S/MIME 署名と併用するための ESA 認証作成

目次

概要

この資料に 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）と併用するため認証を作成する方法を記述されています。

背景説明

署名しているメッセージのための S/MIME 認証を作成するとき RFC 5750 に説明がある要件を満たす必要があります: /Multipurpose Internet Mail Extensions（S/MIME）バージョン 3.2 -認証処理保護して下さい。

このプロセスに関しては認証を生成するために、外部アプリケーションの使用が必要となります。 非対称キーを、Rivest シャミールAddleman（RSA）または Digital Signature Algorithm（DSA）のような管理し、認証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 X 認証およびキー管理（XCA）はアプリケーションです。 それは暗号操作のために Secure Sockets Layer 開いた（OpenSSL）ライブラリを使用します。

> **注:** XCA は Cisco によってサポートされないサードパーティ製のアプリケ– ションです。 このアプリケーションの使用は S/MIME 管理、テスト、および設定のための管理のおよび容易さ実例としてだけ提供されます。 XCA に関する詳細および説明に関しては、XCA を- X 認証およびキー管理 資料参照して下さい。

これらの場所のどちらかで XCA アプリケーションをダウンロードできます:

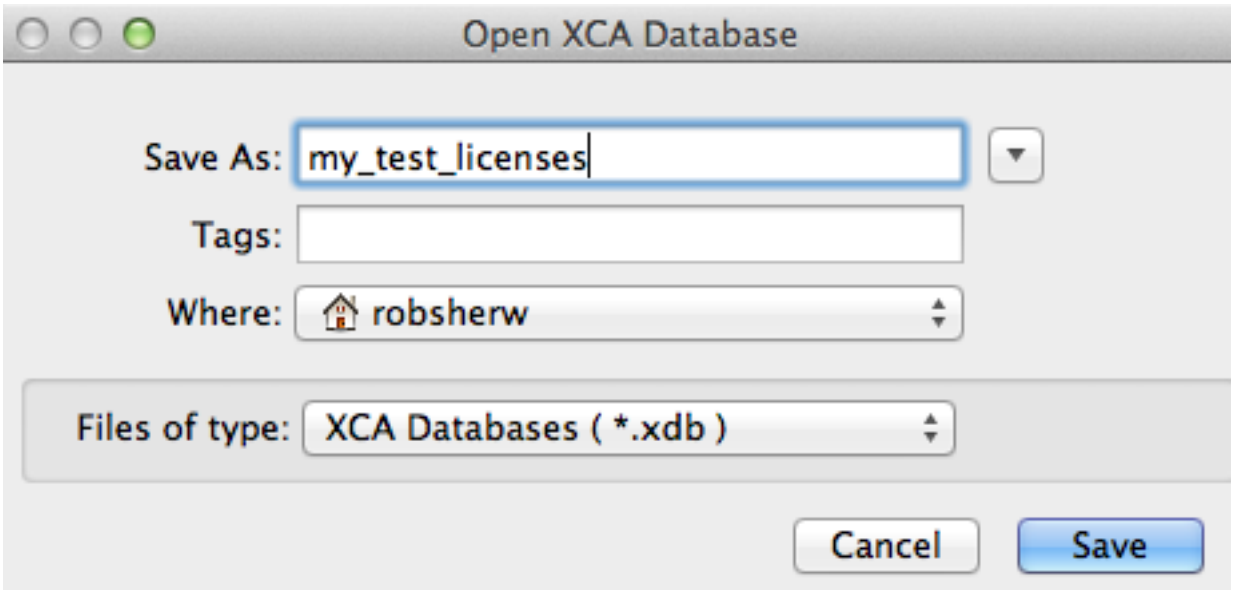
- マッキントッシュ オペレーティング システム（OSX）: Sourceforge
- Microsoft Windows システム: Softpedia

認証を作成して下さい

S/MIME 認証を作成するためにこれらのステップを完了して下さい:

1. 新しい XCA データベースを作成するか、または電流 XCA データベースを使用可能にするために XCA アプリケーションを既に存在 する 1 つ使用して下さい。

   メニューバーから、**> 新しいデータベース > choice> の <DB 名前はファイル**にナビゲートします:

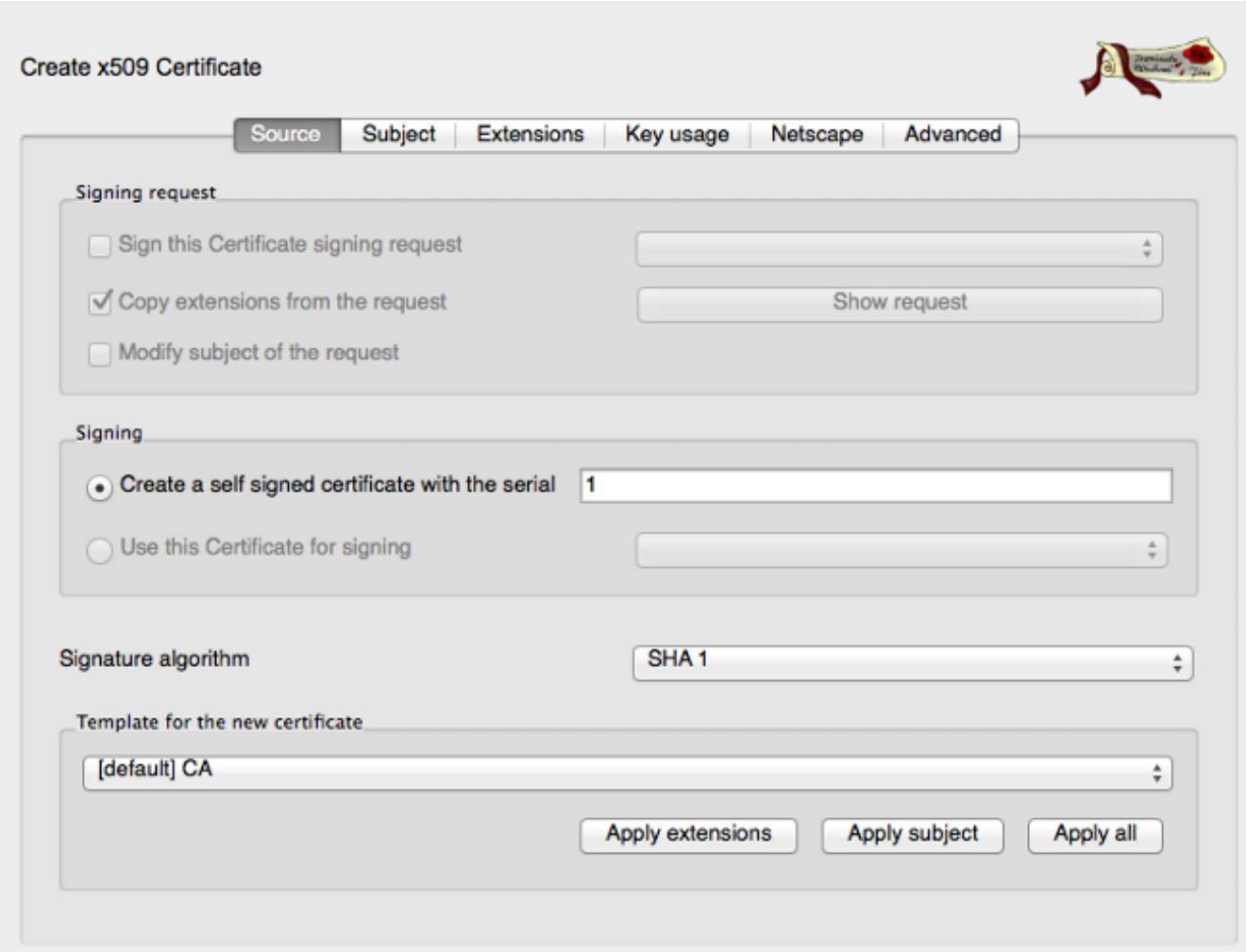


   [Save] をクリックします。 この場合このデータベースに関連付けられるプライベートキーの暗号化のためのパスワードを入力して下さい。 このパスワードは XCA データベースのためだけです。

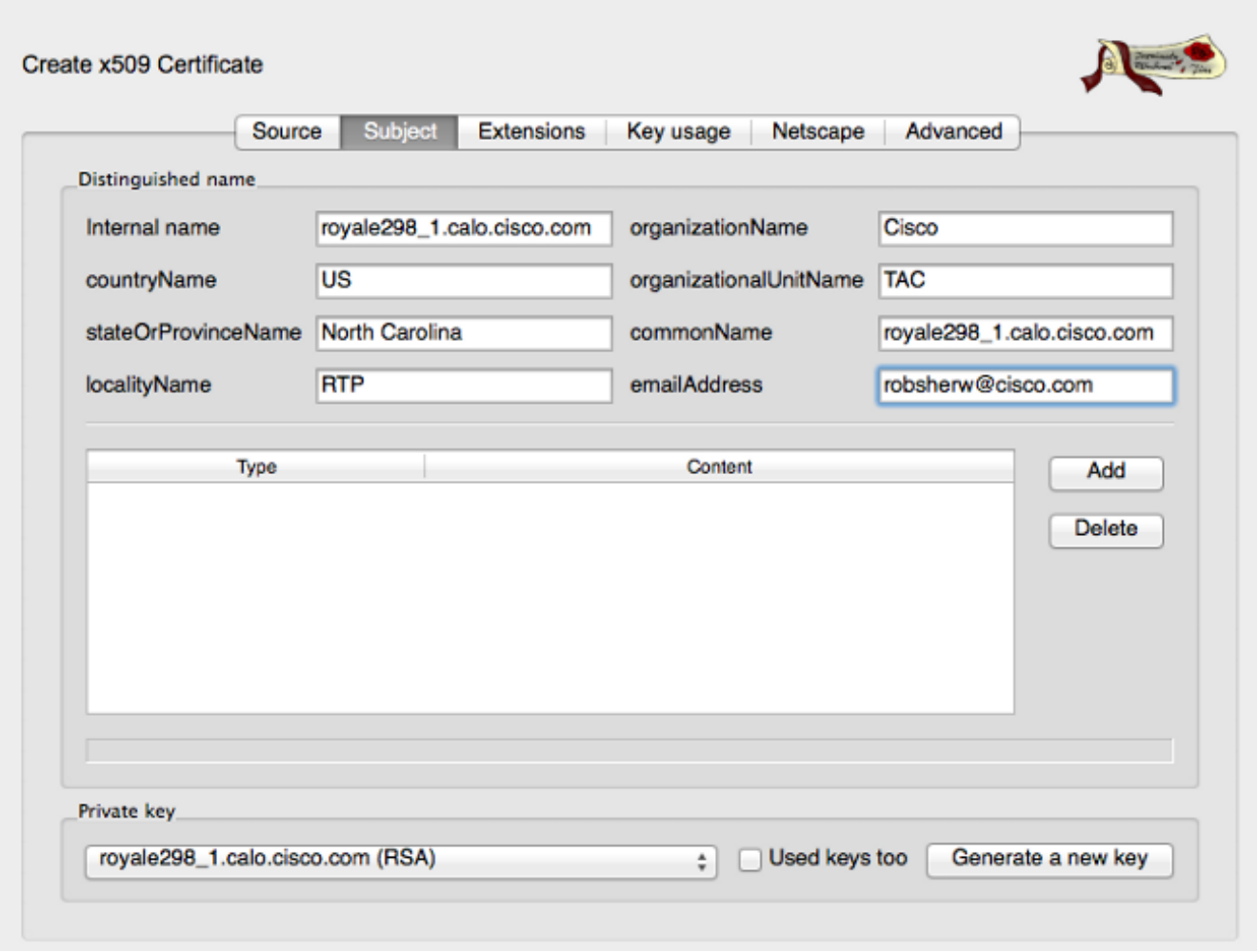
   データベース作成を終えるために『OK』 をクリック して下さい。

2. Certificates タブから、**認証を**『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することができるので、Source タブからの変更が必要となりません:

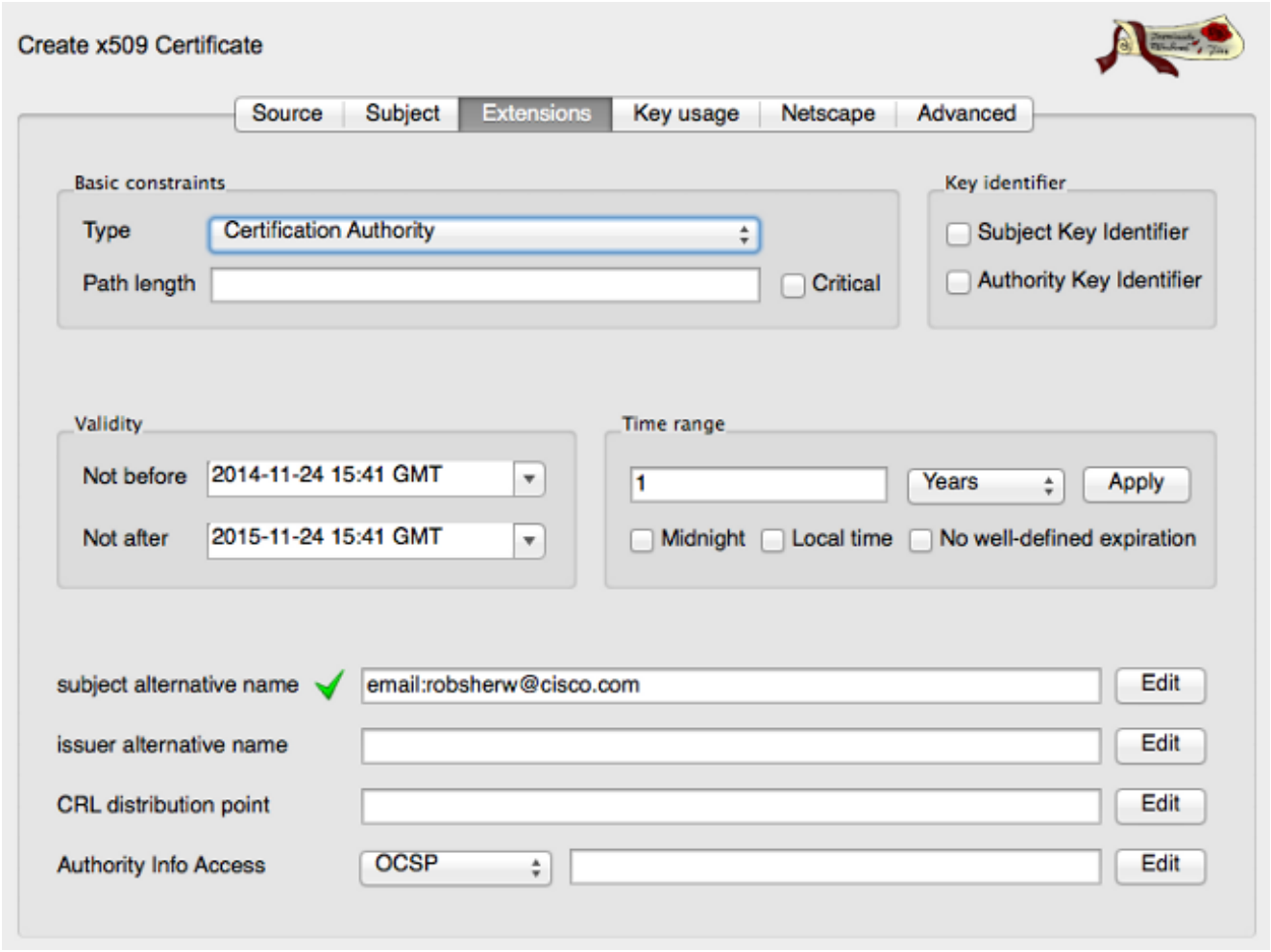


認証対象タブから、識別名 セクションに必要情報を入力して下さい。 プライベートキー セクションで、**New 鍵を**『Generate』 をクリック し、**2048 ビットを**か keysize のための **1024 ビット**選択して下さい。 プライベートキーを生成し、この認証と関連付けるために『Create』 をクリック して下さい。

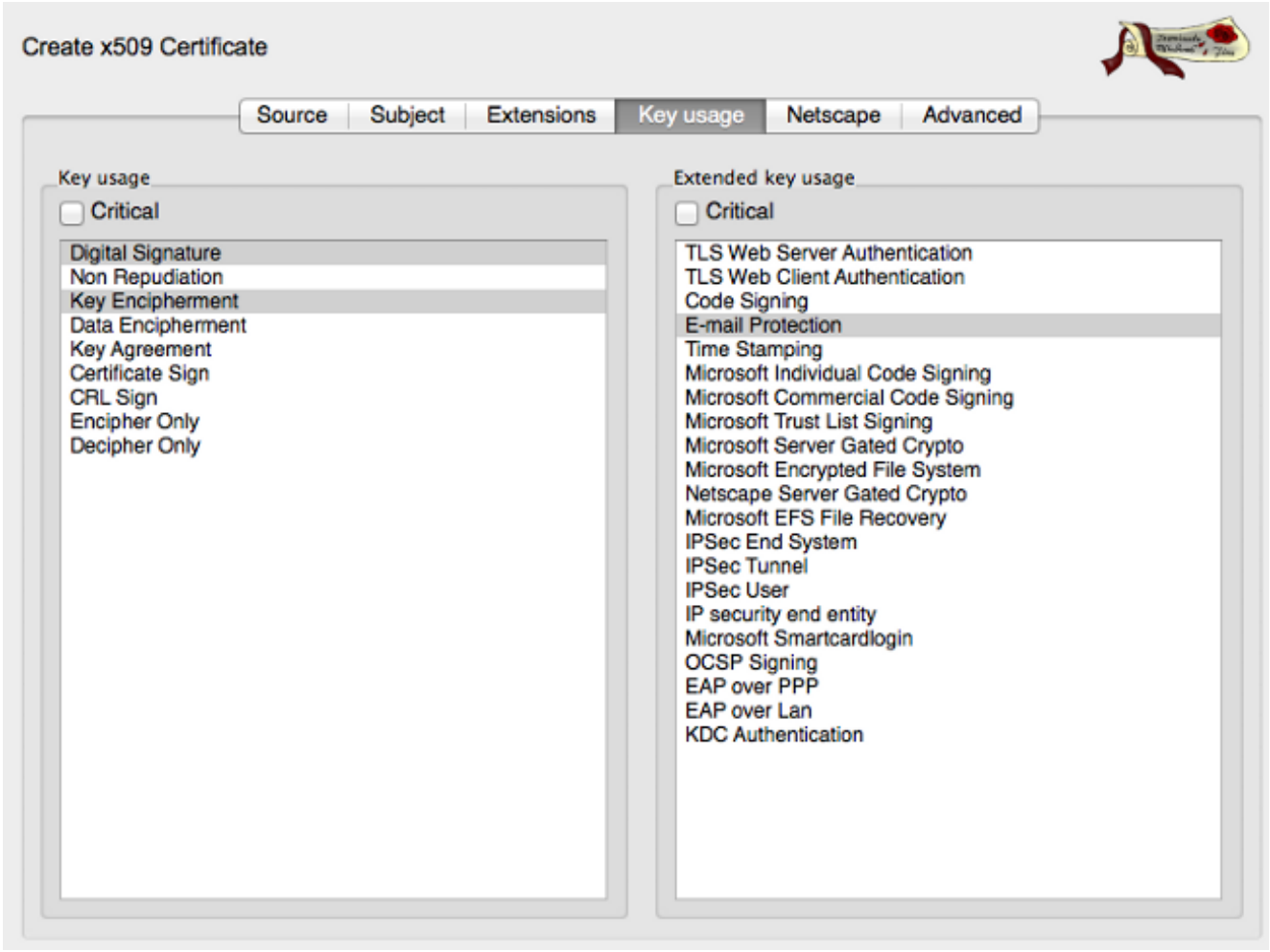


拡張タブから、基本制約セクションで、型に**認証局を**選択して下さい。

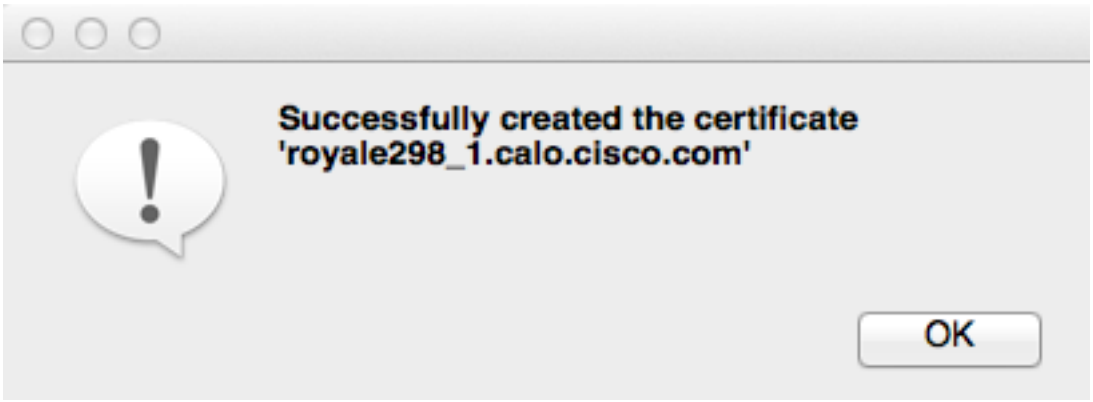
注: それに続く証明書署名要求（CSR）は**定義されない**への型セットのこの CA によって署名することができます。
有効性セクションでは、必要条件（365 日デフォルトで）によって詳細を入力して下さい。そのラインのための **Edit ボタン**の使用との Domain Name System （DNS）、eメールアドレス、および類似したの認証対象代替名前（SAN）を追加することを選択できます。 SAN ポップアップ ウィンドウから、**SAN 型および関連コンテンツを『Add』 をクリック し、選択して下さい。** 完了される、これらの変更を加え、拡張タブ ウィンドウに戻るために『Apply』 をクリック して下さい:



キー使用法タブから、キー使用法 セクションで、**デジタル署名**および**キー暗号化を**強調表示して下さい。 拡張キー使用法 セクションでは、**E メール 保護を**強調表示して下さい。 これらは S/MIME のための必須要素です:

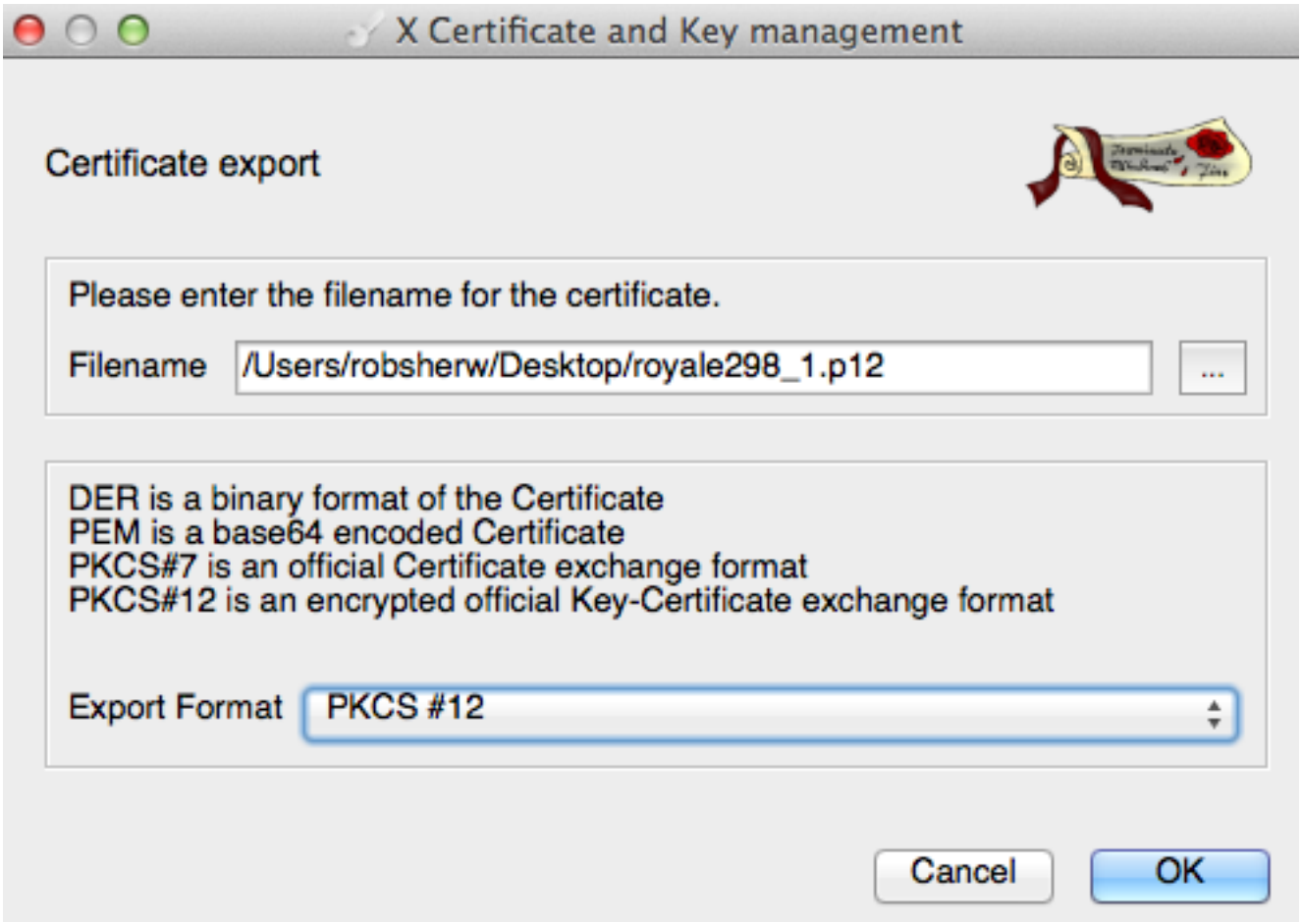


3. スクリーンの一番下で『OK』 をクリック すればポップアップ通知は現われます:



4. 新しく作成された認証は Certificate タブに今現われます。 それを強調表示し、『Export』 をクリック するために認証をクリックして下さい。 認証が保存する必要があるおよび工クスポート形式を選択して下さいファイル名を、位置。

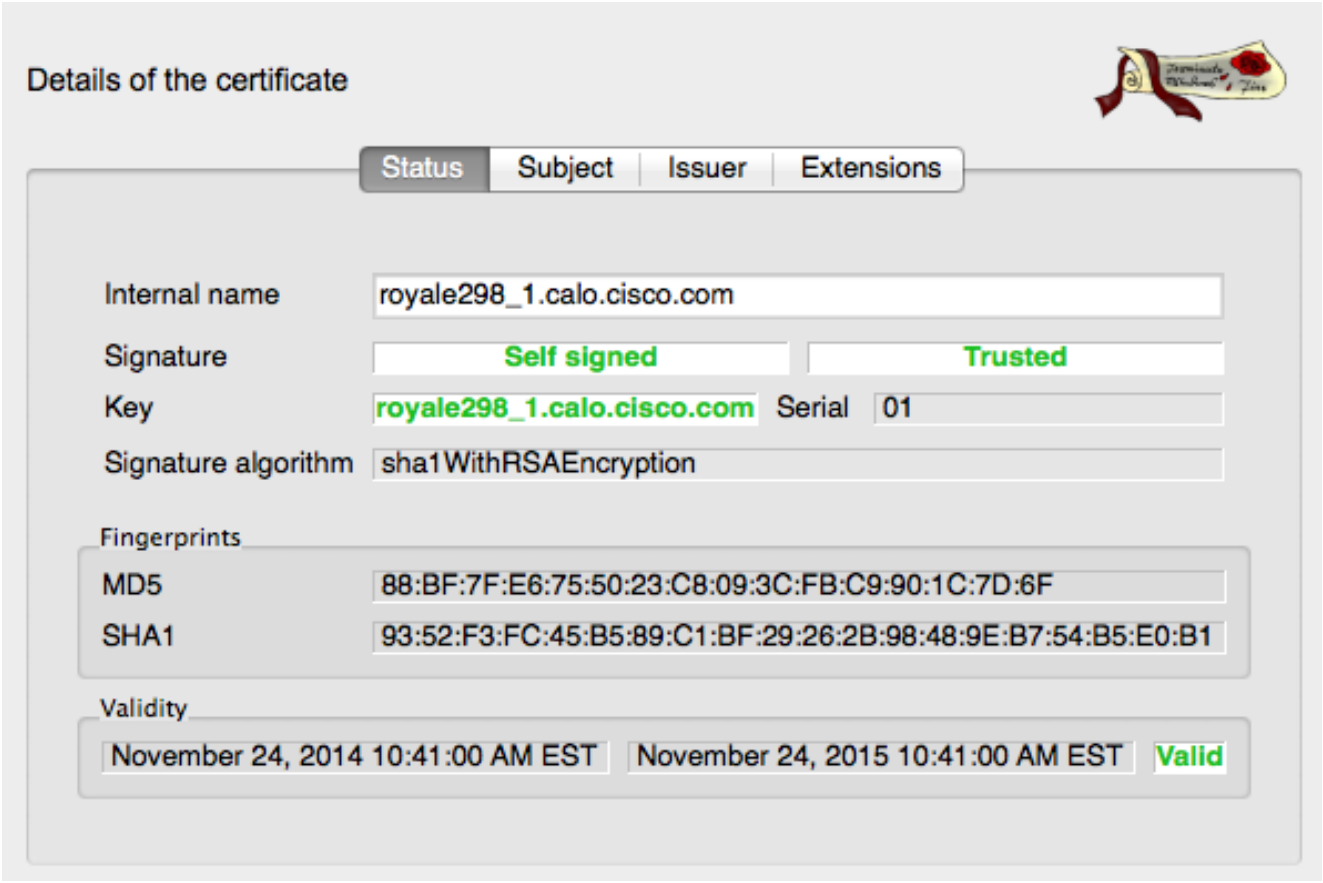
注: PKCS12 およびプライバシー強化メール（PEM）フォーマットされていた認証両方の認証をエクスポートする必要があります。 PKCS12 認証は **.p12 によって**フォーマットされているファイル名として保存します。 PEM 認証は **.crt によって**フォーマットされているファイル名として保存します。



『OK』 をクリック すれば ESA に認証をインポートするとき必要である PKCS12 認証のための暗号化 パスワードが表示されます、:

注: PEM フォーマットされた認証をエクスポートするとき、必要ではないので、パスワードのためにプロンプト表示されません。
認証の詳細を表示するために、ステータス、サブジェクト、発行元および拡張タブを通して

認証および移動をクリックします:



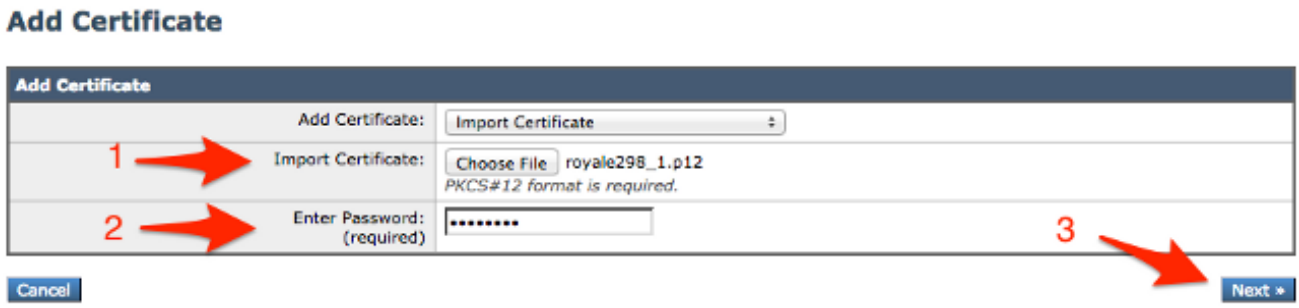
この時点で認証は ESA で使用されて準備ができています。

認証をインポートして下さい

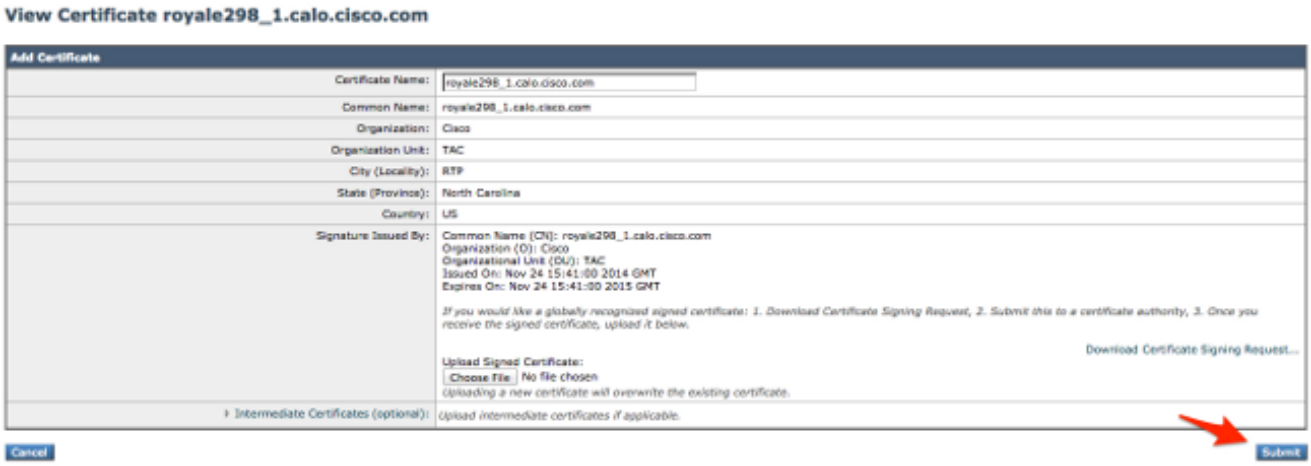
認証が作成されるので、ESA にそれをインポートして下さい。 認証をインポートするためにこれらのステップを完了して下さい:

1. **ネットワーク > 認証 > Add** へのナビゲート **認証... > 輸入 証明書**。

2. 前のセクションで作成した PKCS12 （ .p12 ）フォーマットされていたファイルを、入力しその認証に関連付けられる、『Next』 をクリック します選択して下さいパスワードを:



3. 認証を検討し、変更を保存するために『SUBMIT』 をクリック して下さい:



この時点で認証は ESA の S/MIME に使用して現在準備ができています。

PEM 認証を関連付けて下さい

S/MIME 公開キーに今 PEM フォーマットされた認証を追加して下さい。 PEM フォーマットされた認証を追加するためにこれらのステップを完了して下さい:

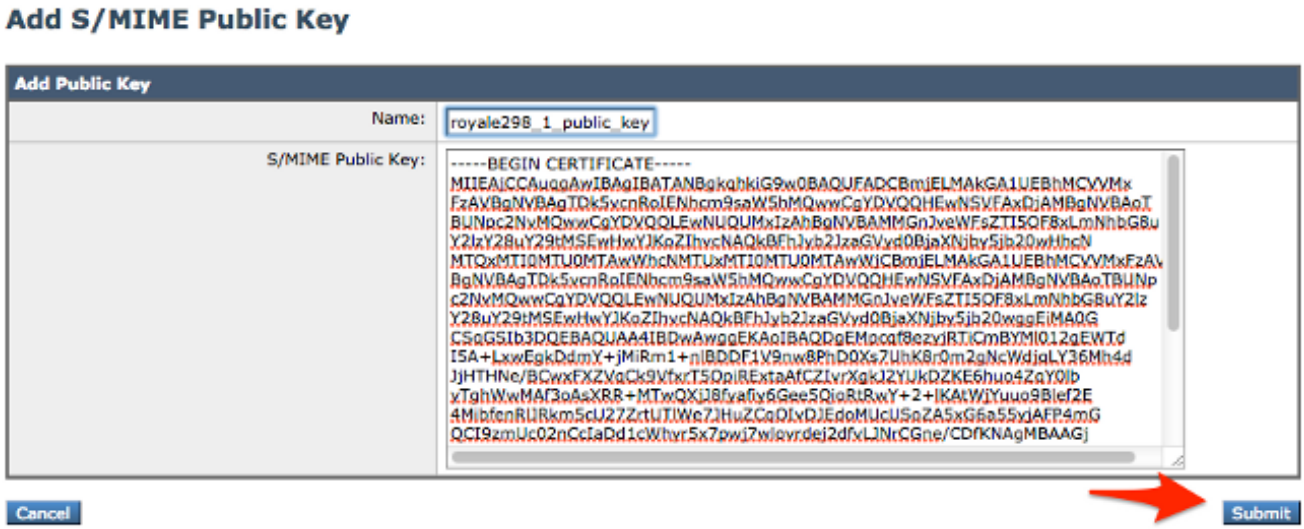
1. ナビゲート して下さい**ポリシー > S/MIME 公開キー > Add 公開キーを郵送するために....**

2. 名前を、要求に応じて入力して下さい。

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認証を開いて下さい （ Notepad++ か原子のような ）。

4. コンテンツをからコピーして下さい **----------BEGIN CERTIFICATE----------** によって **----------END CERTIFICATE----------**を探します。

5. このコンテンツを S/MIME 公開キー セクションに貼り付け、『SUBMIT』 をクリック して下さい:



6. すべての変更を保存して下さい。 この時点で S/MIME 公開キーは ESA のために今設定 され

ます。

関連情報

- 電子メール ユーザガイドのための AsyncOS 9.0
- テクニカルサポートとドキュメント - Cisco Systems