コラボレーション エッジ（MRA）証明書の設定とトラブルシューティング

内容

はじめに

このドキュメントでは、モバイルリモートアクセス(MRA)導入に関する証明書について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

パブリック認証局（CA）とプライベート認証局の比較

Expressway-C および E サーバでの証明書への署名では、いくつかのオプションがあります。証明書署名要求(CSR)をGoDaddy、Verisignなどのパブリックで署名するように選択するか、または独自の認証局（OpenSSLを使用して自己署名するか、Microsoft Windowsサーバなどの内部エンタープライズCA）を使用している場合は、内部的に署名することができます。 これらの方法で使用されるCSRの作成方法と署名方法の詳細については、『Video Communication Server(VCS)証明書作成ガイド』を参照してください。

実際にパブリック CA による署名を必要とするサーバは Expressway-E のみです。 これは、クライアントがMRA経由でサインインするときに証明書を参照する唯一のサーバです。したがって、ユーザが手動で証明書を受け入れる必要がないことを保証するためにパブリックCAを使用します。 Expressway-Eは内部CA署名付き証明書を使用できますが、初めて使用するユーザには信頼できない証明書を受け入れるように求められます。7800および8800シリーズの電話機のMRA登録は、証明書信頼リストを変更できないため、内部証明書では機能しません。 説明を簡単にするため、Expressway-C証明書とExpressway-E証明書の両方を同じCAで署名することを推奨します。ただし、両方のサーバで信頼済みCAリストを適切に設定していれば、これは必須ではありません。

証明書チェーンの仕組み

証明書は、サーバの証明書に署名した発行元の検証に使用される2つ以上の証明書のチェーンでリンクされます。 チェーンには、クライアント/サーバ証明書、中間証明書（場合によっては）、ルート証明書（証明書に署名した最上位レベルの認証局であるため、ルートCAとも呼ばれます）の3種類の証明書があります。

証明書には、チェーンを構築する2つの主なフィールドであるサブジェクトと発行者が含まれます。

サブジェクトは、この証明書によって表されるサーバまたは認証局の名前です。Expressway-CまたはExpressway-E(またはその他のユニファイドコミュニケーション(UC)デバイス)の場合、これ

は完全修飾ドメイン名(FQDN)から構築されます。

発行者は、その特定の証明書を検証する認証局です。 誰でも証明書（最初に証明書を作成したサーバーを含む、自己署名証明書とも呼ばれる）に署名できるため、サーバーおよびクライアントは、本物と信頼する発行者またはCAのリストを持ちます。

証明書チェーンは、常に自己署名のトップレベル証明書またはルート証明書で終わります。 証明書階層を移動すると、各証明書にはサブジェクトに関連する異なる発行者が存在します。最終的には、サブジェクトと発行者が一致するルートCAが検出されます。これは、それが最上位レベルの証明書であり、したがって、クライアントまたはサーバの信頼済みCAリストによって信頼される必要がある証明書であることを示します。

SSL ハンドシェイクの概要

トラバーサルゾーンの場合、Expressway-Cは常にクライアントとして機能し、Expressway-Eは常にサーバとして機能します。 簡素化された交換は次のように機能します。

Expressway-C Expressway-E

---------クライアントHello-------->

<--------サーバHello---------

<----サーバ証明書-------

<----証明書要求 –

------クライアント証明書------>

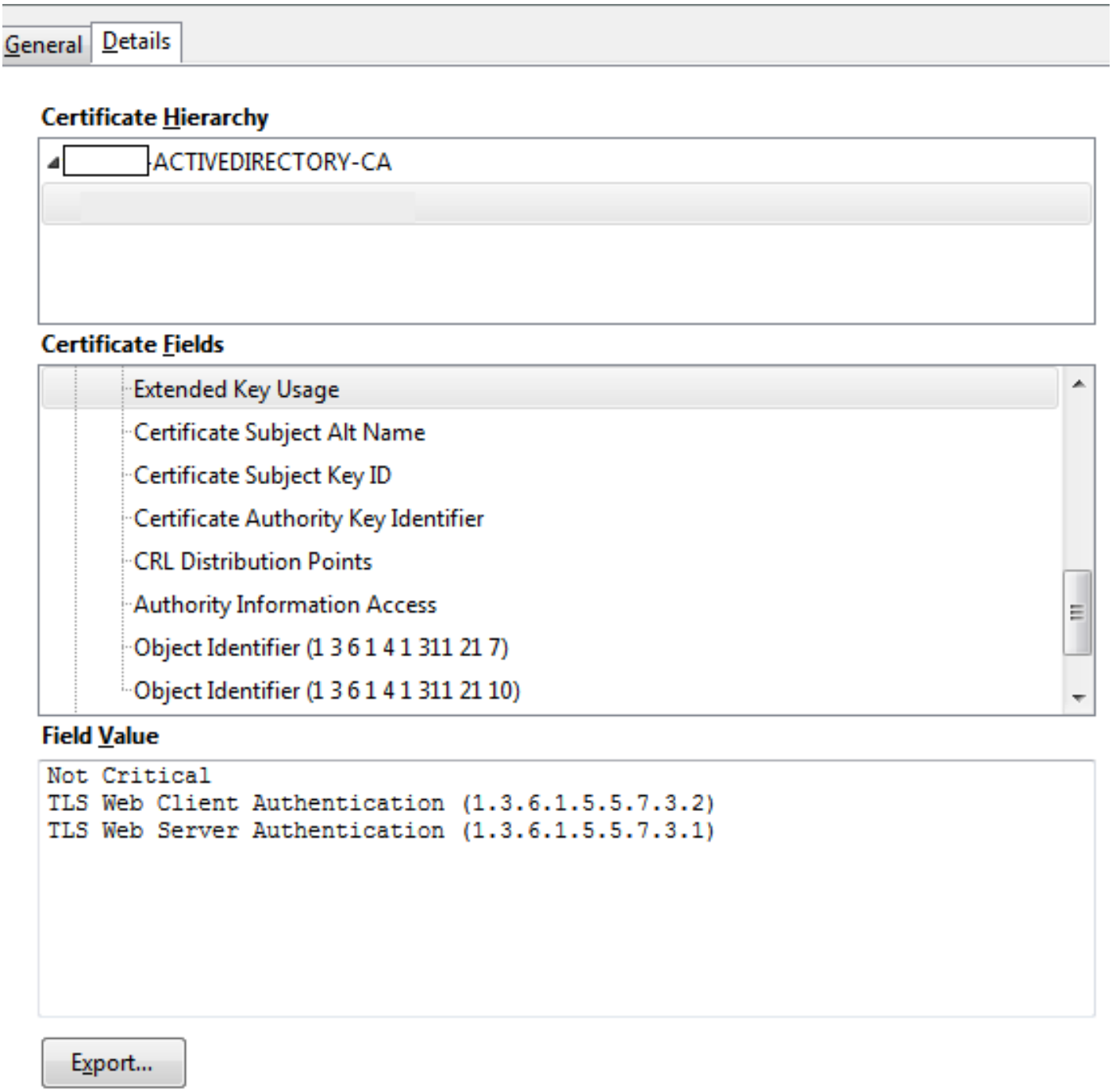
Expressway-Cは常に接続を開始し、常にクライアントであるため、ここでのキーは交換にあります。Expressway-Eは、自身の証明書を最初に送信するルータです。Expressway-Cがこの証明書を検証できない場合、ハンドシェイクを切断して自身の証明書をExpressway-Eに送信することはできません。

また、証明書に含まれている、 Transport Layer Security（TLS）Web クライアント認証および TLS Web サーバ認証の属性も重要です。これらの属性は、CSRに署名したCA上で決定され（Windows CAを使用する場合、選択したテンプレートによって決定されます）、証明書がクライアントまたはサーバ（あるいはその両方）の役割で有効であるかどうかが示されます。VCSまたはExpresswayの場合は、状況に基づいて設定でき（トラバーサルゾーンの場合は常に同じ）、証明書にクライアントとサーバの両方の認証属性が含まれている必要があります。

Expressway-CとExpressway-Eの両方が適用されていない場合、新しいサーバ証明書にアップロードすると エラーが表示されます。

証明書にこれらの属性があるかどうかわからない場合は、ブラウザまたはOSで証明書の詳細を開き、「拡張キー使用法」セクションを確認します（図を参照）。 形式は、証明書の表示方法によって異なる場合があります。

以下に例を挙げます。



設定

Expressway-C および Expressway-E トラバーサル ゾーン/信頼

CSR の生成と署名

前述のように、Expressway-CおよびExpressway-E証明書は、内部または外部CAによって、または自己署名のためにOpenSSLによって署名される必要があります。

注:Expresswayサーバに付属する一時証明書はサポートされていないため、使用できません。CA署名証明書があり、件名行が明確に定義されていないワイルドカード証明書を使用す

る場合、その証明書はサポートされません。

最初のステップとして、CSR を生成し、優先する CA タイプによる署名を行います。このプロセスの詳細については、『証明書作成ガイド』を参照してください。CSRを作成する際には、証明書に含める必要があるサブジェクト代替名(SAN)を覚えておくことが重要です。SAN は証明書ガイドおよび『モバイル リモート アクセス導入ガイド』にも記載されています。新機能の追加が可能な最新バージョンのガイドを確認してください。使用されている機能に基づいて、含める必要がある一般的なSANのリスト：

Expressway-C

- ドメインリストに追加されたドメイン（内部または外部）。
- XMPPフェデレーションが使用されている場合は、すべての常設チャットノードのエイリアス。
- セキュアデバイスプロファイルを使用している場合は、CUCMでデバイスプロファイル名を保護します。

Expressway-E

- Expressway-C で設定されたすべてのドメイン
- XMPPフェデレーションが使用されている場合は、すべての常設チャットノードのエイリアス。
- XMPP フェデレーション用にアドバタイズされたすべてのドメイン。

注：外部サービスレコード(SRV)ルックアップに使用されるベースドメインがExpressway-E証明書(xxx.comまたはcollab-edge.xxx.com)にSANとして含まれていない場合でも、Jabberクライアントはエンドユーザに最初の接続で証明書を受け入れる必要があり、TCエンドポイントは接続に失敗します。

Expressway-CとExpressway-Eが互いを信頼するように設定する

ユニファイドコミュニケーションのトラバーサルゾーンで接続を確立するには、Expressway-CとExpressway-Eが互いの証明書を信頼する必要があります。この例では、Expressway-E証明書がこの階層を使用するパブリックCAによって署名されていると仮定します。

証明書 3

発行者： GoDaddyルートCA

件名： GoDaddyルートCA

証明書 2

発行者： GoDaddyルートCA

件名：GoDaddy中間認証局

証明書 1

発行者：GoDaddy中間認証局

件名：Expressway-E.lab

Expressway-Cは、信頼証明書1を使用して設定する必要があります。ほとんどの場合、サーバに適用された信頼できる証明書に基づいて、サーバは最も低いレベルのサーバ証明書のみを送信します。 つまり、Expressway-Cが証明書1を信頼するためには、証明書2と3の両方をExpressway-Cの信頼済みCAリスト(メンテナンス>セキュリティ>信頼済みCAリスト)にアップロードする必要があります。 Expressway-CがExpressway-E証明書を受信するときに中間証明書2を省略すると、信頼されたGoDaddyルートCAに関連付ける方法がないため、拒否されます。

証明書 3

発行者： GoDaddyルートCA

件名： GoDaddyルートCA

証明書 1

発行者： GoDaddy中間認証局 – 信頼されていません！

件名：Expressway-E.lab

さらに、ルートのない中間証明書のみをExpressway-Cの信頼されたCAリストにアップロードすると、GoDaddy中間認証局は信頼されているようですが、より高い認証局によって署名されています。この場合、信頼されていないGoDaddyルートCAは失敗します。

証明書 2

発行者： GoDaddyルートCA – 信頼されていません！

件名：GoDaddy中間認証局

証明書 1

発行者：GoDaddy中間認証局

件名：Expressway-E.lab

すべての中間認証局とルートが信頼済み CA リストに追加されると、証明書を検証できます。

証明書 3

発行者： GoDaddyルートCA – 自己署名トップレベル証明書が信頼され、チェーンが完了しました。

件名： GoDaddyルートCA

証明書 2

発行者： GoDaddyルートCA

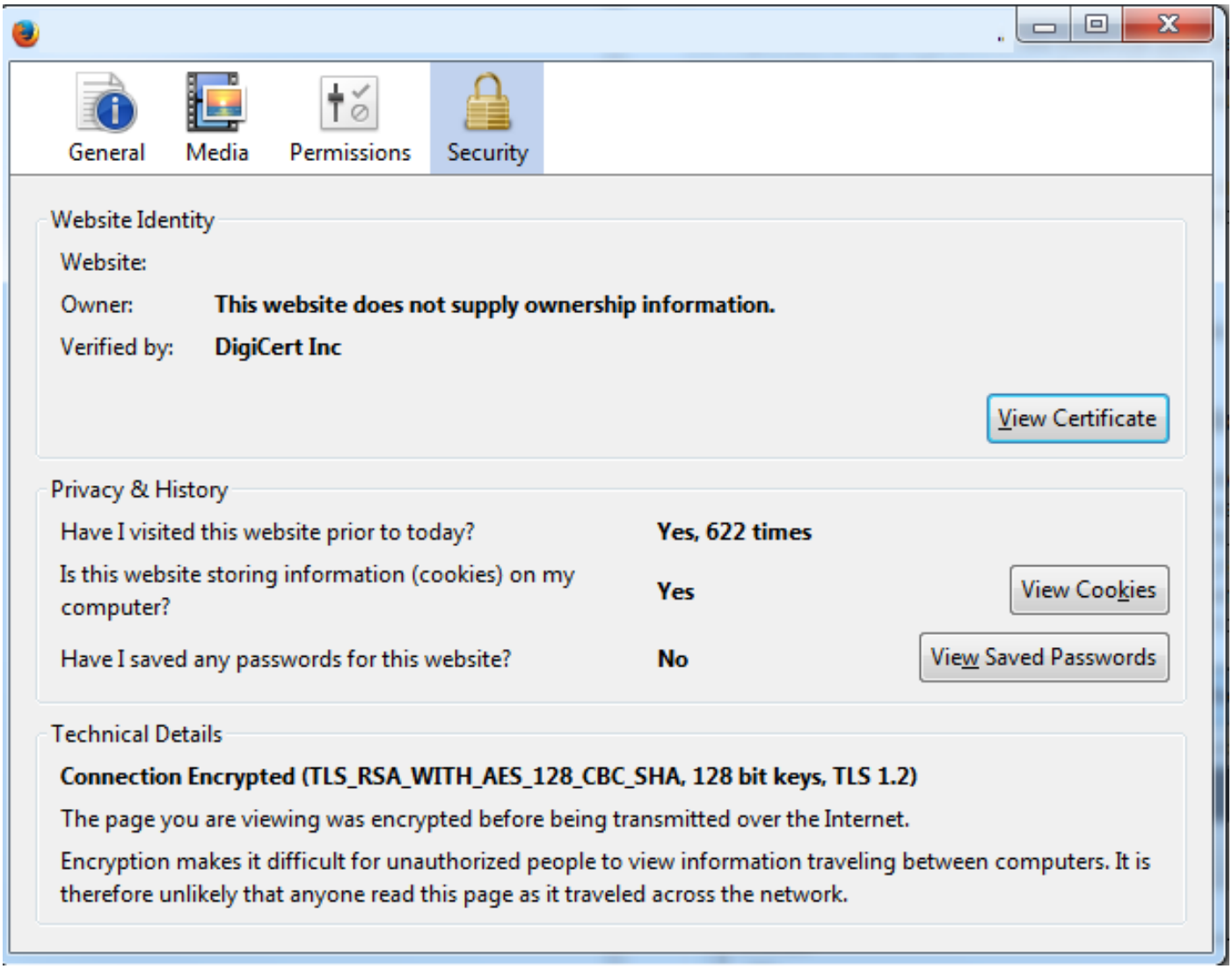
件名：GoDaddy中間認証局

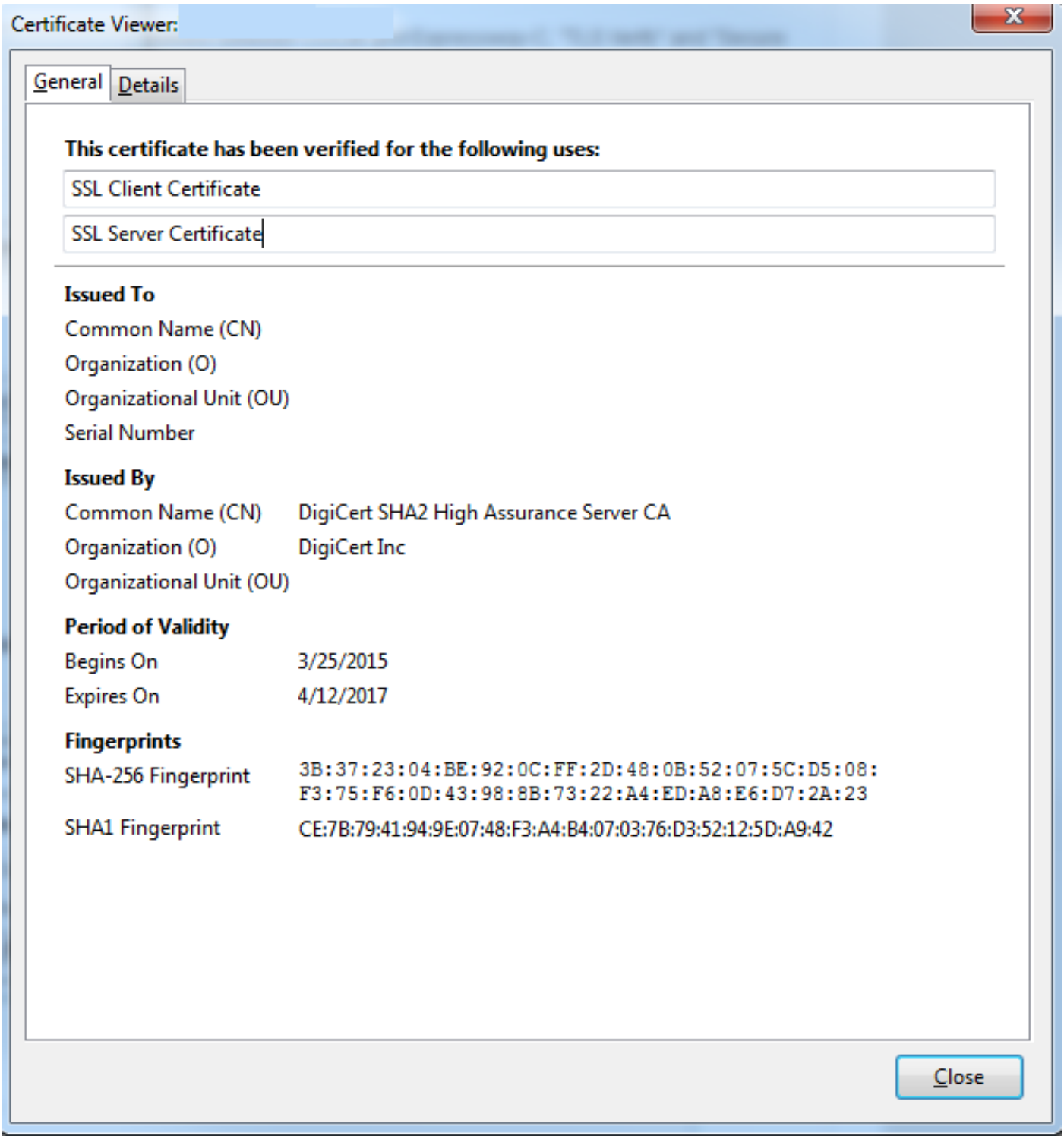
証明書 1

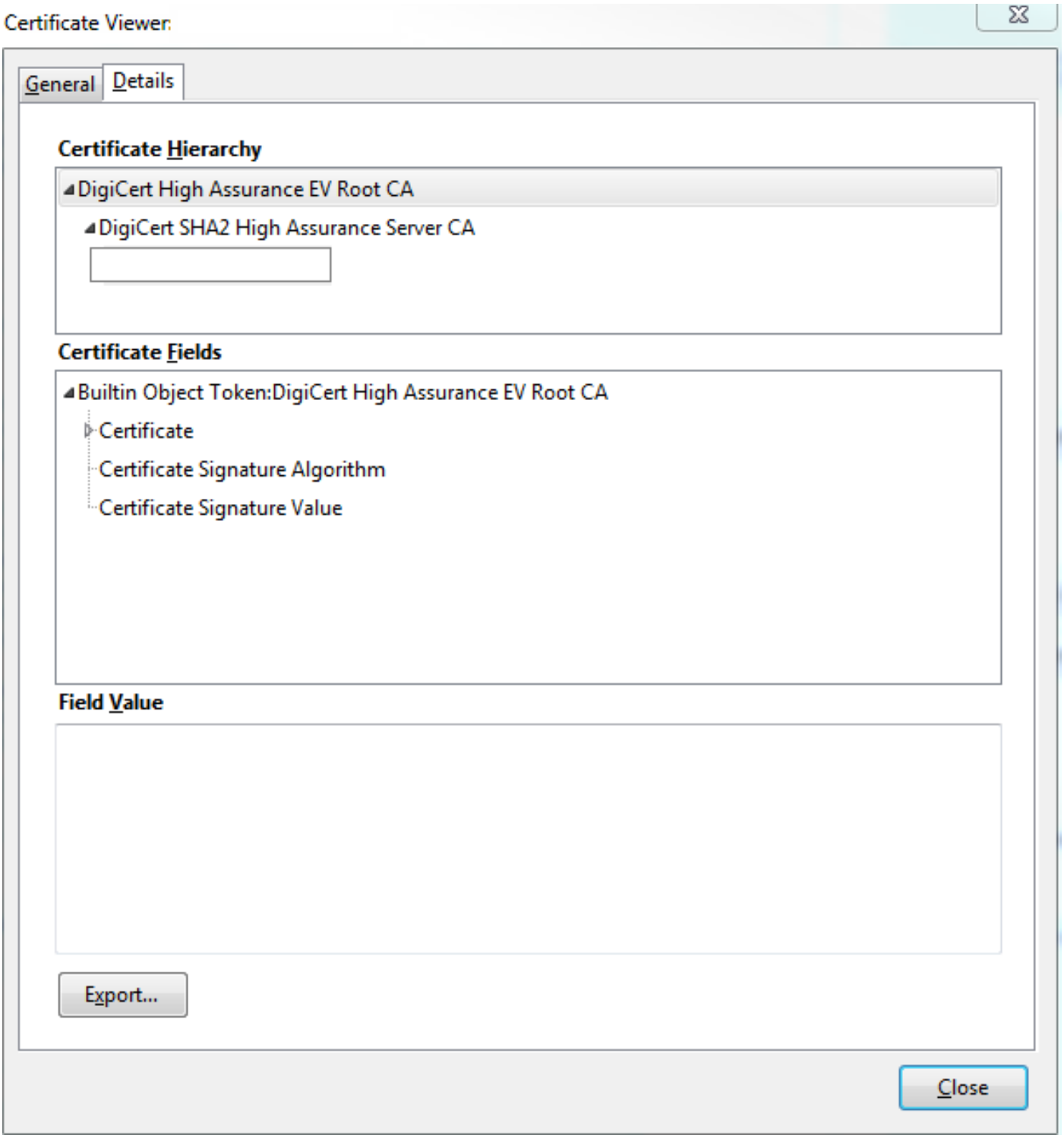
発行者：GoDaddy中間認証局

件名：Expressway-E.lab

証明書チェーンが不明な場合は、特定のExpresswayのWebインターフェイスにログインしたときにブラウザを確認できます。 プロセスはブラウザによって若干異なりますが、Firefoxでは、アドレスバーの左端にあるロックアイコンをクリックできます。 表示されるポップアップで、[詳細情報（More Information）] > [証明書の表示（View Certificate）] > [詳細（Details）] をクリックします。 ブラウザでチェーン全体を結合できる場合は、チェーンを上から下に表示できます。 トップレベル証明書に一致するサブジェクトと発行者がない場合、チェーンは完了していません。 必要な証明書を強調表示した状態でexportをクリックすると、チェーン内の各証明書を単独でエクスポートすることもできます。 これは、正しい証明書を CA の信頼リストに確実にアップロードしたかどうかわからない場合に役立ちます。


General
Media
Permissions
Security
Website Identity
Website:
Owner: This website does not supply ownership information.
Verified by: DigiCert Inc
View Certificate
Privacy & History
Have I visited this website prior to today? Yes, 622 times
Is this website storing information (cookies) on my computer? Yes
View Cookies
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.


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



Expressway-CがExpressway-Eからの証明書を信頼するようになったので、反対方向で動作することを確認します。Expressway-C証明書がExpressway-Eに署名したのと同じCAによって署名されている場合、プロセスは簡単です。Expressway-Eの信頼済みCAリストに、Cで実行したのと同じ証明書をアップロードします。 Cが別のCAによって署名されている場合は、図に示すように同じプロセスを使用する必要がありますが、代わりにExpressway-C証明書に署名したチェーンを使用します。

Cisco Unified Communications Manager（CUCM）と Expressway-C 間のセキュア通信

概要

Expressway-CとExpressway-E間のトラバーサルゾーンとは異なり、Expressway-CとCUCM間のセキュアなシグナリングは必要ありません。内部セキュリティポリシーで許可されていない場合を除き、この手順を続行する前に、最初にMRAをCUCM上の非セキュアなデバイスプロファイルで動作するように設定する必要があります。

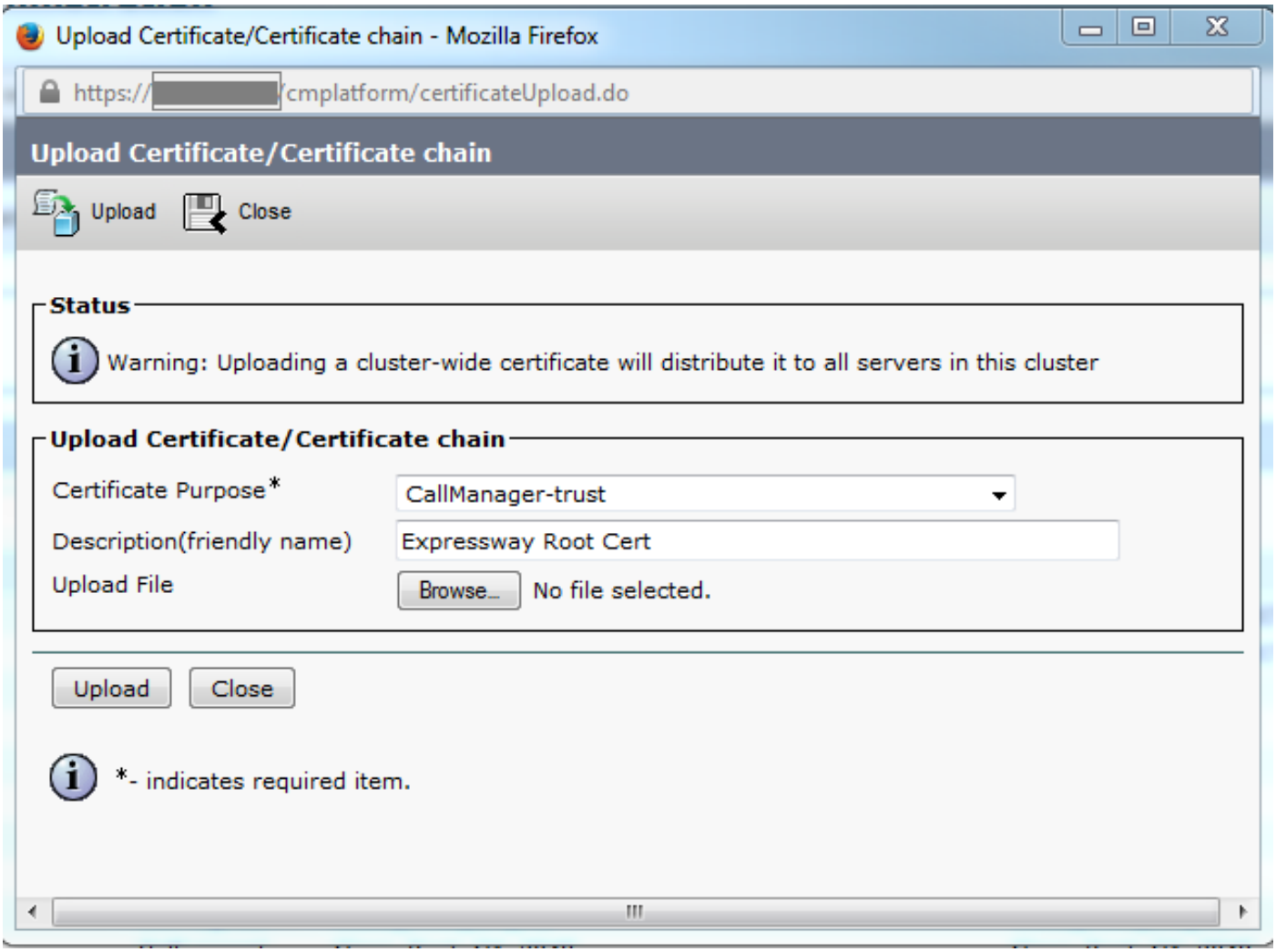
CUCMとExpressway-Cの間で有効にできる主なセキュリティ機能は、TLS検証とセキュアデバイス登録の2つです。 SSL ハンドシェイクにおいて CUCM 側からの 2 つの異なる証明書を使用するため、これら 2 つの機能には重要な違いがあります。

TLS 検証 - tomcat 証明書

セキュア SIP 登録 - callmanager 証明書

CUCMとExpressway-C間の信頼の設定

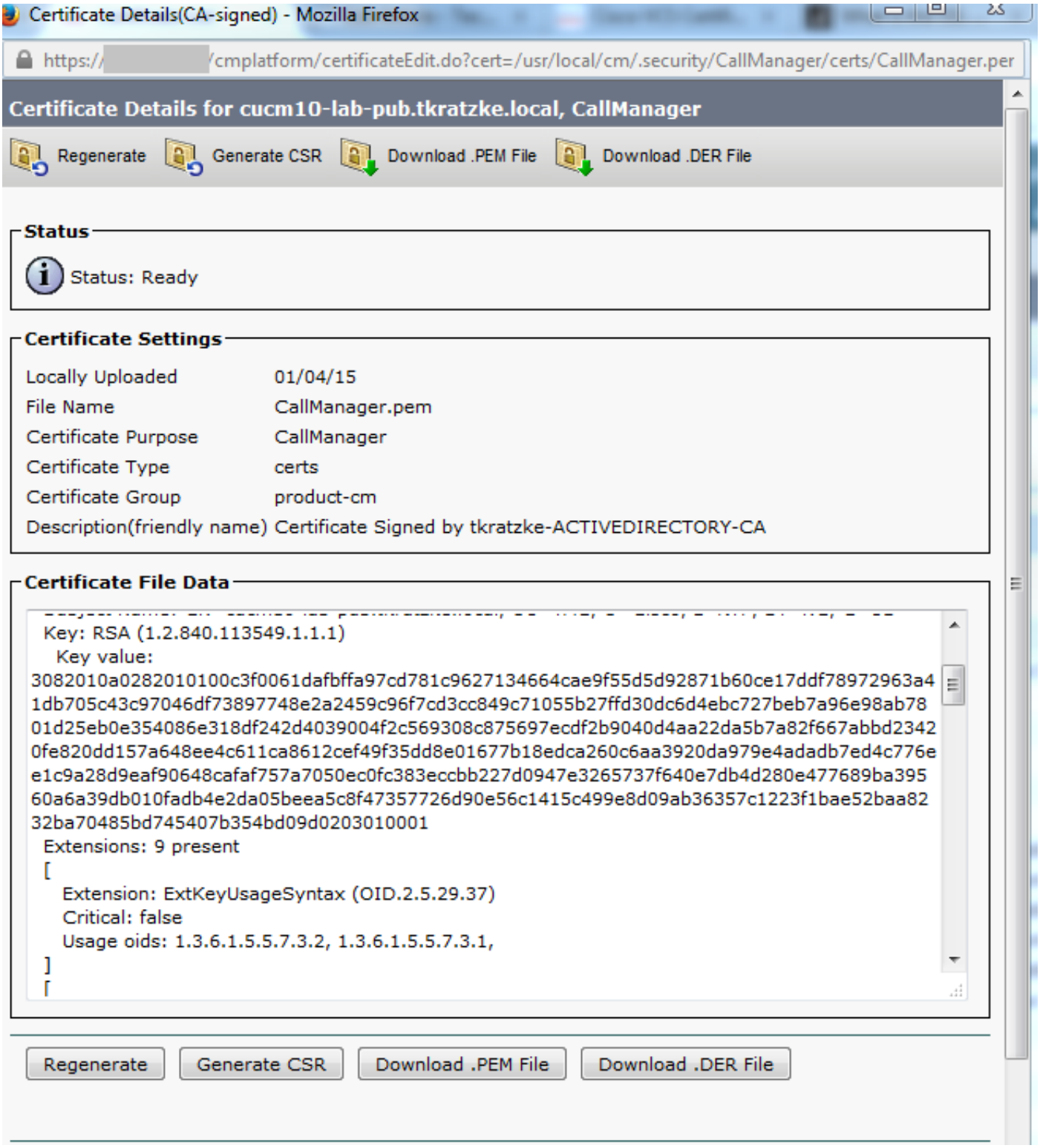
この場合の概念は、Expressway-CとExpressway-Eの間とまったく同じです。 最初に、CUCM が Expressway-C のサーバ証明書を信頼する必要があります。 つまり、CUCMでは、Expressway-Cの中間証明書とルート証明書を、TLS検証機能の場合はtomcat-trust証明書、セキュアなデバイス登録の場合はCallManager-trust証明書としてアップロードする必要があります。 これを行うには、CUCM Web GUIの右上にあるCisco Unified OS Administrationに移動し、Security> Certificate Managementの順に選択します。 ここでは、[証明書/証明書チェーンをアップロード（Upload Certificate/Certificate Chain）] をクリックして正しい信頼形式を選択するか、[検索（Find）] をクリックして現在アップロードされている証明書のリストを表示することができます。



Expressway-CがCUCM証明書に署名したCAを信頼していることを確認する必要があります。これを行うには、信頼済みCAリストにこれらの証明書を追加します。 ほとんどの場合、CAを使用してCUCM証明書に署名した場合、tomcat証明書とCallManager証明書は同じCAによって署名される必要があります。これらが異なる場合は、TLS検証とセキュア登録を使用する場合に両方を信頼する必要があります。

セキュアSIP登録の場合、デバイスに適用されるCUCMのセキュアデバイスプロファイル名がExpressway-C証明書にSANとしてリストされていることを確認する必要もあります。これがセキュア登録メッセージを含まない場合、CUCMからの403で失敗し、TLSの失敗を示します。

注：セキュアなSIP登録のためにCUCMとExpressway-Cの間でSSLハンドシェイクが発生する場合、2つのハンドシェイクが発生します。まず、Expressway-Cがクライアントとして動作し、CUCMとの接続を開始します。これが正常に完了すると、CUCMは応答するクライアントとして別のハンドシェイクを開始します。 つまり、Expressway-C の場合とまったく同様に、CUCM 上の callmanager 証明書で TLS Web クライアントと TLS Web サーバの両方の認証属性が適用されている必要があります。 違いは、CUCMではこれらの証明書を両方なしでアップロードでき、CUCMにサーバ認証属性しかない場合は、内部のセキュア登録が正常に動作することです。リストでCallManager証明書を探して選択すると、CUCMでこれを確認できます。 ここでは、Extensionセクションの下のUsage OIDを確認できます。Client Authenticationには1.3.6.1.5.5.7.3.2、Server Authenticationには1.3.6.1.5.5.7.3.1が表示されています。このウィンドウから証明書をダウンロードすることもできます。



注：クラスタ内のパブリッシャに適用される信頼証明書は、サブスクライバに複製する必要があります。新しい設定で個別にログインして確認することをお勧めします。

注:Expressway-CがCUCMからの証明書を正しく検証するには、CUCMサーバをIPアドレスではなくFQDNを使用してExpressway-Cに追加する必要があります。 IPアドレスが機能する唯一の方法は、各CUCMノードのIPが証明書にSANとして追加されている場合です。これは、ほとんど行われません。

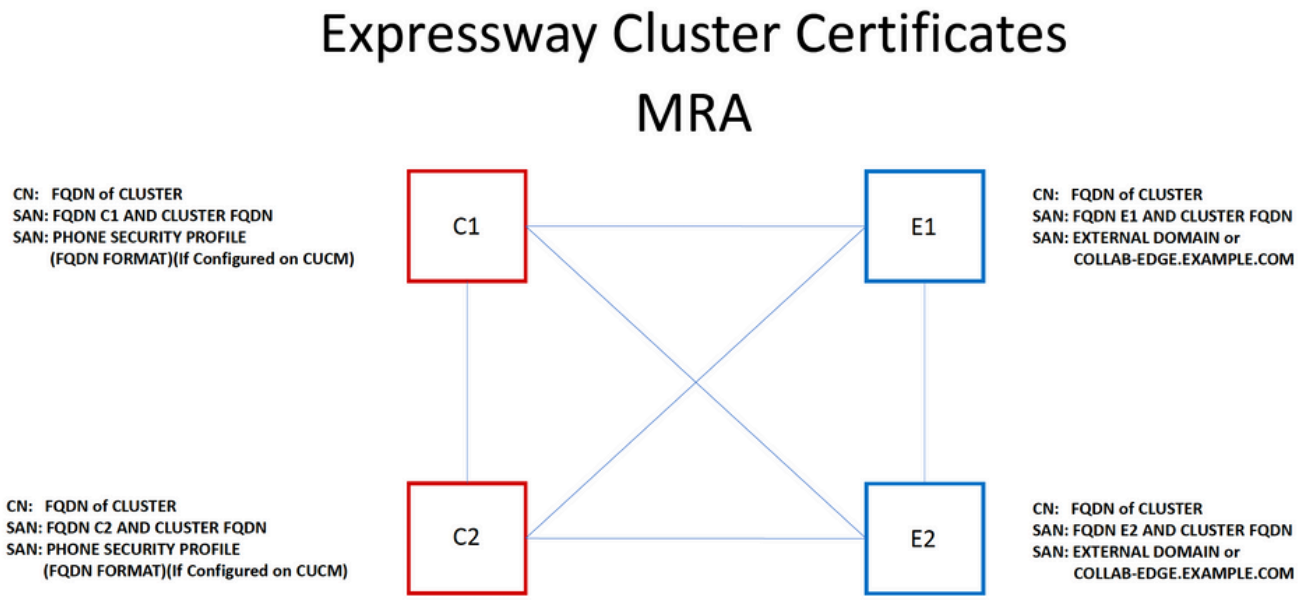
自己署名証明書を持つCUCMサーバ

デフォルトでは、CUCMサーバには自己署名証明書が付属しています。 これらが設定されている場合、TLS検証とセキュアデバイス登録の両方を同時に使用することはできません。 どちらの機能も単独で使用できますが、証明書は自己署名であるため、自己署名Tomcat証明書と自己署名CallManager証明書の両方をExpressway-Cの信頼済みCAリストにアップロードする必要があります。 Expressway-Cが自身の信頼リストを検索して証明書を検証する場合、サブジェクトが一致する証明書が見つかると停止します。このため、信頼リストでtomcatまたはCallManagerのどちらか上位にある機能が動作します。 低い方のAPは、存在しないかのように失敗します。 この問題を解決するには、CA（パブリックまたはプライベート）を使用して CUCM 証明書に署名し、その CA のみを信頼します。

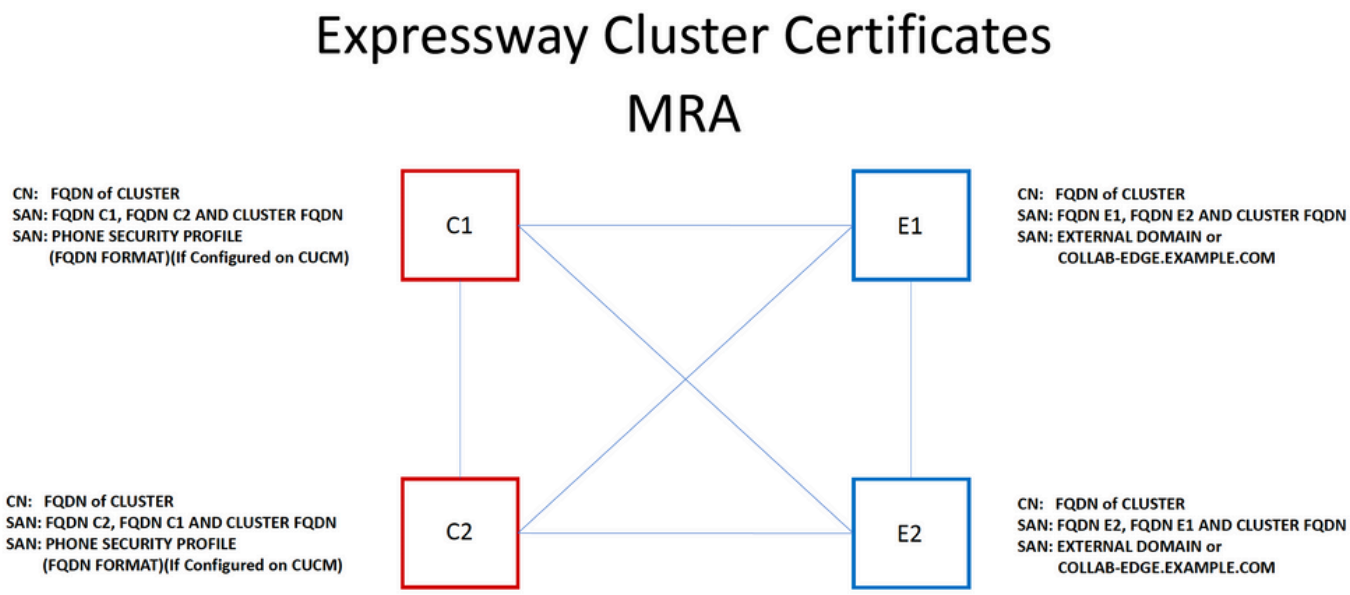
Expressway-C および Expressway-E クラスタの考慮事項

クラスタ証明書

冗長化の目的で Expressway-C サーバまたは Expressway-E サーバのクラスタを使用している場合は、サーバごとに個別の CSR を生成して CA による署名を行うことを強くお勧めします。前のシナリオでは、図に示すように、各ピア証明書の共通名(CN)は同じクラスタの完全修飾ドメイン名(FQDN)になり、SANはクラスタのFQDNとそれぞれのピアのFQDNになります。



クラスタFQDNをCNとして使用し、SAN内の各ピアのFQDNとクラスタFQDNを使用することで、クラスタ内のすべてのノードで同じ証明書を使用できるため、パブリックCAによって署名される複数の証明書のコストを回避できます。



注:Cs証明書の電話セキュリティプロファイル名が必要になるのは、UCMでセキュア電話セキュリティプロファイルを使用する場合だけです。外部ドメインまたはcollab-edge.example.com(example.comはユーザのドメイン)は、IP PhoneおよびTCエンドポイントをMRA経由で登録する場合にのみ必要です。これは、MRA経由のJabber登録ではオプションです。存在しない場合、JabberはMRA経由でログインするときに証明書を受け入れるように求めます。

どうしても必要な場合は、次のプロセスでこれを実行するか、OpenSSLを使用して秘密キーとCSRの両方を手動で生成できます。

手順1：クラスタのプライマリでCSRを生成し、クラスタエイリアスをCNとしてリストするように設定します。クラスタ内のすべてのピアを、他のすべての必要なSANとともに代替名として追加します。

ステップ2：このCSRに署名し、プライマリピアにアップロードします。

ステップ3：プライマリにrootとしてログインし、/Tandberg/persistent/certsにある秘密キーをダウンロードします。

ステップ4：署名付き証明書と一致した秘密キーの両方をクラスタ内の他のピアにアップロードします。

注：これは次の理由から推奨されません。
1.すべてのピアが同じ秘密キーを使用するため、セキュリティ上のリスクがあります。 何らかの方法で侵害された場合、攻撃者は任意のサーバからのトラフィックを復号化できます。
2.証明書を変更する必要がある場合は、単純なCSRの生成と署名ではなく、このプロセス全体を繰り返す必要があります。

信頼済み CA リスト

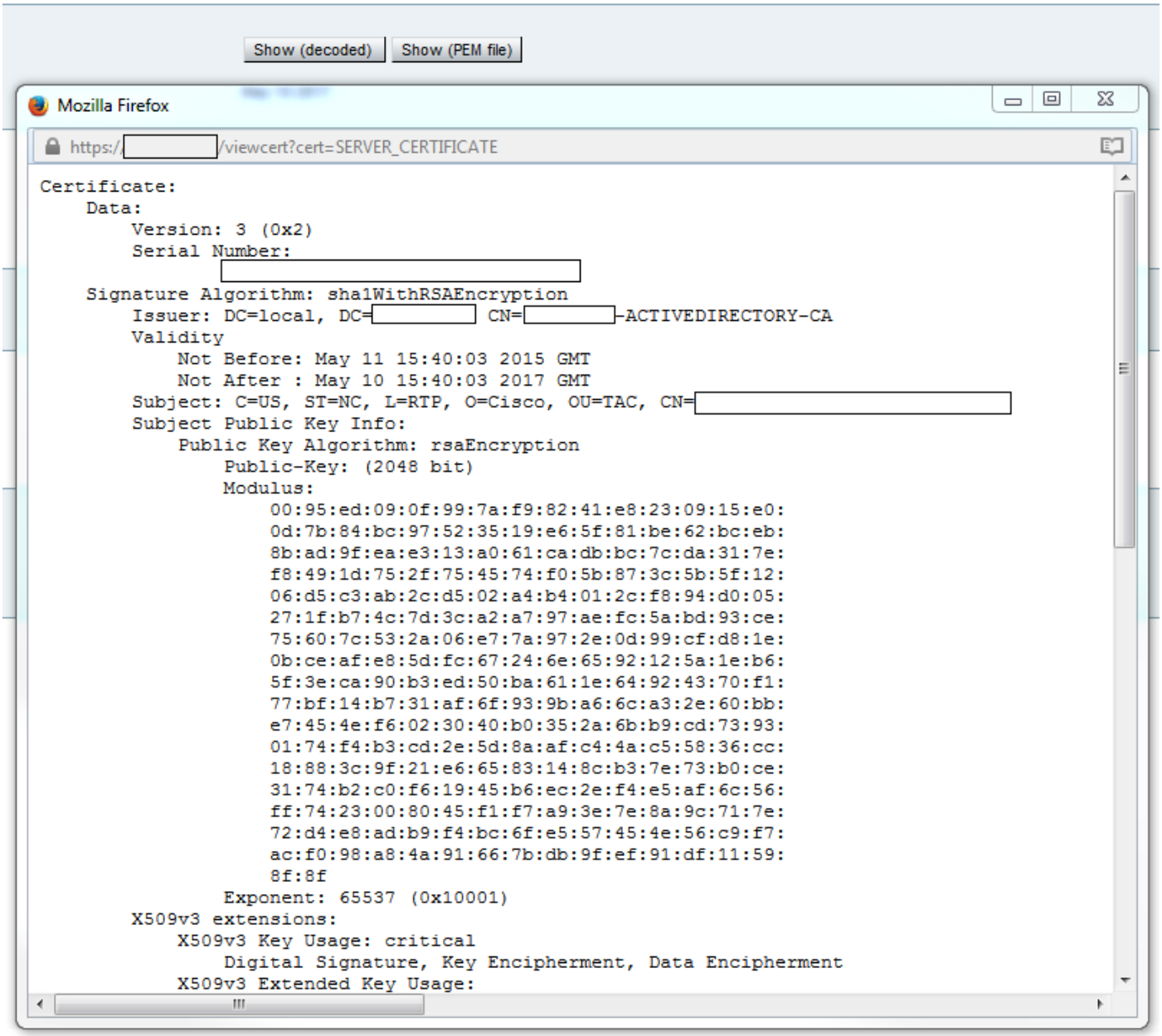
クラスタ内の CUCM サブスクライバとは異なり、Expressway または VCS クラスタ内のピア間で信頼済み CA リストは複製されません。 つまり、クラスタがある場合は、信頼できる証明書を各ピアのCAリストに手動でアップロードする必要があります。

確認

このセクションでは、設定が正常に動作していることを確認します。

現在の証明書情報の確認

既存の証明書の情報を確認するにはいくつかの方法があります。 最初のオプションは、Webブラウザを使用することです。前のセクションで説明した方法を使用します。この方法は、チェーン内の特定の証明書のエクスポートにも使用できます。 SAN、またはExpresswayサーバ証明書に追加されたその他の属性を確認する必要がある場合は、Web Graphical User Interface（GUI；グラフィカルユーザインターフェイス）を使用して直接確認できます。確認するには、Maintenance > Security Certificates > Server Certificateの順に移動し、Show Decodedをクリックします。

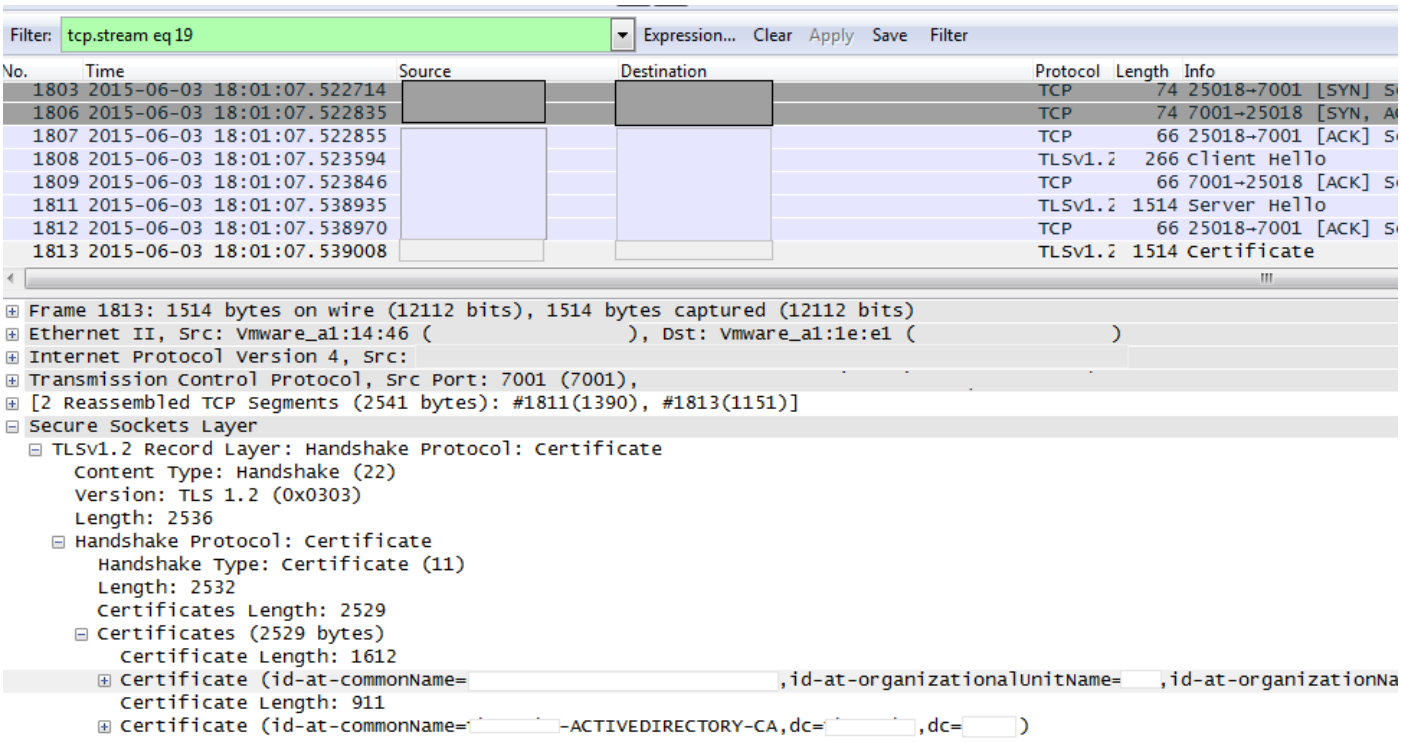


ここでは、証明書をダウンロードしなくても、証明書の特定の詳細をすべて確認できます。 アクティブな CSR についても、関連する署名済み証明書をまだアップロードしていなければ、同じ手順を実行できます。

Wiresharkでの証明書の読み取り/エクスポート

証明書交換を含むSSLハンドシェイクのWiresharkキャプチャがある場合、Wiresharkは実際に証明書を復号化でき、チェーン内のすべての証明書を内部からエクスポートできます（チェーン全体が交換されている場合）。 証明書の交換における特定のポート（トラバーサル ゾーンの場合は一般に 7001）について、パケット キャプチャをフィルタで絞り込みます。 次に、クライアントとサーバのhelloパケットがSSLハンドシェイクとともに表示されない場合、TCPストリーム内のパケットの1つを右クリックして、decode asを選択します。 ここで、SSLを選択して、applyをクリックします。 ここで、正しいトラフィックをキャプチャした場合は、証明書交換を確認する必要があります。 ペイロードに証明書が含まれている正しいサーバからのパケットを見つけます。 図に示すように、証明書のリストが表示されるまで、下部ペインのSSLセクションを

展開します。



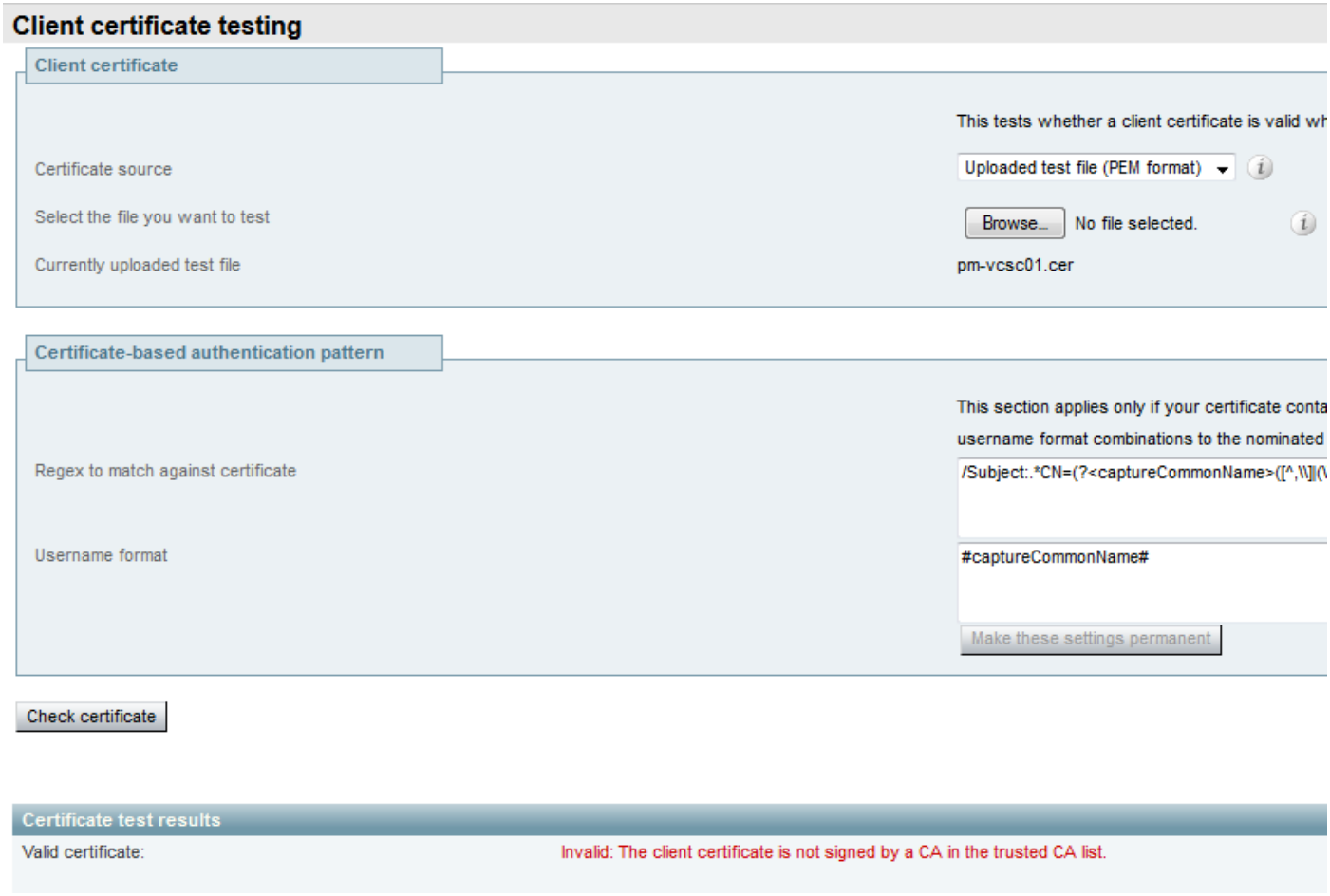
証明書を展開すると、すべての詳細を確認できます。 証明書をエクスポートする場合は、チェーン内の目的の証明書を右クリックし（複数ある場合）、Export Selected Packet Bytesを選択します。 証明書の名前を入力し、[保存（Save）] をクリックします。 ここで、Windows証明書ビューアで証明書を開くか（.cer拡張子を付けた場合）、他の分析ツールにアップロードする必要があります。

トラブルシュート

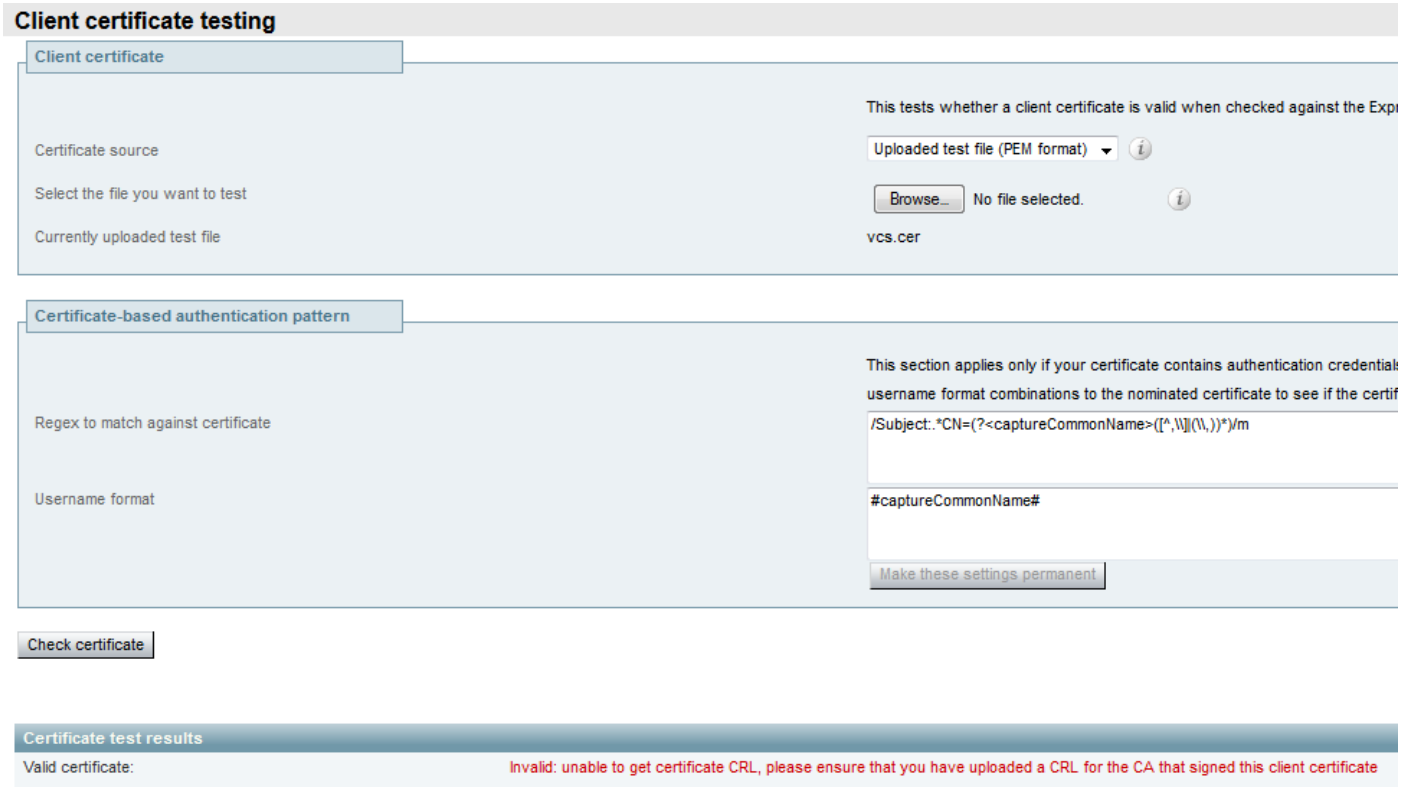
このセクションでは、設定のトラブルシューティングに役立つ情報を説明します。

証明書がExpresswayで信頼されているかどうかをテストする

最良の方法は、証明書チェーンを手動で確認し、すべてのメンバーがExpresswayの信頼済みCAリストに含まれていることを確認することですが、Web GUIのメンテナンス> [セキュリティ証明書]の下にあるクライアント証明書テストを使用して、Expresswayが特定のクライアントの証明書を信頼しているかどうかをすばやく確認できます。すべてのデフォルト設定を同じにしてください。ドロップダウンからUpload Test File（pem形式）を選択し、検証するクライアント証明書を選択します。 証明書が信頼されていない場合、図に示すように、拒否された理由を説明するエラーが表示されます。表示されるエラーは、参照用にアップロードされた証明書のデコードされた情報です。



Expresswayが証明書CRLを取得できないことを示すエラーが表示されても、ExpresswayがCRLチェックを使用しない場合は、証明書が信頼され、他のすべての検証チェックに合格することを意味します。



Synergy ライト エンドポイント（7800/8800 シリーズの電話機）

これらの新しいデバイスには、事前に入力された証明書信頼リストが付属しています。このリストには、既知のパブリックCAが多数含まれています。 この信頼リストは変更できません。つまり、これらのデバイスを使用するには、Expressway-E証明書をこれらの一致したパブリックCAのいずれかによって署名する必要があります。 内部CAまたは別のパブリックCAによって署名されている場合、接続は失敗します。 Jabber クライアントのようにユーザが手動で証明書を承諾するオプションはありません。

注：一部の導入では、Expressway-Eが内部CAを使用する場合でも、7800/8800シリーズの電話機に含まれるリストからCAを使用するCitrix NetScalerなどのデバイスを使用してMRA経由で登録できることが判明しています。SSL認証を機能させるには、NetScalerのルートCAをExpressway-Eにアップロードし、内部のルートCAをNetscalerにアップロードする必要があります。これは動作することが実証されており、ベストエフォート型のサポートです。

注：信頼されたCAリストにすべての正しい証明書が含まれているように見えても、拒否される場合は、リストの上位に、同じサブジェクトを持ち、正しい証明書と競合する可能性がある別の証明書が存在しないことを確認してください。 他のすべてが失敗した場合は、ブラウザまたはWiresharkからチェーンを直接エクスポートし、すべての証明書を反対側のサーバのCAリストにアップロードできます。 これにより、信頼できる証明書であることが保証されます。

注：トラバーサルゾーンの問題をトラブルシューティングする際に、証明書に関連した問題のように見える場合がありますが、実際にはソフトウェア側の問題です。 トラバーサルに使用しているアカウントのユーザ名とパスワードが正しいか確認してください。

注:VCSまたはExpresswayでは、証明書のSANフィールドで999文字を超える文字はサポートされていません。この制限を超えているSAN（多くの代替名が必要）は、存在しないものとして無視されます。

ビデオ リソース

このセクションでは、すべての証明書設定プロセスを説明するビデオ情報を提供します。

MRAまたはクラスタ化ExpresswayのCSRの生成

Expresswayへのサーバ証明書のインストール

Expressway間の証明書信頼の設定方法

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。