Expressway証明書の更新

内容

概要

このドキュメントでは、Expressway/Video Communication Server(VCS)証明書の更新プロセスについて説明します。

このドキュメントの情報は、ExpresswayとVCSの両方に適用されます。このドキュメントではExpresswayを参照していますが、VCSと相互交換できます。

> **注**：このドキュメントは証明書の更新プロセスを支援することを目的としていますが、ご使用のバージョンの『Cisco Expressway証明書の作成と使用の導入ガイド』も参照することをお勧めします。

背景説明

証明書を更新する場合は、新しい証明書をインストールした後もシステムが正常に機能し続けるようにするために、考慮する必要がある主なポイントが2つあります。

1.新しい証明書の属性は、古い証明書の属性（主にサブジェクト代替名と拡張キーの使用）と一致する必要があります

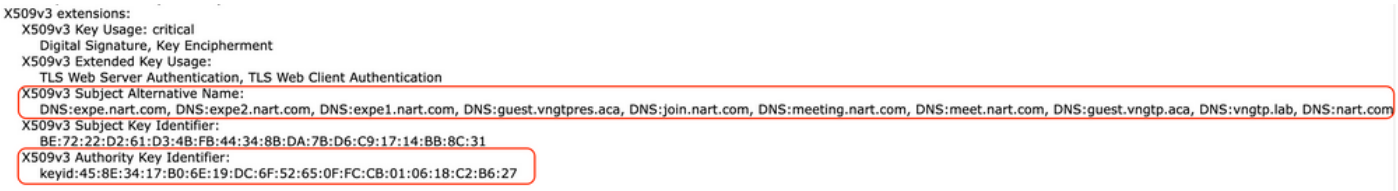
2.新しい証明書の署名に使用されるCA（認証局）は、Expresswayと直接通信する他のサーバ（CUCM、Expressway-C、Expressway-Eなど）によって信頼される必要があります

プロセス

A)現在の証明書から情報を取得する

1. Expressway Webページの[Maintenace] > [Security] > [Server certificate] > [Show decoded] を開きます。

2.開いた新しいウィンドウで、「Subject Alternative name」および「Authority Key Identifier」のX509v3拡張をメモ帳の文書にコピーします。

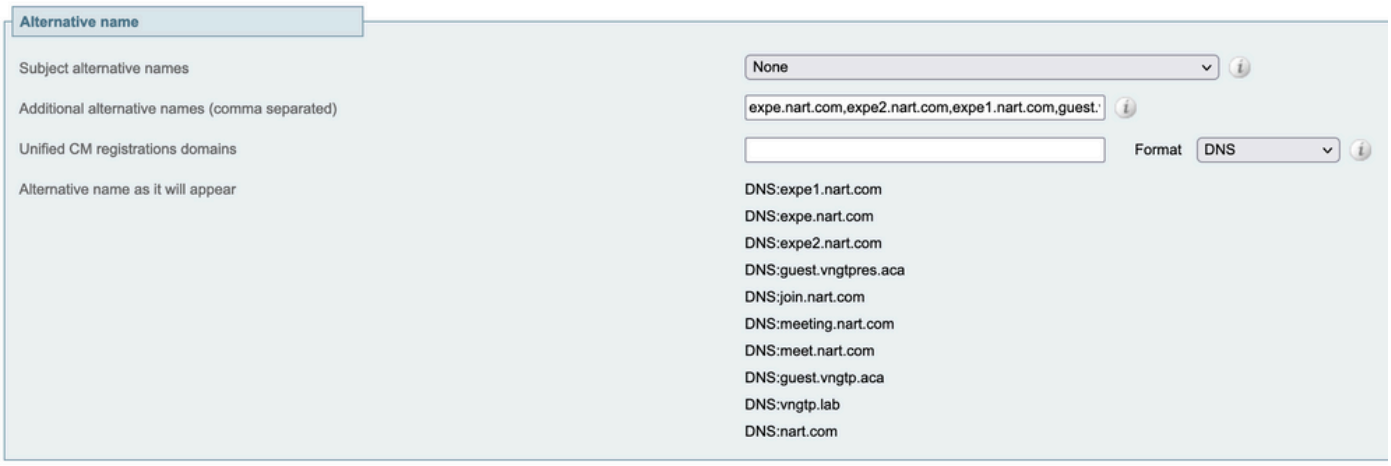


「Show decoded」証明書ウィンドウ

B) CSR（証明書署名要求）を生成し、CA（認証局）に送信して署名します。

1. ExpresswayのWebページから、[Maintenace] > [Security] > [Server certificate] > [**Generate CSR]を選択します。**

2. [Generate CSR]ウィンドウの[Additional alternative names (comma separated)] フィールドに、セクションAに保存した[Subject Alternative Names]のすべての値を入力し、「DNS:」を削除してカンマで区切ります。次の画像を参照してください（「Alternative name as it will appeared」の横に、証明書で使用されるすべてのSANのリストが表示されます）。



CSR SANエントリの生成

3. [Additional Information] セクションの残りの情報（国、会社、州など）を入力し、[Generate CSR] をクリックします。

4. CSRを生成すると、[Maintenance] > [Security] > [Server Certificate] ページに[Discard CSR] と[Download] のオプションが表示されるので、[Download] を選択し、署名のためにCSRをCAに送信する必要があります。

> **注**：新しい証明書をインストールする前に[CSRを破棄する(Discard CSR)] を実行していないことを確認します。[CSRを破棄する(Discard CSR)] を実行した後、破棄されたCSRで署名された証明書をインストールしようとすると、証明書のインストールは失敗します。

C)新しい証明書のSANリストおよび拡張/拡張キー使用属性を確認します

Windows証明書マネージャで新しく署名された証明書を開き、次の項目を確認します。

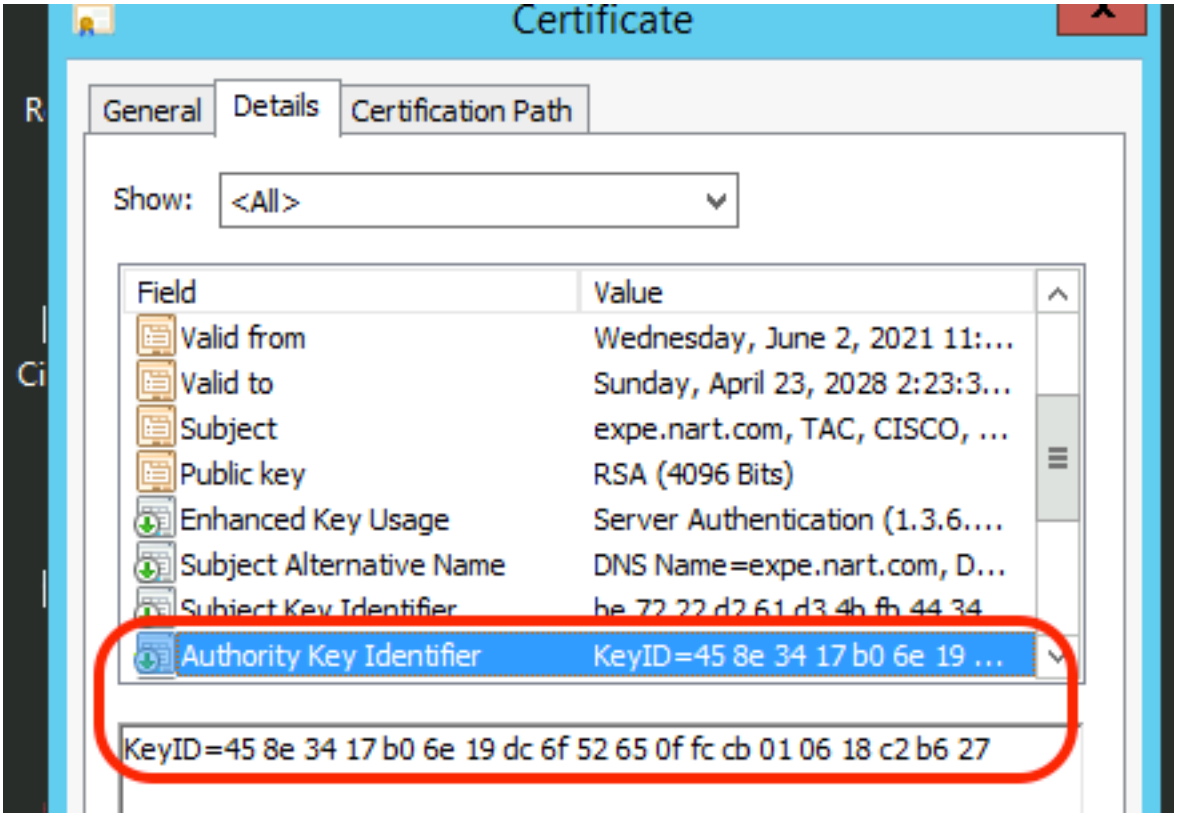
1. SANリストは、CSRを生成したセクションAで保存したSANリストと一致します。

2. [Extended/Enhanced key usage]属性には、[Client Authentication]と[Server Authentication]の両方が含まれている必要があります。

注：証明書の拡張子が.pemの場合は、.cerまたは.crtに名前を変更して、Windows証明書マネージャで開けるようにします。証明書をWindows証明書マネージャで開くと、[Details] タブ> [Copy to File] に移動して、Base64エンコードファイルとしてエクスポートできます。Base64エンコードファイルは、通常、テキストエディタで開くと上部に「-----BEGIN CERTIFICATE-----」、下部に「-----END CERTIFICATE-----」と表示されます

D)新しい証明書に署名したCAが、古い証明書に署名したCAと同じであるかどうかを確認します

Windows証明書マネージャで新しく署名された証明書を開き、「Authority Key Identifier」の値をコピーして、セクションAで保存した「Authority Key Identifier」の値と比較します。



Windows証明書マネージャーで開かれた新しい証明書

両方の値が同じ場合、新しい証明書の署名に使用されたCAと、古い証明書の署名に使用されたCAが同じであることを意味します。セクションEに進み、新しい証明書をアップロードできます。

値が異なる場合は、新しい証明書の署名に使用されるCAが古い証明書の署名に使用されるCAと異なっていることを意味します。セクションEに進む前に従う必要がある手順は次のとおりです。

1.すべての中間CA証明書（ある場合）とルートCA証明書を取得します。

2. [Maintenance] > [Security] > [Trusted CA certificate] に移動し、[Browse] をクリックして、コンピュータ上の中間CA証明書を検索し、アップロードします。他の中間CA証明書とルートCA証明書についても同じことを行います。

3.このサーバに接続するすべてのExpressway-E（更新対象の証明書がExpressway-C証明書の場合）またはこのサーバに接続するすべてのExpressway-C（更新対象の証明書がExpressway-E証明書の場合）で同じことを実行します。

4.更新する証明書がExpressway-C証明書で、CUCMに対してMRAまたはセキュアゾーンがある場合は、CUCMが新しいルートおよび中間CAを信頼し、ルートおよび中間CA証明書をCUCM tomcat-trustおよびcallmanager-trustストアにアップロードして、CUCMで関連サービスを再起動する必要があります。

E)新しい証明書のインストール

以前のすべてのポイントを確認したら、[メンテナンス(Maintenance)] > [セキュリティ(Security)] > [サーバ証明書(Server Certificate)] からExpresswayに新しい証明書をインストールできます。[参照(Browse)] をクリックし、コンピュータから新しい証明書ファイルを選択してアップロードします。

新しい証明書をインストールした後、Expresswayを再起動する必要があります。

> **注**：[メンテナンス(Maintenance)] > [セキュリティ(Security)] > [サーバ証明書(Server Certificate)] からExpresswayにアップロードする証明書にExpresswayサーバ証明書だけが含まれ、完全な証明書チェーンが含まれていないことを確認し、その証明書がBase64証明書であることを確認します

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。