証明書署名要求の生成

証明書署名要求（CSR）には、秘密キーの所有者に関するアイデンティティ情報が含まれています。また、署名済み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、ACME、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。Expressway は、楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）または RSA ベースの公開キーアルゴリズムを使用した証明書署名要求の生成をサポートするようになりました。

Note 新しいサーバー証明書署名要求（CSR）を生成しても、Expressway にインストールされている既存のアクティブなサーバー証明書は無効になりません。

この章では、次の内容について説明します。

Expressway を使用する証明書署名要求の作成

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。

手順

Step 1 [メンテナンス（Maintenance）]>[セキュリティ（Security）]>[サーバ証明書（Server certificate）]に移動します。

Step 2 **[CSR の作成（Generate CSR）]**をクリックして **[CSR の作成（Generate CSR）]** ページに移動します。

Step 3 証明書に必要なプロパティを入力します。

1. **[追加情報（Additional Information）]** セクションで、**[公開キーアルゴリズム（Public key algorithm）]** を選択します。ドロップダウンで [RSA] または [ECDSA] を選択します。

2. 公開キーアルゴリズムに基づいて、ドロップダウンで目的の**キー長**（ビット単位）を選択します。

   （注） ECDSA – 256、384、521、RSA：2048、4096 の定義済みキー長（ビット単位）

3. Expressway がクラスタの一部である場合、サーバ証明書とクラスタ化システムを参照してください。
4. Expressway が Unified Communications ソリューションの一部である場合は、「Unified Communications 向けサーバー証明書要件」項を参照してください。
5. 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ー認証の Enhanced Key Usage（EKU）の拡張が自動的に含まれます。

Step 4 [CSR の作成（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。

Step 5 [サーバ証明書（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。

1. 認証局に送信できるように、要求をローカルファイルシステムに**ダウンロード**します。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）。
2. 現在の要求の表示（人間可読フォーマットで表示するには**[表示（復号化（Show (decoded)）]** をクリック、または raw フォーマットでファイルを表示するには **[表示（PEM ファイル）（Show (PEM file）]** をクリックします）。
3. 手動または自動 ACME の証明書に署名する CA に CSR を送信するには、ACME を使用します。

（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。
- バージョン X8.5.1 から、ユーザ インタフェースにダイジェスト アルゴリズムを設定するオプションがあります。デフォルトでは SHA-256 に設定されており、SHA-1、SHA-384、または SHA-512 に変更するオプションがあります。
- バージョン X8.10 以降では、SHA-1 を選択できません。
- Let's Encrypt から返される証明書の [発行元（Issuer）] と [件名（Subject）] フィールドには、都道府県、国、組織などの属性は含まれません。Expressway UI では CSR のこれらのフィールドにも入力する必要がありますが、入力した値は認証局では無視されます。

署名済みPEM証明書ファイルを生成するには、証明書署名要求を使用する必要があります。サードパーティまたは内部認証局に渡したり、Microsoft 認証局（「付録 6：Microsoft 認証局を使用す

る要求の承認と証明書の生成」）や OpenSSL（「OpenSSL を使用する承認局としての操作」）などのアプリケーションと連動して使用できます。

SAN に複数のエントリまたは FQDN がある場合（MRA 展開など）、単一の証明書ではなく、認証局からマルチドメイン/マルチ SAN 証明書を要求していることを確認します。一部の認証局は、特に要求しない限り、このオプションを推奨しません。

署名済みのサーバー証明書を認証局から受信したときは、「証明書とキーを Expressway にロード」で説明されている Expressway にアップロードします。

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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。