

S/MIME シグニチャで使用する ESA 証明書の作成

目次

[はじめに](#)

[背景説明](#)

[ESA からの S/MIME 証明書を作成して下さい](#)

[サードパーティ製のアプリケーションからの S/MIME 証明書を作成して下さい](#)

[証明書の作成](#)

[ESA に証明書をインポートして下さい](#)

[PEM 証明書の関連付け](#)

[関連情報](#)

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ーションからの 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。

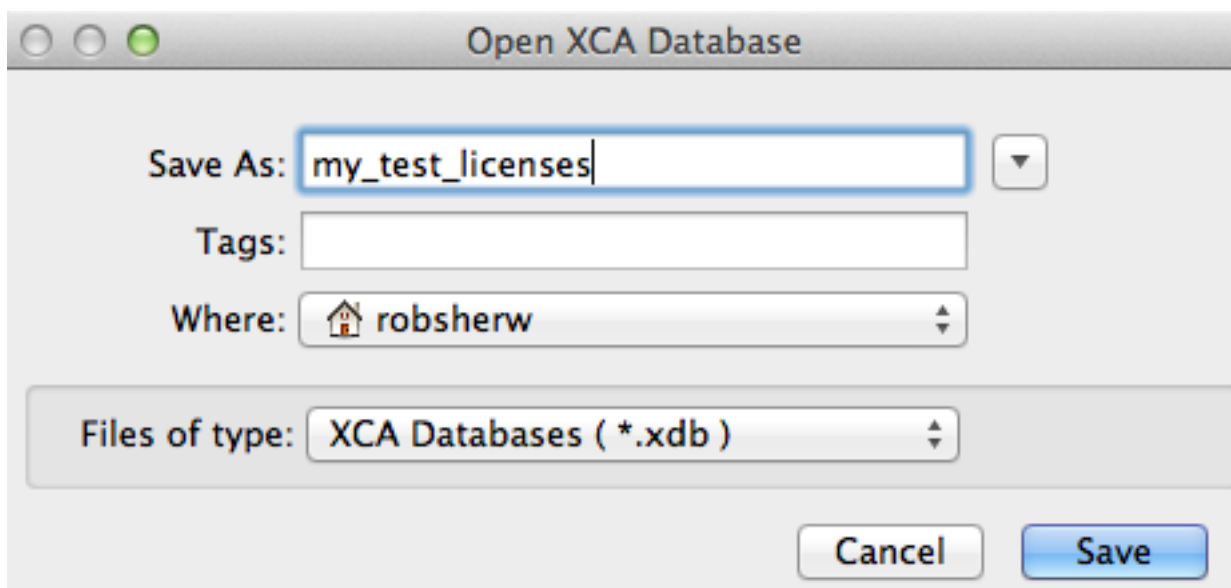
- Macintosh オペレーティングシステム (OSX) : [Sourceforge](#)
- Microsoft Windows システム : [Sourceforge](#)

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。

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


Use this Certificate for signing

Signature algorithm

Template for the new certificate

Apply extensions Apply subject Apply all

[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。

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。

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

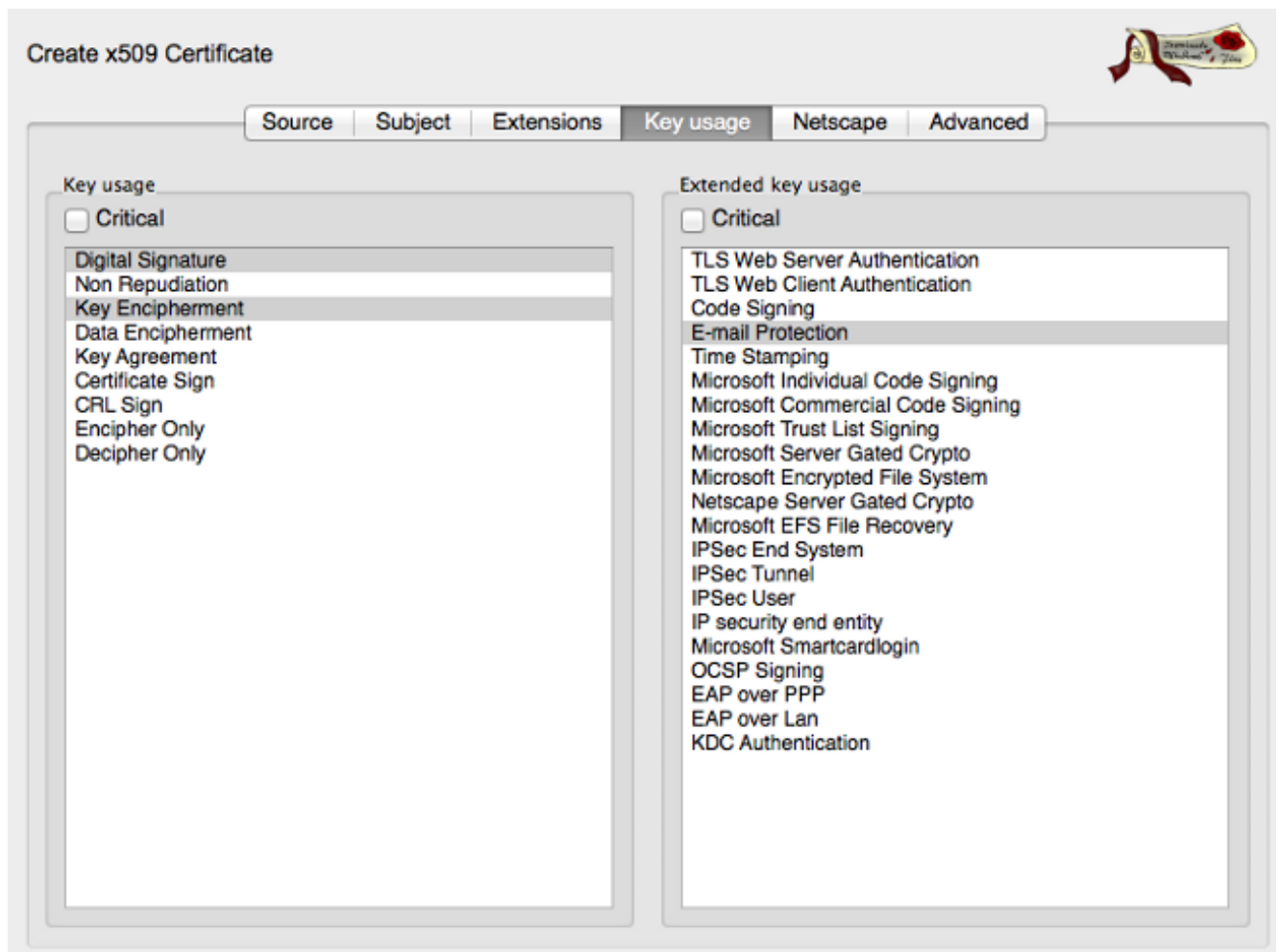
Not before
Not after

Time range

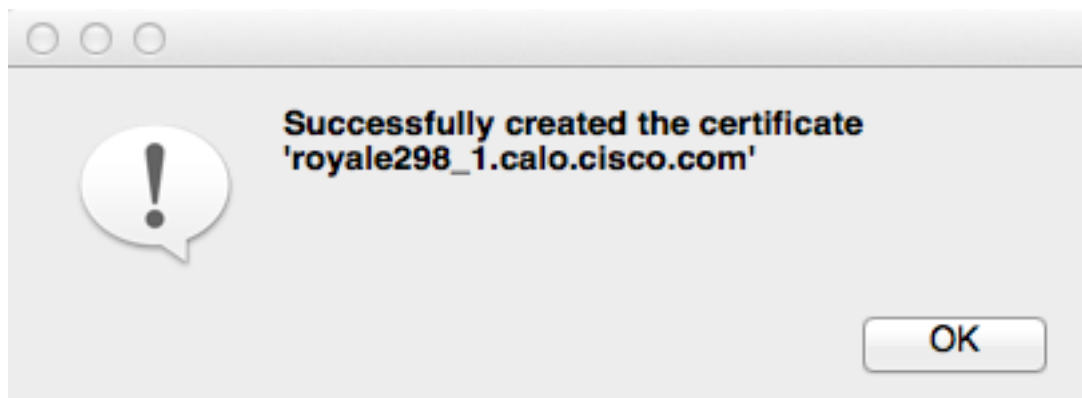
Midnight Local time No well-defined expiration

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

[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。

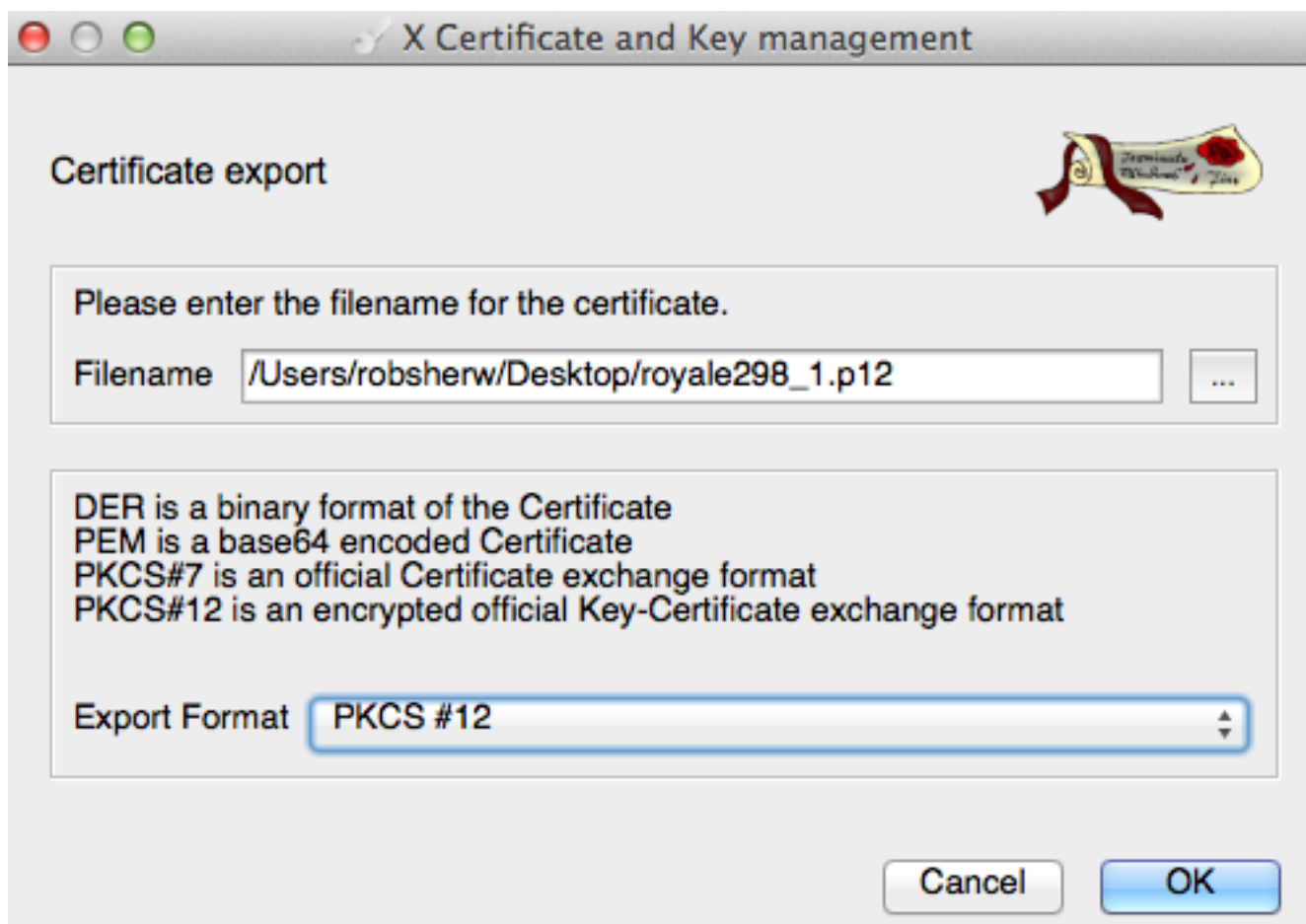


3. 画面最下部の [OK] をクリックすると、ポップアップ通知が表示されます。

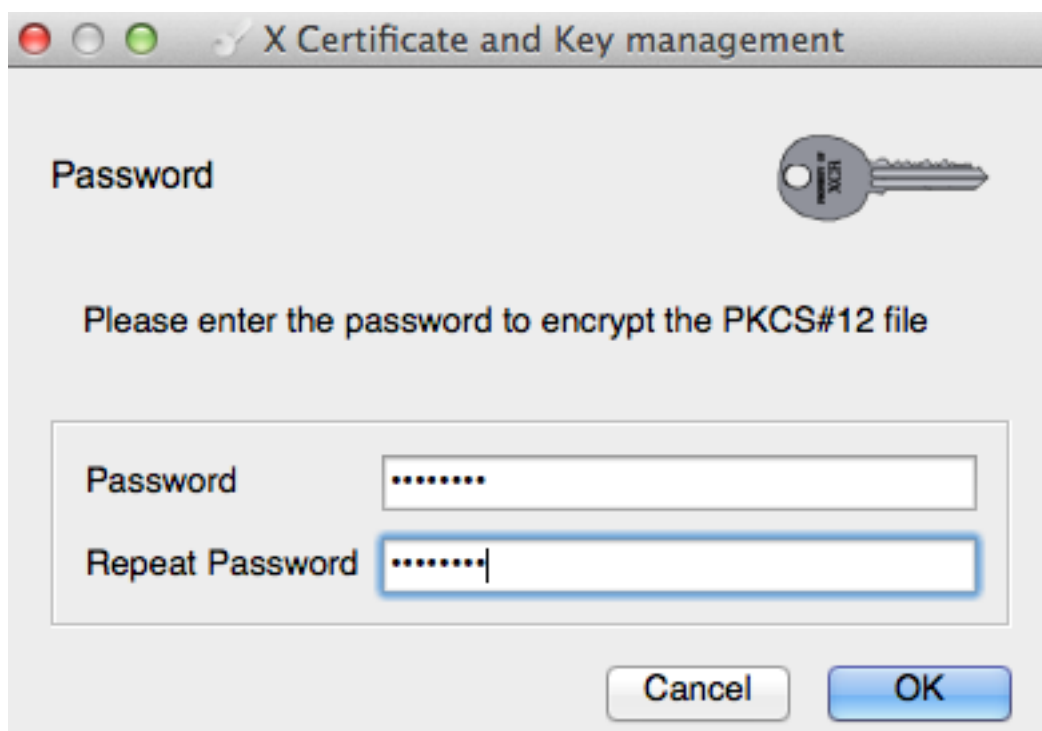


4. 新規作成した証明書が [Certificate] タブに表示されます。その証明書をクリックして強調表示し、[Export] をクリックします。ファイル名、証明書の保存場所、およびエクスポート形式を選択します。


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。

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。

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 →

Cancel Next *

3. 証明書を確認し、[Submit] をクリックして変更を確定します。

View Certificate royale298_1.calo.cisco.com

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 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. Download Certificate Signing Request...
Upload Signed Certificate:	<input type="button" value="Choose File"/> No file chosen Uploading a new certificate will overwrite the existing certificate.
Intermediate Certificates (optional):	Upload intermediate certificates if applicable.



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。

Add S/MIME Public Key

Add Public Key	
Name:	royale298_1 public key
S/MIME Public Key:	<pre>-----BEGIN CERTIFICATE----- MIIEAICCAuqaAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmIEMAKGA1UEBhMCVVMx FzAVBgNVBAAgTDk5xcnRoLENhcm9saW5hMQwwCgYDVQQHEwNSVFAxDMBAgNVBAoT BUJnc2NwMQwwCgYDVQQLEwNUQUxhZAhBgNVBAMMGnJveWZsZTI1OF8xLmNhbG8u Y2IzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJyb2JzaGVyY29tMSEwHwYJKoZI hvcNAQkBFhJyb2JzaGVyY29tMSEwHwYJKoZIhvcNAQkBFhJyb2JzaGVyY29t MTQxMTI0MTU0MTAwW3BmIEMAKGA1UEBhMCVVMxMSEwHwYJKoZIhvcNAQkBFh BgNVBAAgTDk5xcnRoLENhcm9saW5hMQwwCgYDVQQHEwNSVFAxDMBAgNVBAoT BUJnc2NwMQwwCgYDVQQLEwNUQUxhZAhBgNVBAMMGnJveWZsZTI1OF8xLmNhbG8u Y2IzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJyb2JzaGVyY29tMSEwHwYJKoZI hvcNAQkBFhJyb2JzaGVyY29tMSEwHwYJKoZIhvcNAQkBFhJyb2JzaGVyY29t CScGSIb3DQEBAQAIAAIBDwAwggEKAoIBAQCdEMocaf8ezvRTICmBYMIQ12qEWTd ISA+LxwEgkDdmY+jMIRm1+nIBDDF1V9nw8PhD0Xs7UhhK8r0m2qNcWdjaLY36Mh4d JJHThNe/BcWwFXZVaCk9VfxrT5DpiBExtAfcZlvrXgkJ2YUkDZKE6huo4ZqY0Ib yTghWwMAF3oAaXRR+MTwQXJ38fvafv6Gee5QioRtRwY+2+IKAtWjYuuo9Bf2E 4MibfenRUIRkm5cUz7ZrtUjWeZJHuZCgDIvDJEdoMUcUsaZA5xG6a55vjAFP4mG QCI9zmUc02nCiaDd1cWthv5x7owi7wlvvrdej2dfvLJNtCGne/CDfKNAGMBAAGJ -----END CERTIFICATE-----</pre>



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](#)