Naviguer dans le coucher de soleil EKU client avec Expressway x15.5

Introduction

Ce document décrit la navigation dans le coucher de soleil EKU du client avec Cisco Expressway x15.5.

Informations générales

Les certificats numériques sont des informations d'identification électroniques émises par des autorités de certification (CA) de confiance qui sécurisent la communication entre les serveurs et les clients en garantissant l'authentification, l'intégrité des données et la confidentialité. Ces certificats contiennent des champs d'utilisation de clé étendue (EKU) qui définissent leur objectif :

- Server Authentication EKU (id-kp-serverAuth) est utilisé lorsqu'un serveur présente son certificat pour prouver son identité.
- L'EKU d'authentification client (id-kp-clientAuth) est utilisée dans les connexions TLS mutuelles (mTLS) où les deux parties s'authentifient l'une l'autre.

Traditionnellement, un seul certificat peut contenir à la fois des UEC d'authentification de serveur et de client, ce qui lui permet de remplir deux fonctions. Ceci est particulièrement important pour les produits tels que Cisco Expressway qui agissent à la fois comme serveur et comme client dans différents scénarios de connexion.

Définition du problème

Modification de la politique du programme racine Chrome

À compter de juin 2026, la politique du programme racine Chrome restreint les certificats de l'autorité de certification racine (CA) inclus dans le magasin racine Chrome, éliminant progressivement les racines polyvalentes pour aligner toutes les hiérarchies d'infrastructure à clé publique (PKI) afin de servir uniquement les cas d'utilisation d'authentification du serveur TLS.

Principales exigences de stratégie

- Les autorités de certification racines publiques doivent affirmer l'utilisation de clé étendue (EKU) UNIQUEMENT pour l'authentification du serveur (id-kp-serverAuth).
- Il est interdit d'inclure l'EKU d'authentification client dans ces certificats.
- Plus d'autorités de certification racine à utilisation mixte pour les certificats TLS de serveur public.
- Délai d'application : Juin 2026

Délai de réponse de l'AC publique

- Octobre 2025 : Par défaut, de nombreuses autorités de certification publiques (DigiCert, Sectigo, SSL) ont commencé à émettre des certificats de serveur uniquement.
- Mai 2026 : Les serveurs CA publics arrêtent d'émettre des certifications EKU d'authentification client
- Juin 2026 : La politique du programme racine de Chrome devient pleinement efficace

---

Remarque : Cette politique s'applique uniquement aux certificats émis par des autorités de certification publiques. L'ICP privée et les certificats auto-signés ne sont pas affectés par cette stratégie.

Si vous êtes intéressé à lire sur l'impact de la temporisation de l'EKU client sur Expressways, référez-vous à [Préparer Expressway pour l'authentification client EKU temporisation dans les certificats d'autorité de certification publique.]

Expressway version x15.5 avec solution

Expressway x15.5

Expressway x15.5 est livré avec une solution proposée pour un problème qui se pose en raison de la temporisation de l’EKU client par toutes les autorités de certification publiques. Il s'agit d'un problème global qui affecte tous les fournisseurs/déploiements qui choisissent d'utiliser des certificats PKI publics.

x15.4, une version antérieure, avait un commutateur de commande CLI qui permettait à l’administrateur de télécharger le certificat Server EKU only (pas d’EKU client présent) sur Expressway E.

xConfiguration Certificat XCP TLS CVS EnableServerEkuUpload : On (activé)

Remarque : Cette commande est déconseillée sur x15.5.

Ajout au magasin de certificats X15.5

x15.5 possède deux magasins de certificats :

1. Magasin de certificats du serveur

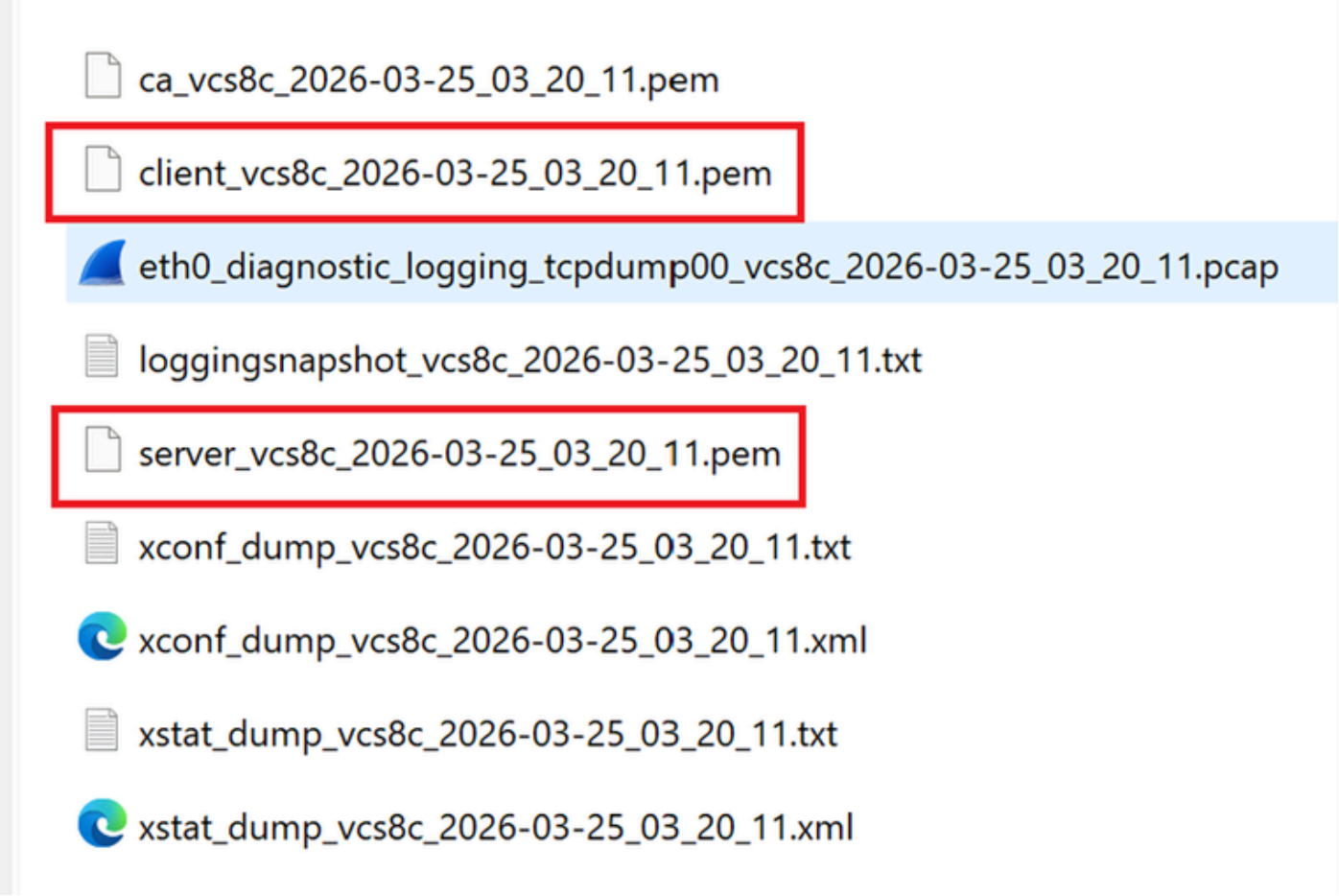
2. Magasin de certificats client

Expressways (carte réseau simple ou double) : Les deux interfaces Expressway peuvent utiliser 2 magasins de certificats en fonction des besoins.

Exemple :

- Lorsqu'expressway agit en tant que client pendant la connexion TLS, le certificat client est présenté.
- Lorsque expressway agit en tant que serveur lors de la connexion TLS, le certificat de serveur est présenté.

Remarque : Les deux magasins de certificats (client et serveur) utilisent la même bibliothèque d'autorités de certification approuvées. Assurez-vous que l'autorité de certification qui a signé les certificats du serveur et du client est correctement téléchargée sur le magasin d'approbations. Les journaux de diagnostic incluent désormais le certificat du serveur et le certificat du client au format de fichier PEM.



Mise à niveau de X15.4 ou version antérieure vers X15.5

Lorsqu'une mise à niveau est effectuée, le certificat du serveur à partir de x15.4 ou d'une version antérieure, le magasin de certificats du serveur Expressway est copié dans le magasin de certificats du client sur x15.5. Les magasins de certificats du client et du serveur sur x15.5 ont le même certificat.

Exemple avec captures d'écran

Serveur Expressway sur 15.4, certificat de serveur actuel Numéro de série 46:df:76:aa:00:00:00:00:00:29

Certificat:

Version : 3 (0x2)

Numéro de série:

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

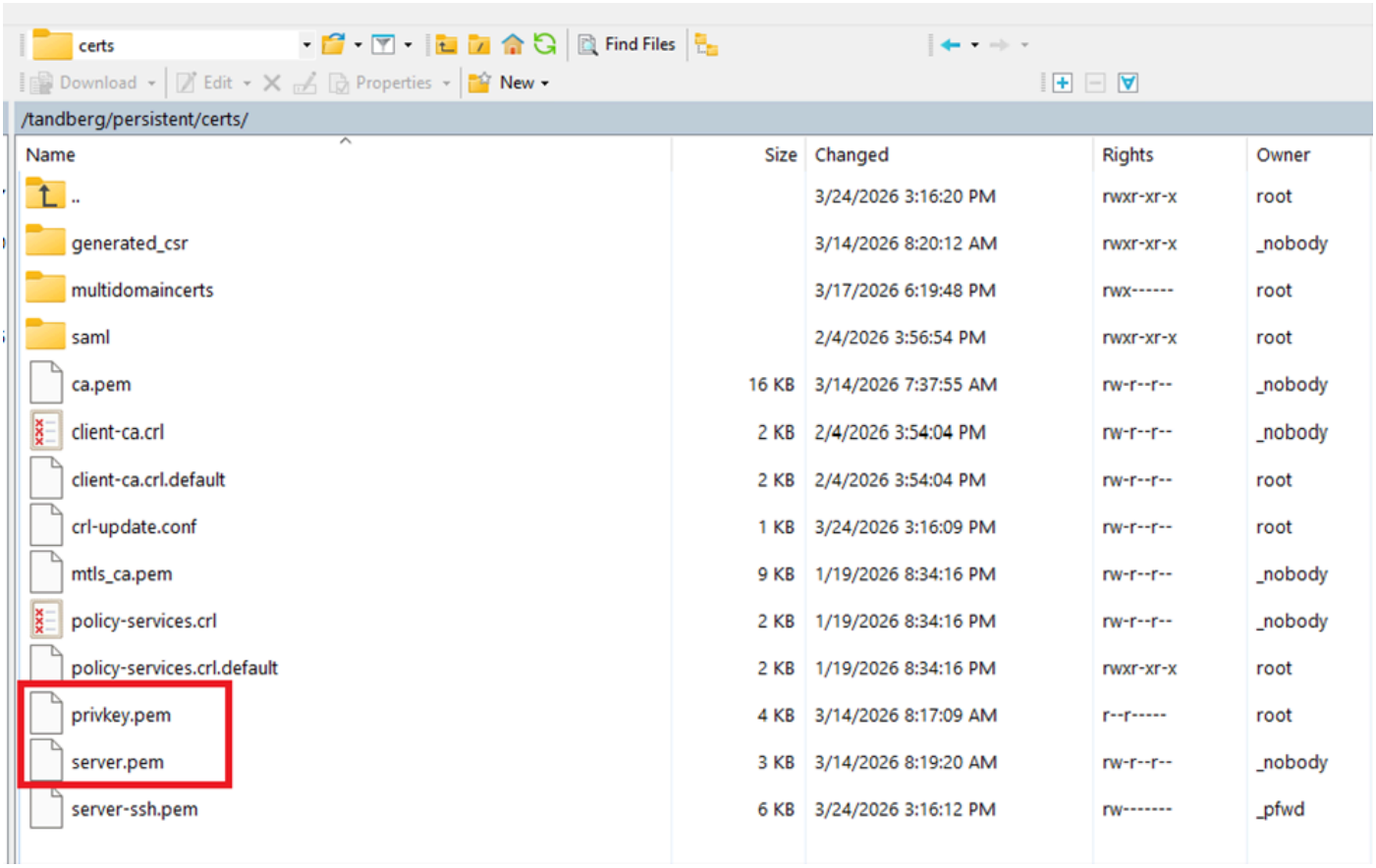
Validité

Pas avant : 14 mars 02:37:40 2026 GMT

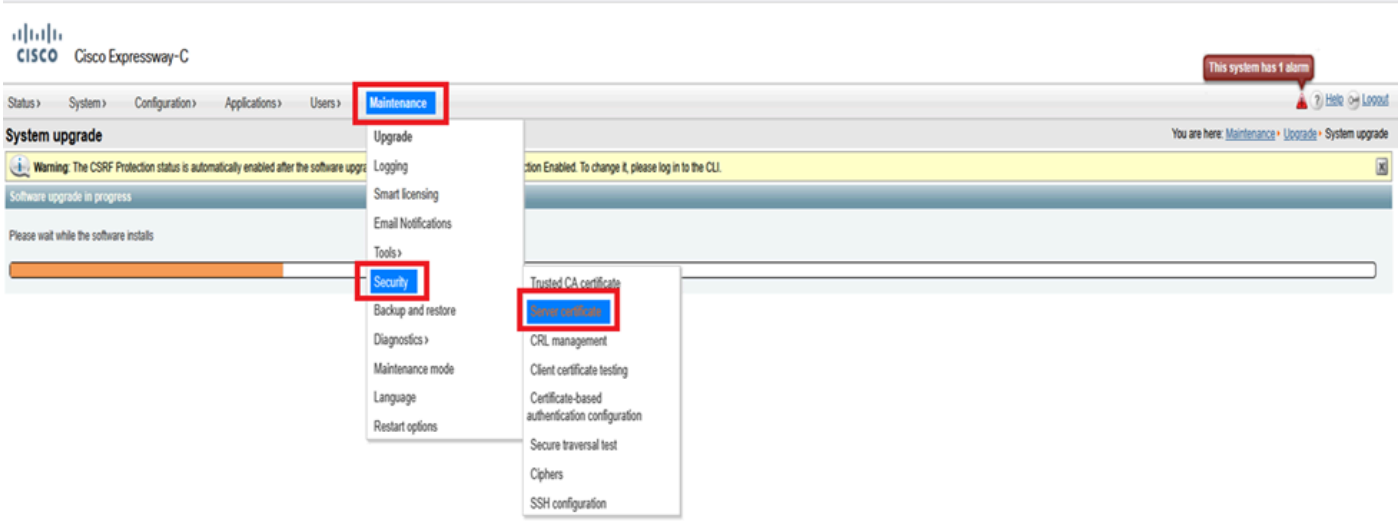
Pas après : 14 mars 02:47:40 2028 GMT

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

Répertoire persistant/cert du système de fichiers Expressway sur x15.4 :

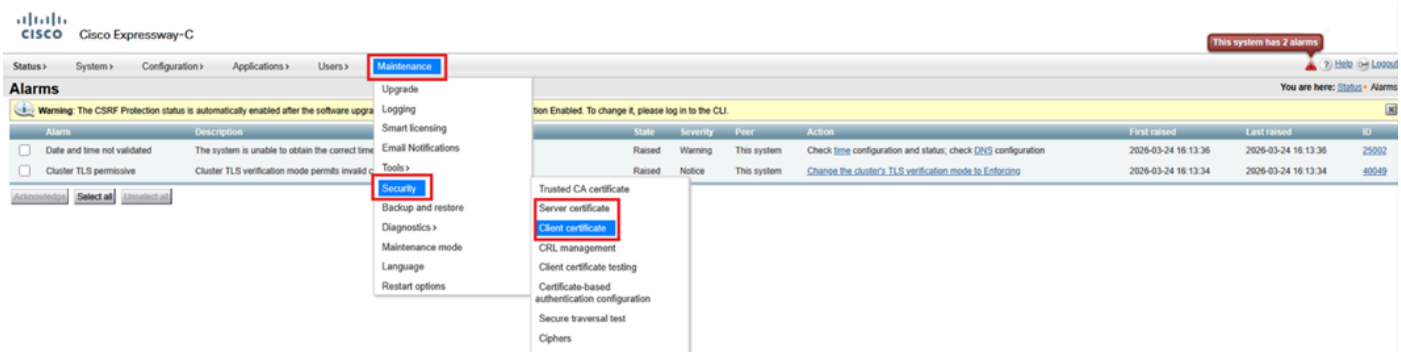


Menu Expressway (Maintenance > Security > Server certificate) sur x15.4 (seul champ de certificat de serveur présent) :



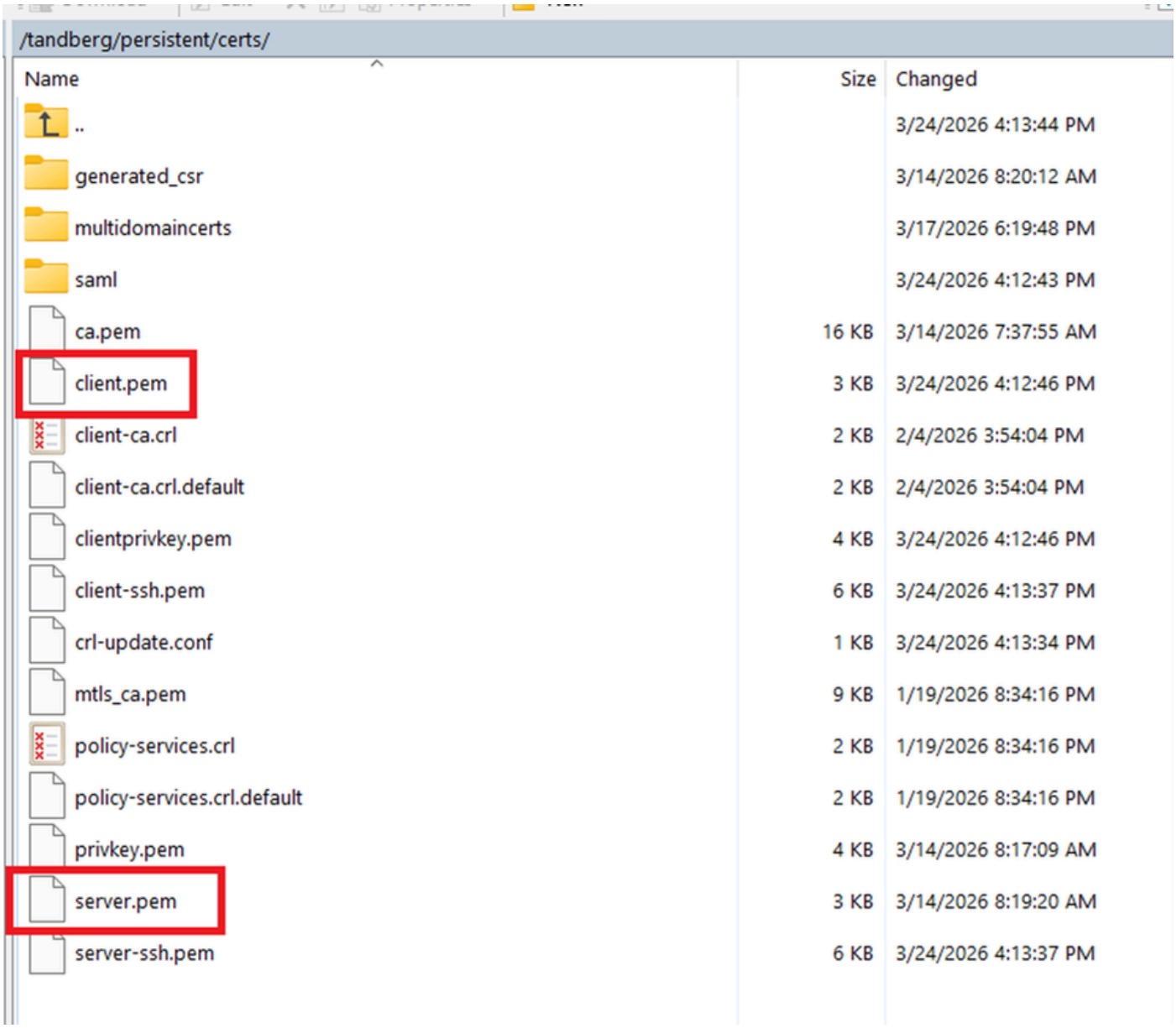
Après une mise à niveau réussie vers x15.5

Ici, vous voyez 2 options de certificat sous Maintenance > Security > client certificate and server certificates. Après la mise à niveau vers x15.5, les portails de certificats Serveur et Client de l'administrateur Web affichent le même certificat, car le certificat du serveur de x15.4 a été copié dans le magasin de certificats client sur x15.5.



Une mise à niveau vers un certificat et une clé privée x15.5 existants a été copiée dans le magasin de certificats client.

Répertoire persistant/cert du système de fichiers Expressway sur x15.5 :



Vérification de l'UKE X15.5 pendant la connexion TLS

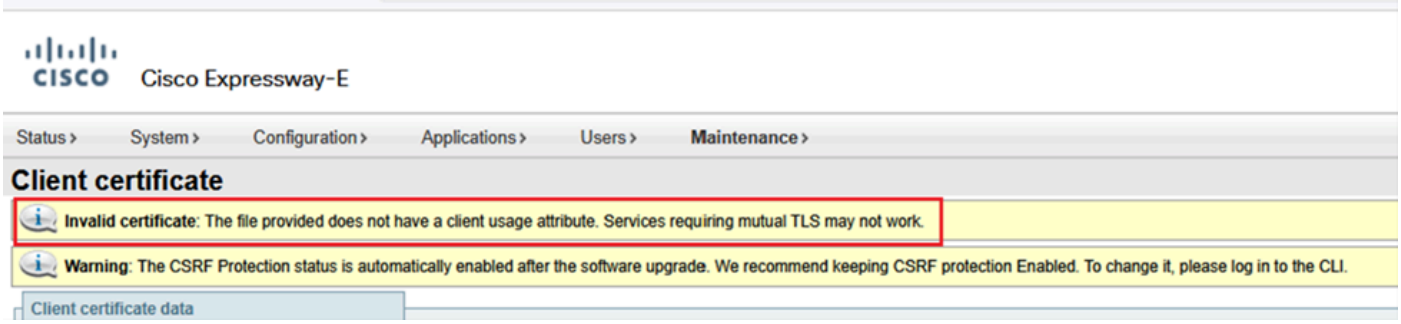
Sur x15.5, une nouvelle commande CLI a été introduite pour vérifier l'utilisation de la clé étendue (EKU) pendant la connexion TLS. La valeur par défaut est « ON ». Le jeu de commandes est valide sur Expressway Core et Edge.

La commande set déclenche une vérification de toutes les connexions INBOUND SIP TLS dans Expressway. (hello/certificat client entrant présenté). Lorsque cette option est activée, elle vérifie si le certificat présenté par l'initiateur TLS contient ou non l'EKU client dans le certificat. S'il est désactivé, la vérification est ignorée ; cependant, l'UKE du serveur est vérifiée si elle est présente sur le certificat.

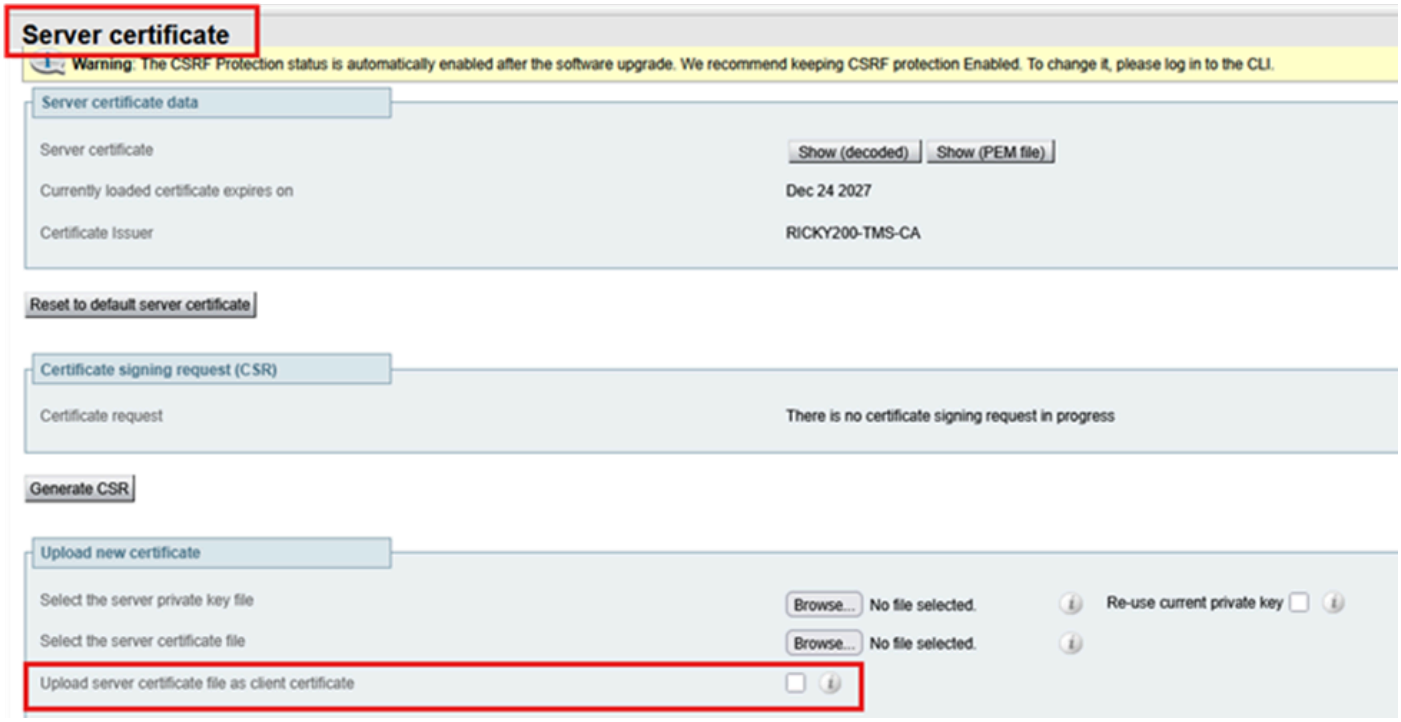
xconfiguration SIP TLS Certificate ExtendedKeyMode de vérification de l'utilisation : ACTIVÉ/DÉSACTIVÉ :

Remarque : Si vous générez un certificat client en signant un CSR qui ne contient pas l'EKU client (un exemple de certificat signé par une autorité de certification publique), vous ne pouvez pas télécharger ce certificat manuellement sur le magasin de certificats client. Vous devez donc vous assurer que les certificats générés par la signature d'un CSR contiennent toujours l'EKU client (une autorité de certification privée peut être utilisée pour insérer l'EKU client).

Conseil : Cette erreur devient évidente lorsque vous tentez de télécharger un certificat signé CSR, qui ne contient pas l'EKU client, à partir du magasin de certificats client.



Cependant, si vous choisissez de télécharger un certificat qui a une EKU serveur seulement (pas d'EKU client) via le magasin de certificats du serveur et sélectionnez Télécharger le fichier de certificat du serveur comme certificat client, le certificat est copié dans le magasin de certificats du client. Les administrateurs qui ne veulent pas utiliser un certificat signé par une autorité de certification privée sur Expressway-Edge peuvent choisir de copier l'UKE du serveur seulement du magasin de certificats du serveur vers le magasin de certificats du client.

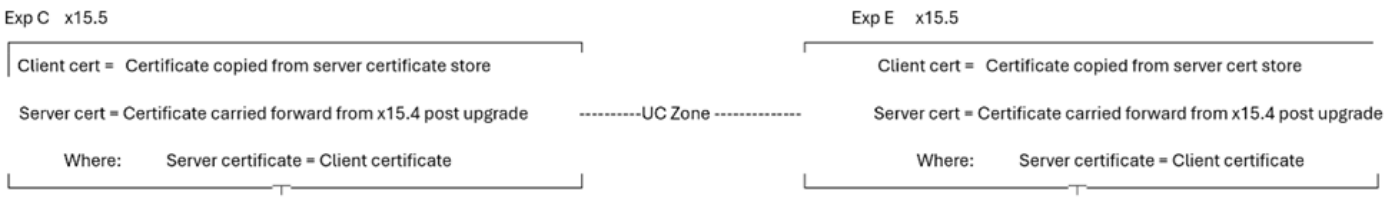


Plusieurs magasins de certificats, plusieurs scénarios de déploiement

Étant donné qu'il existe maintenant deux magasins de certificats sur Expressway, il existe plusieurs scénarios de magasins de certificats.

Condition 1 : Mise à niveau

Lorsque Expressway est mis à niveau à partir de x15.4 ou avant x15.5, cette condition est vraie. Les certificats existants de la version x15.4 sont copiés dans deux (2) magasins de certificats. Sur le client et le serveur x15.5, les certificats sont identiques.

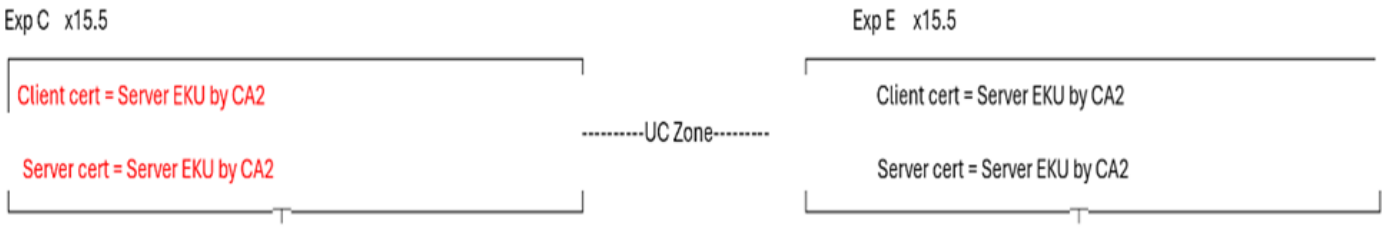


Condition 2 : Lorsque l'administrateur installe un nouveau certificat sur x15.5 (les certificats existants ont expiré)

CA 1 = CA interne

CA 2 = CA publique

Dans la figure ci-dessous, Expressway Core possède un certificat client avec l'EKU du serveur signé uniquement par CA 2 (Autorité de certification publique) et un certificat de serveur avec l'EKU du serveur signé uniquement par CA 2 (Autorité de certification publique). De même, Expressway E dispose d'un certificat client avec l'EKU serveur signé par CA2 (AC publique) et d'un certificat serveur avec l'EKU serveur signé uniquement par CA2 (AC publique).



Si le certificat du serveur principal Expressway n'a pas d'EKU client, de zone de traversée des communications unifiées, de MRA, le proxy WebRTC ne fonctionne pas. Assurez-vous que le certificat du serveur Expressway Core a une unité d'évaluation du client. Il s'agit d'un cas d'utilisation courant où les utilisateurs choisissent de signer tous les certificats de l'autorité de certification publique. Puisque l'autorité de certification publique n'inclut pas l'UKE du client dans les certificats, la zone de traversée des communications unifiées devient active.

Pour rendre la zone UC active, une solution rapide consiste à désactiver la vérification EKU sur l'Expressway E. La zone UC s'affiche. Cependant, les tunnels SSH restent inactifs. À partir d'aujourd'hui, la communication du tunnel SSH sur le 2222 nécessite la validation de l'EKU client.

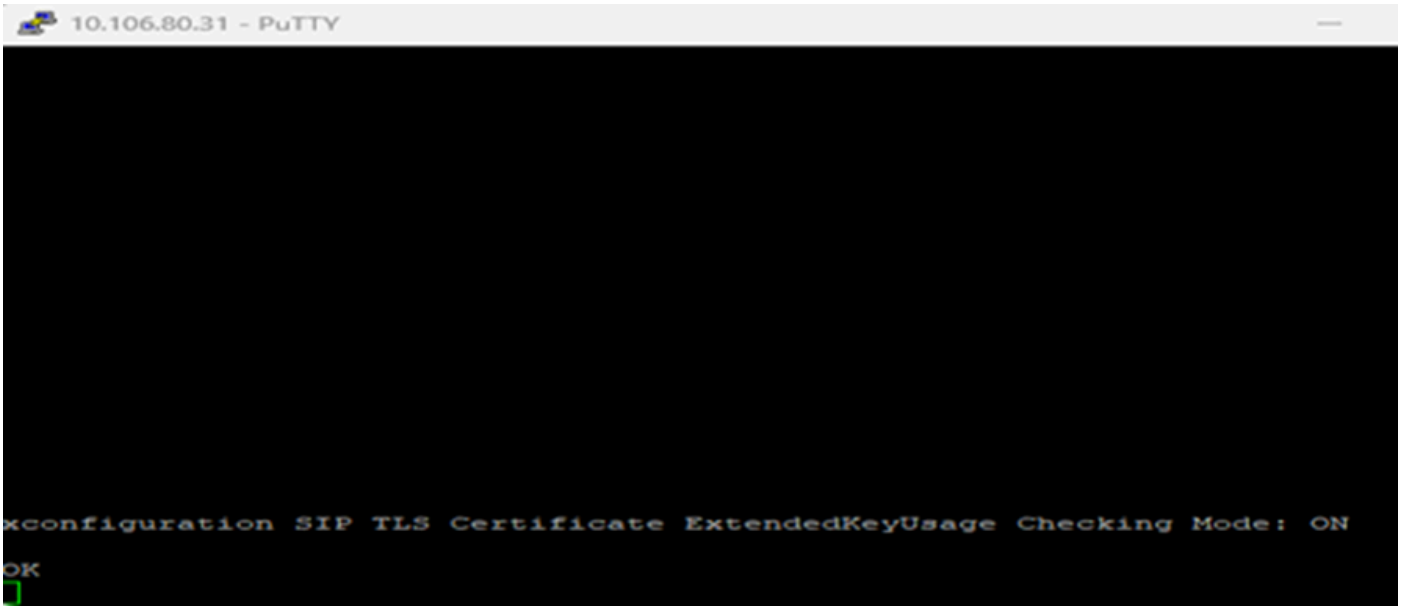
Les fonctions de connexion au client MRA et de proxy WebRTC ne fonctionnent pas. Vous pourriez devoir recourir à une autorité de certification privée.

Cas de test 1

- Lorsque la vérification EKU est activée sur l'Expressway E
- Lorsque le certificat Client et Serveur sur Expressway Core a Server EKU seulement
- L'état de la zone UC est FAILED

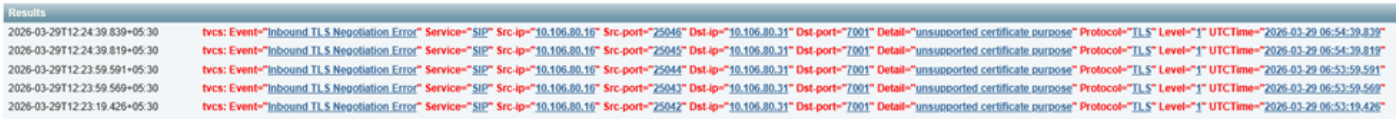
Sur Expressway-Edge ExtendedKeyUsage, activez la case à cocher.

xconfiguration SIP TLS Certificate ExtendedKeyMode de vérification de l'utilisation : Activé:



Échec de la zone de communication unifiée :

Les journaux d'Expressway E indiquent où 10.106.80.16 = Expressway Core, 10.106.80.31 = Expressway Edge :

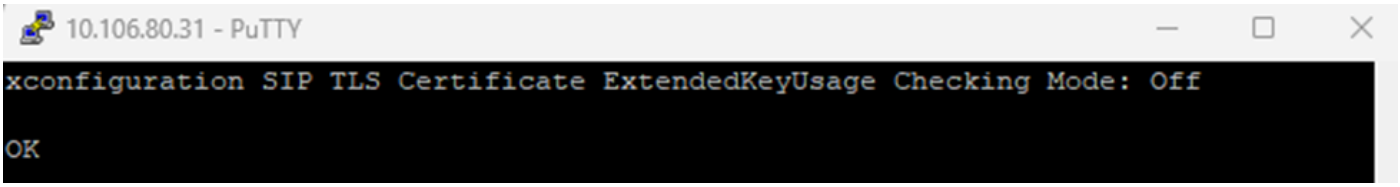


Cas de test 2

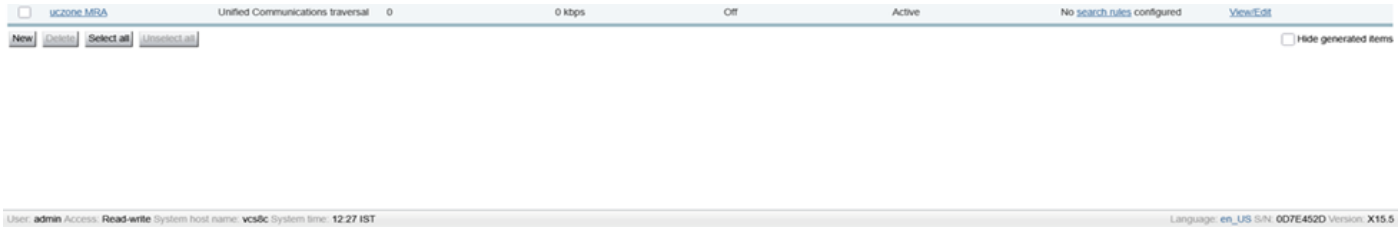
- Lorsque le contrôle EKU est désactivé sur l'Expressway E
- Lorsque le certificat Client et Serveur sur Expressway Core a une UER serveur seulement
- L'état de la zone UC est ACTIF

Désactivez le contrôle EKU sur l'Expressway E.

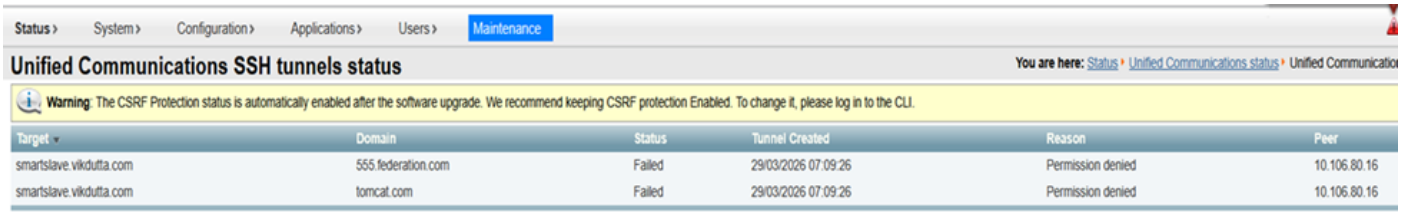
xconfiguration SIP TLS Certificate ExtendedKeyMode de vérification de l'utilisation : Off (désactivé)



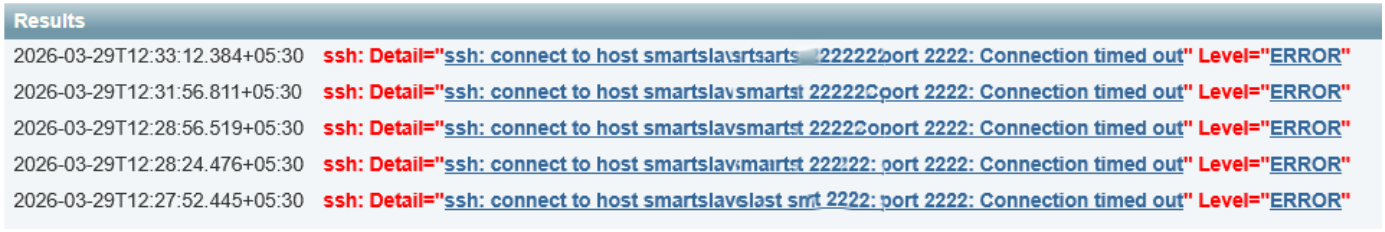
Zone de communication unifiée active :



Cependant, les tunnels ssh ont toujours échoué :



Journaux des événements Expressway :



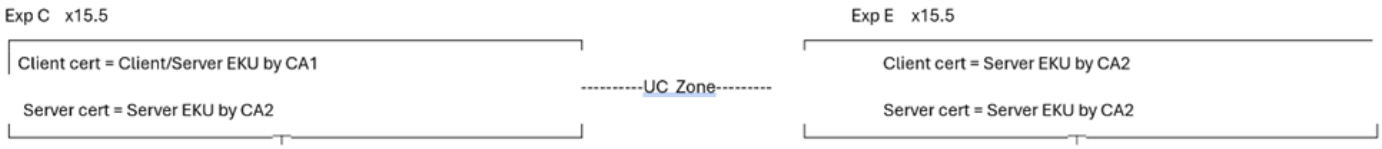
Condition 2.1 : Cas de réussite

CA 1 = CA interne

CA 2 = CA publique

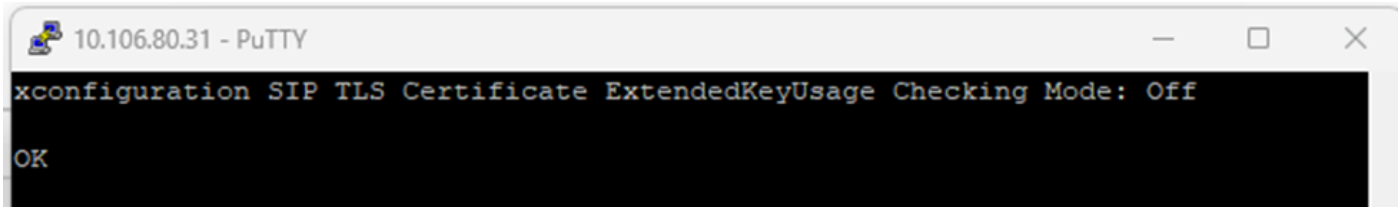
- Où le certificat client principal d'Expressway est signé par CA 1 (CA interne) et inclut, Client/Server EKU les deux.
- Le certificat de serveur principal Expressway est signé par l'autorité de certification publique CA 2 et inclut l'unité de clé du serveur uniquement.

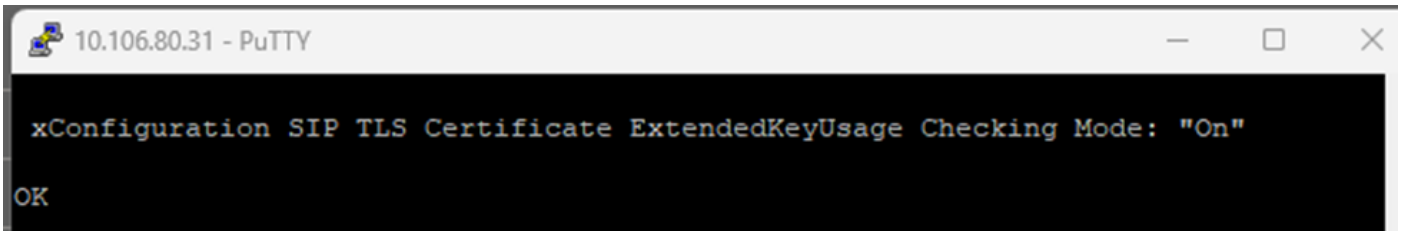
- Le certificat du serveur de périphérie Expressway est signé par l'autorité de certification publique CA2 et inclut l'unité de clé du serveur seulement.
- Le certificat client Expressway Edge est signé par l'autorité de certification publique CA 2 et inclut l'unité de clé du serveur uniquement.



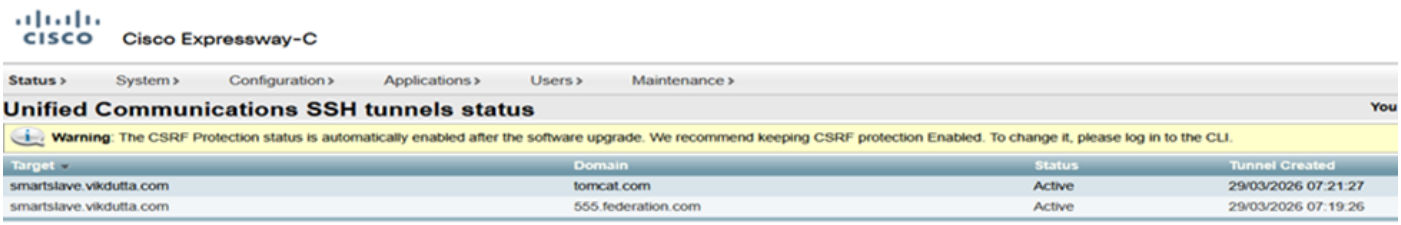
Cette condition est un cas de réussite. Que le mode de vérification EKU soit ON/OFF ou non, la zone de communication unifiée et le tunnel SSH deviennent tous deux actifs. Les clients MRA fonctionnent.

Peu importe que la vérification EKU de l'Expressway Edge soit activée ou désactivée. Le certificat du client principal Expressway contient l'EKU du client :

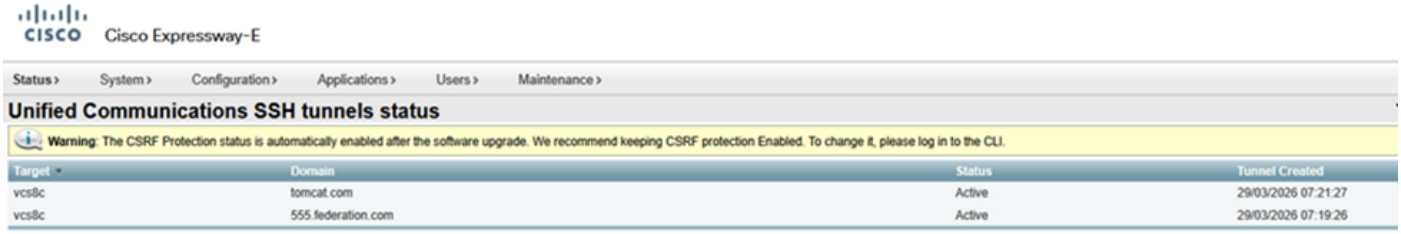




Tunnels SSH sur le coeur Expressway actif :

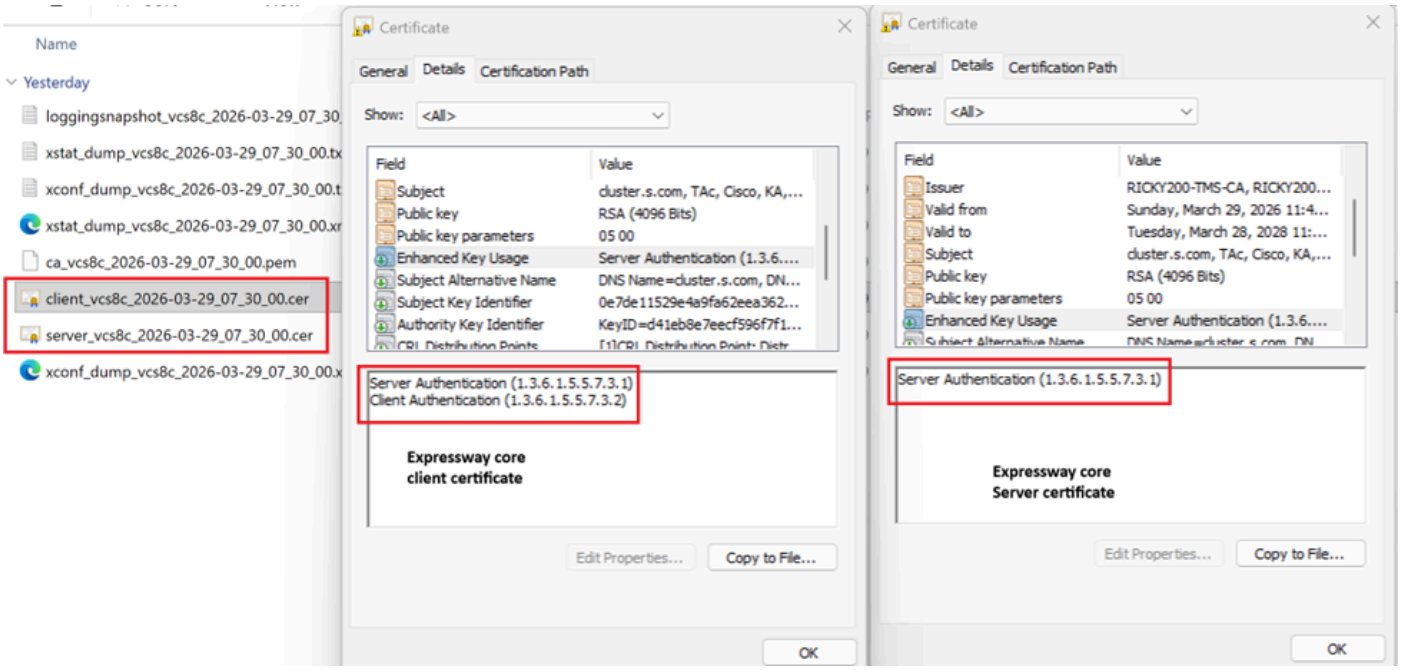


Tunnels SSH sur Expressway Edge Active :

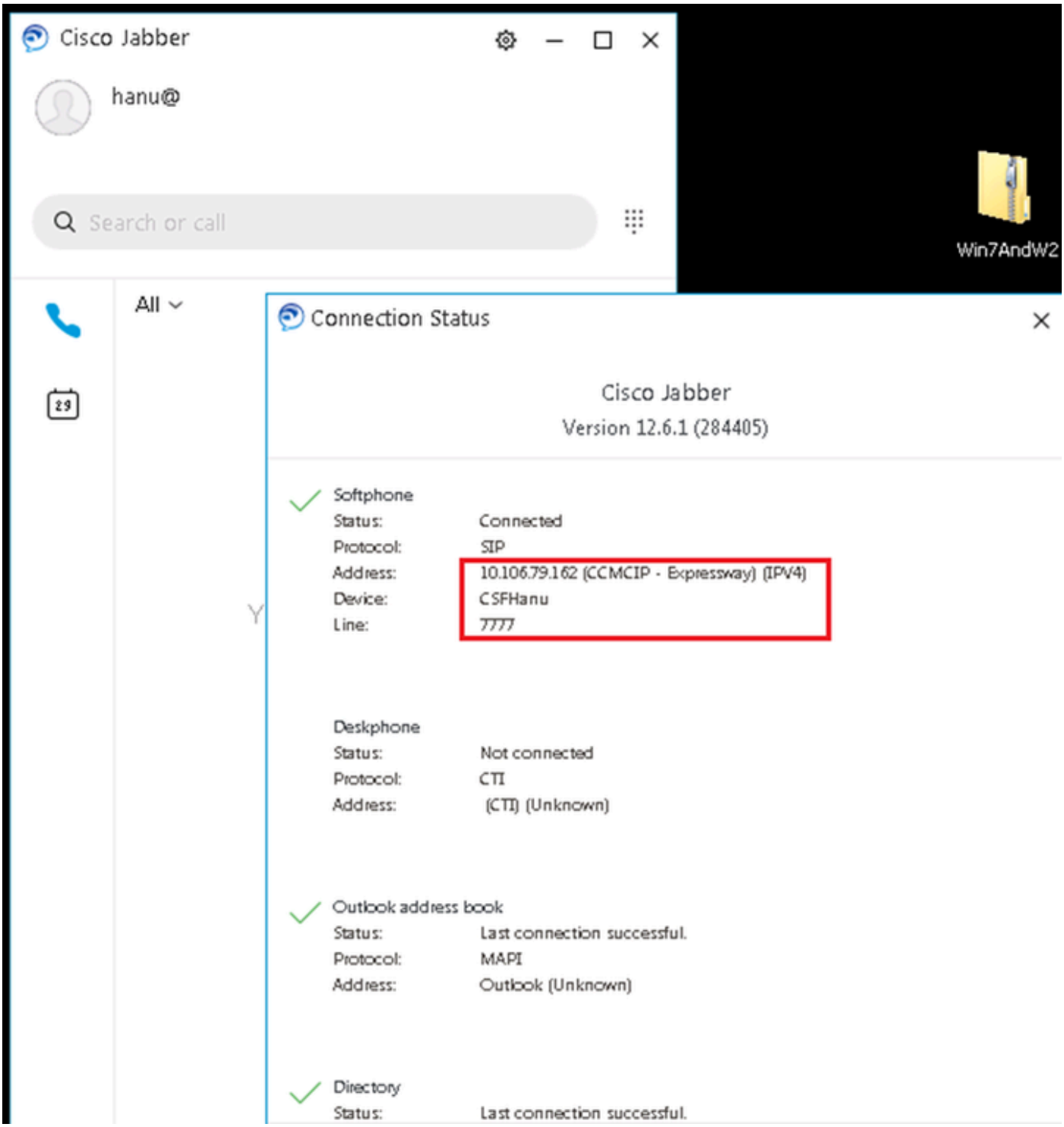


État de la zone MRA Unified Communication Actif :

- Le certificat du client Expressway-Core a l'EKU du serveur et l'EKU du client.
- Le certificat Expressway Core Server comporte uniquement l'EKU du serveur.



Le client MRA se connecte et s'inscrit :

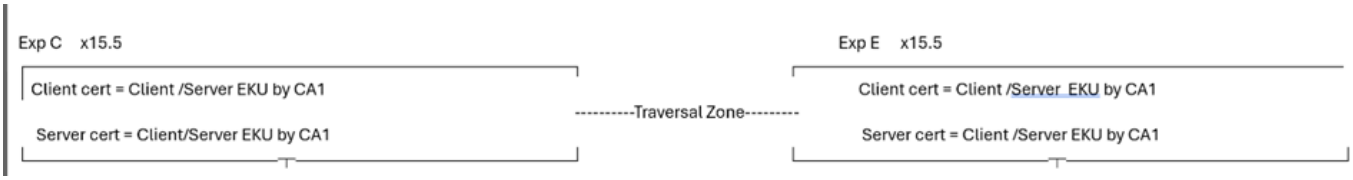


Remarque : Comparer et prendre note des unités EKU présentes dans les certificats pour que MRA et le proxy WebRTC fonctionnent. Il s'agit d'une comparaison entre un déploiement actif et un déploiement inactif.

Condition 3 : Signer tous les certificats avec une autorité de certification privée

CA 1 = CA interne

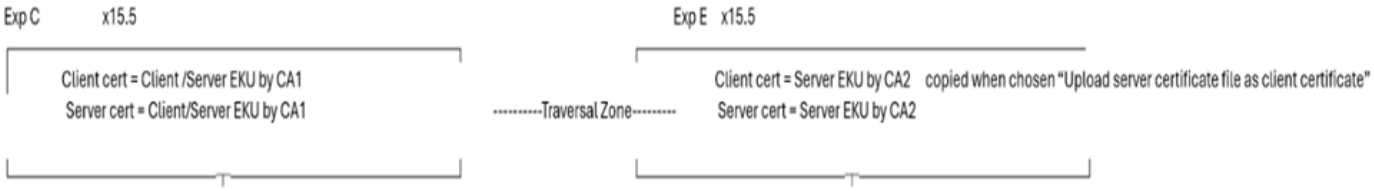
CA 2 = CA publique



Dans la condition 3, tous les certificats sont signés par l'autorité de certification interne (CA1) .

- Lorsque Expressway-E envoie une connexion TLS, la racine/l'intermédiaire CA1 doit être échangée avec l'entité distante. Si l'extrémité distante n'a pas la capacité ou ne permet pas le téléchargement du certificat d'autorité de certification privée, la connexion TLS échoue.
- Les clients MRA obtiennent des certificats pour accepter les fenêtres intempestives si le certificat privé ne se trouve pas dans le magasin d'approbation du système d'exploitation.

Condition 4 : L'Expressway Edge possède des certificats publics avec une clé d'activation de serveur uniquement



Dans la condition 4, les certificats de client et de serveur principaux d'Expressway sont signés par l'autorité de certification interne (CA1) et comportent l'unité EKU du client et du serveur. Le certificat du serveur Expressway E est signé par une autorité de certification publique et ne comporte que l'unité EKU du serveur. Le certificat du serveur est copié dans le magasin de certificats client en choisissant Upload server certificate file as client certificate.

Dans la Condition 4, quand la connexion TLS est faite à l'extrémité distante, si Expressway -E envoie un bonjour client TLS, l'extrémité distante doit désactiver la vérification de l'EKU du client (car le certificat client n'a pas d'EKU d'authentification du client) sinon la connexion TLS échoue.

Il peut y avoir beaucoup plus de conditions ou de scénarios sur le terrain en fonction du déploiement de l'utilisateur et des cas d'utilisation et tous ne peuvent pas être couverts en raison de mon flux de pensée limité. Cependant, les points à retenir sont les suivants :

- # Si Expressway devient un client pendant la connexion TLS, le certificat client est présenté aux homologues.

- #IF Expressway devient serveur pendant la connexion TLS ; le certificat du serveur est présenté à l'homologue.

Ce raisonnement a été établi avec ces scénarios de tests.

Scénario 1

Pour ce scénario, Expressway présente le certificat client lors de la connexion MTLS avec Webex.

Un appel vidéo à une réunion Webex :

Exemple de flux d'appels Jabber -à CUCM -à Exp Core —à Exp Edge —à Webex

10.106.80.31= Périphérie Expressway

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="Envoyé" Local-ip="10.106.80.31" Local-port="25002" Dst-ip="163.129.37.33" Dst-port="5061"

Expressway Edge possède un certificat client portant ce numéro de série (2f0000004c869c77c8981becde00000000004c).

Expressway Edge envoie un Hello client à « Webex » pendant la négociation TLS, puis envoie un certificat client.

Numéro de série 2f0000004c869c77c8981becde00000000004c :

1. Expressway Edge envoie un message Hello client (pkt= 13699) à « Webex » pendant la négociation mTLS.

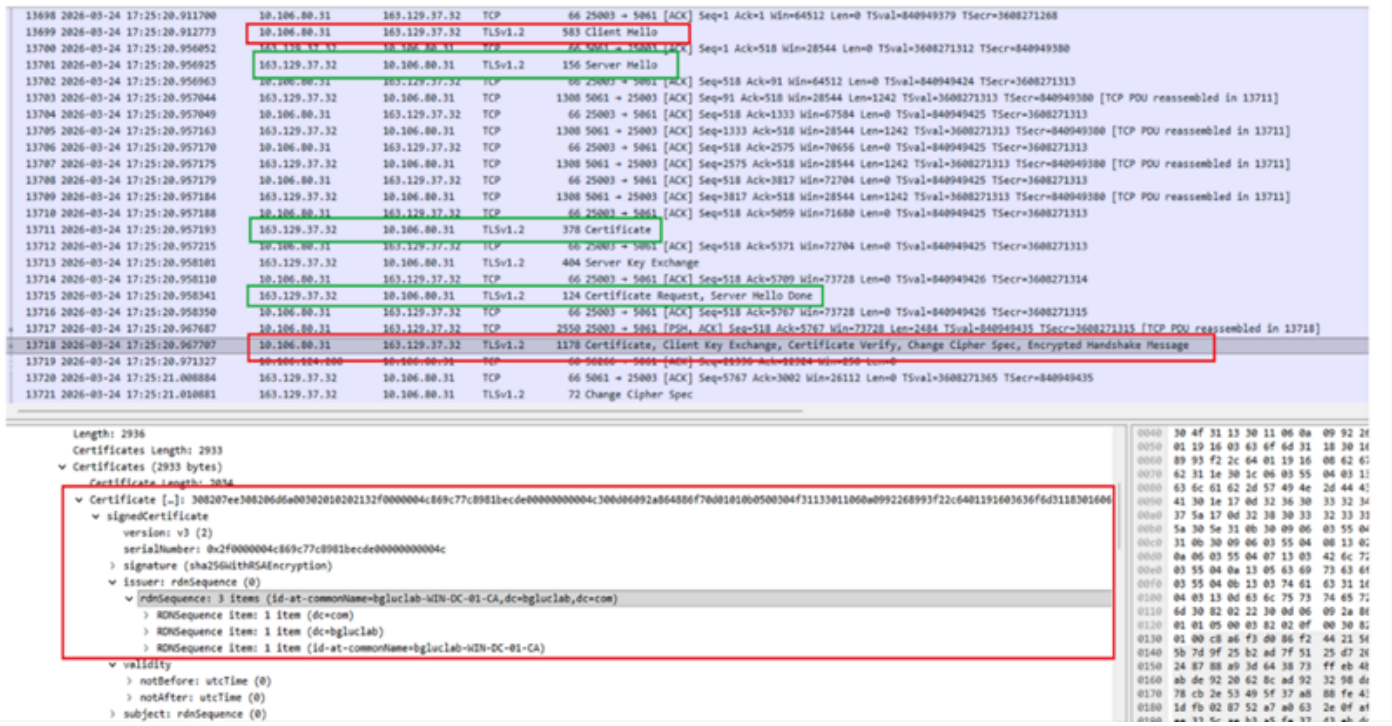
2. Webex envoie un paquet Hello de serveur à Expressway Edge (pkt=13701).

3. Webex envoie son certificat à Expressway Edge (pkt=13711).

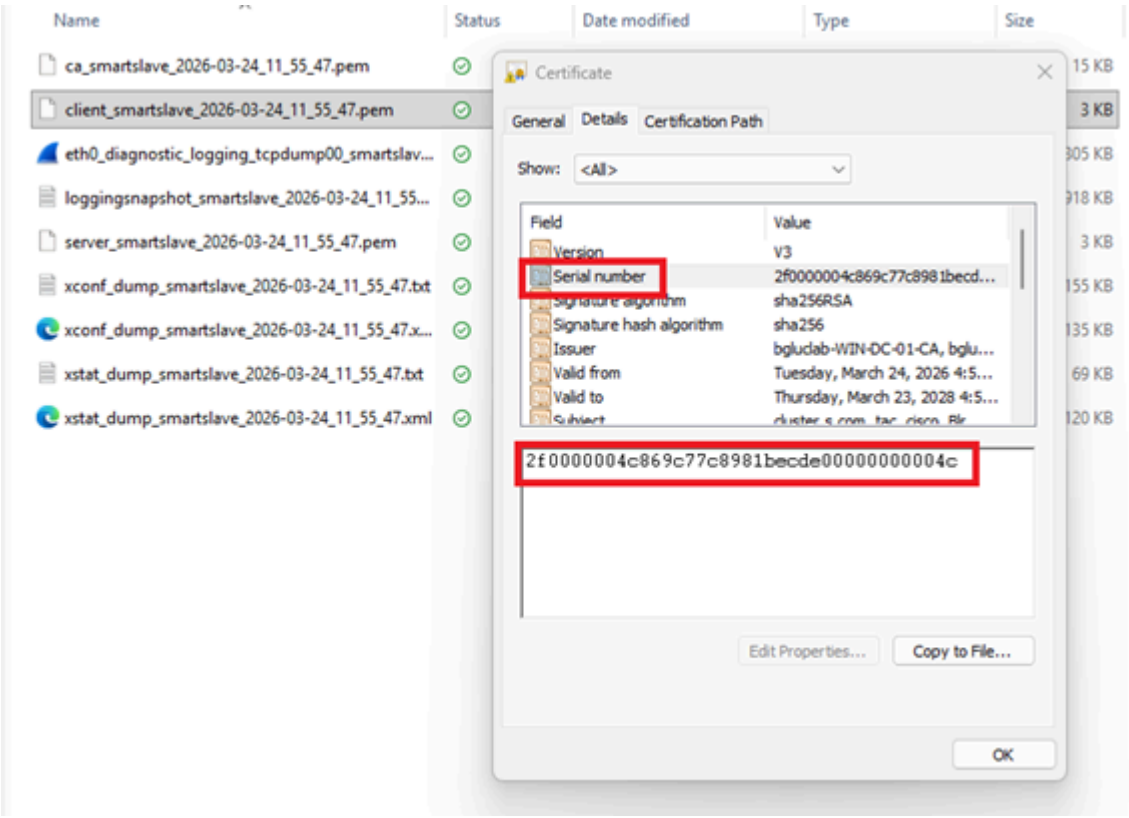
4. Webex demande un certificat de périphérie Expressway « CertificateRequest » (pkt=13715).

5. Expressway Edge envoie son certificat à Webex (pkt=13718).

(capture d’écran)



Certificat client d’Expressway Edge :



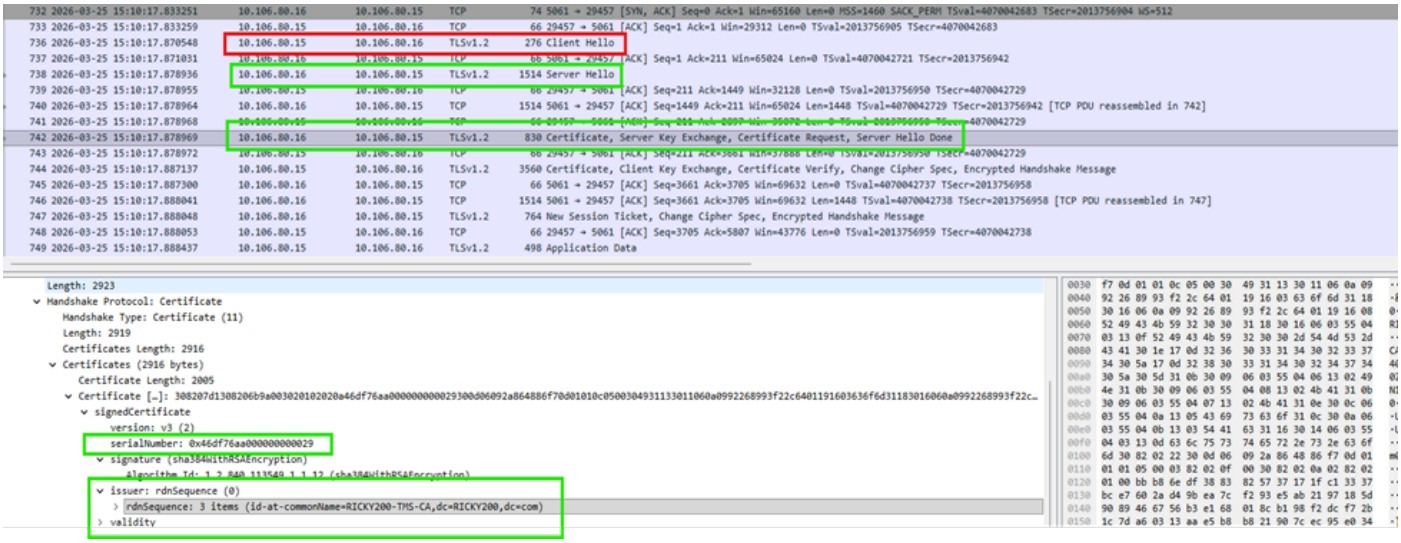
Scénario 2

Expressway devient une entité de serveur lors de la connexion mTLS et présente son certificat de serveur :

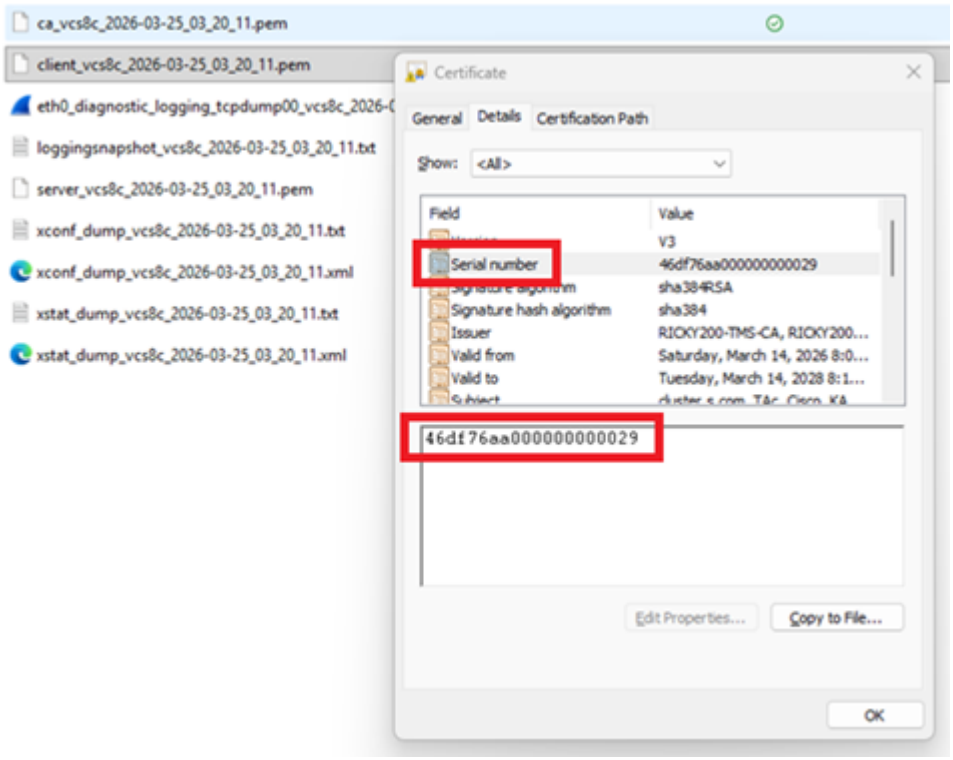
Lorsque Expressway présente un certificat de serveur, Expressway a une zone de voisinage sécurisée sur 5061 avec le nom de vérification ON.

Zone de voisinage sécurisée entre les noeuds Expressway x15.5 et Expressway 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)
```



Cette capture d'écran montre le certificat du serveur comme correspondant au numéro de série :

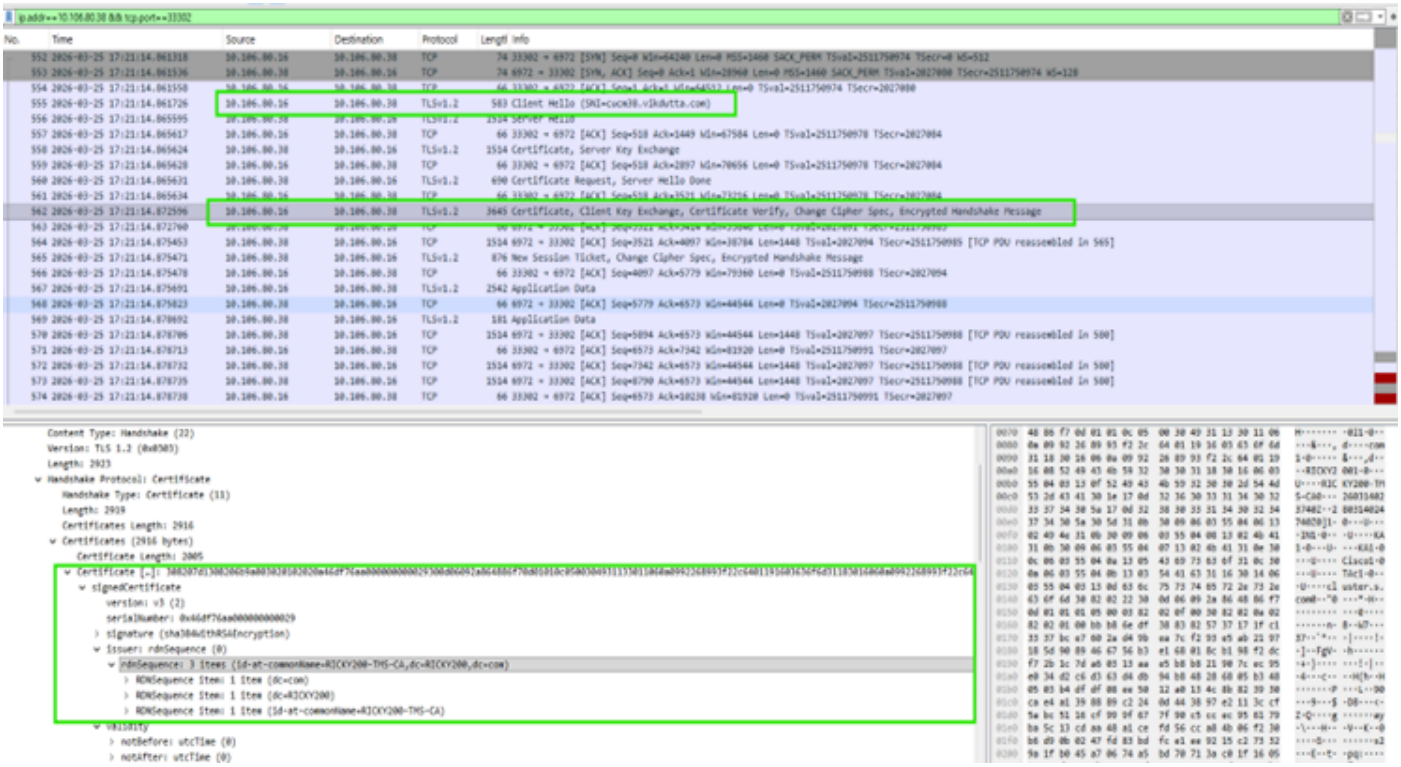


Cas de test 3 : le client MRA est configuré pour la connexion et le workflow inclut la vérification du certificat du serveur de trafic entre Expressway Core et CUCM.

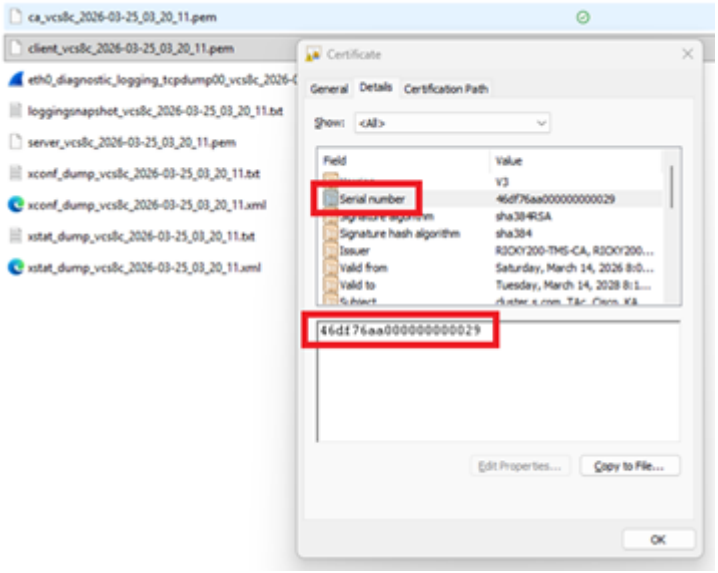
10.106.80.16 = Expressway Core x15.5

10.106.80.38 = CUCM

- L’exp C 16 envoie un hello client sur TFTP 6972.
- Exp C 16 envoie un certificat client pendant la connexion TLS.



Certificat du client principal Expressway :



À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.