# Cisco Expressway 証明書の作成と使用

## 導入ガイド

Cisco Expressway X8.2

D15061.03
2014 年 8 月

# 目次

# はじめに

この導入ガイドでは、Cisco Expressway（Expressway）で使用する X.509 暗号化証明書を作成する方法と、それを Expressway にロードする方法について説明します。

## PKI の概要

公開キー インフラストラクチャ（PKI）では、セキュアな通信を確立し（暗号化され完全性が保護される）、ID を確認できるメカニズムが提供されます。基本的な PKI は次のとおりです。

- **公開/秘密キーのペア**：公開キーがサーバに送信されるデータを暗号化するために使用されますが、そのデータを復号化するには秘密キー（サーバによって秘密が保持される）のみを使用できます。
- **データのシグニチャ**：データは、データおよびサーバの秘密キーの暗号化ハッシュの組み合わせを使用してサーバで「署名」ができます。クライアントは、サーバの公開キーを使用して、同じハッシュを確認することにより、シグニチャを確認できます。これにより、データが予期されたサーバから送信され、改ざんされていないことが保証されます。
- **証明書**：証明書は公開キーのラッパーで、キーの所有者に関する情報を提供します。このメタデータは X.509 形式で提供され、通常、所有者のサーバ名と連絡先の詳細が含まれます。
- **証明書チェーン**：証明書には、認証局（CA）が独自の秘密キーを使用して署名できます。したがって、証明書は CA の証明書（公開キー）に対するシグニチャを確認して、証明書が CA によって署名されていることを検証できます。Web ブラウザと他のクライアントには、信用する CA 証明書のリストがあり、個々のサーバの証明書を確認することができます。

Transport Layer Security（TLS）は、TCP/IP ネットワーク上のホスト間のセキュアな TCP 接続を確立する標準メカニズムです。たとえば、セキュアな HTTP（HTTPS）は TLS を使用してトラフィックを暗号化し確認します。TLS 接続を確立するには、次の手順に従います。

1. 最初の TCP 接続が行われると、クライアントがその機能（暗号スイートを含む）と乱数を送信します。
2. サーバはこれらの機能の選択、別の乱数およびその証明書に対応します。
3. クライアントは、サーバ証明書が信頼する CA によって発行（署名）され、廃止されていないことを確認します。
4. クライアントは、サーバの公開キーで暗号化された「プリマスタ シークレット」を送信します。
5. このプリマスタ シークレット（リプレイ アタックを防ぐため交換された乱数と組み合わせたもの）は、「マスター シークレット」を生成するために使用され、このマスター シークレットを使用してこの TLS セッションの残りの通信がクライアントとサーバ間で暗号化されます。

次の項では、これらの PKI コンポーネントを Expressway でどのように使用できるかについて説明します。

## Expressway での証明書使用の概要

Expressway は次の目的で証明書を必要とします。

- TLS（HTTPS）接続によるセキュアな HTTP
- SIP シグナリング、エンドポイントおよびネイバー ゾーンの TLS 接続
- Unified CM、Cisco TMS、LDAP サーバおよび syslog サーバなどの他のシステムへの接続

信頼できる認証局（CA）の証明書のリストと関連する証明書失効リスト（CRL）を使用して接続している他のデバイスを検証します。

サーバ証明書と秘密キーを使用して、署名付き証明書を提供し、Expressway がそのデバイスであるという証拠を提示します。これは、Microsoft Lync または Unified CM などの隣接デバイスおよび Web インターフェイスを使用する管理者が使用できます。

証明書は、Expressway を識別します。これには、それによって認識されトラフィックがルーティングされる名前が含まれます。クラスタの一部である場合など、これらの目的で Expressway が複数の名前によって認識される場合、RFC5922 のガイダンスに従って X.509 のサブジェクト データでこれを表す必要があります。証明書には、Expressway 自体とクラスタの両方の FQDN が含まれている必要があります。証明書がクラスタ ピアで共有される場合、考えられるすべてのピア FQDN をリスト化する必要があります。次のリストには、選択された導入モデルに応じて X.509 サブジェクトに含める必要があるものを示します。

Expressway がクラスタ化されない場合:

- サブジェクトの共通名 = Expressway の FQDN
- サブジェクトの代替名 = 空欄のまま

Expressway がクラスタ化され、Expressway ごとに個別の証明書がある場合:

- サブジェクトの共通名 = Expressway の FQDN
- サブジェクトの代替名 = Expressway の FQDN、クラスタの FQDN

ワイルドカード証明書は、サポートする複数のサブドメインとサービス名を管理し、SAN(サブジェクトの代替名)証明書よりも安全度が低い場合があります。Expressway はワイルドカード証明書をサポートしていません。

# 証明書生成の概要

X.509 証明書がサードパーティから提供されることがあります。または、OpenSSL などの証明書発行システムや Microsoft 認証局などのアプリケーションで使用できるツールで生成されることがあります。管理された環境またはテスト環境での Expressway の導入では内部で生成された証明書を使用できますが、認識された認証局から提供されたサードパーティ証明書を推奨します。

証明書の生成には通常 3 段階のプロセスがあります。

- ステージ 1:秘密キーの生成
- ステージ 2:証明書要求の作成
- ステージ 3:証明書の承認と作成

このマニュアルでは、ルート証明書、Expressway 用のクライアント/サーバ証明書、および秘密キーを生成する代替方法を提示します。

- 「証明書署名要求(CSR)の生成(5 ページ)」では、Expressway 自体を使用して、秘密キーと証明書要求を生成する方法について説明します。
- 「付録 2:OpenSSL のみを使用した証明書生成(15 ページ)」では、サードパーティまたは内部で管理された CA で使用できる OpenSSL 専用のプロセスについて説明します。

相互 TLS 認証の場合、Expressway **サーバ**証明書は、**クライアント**証明書としても使用できる必要があります。その場合に、Expressway が隣接サーバに対しクライアント デバイスとして認証することができます(「付録 5:「クライアントおよびサーバ」の証明書テンプレートによる Windows Server Manager の設定(23 ページ)」を参照)。

# 証明書署名要求(CSR)の生成

CSR には、秘密キーの所有者の ID 情報が含まれます。また、署名付き証明書の生成のためにサードパーティまたは内部の認証局に渡すことができます。また、Microsoft 認証局または OpenSSL などのアプリケーションとともに使用できます。

**注**:Expressway は SHA-256 ハッシュで生成された証明書を受け入れて使用できますが、ユーザ インターフェイスの CSR(証明書署名要求)ジェネレータは SHA-256 を選択するオプションを提供しません。

## Expressway を使用した CSR の作成

Expressway はサーバの証明書署名要求を生成できます。これにより、証明書要求を生成し取得するために外部メカニズムを使用する必要がなくなります。

CSR を生成するには、次の手順を実行します。

1. [Maintenance] > [Security certificates] > [Server certificate] を選択します。
2. [Generate CSR] をクリックして [Generate CSR] ページに移動します。
3. 証明書に必要なプロパティを入力します。
   - Expressway がクラスタの一部である場合は、「サーバ証明書とクラスタ化システム(5 ページ)」を参照してください。
   - この Expressway がユニファイド コミュニケーション ソリューションの一部である場合は、「ユニファイド コミュニケーションのサーバ証明書要件(6 ページ)」を参照してください。
   - 証明書要求には、証明書で使用される公開キーと、クライアントおよびサーバ認証の Enhanced Key Usage(EKU)の拡張が自動的に含まれます。
4. [Generate CSR] をクリックします。システムが署名要求と関連する秘密キーを生成します。
   秘密キーは、Expressway に安全に保存され、表示またはダウンロードすることはできません。認証局に対しても秘密キーを開示してはなりません。
5. [Server certificate] ページに戻ります。グローバル設定に関して実行できることは次のとおりです。
   - 認証局に送信できるようにローカル ファイル システムに要求を**ダウンロード**。ファイルを保存するよう求められます(実際の表現はブラウザによって異なります)。
   - 現在の要求の表示(人間可読形式で表示するには [Show (decoded)] をクリック、または raw 形式でファイルを表示するには [Show (PEM file)] をクリックします)。

注:1 回に 1 つの署名要求だけを進行させることができます。これは、Expressway が現在の要求に関連付けられた秘密キー ファイルを追跡する必要があるためです。現在の要求を廃棄し、新しい要求を開始するには、[Discard CSR] をクリックします。

ここで要求を承認し、署名済み PEM 証明書ファイルを生成する必要があります。サードパーティまたは内部の認証局に渡したり、Microsoft 認証局(「Microsoft 認証局を使用した要求の承認と証明書の生成(8 ページ)」を参照)や OpenSSL(「OpenSSL を使用した認証局としての動作(16 ページ)」)などのアプリケーションとともに使用できます。

署名済みのサーバ証明書を認証局から受信したときは、「Expressway での証明書およびキーのロード(10 ページ)」で説明されているとおりに Expressway にアップロードする必要があります。

### サーバ証明書とクラスタ化システム

CSR の生成時には、1 つの要求および秘密キーの組み合わせがそのピア専用に生成されます。

Expressway のクラスタがある場合は、各ピアで個別の署名要求を生成する必要があります。これらの要求はその後、認証局に送信し、返されたサーバ証明書を関連する各ピアにアップロードする必要があります。

正しいサーバ証明書が適切なピアにアップロードされていることを確認する必要があります。そうでないと、各ピアに保存された秘密キーがアップロードされた証明書に対応しません。

# ユニファイド コミュニケーションのサーバ証明書要件

Expressway の証明書署名要求（CSR）ツールでは、Expressway でサポートされるユニファイド コミュニケーション機能に適した関連するサブジェクト名の代替名（SAN）について確認が求められ、組み込まれます。

次の表は、どのユニファイド コミュニケーションの機能に CSR の代替名が適用されるかを示します。

| CSR SAN 要素 | Mobile & Remote Access | Jabber Guest | XMPP フェデレーション |
|---|---|---|---|
| Unified CM 登録ドメイン | ✓（Expressway-E のみ） | X | X |
| XMPP フェデレーション ドメイン | X | X | ✓（Expressway-E のみ） |
| IM and Presence のチャット ノード エイリアス（フェデレーテッド グループ チャット） | X | X | ✓ |
| Unified CM 電話セキュリティ プロファイル名 | ✓（Expressway-C のみ） | X | X |

**（注）**

- IM and Presence ノードの追加または名前変更、新しい TLS 電話セキュリティ プロファイルの追加などにより、チャット ノード エイリアスが追加または名前変更された場合は、Expressway-C 用に新しい Expressway-C 証明書を作成することが必要になる場合があります。
- 新しい Expressway-E 証明書は、新しいチャットのノード エイリアスがシステムに追加されるか、Unified CM または XMPP フェデレーション ドメインが変更された場合に生成する必要があります。
- 新しくアップロードされたサーバ証明書を有効にするには、Expressway を再起動する必要があります。

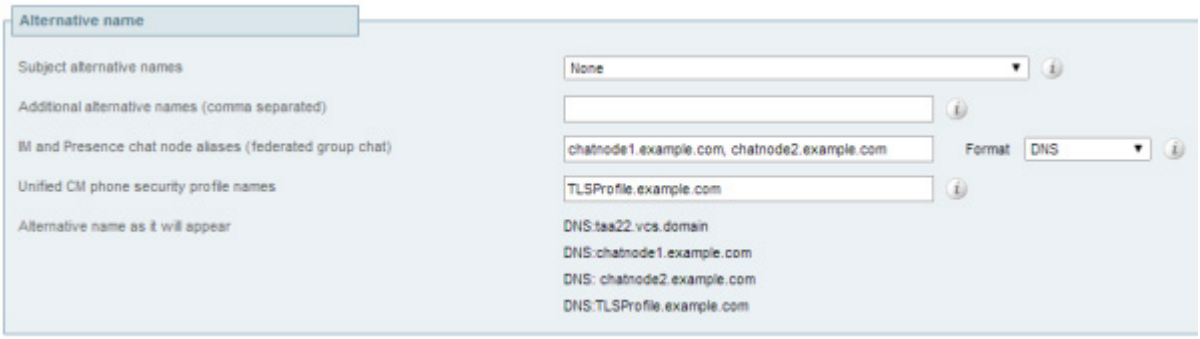
Expressway-C/Expressway-E の個々の機能要件についての詳細は、次のとおりです。

## Expressway-C のサーバ証明書の要件

Expressway-C サーバ証明書ではサブジェクト名の代替名のリストに、次の要素を含める必要があります。

- **Unified CM 電話セキュリティ プロファイル名**：暗号化された TLS 用に設定され、リモート アクセスを必要とするデバイスに使用される Unified CM のすべての**電話セキュリティ プロファイル**の FQDN 形式での名前。これにより、それらのセキュリティ プロファイルで設定されたデバイスからメッセージを転送するときに、Unified CM は TLS 接続を介して確実に Expressway-C と通信できます。
- **IM and Presence チャット ノード エイリアス（フェデレーテッド グループ チャット）**：IM and Presence サーバで設定される**チャット ノード エイリアス**（たとえば chatroom1.example.com）。これらは、フェデレーテッド連絡先との TLS を介したグループ チャットをサポートするユニファイド コミュニケーション XMPP フェデレーション導入にのみ必要です。
  Expressway-C は一連の IM&P サーバを検出すると、CSR にチャット ノード エイリアスを自動的に含めます。CSR を生成するときは、チャット ノード エイリアスに DNS 形式を使用することを推奨します。Expressway-E サーバ証明書の代替名には、同一のチャット ノード エイリアスを含める必要があります。

図 1：Expressway-C の CSR ジェネレータでのセキュリティ プロファイルおよびチャット ノード エイリアスに対するサブジェクト代替名の入力

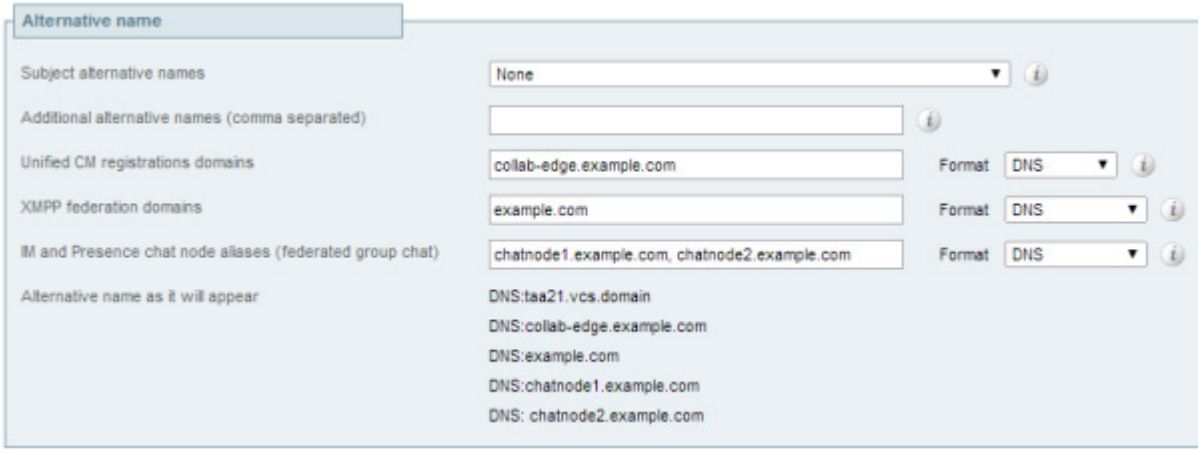



## Expressway-E のサーバ証明書の要件

Expressway-E サーバ証明書には、そのサブジェクト代替名のリストに次の要素が含まれる必要があります。

- **Unified CM 登録ドメイン**：Unified CM の登録用に Expressway-C で設定されているすべてのドメイン。これらはエンドポイント デバイスと Expressway-E 間のセキュアな通信に必要です。
  複数のドメインを必要とする場合は、*DNS* 形式を選択し、必要な FQDN をカンマで区切って手動で指定する必要があります。*SRVName* 形式は、選択した CA でサポートされないことがあります。
  また、それぞれの先頭に **`collab-edge.`** を付ける必要があります。（次のスクリーンショットの例を参照）
- **XMPP フェデレーション ドメイン**：ポイントツーポイント XMPP フェデレーションに使用するドメイン。これらは、IM&P サーバで設定され、XMPP フェデレーション用のドメインとして Expressway-C でも設定する必要があります。
  複数のドメインを必要とする場合は、*DNS* 形式を選択し、必要な FQDN をカンマで区切って手動で指定することを推奨します。*XMPPAddress* 形式は、選択した CA でサポートされていない場合があります。
- **IM and Presence チャット ノード エイリアス（フェデレーテッド グループ チャット）**：Expressway-C の証明書で入力されたものと同じ**チャット ノード エイリアス**のセット。フェデレーテッド連絡先との TLS を介したグループ チャットをサポートする音声とプレゼンスの導入にのみ必要です。
  複数のドメインを必要とする場合は、*DNS* 形式を選択し、必要な FQDN をカンマで区切って手動で指定することを推奨します。*XMPPAddress* 形式は、選択した CA でサポートされていない場合があります。
  注：必須エイリアスのリストは Expressway-C の同等の [Generate CSR] ページから、表示（およびコピー、ペースト）できます。

図 2：Expressway-E の CSR ジェネレータでの Unified CM 登録ドメイン、XMPP フェデレーション ドメイン、およびチャット ノード エイリアスに対するサブジェクト代替名の入力

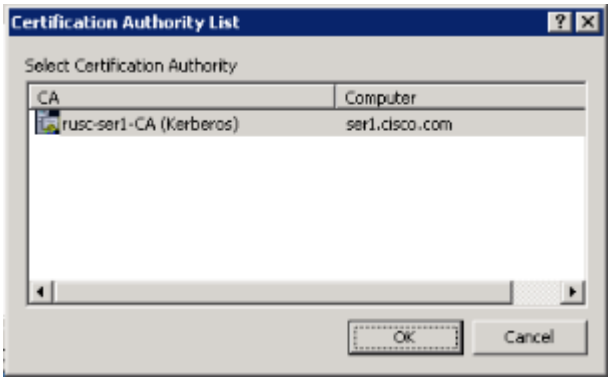


# Microsoft 認証局を使用した要求の承認と証明書の生成

ここでは、Microsoft 認証局を使用して、証明書要求を承認し PEM 証明書ファイルを生成する方法について説明します。

1. 証明書要求ファイル（たとえば、OpenSSL 経由で生成した場合は **certcsr.der** など）を、Microsoft 認証局のアプリケーションがインストールされているサーバのデスクトップなどの場所にコピーします。
2. コマンド プロンプトから証明書要求を送信します。
   - サーバ認証とクライアント認証で証明書を生成するには（これはネイバーまたはトラバーサル ゾーンを相互認証（**TLS 確認モード**）で設定する場合に必要になります）、次を入力します。
     **`certreq -submit -attrib "CertificateTemplate:Webclientandserver" C:\Users\<user>\Desktop\certcsr.der`**
     **`Webclientandserver`** 証明書テンプレートをセットアップする方法の詳細については、「付録 5:「クライアントおよびサーバ」の証明書テンプレートによる Windows Server Manager の設定（23 ページ）」を参照してください。
   - サーバ認証のみを使用して証明書を生成するには、次を入力します。
     **`certreq -submit -attrib "CertificateTemplate:WebServer" C:\Users\<user>\Desktop\certcsr.der`**

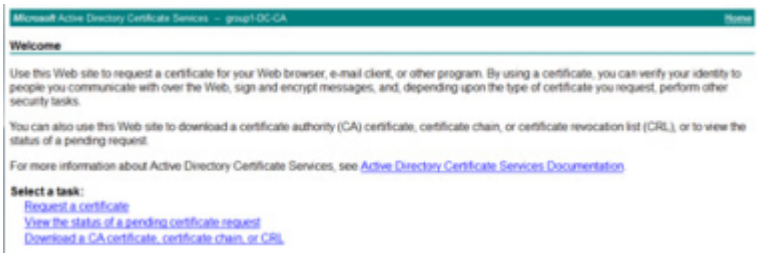
   これにより [Certification Authority] ウィンドウが開きます。



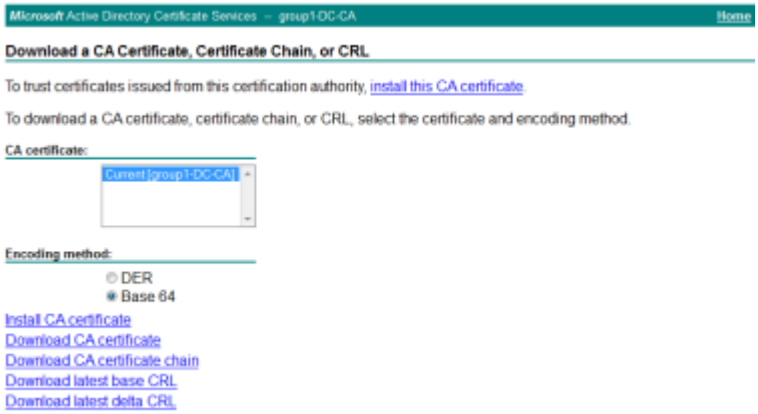

   コマンドは、管理者ユーザとして実行する必要があります。
3. 使用する**認証局**を選択し（通常は 1 つのみ提供されます）、[OK] をクリックします。
4. 要求されたら、**server.cer** などの名前を付けてその証明書を保存します（デフォルトの [Libraries] > [Documents] フォルダが使用されない場合は必要なフォルダを閲覧してください）。
5. Expressway で使用するために、名前を **server.cer** から **server.pem** に変更します。

### Microsoft の CA 証明書の取得

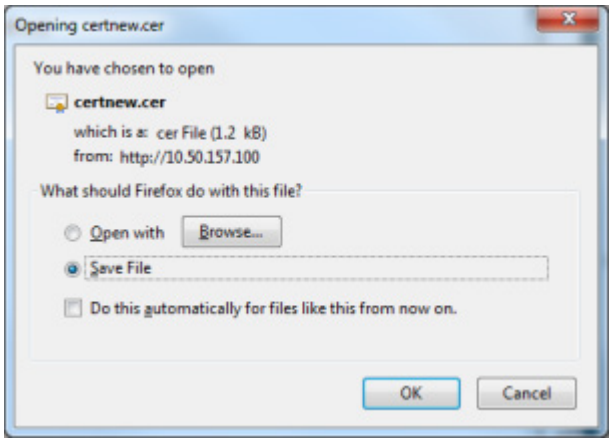
1. Web ブラウザで、[<IP or URL of the Microsoft Certificate Server>/certsrv] を選択し、ログインします。




2. [Download a CA certificate, certificate chain or CRL] を選択します。




3. [Base 64] を選択します。
4. [Download CA certificate] を選択します。




5. [Save File] を選択し、[OK] をクリックします。
6. 名前を **certnew.cer** から **certnew.pem** に変更します。

ファイル **server.pem** と **certnew.pem** が使用可能になりました。

このドキュメントの「Expressway での証明書およびキーのロード（10 ページ）」の項に移動し、**server.pem** および **certnew.pem** を Expressway にアップロードします。

# Expressway での証明書およびキーのロード

Expressway は、標準の X.509 証明書を使用します。証明書情報は、PEM 形式で Expressway に提供される必要があります。通常、次の 3 つの要素がロードされます。

- サーバ証明書(証明書の所有者の ID を識別することで認証局によって生成され、クライアントおよびサーバ両方の証明書として機能できる必要があります)。
- 秘密キー(クライアントに送信されるデータに署名し、サーバ証明書の公開キーで暗号化されたクライアントから送信されたデータを複合化するために使用されます)。これは、Expressway 上でのみ保持し、安全な場所にバックアップする必要があります。TLS 通信のセキュリティはこの保持された秘密に依存します。
- 信頼できる認証局の証明書のリスト。

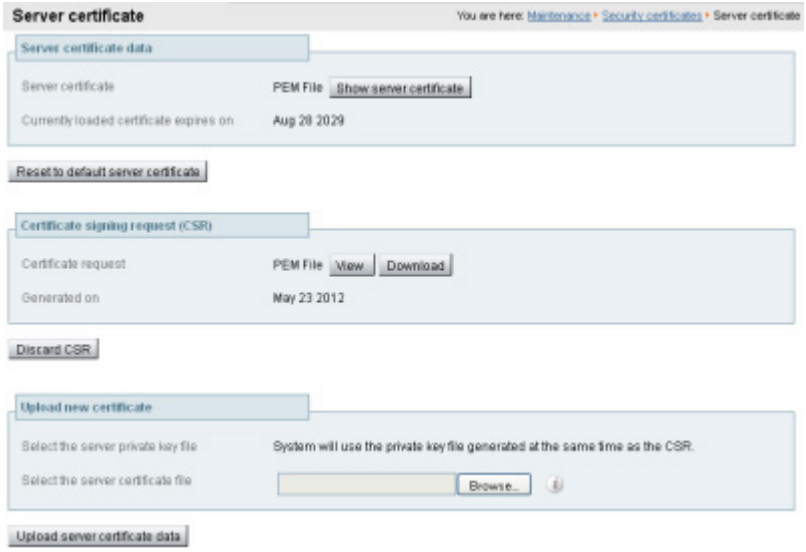
**注**:Expressway ソフトウェア(X8.1 以降)の新規インストールには、一時的に信頼された CA と、その一時的な CA によって発行されたサーバ証明書が付属しています。サーバ証明書を信頼できる認証局により生成された証明書に置き換え、信頼する認証局の CA 証明書をインストールすることを強く推奨します。

## Expressway でのサーバ証明書と秘密キーのロード

Expressway のサーバ証明書は、TLS 暗号化および HTTPS を介した Web ブラウザを使用してクライアントシステムと通信するときに Expressway を識別するために使用されます。

サーバ証明書をアップロードするには、次の手順を実行します。

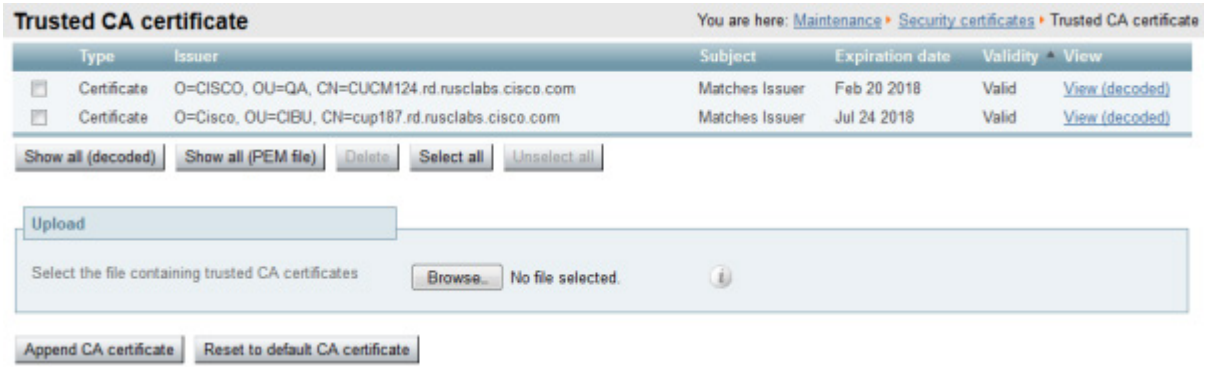
1. [Maintenance] > [Security certificates] > [Server certificate] を選択します。
2. [Upload new certificate] セクションの [Browse] ボタンを使用して、**サーバ証明書**の PEM ファイルを選択してアップロードします。
3. 証明書署名要求(CSR)を生成するために外部システムを使用した場合は、サーバ証明書を暗号化するために使用された**サーバ秘密キー**の PEM ファイルもアップロードする必要があります。(Expressway がこのサーバ証明書用の CSR を生成するために使用された場合、秘密キー ファイルがすでに自動的に生成され保存されています。)
   - **サーバ秘密キー**の PEM ファイルはパスワードで保護してはいけません。
   - 証明書署名要求の進行中は、サーバの秘密キーをアップロードできません。
4. [Upload server certificate data] をクリックします。



# 信頼できる CA 証明書リストの管理

[Trusted CA certificate] ページ（[Maintenance] > [Security certificates] > [Trusted CA certificate]）では、この Expressway で信頼される認証局（CA）の証明書のリストを管理できます。Expressway への TLS 接続が証明書検証を要求したときは、Expressway に提示された証明書が、このリストの信頼できる CA によって署名され、ルート CA に対する完全なトラスト チェーン（中間 CA）がある必要があります。

- 1 つ以上の CA 証明書を含む新しいファイルをアップロードするには、必要な PEM ファイルを**参照**し、[Append CA certificate] をクリックします。これにより、新しい証明書が CA 証明書の既存リストに加えられます。特定の発行者およびサブジェクトの既存の証明書を交換する場合は、手動で以前の証明書を削除する必要があります。
- 現在アップロードされたすべての CA 証明書をシステムの信頼できる CA 証明書の元のリストと交換するには、[Reset to default CA certificate] をクリックします。
- 現在アップロードされた信頼できる CA 証明書のリスト全体を表示する場合、人間可読形式で表示するには [Show all (decoded)] をクリック、または raw 形式でファイルを表示するには [Show all (PEM file)] をクリックします
- 個別の信頼できる CA 証明書を表示するには、特定の CA 証明書の行で [View (decoded)] をクリックします。
- 1 つ以上の CA 証明書を削除するには、該当する CA 証明書の隣にあるボックスにチェックを入れて、[Delete] をクリックします。



# 証明書失効リスト(CRL)の管理

証明書失効リスト(CRL)のファイルは、TLS/HTTPS を介して Expressway と通信するクライアント ブラウザおよび外部システムにより提示される証明書を検証するために Expressway によって使用されます。CRL は、廃棄され Expressway との通信に使用できなくなった証明書を識別します。

TLS/HTTPS クライアントおよびサーバ証明書に署名する CA の CRL データをアップロードすることを推奨します。イネーブルの場合、CRL のチェックはトラスト チェーンのすべての CA に適用されます。

## CRL 送信元

Expressway は、複数のソースから CRL 情報を取得できます。

- CRL 分散ポイントからの CRL データの自動ダウンロード
- チェックされる証明書の OCSP(Online Certificate Status Protocol)レスポンダ URI を経由(SIP TLS のみ)
- CRL データの手動アップロード
- Expressway の**信頼できる CA 証明書**ファイル内に組み込まれた CRL データ

次の制約事項および使用上のガイドラインが適用されます。

- SIP TLS 接続を確立するときに、CRL データ ソースは、[SIP] 設定ページの [Certificate revocation checking] 設定に従います。
- 自動的にアップロードされた CRL ファイルは、手動でロードされた CRL ファイルを上書きします(両方が手動でアップロートされたか自動的にダウンロードされた CRL データが使用されるときの SIP TLS 接続性を確認する場合を除く)。
- 外部ポリシー サーバによって提示された証明書を検証するとき、Expressway は手動でロードされた CRL のみを使用します。
- リモート ログイン アカウントの認証のために LDAP サーバとの TLS 接続を検証するとき、Expressway は、**信頼できる CA 証明書**内の CRL データのみを使用します。

### 自動 CRL 更新

自動 CRL 更新を実行するように Expressway を設定することを推奨します。これにより、最新の CRL が証明書の検証に使用できるようになります。

自動 CRL 更新を使用するように Expressway を設定するには、次の手順を実行します。

1. [Maintenance] > [Security certificates] > [CRL management] を選択します。
2. [Automatic CRL updates] を [Enabled] に設定します。
3. Expressway が CRL ファイルを取得できる **HTTP/HTTPS 分散ポイント**のセットを入力します。次の点に注意してください。
   - 新しい行にそれぞれ分散ポイントを指定する必要があります。
   - HTTP/HTTPS 分散ポイントのみがサポートされます。HTTPS を使用する場合、分散ポイントのサーバ自体に有効な証明書が必要です。
   - PEM および DER エンコード CRL ファイルがサポートされています。
   - 分散ポイントは、CRL ファイルまたは複数の CRL ファイルを含む ZIP および GZIP アーカイブを直接示す場合があります。
   - URL またはダウンロードしたアーカイブから解凍されたファイルのファイル拡張子は、Expressway がその基盤となるファイル タイプを決定するため、重要ではありませんが、代表的な URL は次の形式となります。
     - http://example.com/crl.pem
     - http://example.com/crl.der
     - http://example.com/ca.crl
     - https://example.com/allcrls.zip
     - https://example.com/allcrls.gz

4. [Daily update time] を入力します(UTC 単位で)。これは、Expressway が分散ポイントからその CRL の更新を試行するおおよその時刻です。
5. [Save] をクリックします。

### 手動 CRL の更新

CRL ファイルは、Expressway に手動でアップロードすることもできます。外部ポリシー サーバによって提示された証明書は、手動でロードされた CRL に対してのみ検証できます。

CRL ファイルをアップロードするには、次の手順を実行します。

1. [Maintenance] > [Security certificates] > [CRL management] を選択します。
2. [Browse] をクリックして、ファイル システムから必要なファイルを選択します。また、PEM エンコード形式である必要があります。
3. [Upload CRL file] をクリックします。
   これにより、選択されたファイルがアップロードされ、以前にアップロードされた CRL ファイルが置き換えられます。

Expressway から手動でアップロードされたファイルを削除する場合は、[Remove revocation list] をクリックします。

注:認証局の CRL が期限切れの場合、その CA から発行されたすべての証明書が無効として扱われます。

## SIP TLS 接続の失効確認の設定

また、証明書失効確認が SIP TLS 接続でどのように管理されるかを設定する必要があります。

1. [Configuration] > [SIP] を選択します。
2. [Certificate revocation checking] セクションまでスクロールし、適宜設定を行います。

| フィールド | 説明 | 使用方法のヒント |
|---|---|---|
| **Certificate revocation checking mode** | 失効確認が SIP TLS 接続の確立時に交換された証明書に対し実行されるかどうかを制御します。 | 失効確認をイネーブルにすることを推奨します。 |
| **Use OCSP** | Online Certificate Status Protocol(OCSP)を証明書失効確認を実行するために使用するかどうかを制御します。 | OCSP を使用するには、チェック対象の X.509 証明書に OCSP レスポンダの URI が含まれている必要があります。 |
| **Use CRLs** | 証明書失効リスト(CRL)を証明書失効確認を実行するために使用するかどうかを制御します。 | CRL は、証明書が OCSP をサポートしていない場合に使用できます。 |
| **Allow CRL downloads from CDPs** | X.509 証明書に含まれる CDP URI からの CRL のダウンロードを許可するかどうかを制御します。 | |
| **Fallback behavior** | たとえば、失効の送信元に連絡を取れないなど、失効ステータスを確立できない場合に、失効確認の動作を制御します。<br>[Treat as revoked]:証明書を失効したとして処理します(そのため、TLS 接続を許可しません)。<br>[Treat as not revoked]:証明書を失効していないとして処理します。<br>デフォルト:[Treat as not revoked] | [Treat as not revoked] では、失効の送信元に連絡を取れない場合、システムは通常の方法で稼働し続けますが、失効した証明書が承認される可能性があることを意味します。 |

# 付録 1：トラブルシューティング

## ネイバーおよびトラバーサル ゾーンでの SIP TLS ネゴシエーション エラー

**TLS 検証モード**がイネーブルの場合、ゾーン設定の [Peer address] フィールドに指定されたネイバー システムの FQDN または IP アドレスがそのシステムで提示された X.509 証明書に含まれる証明書の所有者名と照合するために使用されます。（名前は、証明書のサブジェクト共通名またはサブジェクト代替名の属性のどちらかに含まれている必要があります。）証明書自体も有効で信頼できる認証局によって署名される必要があります。

そのため、証明書がピアまたはクラスタ FQDN で生成されている場合は、ゾーンの [Peer address] フィールドが IP アドレスではなく FQDN で設定されていることを確認します。

## 8192 ビットのキー長を有する証明書

8192 ビットのキー長を有する証明書を使用する場合、SIP TLS ゾーンがアクティブになれない場合があります。4096 ビットのキー長を有する証明書を使用することを推奨します。

## Mobile & Remote Access 使用時のサービス障害

末尾の改行文字を含まない秘密キー ファイルをアップロードした場合、証明書のエラーによりユニファイド コミュニケーションの Mobile & Remote Access サービスが失敗する場合があります。

秘密キー ファイルに末尾の改行文字が含まれていることを確認してください。

# 付録 2:OpenSSL のみを使用した証明書の生成

ここでは、OpenSSL を使用した Expressway の秘密キーと証明書要求の生成プロセスについて説明します。これは、フリーの OpenSSL パッケージのみに依存する一般的なプロセスで、他のソフトウェアには依存しません。これは、証明書がテスト目的でネイバー デバイスとの連動を必要とする場合や、認証局と相互作用するために出力の提供を必要とする場合に適しています。

**注**:Expressway は SHA-256 ハッシュで生成された証明書を受け入れて使用できますが、ユーザ インターフェイスの CSR(証明書署名要求)ジェネレータは SHA-256 を選択するオプションを提供しません。

証明書要求の生成プロセスの出力は、組織の内部または外部の認証局に提供され、Expressway が隣接デバイスとの認証に必要とする X.509 証明書を作成するために使用できます。

ここでは、プライベート認証局の管理に OpenSSL をどのように使用できるかについても簡単に説明しますが、包括的なものではありません。これらのプロセスのさまざまなコンポーネントは、サードパーティ CA とやりとりするときに使用できます。

### OpenSSL および Mac OS X または Linux

OpenSSL は、Mac OS X にすでにインストールされており、通常は Linux にインストールされています。

### OpenSSL と Windows

OpenSSL をまだインストールしていない場合は、http://www.openssl.org/related/binaries.html から無料でダウンロードできます。

適切な 32 ビットまたは 64 ビットの OpenSSL を選択します。「Light」バージョンで十分です。

OpenSSL のインストール中に C++ ファイルを検出できないという警告を受信した場合は、このサイトでも使用可能な「Visual C++ Redistributables」をロードし、OpenSSL ソフトウェアをリロードします。

## OpenSSL を使用した証明書要求の作成

このプロセスでは、後で CA によって検証される場合があるサーバの秘密キーと証明書要求が作成されます。これは、ローカルで作成および管理されている CA やサードパーティ CA にすることができます。

コマンド プロンプトから次を実行します。

1. Windows の場合:OpenSSL がインストールされているディレクトリに変更します(通常は「bin」ディレクトリ)。
   Mac OS X の場合:ユーザ ディレクトリのルートを維持します。
2. openssl.cfg ファイルをパーソナライズします。
   a. Windows の場合:**openssl.cfg** を **openssl_request.cfg** にコピーします。
      Mac OS X の場合:**/System/Library/OpenSSL/openssl.cnf** を **openssl_request.cfg** としてユーザ ディレクトリのルートにコピーします。
   b. 上記のコピー コマンドにより作成された openssl_request.cfg ファイルをテキスト エディタを使用して編集し、「**`req_extensions = v3_req # The extensions to add to a certificate request`**」の行の最初に # がないことを確認します。# がある場合は、削除します。
   c. 「**`[v3_req]`**」セクションまでスクロールし、このセクションのタイトルの下に次を追加します。
      **`extendedKeyUsage=serverAuth, clientAuth`**
   d. ファイルを保存します。

3. 証明書が Expressway のクラスタ用の場合:
   a. 同じく「**[v3_req]**」セクションの下に次を追加します。
      **subjectAltName="DNS:<FQDN of Expressway cluster>,DNS:<FQDN of peer 1>, DNS:<FQDN of peer 2>,DNS:<FQDN of peer n>"**
      このセクションの下の行(「[ v3_ca ]」の前)に、必要に応じて Expressway の導入の詳細を記入します(すべてのピアのクラスタ FQDN と FQDN)。
   b. ファイルを保存します。
4. 次のコマンドを実行して、秘密キーを生成します。
   **openssl genrsa -out privatekey.pem 2048**
   **privatekey.pem** ファイルが証明書要求を作成するために使用され、Expressway へのロードにも必要になります。ファイルは、openssl コマンドが実行されるディレクトリに作成されます。
5. 次のコマンドを実行して、(Microsoft 認証局での使用に適した)証明書要求を生成します。
   **openssl req -new -key privatekey.pem -config openssl_request.cfg -out certcsr.der -outform DER -sha1**
6. 次の項目を含む、要求されたデータを入力します。
   - 国
   - 都道府県
   - 地域名
   - 組織名
   - 組織単位
   - 共通名:証明書が Expressway のクラスタ用である場合は Expressway クラスタ FQDN になり、証明書が単一の Expressway 用である場合は Expressway の FQDN になります。
   - 電子メール アドレス:任意、空欄のままでも可
   - チャレンジ パスワード:任意、空欄のままでも可
   - 任意の会社名:任意、空欄のままでも可

   要求されたデータを入力後、証明書要求ファイル **certcsr.der** が使用可能になります。

DNS エントリが要求に正しく入力されたことを検証するために、次のコマンドを使用して **certcsr.der** ファイルを復号することができます。

**openssl req -text -noout -in certcsr.der -inform DER**

この証明書要求ファイルは、X.509 証明書を生成するために内部またはサードパーティの認証局に渡すことができます。OpenSSL は下記のように、プライベート CA を運用するために使用できます。

# OpenSSL を使用した認証局としての動作

主要な導入では、サードパーティの認証局を使用するか、または組織の IT 部門にすでに内部認証局が 1 つ存在する可能性があります。ただし、次に説明するように、OpenSSL を使用してプライベート認証局で証明書を管理することができます。

CA として機能するように OpenSSL をすでに設定している場合は、「OpenSSL を使用した署名付き証明書の作成(18 ページ)」の項に進んでください。

## CA として機能するよう OpenSSL を設定する

OpenSSL は強力なソフトウェアで、CA として動作するには、発行された証明書を追跡するためのいくつかのディレクトリとデータベースの設定が必要です。

ディレクトリとファイルのリストは、セクション **[CA_default]** の下の OpenSSL コンフィギュレーション ファイルで確認できます。デフォルトでは、作成が必要なファイル/ディレクトリは次のとおりです。

- 3 つのサブディレクトリ **certs**、**newcerts** および **private** を含む現在のディレクトリ内の **demoCA** ディレクトリ。
- **demoCA** ディレクトリ内の **index.txt** という名前の空ファイル。
- 2 桁の番号(10 など)を保存している **demoCA** ディレクトリ内の **serial** という名前のファイル。

たとえば、次のコマンドを使用します。

```
mkdir demoCA
cd demoCA
mkdir certs
mkdir newcerts
mkdir private
touch index.txt
echo 10 > serial
```

## OpenSSL を使用した認証局の作成

このプロセスで、認証局(CA)の秘密キーと証明書が作成され、他の証明書を検証するために使用可能になります。これは明示的にインストールされるもの以外のデバイスから信頼されることはありません。

コマンド プロンプトから次を実行します。

1. **demoCA** ディレクトリに移動していることを確認します。
2. Windows の場合:OpenSSL が **demoCA** ディレクトリにインストールされているディレクトリから **openssl.cfg** をコピーし、その名前を **openssl_local.cfg** に変更します。
   Mac OS X の場合:**/System/Library/OpenSSL/openssl.cnf** を **demoCA** ディレクトリにコピーし、その名前を **openssl_local.cfg** に変更します。
3. 上記のコピー コマンドにより作成された **openssl_local.cfg** ファイルをテキスト エディタを使用して編集します。**[CA_default]** セクションに次の変更を行います。
   a. **copy_extensions = copy** の行の最初に # がないことを確認します。# がある場合は、削除します。その行がコメント アウトされたままの場合は、CSR の属性が除去され、SSL サーバと SSL クライアントの属性は証明書に表示されません。
   b. **policy = policy_match** を **policy = policy_anything** に変更します。
   c. **dir = ./demoCA** を **dir =** に変更します。
   d. 任意で、**default_days = 365**(生成された証明書の効力が 1 年)を **default_days = 3650**(10 年、または適切な値を選択)に変更します。
   e. ファイルを保存します。
4. 次のコマンドを実行して、CA の秘密キーを生成します。
   **openssl genrsa -aes256 -out private/cakey.pem 4096**
   ここで、秘密キーを暗号化するパスワードが求められるので、強力なパスワードを選択し、安全な場所に記録します。cakey.pem ファイルが CA 証明書を作成し、他の証明書に署名するために使用されるので、安全に保持する必要があります。
5. 次のコマンドを実行して、CA 証明書を生成します。
   Windows の場合:**openssl req -new -x509 -days 3650 -key private/cakey.pem -config openssl_local.cfg -sha1 -extensions v3_ca -out cacert.pem**
   OS X の場合:**openssl req -new -x509 -days 3650 -key private/cakey.pem -config openssl_local.cfg -sha1 -extensions v3_ca -out cacert.pem**
6. キーのパスフレーズを入力し、次の項目を含む要求されたデータを入力します。
   - 国
   - 都道府県
   - 地域名
   - 組織名
   - 組織単位
   - 共通名:通常は、この CA の担当者の名前になります
   - 電子メール アドレス:任意、空欄のままでも可

要求されたデータを入力すると、処理が完了し、認証局の証明書 **cacert.pem** が使用可能になります。

## OpenSSL を使用した署名付き証明書の作成

このプロセスでは、以前に生成された証明書要求を使用して生成された CA キーでサーバ証明書に署名します。

コマンド プロンプトから次を実行します。

1. **demoCA** ディレクトリに存在することを確認します。
2. 証明書要求ファイル(**certcsr.pem**)が使用できることを確認してください。
   - 証明書要求が Expressway を使用して作成された場合は、次の手順を実行します(推奨プロセス)。
     Expressway からダウンロードしたファイルを **demoCA** ディレクトリにコピーし、その名前を **certcsr.pem** に変更します。
   - 証明書要求が OpenSSL を使用して作成された場合は、次の手順を実行します。
     以前に生成された証明書要求を **demoCA** ディレクトリにコピーして、次のコマンドを実行して PEM 形式に変換します。
     **`openssl req -in certcsr.der -inform DER -out certcsr.pem -outform PEM`**
3. 次のコマンドを実行して、署名済みサーバ証明書を生成します。
   **`openssl ca -config openssl_local.cfg -cert cacert.pem -keyfile private/cakey.pem -in certcsr.pem -out certs/server.pem -md sha1`**
   「failed to update database TXT_DB error number 2」というエラー メッセージを受信した場合は、**index.txt** ファイルの内容を削除してから、コマンドを再実行できます。
4. CA の秘密キーのパスワードを入力するように求められます。

サーバの署名付き証明書が **demoCA/certs/server.pem** として使用できるようになりました。

# OpenSSL を使用した自己署名証明書の作成

自己署名証明書を作成することは推奨しません。それらは、ユニファイド コミュニケーションの導入環境では動作しません。

その代わりに、前述のように OpenSSL を使用して認証局を作成する必要があります。

# 付録 3:DER 証明書ファイルの PEM 形式への変換

秘密キー、ルート(CA)証明書およびサーバ/クライアント証明書は、サードパーティ製ツール(または認証局から購入したツール)を使用して生成でき、PEM(必須形式、拡張子 .pem)または DER(拡張子 .cer)形式のファイルとして生成できます。

証明書は、Expressway で使用するには PEM 形式にする必要があります。DER から PEM 形式への変換は、次の項に記載されているように、OpenSSL または Windows を使用する 2 通りの方法のいずれかで行うことができます。

## OpenSSL を使用した DER 証明書ファイルの PEM ファイルへの変換

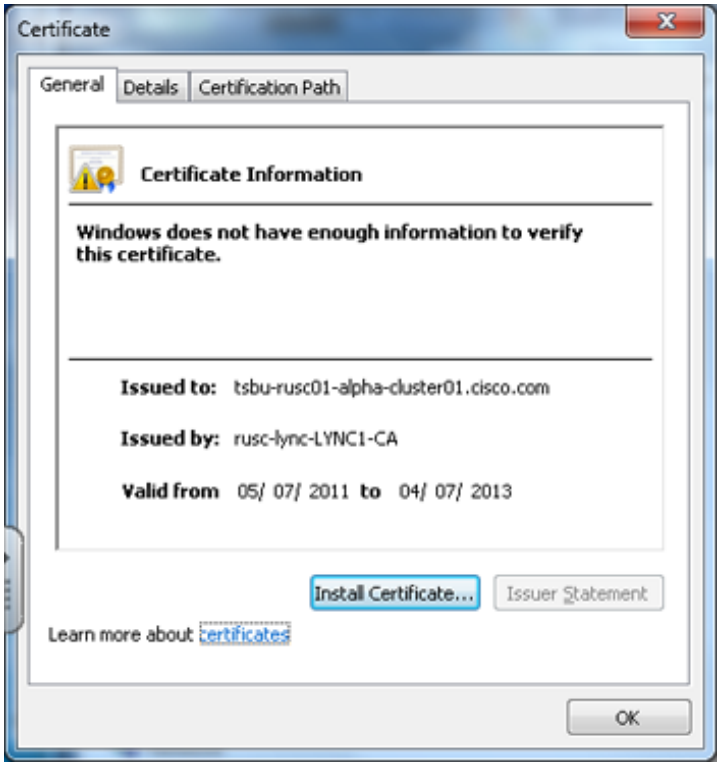
DER から PEM 形式へ変換するには、openssl を実行しているシステム上で次のコマンドを実行します。

```
openssl x509 -in <filename>.cer -inform DER -out <filename>.pem -outform PEM
```

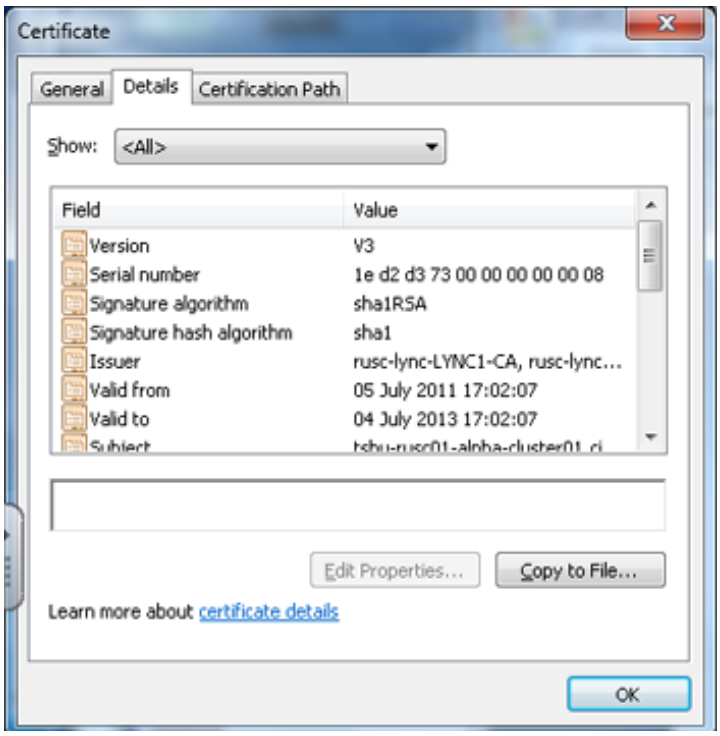
## Microsoft Windows を使用した DER 証明書ファイルの PEM ファイルへの変換

Microsoft Windows を使用して DER から PEM 形式へ変換するには、次の手順を実行します。

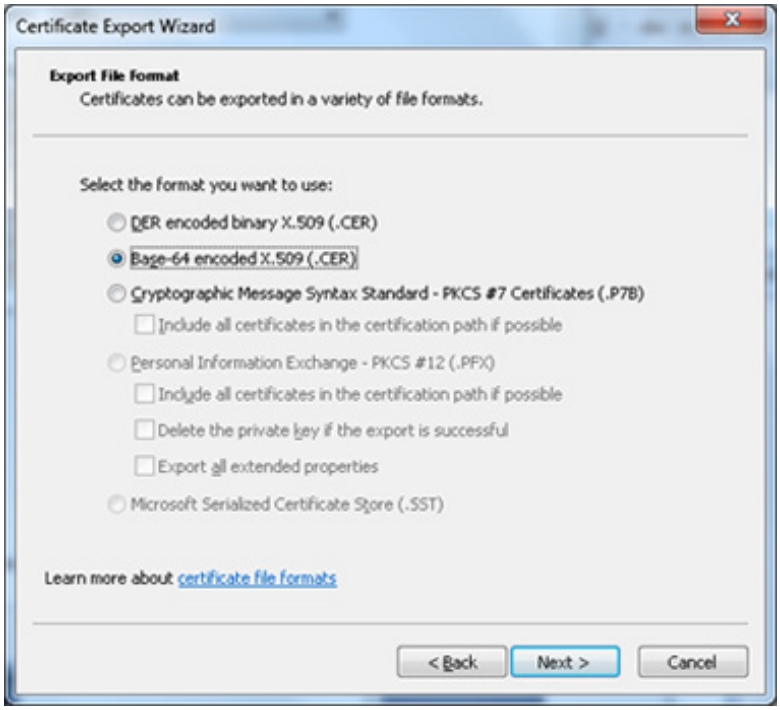
1. 変換する DER ファイルをダブルクリックします(拡張子は「.cer」である可能性があります)。




2. [Details] タブを選択します。




3. [Copy to File…] をクリックします。
4. [Welcome] ページで [Next] をクリックします。
5. [Base-64 encoded X.509 (.CER)] を選択して、[Next] をクリックします。




6. [Browse] をクリックして要求されるファイルの宛先(たとえば **server.pem**)を選択し、[Next] をクリックします。
7. [Finish] をクリックします。
8. **server.pem.cer** から **server.pem** にファイル名を変更します。
9. これは、このドキュメントの「Expressway での証明書およびキーのロード(10 ページ)」で使用されます。

# 付録 4:証明書の復号

ここでは、証明書の内容を復号して表示する方法についていくつか説明します。

### OpenSSL

PEM ファイル(**cert.pem** など)は、次のコマンドによって復号できます。

```
openssl x509 -text -in cert.pem
```

DER ファイル(**cert.cer** など)は、次のコマンドによって復号できます。

```
openssl x509 -text -inform DER -in cert.cer
```

### Firefox

閲覧している Web サイトで使用中の証明書は、アドレス バーのセキュリティ情報ボタンをクリックして、[More Information] と [View Certificate] をクリックすることで Firefox に表示できます。

### Internet Explorer

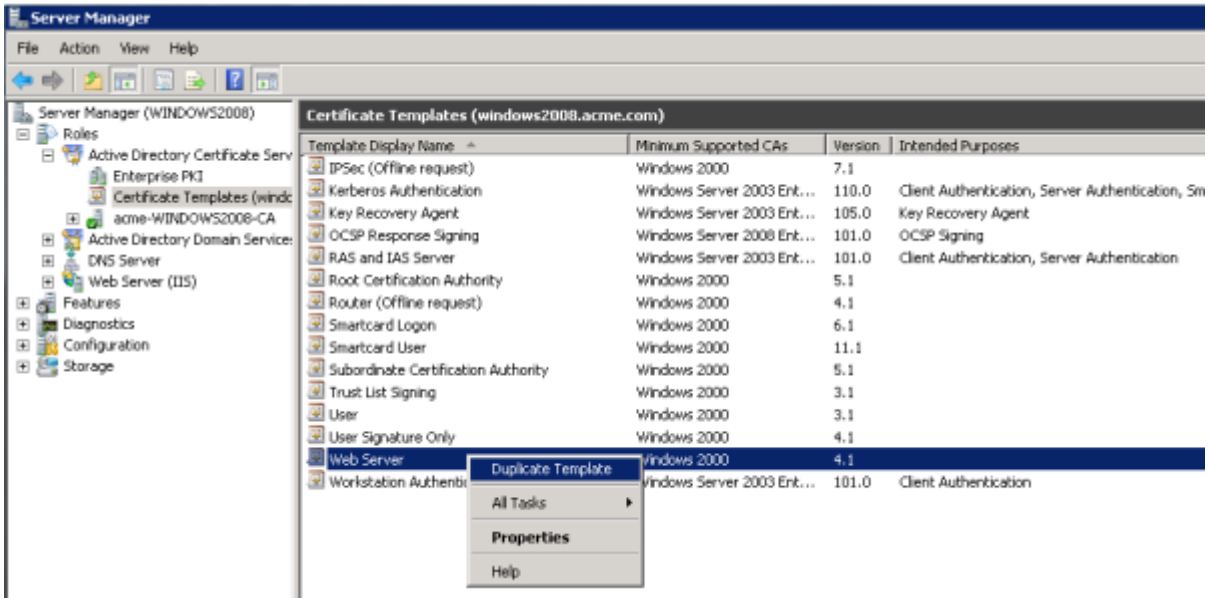
閲覧している Web サイトで使用中の証明書は、アドレス バーの右側にあるロック アイコンをクリックすることで Internet Explorer に表示できます。[Website Identification] ダイアログが表示されます。下にある [View Certificates] リンクをクリックします。

# 付録 5:「クライアントおよびサーバ」の証明書テンプレートによる Windows Server Manager の設定

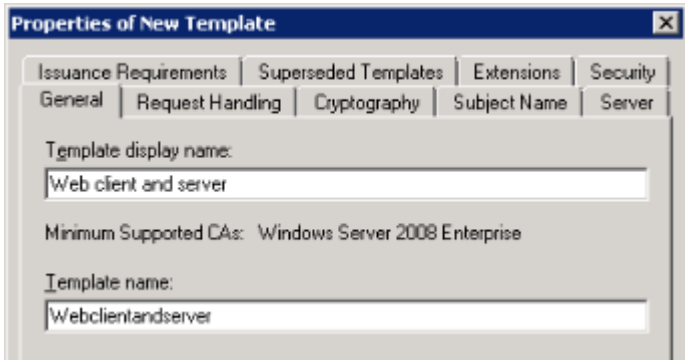
Microsoft 認証局のアプリケーションが使用するデフォルトの「Web サーバ」証明書テンプレートは、サーバ認証用の証明書のみを作成します。(**TLS 確認モード**がイネーブルの)相互認証でネイバーまたはトラバーサル ゾーンを設定する場合は、Expressway のサーバ証明書にもクライアント認証が必要です。

サーバおよびクライアント認証で証明書テンプレートを設定するには、次の手順を実行します。

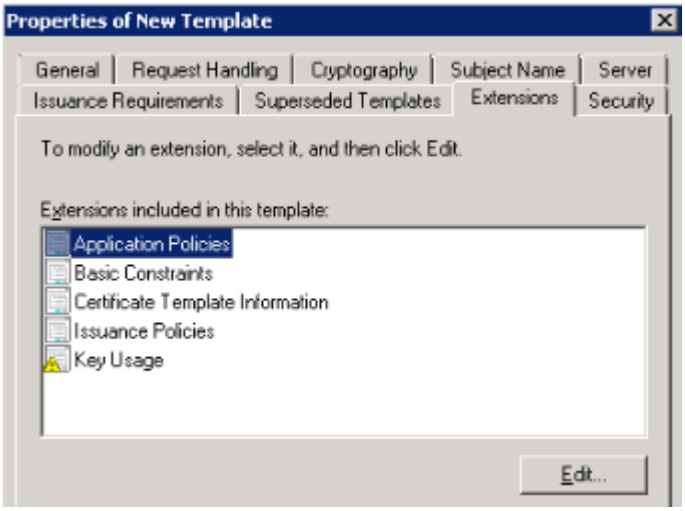
1. Windows で、**Server Manager** を開始します([Start] > [Administrative Tools] > [Server Manager])。(Server Manager は、Windows のサーバー エディションに含まれる機能です。)
2. [Server Manager] ナビゲーション ツリーを [Roles] > [Active Directory Certificate Services] > [Certificate Templates (<domain>)] まで展開します。
3. [Web Server] を右クリックして、[Duplicate Template] を選択します。



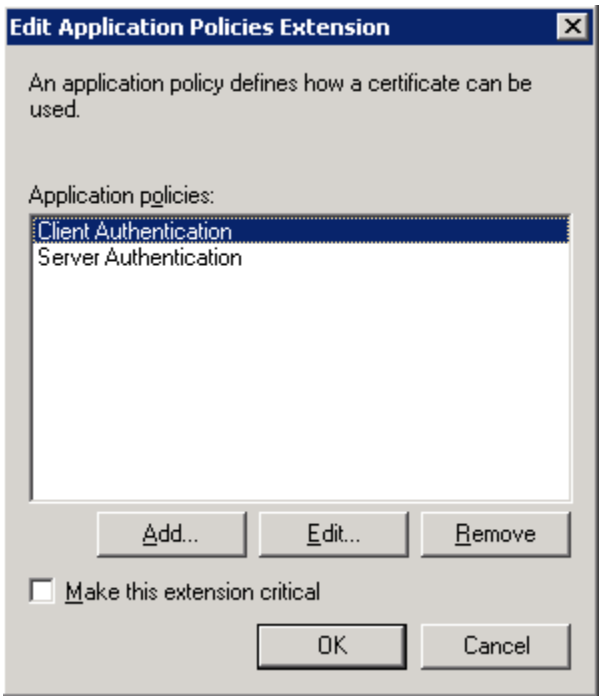

4. [Windows Server 2003 Enterprise] を選択し、[OK] をクリックします。
5. [General] タブで、[Template display name] と [Template name] をたとえば **`Web client and server`** や **`Webclientandserver`** などのように入力します。



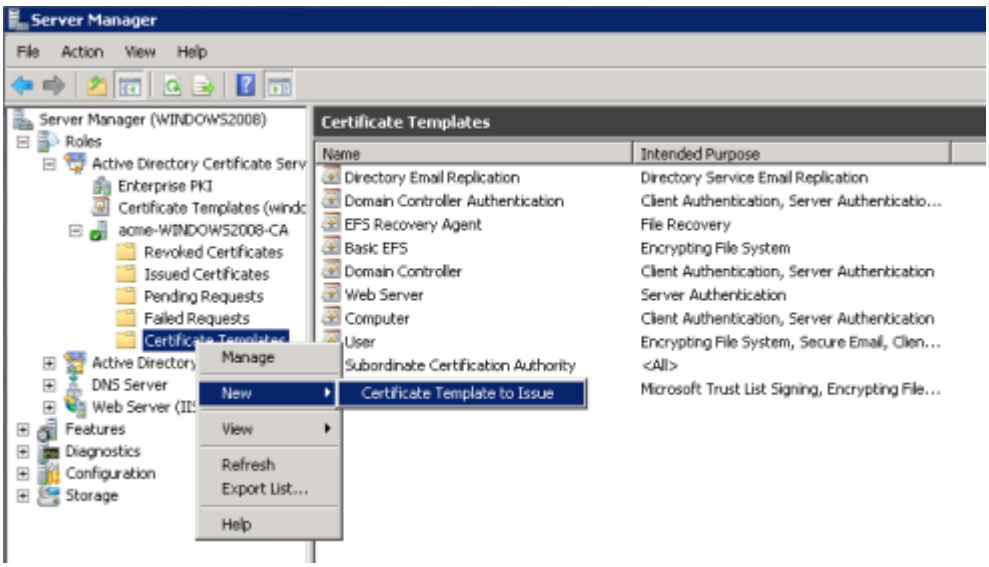
6. [Extensions] タブで、[Application Policies] を選択し、[Edit] をクリックします。



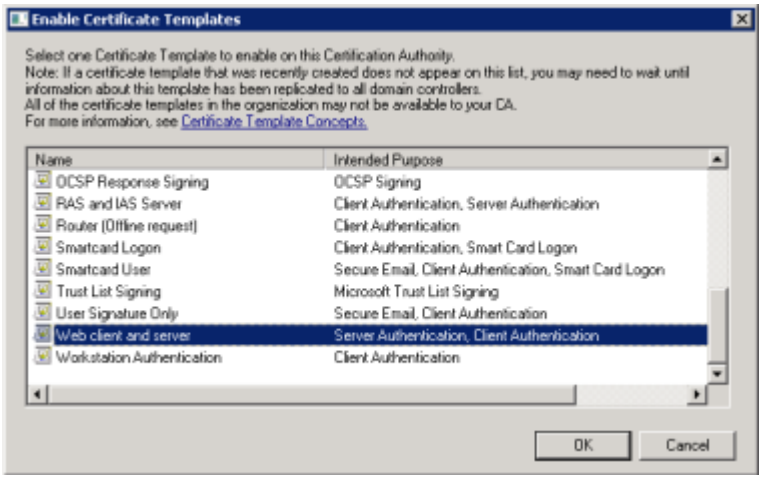

7. [Client Authentication] をアプリケーション ポリシーのセットに追加します。
   a. [Add] をクリックします。
   b. [Client Authentication] を選択し、[OK] をクリックします。
   c. [OK] をクリックします。




8. [OK] をクリックして、新しいテンプレートの追加を完了します。
9. 認証局に新しいテンプレートを追加するには、次の手順を実行します。
   a. [Roles] > [Active Directory Certificate Services] > [<ご自身の認証局>] を選択します。
   b. [Certificate Templates] を右クリックして、[New] > [Certificate Template to Issue] を選択します。




c. 新しい [Web client and server] テンプレートを選択し、[OK] をクリックします。




新しい [Web client and server] テンプレートが証明書要求をその Microsoft 認証局に送信するときに使用できるようになりました。

# マニュアルの変更履歴

次の表に、このマニュアルの変更履歴の要約を示します。

| リビジョン | 日付 | 説明 |
|---|---|---|
| 3 | 2014 年 7 月 | X8.2 用に再発行されました。ユニファイド コミュニケーション導入時のサーバ証明書用に変更された推奨されるオプション。 |
| 2 | 2014 年 6 月 | X8.2 向けに再発行。ユニファイド コミュニケーションの導入に関するサーバ証明書の要件が強化されました。 |
| 1 | 2013 年 12 月 | 初回リリース |