Expressway-E での ACME の使用

X12.5 以降、Cisco Expressway シリーズでは、ACME（AutomatedCertificate Management Environment）プロトコルをサポートするようになっています。このプロトコルにより、Let's Encrypt などの認証局から Cisco Expressway-E に署名済みの証明書を自動的に導入することが可能になります。この機能の主な利点は、Expressway-E を識別するサーバ証明書を低コストで生成できることです。したがって、MRA (モバイルおよび Remote Access) などの Expressway-E ベースの導入環境のコストを削減できます。

基礎となる検証メカニズムにより、この機能は MRA 導入環境に最も役立つ可能性があります。ビジネス ツー ビジネス (B2B) アプリケーションでは、ACME 証明書にプライマリ ドメインを含めるのが常に実用的であるとは限りません。

設定プロセスはシンプルです。Cisco Expressway-E で、証明書署名要求 (CSR) を作成するための情報を入力します。これにより、Expressway の ACME クライアントが認証局とやり取りして証明書を要求します。Expressway が証明書をダウンロードするので、ボタンをクリックするだけで展開できます。ACME 証明書の有効期間は意図的に短くされているため、この手動による手順を行った後、証明書が期限切れにならないように更新をスケジュールできます。

ACME プロトコルに伴う潜在的なセキュリティ侵害の 1 つとして、Cisco Expressway-E 上のポート 80 でのインバウンド HTTP 接続が必要になることです。このリスクを管理するには Expressway のセキュリティ機能を使用できますが、極めてセキュアな環境では、ACME を無効にして、任意の認証局で従来の CSR 手順を使用することもできます。

ACME での Jabber Guest サポートなし。

現在、Expressway では Jabber Guest 展開で ACME をサポートしていません。

この章では、次の内容について説明します。

ACME 展開の概要

1. ACME 証明書サービスの展開
2. Expressway-E で ACME 証明書サービスを構成
3. ACME に証明書署名要求を生成
4. ACME プロバイダーを使用して証明書署名要求に署名
5. （オプション）署名付き ACME 証明書の確認
6. ACME 証明書の展開
7. ACME 証明書の自動更新の有効化

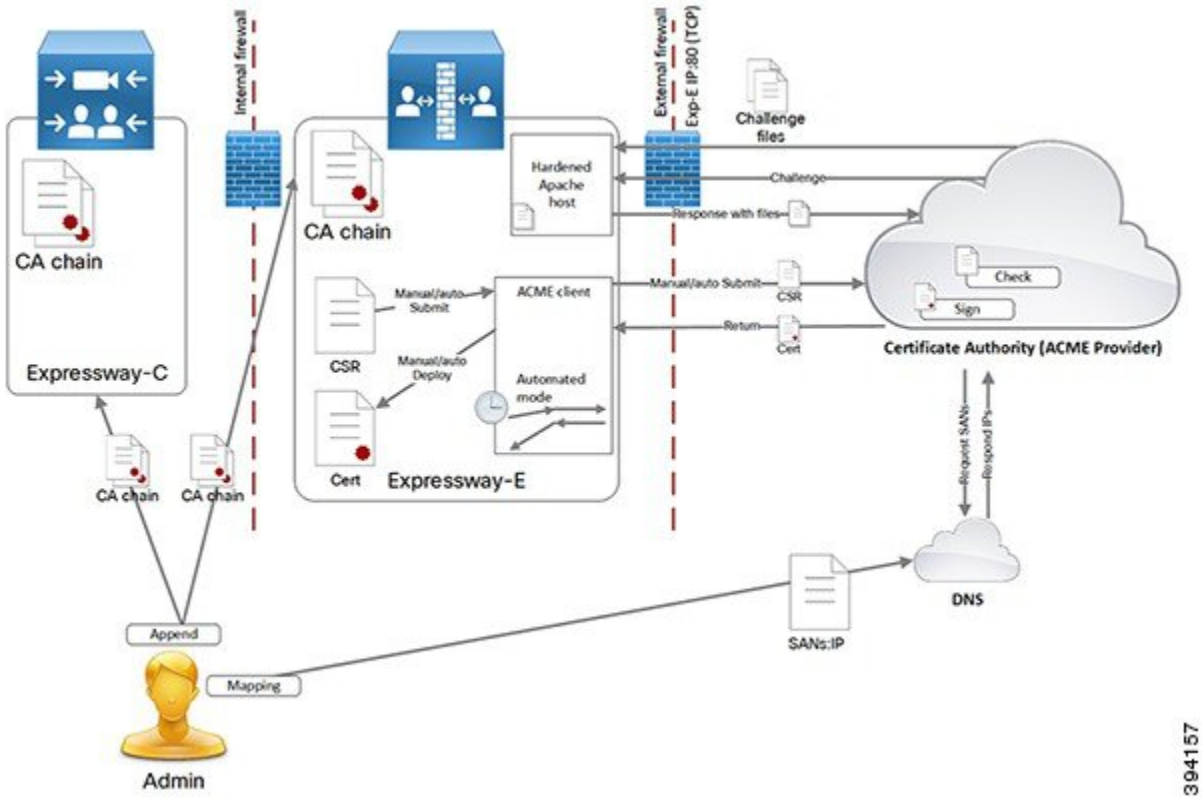
クラスタ展開の場合、ACME はクラスタレベルではなく**各ピアで個別に有効にする必要があります。**ほとんどの証明書操作はノードごとに実行されます。

ACME の仕組み

ACME は、Web ホストの自動証明書管理を可能にするクライアント サーバー プロトコルです。Expressway-E には、認証局の制御下にある ACME プロバイダーと双方向対話する ACME クライアントがあります。

現在、Let's Encrypt 機関と協力してサーバー証明書を生成しています。

また、ACME を使用して SNI（マルチテナンシー）のドメイン証明書を生成します。このプロセスは基本的にサーバー証明書プロセスと同じです。マルチテナンシーはHCS展開でのみサポートされており、SNI での ACME の使用に関する詳細は、Collaboration Knowledge ポータルの [証明書管理とサービス検出（Certificate Management and Service Discovery）] エリアを参照してください。



Expressway-E の ACME 証明書サービスは、このドキュメントの他の部分で説明されている方法とは異なる方法で、サーバー証明書を要求して Expressway-E に適用します。

重要な署名プロセスは次のとおりです。

- [要求の定義（Define request）] > [CA に送信（Submit to CA）] > [CA の生成（CA generates）] の順に選択し、[証明書にサイン（signs the certificate）] > [証明書の適用（Apply certificate）] の順に選択します。
- ACME証明書サービスはこのプロセスに従いますが、費用と手動作業の一部を取り除きます。
- このプロセスに関する注意点の1つは、CAが送信ホストに問い合わせて、証明書署名要求内のドメインを制御していることを確認する必要があることです。

共通の設定

ACME 証明書サービスを使用する場合は、常に次のタスクが必要です。

1. Expressway-E で証明書署名要求を作成します。
2. 証明書署名要求のドメインを使用してドメインネームシステム（DNS）を構成し、それらを Expressway-E のパブリック IP アドレスにマッピングします。
3. 各ドメインには、FQDN だけでなく、A レコードが必要です。

4. プロバイダーの詳細と電子メールアドレスを使用してACMEクライアントを設定します。

検証プロセスの暗号化

Let's Encryptは、証明書署名要求で要求されたすべてのドメインが要求元の制御下にあることを確認するために、それぞれに対してチャレンジを実行します。要求元が証明書署名要求の各ドメインのポート 80 でサービスを提供できる必要があるランダムな文字列を含むファイルを提供します。

Let's Encryptは、すべてのチャレンジファイルを正常に読み取った後にのみ証明書を発行します。

プロセスを手動で制御する場合の動作は次のとおりです。

手順

Step 1 署名プロセスを開始します。

1. ACME クライアントは、Let's Encrypt への HTTPS 接続を開き、証明書署名要求をアップロードします。
2. Let's Encrypt は、証明書署名要求内のドメインごとに 1 つずつ、チャレンジファイルのリストで応答します。
3. クライアントは、Expressway-E クラスタ内のすべてのピアにチャレンジファイルを配置します。
4. 各 Expressway-E ピアは、チャレンジファイルのみを提供するように設定された仮想 Apache ホストを起動します。
5. クライアントは、チャレンジファイルを提供する準備ができたことを Let's Encrypt に通知します。
6. Let's Encrypt は、チャレンジファイルの取得を試みます。
7. クライアントは、Let's Encrypt をポーリングして、チャレンジプロセスが成功したかどうかを確認します。
8. チャレンジ交換が成功した場合、クライアントは署名済み証明書をダウンロードしてステージングエリアに保存し、証明書を展開する準備ができたことを通知します。
9. Expressway-E ピアは仮想 Apache ホストを閉じます。

Step 2 展開プロセスを開始します。

1. Expressway-E は、既存のサーバー証明書にステージングされた証明書をコピーします。
2. 証明書署名要求に関連付けられた秘密キーを既存の秘密キーに上書きコピーします。

3. Expressway-Eは、サーバー証明書をリロードする必要があることを他の内部プロセスに通知します。（Expressway-E を再起動する必要はありません）。

Expressway-E は、TLS 接続を行うときに ACME 証明書を提示するようになりました。

頻繁な有効期限切れと影響の少ない更新

Let's Encrypt証明書は、設計上90日間のみ有効です。これは、証明書をより頻繁に更新する必要があることを意味します。ACME 証明書サービスでは、次のように対処しています。

- 有効期間の3分の2が期限切れになったときに新しい証明書を取得する自動更新モードを提供します。

  サービスが自動モードでない場合、3 分の 2 の時点で通知はありません。新しい署名要求を送信する必要があります。Let's Encrypt は、Expressway-E で ACME クライアントを構成するために使用するアカウントに期限切れ警告電子メールを送信します。

- ACME 証明書サービスを使用して新しい証明書を展開するときに Expressway-E を再起動する必要がなくなります（自動展開または手動展開）。

  証明書を使用する Expressway プロセスは、再起動せずに新しい証明書をロードできます。Expressway-E は TLS 接続をドロップせず、新しい接続試行に対して新しい証明書を提示します。

  モバイルおよびリモートアクセス クライアントのサービスは中断されません。

（注） 別の方法を使用して新しいサーバー証明書をアップロードする場合は、Expressway-E を再起動する必要があります。この動作は、ACME 証明書サービスの導入でも変更されていません。

自動更新モード

自動更新を構成するときに、1 週間のうち 1 日以上の特定の時刻をスケジュールできます。スケジュールは、新しい証明書の要求ではなく、証明書の展開にのみ使用されます。

サービスを自動モードにすると、サービスは最初の証明書を要求して受信し、次にスケジュールされた機会に証明書を展開します。その証明書の有効期間の 3 分の 2 が経過すると、ACME 証明書サービスは、保存されている証明書署名要求を自動的に再送信して新しい証明書を取得します。

1 日に 2 回の自動再送信の機会があります。これらは、チャレンジプロセスのセキュリティを向上させるために、意図的にランダムな時間に設定されています。このような場合、Expressway-E はポート 80 で要求を受け入れる必要があるため、予測不能にすることをお勧めします。

自動署名が成功すると、ACME 証明書サービスは、次にスケジュールされた機会にステージングされた証明書を自動的に展開します。これには数秒かかり、証明書を使用する実行中のプロセスには影響しません。

仮想 Apache ホストの詳細

Let's Encrypt は、上記のチャレンジと検証プロセスを使用して、証明書要求者が証明書署名要求のドメイン名を制御していることを確認する必要があります。ドメインが複数の IP アドレスに解決されると、Let's Encrypt はそれらのいずれかにランダムに接続するため、Let's Encrypt はクラスタ内のすべてのピアのポート 80 にアクセスできる必要があります。

送信元アドレスに基づいて Expressway-E ポートへのアクセスを制限することは実用的ではありません。これは、Let's Encrypt には、すべてのサーバーを含む簡潔なリストまたは CIDR がないためです。

悪意のあるアクセスのリスクを軽減するために、Apache 仮想ホストはチャレンジフェーズ中にのみ実行され、チャレンジファイルへの HTTP アクセスのみを許可するように制限されます。

Apache は、ポート 80 でリッスンするように構成され（そのポートでまだリッスンしていない場合）、ACME チャレンジトラフィック（のみ）を仮想 Apache ホストに転送します。

仮想ホストは、localhost インターフェイス上の 1 つの非特権ポートでのみリッスンします。仮想ホストは通常の方法で強化されます。ディレクトリの参照、シンボリックリンク、すべてのオプション、.htaccess ファイルの使用を拒否します。このため、HTTP から HTTPS へのリダイレクトは、Expressway E の Web 管理ポートがデフォルトの 443 ポートとして構成されている場合にのみサポートされます。

Expressway-E がポート 80 を 443 にリダイレクトするように構成されている場合：

- ACME チャレンジトラフィックの 80 から 443 へのリダイレクトルールに例外を追加します。この例外はバックグラウンドで自動的に追加され、手動で構成することはできません。
- 例外は、必要なパス（.well-known/acme-challenge/）への GET 要求でのみフィルタリングされます。

  したがって、特定のファイルパスへのポート 80 での GET 要求のみが仮想ホストに到達します。他のすべての要求は、通常どおりポート 443 にリダイレクトされます。

Expressway-E でポート 80 が有効になっていない場合：

- ポート 80 でリッスンするように Apache を構成します。
- ACME チャレンジファイルの GET 要求をポート 80 で仮想 Apache ホストにリダイレクトするルールを追加します。
- 他のすべての要求は、HTTP エラー 404（not found）を返します。

チャレンジプロセスは、証明書署名要求内のドメインの数と Expressway クラスタ内のピアの数に応じて、数分間続くことがあります。

チャレンジが完了すると、次のようになります。

- チャレンジファイルを削除します。
- 80 から 443 へのリダイレクトルールの例外を削除します。
- 443 へのリダイレクトを許可するように構成されていない場合、Apache がポート 80 でリッスンしないようにします。
- Apache 仮想ホストを停止します。

ACME 証明書サービスの展開

前提条件

- 法定代理人に連絡して、Let's Encrypt の利用規約を確認してください。
- 証明書で CN または SAN として必要な Expressway-E へのマッピングを使用してドメインネームシステム（DNS）を設定します。
- Let's Encrypt CA で使用する電子メールアカウントを作成します。
- Let's Encrypt ルート CA 証明書を Expressway の信頼ストアに追加します。
- Let's Encrypt 中間 CA 証明書を Expressway の信頼ストアに追加します。
- インターネットから Expressway-E のパブリックアドレスへの TCP 80 インバウンドを有効にします。
- SAN 上のすべてのドメインに（FQDN だけでなく）有効な A レコードがあることを確認します。**ドメイン**のレコードが別の Web サーバーによってすでに使用されている場合は、証明書署名要求で *collab-edge* ドメインを構成し、その A レコードを設定できます。

Expressway 信頼ストアへの Let's Encrypt ルート CA 証明書の追加

Let's Encrypt は比較的新しい CA であるため、独自の CA ルート証明書は、確立された IdenTrust CA によってクロス署名されます。次の手順に従って、すべての Expressway が Internet Security Research Group Root X1 を信頼していることを確認します。

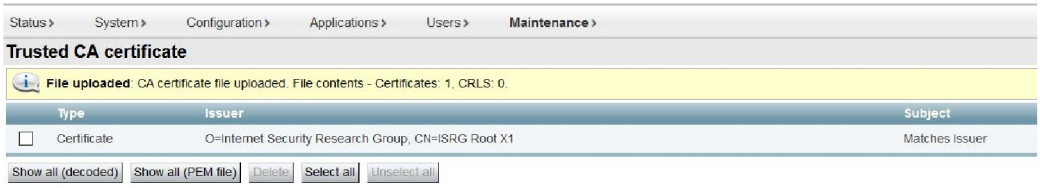
手順

Step 1 「https://letsencrypt.org/certs/isrgrootx1.pem」に進みます。

Step 2 展開内の各 Expressway-E（およびトラバーサル Expressway-C）の場合、Let's Encrypt が署名した証明書で保護します。

1. Expressway の Web インターフェイスにログインします。
2. **[メンテナンス（Maintenance）]>[セキュリティ（Security）]>[信頼できる CA 証明書（Trusted CA certificate）]** の順に選択します。
3. ページの **[アップロード（Upload）]** セクションで、作成した証明書ファイルを選択します。
4. [CA 証明書の追加（Append CA certificate）] をクリックします。

   これで、信頼できる CA 証明書リストに、Internet Security Research Group のルート証明書が含まれます。



394147

Expressway 信頼ストアへの Let's Encrypt 中間 CA 証明書の追加

手順

Step 1 「https://letsencrypt.org/certs/lets-encrypt-r3.pem」に進みます。

Step 2 展開内の各 Expressway-E（およびトラバーサル Expressway-C）について、Let's Encrypt によって署名された証明書で保護します。

1. Expressway の Web インターフェイスにログインします。
2. **[メンテナンス（Maintenance）]>[セキュリティ（Security）]>[信頼できる CA 証明書（Trusted CA certificate）]** の順に選択します。
3. ページの **[アップロード（Upload）]** セクションで、作成した証明書ファイルを選択します。
4. [CA 証明書の追加（Append CA certificate）] をクリックします。

   信頼できる CA 証明書リストには、Internet Security Research Group のルート証明書と Let's Encrypt CA 証明書の両方が含まれている必要があります。

394148

Expressway-E で ACME 証明書サービスを構成

手順

Step 1 Expressway-E のサインインし、**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [サーバー証明書（Server certificate）]** の順に選択します。

Step 2 **[ACME 証明書サービス（ACME Certificate Service）]** セクションまで下にスクロールします。

Step 3 ドロップダウンリストで、ACME **プロバイダー**を選択します。

これは、証明書に署名する CA です。現在、Let's Encrypt® でのみ動作します。

Step 4 プロバイダーで使用する**管理者の電子メールアドレス**を入力します。

これは、必要に応じてACMEプロバイダーからの通信を受信できるように、実際のアドレスである必要があります。

このアドレスは、プロバイダーのアカウント名であり、このプロバイダーで行うすべての証明書署名要求にリンクされています。

Step 5 利用規約をお読みください。

法定代理人がまだ確認していない場合は、コピーを保存して確認することをお勧めします。

Step 6 **[利用規約に同意します（I accept the terms and conditions）]** をクリックします。

Expressway-E の ACME クライアントは、選択したプロバイダーでアカウントを作成します。

これで、Expressway-E クライアントの ACME 証明書サービスが ACME プロバイダーと対話する準備が整いました。

各ドメイン証明書の ACME 構成

Expressway-E での ACME サービスでは、バージョン X12.5 以降から、（SNI で使用する）ドメイン証明書を要求して導入できるようになっています。

[メンテナンス（Maintenance）] > **[セキュリティ（Security）]** > **[ドメイン証明書（Domain certificates）]** の順に選択し、ドメインのリストに [ACME] 列が表示され、ここに各ドメインの ACME サービスのステータスが表示されます。

ACME サービスを有効にするドメイン名の横にある **[表示/編集（View/Edit）]** をクリックします。

ドメイン証明書用に ACME サービスを設定するプロセスは、サーバ証明書用に設定する場合と同じで、Expressway-E インターフェイスで使用する場所が異なるだけです。

ACME に証明書署名要求を生成

証明書署名要求を作成するプロセスは、ACME クライアントを使用する場合と変わりません。「証明書署名要求（証明書署名要求）」のガイダンスに従います。

ACME プロバイダーを使用して証明書署名要求に署名

Expressway-E に証明書署名要求を保存し、ACME サービスを構成したら、証明書署名要求を ACME プロバイダーに送信して検証および署名できます。

手順

Step 1 **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[サーバー証明書（Server certificate）]** の順に選択します。

Step 2 [ACME サービス構成（ACME Service Configuration）] までスクロールします。

Step 3 **[ACME プロバイダーで証明書署名要求に署名（Sign CSR with ACME Provider）]** をクリックします。

Expressway-E の ACME クライアントは、選択したプロバイダーに保存された証明書署名要求を送信します。

Step 4 署名プロセスが完了するまで、数分待ちます。

プロバイダーは、証明書署名要求の CN および SAN 属性のドメインネームシステム（DNS）をチェックし、署名要求を受信した Expressway-E アドレスと一致することを確認します。プロバイダーは証明書に署名して返します。ACME クライアントはこの証明書を Expressway-E に保存し、展開を待機します。

Step 5 **[サーバー証明書（Server certificate）]** ページを手動で更新します。

証明書が署名され、使用できる状態になると、成功バナーが表示されます。

（オプション）署名付き ACME 証明書の確認

手順

Step 1 **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [サーバー証明書（Server certificate）]** の順に選択し、**[ACME Certificate Service（ACME 証明書サービス）]** セクションに移動します。

[ステータス（Status）] フィールドには、署名付き証明書を展開する準備ができていることが示されます。

Step 2 **[保留中の ACME（Pending ACME Certificate）]** フィールドで、**[表示（復号化）（Show (decoded)）]** をクリックします。

Step 3 詳細が期待どおりであることを確認します。そうでない場合は、保留中の証明書を破棄し、新しい証明書署名要求を生成する必要があります。

（注） Let's Encrypt CA は、証明書署名要求で指定した属性の一部を無視する可能性があります。

ACME 証明書の展開

手順

Step 1 **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [サーバー証明書（Server certificate）]** の順に選択し、**[ACME Certificate Service（ACME 証明書サービス）]** セクションに移動します。

[ステータス（Status）] フィールドには、署名済み証明書を展開する準備ができていることが示されます。

Step 2 **[保留中の証明書の展開（Deploy Pending Cert）]** をクリックします。

Expressway-E は、相手側に対して自身を認証する必要があるトランザクションで、この証明書の使用を開始します。Expressway-E を再起動する必要はありません。

ACME 証明書の自動更新の有効化

ACME 証明書は、セキュリティ上の予防措置として意図的に短命です。執筆時点では、有効期間は発行日から 90 日間です。

Expressway-E の ACME 証明書サービスは、証明書の有効期間をモニターし、有効期間の 3 分の 2 が経過すると警告します。前のトピックで説明した手順に従って、手動で応答できます。

この頻繁なタスクを回避するために、自動更新オプションを使用して、ACME 証明書サービスに証明書を更新して展開させることができます。

手順

Step 1 **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[サーバー証明書（Server certificate）]** の順に選択し、**[ACME Certificate Service（ACME 証明書サービス）]** セクションに移動します。

Step 2 **[ACME 自動スケジューラ（ACME Automated Scheduler）]** フィールドを *[オン（On）]* に変更します。

Step 3 1 つ以上の **[スケジュール日（Schedule Days）]** と **[スケジュール時刻（Schedule Time）]** を選択します。

証明書の有効期限の 3 分の 2 が経過すると、ACME 証明書サービスは、選択された翌日の指定時刻にサーバー証明書の更新と展開を試行します。

Step 4 [**Save**] をクリックします。

[ステータス（Status）]には、自動モードのサービスが表示されます。次に証明書を更新して展開するときに、**[最終展開ステータス（Last Deploy Status）]** と **[最終署名ステータス（Last Sign Status）]** を更新します。

ACME 証明書の取消

Expressway-E で ACME 証明書を取り消す理由の一部を次に示します。

- Expressway-E が侵害された。
- Expressway-E を初期設定にリセットした。
- Expressway-E の目的が変更された。
- ACME アカウントは無効になった。

ACME 証明書を取り消すには、Expressway-E のドメインネームシステム（DNS）アドレスを所有していること、および証明書の元のエントリを管理していることをプロバイダーに証明する必要があります。これを行うには、証明書に使用される署名証明書署名要求プロセスを繰り返す必要がありますが、結果の証明書を再展開する必要はありません。

元の証明書を取り消す前に、新しい証明書を展開する必要があります。取り消す証明書のコピーを保持します。

⚠

注意 使用中の証明書を取り消すと、この証明書を使用するすべてのサービスが中断されるため、取り消さないでください。

手順

Step 1 現在の証明書のバックアップを作成します。

この予防措置は、現在の証明書を失効させる予定の証明書で誤って上書きした場合に役立ちます。

Step 2 失効させる証明書を Expressway-E の一時的な場所にコピーします。場所へのパスを覚えておいてください。

取り消す証明書のコピーがない場合は、https://crt.sh/ から取得できる場合があります。

Step 3 失効させる証明書のすべてのドメイン名を含む証明書署名要求を作成します。ACME に証明書署名要求を生成を参照してください。

Step 4 元の証明書に署名した ACME プロバイダーによって署名される証明書署名要求を送信します。ACME プロバイダーを使用して証明書署名要求に署名を参照してください。

これで、失効させる証明書に一致する SAN エントリを持つ新しい保留中の証明書が作成されます。

このプロセスにより、元の証明書を取り消す権限があることが証明されました。

Step 5 Expressway-E の CLI に（管理者として）サインインします。

Step 6 次のいずれかの方法で acmerevoke コマンドを実行します。

- デフォルトのプロバイダーが証明書に署名した場合：`xcommand Acmerevoke "/path_to_cert_to_be_revoked"`
- 証明書に署名したプロバイダーを特定する場合：`xcommand Acmerevoke CertPath:"/path_to_cert_to_be_revoked" Provider:"ACME_Provider_Name"`

  （証明書に署名したのと同じプロバイダーが証明書を失効させる必要もあります）。

証明書の失効に成功すると、プロバイダーは 200 OK で応答します。

Step 7 失効した証明書の保存済みコピーを削除します。

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。