

S/MIME 署名と併用するための ESA 認証作成

目次

[概要](#)

[背景説明](#)

[認証を作成して下さい](#)

[認証をインポートして下さい](#)

[PEM 認証を関連付けて下さい](#)

[関連情報](#)

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ーションです。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:

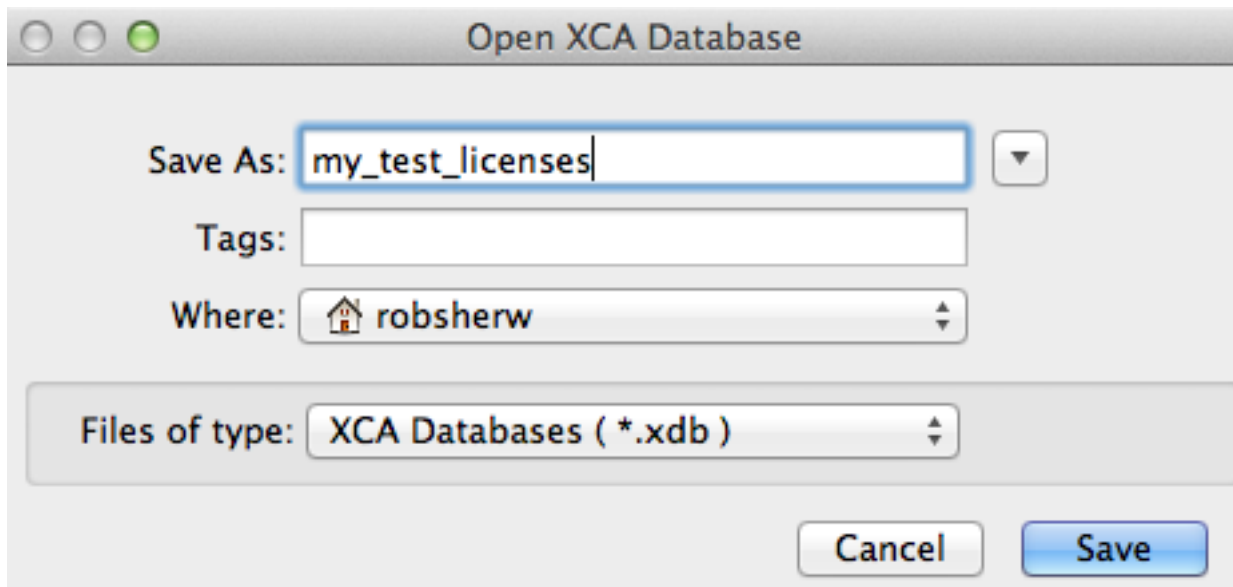
- マッキントッシュ オペレーティング システム (OSX) : [Sourceforge](#)
- Microsoft Windows システム: [Softpedia](#)

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:

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced

Signing request

Sign this Certificate signing request

Copy extensions from the request

Modify subject of the request

Signing

Create a self signed certificate with the serial 1

Use this Certificate for signing


Signature algorithm SHA 1

Template for the new certificate

[default] CA

Apply extensions Apply subject Apply all

認証対象タブから、識別名 セクションに必要な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。

Create x509 Certificate 

Source Subject Extensions Key usage Netscape Advanced

Distinguished name

Internal name	royale298_1.calo.cisco.com	organizationName	Cisco
countryName	US	organizationalUnitName	TAC
stateOrProvinceName	North Carolina	commonName	royale298_1.calo.cisco.com
localityName	RTP	emailAddress	robsherw@cisco.com

Type	Content

Add
Delete

Private key

royale298_1.calo.cisco.com (RSA) Used keys too

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:

Create x509 Certificate



Source Subject **Extensions** Key usage Netscape Advanced

Basic constraints

Type
Path length Critical

Key identifier

Subject Key Identifier
 Authority Key Identifier

Validity

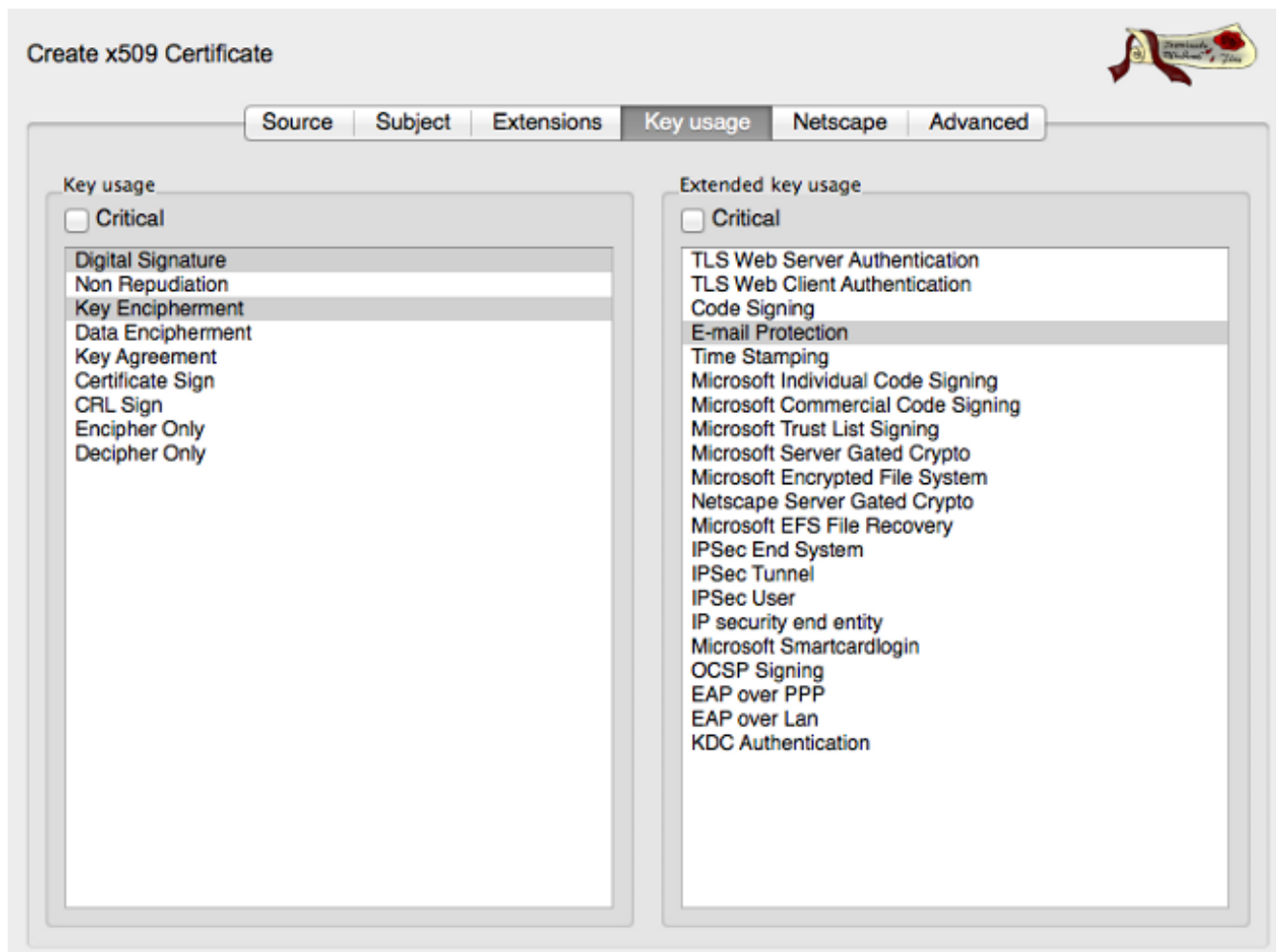
Not before
Not after

Time range

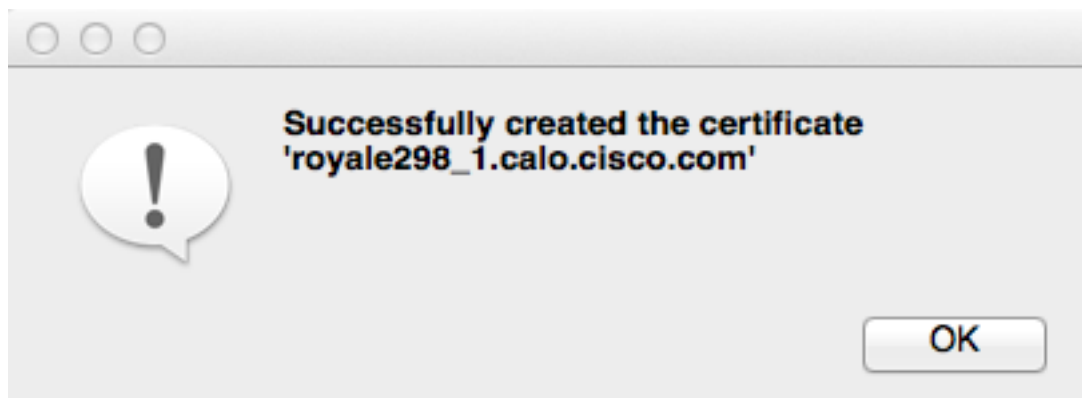
Years
 Midnight Local time No well-defined expiration

subject alternative name
issuer alternative name
CRL distribution point
Authority Info Access

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:

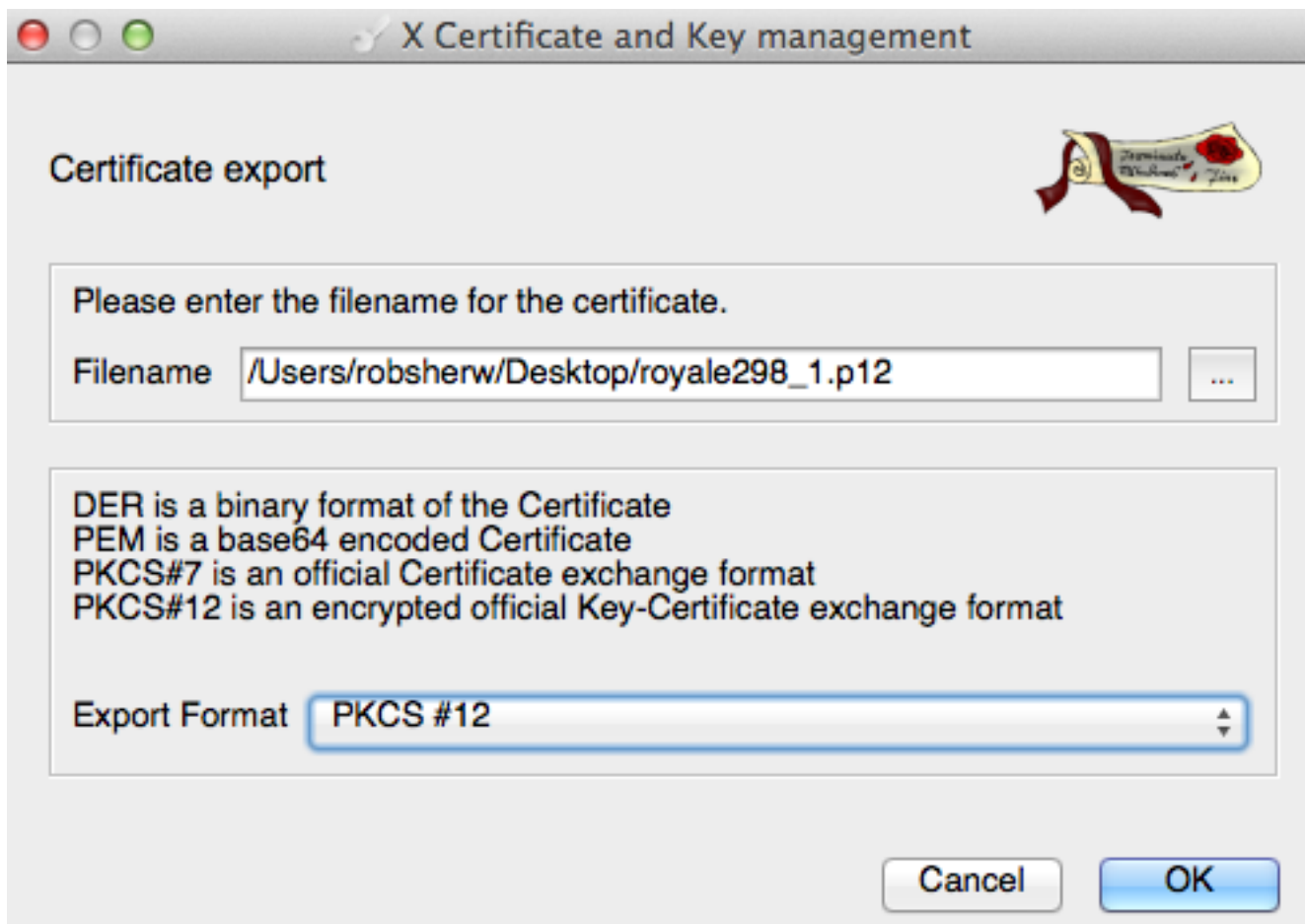


3. スクリーンの一番下で『OK』 をクリック すればポップアップ通知は現われます:

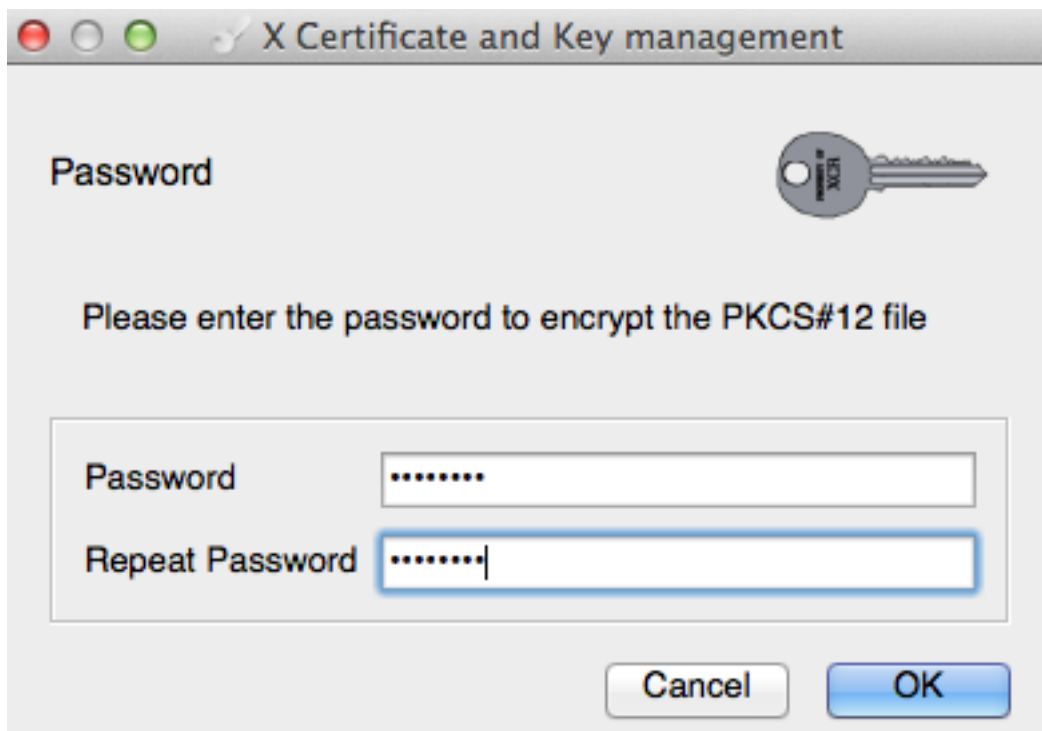


4. 新しく作成された認証は Certificate タブに今現われます。それを強調表示し、『Export』 をクリック するために認証をクリックして下さい。認証が保存する必要があるおよびエクスポート形式を選択して下さいファイル名を、位置。

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:

Details of the certificate

Status | Subject | Issuer | Extensions

Internal name: royale298_1.calo.cisco.com

Signature: Self signed | Trusted

Key: royale298_1.calo.cisco.com | Serial: 01

Signature algorithm: sha1WithRSAEncryption

Fingerprints

MD5: 88:BF:7F:E6:75:50:23:C8:09:3C:FB:C9:90:1C:7D:6F

SHA1: 93:52:F3:FC:45:B5:89:C1:BF:29:26:2B:98:48:9E:B7:54:B5:E0:B1

Validity

November 24, 2014 10:41:00 AM EST | November 24, 2015 10:41:00 AM EST | Valid

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:

Add Certificate

Add Certificate

Add Certificate: Import Certificate

1 → Import Certificate: Choose File royale298_1.p12
PKCS#12 format is required.

2 → Enter Password: (required)

3 → Next *

Cancel

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:

Add Certificate	
Certificate Name:	royale298_1.calo.cisco.com
Common Name:	royale298_1.calo.cisco.com
Organization:	Cisco
Organization Unit:	TAC
City (Locality):	RTP
State (Province):	North Carolina
Country:	US
Signature Issued By:	Common Name (CN): royale298_1.calo.cisco.com Organization (O): Cisco Organizational Unit (OU): TAC Issued On: Nov 24 15:41:00 2014 GMT Expires On: Nov 24 15:41:00 2015 GMT <small>If you would like a globally recognized signed certificate: 1. Download Certificate Signing Request, 2. Submit this to a certificate authority, 3. Once you receive the signed certificate, upload it below.</small>
Upload Signed Certificate:	<input type="button" value="Choose File"/> No file chosen <small>Uploading a new certificate will overwrite the existing certificate.</small>
Intermediate Certificates (optional):	<input type="button" value="Download Certificate Signing Request..."/> <small>Upload intermediate certificates if applicable.</small>

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++ が原子のような)。
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:

Add S/MIME Public Key

Add Public Key	
Name:	royale298_1_public_key
S/MIME Public Key:	<pre> -----BEGIN CERTIFICATE----- MIIEA1CCAuqAAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmIEMAKGA1UEBhMCVVMx FzAVBgNVBAGITDk5xcnRoIENhcj9saW5hMQwwCgYDVQQHEwNSVFAxOjAMBgNVBAoT BUJNc2NvMQwwCgYDVQQLEwNUQUxIzAhBgNVBAMGNjVlWfFsZTI1S0F8xLmNhbg8u Y2IzY28uY29tSEwHwYJKoZIhvcNAQkBFhJyb2JzaGVyY29mY29mY29mY29mY29m MTQxMTI0MTU0MTAwW3cNMTUxMTI0MTU0MTAwW3cNMTUxMTI0MTU0MTAwW3cNMTUx BgNVBAGITDk5xcnRoIENhcj9saW5hMQwwCgYDVQQHEwNSVFAxOjAMBgNVBAoTBUJN c2NvMQwwCgYDVQQLEwNUQUxIzAhBgNVBAMGNjVlWfFsZTI1S0F8xLmNhbg8uY2Iz Y28uY29tSEwHwYJKoZIhvcNAQkBFhJyb2JzaGVyY29mY29mY29mY29mY29mY29m CSsGSIb3DQEBAQUAA4IBDwAwgEKAoIBAQDgEMocaf8ezvRT/CmBYMIQ12qEWTd ISA+LxwEgkDdmY+jMiRm1+nIBDDF1V9nw8PhD0Xs7UhK8r0m2aNcWdjaLY36Mh4d JjHTHNe/BCwxFXZVaCk9VfxrT5OpIReXtaAfcZlvrXgkJ2YUkDZKE6huo4ZqY0Ib yTghWwMAF3oAaXRR+MTwQXj8fyafy6Gee5QioRtRwY+2+IKAtWjYuu09Blf2E 4MibfenRUIRkm5cU2Z7ZrtUJIWeZJHuZCgDIvDJEdeMUcUSoZASxG6a55ydAFP4mG QCI9zmUc02nCcIaRd1cWhtv5x7pwi7wIvvrdej2dfxLJNrCGne/CDfKNAgMBAAGj -----END CERTIFICATE----- </pre>

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](#)