Navigieren Client EKU Sunset mit Expressway x15.5

Einleitung

In diesem Dokument wird die Navigation durch den Client-EKU-Sonnenuntergang mit Cisco Expressway x15.5 beschrieben.

Hintergrundinformationen

Digitale Zertifikate sind von vertrauenswürdigen Zertifizierungsstellen (Certificate Authorities, CAs) ausgestellte elektronische Zertifikate, die die Kommunikation zwischen Servern und Clients durch die Gewährleistung von Authentifizierung, Datenintegrität und Vertraulichkeit schützen. Diese Zertifikate enthalten Extended Key Usage (EKU)-Felder, die ihren Zweck definieren:

- Die Serverauthentifizierungs-EKU (id-kp-serverAuth) wird verwendet, wenn ein Server sein Zertifikat zum Identitätsnachweis vorlegt.
- Die Client-Authentifizierungs-EKU (id-kp-clientAuth) wird in gegenseitigen TLS-Verbindungen (mTLS) verwendet, bei denen sich beide Parteien gegenseitig authentifizieren.

Bisher konnte ein einzelnes Zertifikat sowohl Server- als auch Clientauthentifizierungs-EKUs enthalten, sodass es für zwei Zwecke verwendet werden konnte. Dies ist besonders wichtig für Produkte wie Cisco Expressway, die in verschiedenen Verbindungsszenarien sowohl als Server als auch als Client fungieren.

Problemdefinition

Änderung der Chrome-Stammprogrammrichtlinie

Ab Juni 2026 schränkt die Chrome Root Program Policy die im Chrome Root Store enthaltenen Zertifikate der Root Certificate Authority (CA) ein, wobei die Mehrzweck-Roots schrittweise abgeschafft werden, um alle Public-Key Infrastructure (PKI)-Hierarchien so auszurichten, dass sie nur für Anwendungsfälle der TLS-Serverauthentifizierung verwendet werden.

Wichtige Richtlinienanforderungen

- Öffentliche Stammzertifizierungsstellen müssen die Extended Key Usage (EKU) NUR für die Serverauthentifizierung (id-kp-serverAuth) geltend machen.
- Die Aufnahme der Clientauthentifizierungs-EKU in diese Zertifikate ist nicht zulässig.
- Keine gemischten Stammzertifizierungsstellen mehr für TLS-Zertifikate für öffentliche Server.
- Durchsetzungszeitleiste: Juni 2026

Öffentliche Zertifizierungsstelle - Reaktionszeit

- Oktober 2025: Viele öffentliche CAs (DigiCert, Sectigo, SSL) begannen standardmäßig mit der Ausgabe von Zertifikaten nur für Server.
- Mai 2026: Öffentliche Zertifizierungsstellen-Server stellen keine Client Authentication/EKU-Zertifizierungen mehr aus
- Juni 2026: Chrome Root-Programm-Richtlinie wird voll wirksam

---

Anmerkung: Diese Richtlinie gilt nur für Zertifikate, die von öffentlichen Zertifizierungsstellen ausgestellt wurden. Private PKI und selbstsignierte Zertifikate sind von dieser Richtlinie nicht betroffen.

Wenn Sie mehr über die Auswirkungen der Sonnenuntergang-Einstellung von Client EKU auf Expressways erfahren möchten, lesen Sie Expressway für Client Auth EKU Sonnenuntergang in öffentlichen Zertifizierungsstellenzertifikaten vorbereiten.

Expressway Release x15.5 mit Lösung

Expressway x15,5

Expressway x15.5 kommt mit einem Vorschlag zur Behebung eines Problems, das durch die Sonnenuntergang der Client-EKU durch alle öffentlichen Zertifizierungsstellen entsteht. Dies ist ein globales Problem, das alle Anbieter/Bereitstellungen betrifft, die öffentliche PKI-Zertifikate verwenden möchten.

x15.4, eine frühere Version, verfügte über einen CLI-Befehlsschalter, der es dem Administrator ermöglichte, ein Server-EKU-Only-Zertifikat (kein Client-EKU vorhanden) auf Expressway E hochzuladen.

xConfiguration XCP TLS-Zertifikat CVS EnableServerEkuUpload: On

---

Anmerkung: Dieser Befehl ist für x15.5 veraltet.

X15.5-Zertifikatspeichererweiterung

x15.5 verfügt über zwei Zertifikatspeicher:

1. Server-Zertifikatspeicher

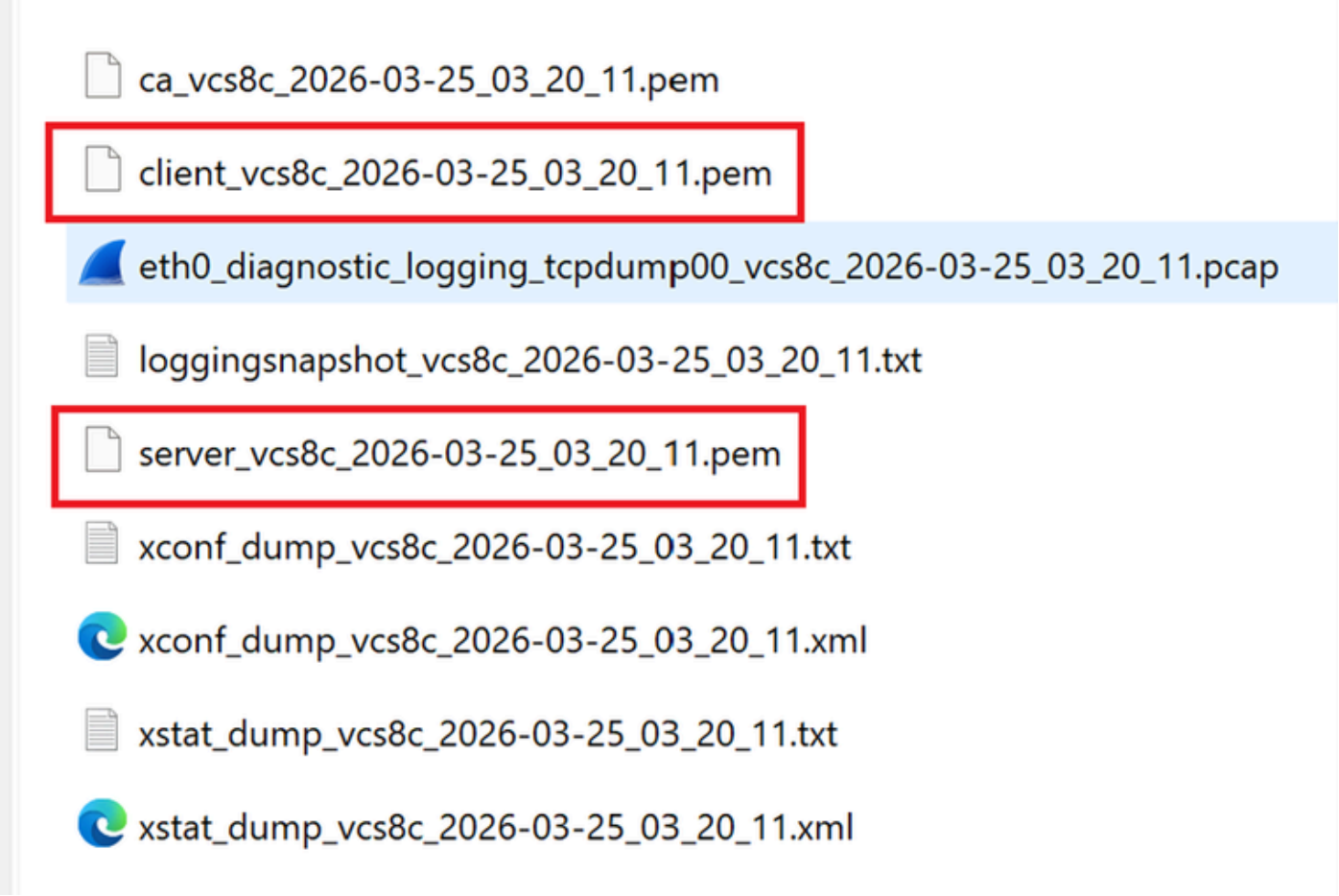
2. Client-Zertifikatspeicher

Expressways (Single NIC oder Dual NIC): Beide Expressway-Schnittstellen können je nach Bedarf zwei Zertifikatspeicher nutzen.

Beispiel:

- Wenn die Schnellstraße während des TLS-Handshakes als Client fungiert, wird ein Client-Zertifikat präsentiert.
- Wenn die Schnellstraße während des TLS-Handshakes als Server fungiert, wird ein Serverzertifikat angezeigt.

Anmerkung: Beide Zertifikatspeicher (Client und Server) verwenden dieselbe Bibliothek vertrauenswürdiger Zertifizierungsstellen. Stellen Sie sicher, dass die Zertifizierungsstelle, die Server- und Clientzertifikate signiert hat, ordnungsgemäß in den Trust Store hochgeladen wird. Diagnoseprotokolle enthalten jetzt Serverzertifikate und Clientzertifikate im PEM-Dateiformat.



Upgrade von X15.4 oder früheren Versionen auf X15.5

Wenn ein Upgrade durchgeführt wird, wird das Serverzertifikat aus x15.4 oder einer früheren Version des Expressway-Serverzertifikatsspeichers in den Clientzertifikatsspeicher auf x15.5 kopiert. Die Client- und Serverzertifikatsspeicher auf x15.5 verfügen über dasselbe Zertifikat.

Beispiel mit Screenshots

Expressway-Server auf 15.4, aktuelles Serverzertifikat Seriennummer 46:df:76:aa:00:00:00:00:29

Zertifikat:

Version: 3 (0 x 2)

Seriennummer:

46:df:76:aa:00:00:00:00:00:29

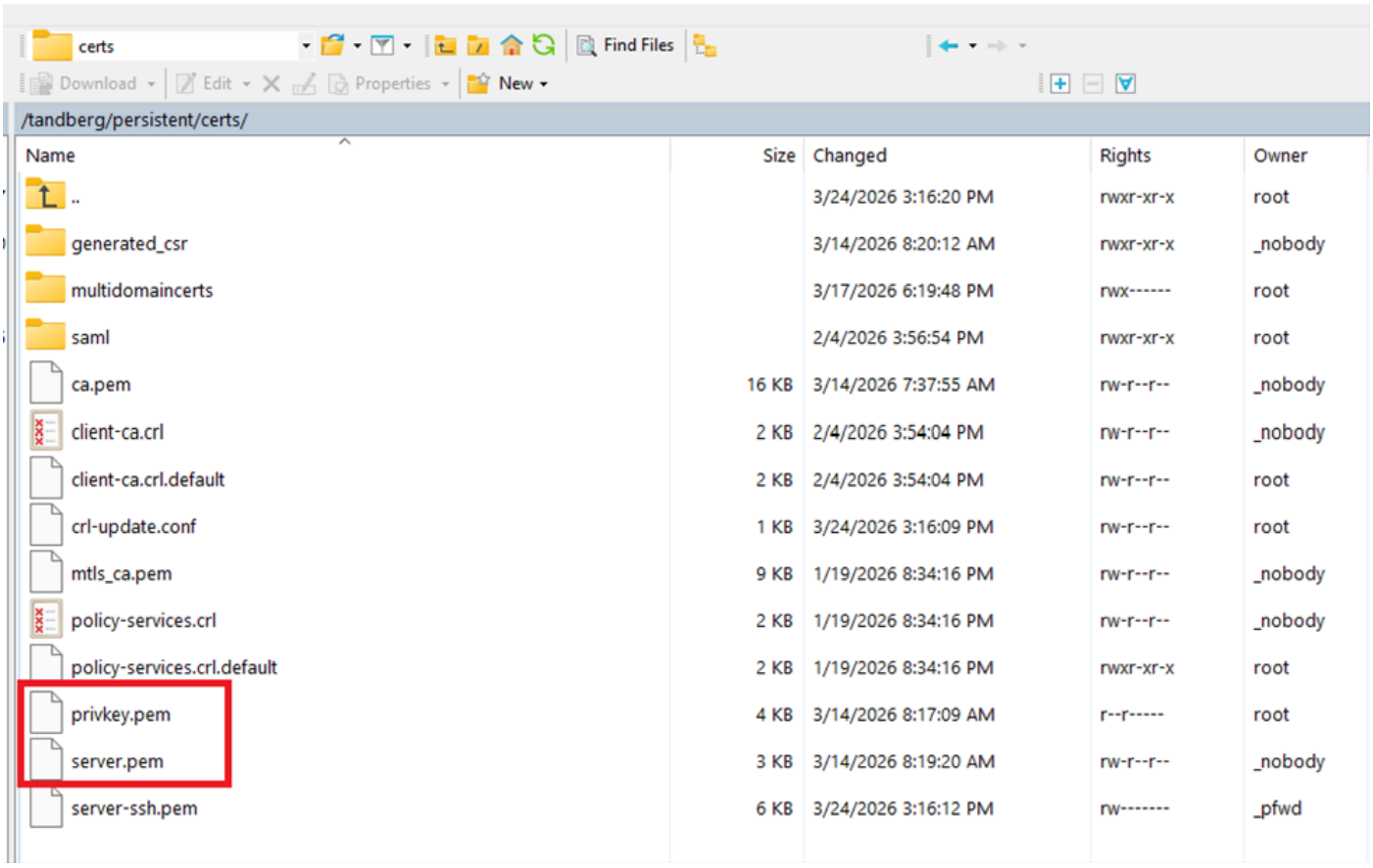
Gültigkeit

Nicht vor: 14. März 2026 02:37:40 Uhr GMT

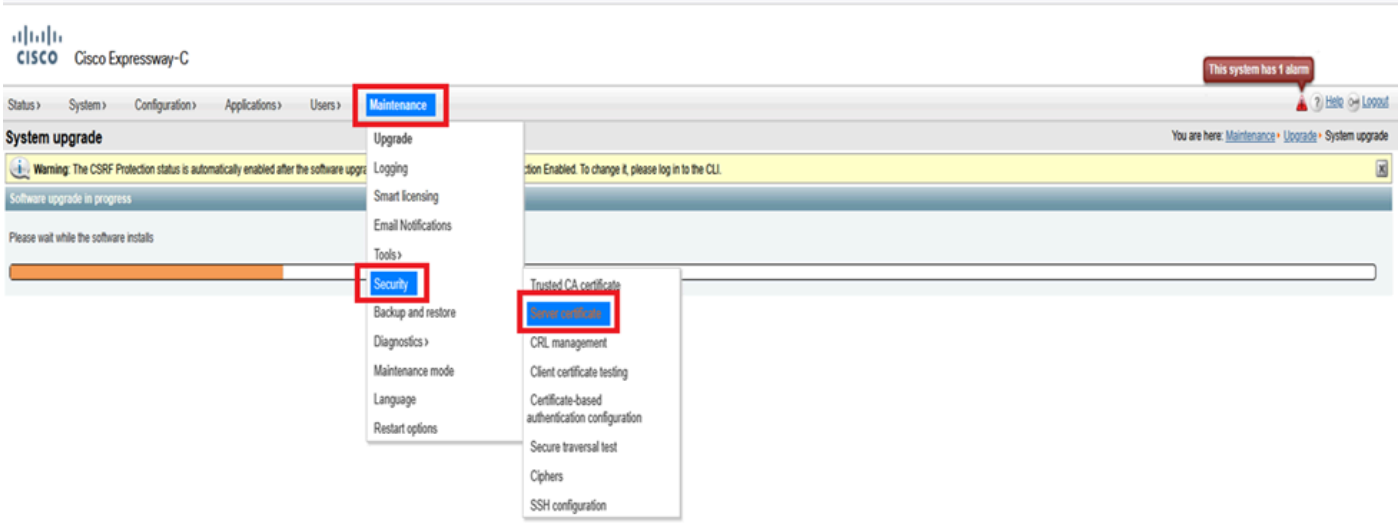
Nicht nachher: 14.03.2028 02:47:40 Uhr GMT

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

Expressway-Dateisystem, Verzeichnis "persistent/cert" auf x15.4:

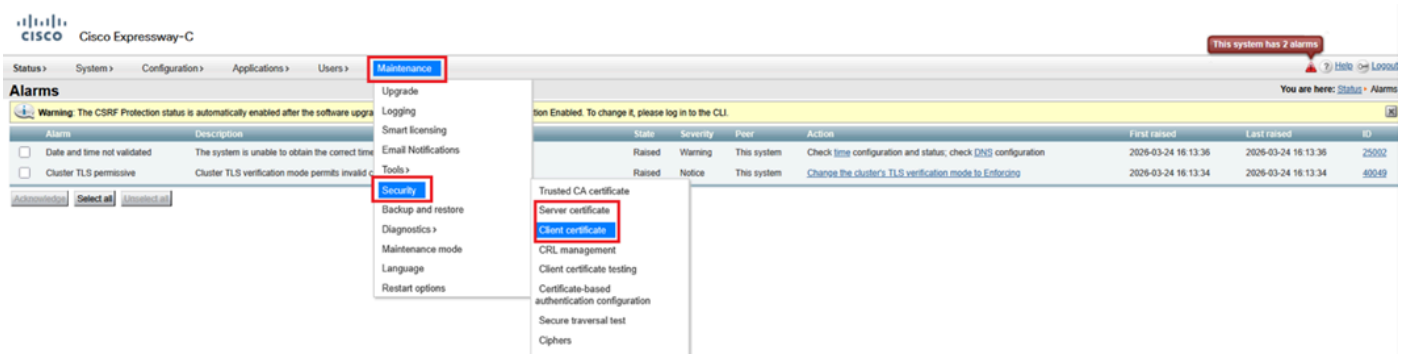


Expressway-Menü (Maintenance > Security > Server certificate) auf x15.4 (nur Server-Zertifikatfeld vorhanden):



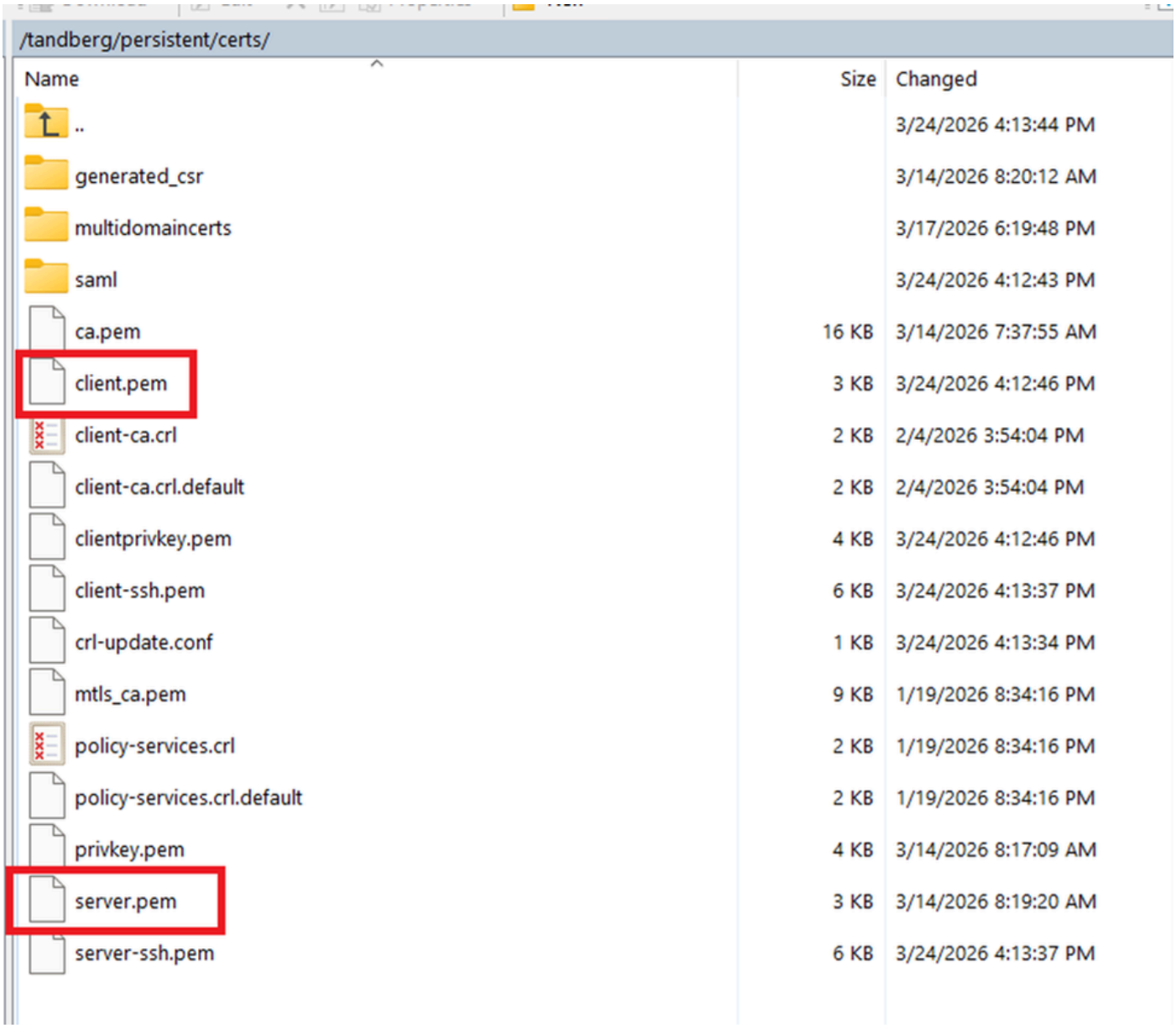
Nach erfolgreichem Upgrade auf x15.5

Hier sehen Sie 2 Zertifikatoptionen unter Wartung > Sicherheit > Clientzertifikat und Serverzertifikate. Nach dem Upgrade auf x15.5 zeigt sowohl das Server- als auch das Client-Zertifikatportal auf dem Webadministrator dasselbe Zertifikat an, da das Serverzertifikat von x15.4 in den Client-Zertifikatspeicher auf x15.5 kopiert wurde.



Nach dem Upgrade auf x15.5 wurden ein vorhandenes Zertifikat und ein privater Schlüssel in den Zertifikatspeicher des Clients kopiert.

Expressway-Dateisystem, Verzeichnis "persistent/cert" auf x15.5:



X15.5-EKU-Prüfung während TLS-Handshake

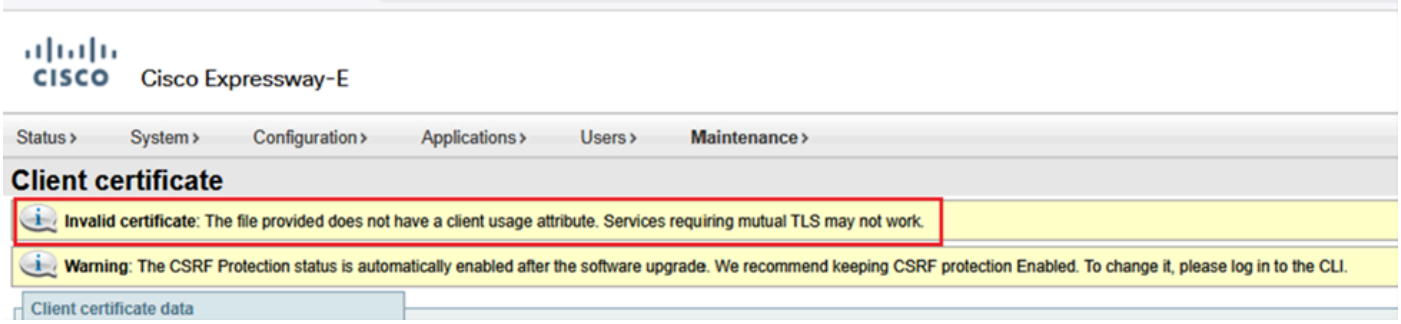
Auf x15.5 wurde ein neuer CLI-Befehl eingeführt, um die Verwendung des erweiterten Schlüssels (Extended Key Usage, EKU) während des TLS-Handshakes zu überprüfen. Der Standardwert ist "ON". Der Befehlssatz ist auf Expressway Core und Edge gültig.

Der Befehlssatz löst eine Überprüfung aller INBOUND SIP TLS-Verbindungen in Expressway aus. (eingehende Client-Hellos/Zertifikat dargestellt). Wenn "ON" aktiviert ist, wird überprüft, ob das vom TLS-Initiator präsentierte Zertifikat die Client-EKU im Zertifikat enthält. WENN DIESE OPTION AUSGESCHALTET IST, WIRD DIE PRÜFUNG UMGEHT. Die Server-EKU wird jedoch überprüft, ob sie im Zertifikat vorhanden ist.

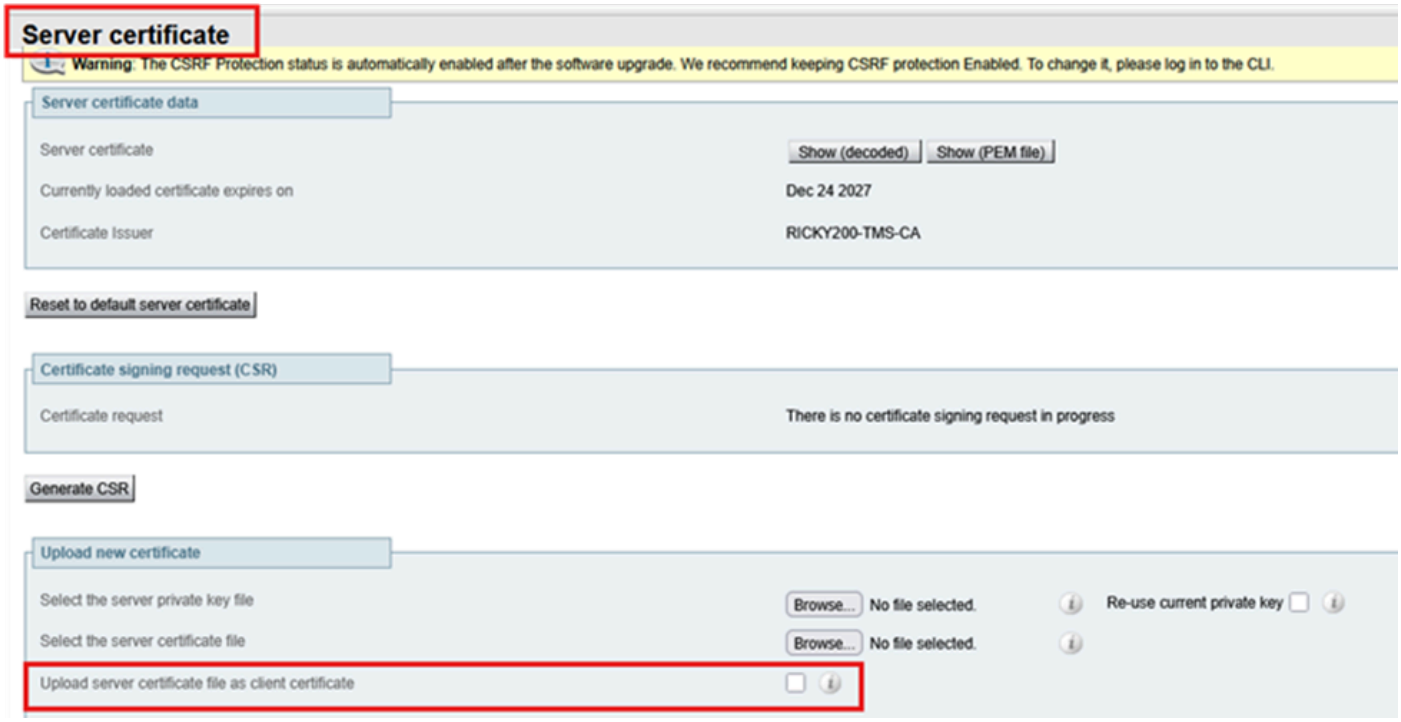
xconfiguration SIP-TLS-Zertifikat, ExtendedKeyUsage-Überprüfungsmodus: EIN/AUS:

Anmerkung: Wenn Sie ein Clientzertifikat generieren und einen CSR signieren, der keine Client-EKU enthält (ein Beispiel für ein öffentlich signiertes CA-Zertifikat), können Sie dieses Zertifikat nicht manuell in den Clientzertifikatsspeicher hochladen. Daher müssen Sie sicherstellen, dass Zertifikate, die durch das Signieren eines CSR generiert werden, immer die Client-EKU enthalten (eine private Zertifizierungsstelle kann verwendet werden, um die Client-EKU einzufügen).

Tipp: Dieser Fehler wird deutlich, wenn Sie versuchen, ein CSR-signiertes Zertifikat, bei dem die Client-EKU fehlt, aus dem Client-Zertifikatspeicher hochzuladen.



Wenn Sie jedoch ein Zertifikat hochladen, das nur über eine Server-EKU (keine Client-EKU) verfügt, über den Server-Zertifikatspeicher, und Server-Zertifikatdatei als Client-Zertifikat hochladen auswählen, wird das Zertifikat in den Client-Zertifikatspeicher kopiert. Administratoren, die auf Expressway-Edge kein privates CA-signiertes Zertifikat verwenden möchten, können die Server-EKU nur aus dem Server-Zertifikatspeicher in den Client-Zertifikatspeicher kopieren.

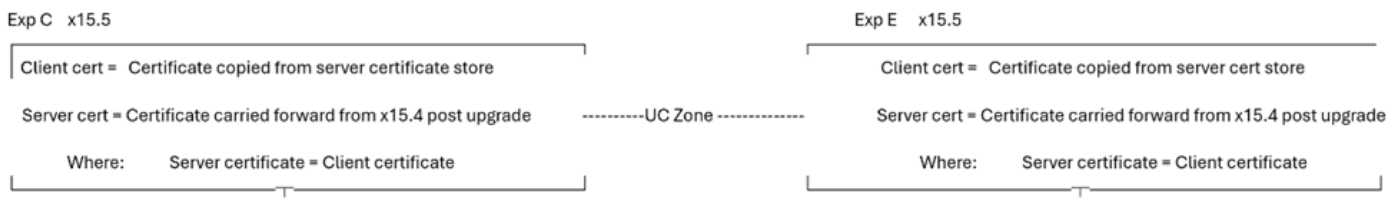


Mehrere Zertifikatspeicher, verschiedene Bereitstellungsszenarien

Da es jetzt zwei Zertifikatspeicher auf Expressway gibt, gibt es mehrere Szenarien für Zertifikatspeicher.

Bedingung 1: Upgrade

Wenn Expressway von x15.4 oder vor x15.5 aktualisiert wird, ist diese Bedingung wahr. Vorhandene Zertifikate aus x15.4-Version werden in zwei (2) Zertifikatspeicher kopiert. Auf dem x15.5-Client und -Server sind die Zertifikate identisch.

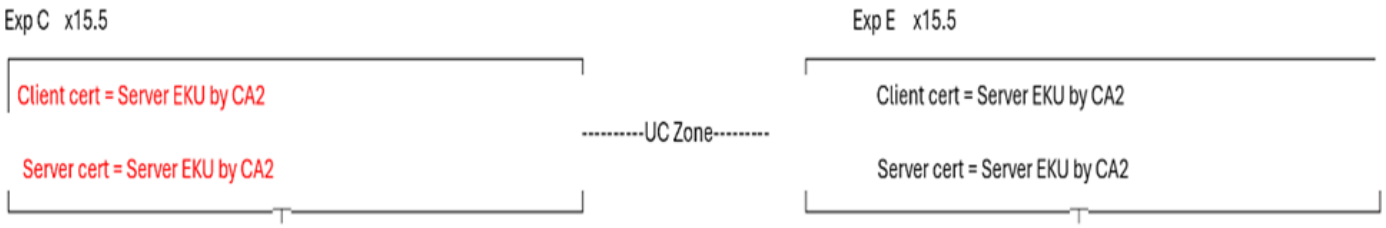


Bedingung 2: Wenn der Administrator ein neues Zertifikat auf x15.5 installiert (vorhandene Zertifikate abgelaufen)

CA 1 = Interne CA

CA 2 = Öffentliche Zertifizierungsstelle

In der Abbildung unten verfügt Expressway Core über ein Client-Zertifikat, bei dem der Server EKU nur von CA 2 (Public CA) signiert ist, und über ein Server-Zertifikat, bei dem der Server EKU nur von CA 2 (Public CA) signiert ist. Ebenso verfügt Expressway E über ein Client-Zertifikat mit dem Server EKU, der von CA2 (öffentliche CA) signiert ist, und ein Server-Zertifikat mit dem Server EKU, das nur von CA 2 (öffentliche CA) signiert ist.



Wenn das Expressway-Core-Serverzertifikat keine Client-EKU, Unified Communications Traversal Zone, MRA, aufweist, funktioniert der WebRTC-Proxy nicht. Stellen Sie sicher, dass das Expressway Core-Serverzertifikat über eine Client-EKU verfügt. Dies ist ein gängiger Anwendungsfall, bei dem Benutzer alle Zertifikate von einer öffentlichen Zertifizierungsstelle signieren. Da die öffentliche CA die Client-EKU nicht in Zertifikaten enthält, wird die Unified Communications-Überbrückungszone aktiviert.

Um die UC-Zone zu aktivieren, können Sie die EKU-Prüfung auf dem Expressway E deaktivieren. Dadurch wird der UC-Bereich aktiviert. SSH-Tunnel bleiben jedoch inaktiv. Ab heute ist für die SSH-Tunnelkommunikation auf 2222 eine Validierung der Client-EKU erforderlich.

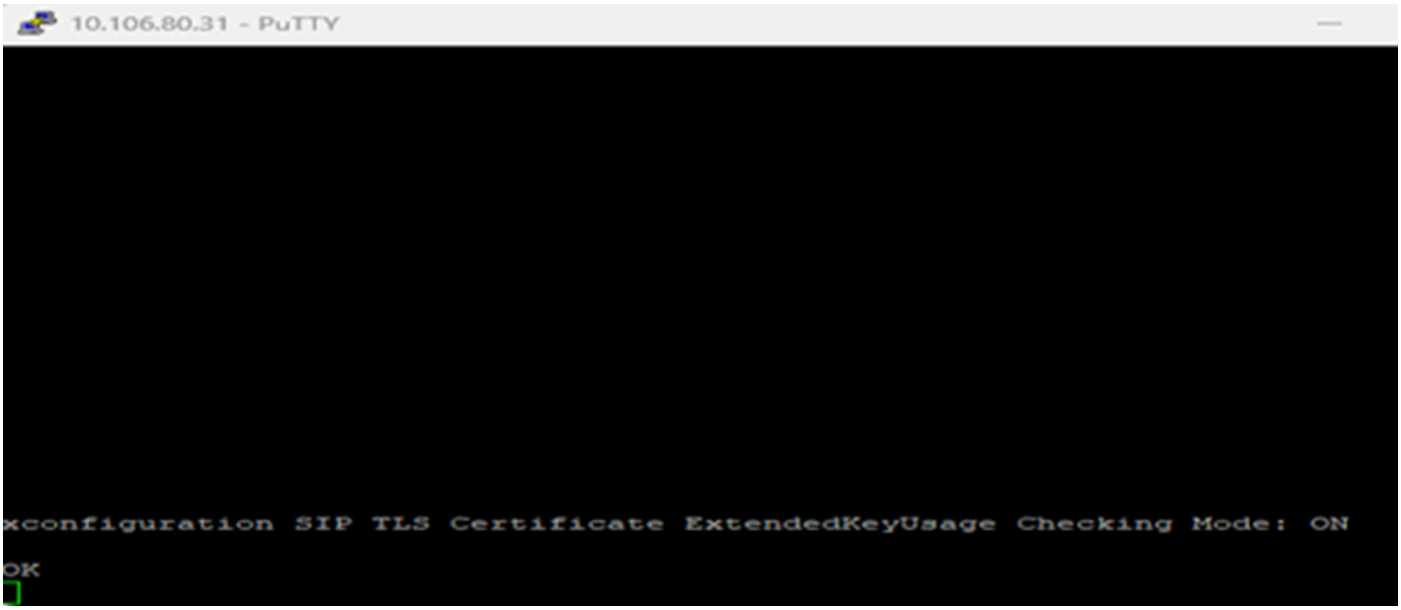
MRA-Client-Anmeldung und WebRTC-Proxy-Funktionen funktionieren nicht. Man könnte auf eine private CA zurückgreifen.

Testfall 1

- Wenn die EKU-Prüfung auf dem Expressway E "ON" ist
- Wenn das Client- und Server-Zertifikat auf dem Expressway-Core nur über Server-EKU verfügt
- UC-Zonenstatus ist FEHLGESCHLAGEN

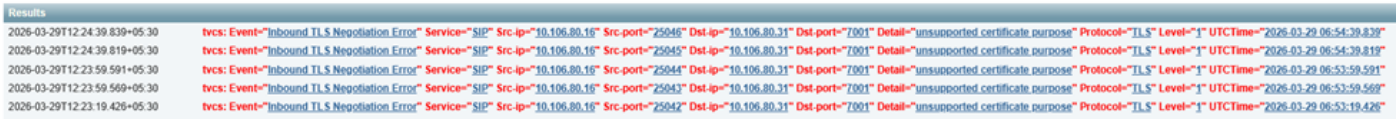
Auf Expressway-Edge ExtendedKeyUsage Check ON.

xconfiguration SIP-TLS-Zertifikat, ExtendedKeyUsage-Überprüfungsmodus: On (Aktiviert):



Ausfall der Unified Communications-Zone:

Expressway-E-Protokolle zeigen an, wo 10.106.80.16 = Expressway Core, 10.106.80.31 = Expressway Edge:

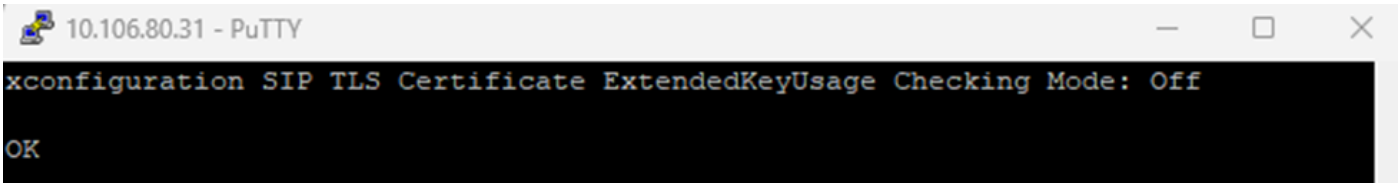


Testfall 2

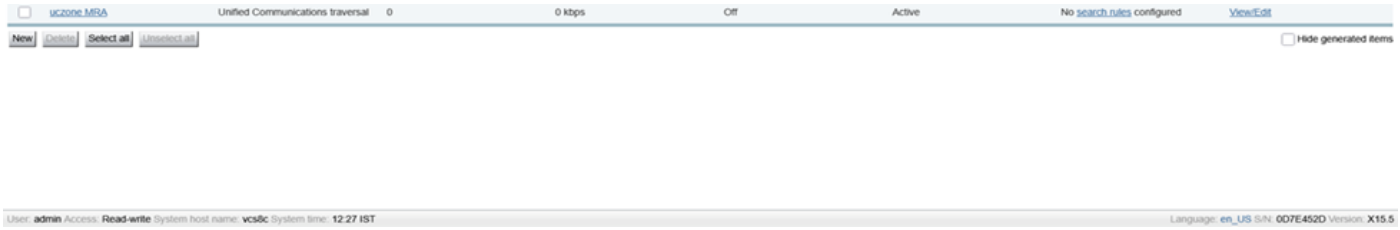
- Bei EKU-Prüfung auf Expressway E
- Wenn das Client- und Server-Zertifikat auf dem Expressway Core nur über den Server EKU verfügt
- Der Status der UC-Zone ist AKTIV.

Deaktivieren Sie die EKU-Prüfung auf dem Expressway E.

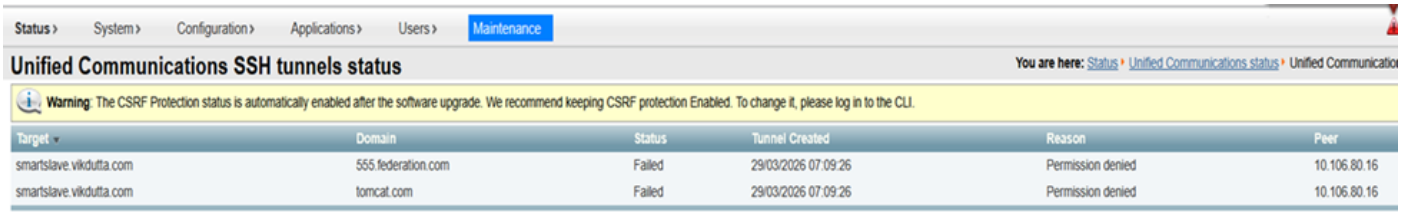
xconfiguration SIP-TLS-Zertifikat, ExtendedKeyUsage-Überprüfungsmodus: Aus



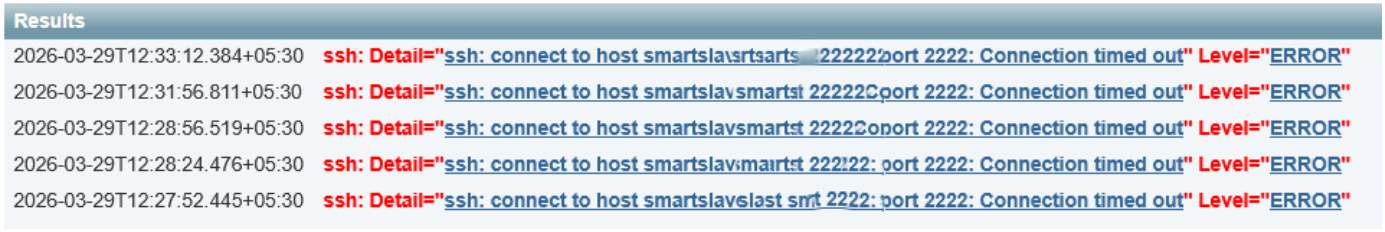
Unified Communication Zone Aktiv:



Allerdings sind die SSH-Tunnel noch immer ausgefallen:



Expressway-Ereignisprotokolle:



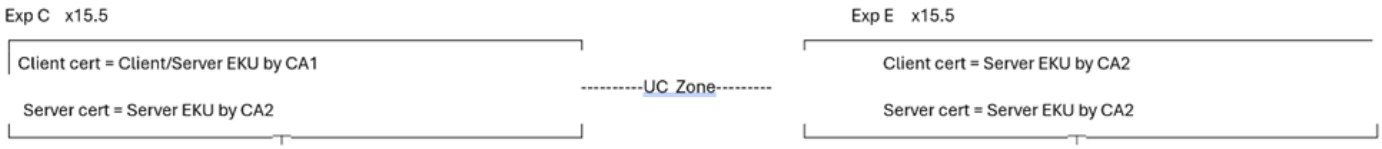
Bedingung 2.1: Erfolgsfall

CA 1 = Interne CA

CA 2 = Öffentliche Zertifizierungsstelle

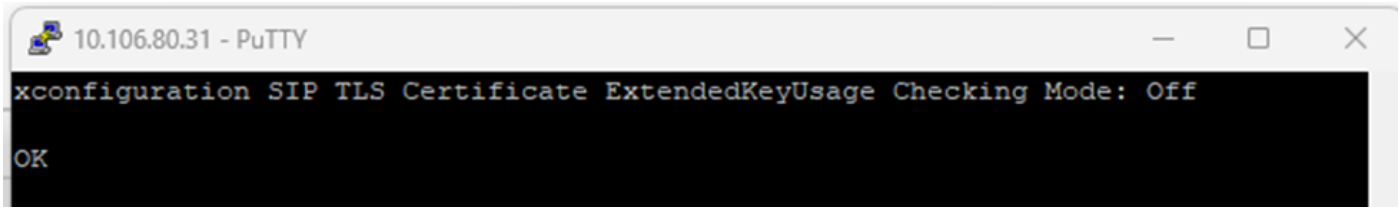
- Wenn das Expressway Core Client-Zertifikat von CA 1 (interne CA) signiert wird und beide enthält, Client/Server EKU.
- Das Expressway Core Server-Zertifikat wird von der öffentlichen CA 2 signiert und enthält nur Server-EKU.

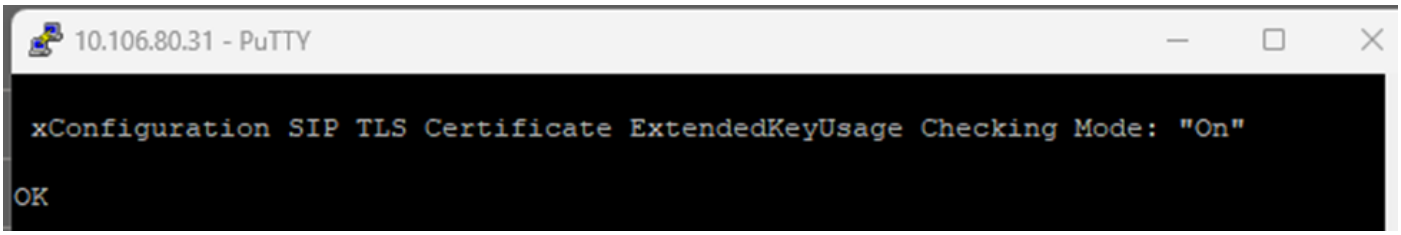
- Das Expressway Edge Server-Zertifikat wird von der öffentlichen CA 2 signiert und enthält nur Server-EKU.
- Das Expressway Edge-Clientzertifikat wird von der öffentlichen CA 2 signiert und enthält nur Server-EKU.



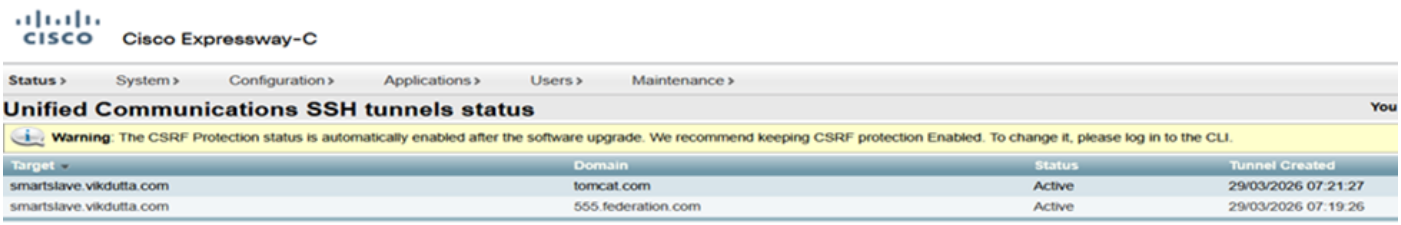
Diese Bedingung ist ein Erfolgsfall. Unabhängig davon, ob der EKU-Prüfmodus ON/OFF ist, werden sowohl die Unified Communication Zone als auch der SSH-Tunnel aktiviert. MRA-Clients arbeiten.

Dabei spielt es keine Rolle, ob der Expressway Edge EKU-Check AUS oder EIN ist. Das Expressway Core Client-Zertifikat enthält die Client-EKU:

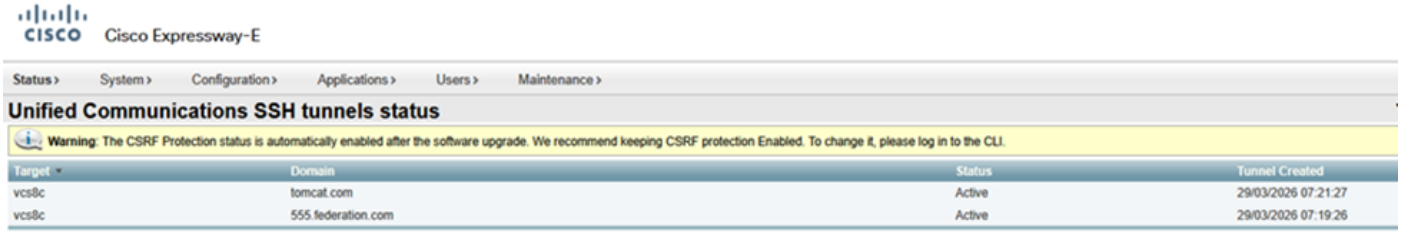




SSH-Tunnel auf Expressway Core Aktiv:

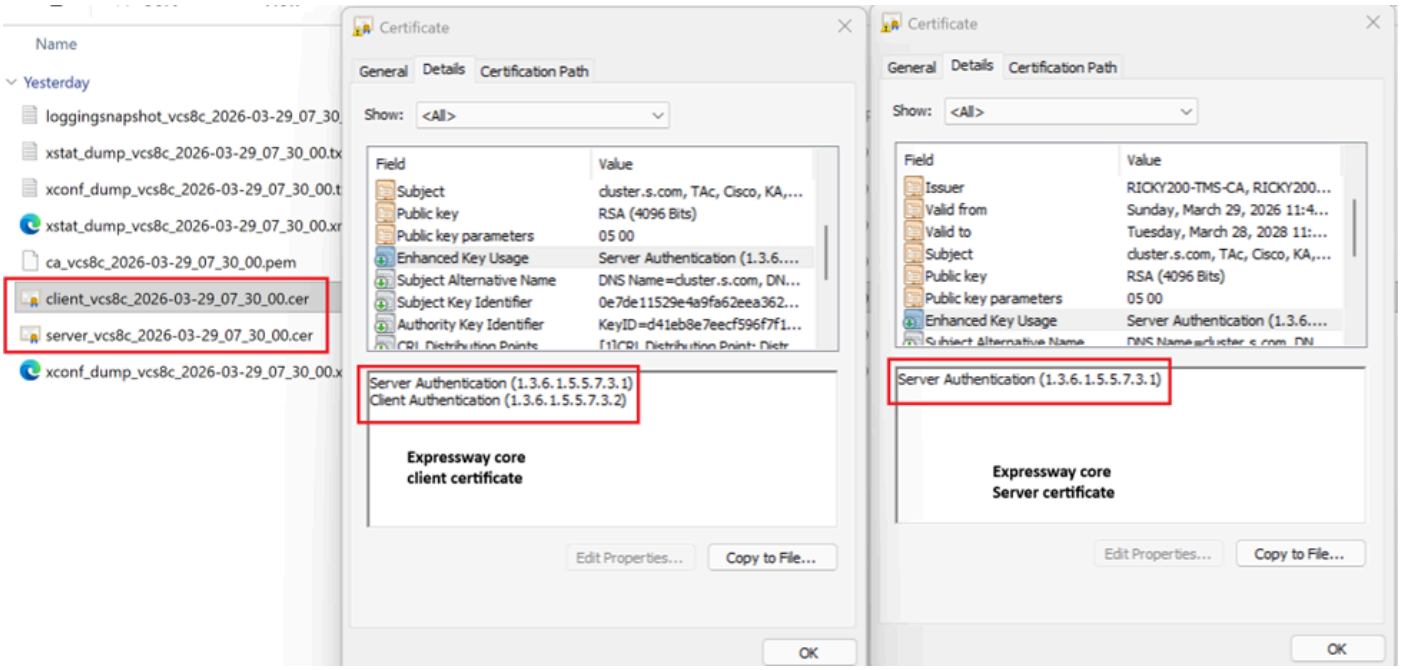


SSH-Tunnel am Expressway Edge aktiv:

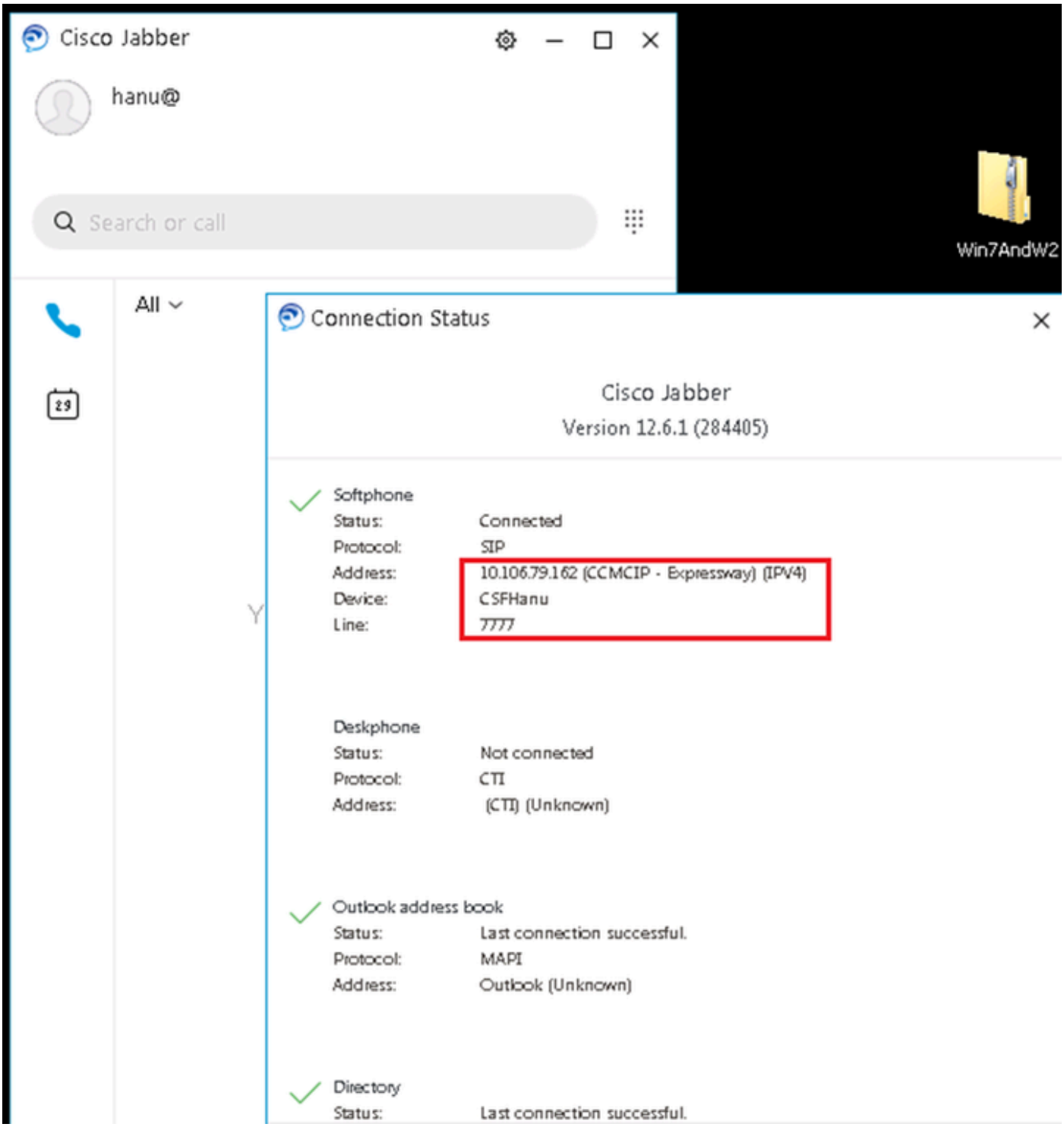


Unified Communications MRA-Zonenstatus Aktiv:

- Das Expressway-Core-Clientzertifikat weist Server-EKU und Client-EKU auf.
- Das Expressway Core Server-Zertifikat enthält nur Server-EKU.



MRA-Client meldet sich an und registriert:

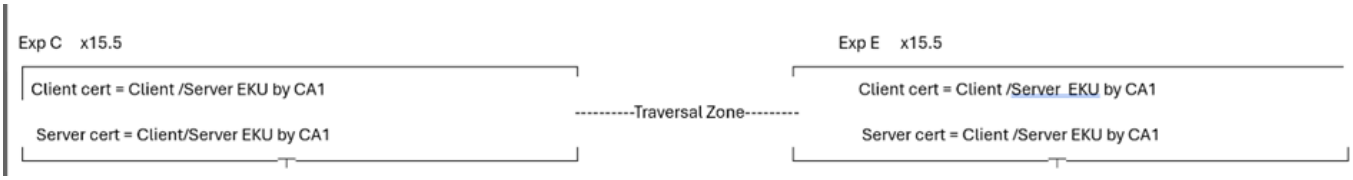


Anmerkung: Vergleichen und notieren Sie die EKUs, die in Zertifikaten für MRA- und WebRTC-Proxy vorhanden sind, damit sie funktionieren. Es handelt sich um einen Vergleich zwischen funktionierender und nicht funktionierender Bereitstellung.

Bedingung 3: Signiert alle Zertifikate mit privater Zertifizierungsstelle

CA 1 = Interne CA

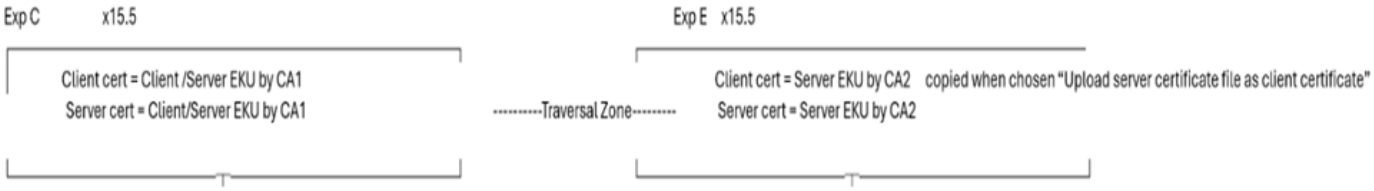
CA 2 = Öffentliche Zertifizierungsstelle



In Bedingung 3 werden alle Zertifikate von der internen CA (CA1) signiert.

- Wenn Expressway-E eine TLS-Verbindung sendet, muss CA1 Root/Intermediate mit einer Gegenstelle ausgetauscht werden. Wenn die Gegenstelle keine Funktion hat oder das Hochladen eines privaten Zertifizierungsstellenzertifikats nicht zulässt, ist die TLS-Verbindung fehlgeschlagen.
- MRA-Clients erhalten Zertifikate für die Annahme von Popup-Fenstern, wenn sich das private Zertifikat nicht im OS Trust Store befindet.

Bedingung 4: Expressway Edge verfügt über öffentliche Zertifikate nur mit Server-EKU



In Bedingung 4 sind die Expressway-Core-Client- und -Serverzertifikate (CA1) von einer internen Zertifizierungsstelle signiert und verfügen über eine Client- und Server-EKU. Das Expressway E-Serverzertifikat ist eine öffentliche CA, die signiert ist, und hat nur eine Server-EKU. Das Serverzertifikat wird in den Clientzertifikatspeicher kopiert. Wählen Sie Serverzertifikatdatei als Clientzertifikat hochladen aus.

Wenn in Bedingung 4 eine TLS-Verbindung mit dem Gegenstück hergestellt wird und Expressway -E einen TLS-Client hello sendet, muss das Gegenstück die Client-EKU-Prüfung deaktivieren (da das Clientzertifikat keine Client-Authentifizierungs-EKU aufweist), andernfalls ist die TLS-Verbindung nicht erfolgreich.

Je nach Anwendungsfall und Bereitstellung durch die Benutzer kann es in der Praxis zu einer Vielzahl von Bedingungen oder Szenarien kommen, die aufgrund meines begrenzten Gedankenguts nicht abgedeckt werden können. Folgende Punkte sollten Sie sich jedoch merken:

- # WENN Expressway während des TLS-Handshakes zum Client wird, wird das Client-

Zertifikat den Peers präsentiert.
- #IF Expressway wird während des TLS-Handshakes zum Server. Das Serverzertifikat wird dem Peer angezeigt.

Diese Argumentation wurde bei diesen Testfällen erarbeitet.

Szenario 1

In diesem Szenario präsentiert Expressway das Client-Zertifikat während des MTLS-Handshakes mit WebEx.

Videoanruf zu WebEx Meeting:

Beispiel für einen Anruffluss: Jabber -à CUCM -à Exp Core -à Exp Edge -à WebEx

10.106.80.31= Expressway-Edge

163.129.37.33 = WebEx

24.03.2026 11:54:26.106+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 verfügt über ein Client-Zertifikat mit dieser Seriennummer (2f0000004c869c77c8981becde00000000004c).

Expressway Edge sendet Client-Hello an "Webex" während der TLS-Aushandlung und sendet dann Client-Zertifikat.

Seriennummer 2f0000004c869c77c8981becde00000000004c:

1. Expressway Edge sendet Client Hello (pkt= 13699) während der mTLS-Aushandlung an "Webex".

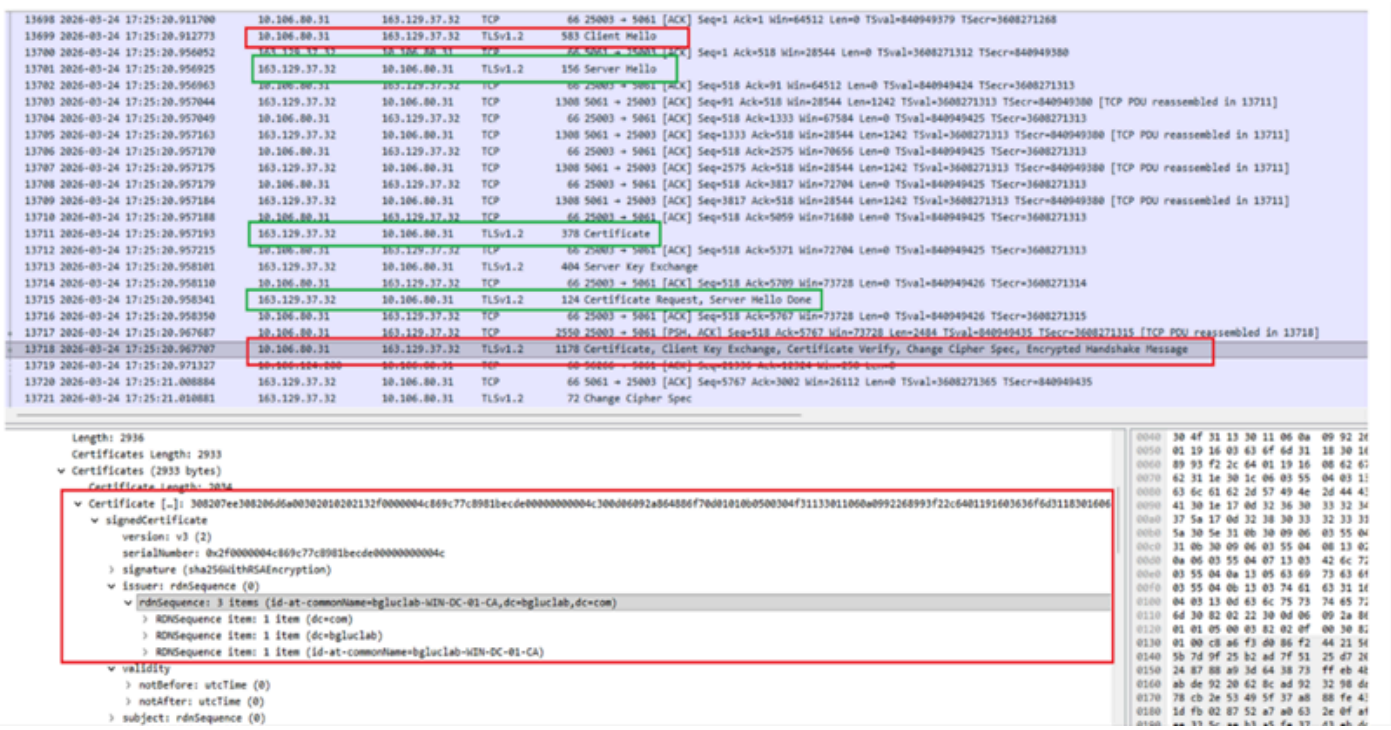
2. WebEx sendet einen Server-Hello an Expressway Edge (pkt=13701).

3. Webex sendet sein Zertifikat an Expressway Edge (pkt=13711).

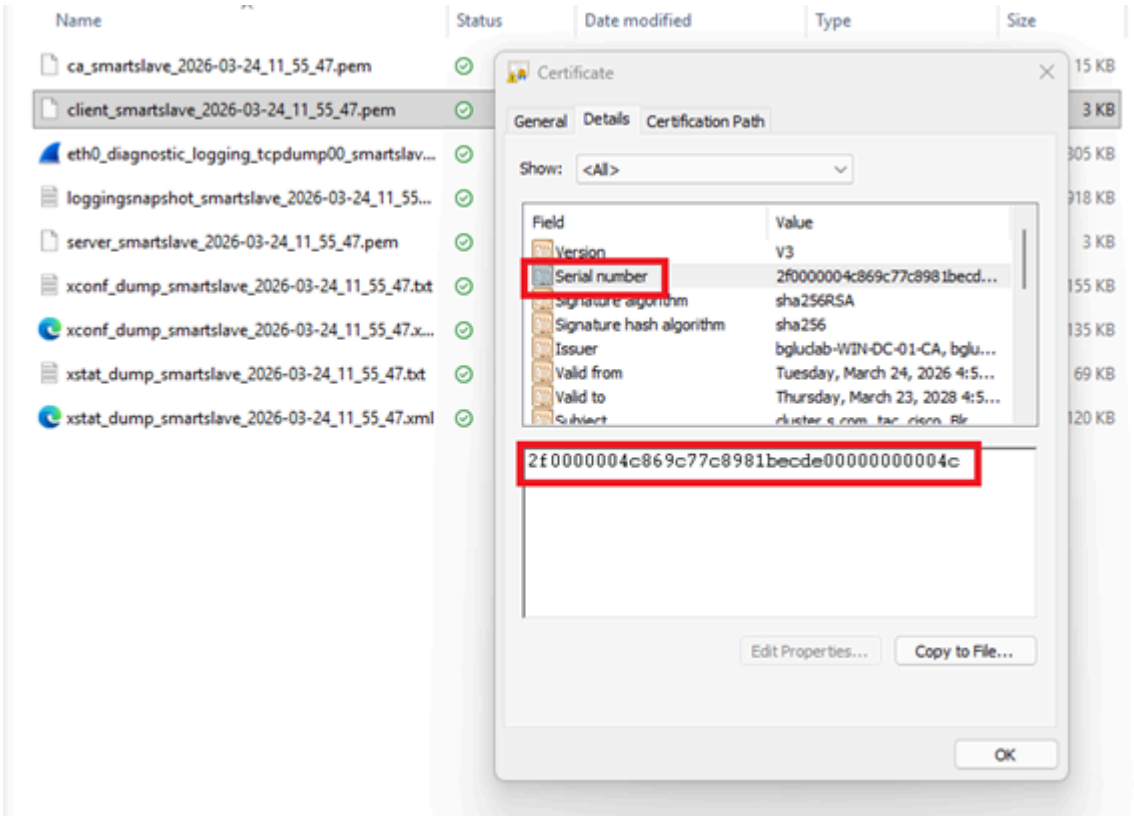
4. WebEx fordert Expressway-Edge-Zertifikat "CertificateRequest" an (pkt=13715).

5. Expressway Edge sendet sein Zertifikat an Webex (pkt=13718).

(Screenshot)



Client-Zertifikat von Expressway Edge:



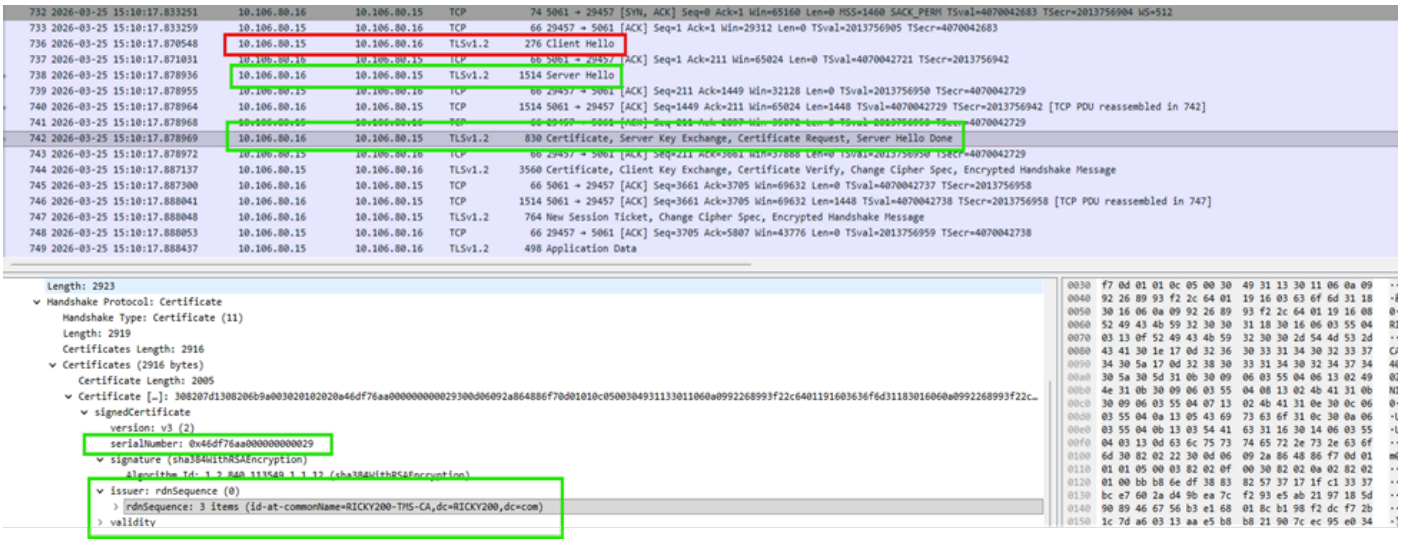
Szenario 2

Expressway wird während des mTLS-Handshakes zur Server-Einheit und präsentiert sein Server-Zertifikat:

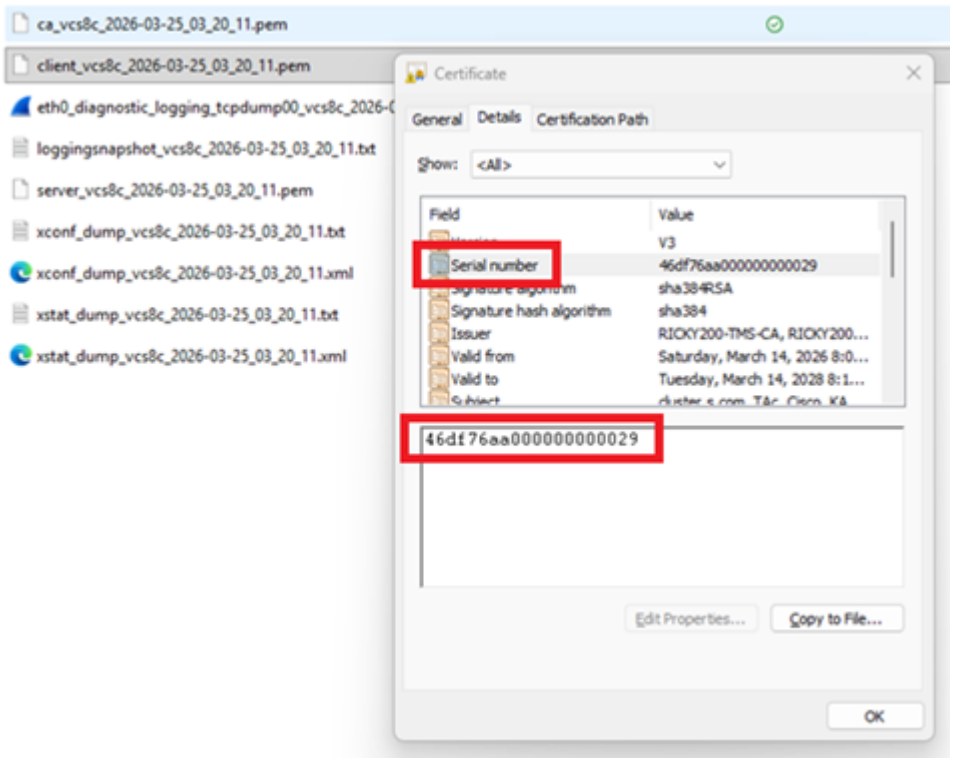
Wenn Expressway ein Serverzertifikat präsentiert, verfügt Expressway über eine sichere Nachbarzone über 5061 mit dem Verifizierungsnamen ON.

Sicherer Nachbarbereich zwischen Expressway-Knoten x15.5 und Expressway-Knoten 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)
```



Dieser Screenshot zeigt das Serverzertifikat als Übereinstimmung mit der Seriennummer:



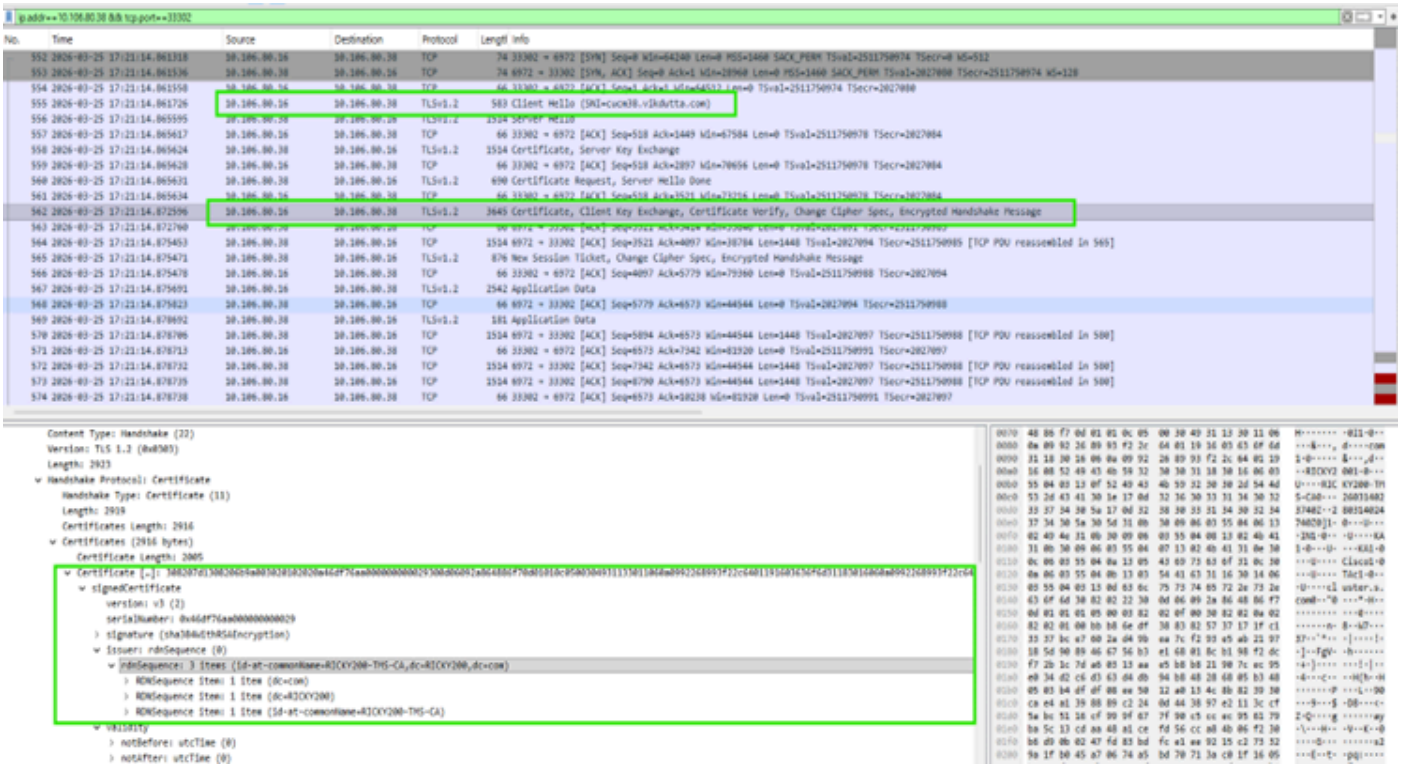
Testfall 3: Der MRA-Client wird für die Anmeldung bereitgestellt, und der Workflow umfasst die Überprüfung der Datenverkehrsserverzertifikate zwischen Expressway Core und CUCM.

10.106.80.16 = Expressway Core x15.5

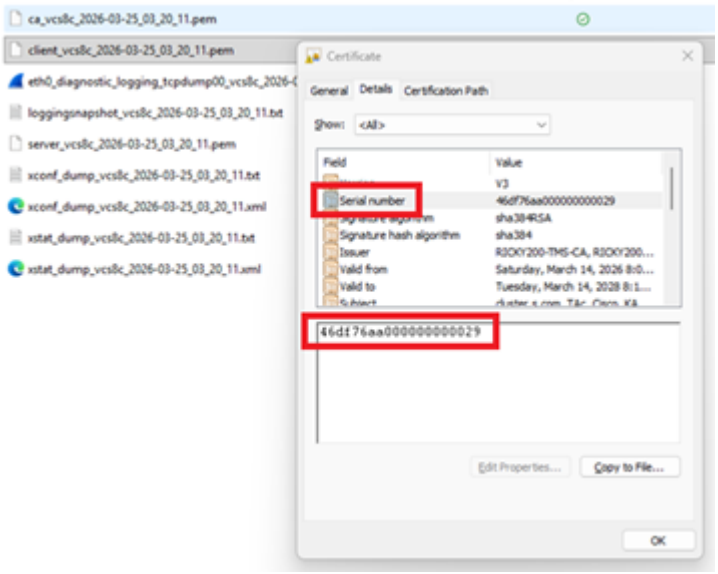
10.106.80.38 = CUCM

- Exp. C 16 sendet einen Client-Hello auf 6972 TFTP.

- Exp C 16 sendet ein Client-Zertifikat während des TLS-Handshakes.



Expressway Core Client-Zertifikat:



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.