

Creación del certificado ESA para el uso con la firma S/MIME

Contenido

[Introducción](#)

[Antecedentes](#)

[Cree el certificado S/MIME del ESA](#)

[Cree el certificado S/MIME de la aplicación de terceros](#)

[Cree un certificado](#)

[Importe un certificado al ESA](#)

[Asocie un certificado PEM](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo crear los Certificados para comprobar con seguro/los Multipurpose Internet Mail Extension (S/MIME) que firman en el dispositivo de seguridad del correo electrónico de Cisco (ESA).

Antecedentes

Cuando usted crea un certificado S/MIME para el mensaje que firma, debe cumplir los requisitos descritos en el [RFC 5750](#): Asegure/versión 3.2 de los Multipurpose Internet Mail Extension (S/MIME) - certifique la dirección.

Cree el certificado S/MIME del ESA

Los certificados autofirmados S/MIME se pueden crear del ESA GUI:

1. Elija el **certificado de la red > de los Certificados > Add...**
2. El lista desplegable, elija **crean el certificado Uno mismo-firmado S/MIME**
3. Complete la información apropiada por requerimiento.
4. Haga clic en Next (Siguiente).
5. El tecleo **somete** para salvar la creación del certificado.
6. **El cometer del tecleo cambia** para salvar los cambios a la configuración.

Para utilizar el certificado y configurar las claves públicas S/MIME, usted necesita hacer guardar una copia del certificado en el formato del .pem:

1. Elija la **red > los Certificados**
2. Haga clic el enlace hipertexto para el certificado que usted acaba de crear.
3. Haga clic el **pedido de firma de certificado de la descarga...**

Esto salva el archivo como *cert.pem localmente* a su ordenador. Salve esto para el uso más adelante en sección "socio del certificado PEM" de este artículo.

Cree el certificado S/MIME de la aplicación de terceros

Los Certificados la prueba (o permanente) se puede crear externamente del ESA también. Por este ejemplo, el certificado y la administración de claves (XCA) X es una aplicación que maneja las claves asimétricas, tales como Rivest-Shamir-Addleman (RSA) o Digital Signature Algorithm (DSA), y se piensa ser un pequeño Certificate Authority (CA) para la creación y la firma de los Certificados. Utiliza la biblioteca abierta de Secure Sockets Layer (OpenSSL) para las operaciones criptográficas.

Note: El XCA es una aplicación de terceros que no es soportada por Cisco. El uso de esta aplicación se proporciona solamente para el ejemplo y la facilidad de la administración para la administración, la prueba, y la configuración S/MIME. Para las profundidades totales y las instrucciones en el XCA, refiera al [XCA - certificado X y](#) documento de la [administración de claves](#).

Usted puede descargar la aplicación XCA en cualquiera de estas ubicaciones:

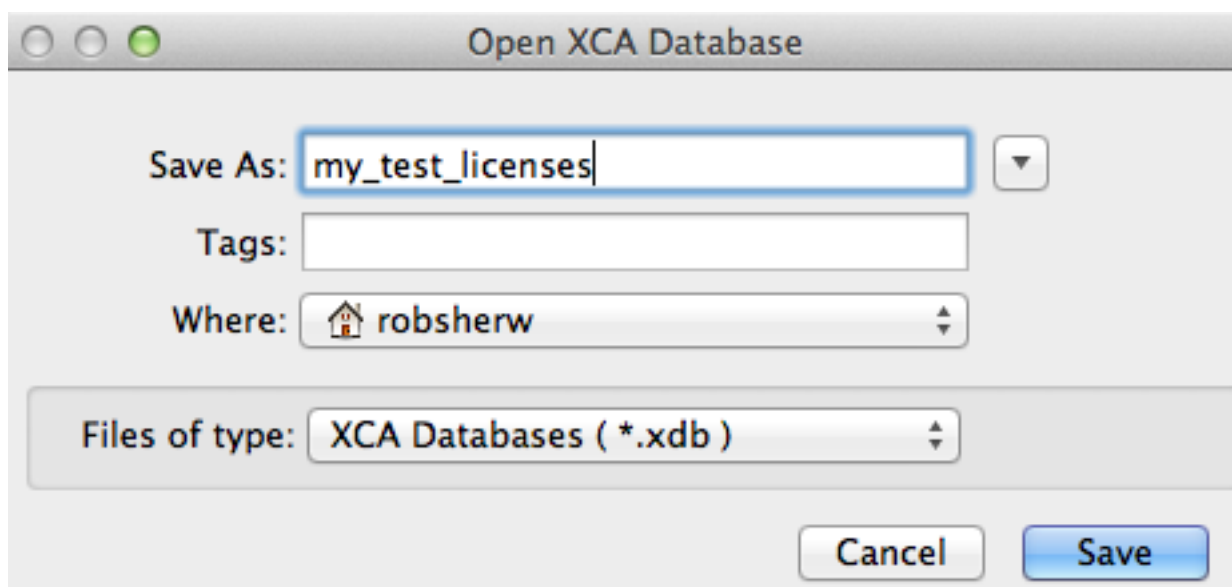
- Sistemas operativos de Macintosh (OSX): [Sourceforge](#)
- Sistemas de Microsoft Windows: [Sourceforge](#)

Cree un certificado

Complete estos pasos para crear un certificado S/MIME:

1. Utilice la aplicación XCA para crear una nueva base de datos XCA o abrir una base de datos actual XCA, si existe una ya.

De la barra de menú, elija el **archivo > nueva base de datos > nombre <DB de su choice>**:




Click **Save**. Ahora usted debe ingresar una contraseña para el cifrado de sus claves privadas que se asocien a esta base de datos. Esta contraseña está solamente para la base de datos XCA.



Haga Click en OK para acabar la creación de la base de datos.

2. De los Certificados tabule, elija el **nuevo certificado** y la pantalla del *certificado del crear x509* aparece.

No se requiere ningunos cambios de la lengüeta de la fuente, pues los valores predeterminados pueden ser utilizados:

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

De la lengüeta **Source**, ingrese la Información requerida en la sección del nombre distintivo. En la sección de la clave privada, el tecléo **genera una nueva clave** y elige **2048 el bit** o el **bit 1024** para el keysize. Haga clic **crean** para generar la clave privada y asociarla a este certificado.

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

De la lengüeta de las Extensiones, en la sección básica de los apremios, elija el **Certificate Authority** para el tipo.

Note: Los pedidos de firma de certificado subsiguientes (CSR) se pueden firmar vía este CA con el conjunto del tipo a **no definido**.

En la sección de la validez, entre los detalles según sus requisitos (365 días por abandono). Usted puede elegir agregar un nombre alternativo sujeto (SAN) para el Domain Name System (DNS), la dirección de correo electrónico, y el similar con el uso del **botón Edit** para esa línea. De la ventana emergente SAN, el tecleo **agrega** y elige el tipo SAN y el contenido asociado. Una vez que está completado, el tecleo **se aplica** para aplicar estos cambios y volver a las Extensiones tabule la ventana:

Create x509 Certificate



Source Subject **Extensions** Key usage Netscape Advanced

Basic constraints

Type Critical

Path length

Key identifier

Subject Key Identifier

Authority Key Identifier

Validity

Not before

Not after

Time range

Midnight Local time No well-defined expiration

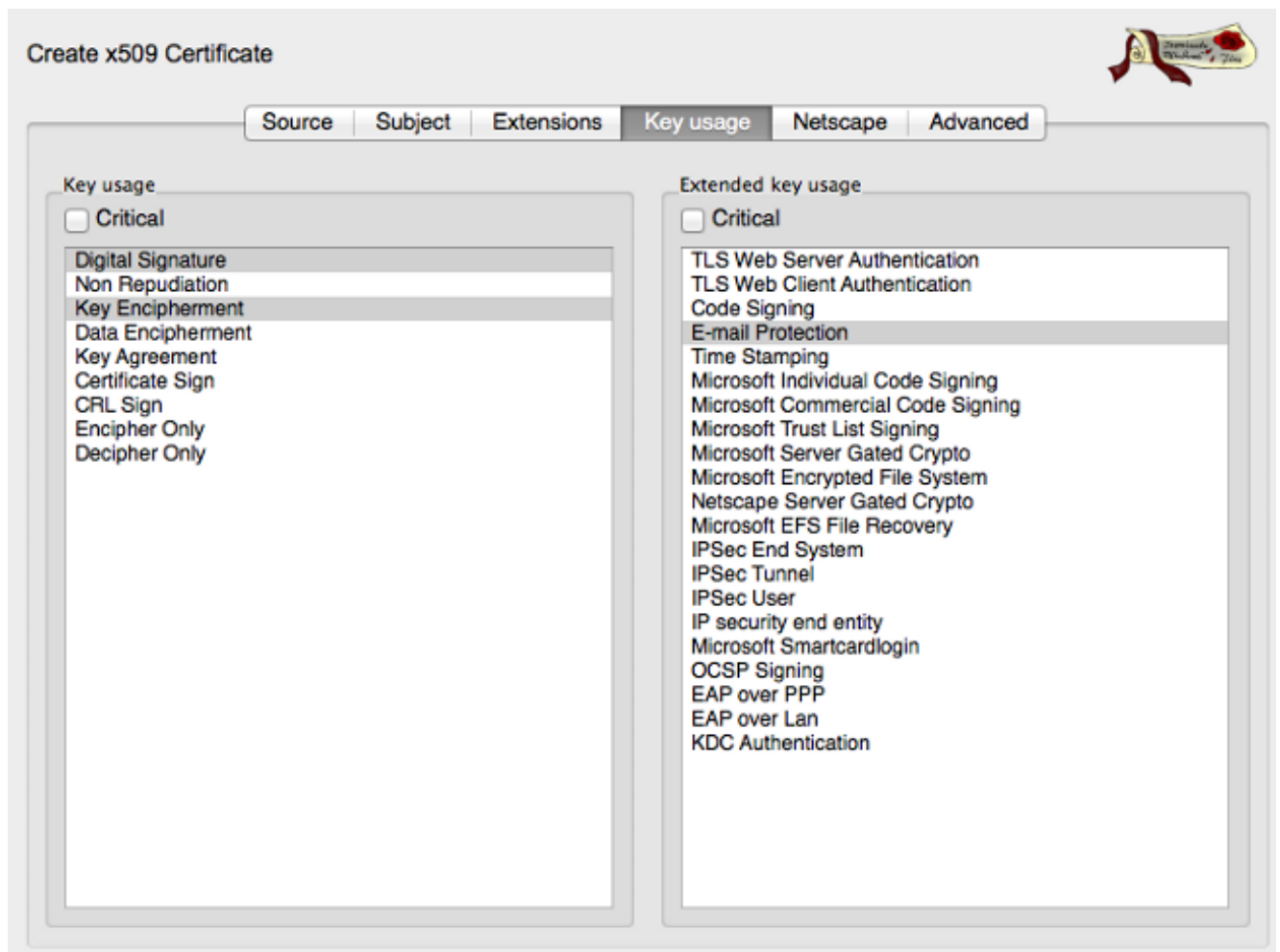
subject alternative name

issuer alternative name

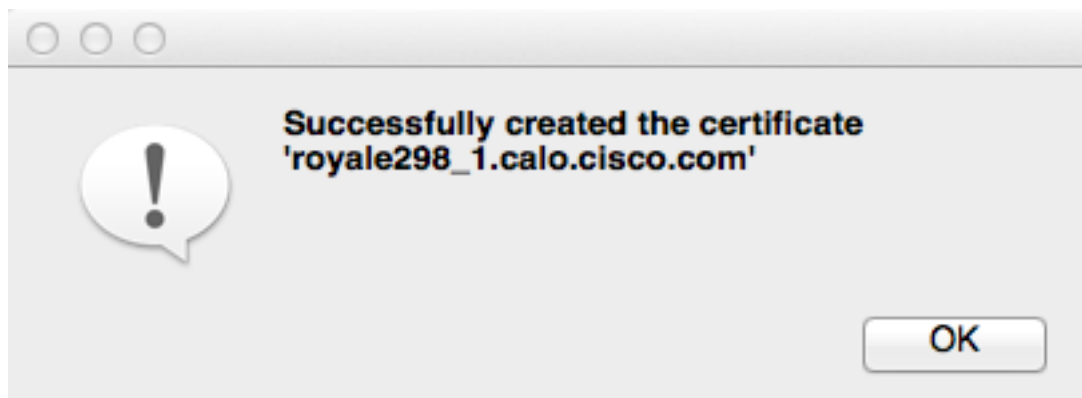
CRL distribution point

Authority Info Access

De la lengüeta dominante del uso, en la sección dominante del uso, resalte la **firma digital** y la **estenografía de la clave**. En la sección dominante extendida del uso, resalte la **protección del email**. Éstos son los elementos requeridos para S/MIME:

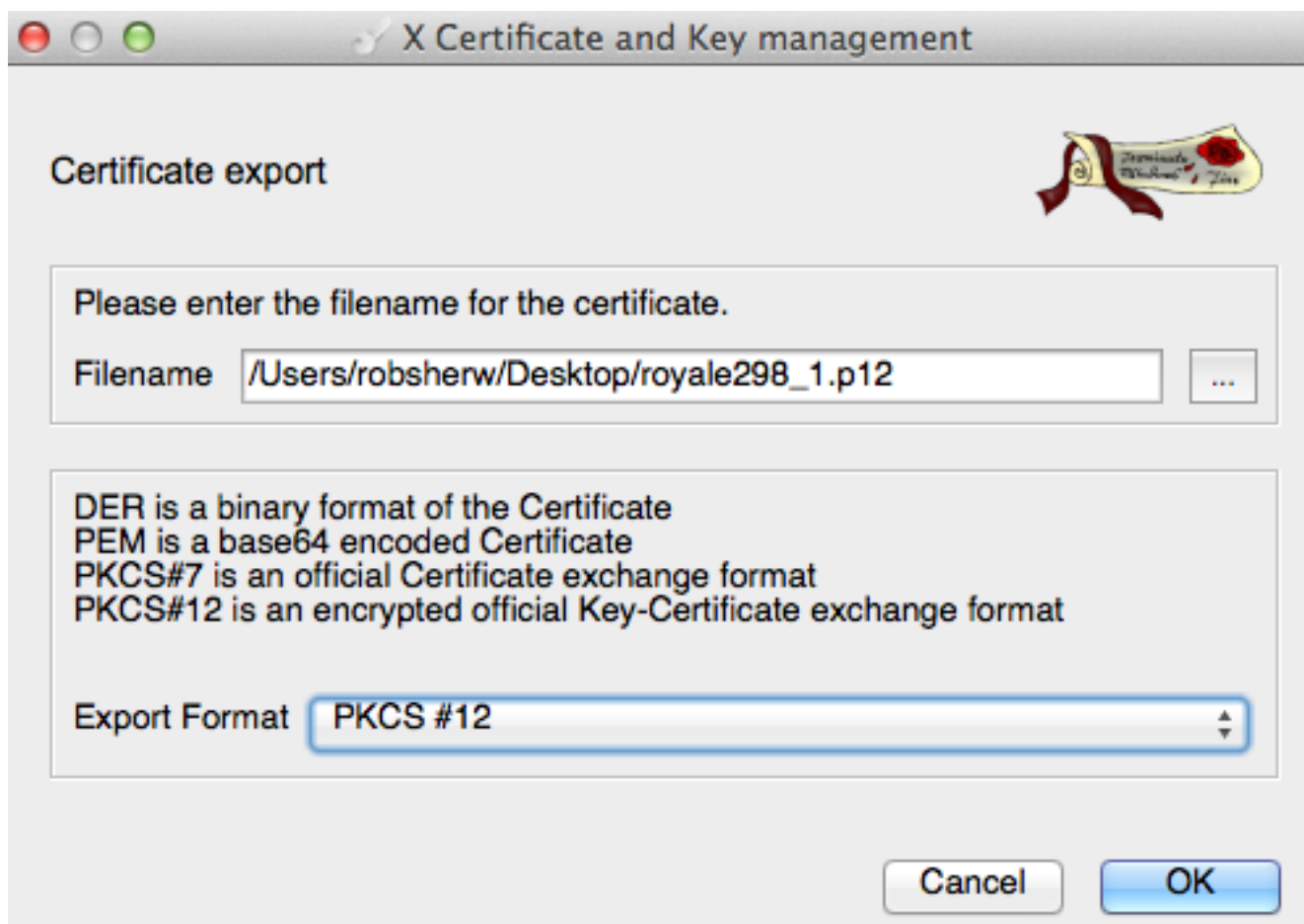


3. El Haga Click en OK en la parte inferior de la pantalla y de una notificación móvil aparece:

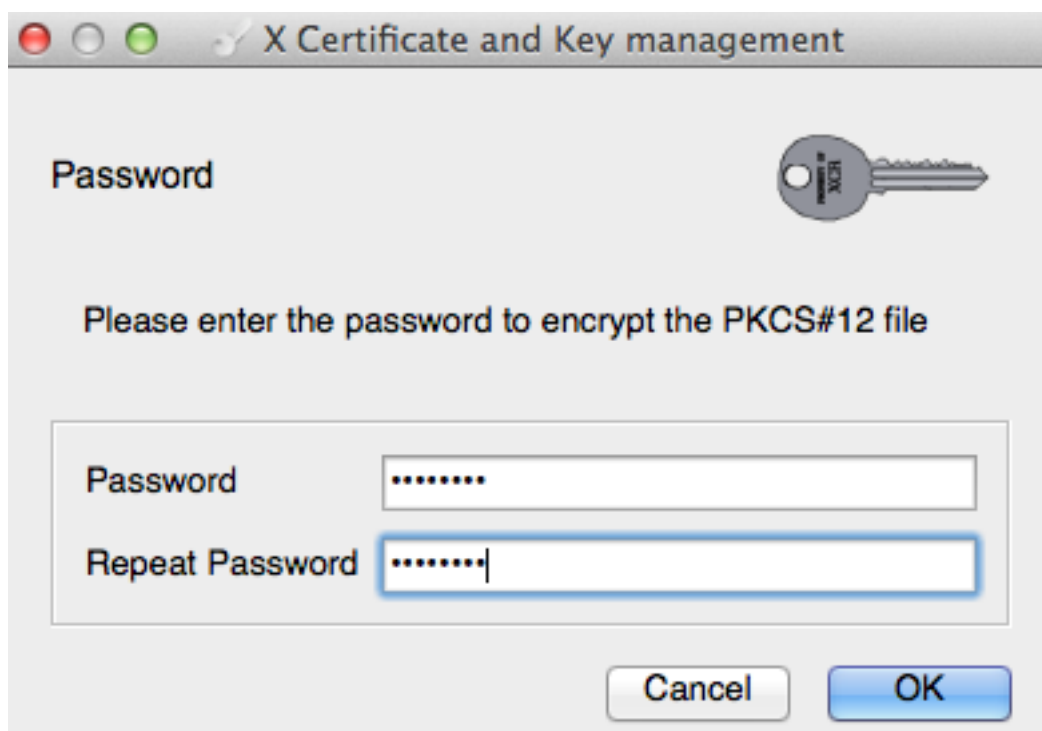


4. Su certificado creado recientemente ahora aparece en el teclado de cuadro del certificado el certificado para resaltar lo y la **exportación del** teclado. Seleccione el nombre de fichero, la ubicación a los cuales el certificado debe ser guardado, y el formato de la exportación.

Note: Usted debe exportar su certificado en ambo PKCS12 y Certificados formados Privacy Enhanced Mail (PEM). El certificado del PKCS12 guarda como nombre del archivo formatado **.p12**. El certificado PEM guarda como nombre del archivo formatado **.crt**.



Presentan el Haga Click en OK y le con la contraseña del cifrado para el certificado del PKCS12, que es necesario cuando usted importa el certificado sobre el ESA:



Note: Cuando usted exporta el certificado PEM-formatado, le no indican para una contraseña, pues no es necesaria. Para ver los detalles del certificado, haga clic los **Certificados** y el movimiento a través de las lengüetas del estatus, del tema, del emisor, y de

las Extensiones:

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

En este momento su certificado está listo para ser utilizado en su ESA.

Importe un certificado al ESA

Si usted ha creado un certificado externamente del ESA usted debe importarlo sobre su ESA. Complete estos pasos para importar el certificado:

1. Elija el **certificado de la red** > de los **Certificados** > **Add...** > **Import Certificate (Importar certificado)**.
2. Elija el archivo formatado del PKCS12 (.p12) que usted creó en la sección anterior, ingresan la contraseña que se asocia a ese certificado, y hacen clic **después**:

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. Revise el certificado y el teclado **some** para confiar sus cambios:

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

En este momento su certificado está listo ahora para ser utilizado para S/MIME en su ESA.

Asocie un certificado PEM

Usted debe ahora agregar su certificado PEM-formatado a las claves públicas S/MIME. Complete estos pasos para agregar el certificado PEM-formatado:

1. Elija la **clave pública de las directivas del correo > de las claves públicas S/MIME > Add....**
2. Ingrese el nombre, en caso de necesidad.
3. Abra el certificado formatado PEM (.crt) en un editor de textos apropiado (tal como [Windows/PC] Notepad++ o [OSX] del átomo).
4. Copie el contenido de **----COMIENZE EL CERTIFICADO----** por **----CERTIFICADO DEL EXTREMO-----**.
5. Pegue este contenido en la sección de la clave pública S/MIME y el tecleo **somete:**

Add S/MIME Public Key

Add Public Key	
Name:	royale298_1 public key
S/MIME Public Key:	<pre> ----BEGIN CERTIFICATE---- MIIEAjCCAuqAAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmIEMAKGA1UEBhMCVVMx FzAVBgNVBAgTDk5xcnRoIEhcm9saW5hMQwwCgYDVQQHEwNSVFAxTAMBAQNVBAoT BUlNc2NvMQwwCgYDVQQLEwNUQUUxZjZlZmZlYmZlZmZlZmZlZmZlZmZlZmZlZmZl Y2ZlY2ZlY2ZlMSEwHwYJKoZIhvcNAQkBFhJyb2JzaGVyd0BjaXNjb3ZlMjQwHhcn MTQxMTI0MTU0MTAwW3cNMTEuMTI0MTU0MTAwWjCBmIEMAKGA1UEBhMCVVMx FzAVBgNVBAgTDk5xcnRoIEhcm9saW5hMQwwCgYDVQQHEwNSVFAxTAMBAQNVBAoT BUlNc2NvMQwwCgYDVQQLEwNUQUUxZjZlZmZlYmZlZmZlZmZlZmZlZmZlZmZlZmZl Y2ZlY2ZlY2ZlMSEwHwYJKoZIhvcNAQkBFhJyb2JzaGVyd0BjaXNjb3ZlMjQwHhcn CSaGSIB3DQEBAQUAAAIBoDwAwqEKAoIBAQQDgEMocaf8ezvRTICmBYMIQ12qEWtd ISA+LxxEgkDdmY+jMIRm1+nIBDDE1V9nw8PhDQx7Uhk8r0m2qNcWdjaLY36Mh4d JJHThNe/BCwxFXZVaCk9VfxrT5DpI8ExtAAtCZlvr7gkZ2YUkDZKE6huo4ZqY0Ib yTghWwMAF3oAaXRR+MTwQXl38fvafv6Gee5QioRtRwY+2+IKaIWjYuuo9Blef2E 4MibfenRUIRkm5cUz7ZrtUJIWeZJHuZCaDiVdJEdoMUcUsqZA5xG6a55vjAfp4mG QCI9zmUc02nCcIaDd1cWhvr5x7pwi7wl9vrdej2dfvLJNcGne/CDfKNAgMBAAGj </pre>
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>

6. Confíe todos los cambios. En este momento su clave pública S/MIME ahora se fija para su ESA.

Información Relacionada

- [Guías del usuario final del dispositivo de seguridad del correo electrónico de Cisco](#)
- [Release Note y información general del dispositivo de seguridad del correo electrónico de Cisco](#)

Cisco

- Soporte Técnico y Documentación - Cisco Systems