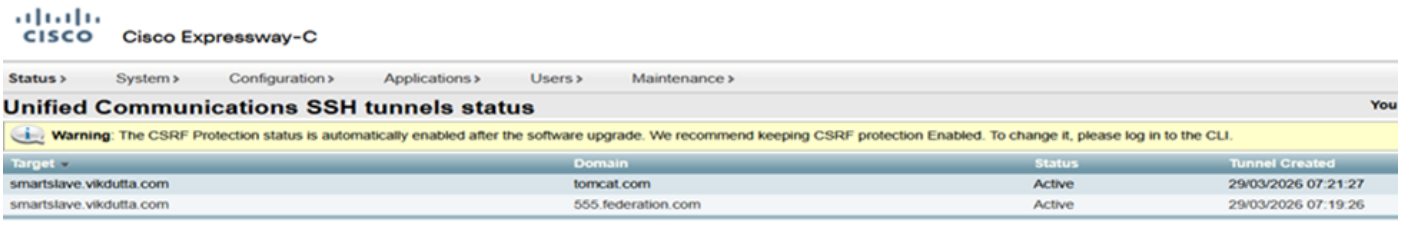
Deze voorwaarde is een succesgeval. Ongeacht of de EKU-controlemodus AAN/UIT is, worden de zone voor Unified Communication en de SSH-tunnel beide actief. MRA-klanten werken.

Het maakt niet uit of de Expressway Edge EKU-controle UIT of AAN is. Het Expressway-kernclientcertificaat bevat client-EKU:

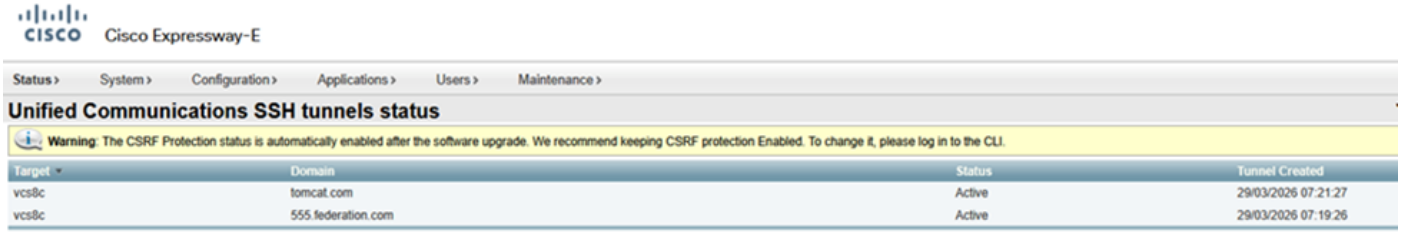




SSH-tunnels op Expressway-kern Actief:

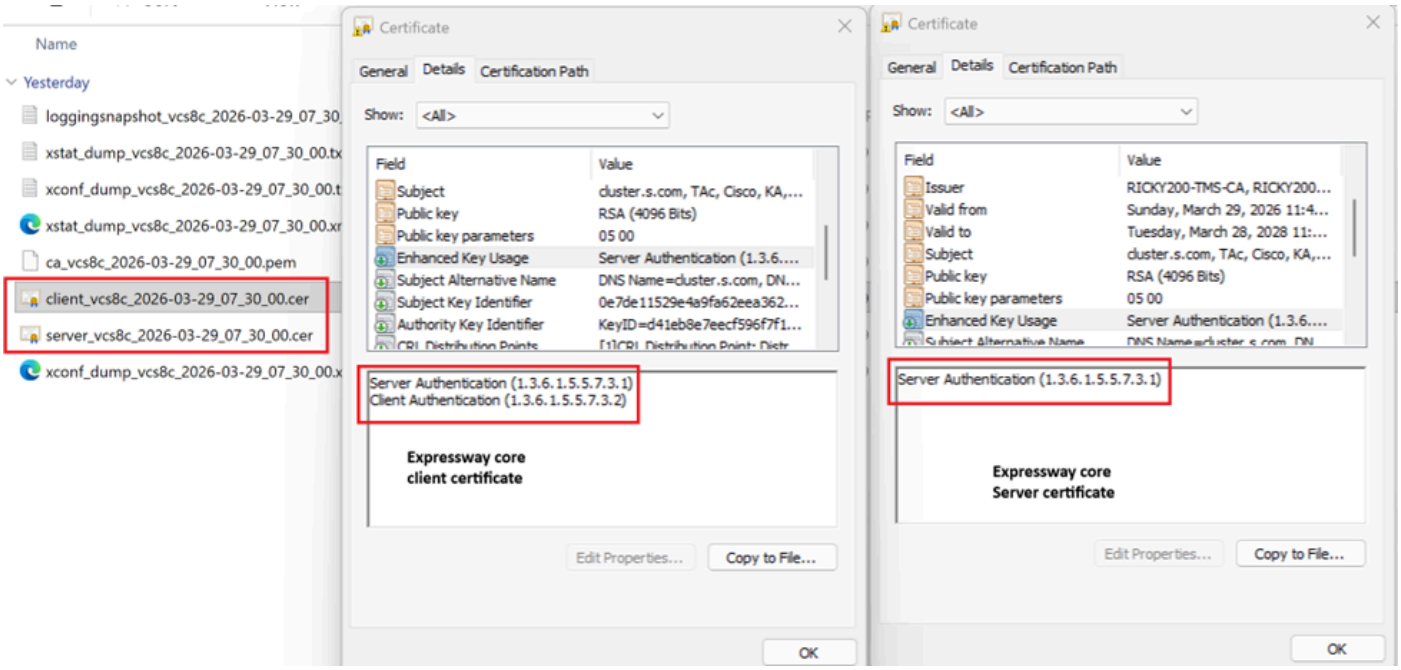


SSH-tunnels op Expressway Edge Active:

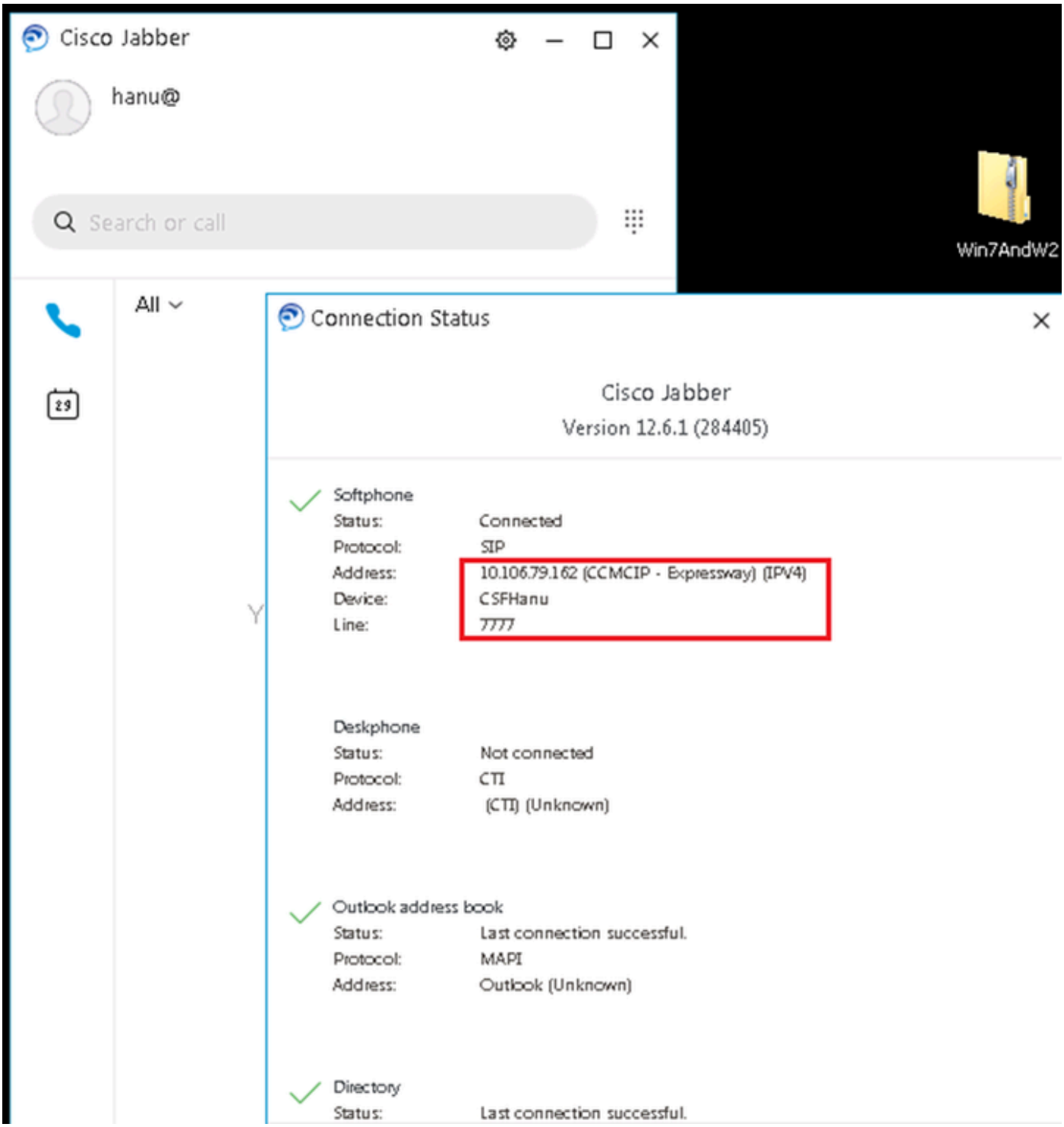


MRA-zonestatus voor Unified Communication Actief:

- Expressway-Core-clientcertificaat heeft Server EKU en Client EKU.
- Expressway Core Server-certificaat heeft alleen server-EKU.



MRA Client logt in en registreert:

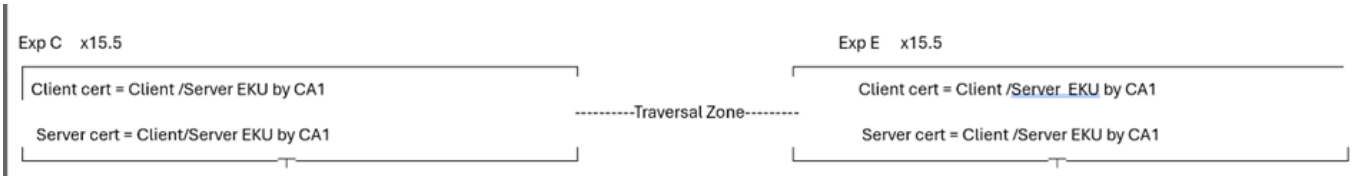


Opmerking: vergelijk en noteer EKU's die aanwezig zijn in certificaten voor MRA en WebRTC-proxy om te werken. Het is een vergelijking tussen werkende en niet-werkende implementatie.

Voorwaarde 3: Ondertekent alle certificaten met privé-CA

CA 1 = Interne CA

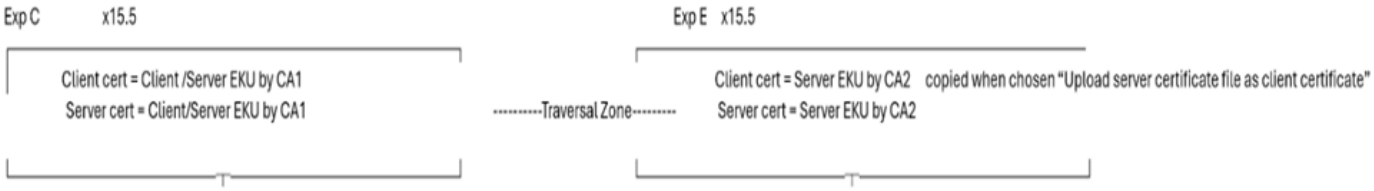
CA 2 = Openbare CA



In voorwaarde 3 worden alle certificaten ondertekend door interne CA (CA1).

- Wanneer Expressway-E een TLS-verbinding verzendt, moet CA 1 root/intermediate worden uitgewisseld met een far-end entiteit. Als far-end geen mogelijkheid heeft of niet toestaat dat een privé CA-certificaat wordt geüpload, is de TLS-verbinding mislukt.
- MRA-clients krijgen certificaten om pop-ups te accepteren als het privécertificaat zich niet in de OS-vertrouwenswinkel bevindt.

Voorwaarde 4: Expressway Edge heeft alleen openbare certificaten met server-EKU



In conditie 4 zijn de Expressway-core client- en servercertificaten (CA1) intern CA-ondertekend en zijn zowel client- als server-EKU aanwezig. Het Expressway E-servercertificaat is openbaar, CA-ondertekend en heeft alleen server-EKU. Servercertificaat wordt gekopieerd naar clientcertificaatarchief en kiest Servercertificaatbestand uploaden als clientcertificaat.

In Voorwaarde 4, wanneer de TLS-verbinding wordt gemaakt naar far-end, als Expressway -E een TLS-client hallo stuurt, moet far-end de client-EKU-controle uitschakelen (omdat het clientcertificaat geen client-authentische EKU heeft), anders is de TLS-verbinding mislukt.

Er kunnen veel meer voorwaarden of scenario's in het veld zijn op basis van gebruikersimplementatie en gebruiksscenario's en alle kunnen niet worden gedekt vanwege mijn beperkte gedachtestroom. Punten om te onthouden zijn echter:

- # ALS Expressway een client wordt tijdens TLS-handshake, wordt het clientcertificaat aan peers gepresenteerd.
- #IF Expressway wordt Server tijdens TLS-handshake; het servercertificaat wordt aan peer gepresenteerd.

Deze redenering is vastgesteld met deze testgevallen.

Scenario 1

Voor dit scenario presenteert Expressway het clientcertificaat tijdens de MTLS-handshake met Webex.

Een videogesprek naar de Webex-bijeenkomst:

Voorbeeld gespreksstroom Jabber -à CUCM -à Exp Core - à Exp Edge - à Webex

10.106.80.31= Rand snelweg

163 129 37 33 = Webex

2026-03-24T11:54:26.106+00:00 smartslave tvcs: UTCTime="2026-03-24 11:54:26,106" Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="10.106.80.31" Local-port="25002" DST-ip="163.129.37.33" DST-port="5061"

Expressway Edge heeft een clientcertificaat met dit serienummer (2f0000004c869c77c8981becde00000000004c).

Expressway Edge stuurt client hallo naar 'Webex' tijdens TLS-onderhandeling en verzendt vervolgens clientcertificaat.

Serienummer 2f0000004c869c77c8981becde0000000004c:

1. Expressway Edge stuurt client hello (pkt= 13699) naar ‘Webex tijdens mTLS-onderhandeling.

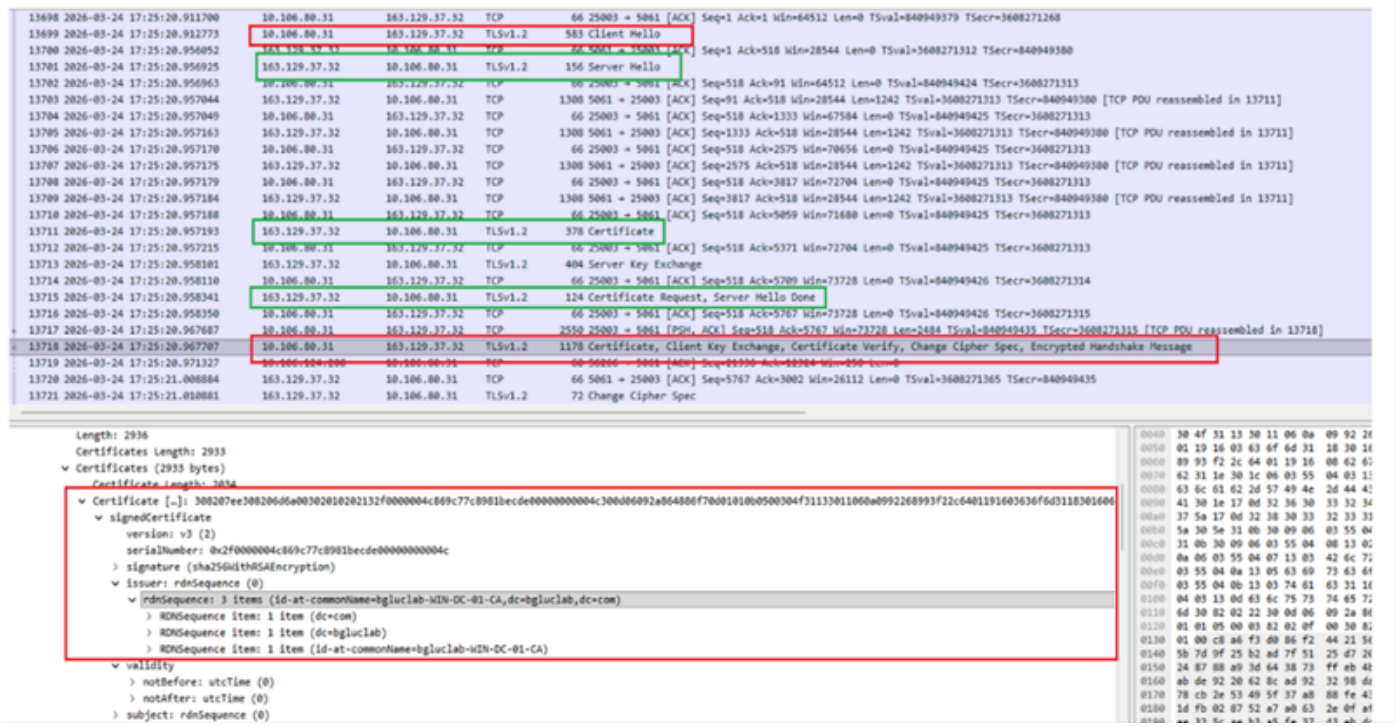
2. Webex stuurt een server hallo naar Expressway Edge (pkt=13701).

3. Webex stuurt het certificaat naar Expressway Edge (pkt=13711).

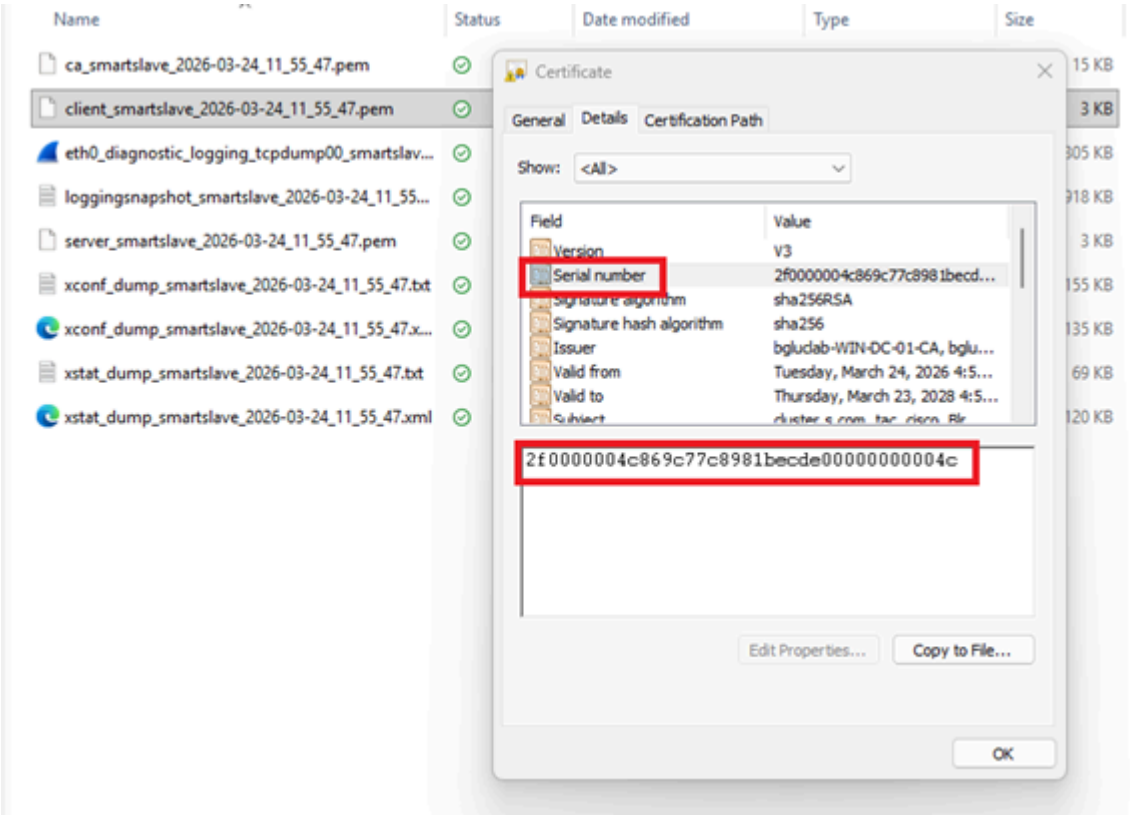
4. Webex vraagt het Expressway edge-certificaat "CertificateRequest" aan (pkt=13715).

5. Expressway Edge stuurt het certificaat naar Webex (pkt=13718).

(screenshot)



Clientcertificaat van Expressway Edge:



Scenario 2

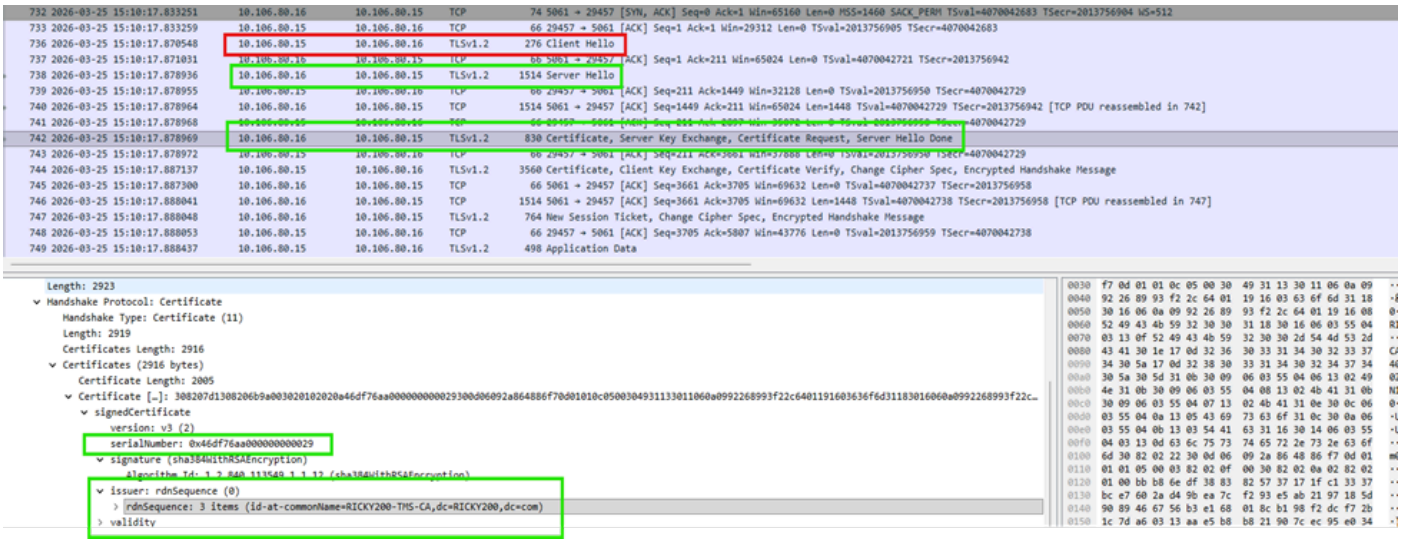
Expressway wordt een serverentiteit tijdens de mTLS-handshake en presenteert het

servercertificaat:

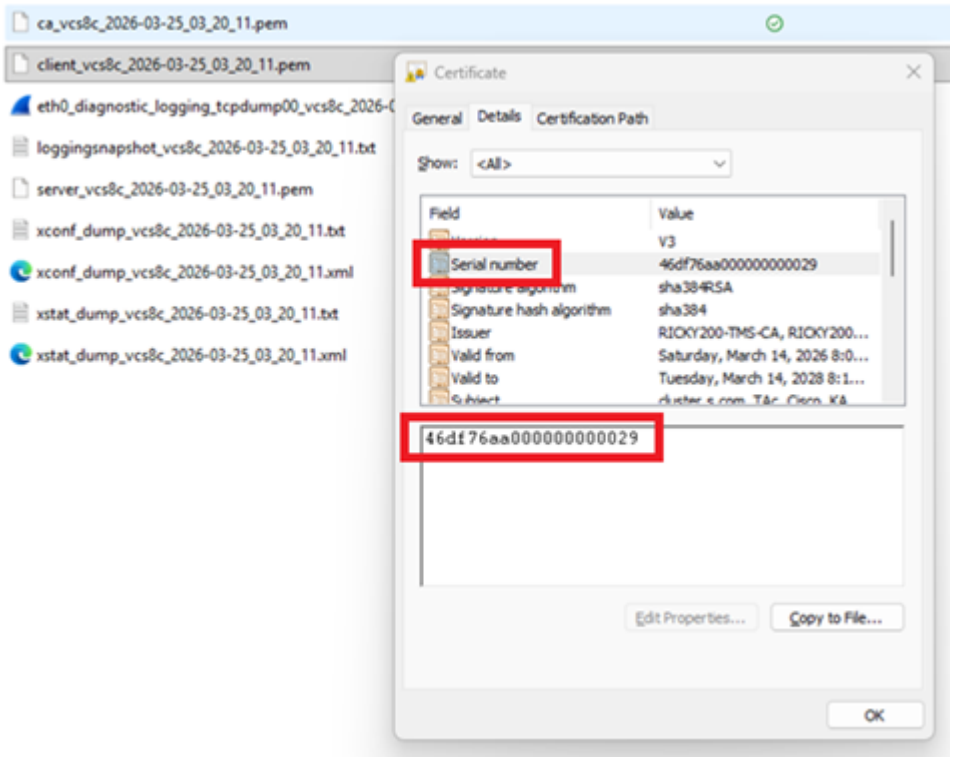
Waar Expressway een servercertificaat presenteert, heeft Expressway een beveiligde buurzone boven 5061 met de verificatienaam ON.

Beveiligde buurzone tussen Expressway node x15.5 en Expressway node x8.11.4:

```
10.106.80.15 (x8.11.4) sends a client hello to 10.106.80.16 (x15.5) (pkt=736)

10.106.80.16 sends a server hello to 10.106.80.15 (pkt=738)

10.106.80.16 (x15.5) presents its server cert during TLS handshake (pkt=742) and requests client's cert

10.106.80.15 (x8.11.4) sends client certificate (pkt=744)
```



Deze schermafbeelding toont het servercertificaat als overeenkomende serienummers:

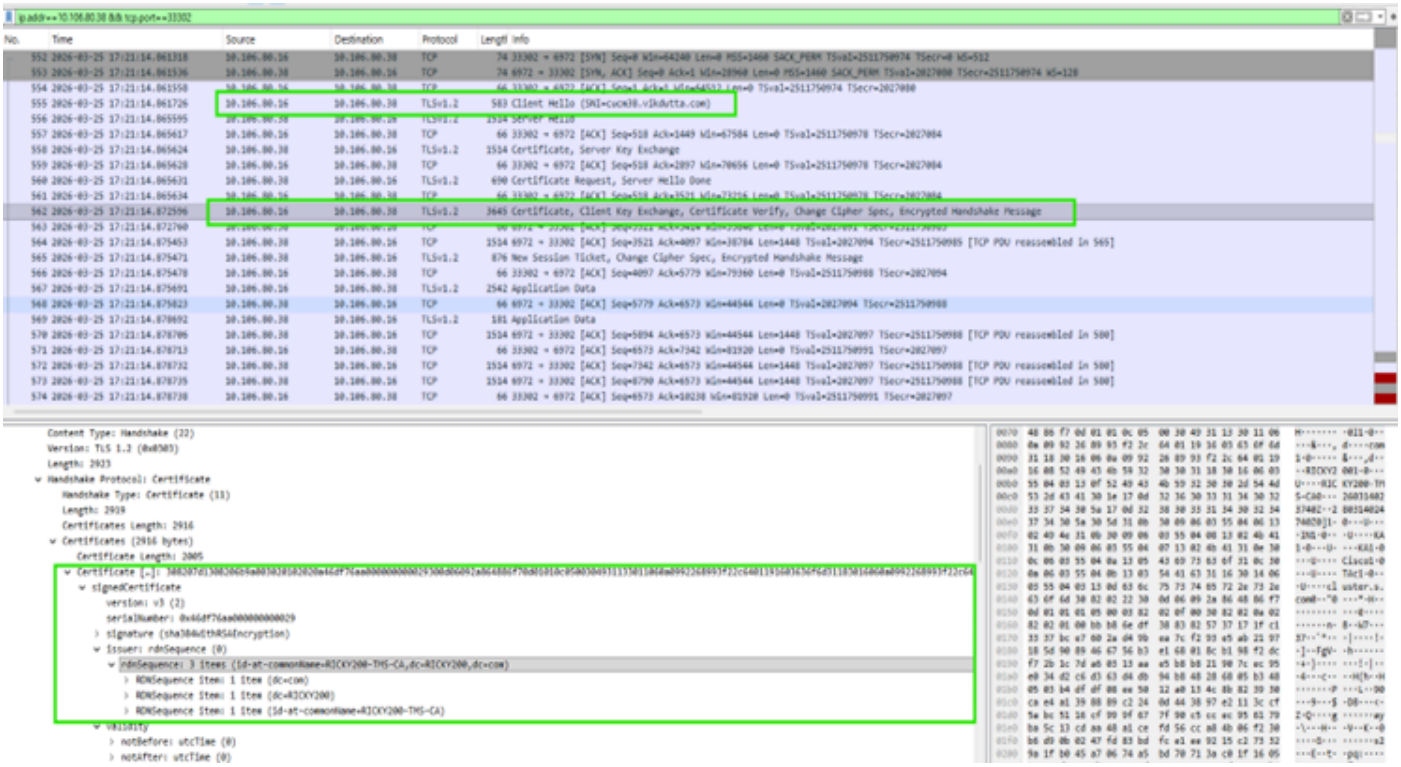


Testcase 3: MRA-client is voorzien voor aanmelding en de workflow omvat verificatie van het verkeersservercertificaat tussen Expressway Core en CUCM.

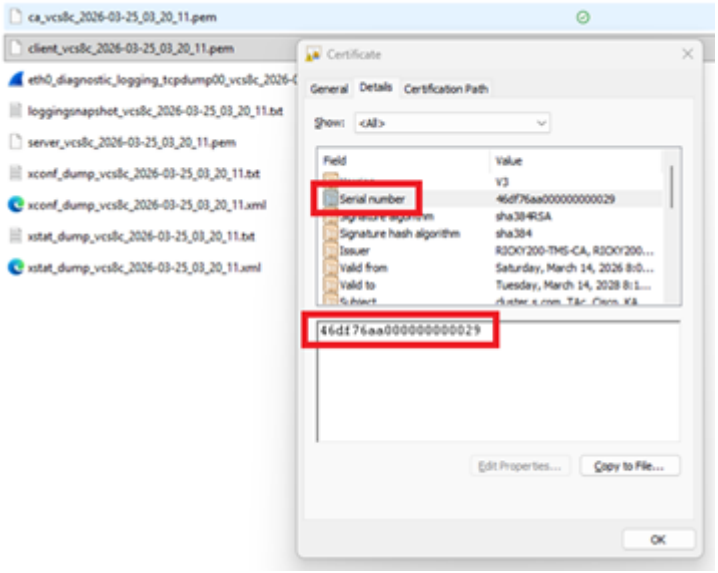
10.106.80.16 = Expressway Core x15.5

10 106 80 38 = CUCM

- Exp C 16 stuurt een klant hallo op 6972 TFTP.
- Exp C 16 verzendt een clientcertificaat tijdens de TLS-handshake.



Expressway Core-clientcertificaat:



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.