S/MIME シグニチャで使用する ESA 証明書の作成

目次

概要

この文書に Cisco E メール セキュリティ アプライアンス (ESA) で署名するセキュア /Multipurpose Internet Mail Extensions （ S/MIME ）で証明書をテストの目的で作成する方法を記述されています。

背景説明

メッセージ署名用の S/MIME 証明書を作成する際、『RFC 5750： Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Certificate Handling』に記載されている要件を満たす必要があります。

ESA からの S/MIME 証明書を作成して下さい

S/MIME 自己署名証明書は ESA GUI から作成することができます:

1. 選択して下さい**ネットワーク > 証明書 > Add 証明書...**
2. ドロップダウン リストから、**自己署名 S/MIME 証明書を**『Create』 を選択 して下さい
3. 要求されるように適切な情報を記入して下さい。
4. [Next] をクリックします。
5. 証明書作成を保存するために『SUBMIT』 をクリック して下さい。
6. 設定への変更を保存するために**保存します変更を**クリックして下さい。

証明書を使用し、S/MIME 公開キーを設定するために、.pem フォーマットの証明書のコピー保存されるある必要があります:

1. **ネットワーク > 証明書を**選択して下さい
2. ちょうど作成した証明書のためのハイパーリンクをクリックして下さい。
3. 『Download』 をクリック して下さい**証明書署名要求を...**

これはコンピュータに *cert.pem* としてファイルを*ローカル*で保存します。 この記事の「仲間 PEM 証明書」の使用以降のためにこれをセクション保存して下さい。

サードパーティ製のアプリケ– ションからの S/MIME 証明書を作成して下さい

（テストするか、または）パーマ ESA から証明書をまた外部に作成することができます。 この例に関しては、X 証明書およびキー管理（XCA）は非対称的なキーを、Rivest シャミール Addleman（RSA）または Digital Signature Algorithm（DSA）のような管理し、証明書の作成および署名のための小さい認証局（CA）であるように意図されているアプリケーションです。 また、暗号化操作にオープン セキュア ソケット レイヤ（OpenSSL）ライブラリを使用します。

> **注:** XCA はシスコがサポートしていないサードパーティ アプリケーションです。 このアプリケーションの使用は、S/MIME の管理やテスト、設定を説明し、管理しやすくする目的でのみ提供します。 XCA の詳細および手順については、『XCA - X Certificate and key management』ドキュメントを参照してください。

次のいずれかの場所で、XCA アプリケーションをダウンロードできます。

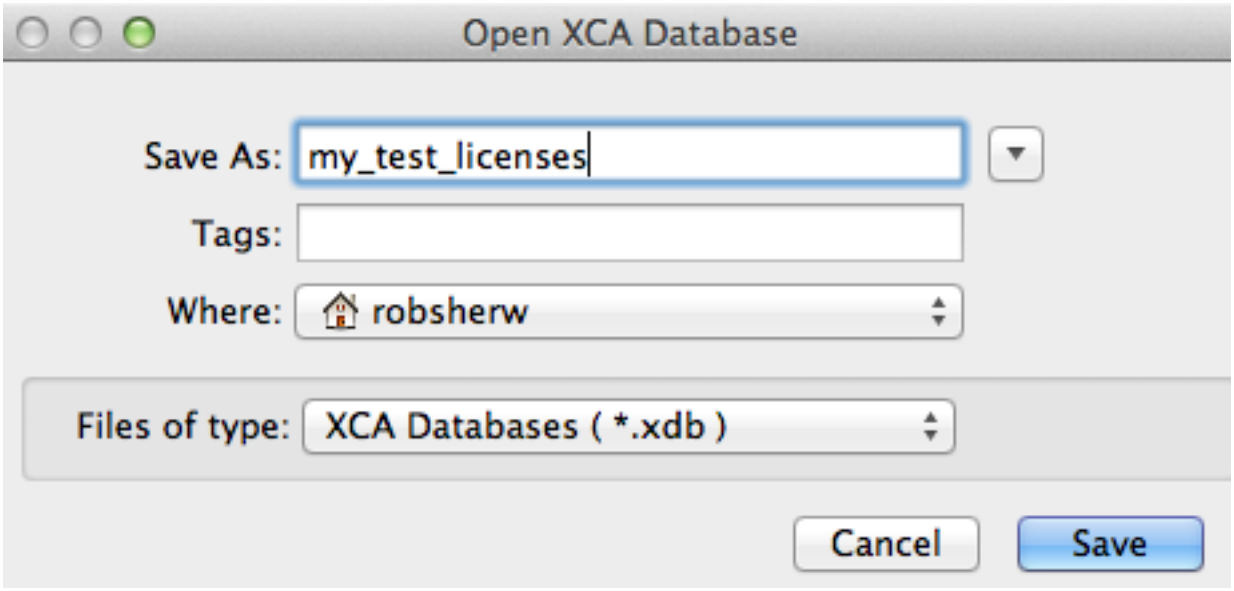
- Macintosh オペレーティング システム（OSX）： Sourceforge
- Microsoft Windows システム： Sourceforge

証明書の作成

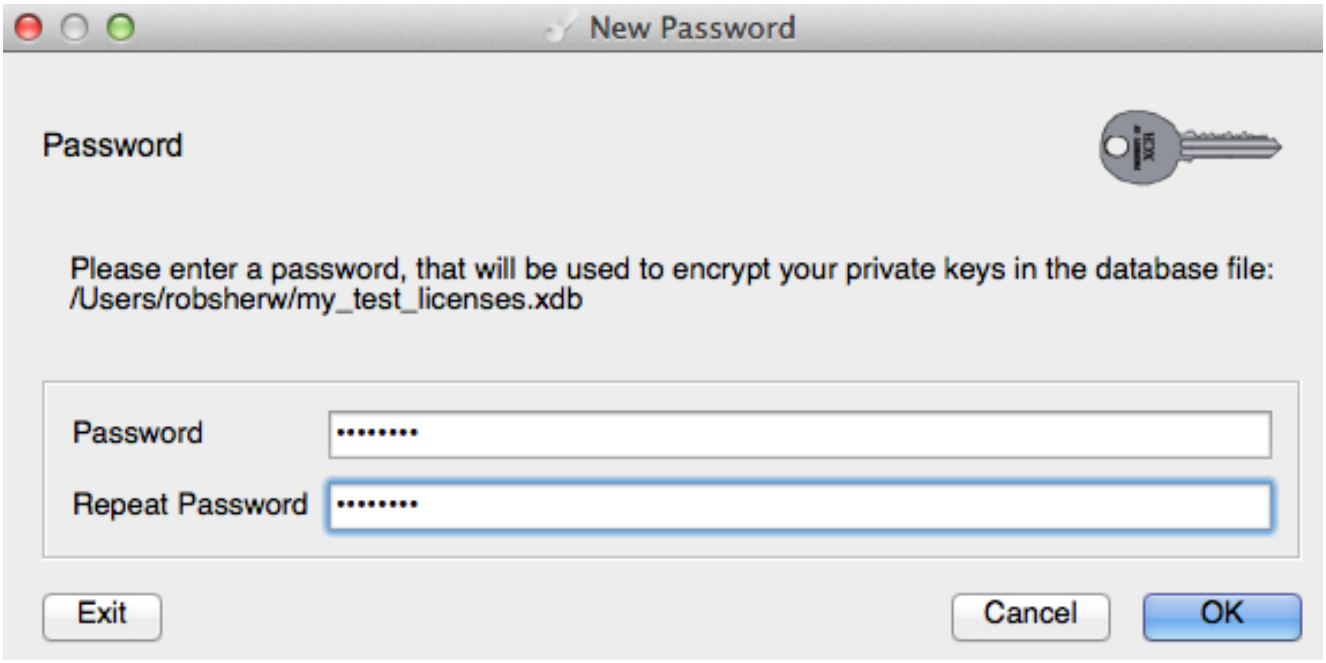
S/MIME 証明書を作成するには、次の手順を実行します。

1. 新しい XCA データベースを作成するには XCA アプリケーションを使用します。または既にある場合は、現行の XCA データベースを開きます。

   メニューバーから、**データベース > choice> の <DB 名前を** File > New の順に選択 して下さい:



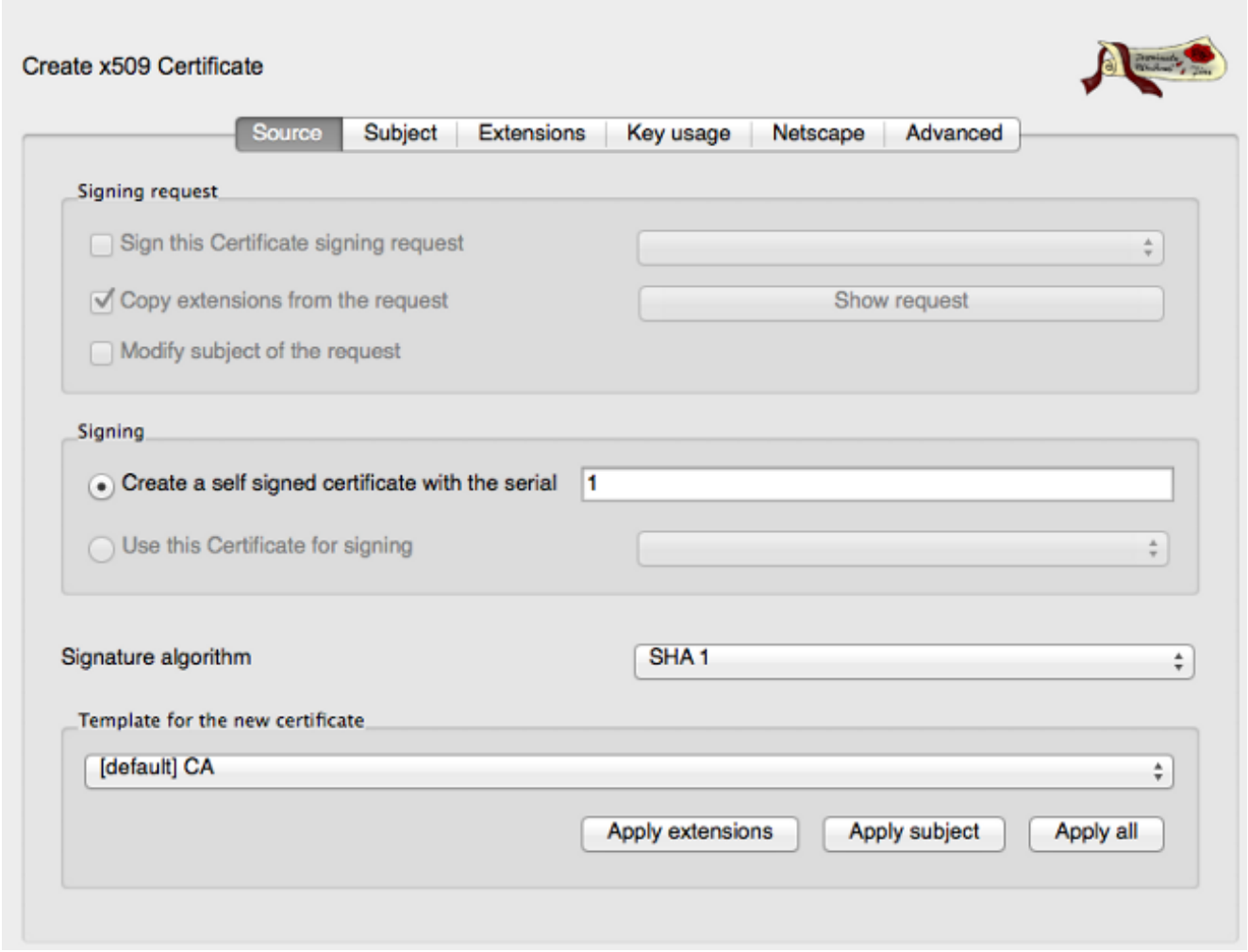
   [Save] をクリックします。 次に、このデータベースに関連付けられている秘密キーの暗号化パスワードを入力します。 このパスワードは XCA データベースのみに該当します。



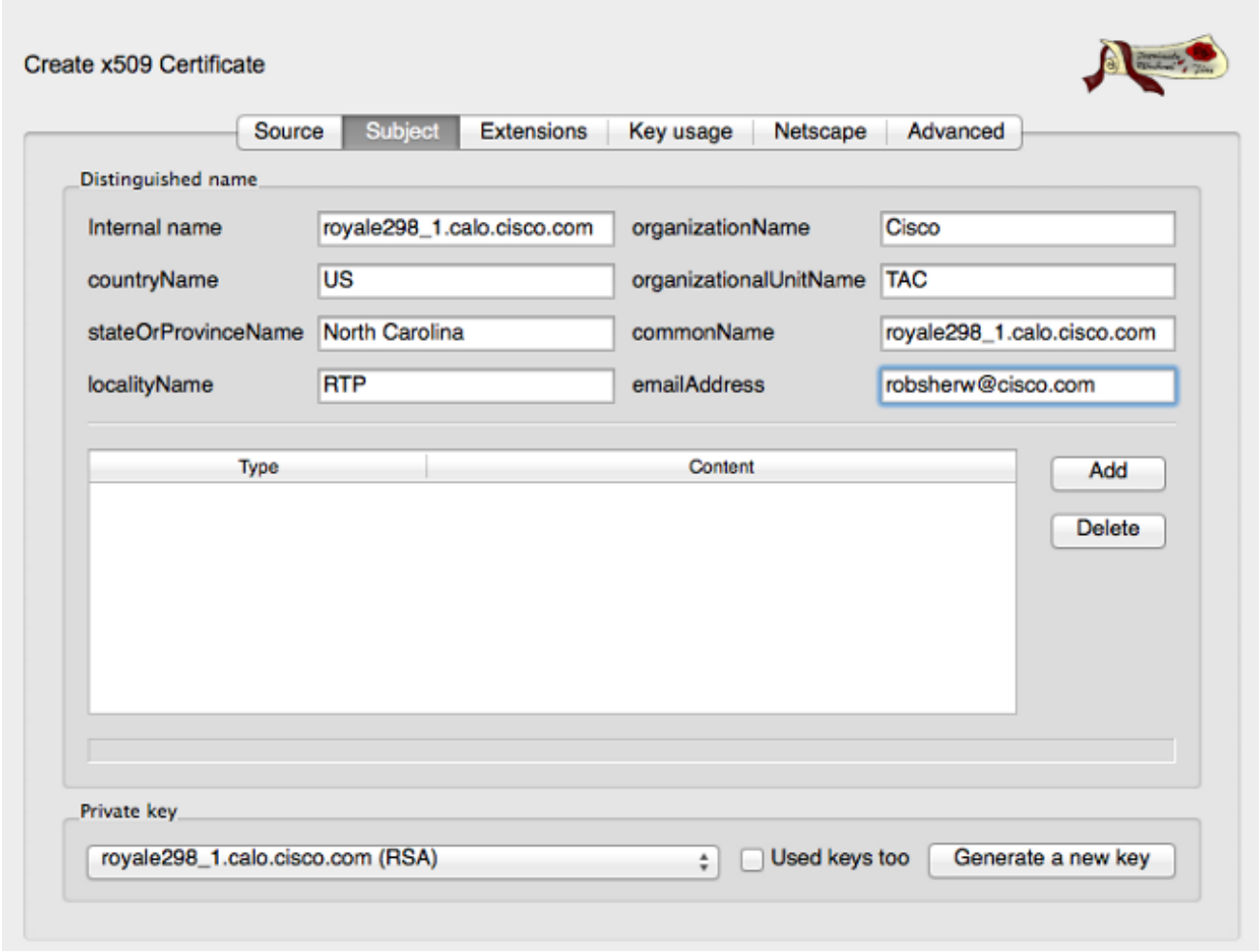
[OK] をクリックしてデータベースの作成を終了します。

2. Certificates タブから、**証明書を**『New』 を選択 すれば *作成 x509 Certificate 画面は*現われます。

   デフォルト値が使用できるため、[Source] タブからの変更は不要です。

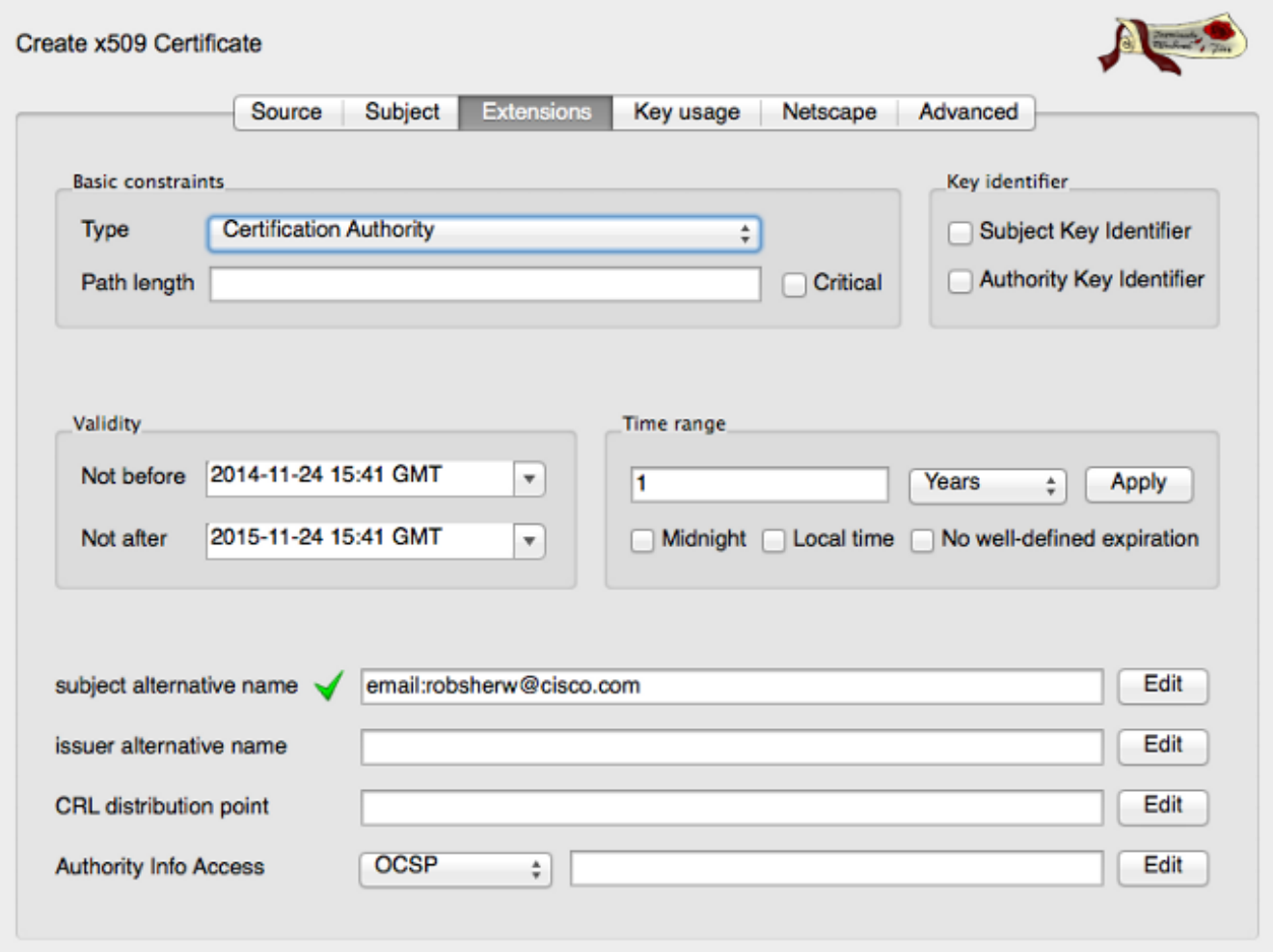


[Subject] タブから [Distinguished name] セクションに必要な情報を入力します。 [Private key] セクションで [Generate a new key] をクリックし、[keysize] で [2048 bit] または [1024 bit] を選択します。 [Create] をクリックし、秘密キーを作成し、この証明書に関連付けます。

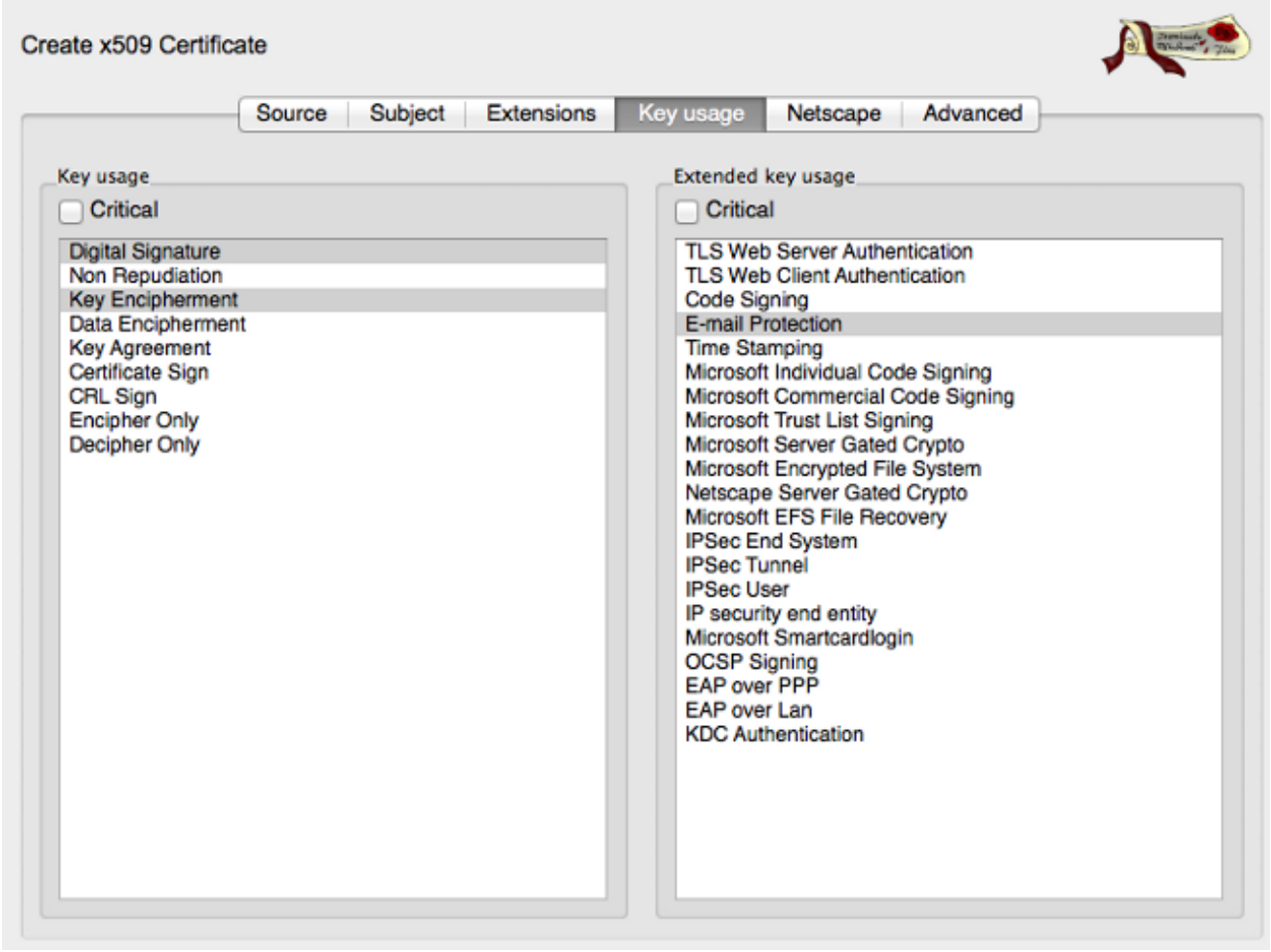


拡張タブから、基本的な制約セクションで、型のための**認証局を**選択して下さい。

注: 後続の証明書署名要求（CSR）は、[Type] に [Not Defined] を指定したこの CA 経由で署名できます。
[Validity] セクションに、要件に沿って詳細を入力します（デフォルトでは 365 日）。 各行の [Edit] ボタンを使用して、ドメイン ネーム システム（DNS）に対するサブジェクト代替名（SAN）、電子メール アドレスなどを追加することができます。 SAN ポップアップ ウィンドウから、**SAN 型および関連する内容を『Add』 をクリック し、選択して下さい。** 完了したら [Apply] をクリックし、これらの変更を適用し、[Extensions] タブ ウィンドウに戻ります。



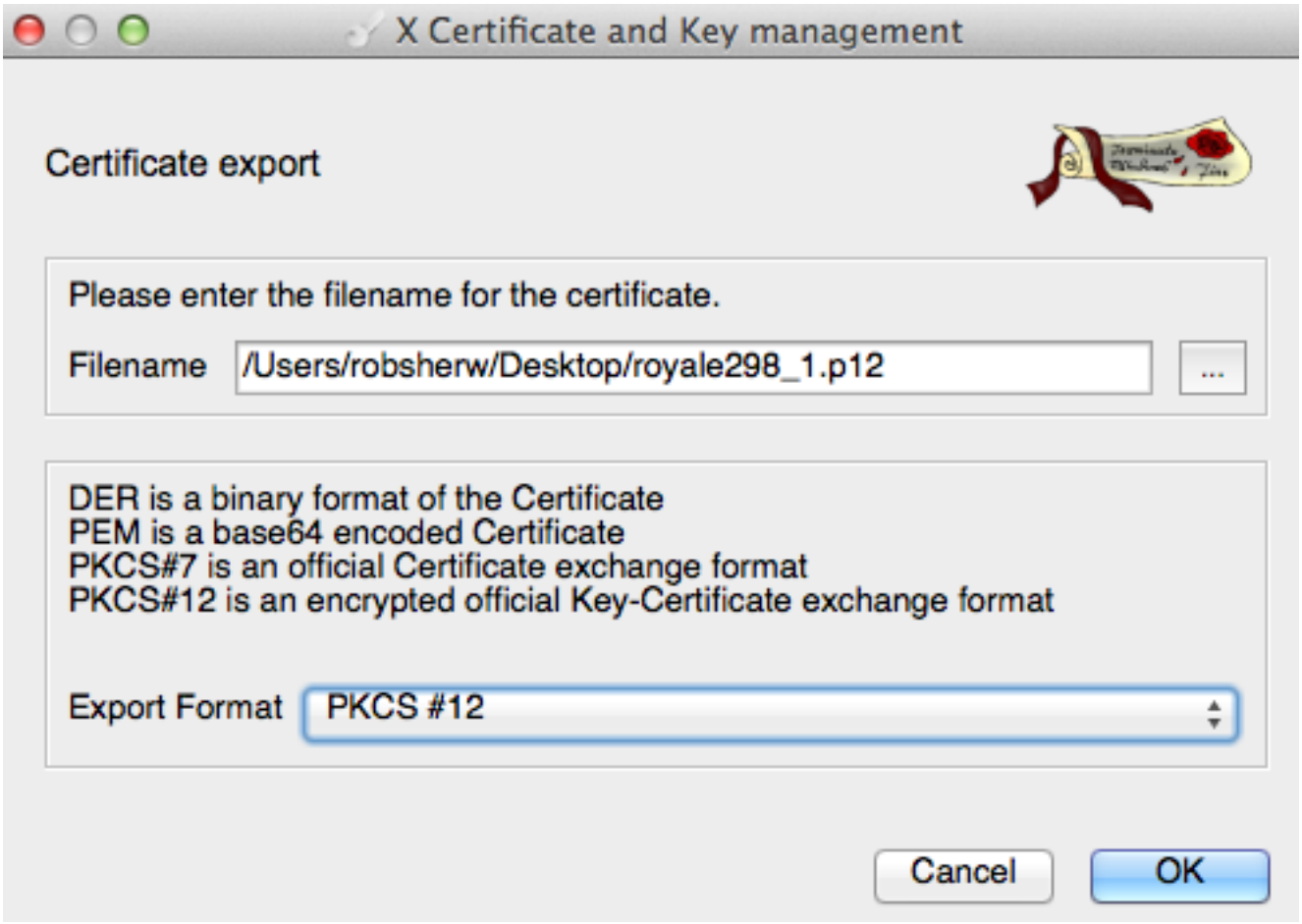
[Key usage] タブの [Key usage] セクションで、[Digital Signature] と [Key Encipherment] を強調表示します。 [Extended key usage] セクションで、[E-mail Protection] を強調表示します。 これらは S/MIME に必要な要素です。



3. 画面最下部の [OK] をクリックすると、ポップアップ通知が表示されます。

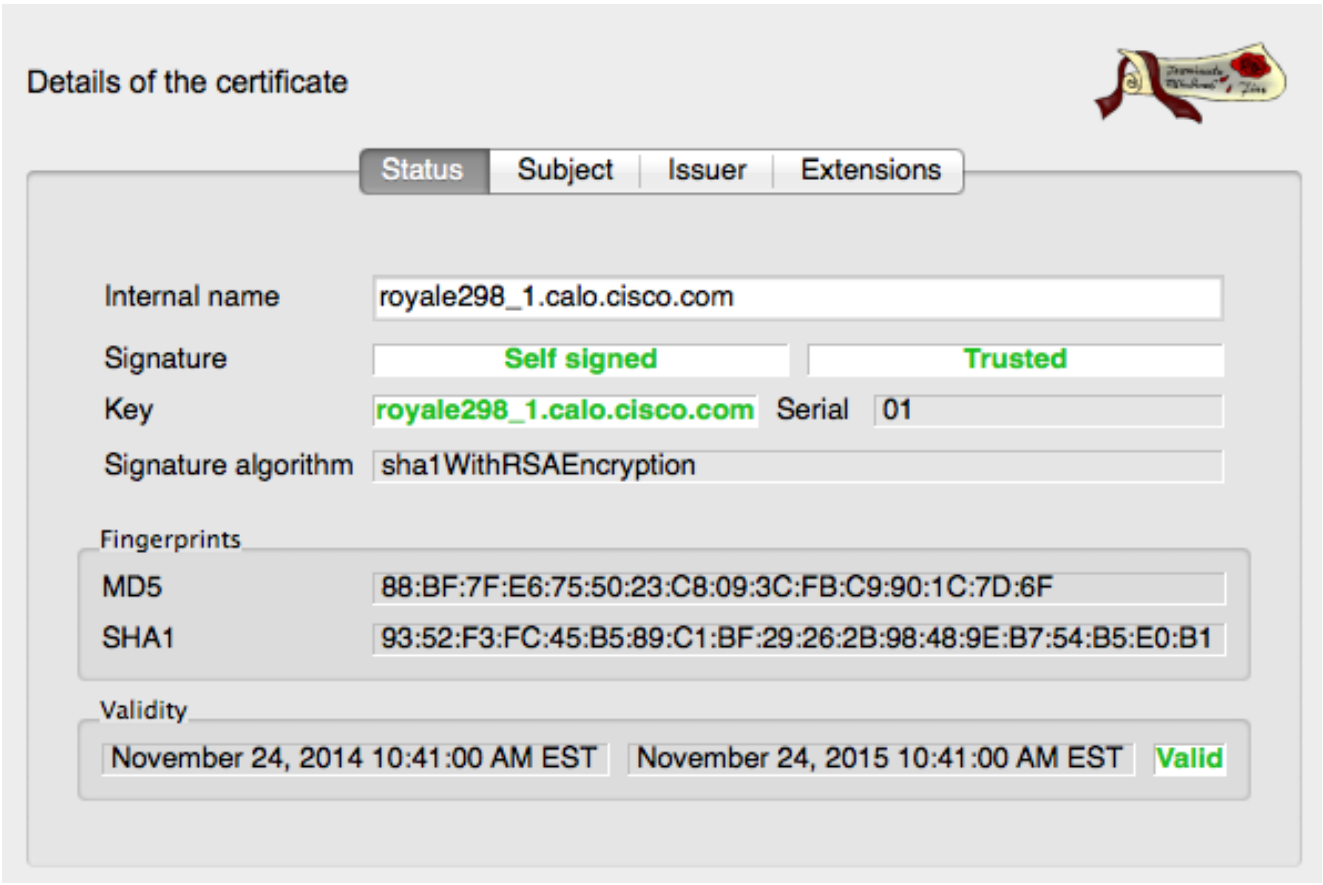
4. 新規作成した証明書が [Certificate] タブに表示されます。 その証明書をクリックして強調表示し、[Export] をクリックします。 ファイル名、証明書の保存場所、およびエクスポート形式を選択します。

   注: 証明書は、PKCS12 およびプライバシー強化メール（PEM）形式の両方でエクスポートする必要があります。 PKCS12 証明書は、**.p12** 形式のファイル名で保存します。 PEM 証明書は、**.crt** 形式のファイル名で保存します。



[OK] をクリックすると、PKCS12 証明書用の暗号化パスワードが提示されます。これは ESA 上に証明書をインポートする際に必要です。

注: PEM 形式の証明書をエクスポートする場合、パスワードは不要なため、要求されません。証明書の詳細を表示するには、[Certificates] をクリックし、[Status]、[Subject]、[Issuer]、[Extensions] とタブを移動します。

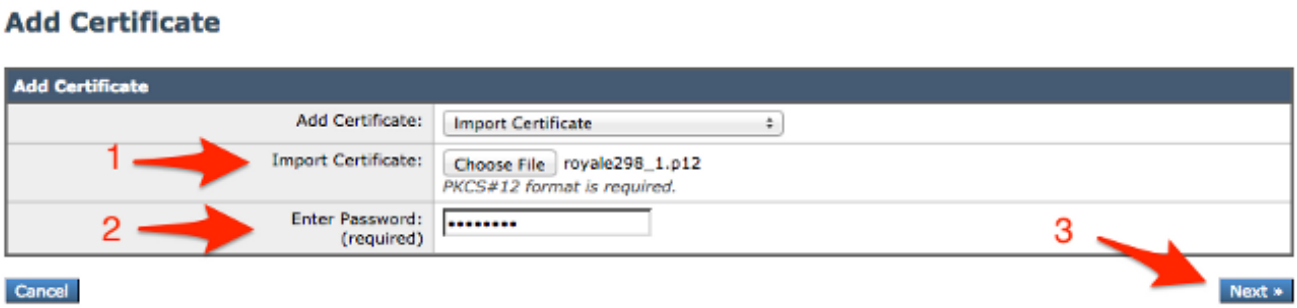


この時点で証明書を ESA で使用する準備ができました。

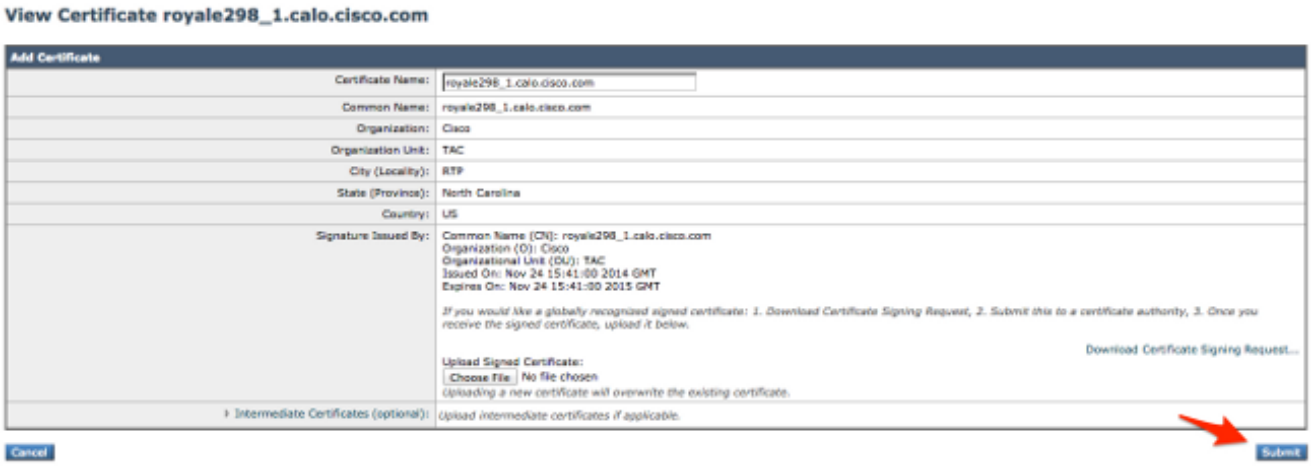
ESA に証明書をインポートして下さい

ESA からの証明書を外部に作成したら ESA にそれをインポートして下さい。 証明書をインポートするには、次の手順を実行します。

1. 選択して下さい**ネットワーク > 証明書 > Add 証明書... > [Import Certificate] に移動します。**
2. 前述のセクションで作成した PKCS12（.p12）形式のファイルを選択し、その証明書に関連付けられたパスワードを入力し、[Next] をクリックします。



3. 証明書を確認し、[Submit] をクリックして変更を確定します。



この時点で証明書を ESA の S/MIME で使用する準備ができました。

PEM 証明書の関連付け

次に PEM 形式の証明書を S/MIME の公開キーに追加します。 PEM 形式の証明書を追加するには、次の手順を実行します。

1. 選択して下さい**メール ポリシー > S/MIME 公開キー > Add 公開キーを....**
2. 必要に応じて名前を入力します。
3. 適切なテキストエディタの PEM （.crt）フォーマットされていた証明書を開いて下さい（Notepad++ [Windows/PC]または原子[OSX]のような）。
4. コンテンツの **----------BEGIN CERTIFICATE----------** Pass **----------END CERTIFICATE----------**を探します。
5. このコンテンツを [S/MIME Public Key] セクションに貼り付け、[Submit] をクリックします。

6. すべての変更を確定します。 この時点で S/MIME の公開キーが ESA に設定されました。

関連情報

- Cisco E メール セキュリティ アプライアンス エンド ユーザ ガイド
- Cisco E メール セキュリティ アプライアンス リリース ノートおよび一般情報
- テクニカル サポートとドキュメント – Cisco Systems