Collaboration Edge (MRA)-certificaten configureren en problemen oplossen

Inhoud

Inleiding

In dit document worden certificaten beschreven met betrekking tot MRA-implementaties (Mobile Remote Access).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Publiek vs. Private certificaatautoriteit (CA)

Er zijn een aantal opties om certificaten op de servers van Expressway-C en E te ondertekenen. U kunt ervoor kiezen om de certificaatondertekeningsaanvraag (CSR) te laten ondertekenen door een openbare CA zoals GoDaddy, Verisign of anderen, of u kunt deze intern ondertekenen als u uw eigen certificeringsinstantie gebruikt (kan zelfondertekend worden met OpenSSL of een interne onderneming CA zoals een Microsoft Windows-server). Raadpleeg de Gids voor het maken van certificaten voor de Video Communication Server (VCS) voor meer informatie over het maken en ondertekenen van de door een van deze methoden gebruikte CSRâ€™s.

De enige server die echt vereist is om te worden ondertekend door een openbare CA is de Expressway-E. Dit is de enige server waar de klanten het certificaat zien wanneer ze inloggen via MRA, daarom gebruik een openbare CA om ervoor te zorgen dat gebruikers het certificaat niet handmatig moeten accepteren. De Expressway-E kan werken met een intern CA-ondertekend certificaat, maar de eerste gebruikers worden gevraagd om het onbetrouwbare certificaat te accepteren. MRA registratie van 7800 en 8800 Series telefoons zou niet werken met interne certificaten omdat hun certificaat vertrouwenslijst niet kan worden gewijzigd. Voor de eenvoud wordt voorgesteld dat uw Expressway-C en Expressway-E certificaten beide worden ondertekend door dezelfde CA; dit is echter geen vereiste zolang u de vertrouwde CA-lijsten op beide servers correct hebt geconfigureerd.

Hoe certificaat ketens werken

Certificaten zijn gekoppeld in een keten van twee of meer die worden gebruikt om de bron te verifiëren die het certificaat van de server heeft ondertekend. Er zijn drie soorten certificaten in een keten; het client/server certificaat, tussenliggend certificaat (in sommige gevallen) en het wortelcertificaat (ook wel aangeduid als de wortel CA als dit de hoogste autoriteit op het niveau is die het certificaat heeft ondertekend).

Certificaten bevatten twee primaire velden die de keten opbouwen: het onderwerp en de emittent.

Het onderwerp is de naam van de server of de autoriteit die dit certificaat vertegenwoordigt. In het geval van een Expressway-C of Expressway-E (of andere Unified Communications (UC)-apparaten), is dit gemaakt van de Fully Qualified Domain Name (FQDN).

De uitgevende instelling is de autoriteit die dat specifieke certificaat heeft gevalideerd. Aangezien iedereen een certificaat kan ondertekenen (dat de server omvat die het certificaat heeft gemaakt, om te beginnen ook bekend als zelfondertekende certificaten), hebben servers en clients een lijst van emittenten of CA's die zij als authentiek vertrouwen.

Een certificaatketen eindigt altijd met een zelfondertekend top-level of root certificaat. Aangezien u zich door de certificaathiërarchie beweegt, heeft elk certificaat een verschillende uitgever met betrekking tot het onderwerp. Uiteindelijk, zou u de wortel CA tegenkomen waar het onderwerp en de emittent aanpassen. Dit geeft aan dat het het top-level certificaat is en dus het certificaat dat moet worden vertrouwd door een client of server's vertrouwde CA-lijst.

SSL Handshake Samenvatting

In het geval van de transversale zone fungeert de Expressway-C altijd als client, terwijl de Expressway-E altijd de server is. De vereenvoudigde uitwisseling werkt zoals getoond:

Expressway-C Expressway-E

---------Client Hallo-------->

<--------Server Hallo---------

<----servercertificaat-------

<----certificaataanvraagâ€”

------Clientcertificaat------>

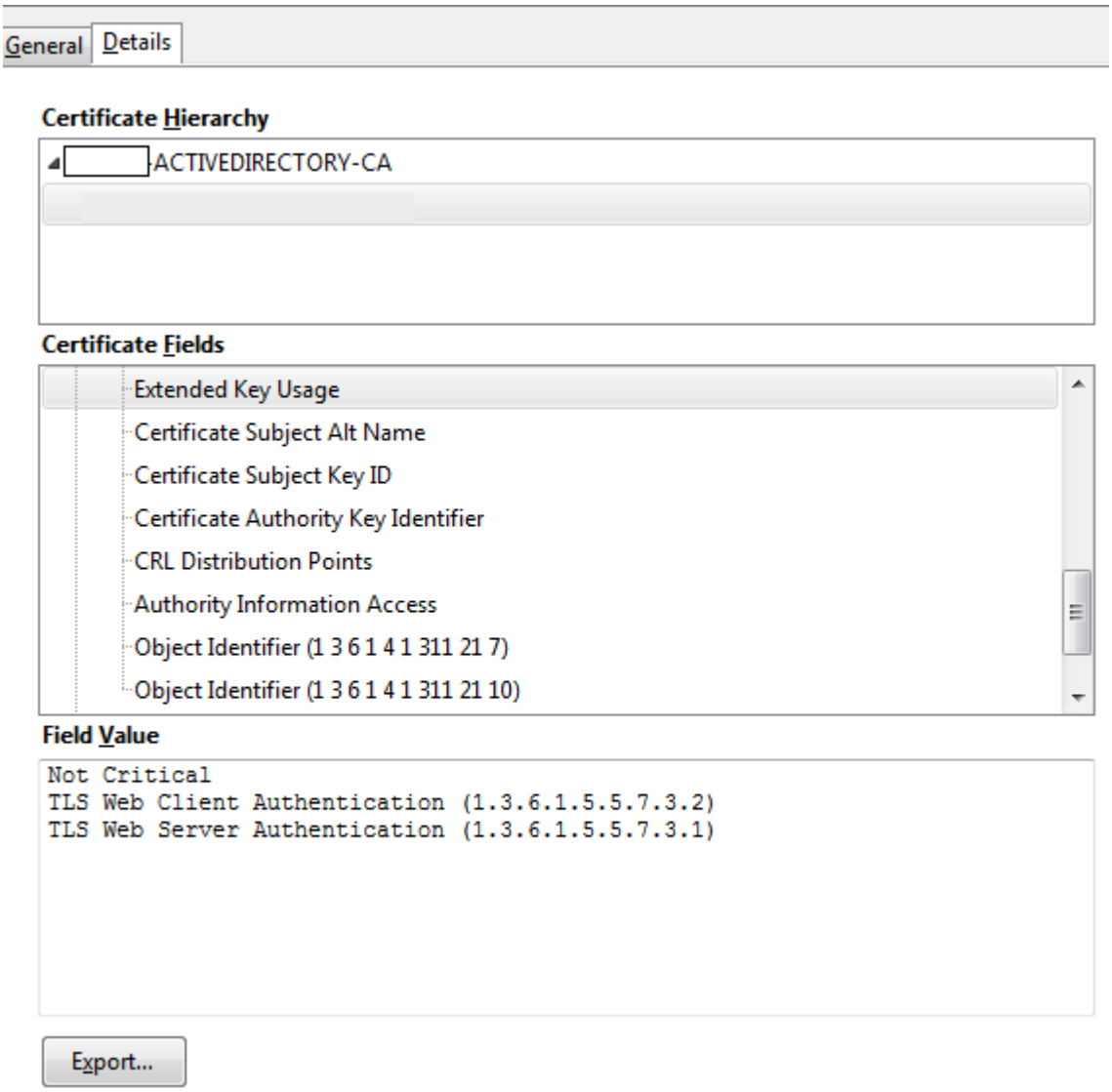
De sleutel ligt in de uitwisseling, omdat de Expressway-C altijd de verbinding initieert, en dus altijd de klant is. De Expressway-E is de eerste die zijn certificaat verstuurt. Als Expressway-C dit certificaat niet kan valideren, wordt de handdruk afgebroken en kan de Expressway-E geen eigen handdruk krijgen.

Een ander belangrijk punt om nota te nemen van is de webclientverificatie van Transport Layer Security (TLS) en de verificatiekenmerken van de TLS-webserver op certificaten. Deze kenmerken worden bepaald op de CA die de CSR heeft ondertekend (als een Windows CA wordt gebruikt, wordt dit bepaald door de geselecteerde sjabloon) en geeft aan of het certificaat geldig is in de rol van de client of de server (of beide). Omdat voor een VCS of Expressway, het kan worden gebaseerd op de situatie (het is altijd hetzelfde voor een traversale zone), en het certificaat moet zowel client- als serverauthenticatie eigenschappen hebben.

Expressway-C en Expressway-E geven een fout bij het uploaden naar een nieuw servercertificaat, als beide niet worden toegepast.

Als u niet zeker weet of een certificaat deze kenmerken heeft, kunt u de certificaatgegevens openen in een browser of in uw besturingssysteem en de sectie Uitgebreid sleutelgebruik (zie de afbeelding) controleren. Het formaat kan variëren en hangt af van hoe u het certificaat bekijkt.

Voorbeeld:



Configureren

Expressway-C en Expressway-E Traversal Zone / Trust

CSRâ€™s genereren en ondertekenen

Zoals eerder beschreven, moeten de Expressway-C- en Expressway-E-certificaten worden ondertekend door een interne of externe CA of door OpenSSL voor zelfondertekening.

> **Opmerking**: u kunt het tijdelijke certificaat dat op de Expressway-server staat niet gebruiken, omdat het niet wordt ondersteund. Als u wildcard-certificaten gebruikt waar u een CA-tekencertificaat hebt en de onderwerpregel niet specifiek is gedefinieerd, wordt deze niet ondersteund.

De eerste stap is het genereren van de MVO en het laten ondertekenen door het voorkeurstype van CA. Het proces hiervoor wordt specifiek beschreven in de Gids voor het maken van certificaten. Tijdens het creëren van MVO, is het belangrijk om in gedachten te houden de noodzakelijke Onderwerp Alternatieve Namen (SAN's) die moeten worden opgenomen in de certificaten. Dit wordt ook vermeld in de certificaatgids en de Mobiele Gids van de Plaatsing van de Toegang van de Verre. Controleer de meest recente versies van de gids aangezien meer kan worden toegevoegd aangezien de nieuwe eigenschappen aankomen. Lijst van veelvoorkomende SANâ€™s die moeten worden opgenomen op basis van de gebruikte functies:

Autoweg-C

- Alle (interne of externe) domeinen die aan de lijst met domeinen worden toegevoegd.
- Alle blijvende chat-nodealiassen als XMPP-federatie wordt gebruikt.
- Beveiligde apparaatprofielnamen op CUCM indien beveiligde apparaatprofielen worden gebruikt.

autoweg-E

- Alle domeinen die zijn geconfigureerd op de snelweg-C.
- Alle blijvende chat-nodealiassen als XMPP-federatie wordt gebruikt.
- Alle domeinen die geadverteerd worden voor XMPP federaties.

Opmerking: als het basisdomein dat wordt gebruikt voor de zoekacties voor externe servicerecords (SRV) niet als SAN is opgenomen in het Expressway-E-certificaat (xxx.com of collab-edge.xxx.com), moeten de Jabber-clients nog steeds van de eindgebruiker eisen dat hij het certificaat voor de eerste verbinding accepteert en kunnen TC-endpoints helemaal geen verbinding maken.

Configureer expressway-C en expressway-E om elkaar te vertrouwen

Opdat de Unified Communications-zone een verbinding tot stand kan brengen, moeten Expressway-C en Expressway-E elkaars certificaten vertrouwen. Dit bijvoorbeeld veronderstelt dat het Expressway-E certificaat is ondertekend door een openbare CA die deze hiërarchie gebruikt.

Certificaat 3

Emittent: GoDaddy Root CA

Betreft: GoDaddy Root CA

Certificaat 2

Emittent: GoDaddy Root CA

Betreft: Intermediaire autoriteit voor GoDaddy

Certificaat 1

Emittent: GoDaddy Intermediate Authority

Betreft: Expressway-E.lab

De Expressway-C moet worden geconfigureerd met vertrouwenscertificaat 1. In de meeste gevallen, gebaseerd op de vertrouwde certificaten die op de server worden toegepast, verstuurt het alleen het laagste niveau servercertificaat. Dat betekent dat voor de Expressway-C om certificaat 1 te vertrouwen, u zowel certificaten 2 als 3 moet uploaden naar de vertrouwde CA-lijst van Expressway-C (**Onderhoud> Beveiliging > Betrouwbare CA-lijst**). Als u het tussencertificaat 2 weglaat wanneer de Expressway-C het Expressway-E certificaat ontvangt, kan het geen manier hebben om het te verbinden met de vertrouwde GoDaddy Root CA, daarom zou het worden afgewezen.

Certificaat 3

Emittent: GoDaddy Root CA

Betreft: GoDaddy Root CA

Certificaat 1

Emittent: GoDaddy Intermediate Authority - Niet vertrouwd!

Betreft: Expressway-E.lab

Bovendien, als u alleen het tussenliggende certificaat zonder de wortel naar de vertrouwde CA-lijst van de Expressway-C uploadt, zou het zien dat de GoDaddy Intermediate Authority wordt vertrouwd, maar het wordt ondertekend door een hogere autoriteit, in dit geval, GoDaddy Root CA die niet wordt vertrouwd, daarom zou het falen.

Certificaat 2

Emittent: GoDaddy Root CA - Niet vertrouwd!

Betreft: Intermediaire autoriteit voor GoDaddy

Certificaat 1

Emittent: GoDaddy Intermediate Authority

Betreft: Expressway-E.lab

Met alle tussenproducten en de wortel toegevoegd aan de vertrouwde CA-lijst, kan het certificaat worden geverifieerd...

Certificaat 3

Uitgever: GoDaddy Root CA - Zelfondertekend top-level certificaat wordt vertrouwd en ketting compleet!

Betreft: GoDaddy Root CA

Certificaat 2

Emittent: GoDaddy Root CA

Betreft: Intermediaire autoriteit voor GoDaddy

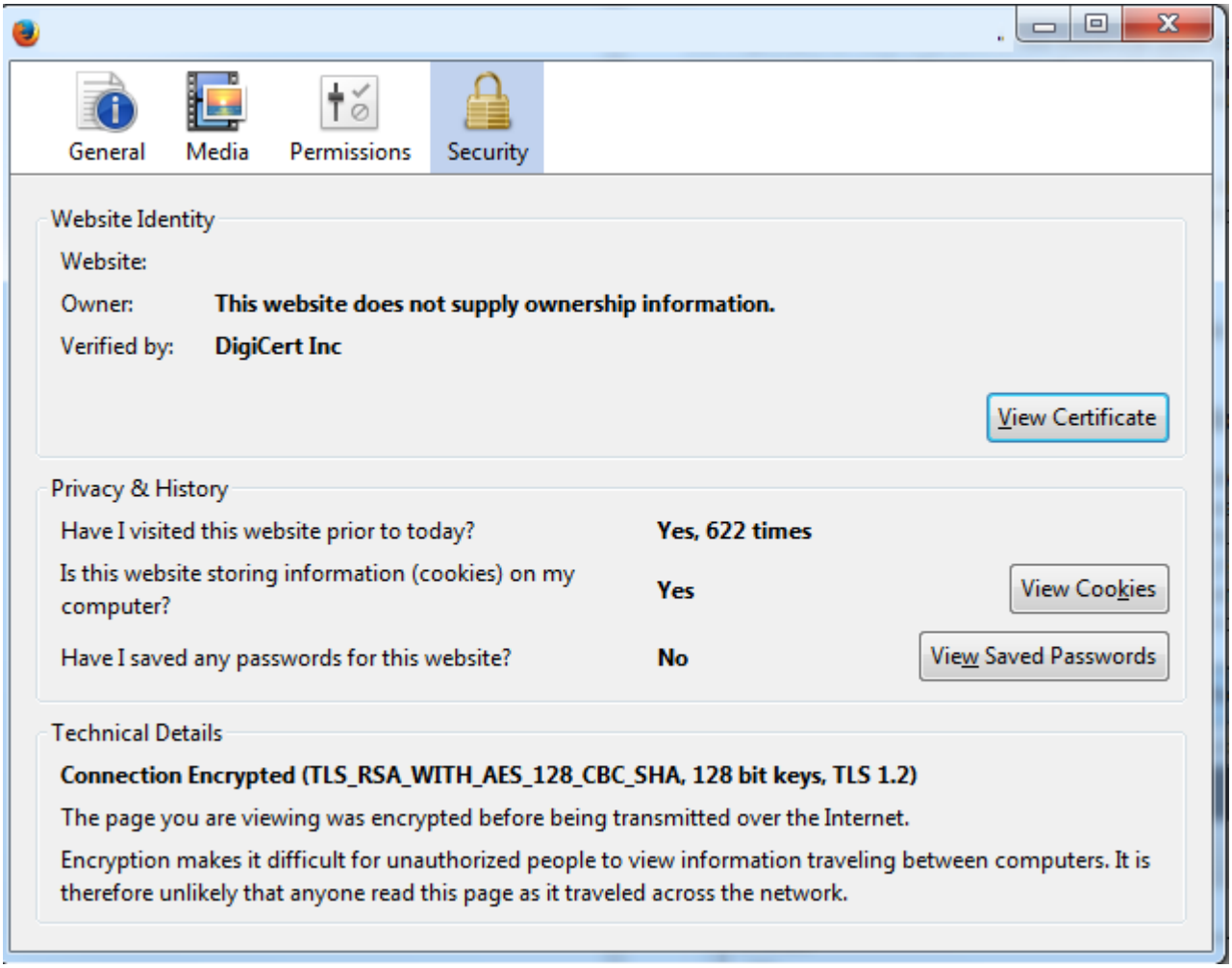
Certificaat 1

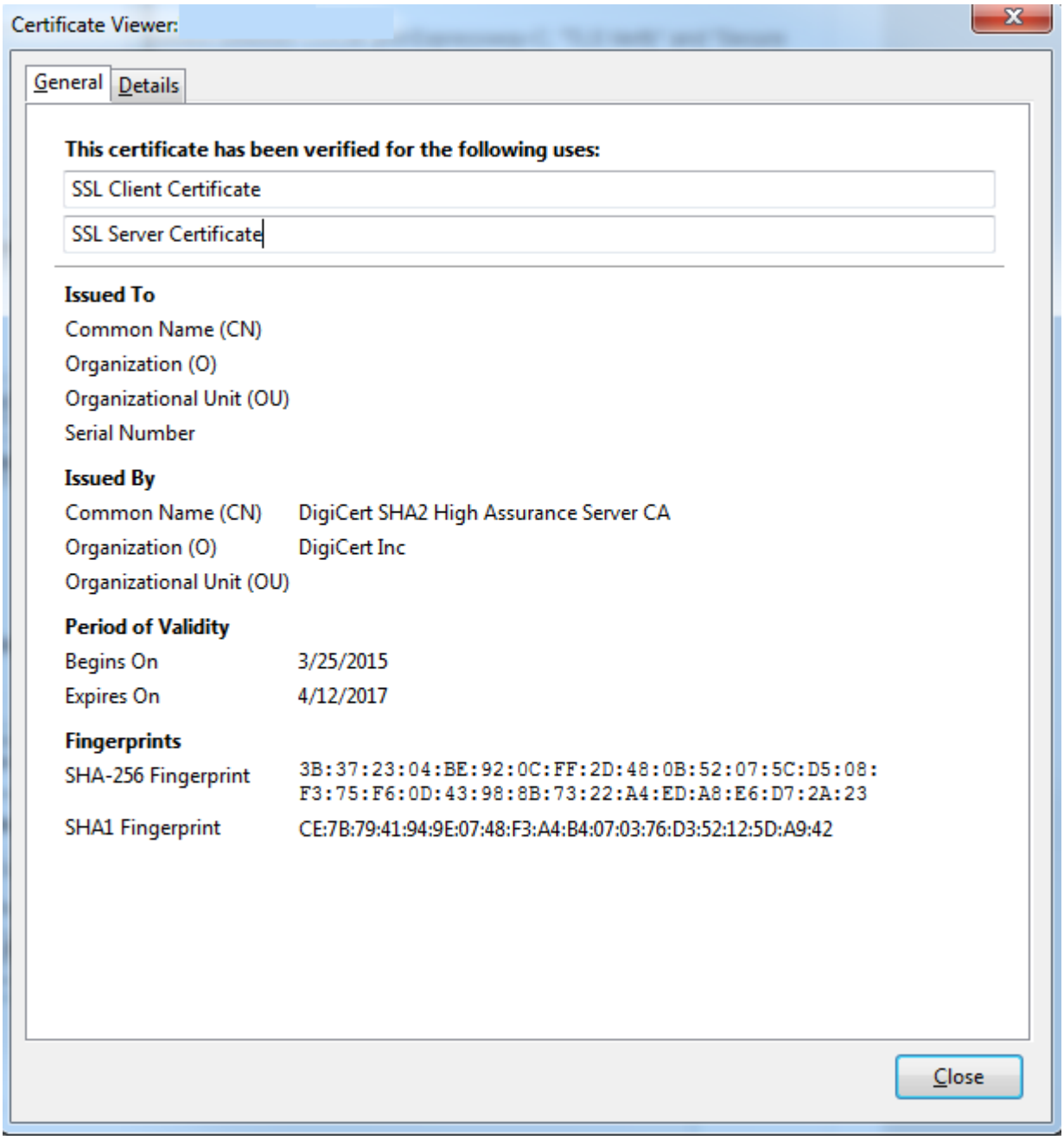
Emittent: GoDaddy Intermediate Authority

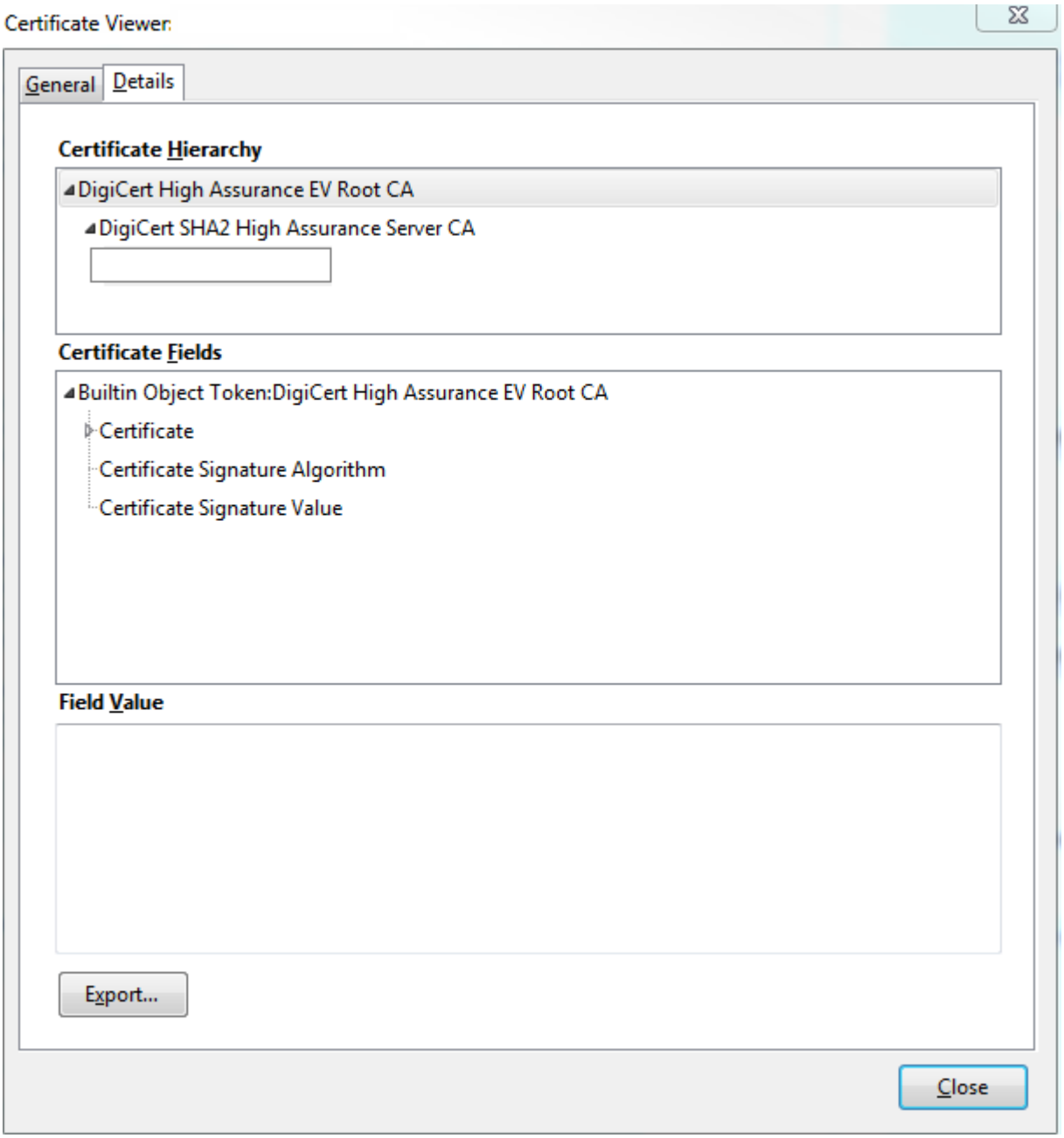
Betreft: Expressway-E.lab

Als u niet zeker weet wat de certificaatketting is, kunt u uw browser controleren wanneer u bent aangemeld in de webinterface van de specifieke Expressway. Het proces varieert enigszins op basis van uw browser, maar in Firefox, kunt u op het slotpictogram links van de adresbalk klikken. Klik vervolgens in het pop-upvenster op **Meer informatie > Certificaat bekijken > Details**. Als uw browser de volledige keten kan samenvoegen, kunt u de keten van boven naar onder zien. Indien het certificaat van het hoogste niveau geen onderwerp en emittent heeft die overeenkomen, betekent dit dat de keten niet is voltooid. U kunt elk certificaat in de keten ook zelf exporteren als u op **exporteren** klikt met het gewenste certificaat

gemarkeerd. Dit is handig als u niet 100% zeker bent dat u de juiste certificaten geüpload naar de CA vertrouwenslijst.




Certificate Viewer:
General
Details
This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate
Issued To
Common Name (CN)
Organization (O)
Organizational Unit (OU)
Serial Number
Issued By
Common Name (CN) DigiCert SHA2 High Assurance Server CA
Organization (O) DigiCert Inc
Organizational Unit (OU)
Period of Validity
Begins On 3/25/2015
Expires On 4/12/2017
Fingerprints
SHA-256 Fingerprint 3B:37:23:04:BE:92:0C:FF:2D:48:0B:52:07:5C:D5:08:
F3:75:F6:0D:43:98:8B:73:22:A4:ED:A8:E6:D7:2A:23
SHA1 Fingerprint CE:7B:79:41:94:9E:07:48:F3:A4:B4:07:03:76:D3:52:12:5D:A9:42
Close



Nu de Expressway-C het certificaat van de Expressway-E vertrouwt, zorg ervoor dat het in de tegenovergestelde richting werkt. Als het certificaat Expressway-C wordt ondertekend door dezelfde CA die de Expressway-E heeft ondertekend, is het proces eenvoudig. Upload dezelfde certificaten naar de Trusted CA-lijst op Expressway-E als u al deed met de C. Als de C is ondertekend door een andere CA, moet u hetzelfde proces gebruiken als in de afbeelding, maar gebruik in plaats daarvan de keten de ondertekende Expressway-C certificaat.

Beveiligde communicatie tussen Cisco Unified Communications Manager (CUCM) en Expressway-C

Overzicht

In tegenstelling tot de transversale zone tussen Expressway-C en Expressway-E is beveiligde signalering NIET vereist tussen Expressway-C en CUCM. Tenzij dit niet is toegestaan door het interne beveiligingsbeleid, moet u altijd MRA configureren om eerst te werken met niet-beveiligde apparaatprofielen op CUCM om te bevestigen dat de rest van de implementatie correct is voordat u doorgaat met deze stap.

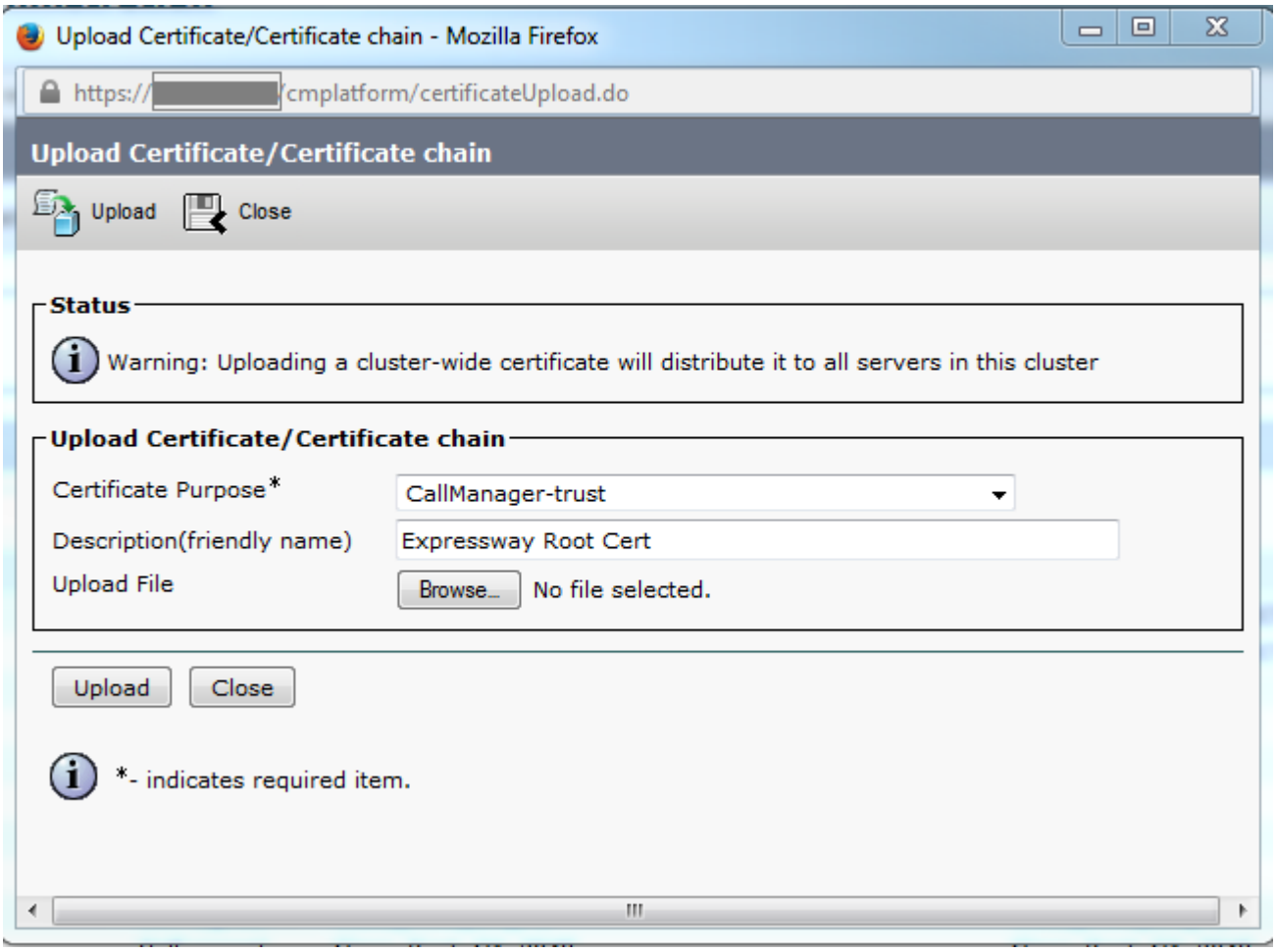
Er zijn twee belangrijke beveiligingsfuncties die kunnen worden ingeschakeld tussen CUCM en Expressway-C; TLS verify en beveiligde apparaatregistraties. Er is een belangrijk onderscheid tussen deze twee omdat ze twee verschillende certificaten van de CUCM kant in de SSL handdruk gebruiken.

TLS verify - tomatecertificaat

Secure SIP-registraties - CallManager-certificaat

Configuratie van vertrouwen tussen CUCM en Expressway-C

Het concept is in dit geval precies hetzelfde als tussen Expressway-C en Expressway-E. De CUCM moet eerst vertrouwen op het servercertificaat van Expressway-C. Dat betekent dat op de CUCM de tussenproducten en basiscertificaten van de Expressway-C moeten worden geüpload als tomcat-trust certificaat voor de TLS verify-functie en een CallManager-trust voor beveiligde apparaatregistraties. Om dit te bereiken, navigeer je naar **Cisco Unified OS Administration** in de rechterbovenhoek van de CUCM web GUI, en vervolgens naar **Security> Certificate Management**. Hier kunt u op **Upload Certificate/Certificate Chain** klikken en het juiste vertrouwensformaat selecteren of op **Find** klikken om de lijst met geüploade certificaten te zien.

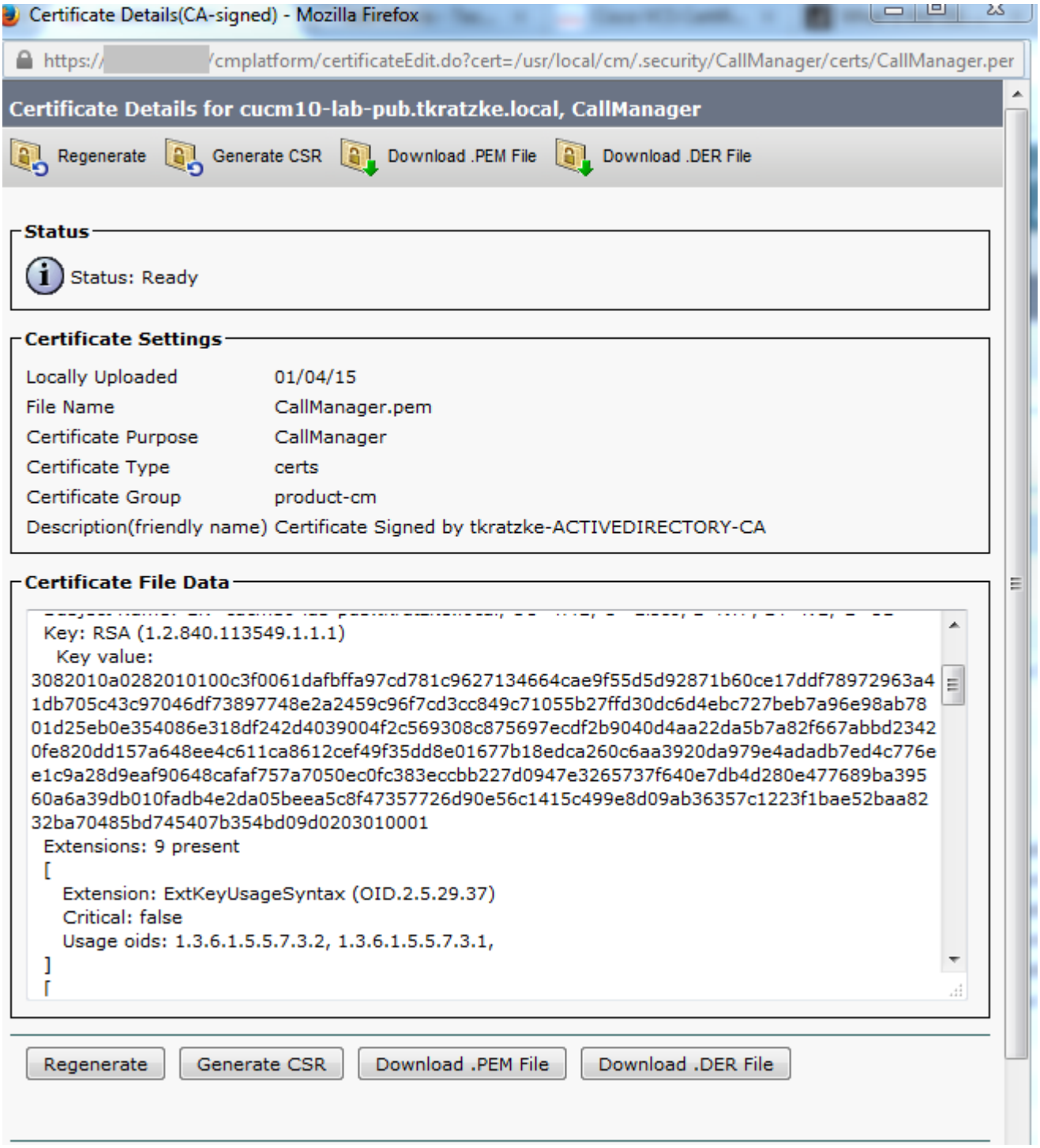


U moet ervoor zorgen dat de Expressway-C vertrouwt op de CA die de CUCM-certificaten heeft ondertekend. Dit kan worden bereikt als u ze toevoegt aan de vertrouwde CA-lijst. In bijna alle gevallen, als u de CUCM-certificaten met een CA ondertekende, moeten de Tomcat- en CallManager-certificaten door dezelfde CA worden ondertekend. Als ze anders zijn, moet u op beide vertrouwen als u TLS verify en beveiligde registraties gebruikt.

Voor beveiligde SIP-registraties moet u er ook voor zorgen dat de naam van het beveiligde apparaatprofiel op de CUCM die op het apparaat wordt toegepast, op het Expressway-C-certificaat als een SAN wordt

vermeld. Als dit niet de beveiligde register berichten bevat, zou het falen met een 403 van de CUCM, wat wijst op een TLS-fout.

Opmerking: Wanneer de SSL-handdruk plaatsvindt tussen de CUCM en Expressway-C voor een beveiligde SIP-registratie, vinden twee handdrukken plaats. Eerst, doet Expressway-C dienst als de cliënt en initieert de verbinding met de CUCM. Zodra dat met succes is voltooid, initieert de CUCM een andere handdruk als client om te antwoorden. Dit betekent dat het CallManager-certificaat op CUCM, net als de Expressway-C, zowel de TLS-webclient- als de TLS-webserververificatiekenmerken moet hebben toegepast. Het verschil is dat de CUCM toestaat dat deze certificaten worden geüpload zonder beide, en de interne beveiligde registraties zouden prima werken als de CUCM alleen de server authenticatie attributen heeft. U kunt dit bevestigen op CUCM als u zoekt naar het CallManager-certificaat in de lijst en het selecteert. Hier kunt u de gebruiksmodi bekijken onder de sectie Extension. Voor de clientverificatie zie 1.3.6.1.5.5.7.3.2 en voor de serververificatie zie 1.3.6.1.5.5.7.3.1. U kunt het certificaat ook downloaden vanuit dit venster.



Opmerking: de vertrouwenscertificaten die worden toegepast op de uitgever in een cluster moeten worden gerepliceerd naar de abonnees. Het is goed om te bevestigen door afzonderlijk in te loggen op een nieuwe configuratie.

Opmerking: Om ervoor te zorgen dat de Expressway-C het certificaat van CUCM goed kan valideren, MOETEN de CUCM-servers worden toegevoegd in de Expressway-C met de FQDN, niet met het IP-adres. De enige manier waarop het IP-adres kan werken is als het IP van elke CUCM-knooppunt in het certificaat wordt toegevoegd als een SAN, wat bijna nooit gebeurt.

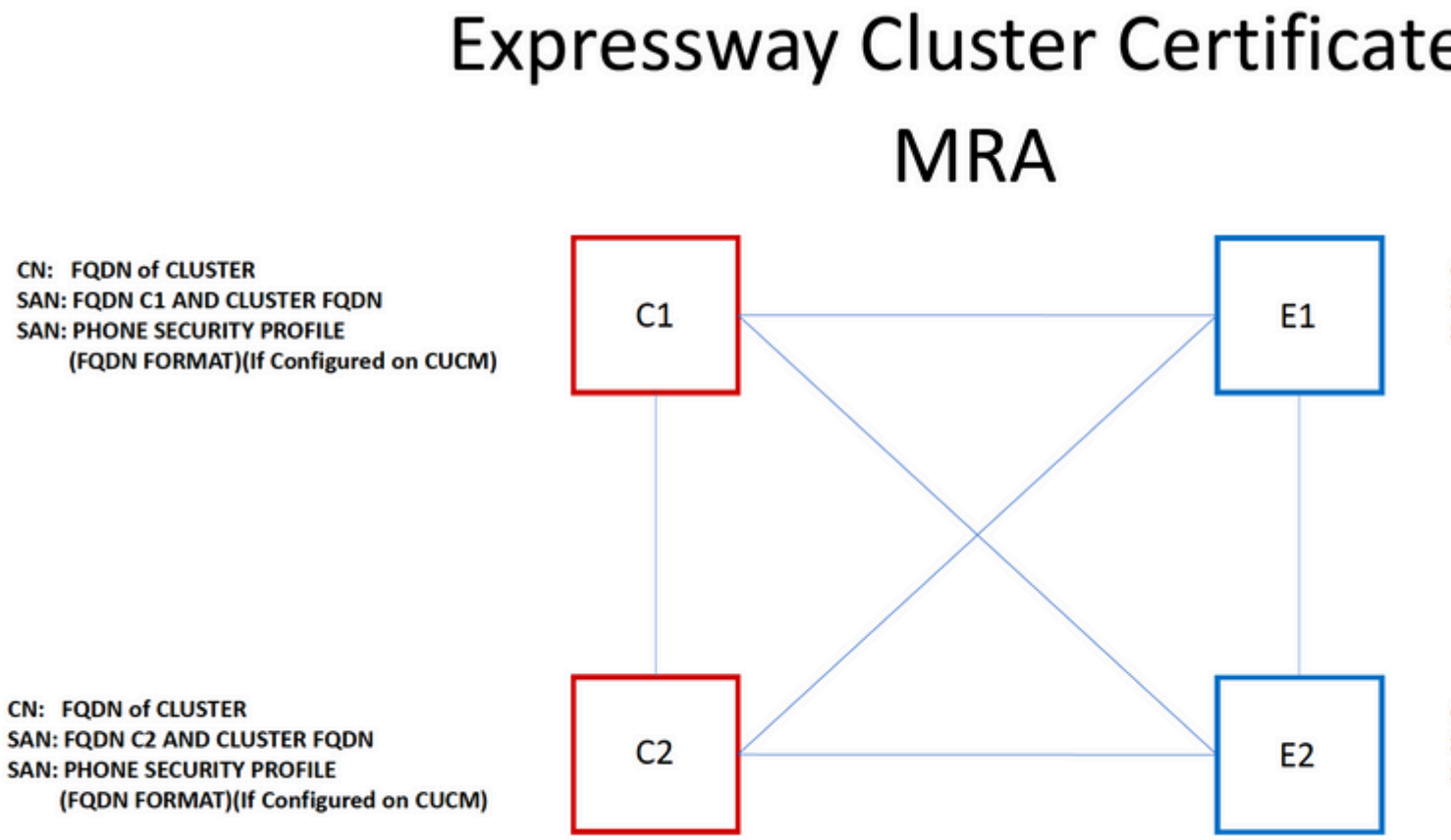
CUCM-servers met zelfondertekende certificaten

Standaard wordt een CUCM-server geleverd met zelfondertekende certificaten. Als deze zijn geïnstalleerd, is het niet mogelijk om zowel TLS verify als beveiligde apparaatregistraties tegelijkertijd te gebruiken. Beide functies kunnen op zichzelf worden gebruikt, maar omdat de certificaten zelf zijn ondertekend, betekent dit dat zowel de zelf-ondertekende Tomcat- als de zelf-ondertekende CallManager-certificaten moeten worden geüpload naar de vertrouwde CA-lijst op de Expressway-C. Wanneer Expressway-C zijn vertrouwenslijst doorzoekt om een certificaat te valideren, stopt het zodra het een met een onderwerp vindt dat overeenkomt. Vanwege dit, welke hoger is op de vertrouwenslijst, tomcat of CallManager, zou die functie werken. Het onderste zou mislukken alsof het niet aanwezig was. De oplossing hiervoor is om uw CUCM-certificaten te ondertekenen met een CA (publiek of privaat) en die CA alleen te vertrouwen.

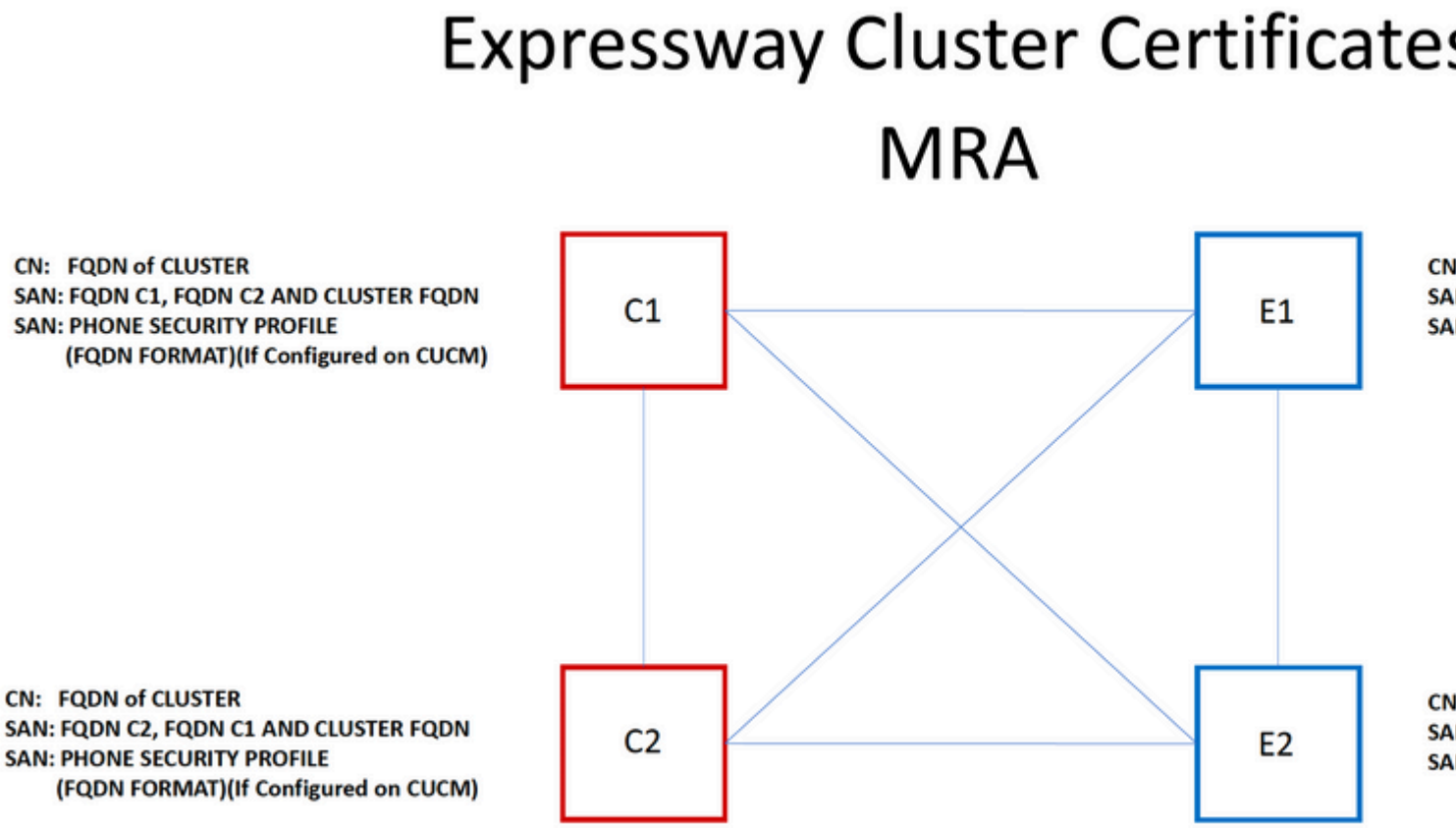
Overwegingen bij Expressway-C en Expressway-E Cluster

Clustercertificaten

Het is sterk aanbevolen dat als u een cluster van Expressway-C of Expressway-E servers voor redundantie hebt dat u een afzonderlijke CSR voor elke server genereert en deze door een CA laten ondertekenen. In het vorige scenario zou de Common Name (CN) van elk peers-certificaat hetzelfde cluster Fully Qualified Domain Name (FQDN) zijn en zouden de SANâ€™s de cluster FQDN en de respectieve peers FQDN zijn zoals in de afbeelding:



Het is mogelijk voor u om de cluster FQDN als de CN en elke peers FQDN en de cluster FQDN in het SAN te gebruiken om hetzelfde certificaat te gebruiken voor alle knooppunten in het cluster, en daarom de kosten van meerdere certificaten te vermijden die door een openbare CA zijn ondertekend.



> **Opmerking**: de namen van het beveiligingsprofiel voor de telefoon op het certificaat van CS zijn alleen vereist als u de beveiligingsprofielen voor de beveiligde telefoon op de UCM gebruikt. Het externe domein of collab-edge.example.com (waar example.com uw domein is) is een vereiste alleen voor IP-telefoon en TC-endpointregistratie via MRA. Dit is optioneel voor Jabber registratie via MRA. Als niet aanwezig, dan zal jabber vragen om het certificaat te accepteren wanneer jabber inlogt via MRA.

Indien absoluut noodzakelijk, kan dit worden gedaan met het volgende proces of u kunt OpenSSL gebruiken om zowel de privé-sleutel als CSR handmatig te genereren:

Stap 1. Genereer een MVO op de primaire van het cluster en vorm het om de cluster-alias op te nemen als de GN. Voeg alle peers in het cluster toe als alternatieve namen, samen met alle andere vereiste SANâ€™s.

Stap 2. Onderteken dit MVO en upload het naar de primaire peer.

Stap 3. Log in in de primaire als root en download de private sleutel gelegen in /Tandberg/persistent/certs.

Stap 4. Upload zowel het ondertekende certificaat als de overeenkomende privésleutel naar elkaar peer in het cluster.

> **Opmerking**: dit wordt om de volgende redenen niet aanbevolen:
> 1. Het is een beveiligingsrisico omdat alle peers dezelfde privésleutel gebruiken. Als men op de een of andere manier gecompromitteerd is, kan een aanvaller verkeer van om het even welke servers ontcijferen.
> 2. Als het certificaat moet worden gewijzigd, moet dit hele proces opnieuw worden gevolgd in plaats

---

van een eenvoudige MVO-generatie en -ondertekening.

Vertrouwde CA-lijsten

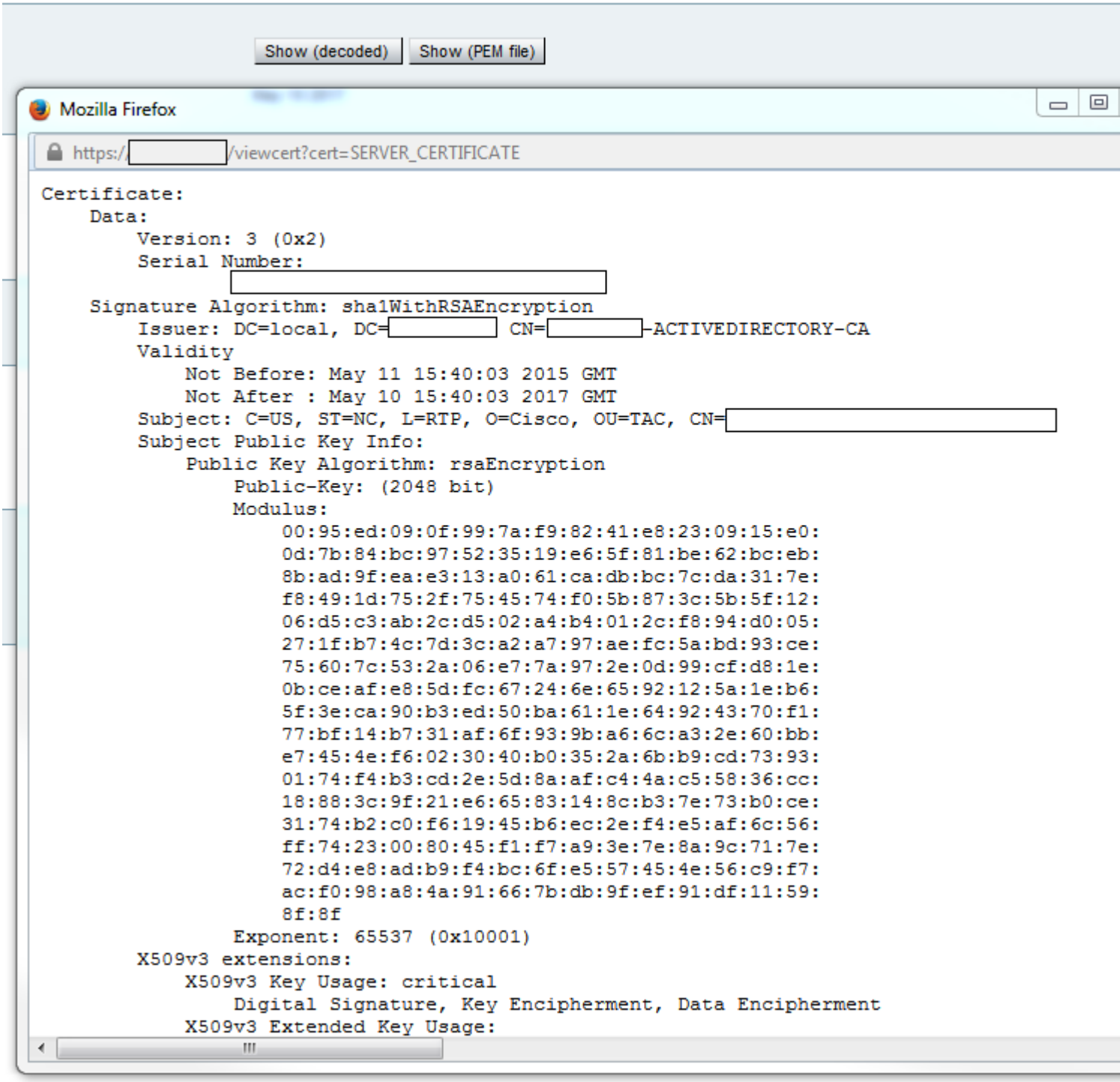
In tegenstelling tot CUCM-abonnees in een cluster wordt de vertrouwde CA-lijst NIET van de ene peer naar de andere gerepliceerd in een Expressway- of VCS-cluster. Dat betekent dat als u een cluster hebt, u handmatig vertrouwde certificaten moet uploaden naar de CA-lijst op elke peer.

Verifiëren

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

De huidige certificaatinformatie controleren

Er zijn een aantal manieren waarop u de informatie op een bestaand certificaat kunt controleren. De eerste optie is via de webbrowser. Gebruik de in de vorige paragraaf beschreven methode die ook kan worden gebruikt voor de export van een specifiek certificaat in de keten. Als u SANâ€™s of andere kenmerken die aan het Expressway-servercertificaat zijn toegevoegd, moet verifiëren, kunt u dit rechtstreeks via de grafische gebruikersinterface (GUI) op het web doen, naar **Onderhoud > Beveiligingscertificaten > Servercertificaat** navigeren, en vervolgens op **Gedecodeerd tonen** klikken.

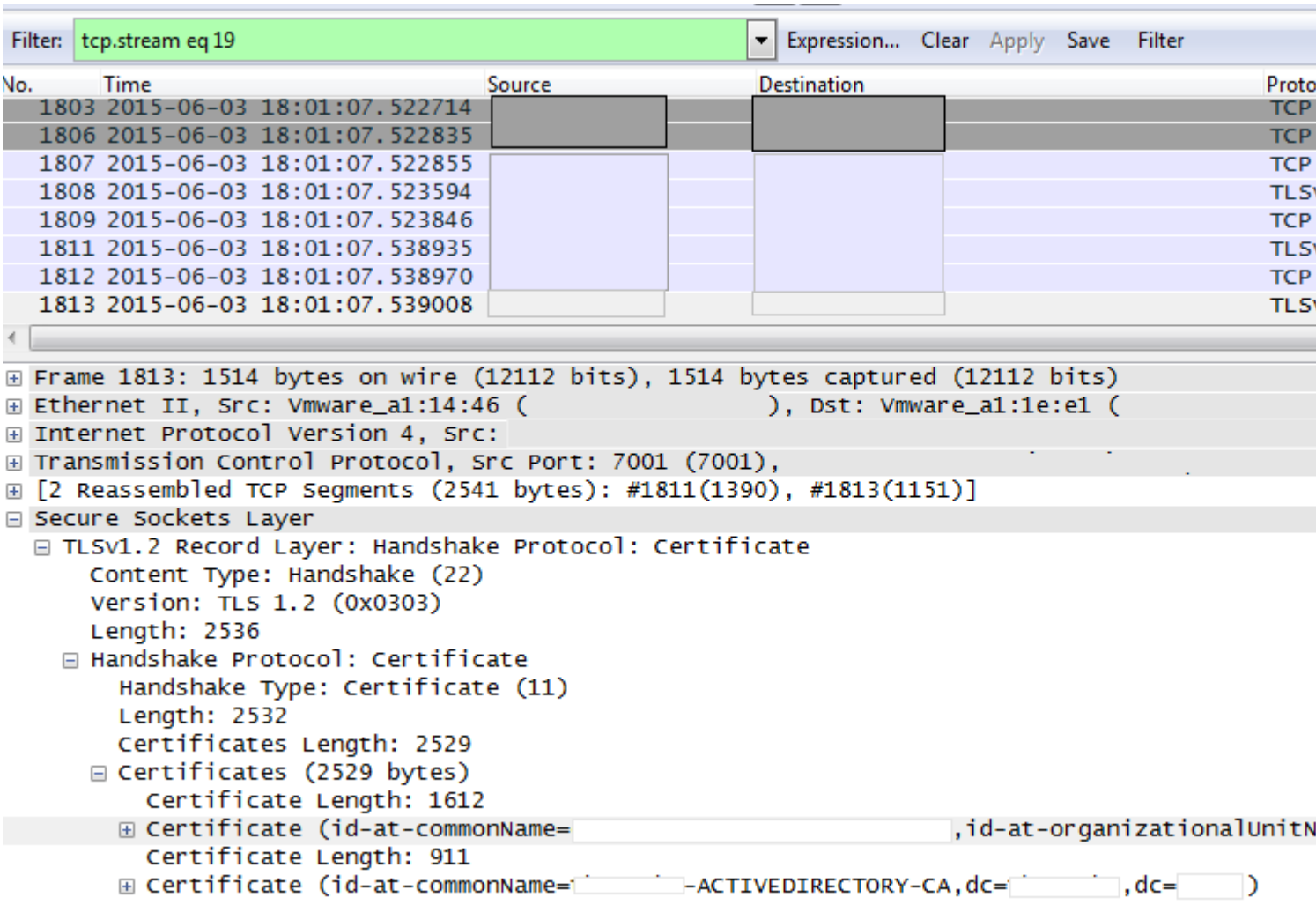


Hier kunt u alle specifieke details van het certificaat zien zonder de noodzaak om het te downloaden. U kunt hetzelfde doen voor een actieve MVO als het bijbehorende ondertekende certificaat nog niet is geüpload.

Lees/exporteer een certificaat in Wireshark

Als u een Wireshark opname van de SSL handdruk hebt die de certificaatuitwisseling omvat, kan Wireshark het certificaat voor u eigenlijk decoderen, en u kunt om het even welke certificaten in de ketting (als de volledige ketting) van binnenuit uitvoeren. Filter uw pakketopname voor de specifieke poort van de certificaatuitwisseling (over het algemeen 7001 in het geval van de doorsnede zone). Als u vervolgens de client- en serverhello-pakketten niet ziet samen met de SSL-handdruk, klikt u met de rechtermuisknop op

een van de pakketten in de TCP-stream en selecteert u **decoderen als**. Selecteer hier **SSL** en klik op **Toepassen**. Als u nu het juiste verkeer hebt opgenomen, moet u de certificaatuitwisseling zien. Vind het pakket van de juiste server die het certificaat in de payload bevat. Breid het SSL-gedeelte in het onderste deelvenster uit totdat u de lijst met certificaten ziet zoals in de afbeelding:



Hier kunt u een van de certificaten uitbreiden om alle details te zien. Als u het certificaat wilt exporteren, klikt u met de rechtermuisknop op het gewenste certificaat in de keten (als er meerdere zijn) en selecteert u **Exporteren geselecteerde pakketbytes**. Typ een naam voor het certificaat en klik op **Opslaan**. Nu, moet u het certificaat in de Kijker van het Certificaat van Windows kunnen openen (als u het een uitbreiding .cer geeft), of het uploaden aan een andere hulpmiddelen voor analyse.

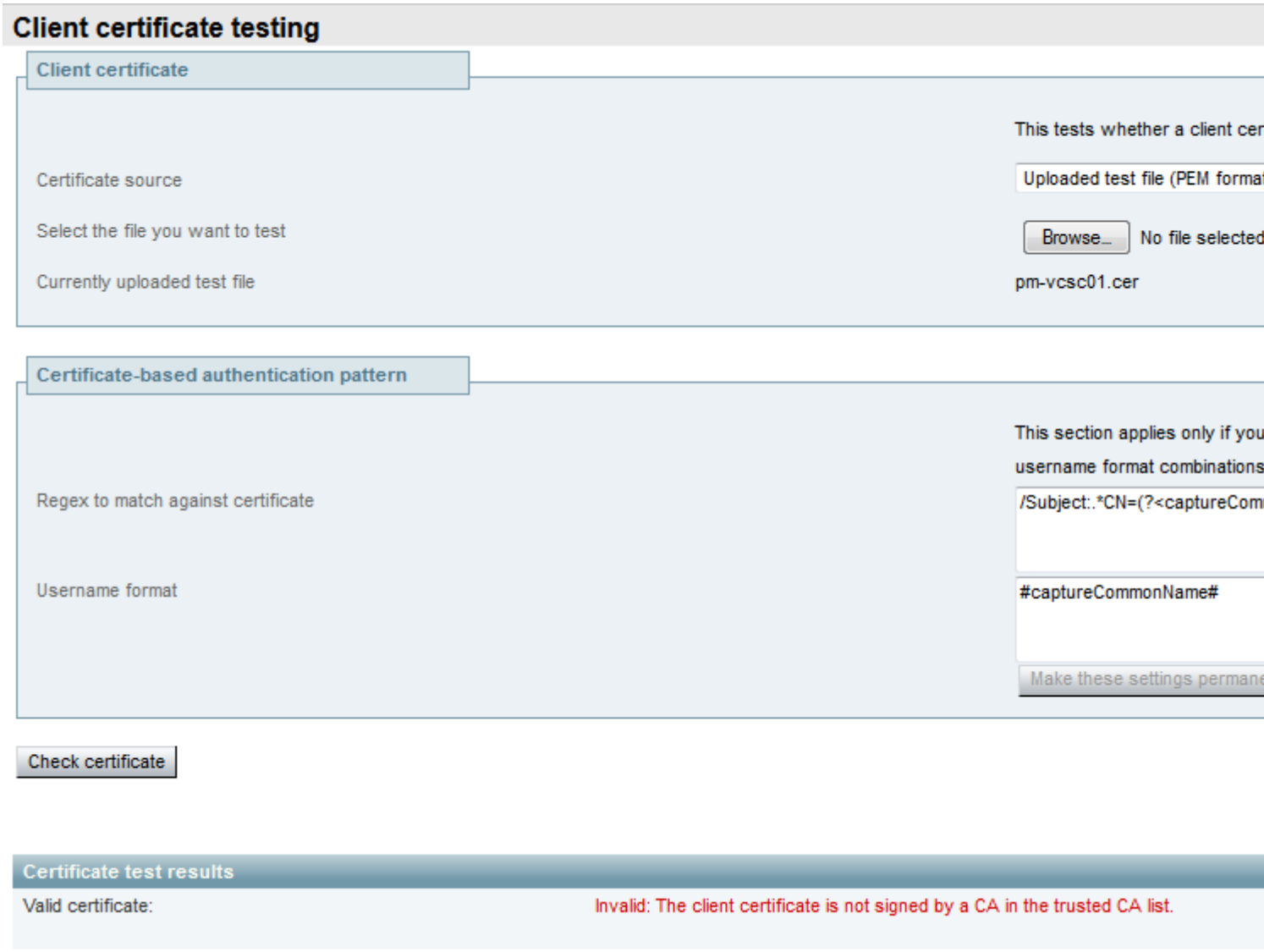
Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

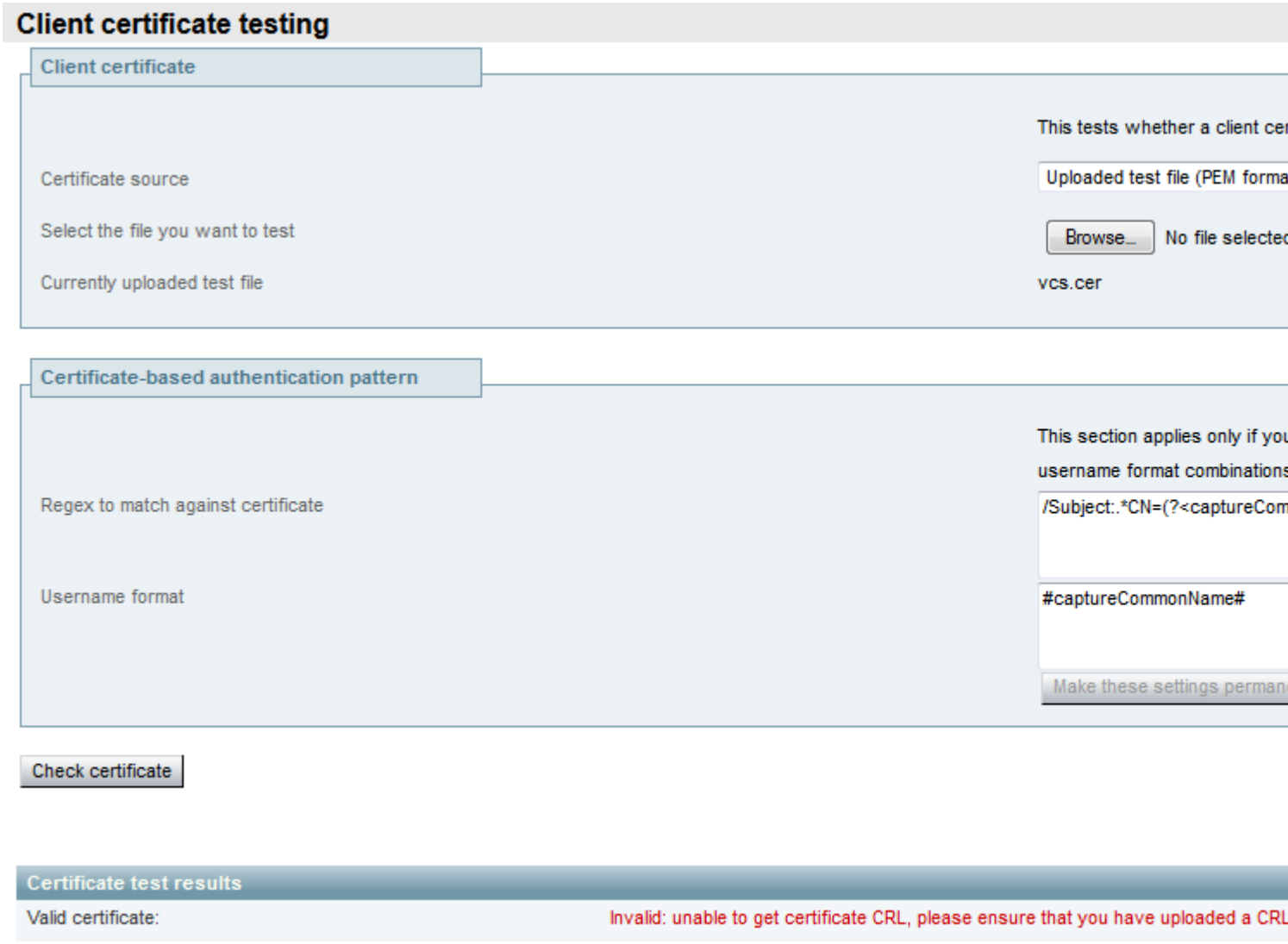
Test om te weten of een certificaat op de snelweg wordt vertrouwd

Terwijl de beste methode is om handmatig de certificaatketen te controleren en ervoor te zorgen dat alle leden zijn opgenomen in de Expressway vertrouwde CA-lijst, kunt u snel controleren of de Expressway vertrouwt op een specifiek klantcertificaat met behulp van de **Client Certificate Testing** onder **Onderhoud > Security Certificates** in de web GUI. Houd alle standaardinstellingen hetzelfde. Selecteer **Upload Test File** (pem-indeling) in de vervolgkeuzelijst en selecteer het clientcertificaat dat u wilt verifiëren. Als het certificaat niet wordt vertrouwd, zou u een fout, zoals getoond in het beeld krijgen, dat verklaart de reden het

werd verworpen. De fout die u ziet, is de gedecodeerde informatie van het geüploade certificaat ter referentie.



Als u een fout krijgt die beweert dat de Expressway niet in staat is om het certificaat CRL te krijgen, maar de Expressway gebruikt niet de CRL-controle, dit betekent dat het certificaat vertrouwd zou worden en alle andere verificatiecontroles heeft doorstaan.



Synergy Light-endpoints (7800/8800 Series-telefoons)

Deze nieuwe apparaten worden geleverd met een vooraf ingevulde certificaatvertrouwenslijst, die een groot aantal bekende publieke CA's bevat. Deze vertrouwenslijst kan niet worden gewijzigd, wat betekent dat uw Expressway-E certificaat MOET worden ondertekend door een van deze openbare CA's om met deze apparaten te werken. Als het wordt ondertekend door een interne CA of een andere openbare CA, zou de verbinding mislukken. Er is geen optie voor de gebruiker om het certificaat handmatig te accepteren zoals er is met Jabber-clients.

Opmerking: voor sommige implementaties is vastgesteld dat het gebruik van een apparaat zoals een Citrix NetScaler met een CA uit de lijst op de 7800/8800 Series-telefoons kan worden geregistreerd via MRA, zelfs als de Expressway-E een interne CA gebruikt. De NetScalers root CA moet geüpload worden naar de Expressway-E en de Interne root CA moet geüpload worden naar de Netscaler om SSL-verificatie te laten werken. Het is aangetoond dat dit werkt en het is steun bij de beste inspanningen.

Opmerking: Als de vertrouwde CA-lijst lijkt te hebben alle juiste certificaten in, maar het wordt nog steeds afgewezen, zorg ervoor dat er niet een ander certificaat hoger op de lijst met hetzelfde onderwerp dat zou kunnen conflicteren met de juiste. Wanneer alle andere faalt, kunt u de keten altijd

---

rechtstreeks vanuit de browser of Wireshark exporteren, en alle certificaten uploaden naar de tegenoverliggende servers CA-lijst. Dit zou garanderen dat het het vertrouwde certificaat is.

Opmerking: wanneer u problemen oplost in een transversale zone probleem, soms kan het probleem lijken te zijn een certificaat gerelateerd, maar het is eigenlijk iets aan de software kant. Controleer of de gebruikersnaam en het wachtwoord voor de transversale account correct zijn.

Opmerking: de VCS of Expressway ondersteunt geen tekens groter dan 999 in het SAN-veld van een certificaat. Alle SANâ€™s die deze limiet overschrijden (waarvoor veel alternatieve namen nodig zijn) zouden worden genegeerd alsof ze er niet waren.

Videobronnen

In deze sectie vindt u informatie in de video die u door alle configuratieprocessen van het certificaat kan leiden.

Een CSR genereren voor MRA of geclusterde expressways

Servercertificaat installeren op Expressway

Hoe te om Certificaatvertrouwen tussen Expressways te vormen

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.