Expressway x15.5でクライアントEKU Sunsetに移動する

はじめに

このドキュメントでは、Cisco Expressway x15.5を使用したクライアントEKUサンセットのナビゲーションについて説明します。

バックグラウンド情報

デジタル証明書は、信頼できる認証局(CA)によって発行される電子証明書で、認証、データの整合性、機密性を確保することによってサーバとクライアント間の通信を保護します。これらの証明書には、その目的を定義する拡張キー使用法(EKU)フィールドが含まれています。

- サーバ認証EKU(id-kp-serverAuthは、サーバが身元を証明するために証明書を提示する場合に使用されます。
- クライアント認証EKU(id-kp-clientAuth)は、両方のパーティが互いを認証する相互TLS(mTLS)接続で使用されます。

従来、1つの証明書にサーバ認証とクライアント認証の両方のEKUを含めることができるため、二重目的で使用できます。これは、異なる接続シナリオでサーバとクライアントの両方として機能するCisco Expresswayなどの製品にとって特に重要です。

問題の定義

Chromeルートプログラムポリシーの変更

2026年6月より、Chromeルートプログラムポリシーは、Chromeルートストアに含まれるルート認証局(CA)証明書を制限し、多用途ルートを段階的に廃止して、すべての公開キーインフラストラクチャ(PKI)階層を調整し、TLSサーバ認証のユースケースのみを提供します。

主要なポリシー要件

- パブリックルートCAは、サーバー認証(id-kp-serverAuth)に対してのみ拡張キー使用法

(EKU)をアサートする必要があります。
- これらの証明書にクライアント認証EKUを含めることは禁止されています。
- パブリックサーバのTLS証明書に使用するルートCAが混在する必要がなくなりました。
- 実施スケジュール：2026年6月

パブリックCA応答のタイムライン

- 2025年10月：多くのパブリックCA(DigiCert、Sectigo、SSL)が、デフォルトでサーバ専用証明書の発行を開始しました。
- 2026年5月：パブリックCAサーバがClient Authentication EKU証明書の発行を停止
- 2026年6月：Chromeルートプログラムポリシーが完全に発効

注：このポリシーは、パブリックCAによって発行された証明書にのみ適用されます。プライベートPKIおよび自己署名証明書は、このポリシーの影響を受けません。

Expresswayでのクライアント EKUのサンセット設定の影響については、「パブリックCA証明書でのクライアント認証EKUのサンセットに対するExpresswayの準備」を参照してください。

Expresswayリリースx15.5およびソリューション

Expressway x15.5

Expressway x15.5には、すべての公開認証局によるクライアントEKUのサンセットが原因で発生する問題の修正案が付属しています。これはグローバルな問題であり、パブリックPKI証明書の使用を選択するすべてのベンダー/導入に影響を与えます。

以前のリリースのx15.4にはCLIコマンドスイッチがあり、管理者はExpressway Eにサーバ EKUのみの証明書（クライアントEKUなし）をアップロードできました。

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload：オン

注：このコマンドはx15.5では使用されなくなりました。

X15.5証明書ストアの追加

x15.5には2つの証明書ストアがあります。

1. サーバー証明書ストア

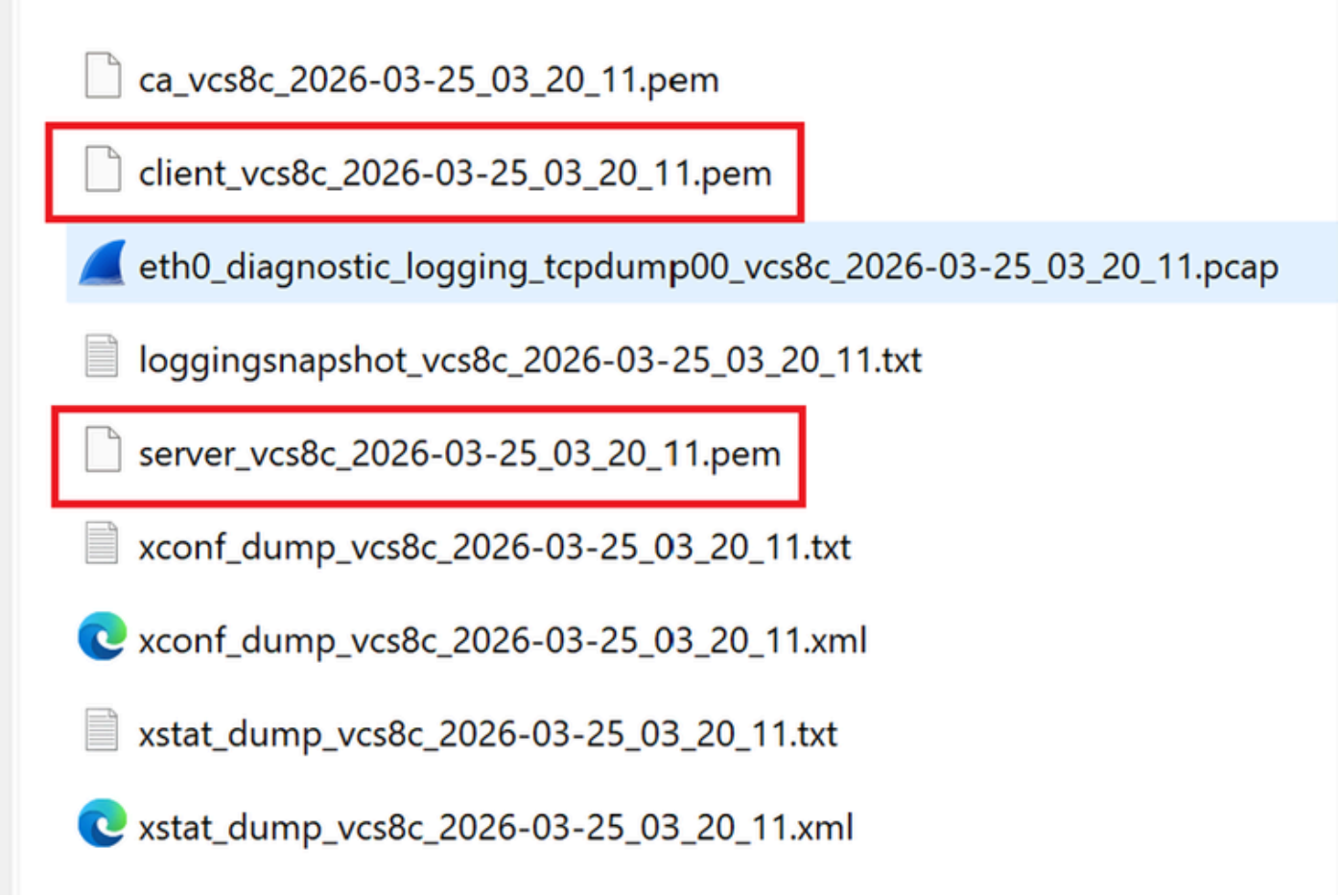
2. クライアント証明書ストア

Expressway（シングルNicまたはデュアルNic）：どちらのExpresswayインターフェイスも、必要に応じて2つの証明書ストアを使用できます。

例：

- TLSハンドシェイク時にExpresswayがクライアントとして動作すると、クライアント証明書が提示されます。
- TLSハンドシェイク中にExpresswayがサーバとして動作すると、サーバ証明書が提示されます。

注：両方の証明書ストア（クライアントとサーバ）で、同じ信頼済みCAライブラリが使用されています。サーバ証明書とクライアント証明書に署名したCAが信頼ストアに正しくアップロードされていることを確認します。 診断ログに、サーバ証明書とクライアント証明書がPEMファイル形式で含まれるようになりました。



X15.4以前のバージョンからX15.5へのアップグレード

アップグレードを実行すると、x15.4以前のバージョンのサーバ証明書が、x15.5のクライアント証明書ストアにExpresswayサーバ証明書ストアがコピーされます。x15.5上のクライアント証明書ストアとサーバ証明書ストアは同じ証明書を持ちます。

スクリーンショットの例

15.4上のExpresswayサーバ、現在のサーバ証明書シリアル番号46:df:76:aa:00:00:00:00:00:29

証明書:

バージョン：3(0x2)

シリアル番号:

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

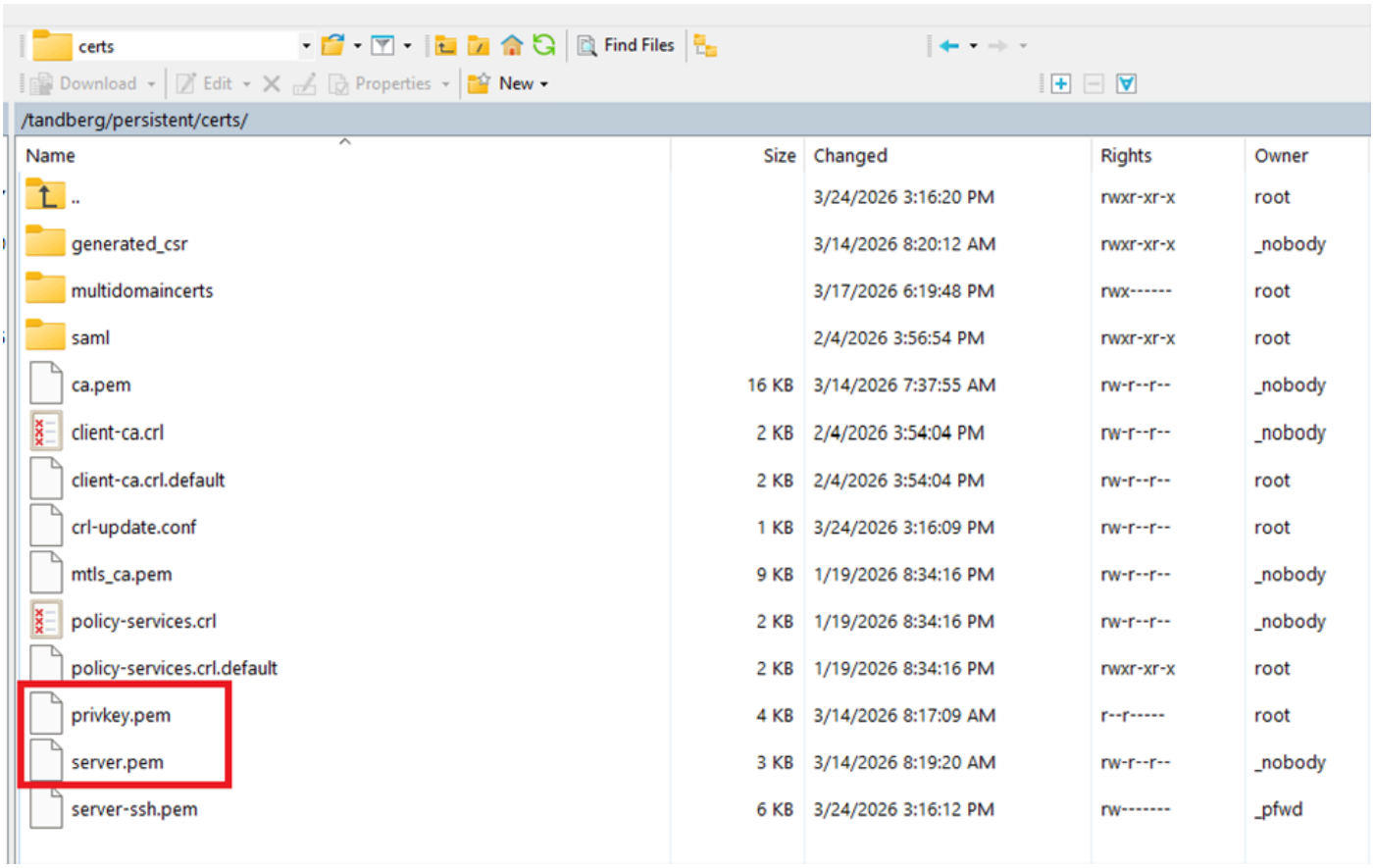
有効性

指定日以前： 3月14日02:37:40 2026 GMT

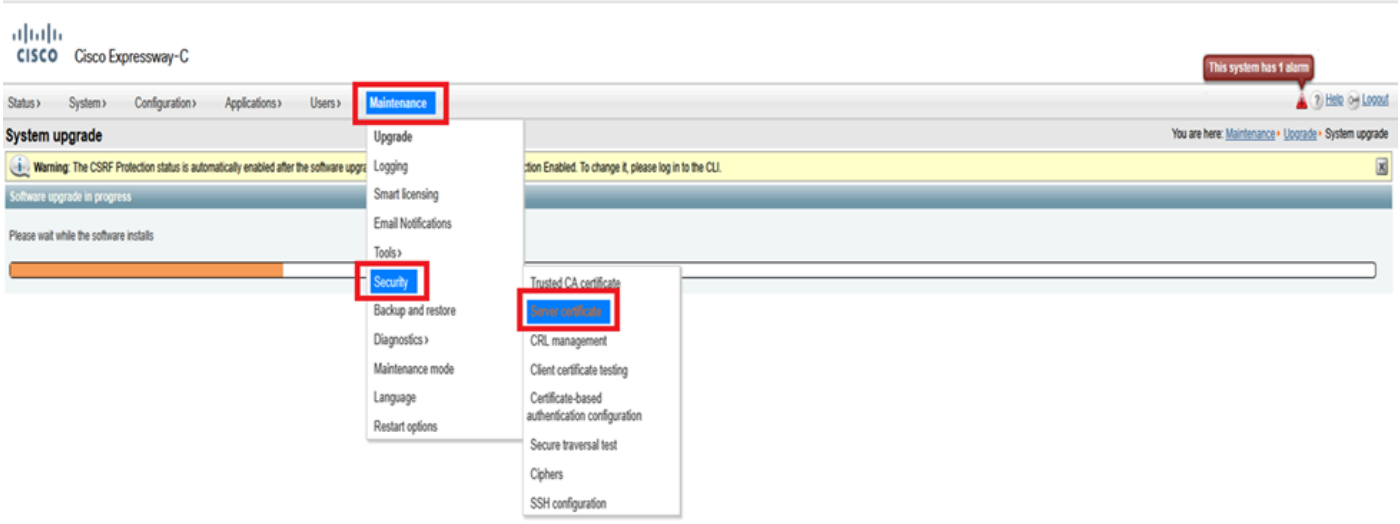
Not After : 3月14日02:47:40 2028 GMT

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

x15.4上のExpresswayファイルシステムの永続的な/証明書ディレクトリ：

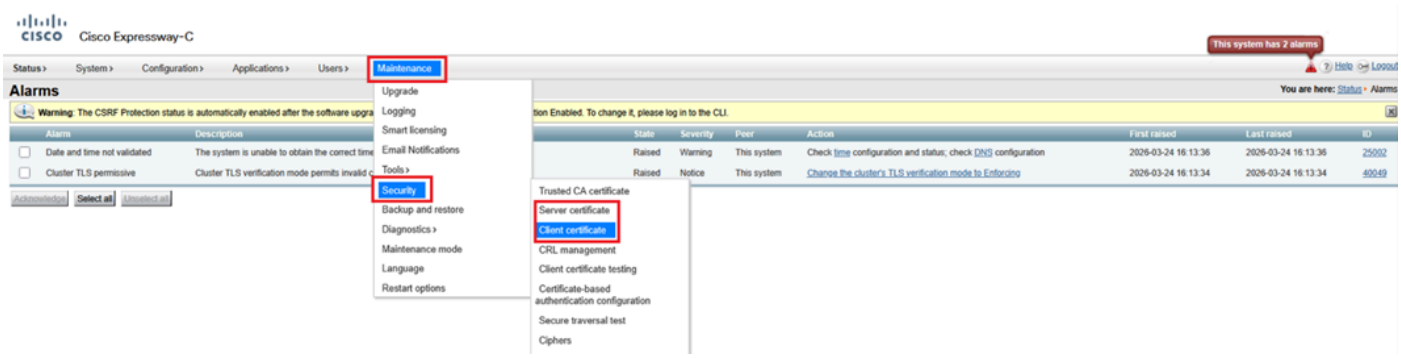


x15.4上のExpresswayメニュー(Maintenance > Security > Server certificate)（サーバ証明書フィールドのみが存在する）：



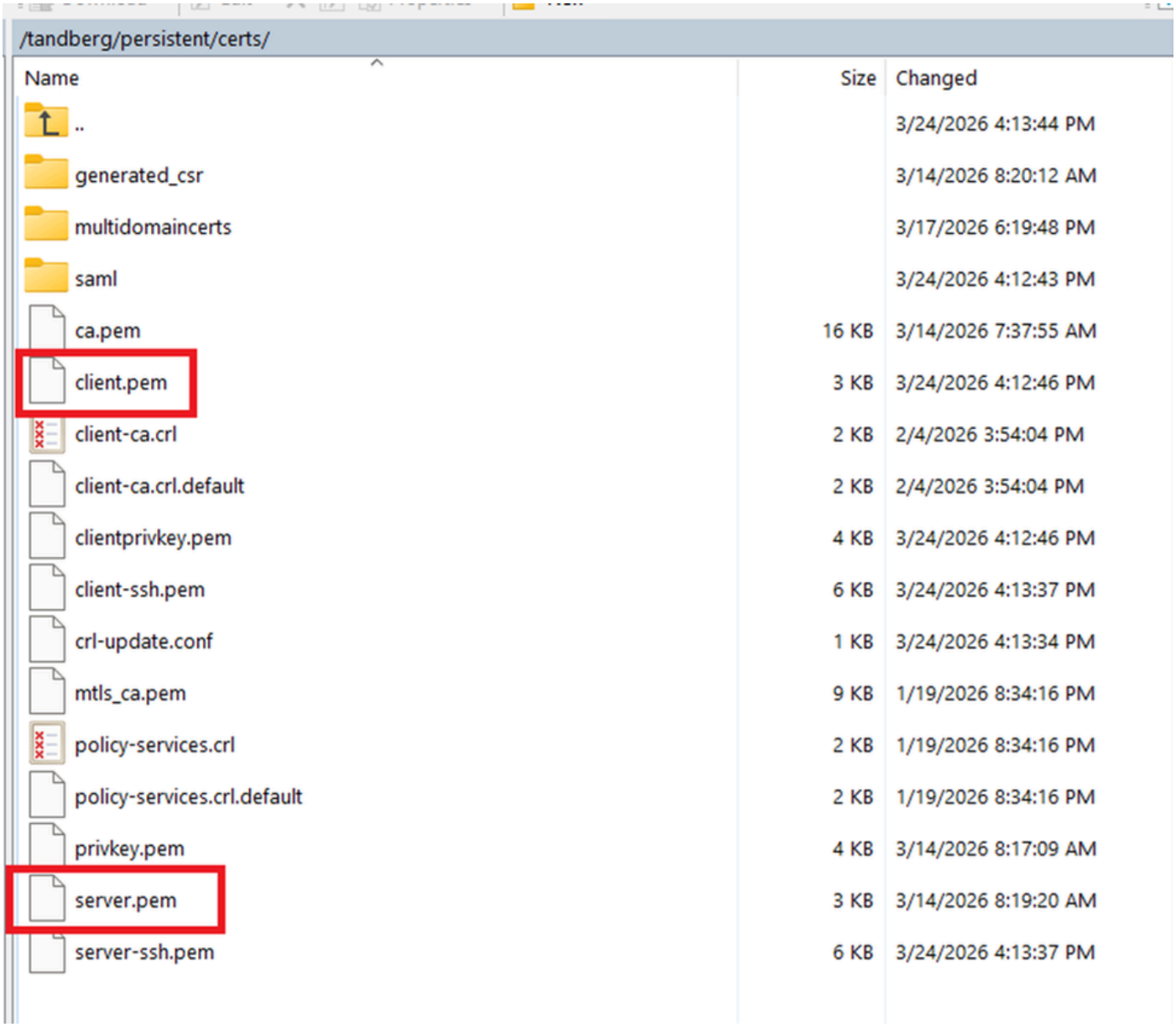
x15.5へのアップグレードに成功した後

この例では、Maintenance > Security > client certificateおよびserver certificatesの下に2つの証明書オプションが表示されています。x15.5へのアップグレード後、x15.4からのサーバ証明書がx15.5のクライアント証明書ストアにコピーされたため、web adminのサーバ証明書ポータルとクライアント証明書ポータルの両方に同じ証明書が表示されます。



x15.5へのアップグレード後の既存の証明書と秘密キーがクライアント証明書ストアにコピーされました。

x15.5上のExpresswayファイルシステムの永続的な/証明書ディレクトリ：



TLSハンドシェイク時のX15.5 EKUチェック

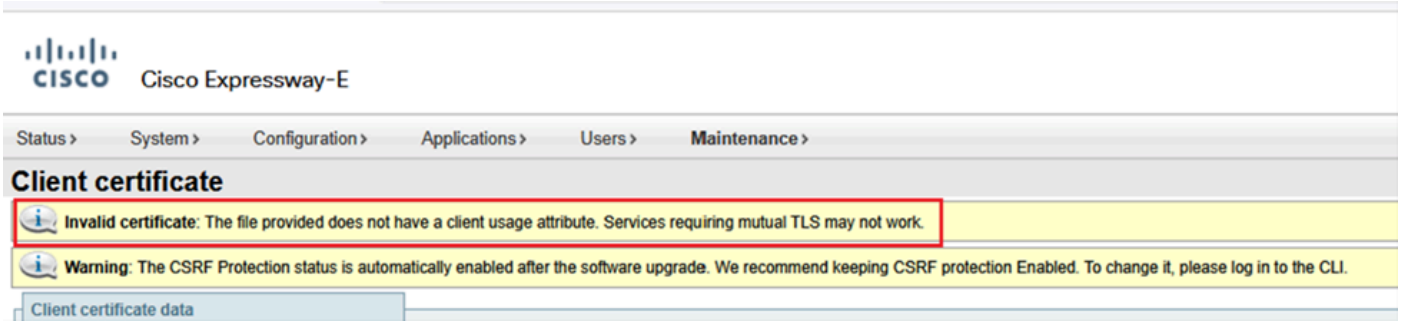
x15.5では、新しいCLIコマンドが導入され、TLSハンドシェイク時に拡張キー使用法(EKU)をチェックできるようになりました。デフォルト値は「オン」です。 コマンドセットはExpressway CoreおよびEdgeで有効です。

コマンドセットにより、Expresswayへのすべての着信SIP TLS接続のチェックがトリガーされます。（インバウンドクライアントhello/証明書が提示されます）。 オンにすると、TLSイニシエータによって提示された証明書に証明書のクライアントEKUが含まれているかどうかがチェックされます。オフにすると、チェックはバイパスされますが、サーバEKUが証明書に存在する場合はチェックされます。

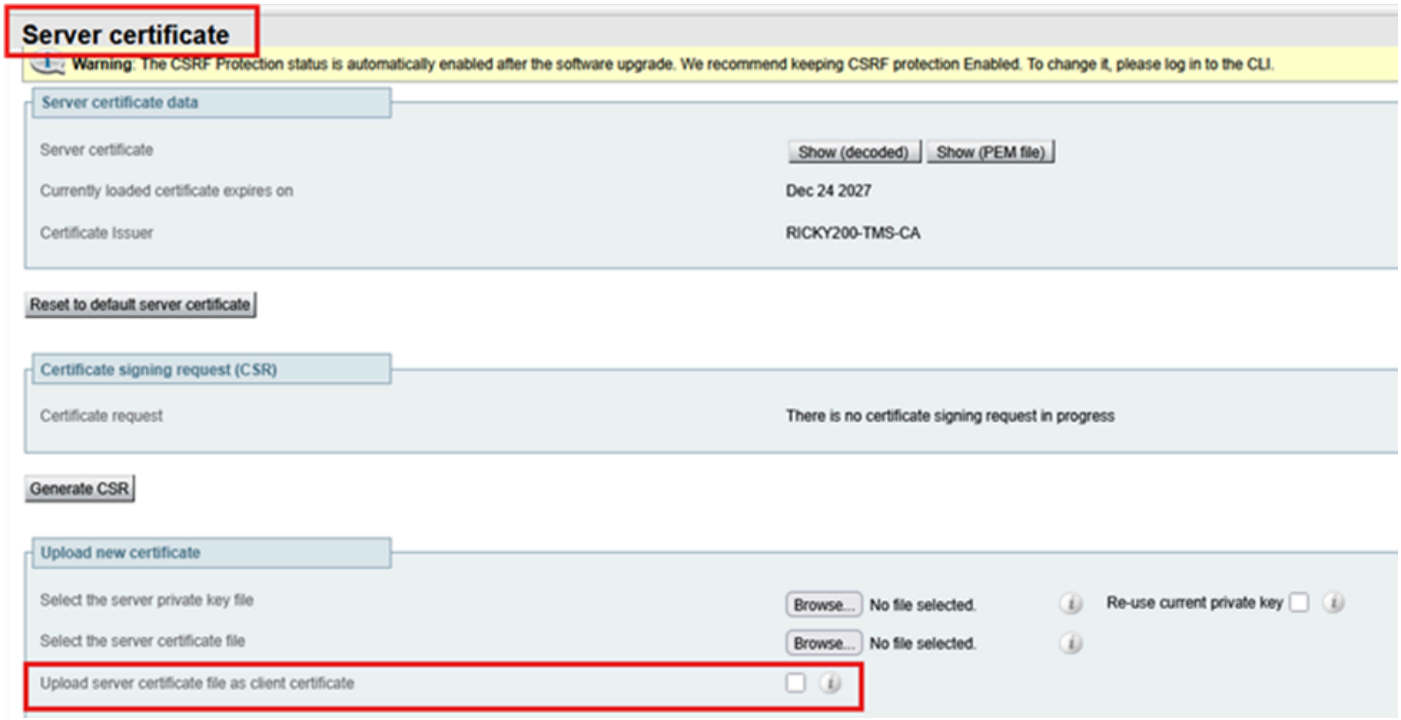
xconfiguration SIP TLS Certificate ExtendedKeyUsageチェックモード：オン/オフ：

注：クライアント証明書を生成し、クライアントEKU（パブリックCA署名付き証明書の例）を含まないCSRに署名する場合は、この証明書をクライアント証明書ストアに手動でアップロードできません。そのため、CSRの署名によって生成された証明書に必ずクライアントEKUが含まれていることを確認する必要があります（プライベートCAを使用して、クライアントEKUを挿入できます）。

ヒント：このエラーは、クライアントのEKUが欠落しているCSR署名付き証明書をクライアント証明書ストアからアップロードしようとすると明らかになります。



ただし、サーバEKUのみ（クライアントEKUなし）が含まれている証明書をサーバ証明書ストア経由でアップロードし、Upload server certificate file as client certificateを選択すると、証明書はクライアント証明書ストアにコピーされます。Expressway-EdgeでプライベートCA署名付き証明書を使用しない管理者は、サーバ証明書ストアからクライアント証明書ストアにのみサーバEKUをコピーすることを選択できます。

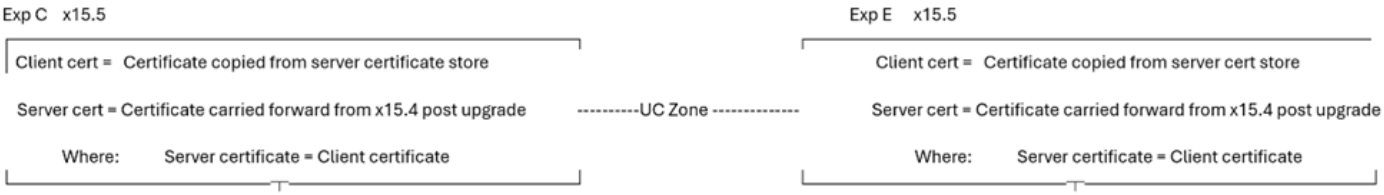


複数の証明書ストア、複数の導入シナリオ

Expresswayには2つの証明書ストアがあるため、証明書ストアには複数のシナリオがあります。

条件1：アップグレード

Expresswayをx15.4またはx15.5より前のバージョンからアップグレードする場合、この条件は成立します。x15.4バージョンの既存の証明書が2つの証明書ストアにコピーされます。x15.5のクライアントとサーバでは、証明書は同じです。

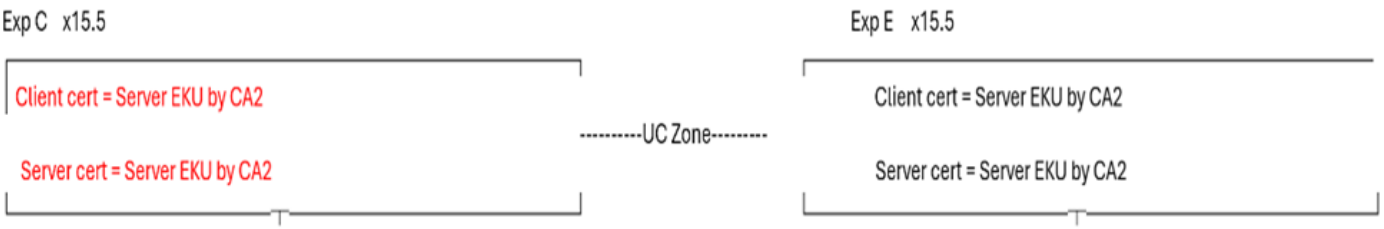


条件2：管理者がx15.5に新しい証明書をインストールしたとき（既存の証明書の有効期限が切れました）

CA 1 =内部CA

CA 2 =パブリックCA

次の図に示すように、Expressway Coreには、CA 2によってのみ署名されたサーバEKU（パブリックCA）を持つクライアント証明書と、CA 2によってのみ署名されたサーバEKU（パブリックCA）を持つサーバ証明書があります。 同様に、Expressway Eには、CA2によって署名されたサーバEKU（パブリックCA）を持つクライアント証明書と、CA 2によってのみ署名されたサーバEKU（パブリックCA）を持つサーバ証明書があります。



Expresswayコアサーバ証明書にクライアントEKU、ユニファイドコミュニケーショントラバーサルゾーン、MRAがない場合、WebRTCプロキシは機能しません。Expressway Coreサーバー証明書にクライアントEKUがあることを確認してください。これは、ユーザーがパブリックCAからすべての証明書への署名を選択する一般的な使用例です。パブリックCAは証明書にクライアントEKUを含めないため、ユニファイドコミュニケーショントラバーサルゾーンはアクティブになります。

UCゾーンをアクティブにするには、Expressway EでEKUチェックをオフにするという手っ取り早い方法があります。これにより、UCゾーンが起動します。ただし、SSHトンネルは非アクティブのままです。現在、2222でのSSHトンネル通信には、クライアントEKUの検証が必要です。

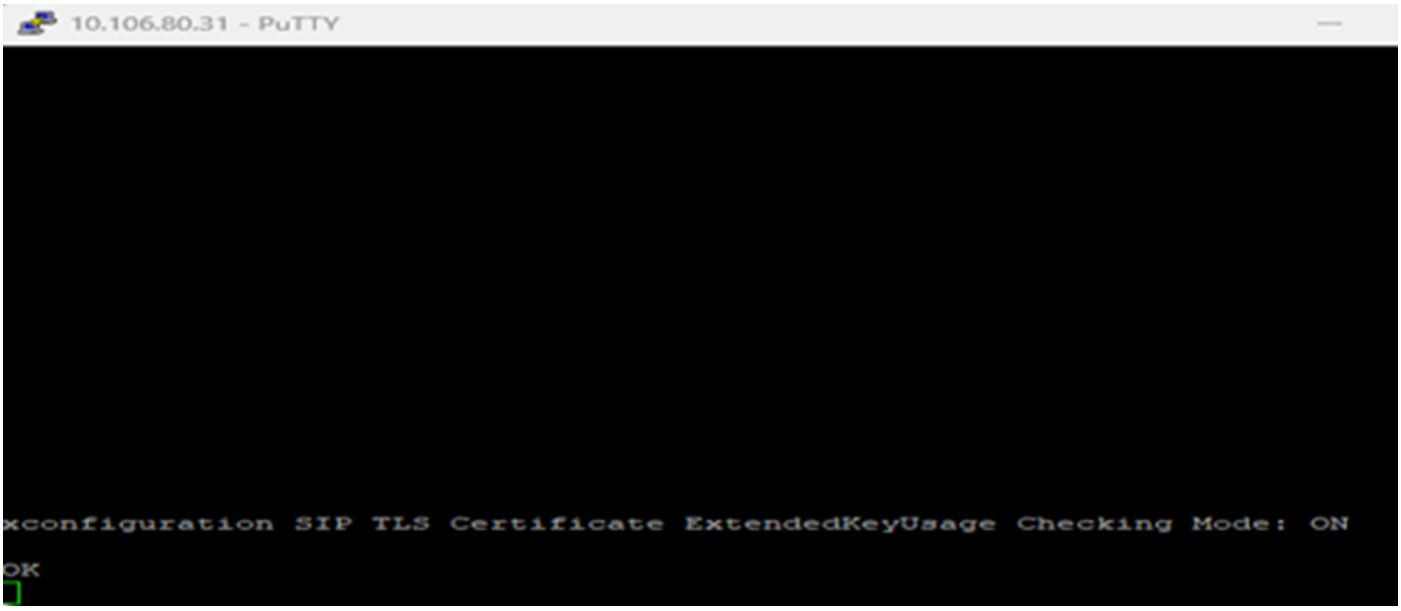
MRAクライアントログインおよびWebRTCプロキシ機能は機能しません。プライベートCAに頼らざるを得ない場合もあります。

テスト ケース 1

- Expressway EでEKUチェックが「ON」のとき
- Expressway Coreのクライアントおよびサーバ証明書にサーバEKUのみがある場合
- UCゾーンステータスがFAILED

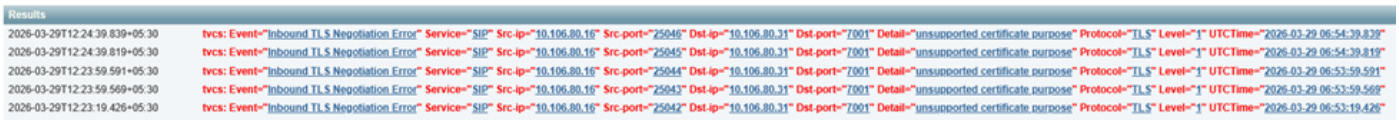
Expressway-EdgeでExtendedKeyUsageをオンにします。

xconfiguration SIP TLS Certificate ExtendedKeyUsageチェックモード：オン：



ユニファイドコミュニケーションゾーン障害：

Expressway Eのログには、10.106.80.16 = Expressway Core、10.106.80.31 = Expressway Edgeと記録されています。

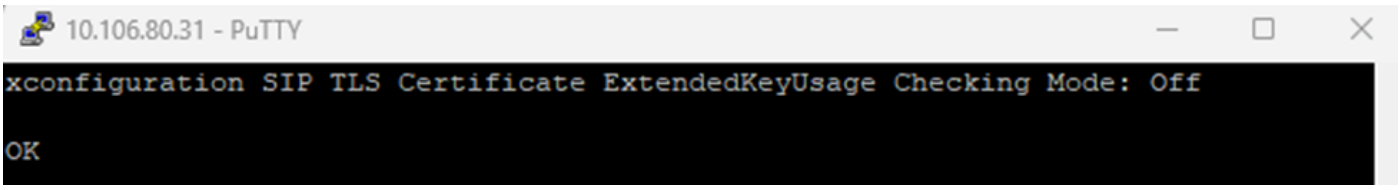


テスト ケース 2

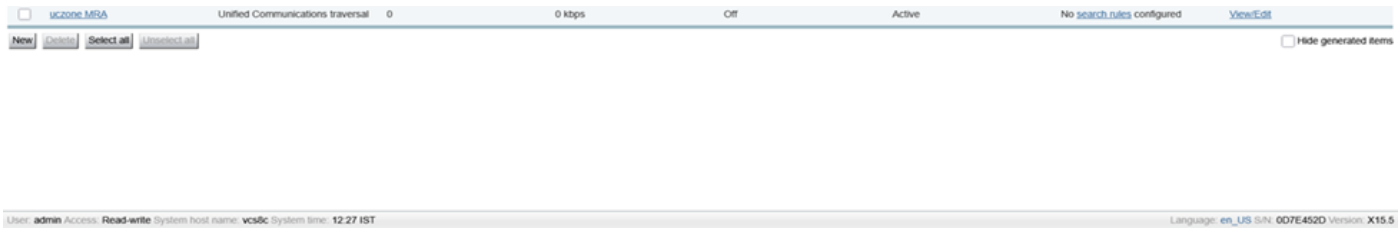
- Expressway EでEKUチェックがオフのとき
- Expressway Coreのクライアント証明書とサーバ証明書にサーバのみのEKUがある場合
- UCゾーンステータスはACTIVE

Expressway EでEKUチェックをオフにします。

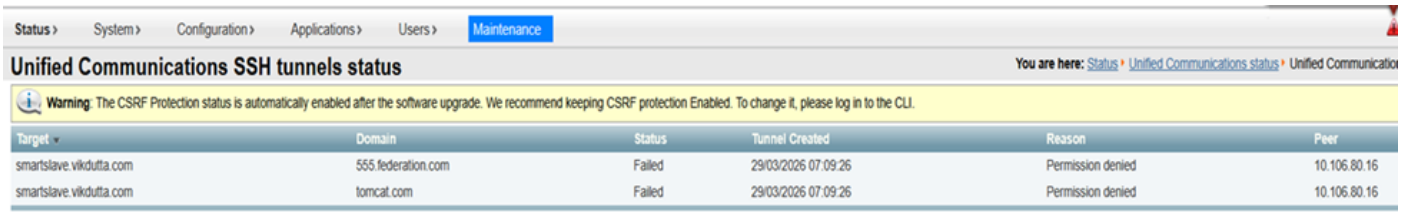
xconfiguration SIP TLS Certificate ExtendedKeyUsageチェックモード：オフ



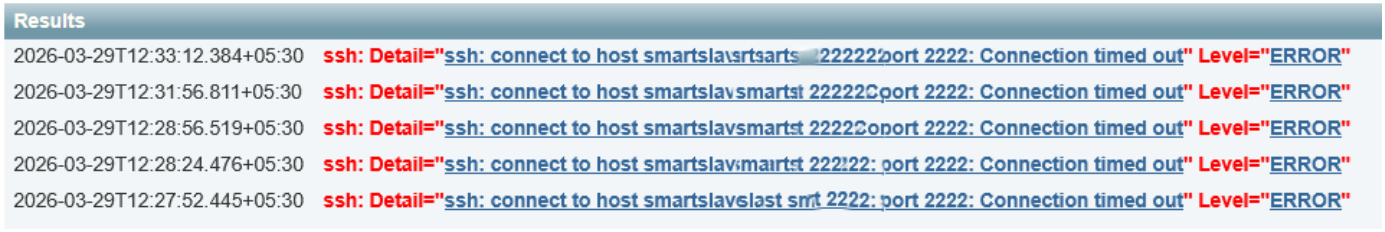
ユニファイドコミュニケーションゾーンアクティブ：



ただし、sshトンネルはまだ失敗しています。



Expresswayイベントログ：

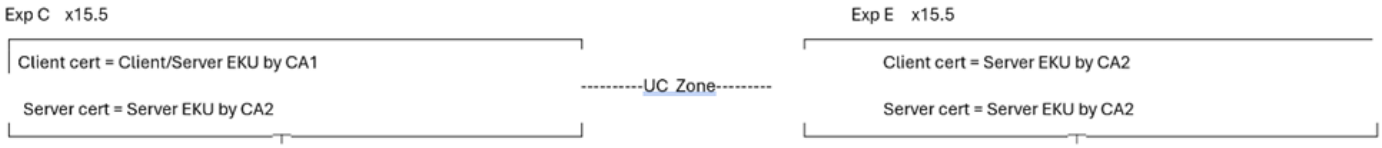


条件2.1：成功事例

CA 1 =内部CA

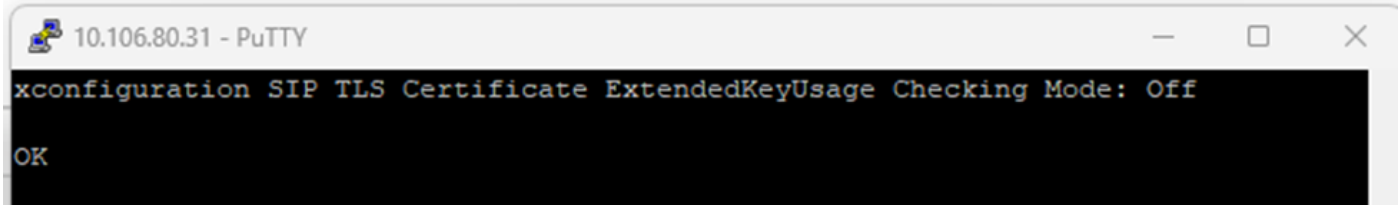
CA 2 =パブリックCA

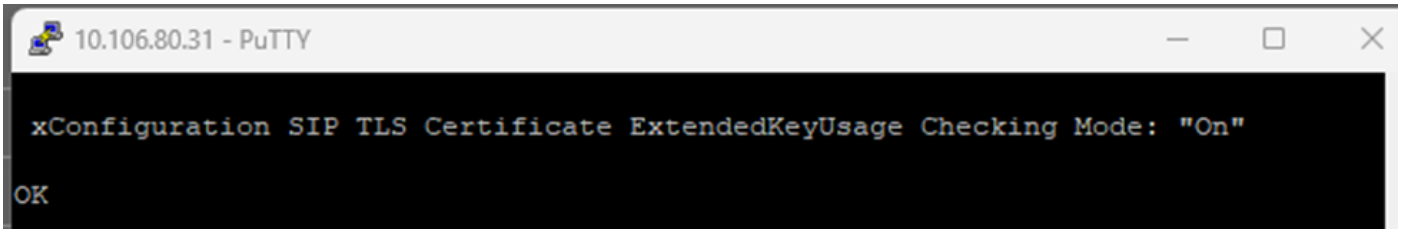
- Expresswayコアクライアント証明書がCA 1（内部CA）によって署名され、クライアント/サーバEKUの両方が含まれている場合。
- Expresswayコアサーバ証明書はCA 2パブリックCAによって署名され、サーバEKUのみを含みます。
- Expressway Edge Server証明書はCA 2のパブリックCAによって署名されており、サーバEKUのみが含まれています。
- Expressway Edgeクライアント証明書はCA 2のパブリックCAによって署名されており、サーバEKUのみが含まれています。



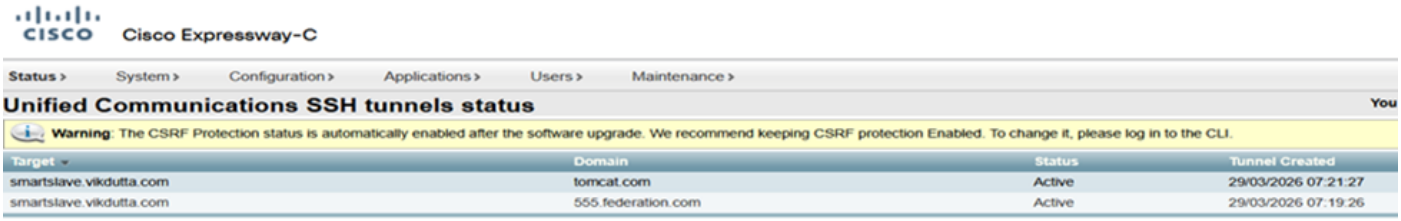
この条件は成功例です。 EKUチェックモードのオン/オフに関係なく、ユニファイドコミュニケーションゾーンとSSHトンネルの両方がアクティブになります。MRAクライアントは動作します。

Expressway EdgeのEKUチェックがOFFであるかONであるかは問題ではありません。Expresswayコアクライアント証明書にクライアントEKUが含まれています。

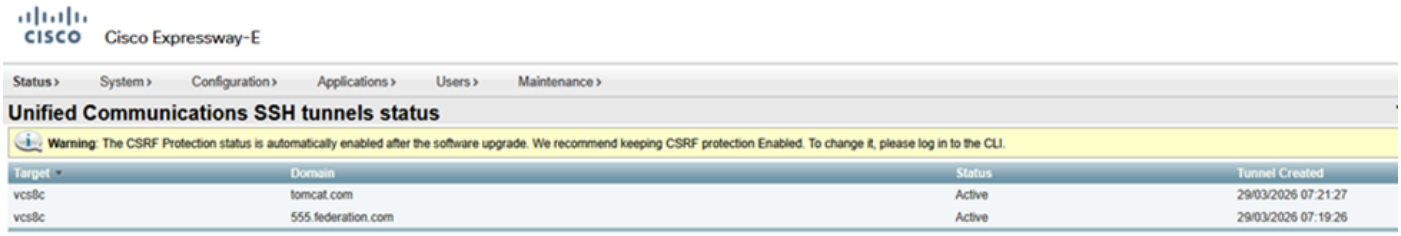




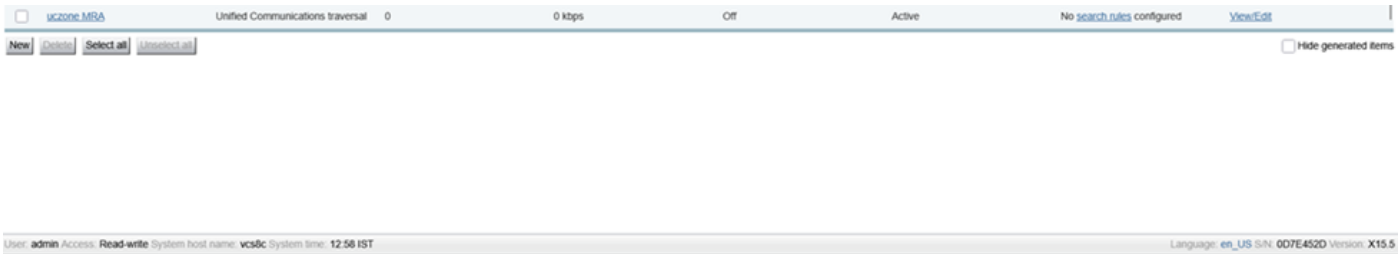
Expressway core ActiveのSSHトンネル：



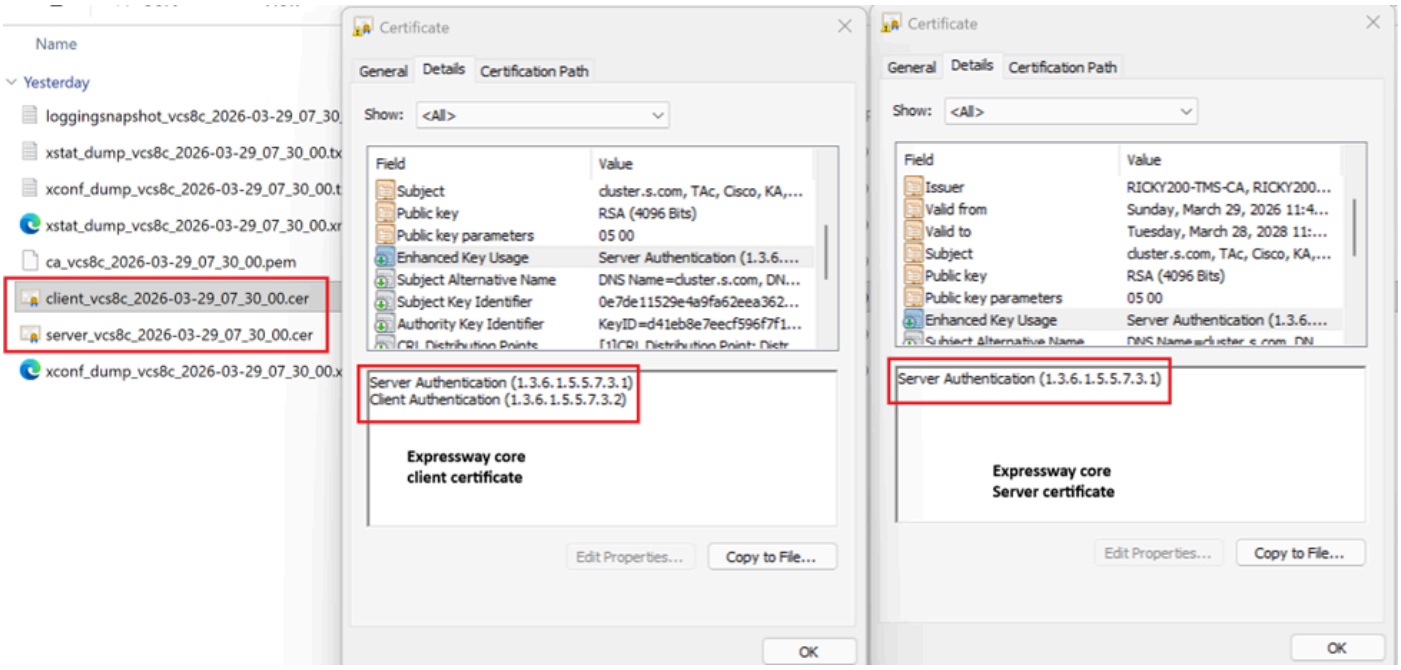
Expressway Edge ActiveのSSHトンネル：



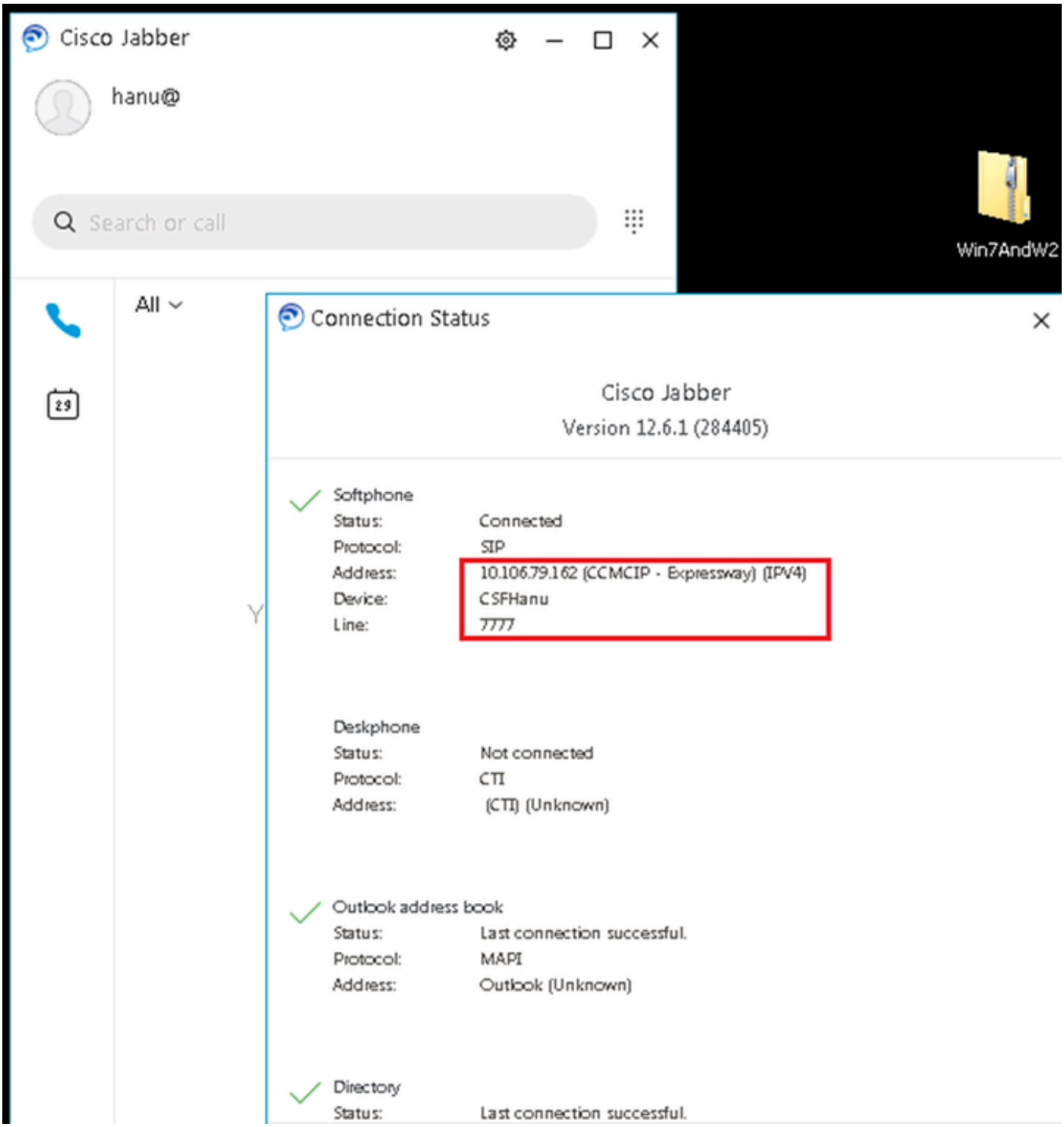
ユニファイドコミュニケーションMRAゾーンのステータスアクティブ：



- Expressway-Coreクライアント証明書にサーバEKUとクライアントEKUがあります。
- Expressway Coreサーバ証明書にはサーバEKUのみがあります。



MRAクライアントがログインし、登録されます。

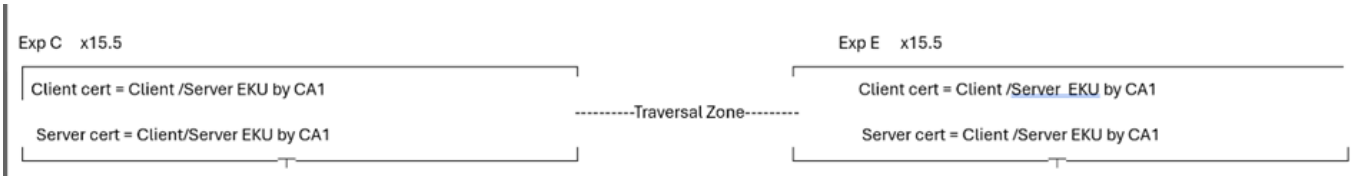


注:MRAおよびWebRTCプロキシが機能するように、証明書に含まれるEKUを比較してメモします。これは、正常に動作する導入と動作しない導入の比較です。

条件3：プライベートCAですべての証明書に署名する

CA 1 =内部CA

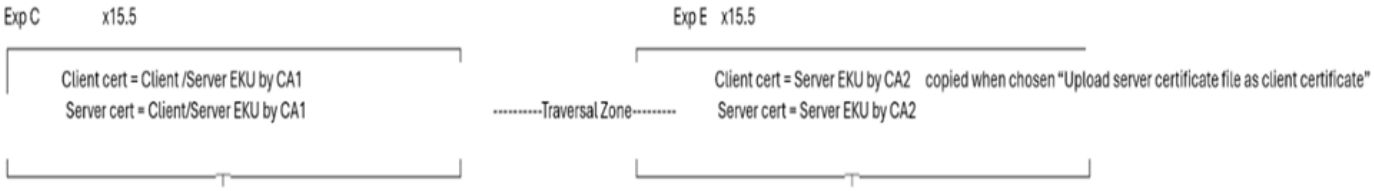
CA 2 =パブリックCA



条件3では、すべての証明書が内部CA(CA1)によって署名されます。

- Expressway-EがTLS接続を送信する場合、CA 1ルート/中間を遠端エンティティと交換する必要があります。遠端に機能がないか、プライベートCA証明書のアップロードが許可されていない場合、TLS接続は失敗します。
- プライベート証明書がOS信頼ストアにない場合、MRAクライアントはポップアップを受け入れるように証明書を取得します。

条件4: Expressway EdgeにサーバEKUのみの公開証明書がある



条件4では、Expresswayのコアクライアント証明書とサーバ証明書は(CA1)内部CAによって署名され、クライアントとサーバの両方のEKUが存在します。Expressway Eのサーバ証明書はパブリックCA署名付きで、サーバEKUのみを含んでいます。サーバ証明書がクライアント証明書ストアにコピーされます。「サーバ証明書ファイルをクライアント証明書としてアップロード」を選択します。

条件4では、TLS接続が遠端に対して行われる場合、Expressway-EがTLSクライアントhelloを送信すると、遠端は（クライアント証明書にクライアント認証EKUがないため）クライアントEKUチェックを無効にする必要があり、そうでない場合はTLS接続が失敗します。

ユーザの導入とユースケースに基づいて、フィールドにはさらに多くの条件やシナリオが存在する可能性があり、私の限られた思考の流れのためにすべてを力バーすることはできません。ただし、次の点に注意してください。

- # TLSハンドシェイク中にExpresswayがクライアントになると、クライアント証明書がピアに提示されます。
- #IF ExpresswayはTLSハンドシェイク時にサーバになります。サーバ証明書はピアに提示さ

れます。

この理由は、これらのテストケースで確立されています。

シナリオ 1

このシナリオでは、ExpresswayはWebexとのMTLSハンドシェイク中にクライアント証明書を提示します。

Webex会議へのビデオ通話：

サンプルコールフローJabber - à CUCM - à Exp Core - à Exp Edge - à Webex

10.106.80.31= Expressway Edge

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="Sent" Local-ip="10.106.80.31" Local-port="25002" Dst-IP 「163.129.37.33」 Dst-port=「5061」

Expressway Edgeには、このシリアル番号(2f0000004c869c77c8981becde00000000004c)のクライアント証明書があります。

Expressway EdgeはTLSネゴシエーション中に「Webex」にclient helloを送信し、クライアント証明書を送信します。

シリアル番号2f0000004c869c77c8981becde00000000004c:

1. Expressway EdgeはmTLSネゴシエーション中に、client hello(pkt= 13699)を「Webex」に送信します。

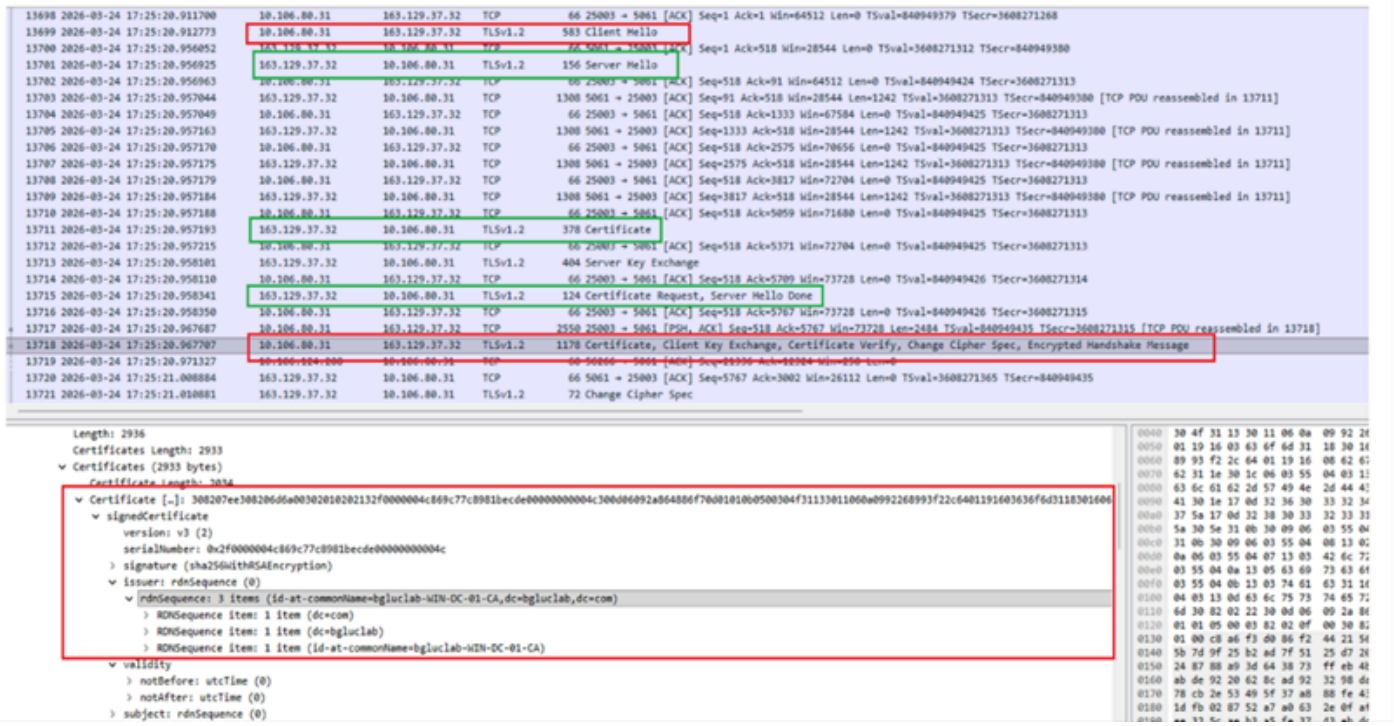
2. WebexがExpressway Edgeにサーバhello(pkt=13701)を送信します。

3. Webexが証明書をExpressway Edge(pkt=13711)に送信します。

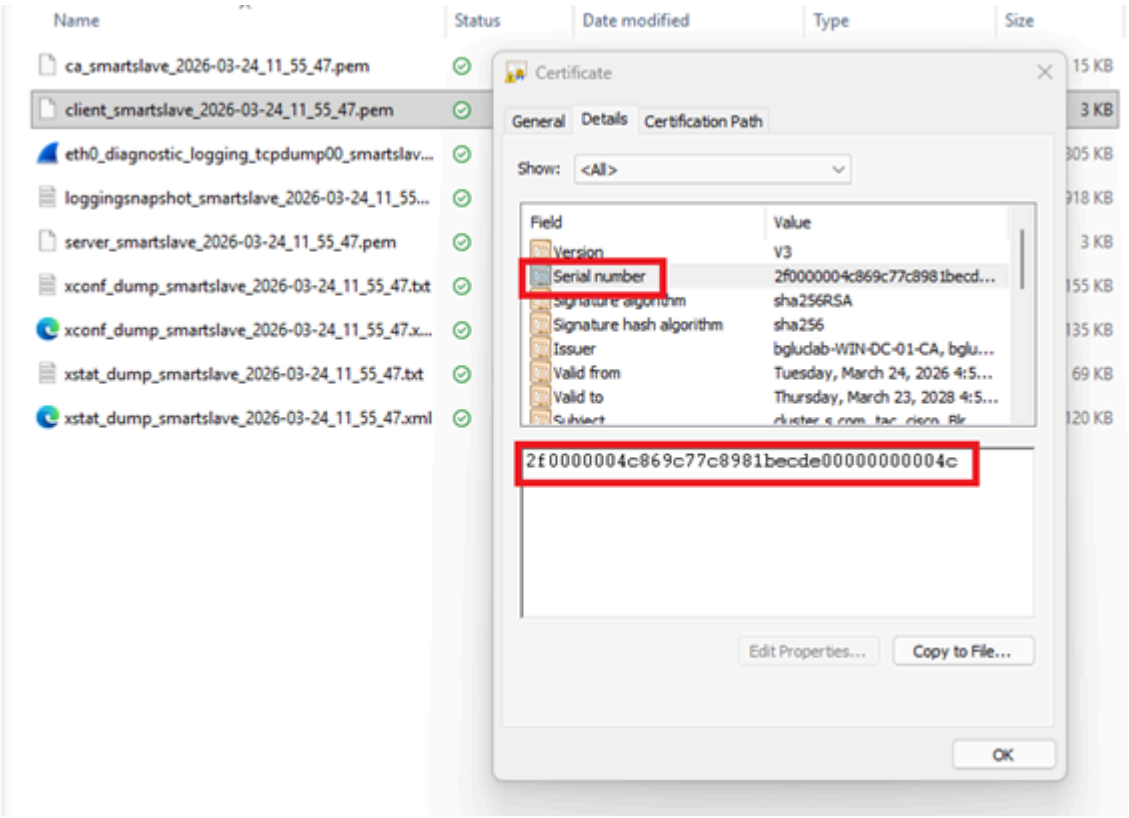
4. WebexがExpresswayエッジ証明書「CertificateRequest」(pkt=13715)を要求します。

5. Expressway Edgeが自身の証明書をWebexに送信します(pkt=13718)。

(screenshot)



Expressway Edgeからのクライアント証明書：



シナリオ 2

ExpresswayはmTLSハンドシェイク中にサーバエンティティになり、そのサーバ証明書を提示します。

Expresswayがサーバ証明書を提示する場合、Expresswayには名前の確認がオンの5061を介したセキュアなネイバーゾーンがあります。

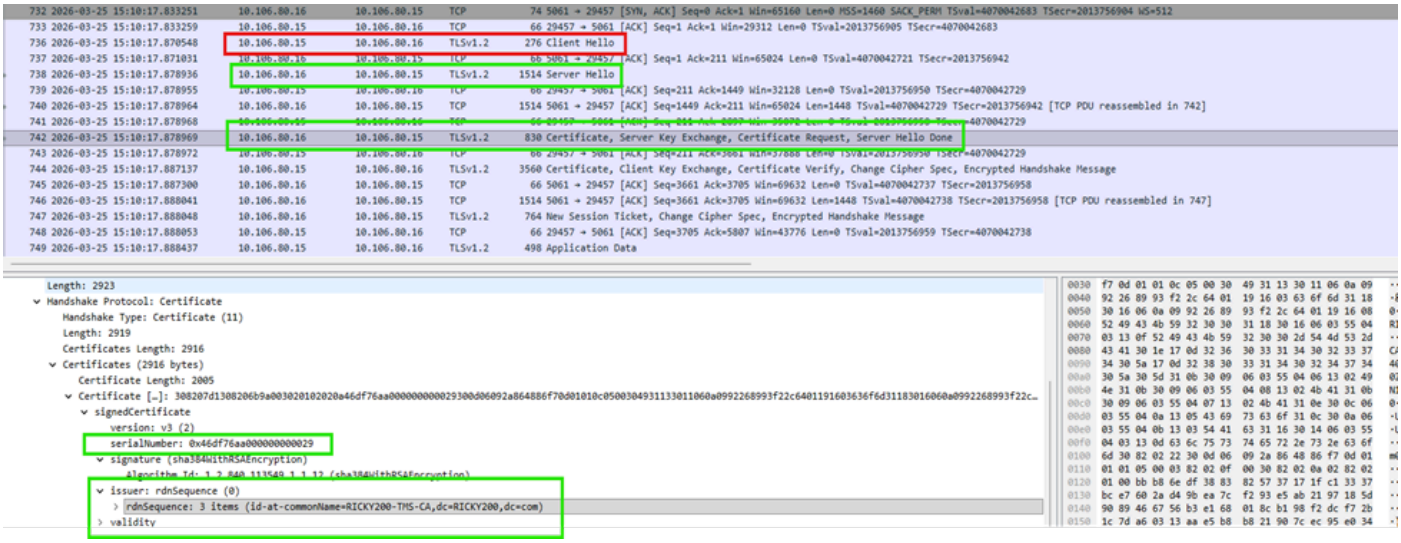
ExpresswayノードX15.5とExpresswayノードX8.11.4の間のセキュアネイバーゾーン：

10.106.80.15 (x8.11.4) sends a client hello to 10.106.80.16 (x15.5) (pkt=736)

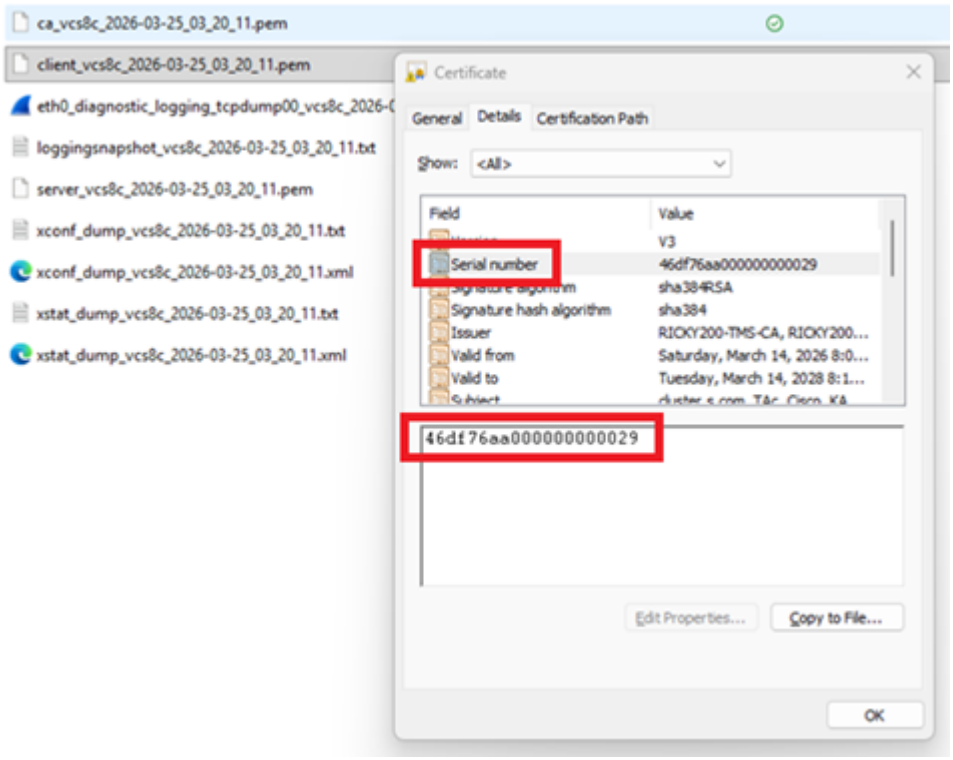
10.106.80.16 sends a server hello to 10.106.80.15 (pkt=738)

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)



次のスクリーンショットは、シリアル番号が一致するサーバ証明書を示しています。

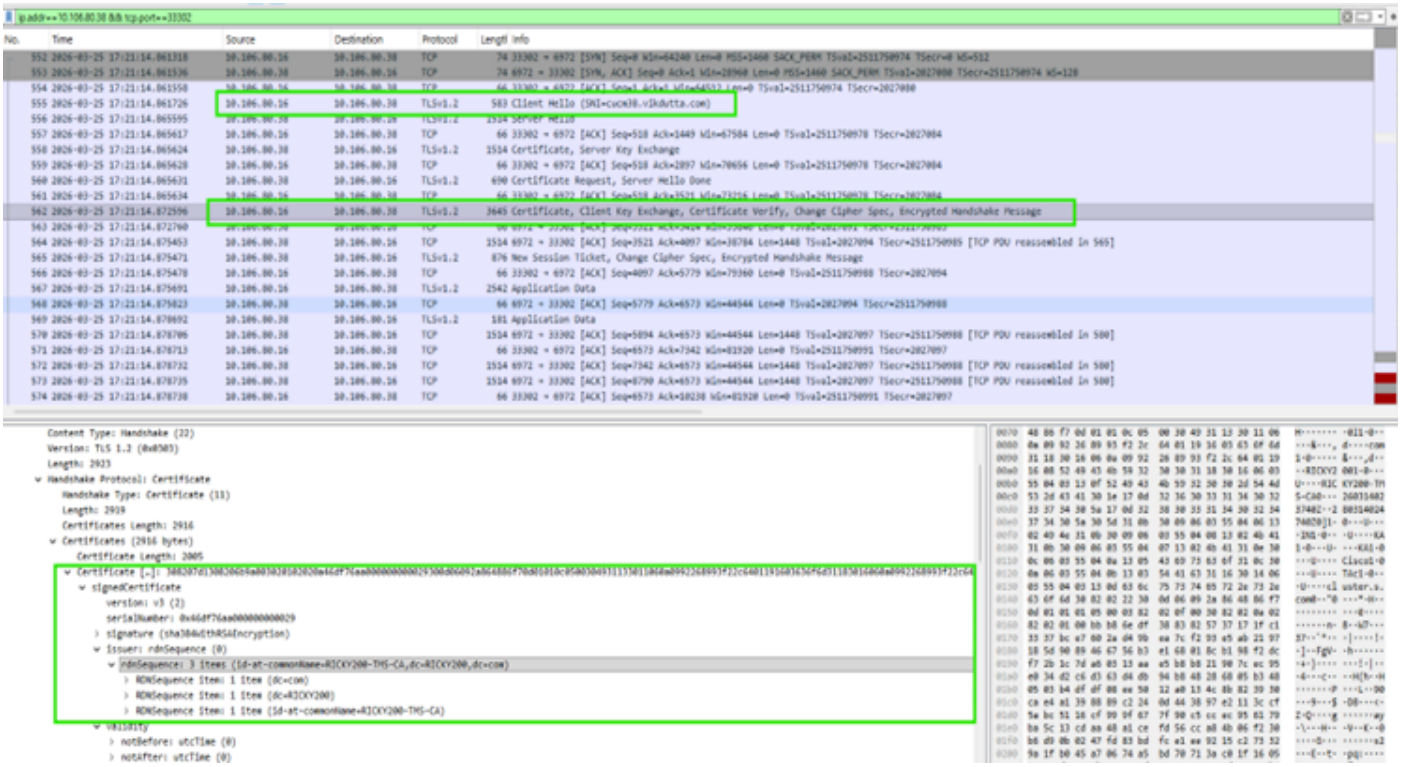


テストケース3:MRAクライアントがログイン用にプロビジョニングされ、ワークフローにExpressway CoreとCUCM間のトラフィックサーバ証明書の検証が含まれています。

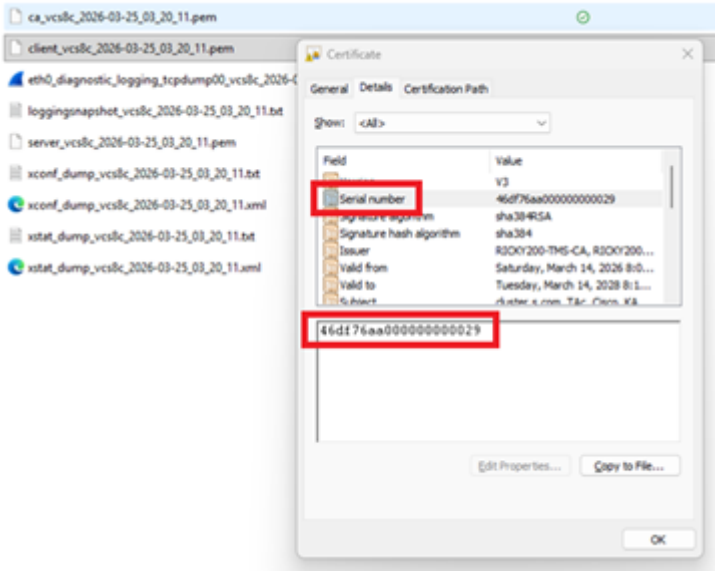
10.106.80.16 = Expressway Core x15.5

10.106.80.38 = CUCM

- Exp C 16は6972 TFTPでクライアントhelloを送信します。
- Exp C 16は、TLSハンドシェイク中にクライアント証明書を送信します。



Expresswayコアクライアント証明書：



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。