Collaboration Edge (MRA)-Zertifikate konfigurieren und Fehlerbehebung durchführen

Inhalt

Einleitung

In diesem Dokument werden Zertifikate für MRA-Bereitstellungen (Mobile Remote Access) beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Öffentliche und private Zertifizierungsstelle (CA)

Es gibt eine Reihe von Optionen zum Signieren von Zertifikaten auf den Expressway-C- und E-Servern. Sie können festlegen, dass die Zertifikatsignierungsanforderung (CSR) von einer öffentlichen Zertifizierungsstelle wie GoDaddy, Verisign oder anderen signiert wird, oder Sie können sie intern signieren, wenn Sie Ihre eigene Zertifizierungsstelle verwenden (kann entweder selbst mit OpenSSL oder einer internen Unternehmenszertifizierungsstelle wie einem Microsoft Windows-Server signiert werden). Weitere Informationen zum Erstellen und Signieren der von diesen Methoden verwendeten CSRs finden Sie im Video Communication Server (VCS) Certificate Creation Guide.

Der einzige Server, der wirklich von einer öffentlichen Zertifizierungsstelle signiert werden muss, ist Expressway-E. Dies ist der einzige Server, auf dem die Clients das Zertifikat sehen, wenn sie sich über MRA anmelden. Verwenden Sie daher eine öffentliche Zertifizierungsstelle, um sicherzustellen, dass die Benutzer das Zertifikat nicht manuell akzeptieren müssen. Der Expressway-E kann mit einem internen CA-signierten Zertifikat arbeiten, aber erstmalige Benutzer werden aufgefordert, das nicht vertrauenswürdige Zertifikat zu akzeptieren. Die MRA-Registrierung von Telefonen der Serien 7800 und 8800 funktioniert nicht mit internen Zertifikaten, da die Zertifikatvertrauensliste nicht geändert werden kann. Der Einfachheit halber wird empfohlen, dass Ihre Expressway-C- und Expressway-E-Zertifikate beide von derselben Zertifizierungsstelle signiert werden. Dies ist jedoch keine Anforderung, solange Sie die Listen der vertrauenswürdigen Zertifizierungsstellen auf beiden Servern ordnungsgemäß konfiguriert haben.

Funktionsweise von Zertifikatsketten

Zertifikate werden in einer Kette von zwei oder mehr miteinander verknüpft, um die Quelle zu überprüfen, die das Zertifikat des Servers signiert hat. Es gibt drei Arten von Zertifikaten in einer Kette: das Client-/Server-Zertifikat, das Zwischenzertifikat (in einigen Fällen) und das Stammzertifikat (auch als Stammzertifizierungsstelle bezeichnet, da es sich um die Behörde auf höchster Ebene handelt, die das Zertifikat signiert hat).

Zertifikate enthalten zwei primäre Felder, die die Kette bilden: den Betreff und den Aussteller.

Der Betreff ist der Name des Servers oder der Autorität, für den bzw. die dieses Zertifikat steht. Im Fall eines Expressway-C oder Expressway-E (oder anderer Unified Communications (UC)-Geräte) wird dieser aus dem vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) erstellt.

Der Aussteller ist die Behörde, die dieses spezifische Zertifikat validiert hat. Da jeder ein Zertifikat signieren kann (einschließlich des Servers, der das Zertifikat erstellt hat, zunächst auch als selbstsignierte Zertifikate bezeichnet), verfügen Server und Clients über eine Liste von Ausstellern oder Zertifizierungsstellen, denen er als authentisch vertraut.

Eine Zertifikatskette endet immer mit einem selbstsignierten Zertifikat der obersten Ebene oder dem Stammzertifikat. Wenn Sie sich durch die Zertifikathierarchie bewegen, hat jedes Zertifikat einen anderen Aussteller in Bezug auf das Thema. Schließlich würden Sie auf die Stammzertifizierungsstelle stoßen, bei der Betreff und Aussteller übereinstimmen. Dies weist darauf hin, dass es sich um das Zertifikat der obersten Ebene und somit um das Zertifikat handelt, das von der Liste der vertrauenswürdigen Zertifizierungsstellen eines Clients oder Servers als vertrauenswürdig eingestuft werden muss.

SSL-Handshake - Zusammenfassung

Im Falle der Traversal-Zone agiert der Expressway-C immer als Client, während der Expressway-E immer der Server ist. Der vereinfachte Austausch funktioniert wie folgt:

Expressway C Expressway E

---------Client-Hello-------->

<--------Server Hello---------

<----Serverzertifikat-------

<----Zertifikatanforderungâ€”

------Client-Zertifikat------>

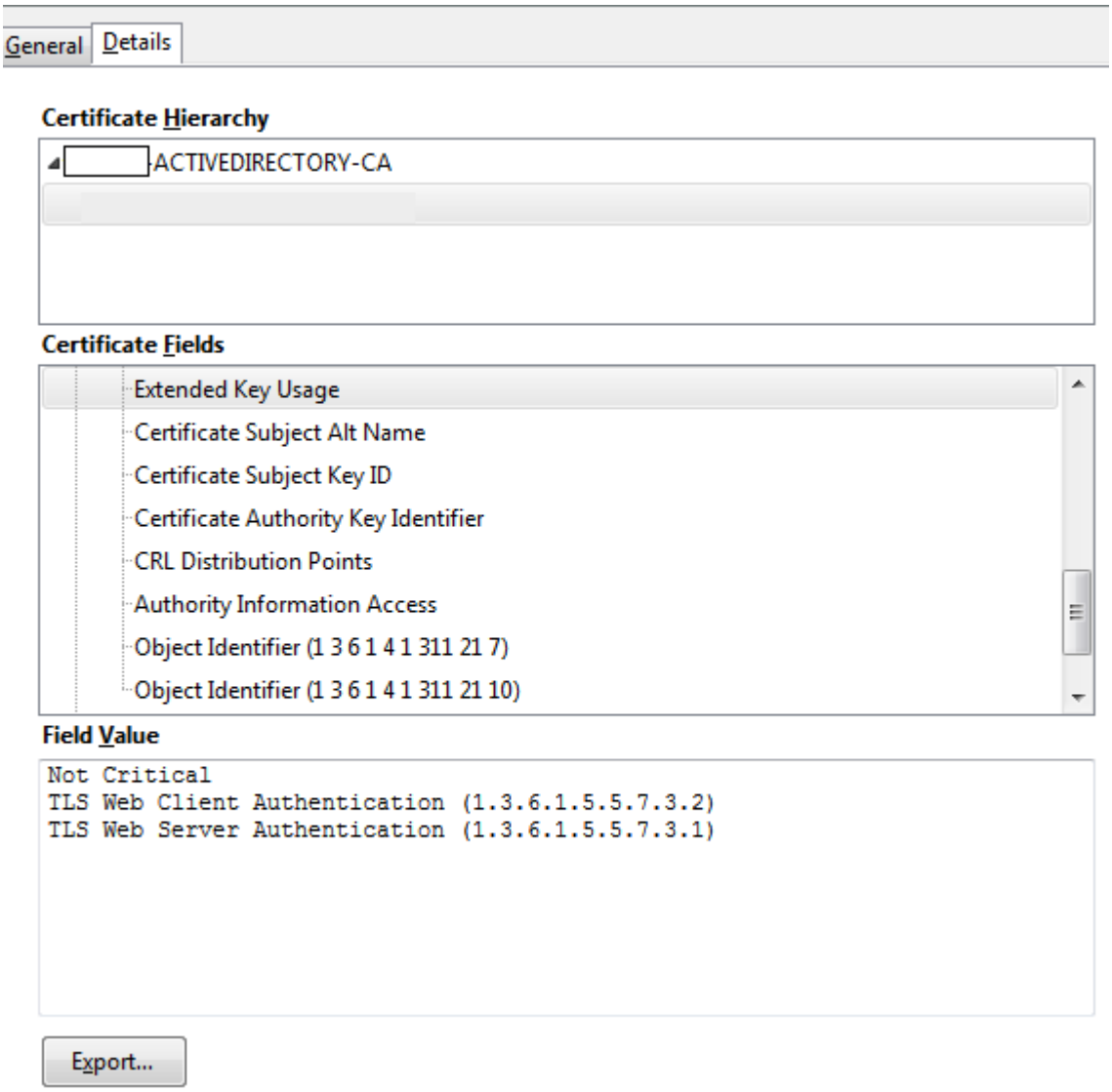
Der Schlüssel liegt hier im Austausch, da der Expressway-C immer die Verbindung initiiert und somit immer der Client ist. Der Expressway-E ist der erste, der sein Zertifikat versendet. Wenn der Expressway-C dieses Zertifikat nicht validieren kann, reißt er den Handshake ab und kann kein eigenes Zertifikat an den Expressway-E senden.

Ein weiterer wichtiger Punkt ist die TLS-Webclient-Authentifizierung (Transport Layer Security) und die TLS-Webserver-Authentifizierungsattribute für Zertifikate. Diese Attribute werden für die Zertifizierungsstelle bestimmt, die den CSR signiert hat (wenn eine Windows-Zertifizierungsstelle verwendet wird, wird dies durch die ausgewählte Vorlage bestimmt), und geben an, ob das Zertifikat in der Rolle des Clients oder des Servers (oder in beiden) gültig ist. Da ein VCS oder Expressway situationsbedingt sein kann (bei einer Traversal-Zone immer gleich), muss das Zertifikat sowohl über Client- als auch über Serverauthentifizierungsattribute verfügen.

Die Expressway-C und Expressway-E geben einen Fehler aus, wenn sie auf ein neues Serverzertifikat hochgeladen werden, wenn beide nicht angewendet werden.

Wenn Sie sich nicht sicher sind, ob ein Zertifikat über diese Attribute verfügt, können Sie die Zertifikatdetails in einem Browser oder in Ihrem Betriebssystem öffnen und den Abschnitt "Extended Key Usage" (Erweiterte Schlüsselverwendung) überprüfen (siehe Abbildung). Das Format kann variieren und hängt davon ab, wie Sie das Zertifikat betrachten.

Beispiel:



Konfigurieren

Expressway-C und Expressway-E Traversal Zone/Trust

Erstellen und Signieren von CSRs

Wie bereits beschrieben, müssen die Expressway-C- und Expressway-E-Zertifikate entweder von einer internen oder externen Zertifizierungsstelle oder von OpenSSL zur Selbstsignierung signiert werden.

> **Hinweis**: Sie können das temporäre Zertifikat auf dem Expressway-Server nicht verwenden, da es nicht unterstützt wird. Wenn Sie Platzhalterzertifikate verwenden, für die ein Zertifikat für das Zertifizierungsstellen-Zeichen vorhanden ist und die Betreffzeile nicht speziell definiert ist, wird dies nicht unterstützt.

Der erste Schritt besteht darin, den CSR zu generieren und durch den bevorzugten CA-Typ signieren zu lassen. Der entsprechende Prozess wird im Certificate Creation Guide beschrieben. Beim Erstellen der CSR-Anfrage sollten Sie unbedingt die erforderlichen alternativen Namen (SANs) für den Betreff berücksichtigen, die in den Zertifikaten enthalten sein müssen. Dies wird auch im Zertifikatsleitfaden und im Mobile Remote Access Deployment Guide aufgeführt. Informieren Sie sich über die aktuellsten Versionen des Leitfadens, da bei Verfügbarkeit neuer Funktionen weitere hinzugefügt werden können. Liste

der gängigen SANs, die je nach den verwendeten Funktionen hinzugefügt werden müssen:

Schnellstraße C

- Alle Domänen (intern oder extern), die der Liste der Domänen hinzugefügt wurden.
- Alle Aliase für persistente Chat-Knoten, wenn ein XMPP-Verbund verwendet wird.
- Sichere Geräteprofilnamen auf dem CUCM bei Verwendung sicherer Geräteprofile.

Expressway E

- Alle auf dem Expressway-C konfigurierten Domänen.
- Alle Aliase für persistente Chat-Knoten, wenn ein XMPP-Verbund verwendet wird.
- Alle Domänen, die für XMPP-Verbünde angekündigt wurden.

> **Hinweis:** Wenn die für externe Service Record (SRV)-Suchvorgänge verwendete Basisdomäne nicht als SAN im Expressway-E-Zertifikat (entweder xxx.com oder collab-edge.xxx.com) enthalten ist, benötigen die Jabber-Clients den Endbenutzer weiterhin, um das Zertifikat auf der ersten Verbindung zu akzeptieren, und die TC-Endpunkte stellen überhaupt keine Verbindung her.

Konfigurieren von Expressway-C und Expressway-E für gegenseitiges Vertrauen

Damit die Unified Communications-Überbrückungszone eine Verbindung herstellen kann, müssen Expressway-C und Expressway-E den Zertifikaten der jeweils anderen Partei vertrauen. In diesem Beispiel wird davon ausgegangen, dass das Expressway-E-Zertifikat von einer öffentlichen Zertifizierungsstelle signiert wurde, die diese Hierarchie verwendet.

Zertifikat 3

Aussteller: GoDaddy Root CA

Betrifft: GoDaddy Root CA

Zertifikat 2

Aussteller: GoDaddy Root CA

Betrifft: GoDaddy Intermediate Authority

Zertifikat 1

Emittent: GoDaddy Intermediate Authority

Betrifft: Expressway E.lab

Der Expressway-C muss mit dem Vertrauenszertifikat 1 konfiguriert werden. In den meisten Fällen sendet er basierend auf den auf den Server angewendeten vertrauenswürdigen Zertifikaten nur das Serverzertifikat der niedrigsten Ebene. Das bedeutet, dass Sie für das Zertifikat 1 von Expressway-C beide Zertifikate 2 und 3 in die Liste der vertrauenswürdigen Zertifizierungsstellen von Expressway-C hochladen müssen (**Wartung > Sicherheit > Liste vertrauenswürdiger Zertifizierungsstellen**). Wenn Sie das Zwischenzertifikat 2 auslassen, wenn der Expressway-C das Expressway-E-Zertifikat empfängt, kann es nicht mit der vertrauenswürdigen GoDaddy-Stammzertifizierungsstelle verknüpft werden, daher wird es abgelehnt.

Zertifikat 3

Aussteller: GoDaddy Root CA

Betrifft: GoDaddy Root CA

Zertifikat 1

Emittent: GoDaddy Intermediate Authority - Nicht vertrauenswürdig!

Betrifft: Expressway E.lab

Wenn Sie das Zwischenzertifikat nur ohne den Stamm in die Liste der vertrauenswürdigen Zertifizierungsstellen von Expressway-C hochladen, würde dies bedeuten, dass die GoDaddy Intermediate Authority vertrauenswürdig ist, aber von einer höheren Behörde signiert wird, in diesem Fall GoDaddy Root CA, die nicht vertrauenswürdig ist, daher würde es fehlschlagen.

Zertifikat 2

Emittent: GoDaddy Root CA - Nicht vertrauenswürdig!

Betrifft: GoDaddy Intermediate Authority

Zertifikat 1

Emittent: GoDaddy Intermediate Authority

Betrifft: Expressway E.lab

Wenn alle Zwischenprodukte und der Stamm zur Liste der vertrauenswürdigen Zertifizierungsstellen hinzugefügt wurden, kann das Zertifikat überprüft werden...

Zertifikat 3

Aussteller: GoDaddy Root CA - Selbstsigniertes Zertifikat auf höchster Ebene ist vertrauenswürdig und vollständig verkettet!

Betrifft: GoDaddy Root CA

Zertifikat 2

Aussteller: GoDaddy Root CA

Betrifft: GoDaddy Intermediate Authority

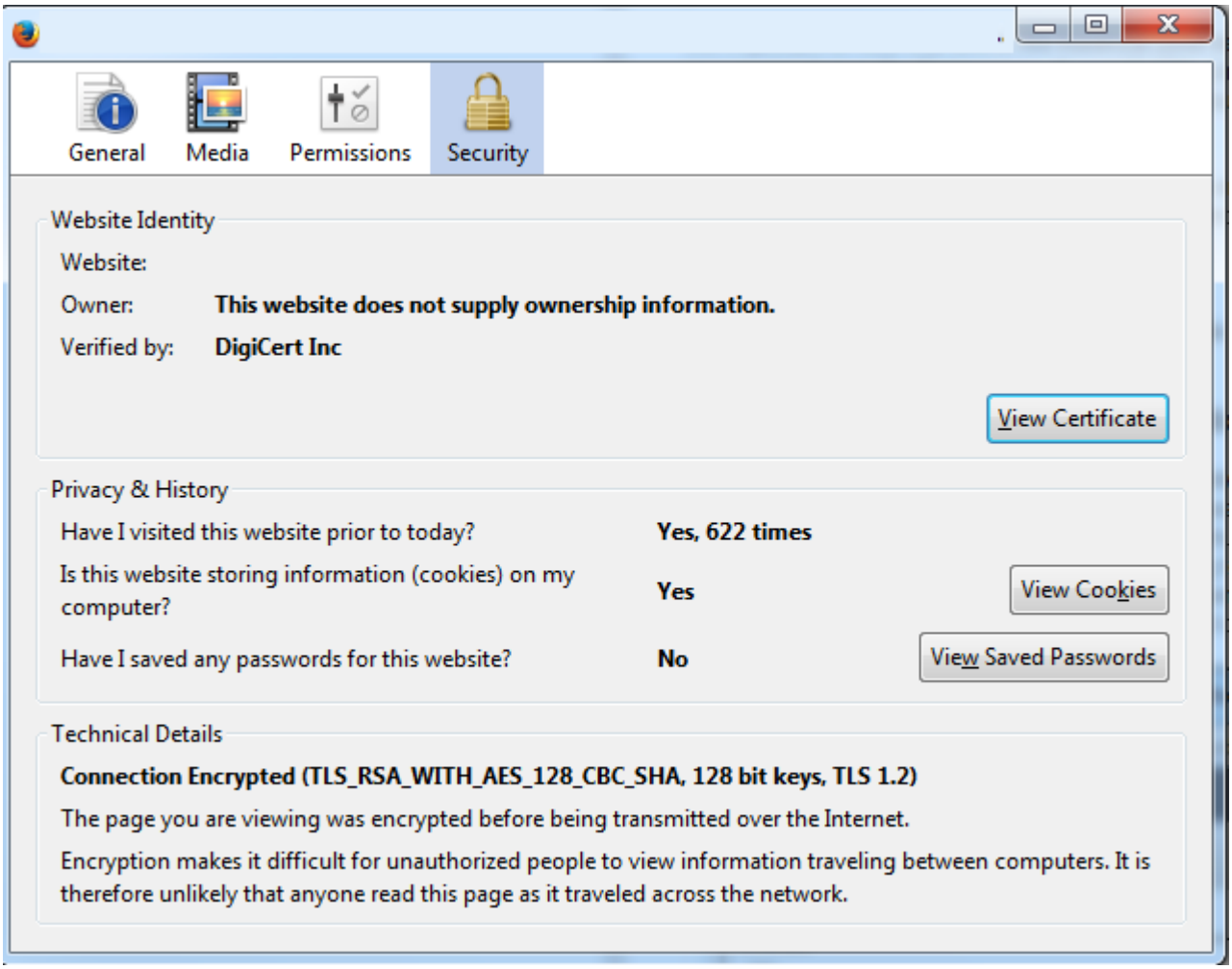
Zertifikat 1

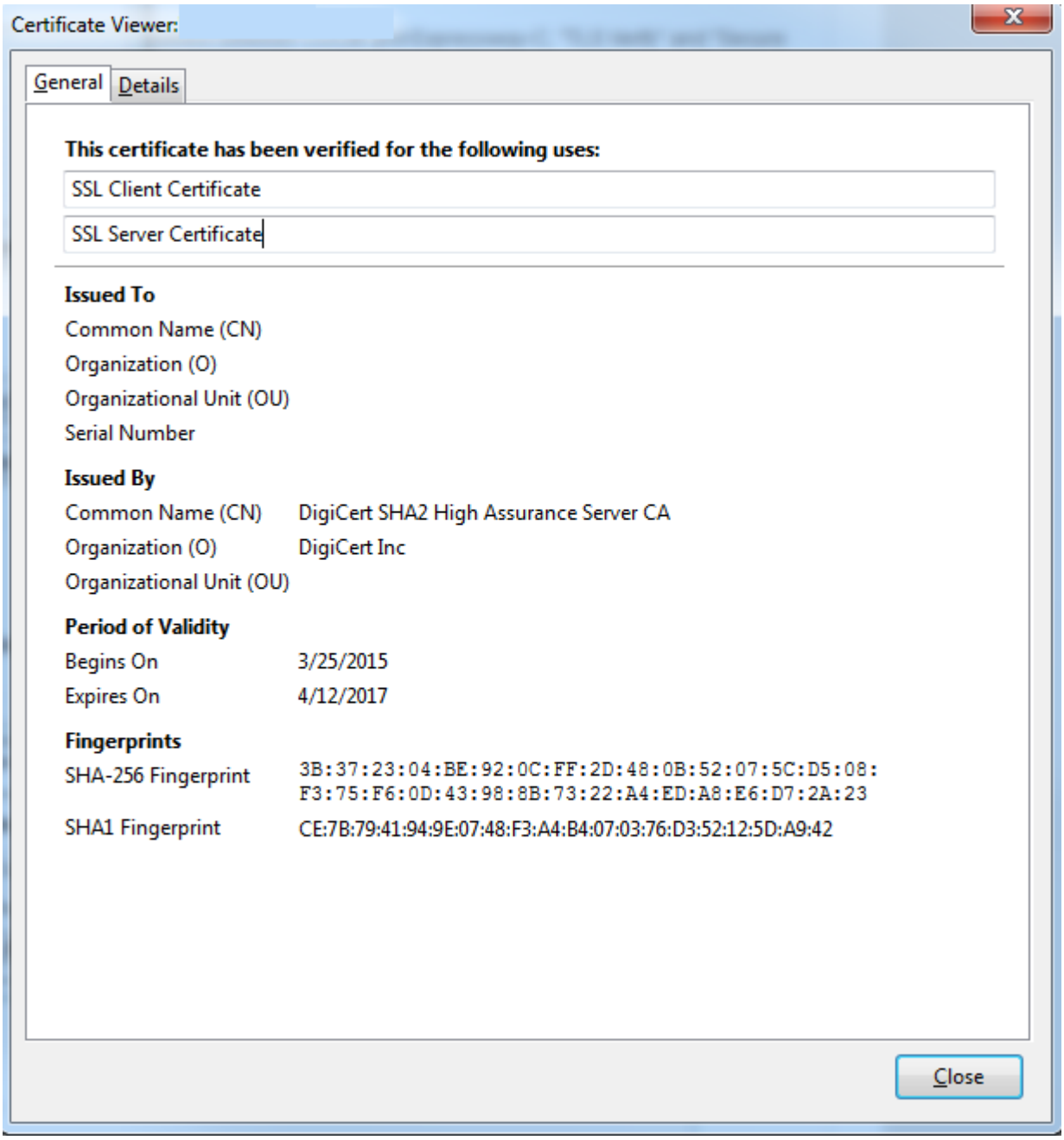
Emittent: GoDaddy Intermediate Authority

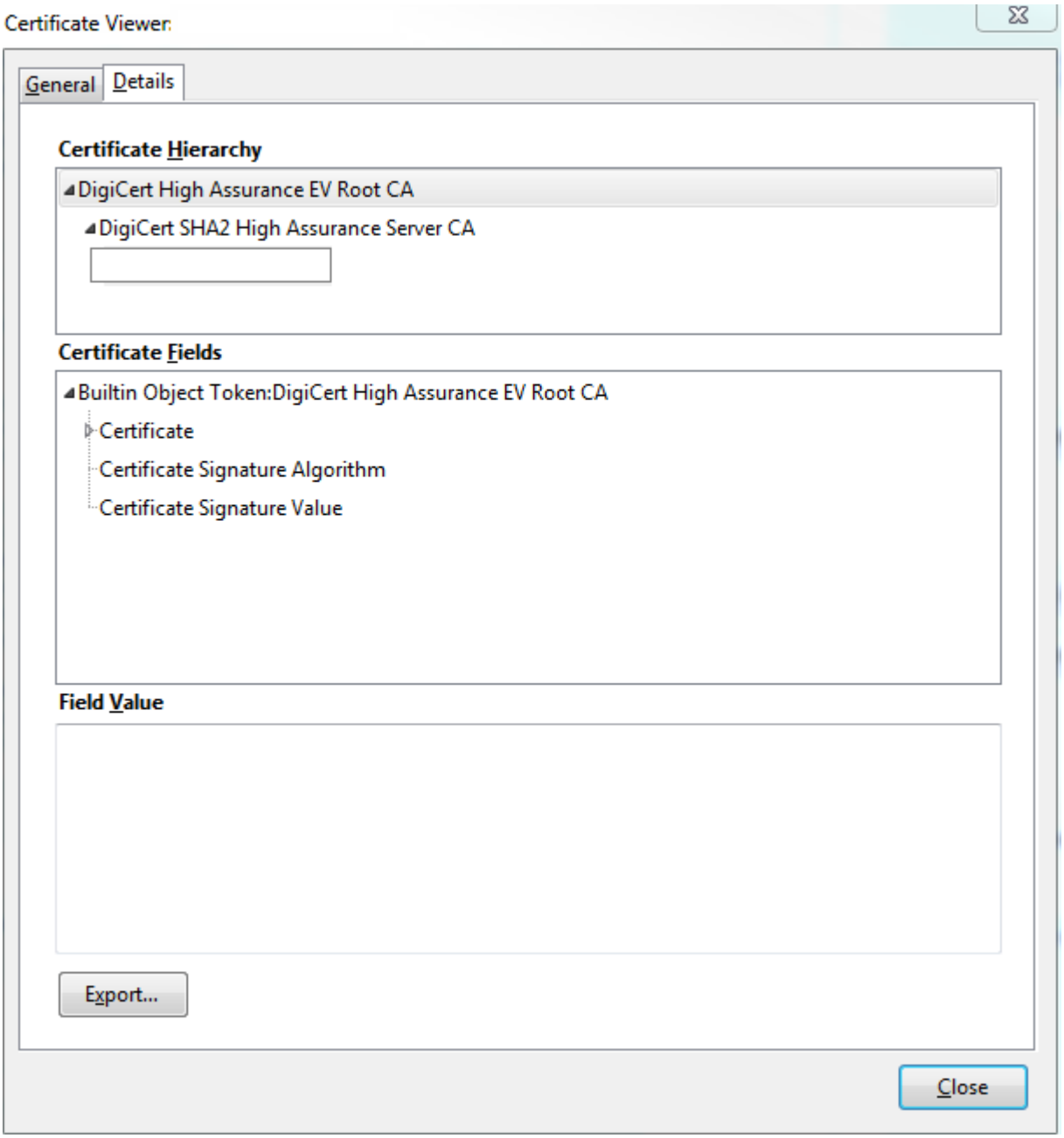
Betrifft: Expressway E.lab

Wenn Sie sich nicht sicher sind, was die Zertifikatskette ist, können Sie Ihren Browser überprüfen, wenn Sie sich bei der Webschnittstelle des jeweiligen Expressway angemeldet haben. Der Prozess variiert leicht je

nach Browser, aber in Firefox können Sie auf das Sperrsymbol ganz links in der Adressleiste klicken. Klicken Sie dann im Popup-Fenster auf **Weitere Informationen > Zertifikat anzeigen > Details**. Wenn Ihr Browser die gesamte Kette zusammensetzen kann, können Sie die Kette von oben nach unten sehen. Wenn für das Zertifikat der obersten Ebene kein entsprechender Betreff und kein entsprechender Aussteller angegeben sind, bedeutet dies, dass die Kette nicht abgeschlossen ist. Sie können die einzelnen Zertifikate der Kette auch einzeln exportieren, wenn Sie auf **Exportieren** klicken und das gewünschte Zertifikat hervorgehoben ist. Dies ist nützlich, wenn Sie nicht hundertprozentig sicher sind, dass Sie die richtigen Zertifikate in die Zertifizierungsstellen-Vertrauensliste hochgeladen haben.




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



Nachdem der Expressway-C dem Zertifikat des Expressway-E vertraut, stellen Sie sicher, dass es in die entgegengesetzte Richtung funktioniert. Wenn das Expressway-C-Zertifikat von derselben Zertifizierungsstelle signiert wird, die auch das Expressway-E signiert hat, ist der Vorgang einfach. Laden Sie die gleichen Zertifikate in die Liste der vertrauenswürdigen Zertifizierungsstellen auf Expressway-E hoch, wie Sie dies bereits für das C getan haben. Wenn das C von einer anderen Zertifizierungsstelle signiert wird, müssen Sie den gleichen Prozess wie im Bild dargestellt verwenden, jedoch die Kette des signierten Expressway-C-Zertifikats verwenden.

Sichere Kommunikation zwischen Cisco Unified Communications Manager (CUCM) und Expressway-C

Überblick

Im Gegensatz zur Überbrückungszone zwischen Expressway-C und Expressway-E ist keine sichere Signalisierung zwischen Expressway-C und CUCM erforderlich. Sofern die internen Sicherheitsrichtlinien dies nicht zulassen, müssen Sie MRAs immer so konfigurieren, dass sie mit nicht sicheren Geräteprofilen auf dem CUCM arbeiten, um sicherzustellen, dass der Rest der Bereitstellung korrekt ist, bevor Sie mit

diesem Schritt fortfahren.

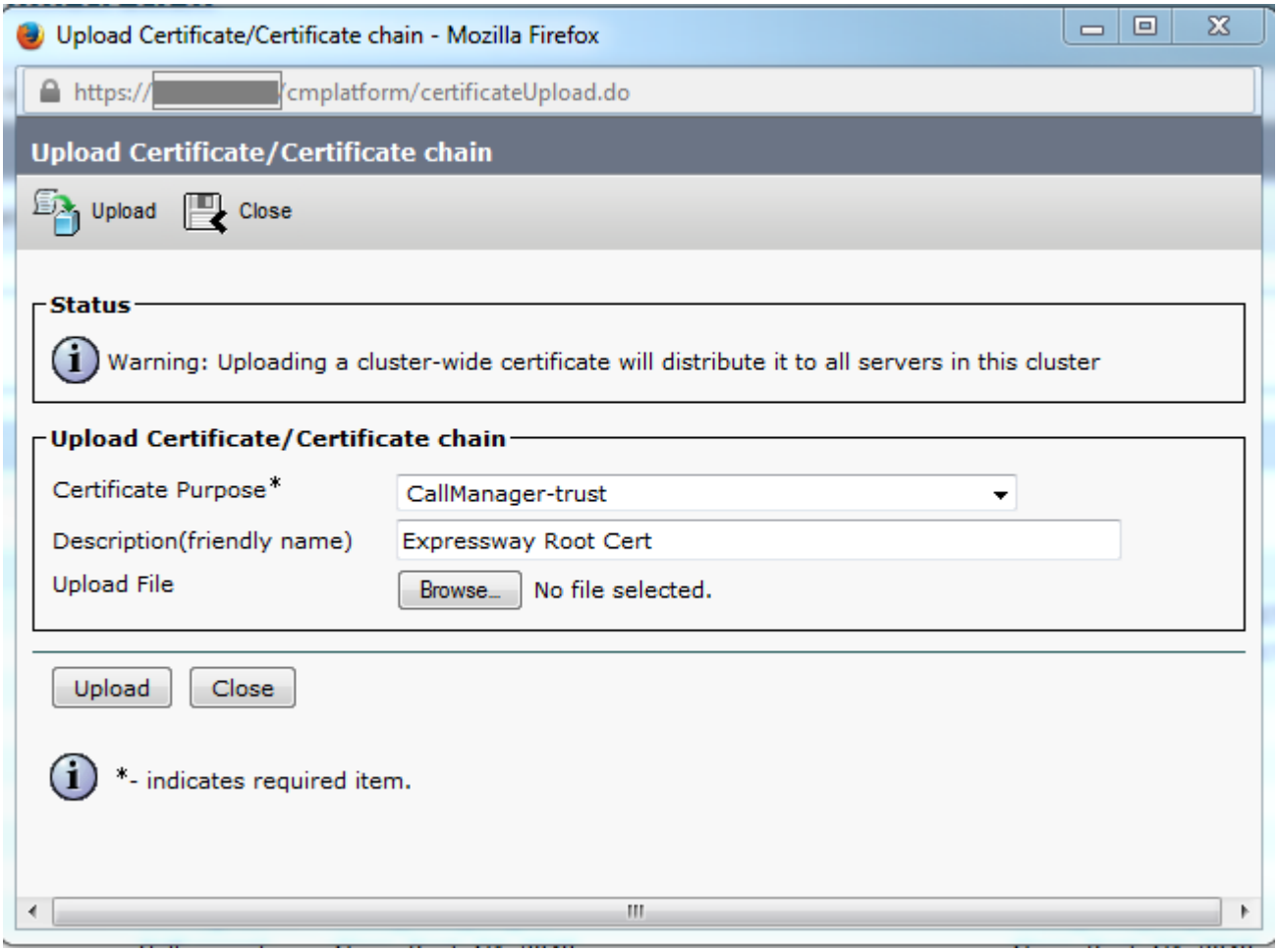
Es gibt zwei Hauptsicherheitsfunktionen, die zwischen CUCM und Expressway-C aktiviert werden können: TLS-Überprüfung und sichere Geräteregistrierung. Es gibt einen wichtigen Unterschied zwischen diesen beiden, da sie zwei verschiedene Zertifikate von der CUCM-Seite im SSL-Handshake verwenden.

TLS-Überprüfung - Tomcat-Zertifikat

Sichere SIP-Registrierungen - CallManager-Zertifikat

Konfigurieren der Vertrauensstellung zwischen CUCM und Expressway-C

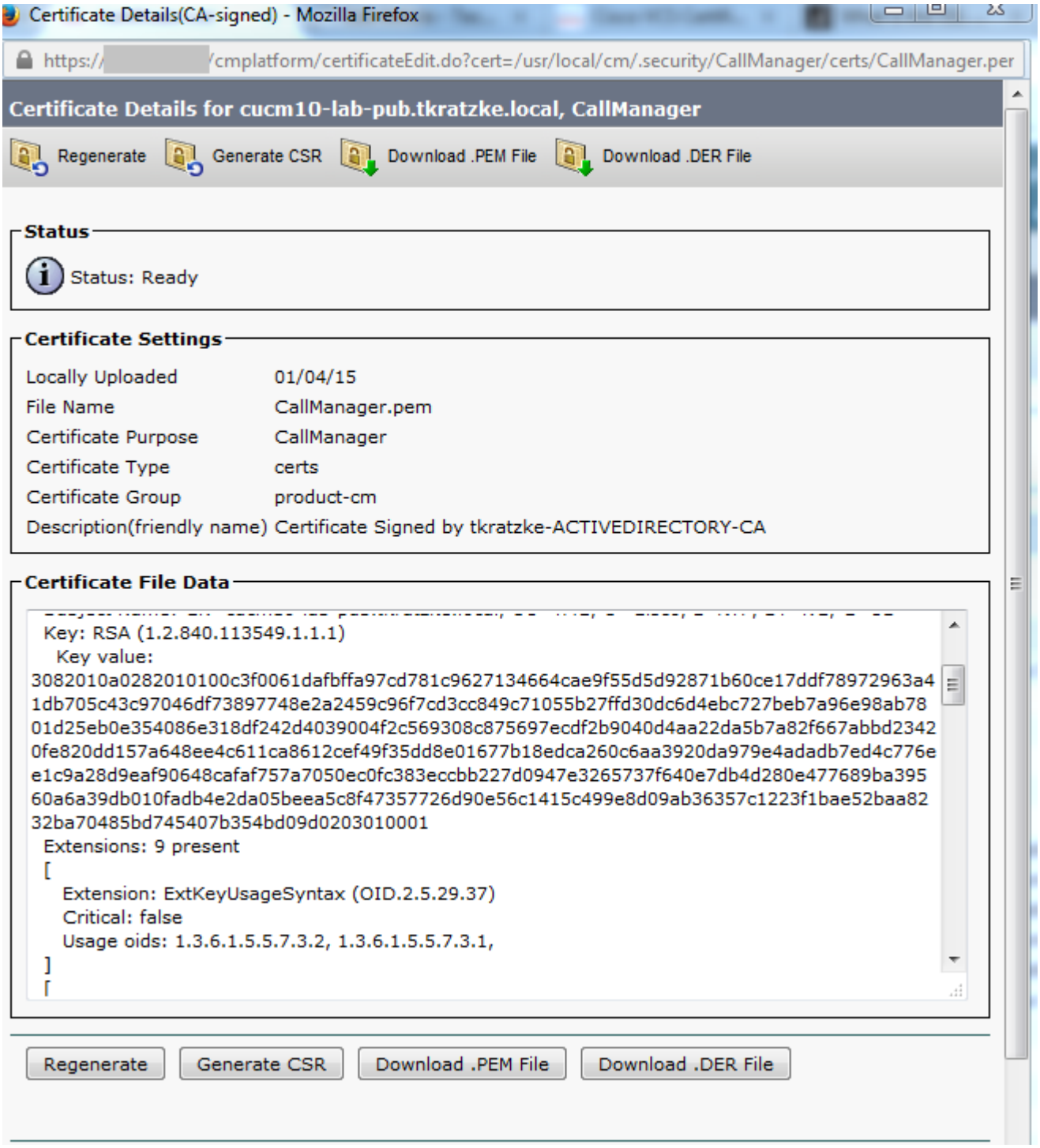
Das Konzept ist in diesem Fall genau das gleiche wie zwischen Expressway-C und Expressway-E. Der CUCM muss zunächst dem Serverzertifikat des Expressway-C vertrauen. Das bedeutet, dass auf dem CUCM die Intermediate und Root-Zertifikate von Expressway-C als Tomcat-Trust-Zertifikat für die TLS-Verifizierungsfunktion und als CallManager-Trust für sichere Geräteregistrierungen hochgeladen werden müssen. Navigieren Sie dazu zu **Cisco Unified OS Administration** oben rechts in der CUCM-Web-GUI, dann **Security > Certificate Management**. Klicken Sie hier auf **Zertifikat hochladen/Zertifikatskette,** und wählen Sie das richtige Vertrauensstellungsformat aus, oder klicken Sie auf **Suchen,** um die Liste der aktuell hochgeladenen Zertifikate anzuzeigen.



Sie müssen sicherstellen, dass Expressway-C der Zertifizierungsstelle vertraut, die die CUCM-Zertifikate signiert hat. Dies ist möglich, wenn Sie sie zur Liste der vertrauenswürdigen Zertifizierungsstellen hinzufügen. Wenn Sie die CUCM-Zertifikate mit einer Zertifizierungsstelle signiert haben, müssen in fast allen Fällen die Tomcat- und CallManager-Zertifikate von derselben Zertifizierungsstelle signiert werden. Wenn sich diese unterscheiden, müssen Sie bei Verwendung von "TLS Verify" und "Secure Registrations" beide Optionen als vertrauenswürdig einstufen.

Für sichere SIP-Registrierungen müssen Sie außerdem sicherstellen, dass der auf das Gerät angewendete sichere Geräteprofilname auf dem CUCM als SAN im Expressway-C-Zertifikat aufgeführt ist. Wenn dies nicht die sicheren Registernachrichten enthält, würde ein Fehler mit 403 vom CUCM auftreten, was auf einen TLS-Fehler hinweist.

Hinweis: Wenn der SSL-Handshake zwischen CUCM und Expressway-C für eine sichere SIP-Registrierung stattfindet, werden zwei Handshakes durchgeführt. Zunächst fungiert der Expressway-C als Client und initiiert die Verbindung mit dem CUCM. Sobald dieser Vorgang erfolgreich abgeschlossen wurde, initiiert der CUCM einen weiteren Handshake als Client für die Antwort. Das bedeutet, dass das CallManager-Zertifikat auf CUCM genau wie der Expressway-C über TLS Web Client- und TLS Web Server-Authentifizierungsattribute verfügen muss. Der Unterschied besteht darin, dass der CUCM das Hochladen dieser Zertifikate ohne beides ermöglicht, und die internen sicheren Registrierungen funktionieren gut, wenn der CUCM nur über das Serverauthentifizierungsattribut verfügt. Sie können dies auf CUCM bestätigen, wenn Sie in der Liste nach dem CallManager-Zertifikat suchen und es auswählen. Dort können Sie sich die Nutzungs-Oiden unter der Erweiterung Sektion ansehen. Sie können 1.3.6.1.5.5.7.3.2 für DIE Client-Authentifizierung und 1.3.6.1.5.5.7.3.1 für die Server-Authentifizierung sehen. Sie können das Zertifikat auch von diesem Fenster herunterladen.



Hinweis: Die Vertrauenszertifikate, die auf den Publisher in einem Cluster angewendet werden, müssen auf die Abonnenten repliziert werden. Es empfiehlt sich, sich bei einer neuen Konfiguration separat bei diesen anzumelden.

Hinweis: Damit der Expressway-C das Zertifikat vom CUCM ordnungsgemäß validiert, MÜSSEN die CUCM-Server im Expressway-C mit dem FQDN und nicht mit der IP-Adresse hinzugefügt werden. Die IP-Adresse kann nur verwendet werden, wenn die IP-Adresse jedes CUCM-Knotens als SAN im Zertifikat hinzugefügt wird, was fast nie der Fall ist.

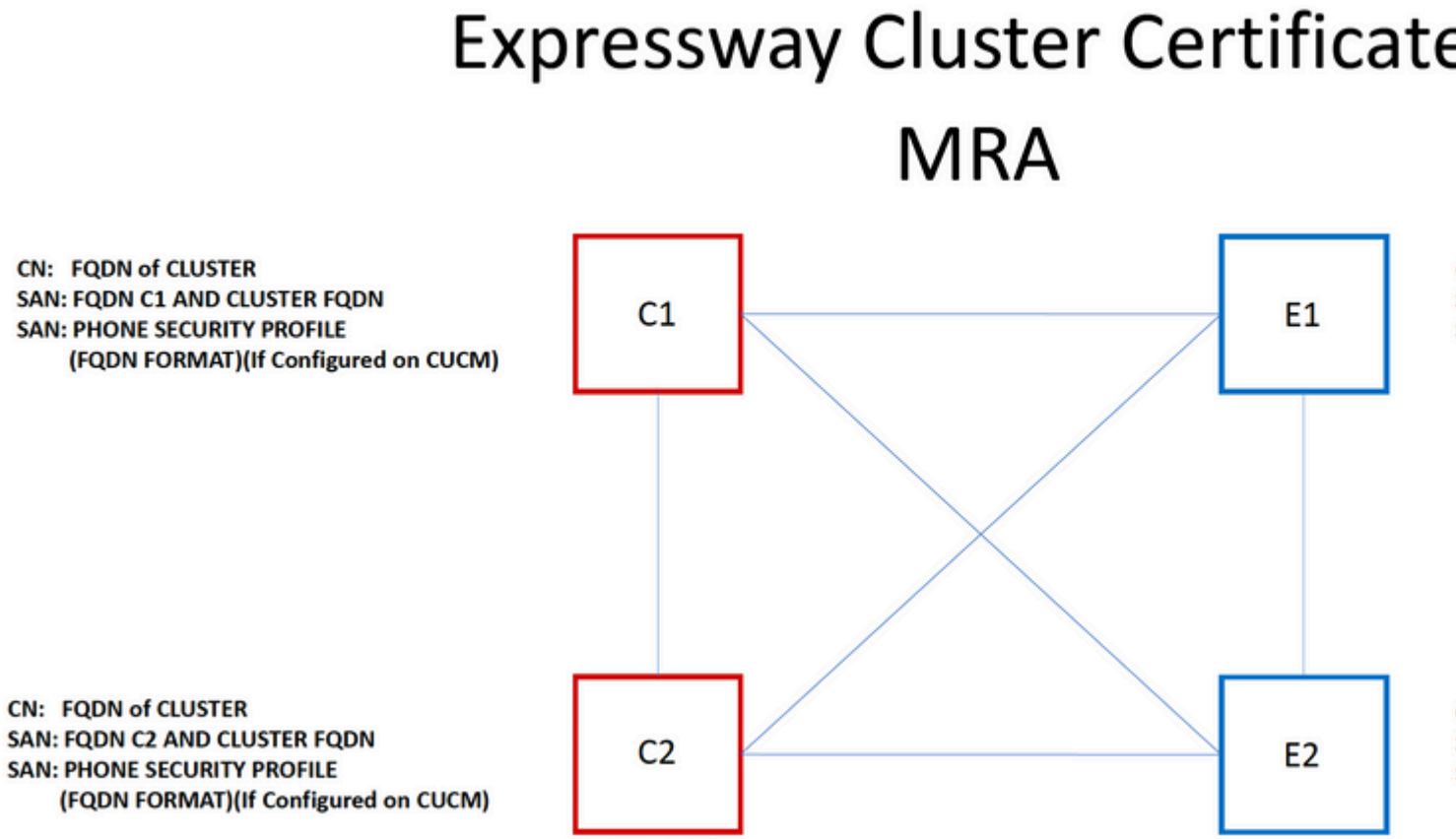
CUCM-Server mit selbstsignierten Zertifikaten

Ein CUCM-Server wird standardmäßig mit selbstsignierten Zertifikaten geliefert. Wenn diese vorhanden sind, ist es nicht möglich, TLS Verify (TLS-Überprüfung) und Secure Device Registration gleichzeitig zu verwenden. Beide Funktionen können separat verwendet werden. Da die Zertifikate jedoch selbst signiert sind, müssen sowohl die selbstsignierten Tomcat- als auch die selbstsignierten CallManager-Zertifikate in die Liste der vertrauenswürdigen Zertifizierungsstellen auf Expressway-C hochgeladen werden. Wenn Expressway-C seine Vertrauensliste durchsucht, um ein Zertifikat zu validieren, wird sie beendet, sobald ein Zertifikat mit einem übereinstimmenden Betreff gefunden wird. Aus diesem Grund würde diese Funktion funktionieren, unabhängig davon, welche Funktion weiter oben auf der Vertrauensliste, in Tomcat oder CallManager aufgeführt ist. Der untere würde genauso versagen, als wäre er nicht vorhanden. Die Lösung hierfür besteht darin, Ihre CUCM-Zertifikate mit einer Zertifizierungsstelle (öffentlich oder privat) zu signieren und nur dieser zu vertrauen.

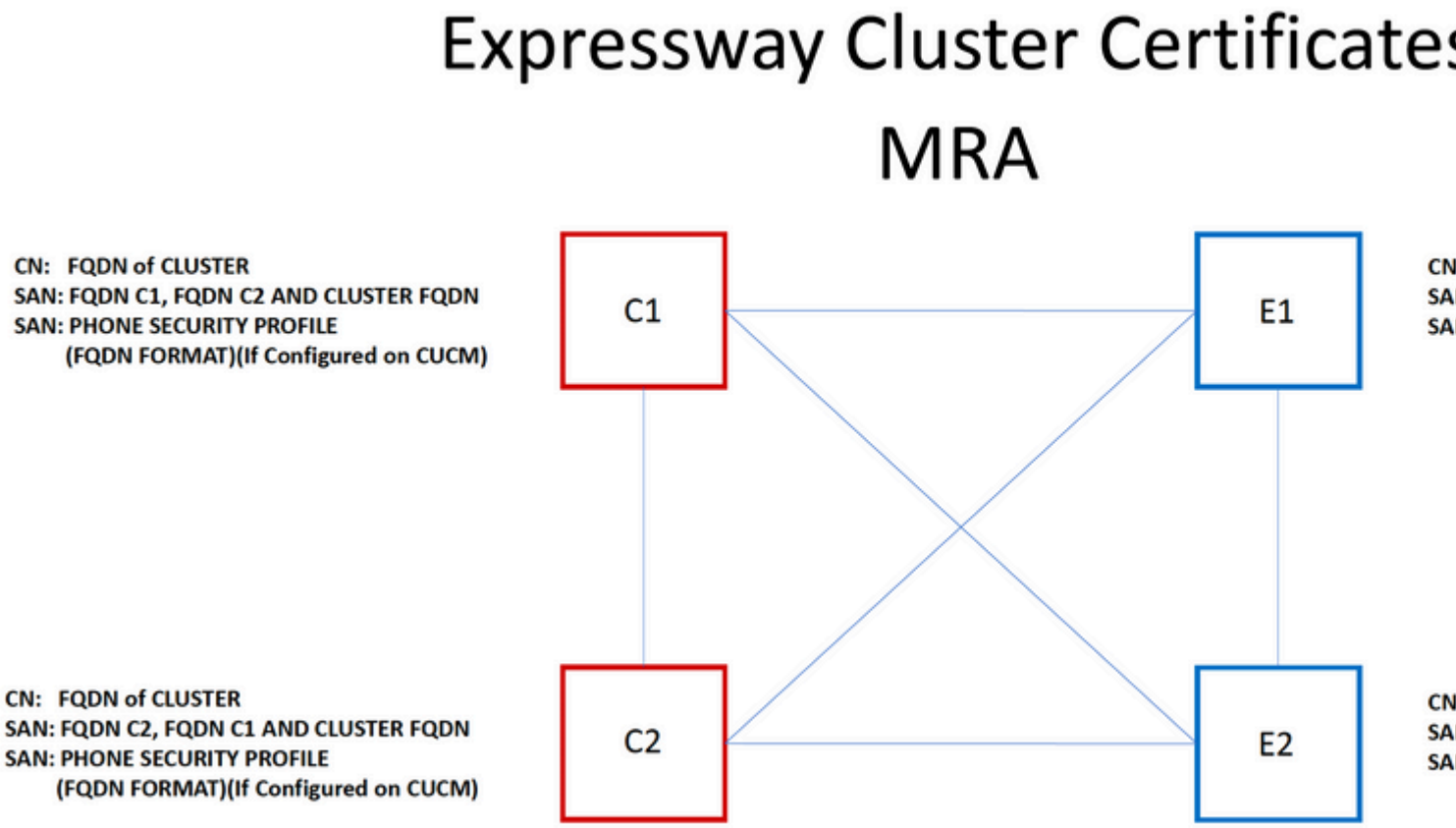
Überlegungen zum Expressway-C- und Expressway-E-Cluster

Cluster-Zertifikate

Wenn Sie einen Cluster von Expressway-C- oder Expressway-E-Servern zur Redundanz haben, wird dringend empfohlen, für jeden Server einen separaten CSR zu generieren, der von einer Zertifizierungsstelle signiert wird. Im vorherigen Szenario wäre der Common Name (CN) jedes Peers-Zertifikats derselbe vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) des Clusters, und die SANs wären der FQDN des Clusters und der entsprechende FQDN des Peers, wie im folgenden Bild gezeigt:



Sie können den Cluster-FQDN als CN verwenden, und jeder Peer-FQDN und der Cluster-FQDN im SAN kann dasselbe Zertifikat für alle Knoten im Cluster verwenden. So vermeiden Sie die Kosten mehrerer Zertifikate, die von einer öffentlichen Zertifizierungsstelle signiert werden.



> **Hinweis**: Die Namen der Telefonsicherheitsprofile im CS-Zertifikat sind nur erforderlich, wenn Sie Secure Phone Security Profiles (Sichere Telefonsicherheitsprofile) für UCM verwenden. Die externe Domäne oder collab-edge.example.com (example.com ist Ihre Domäne) ist nur für die Registrierung von IP-Telefonen und TC-Endgeräten über MRA erforderlich. Dies ist bei der Jabber-Registrierung über MRA optional. Andernfalls wird Jabber aufgefordert, das Zertifikat zu akzeptieren, wenn sich Jabber über MRA anmeldet.

Wenn es absolut notwendig ist, kann dies mit dem nächsten Prozess durchgeführt werden, oder Sie können OpenSSL verwenden, um sowohl den privaten Schlüssel als auch CSR manuell zu generieren:

Schritt 1: Generieren Sie einen CSR auf dem primären Cluster, und konfigurieren Sie ihn so, dass der Cluster-Alias als CN aufgeführt wird. Fügen Sie alle Peers im Cluster als alternative Namen sowie alle anderen erforderlichen SANs hinzu.

Schritt 2: Signieren Sie diese CSR-Anfrage, und laden Sie sie auf den primären Peer hoch.

Schritt 3: Melden Sie sich beim primären System als root an, und laden Sie den privaten Schlüssel unter /Tandberg/persistent/certs herunter.

Schritt 4: Laden Sie das signierte Zertifikat und den zugeordneten privaten Schlüssel zu den Peers im Cluster hoch.

> **Hinweis**: Dies wird aus den folgenden Gründen nicht empfohlen:
> 1. Dies stellt ein Sicherheitsrisiko dar, da alle Peers denselben privaten Schlüssel verwenden. Wird einer dieser Server kompromittiert, kann der Angreifer den Datenverkehr aller Server entschlüsseln.

---

2. Wenn eine Änderung am Zertifikat vorgenommen werden muss, muss der gesamte Prozess erneut ausgeführt werden, anstatt eine einfache CSR-Generierung und -Signierung durchzuführen.

Listen vertrauenswürdiger Zertifizierungsstellen

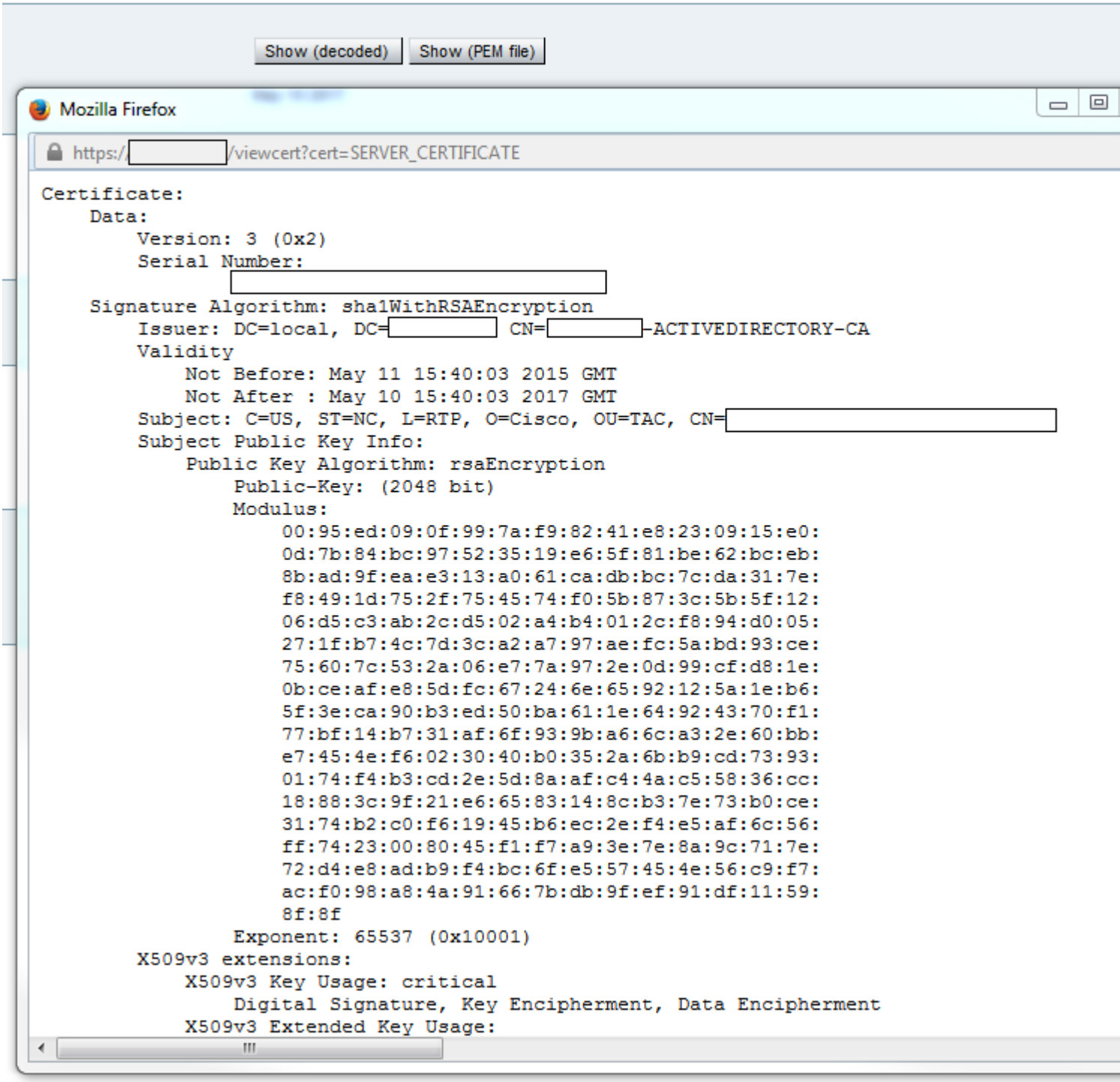
Anders als CUCM-Subscriber in einem Cluster wird die Liste der vertrauenswürdigen CAs NICHT von einem Peer zum anderen in einem Expressway- oder VCS-Cluster repliziert. Das bedeutet, dass Sie, wenn Sie über einen Cluster verfügen, vertrauenswürdige Zertifikate manuell in die Zertifizierungsstellenliste jedes Peers hochladen müssen.

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfen der aktuellen Zertifikatinformationen

Es gibt verschiedene Möglichkeiten, die Informationen in einem vorhandenen Zertifikat zu überprüfen. Die erste Option ist über den Webbrowser. Verwenden Sie die im vorherigen Abschnitt beschriebene Methode, mit der Sie auch ein bestimmtes Zertifikat in die Kette exportieren können. Wenn Sie SANs oder andere dem Expressway-Serverzertifikat hinzugefügte Attribute überprüfen müssen, können Sie dies direkt über die grafische Web-Benutzeroberfläche (GUI) tun. Navigieren Sie zu **Maintenance > Security Certificates > Server Certificate,** und klicken Sie dann auf **Show Decoded (Dekodiert anzeigen)**.

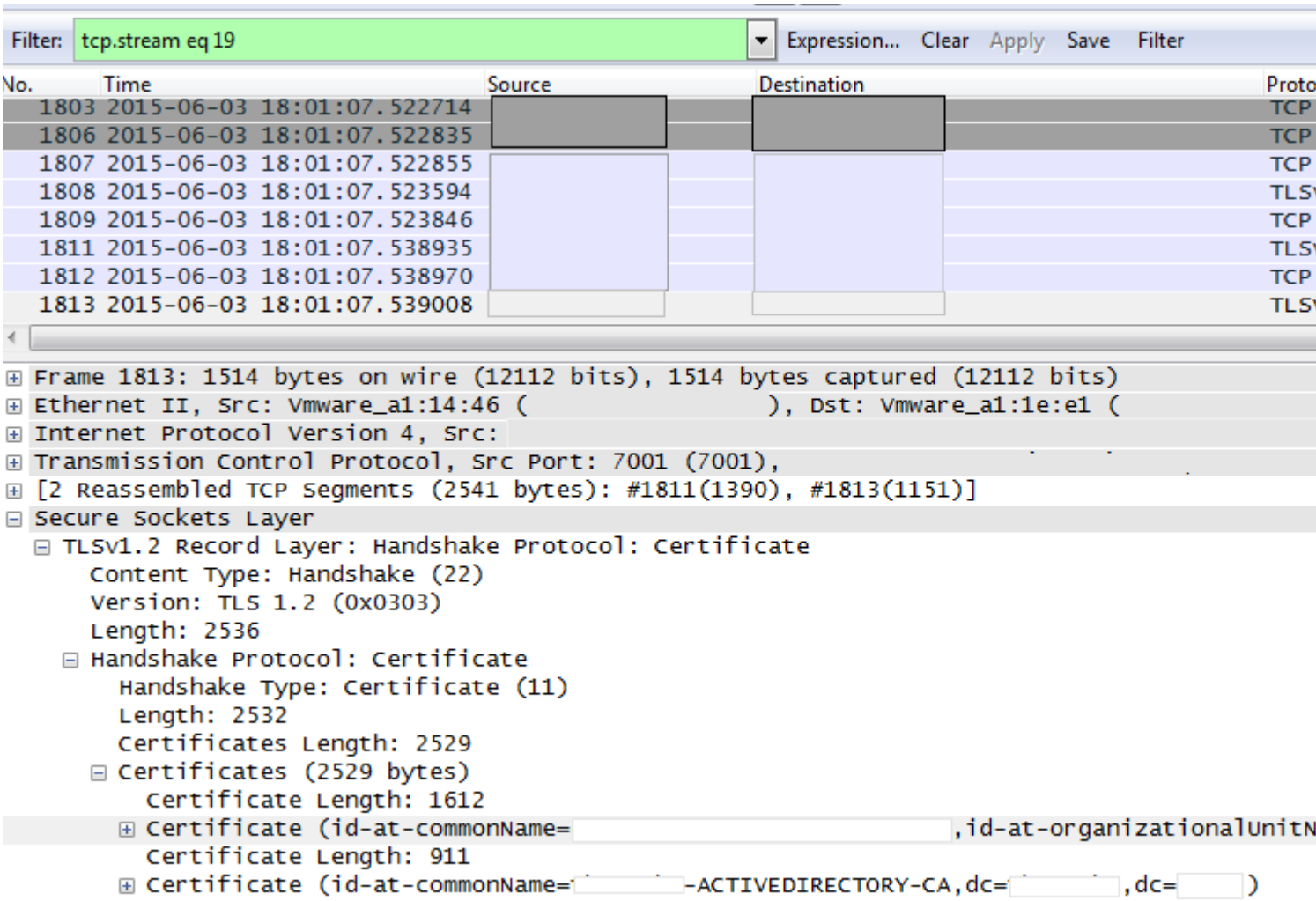


Hier können Sie alle spezifischen Details des Zertifikats sehen, ohne es herunterladen zu müssen. Sie können dies auch für einen aktiven CSR tun, wenn das zugehörige signierte Zertifikat noch nicht hochgeladen wurde.

Lesen/Exportieren eines Zertifikats in Wireshark

Wenn Sie eine Wireshark-Erfassung des SSL-Handshakes haben, der den Zertifikataustausch beinhaltet, kann Wireshark das Zertifikat für Sie decodieren, und Sie können alle Zertifikate in der Kette (wenn die gesamte Kette ausgetauscht wird) von innen exportieren. Filtern Sie die Paketerfassung für den spezifischen Port des Zertifikataustauschs (im Falle der Überbrückungszone in der Regel 7001). Wenn Sie als Nächstes die Hello-Pakete von Client und Server und den SSL-Handshake nicht sehen, klicken Sie mit der rechten

Maustaste auf eines der Pakete im TCP-Stream, und wählen Sie **Decodieren als aus**. Wählen Sie hier **SSL aus**, und klicken Sie auf **Apply**. Wenn Sie jetzt den richtigen Datenverkehr erfasst haben, müssen Sie den Zertifikataustausch sehen. Sucht das Paket vom richtigen Server, der das Zertifikat in der Nutzlast enthält. Erweitern Sie den SSL-Abschnitt im unteren Bereich, bis die Liste der Zertifikate angezeigt wird, wie im Bild gezeigt:



Hier können Sie jedes Zertifikat erweitern, um alle Details anzuzeigen. Wenn Sie das Zertifikat exportieren möchten, klicken Sie mit der rechten Maustaste auf das gewünschte Zertifikat in der Kette (falls mehrere vorhanden sind), und wählen Sie **Ausgewählte Paketbytes exportieren aus**. Geben Sie einen Namen für das Zertifikat ein, und klicken Sie auf **Speichern**. Nun müssen Sie das Zertifikat in der Windows-Zertifikatanzeige öffnen (wenn Sie ihm die Erweiterung .cer zuweisen) oder es zu Analysezwecken in ein anderes Tool hochladen können.

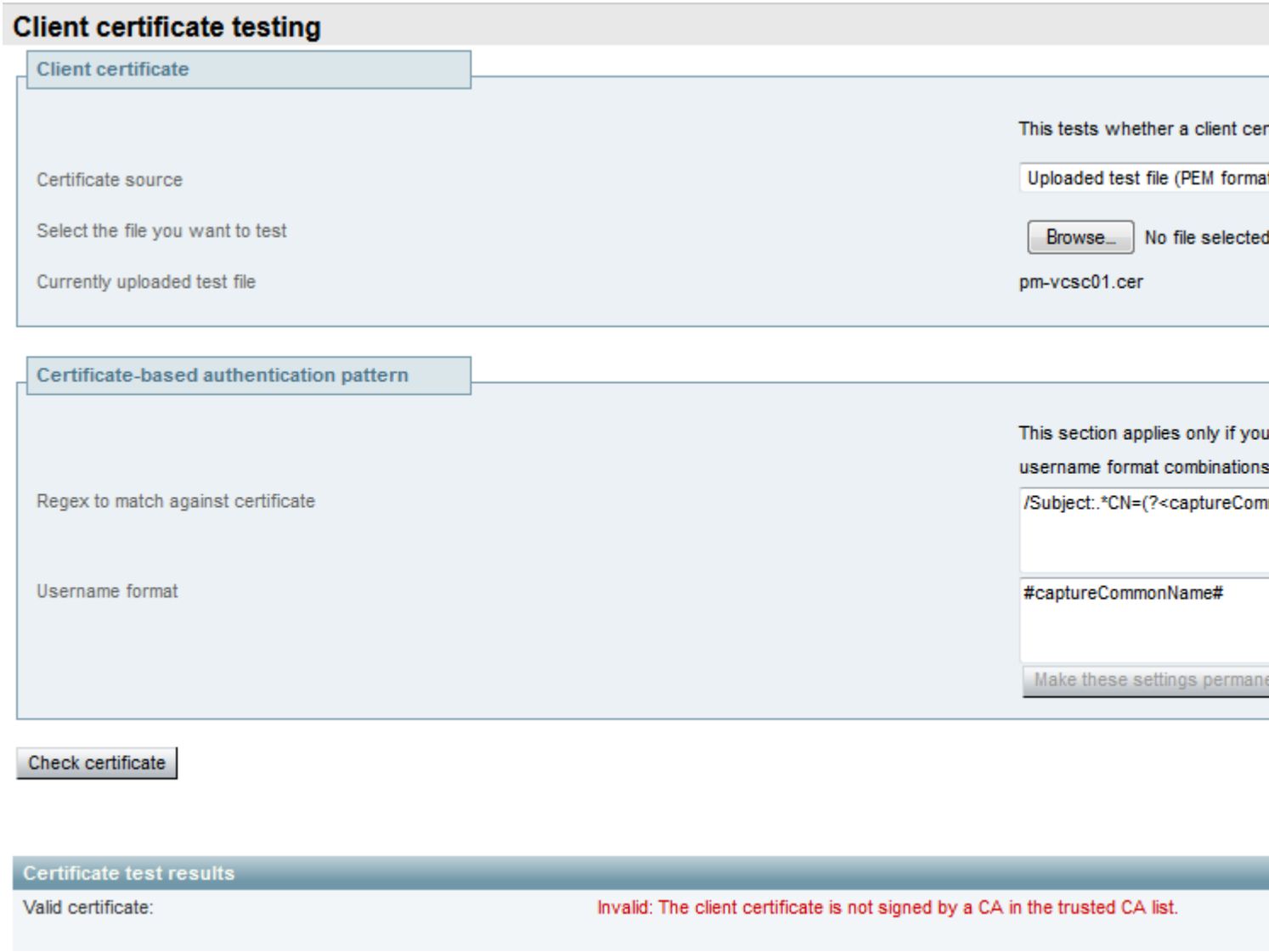
Fehlerbehebung

In diesem Abschnitt finden Sie die Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

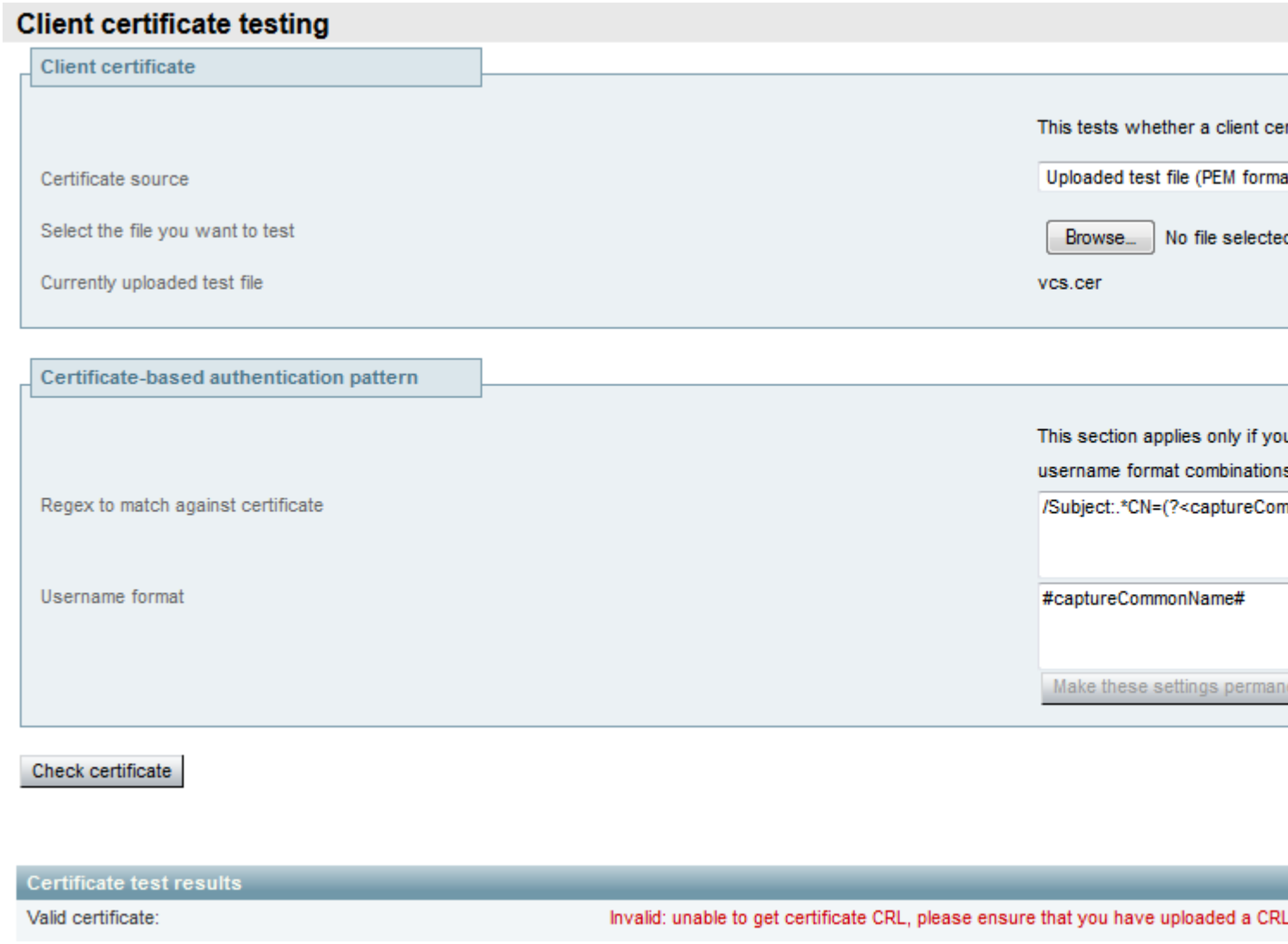
Überprüfen, ob ein Zertifikat auf dem Expressway vertrauenswürdig ist

Die beste Methode besteht darin, die Zertifikatskette manuell zu überprüfen und sicherzustellen, dass alle Mitglieder in der Liste der vertrauenswürdigen Zertifizierungsstellen von Expressway enthalten sind. Sie können jedoch schnell überprüfen, ob Expressway mithilfe des **Clientzertifikattests** unter **Wartung >**

Sicherheitszertifikate in der Web-GUI dem Zertifikat eines bestimmten Clients vertraut. Lassen Sie alle Standardeinstellungen unverändert. Wählen Sie im Dropdown-Menü die Option **Testdatei hochladen** (PEM-Format) aus, und wählen Sie das zu überprüfende Clientzertifikat aus. Wenn das Zertifikat nicht vertrauenswürdig ist, erhalten Sie, wie im Bild gezeigt, einen Fehler, der den Grund für die Ablehnung erklärt. Der Fehler, den Sie sehen, ist die decodierte Information des hochgeladenen Zertifikats als Referenz.



Wenn Sie einen Fehler erhalten, der behauptet, dass Expressway die Zertifikatsperrliste nicht abrufen kann, aber Expressway die Sperrlistenprüfung nicht verwendet, bedeutet dies, dass das Zertifikat vertrauenswürdig wäre und alle anderen Verifizierungsprüfungen bestanden hat.



Synergy Light-Endgeräte (Telefone der Serien 7800/8800)

Diese neuen Geräte werden mit einer vorab ausgefüllten Zertifikatsvertrauensliste ausgeliefert, die eine große Anzahl bekannter öffentlicher Zertifizierungsstellen enthält. Diese Vertrauensliste kann nicht geändert werden, d. h. Ihr Expressway-E-Zertifikat MUSS von einer dieser übereinstimmenden öffentlichen Zertifizierungsstellen signiert werden, damit Sie mit diesen Geräten arbeiten können. Wenn sie von einer internen oder einer anderen öffentlichen Zertifizierungsstelle signiert wird, schlägt die Verbindung fehl. Es gibt keine Option für den Benutzer, das Zertifikat manuell zu akzeptieren, wie dies bei Jabber-Clients der Fall ist.

Hinweis: Für einige Bereitstellungen wurde festgestellt, dass die Verwendung eines Geräts wie Citrix NetScaler mit einer CA aus der Liste auf den Telefonen der 7800/8800-Serie über MRA registriert werden kann, auch wenn Expressway-E eine interne CA verwendet. Die NetScalers-Stammzertifizierungsstelle muss in Expressway-E hochgeladen werden, und die interne Stammzertifizierungsstelle muss in Netscaler hochgeladen werden, damit die SSL-Authentifizierung funktioniert. Dies hat sich als funktionierend erwiesen und ist bestmögliche Unterstützung.

Hinweis: Wenn die Liste der vertrauenswürdigen Zertifizierungsstellen alle richtigen Zertifikate enthält, aber dennoch abgelehnt wird, stellen Sie sicher, dass sich in der Liste kein weiteres Zertifikat

---

mit demselben Betreff befindet, das mit dem richtigen Zertifikat kollidieren könnte. Wenn alles andere fehlschlägt, können Sie die Kette immer direkt aus dem Browser oder Wireshark exportieren und alle Zertifikate auf die gegenüberliegende Liste der Serverzertifizierungsstellen hochladen. Dies würde garantieren, dass es sich um das vertrauenswürdige Zertifikat handelt.

Hinweis: Wenn Sie ein Problem mit einer Traversal-Zone beheben, kann das Problem manchmal als zertifikatsbezogen erscheinen, es ist jedoch etwas softwareseitiges. Stellen Sie sicher, dass der Benutzername und das Passwort für das Traversal richtig sind.

Hinweis: Der VCS oder Expressway unterstützt maximal 999 Zeichen im SAN-Feld eines Zertifikats. SANs, die diesen Grenzwert überschreiten (was viele alternative Namen erfordert), werden ignoriert, als wären sie nicht vorhanden.

Videoressourcen

In diesem Abschnitt finden Sie im Video Informationen, die Sie durch alle Zertifikatkonfigurationsprozesse führen können.

CSR für MRA oder geclusterte Expressways generieren

Serverzertifikat auf Expressway installieren

So konfigurieren Sie die Zertifikatvertrauensstellung zwischen Expressways

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.