

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

Contenido

[Introducción](#)

[Antecedentes](#)

[Cree un certificado](#)

[Importe un certificado](#)

[Asocie un certificado PEM](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo crear los Certificados para el uso 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.

Para este proceso, el uso de una aplicación externa se requiere para generar el certificado. 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.

Nota: 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](#)

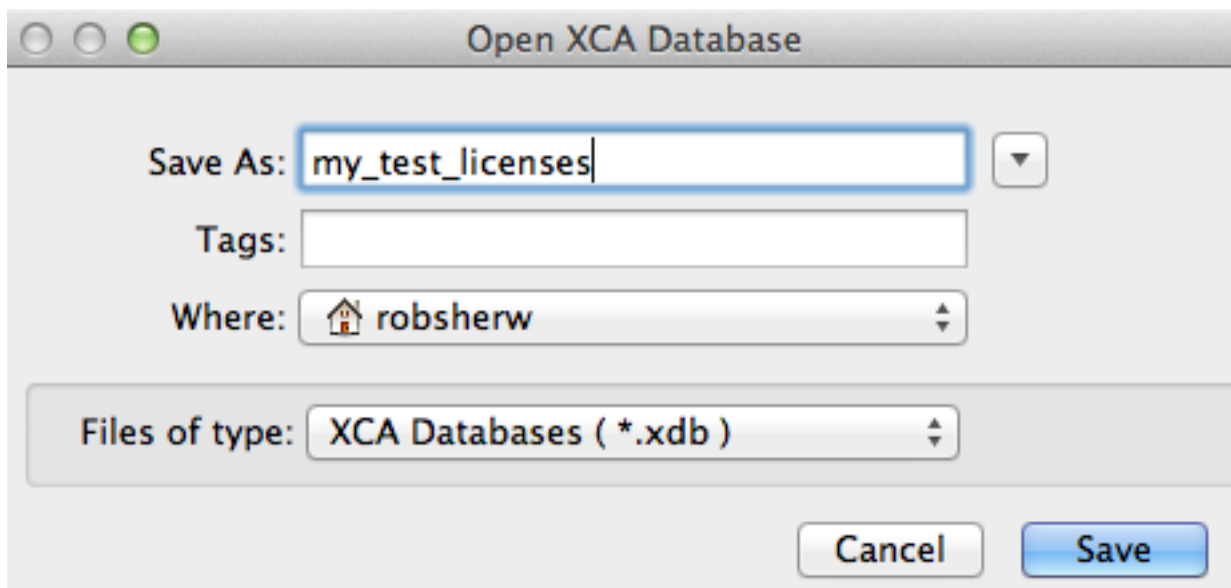
- Sistemas de Microsoft Windows: Softpedia

Cree un certificado

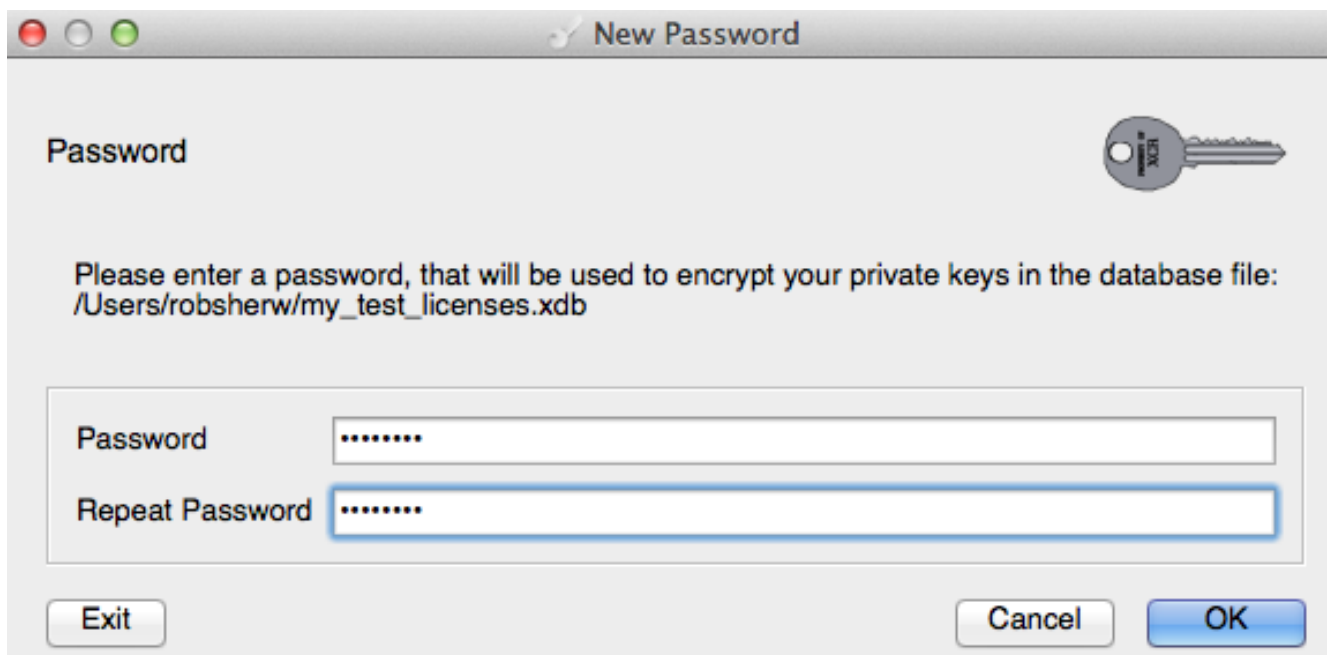
Complete estos pasos para crear un certificado S/MIME:

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, navegue **para clasificar > nueva base de datos > nombre <DB de su choice>**:



Haga clic en Save (Guardar). 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, **nuevo certificado** selecto 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

Show 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

De la lengüeta *sujeta*, ingrese la Información requerida en la sección del nombre distintivo. En la sección de la clave privada, el tecleo **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, seleccione el **Certificate Authority** para el tipo.

Nota: 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 selecciona 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

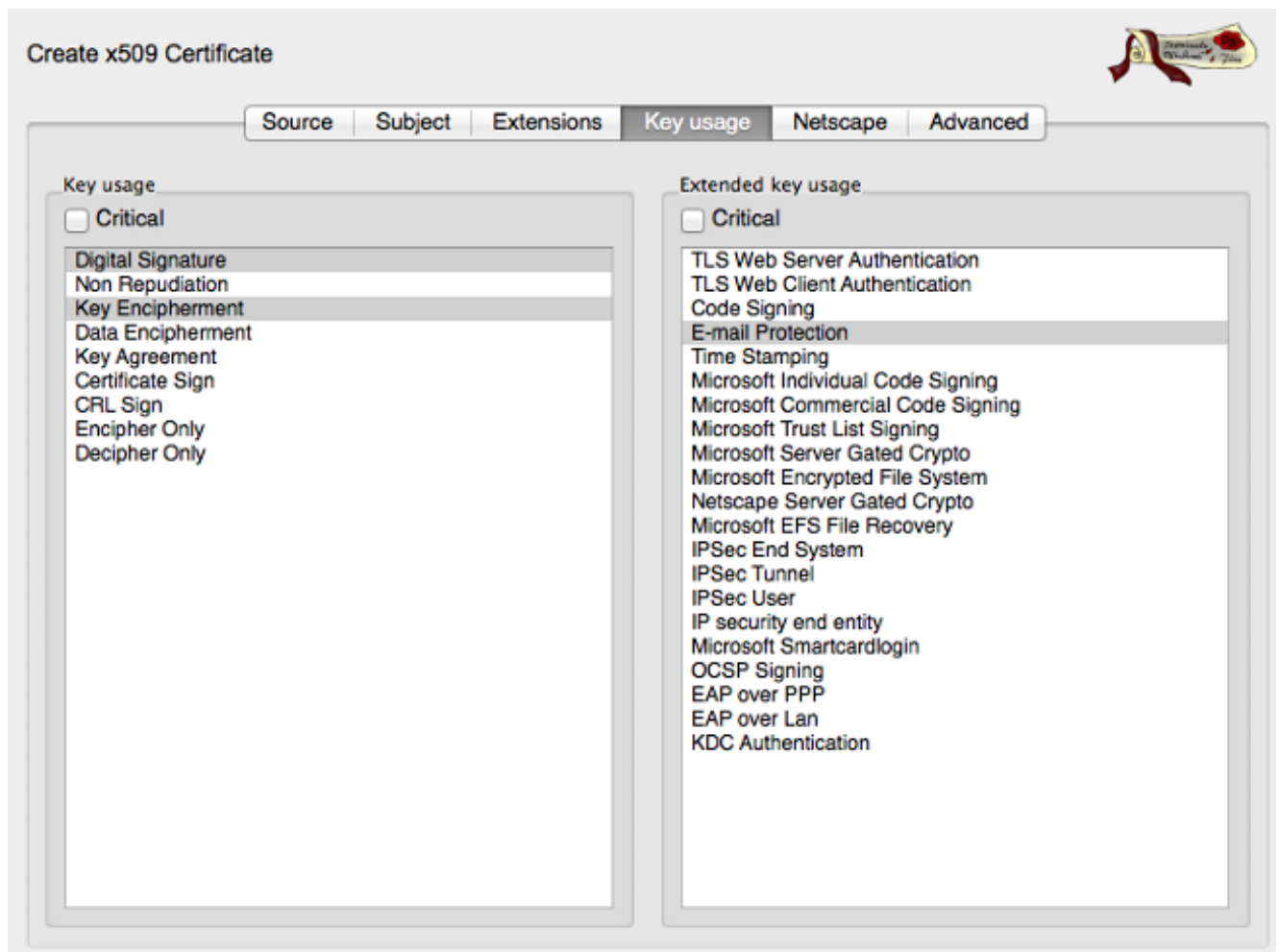
subject alternative name

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:

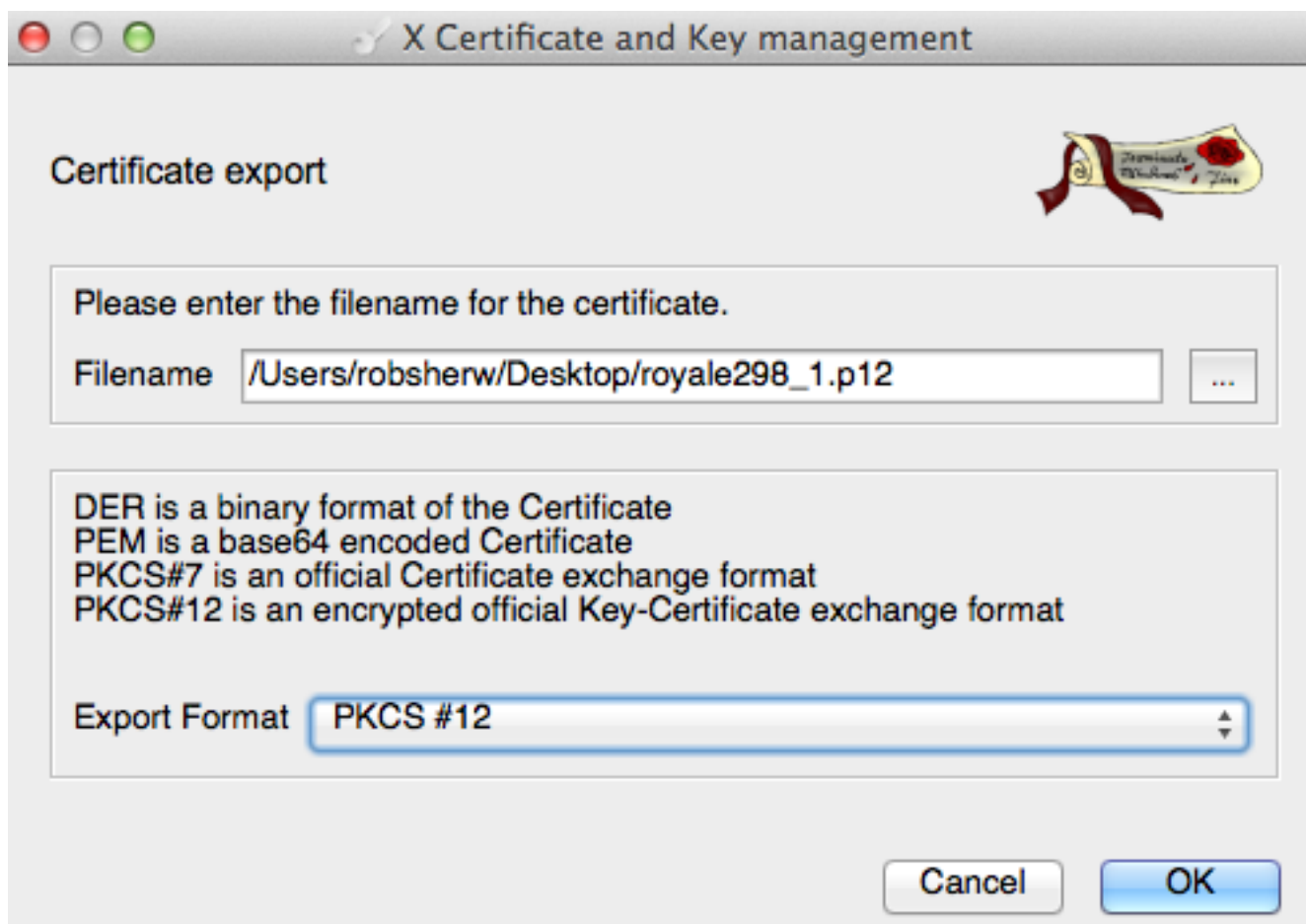


3. El Haga Click en OK en la parte inferior de la pantalla y de una notificación móvil aparece:

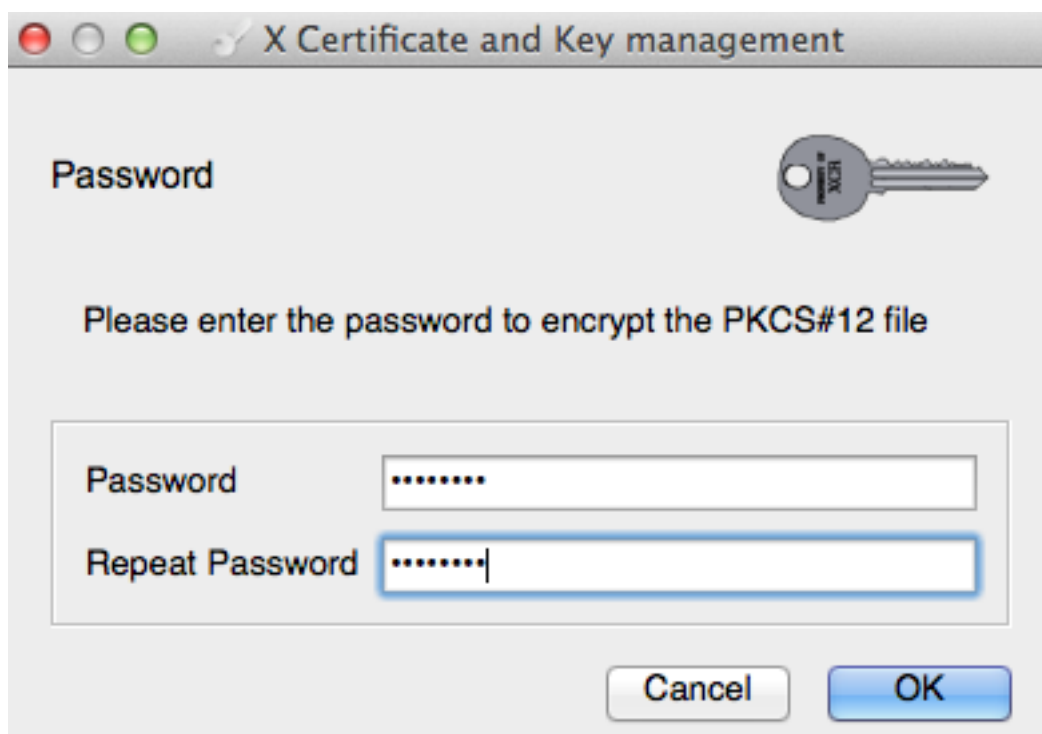


4. Su certificado creado recientemente ahora aparece en el teclado de cuadro del certificado el certificado para resaltar lo y la **exportación del** teclado. Seleccione el nombre de fichero, la ubicación a los cuales el certificado debe ser guardado, y el formato de la exportación.

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



Nota: 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

lenguetas 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

Ahora que se crea el certificado, usted debe importarlo sobre su ESA. Complete estos pasos para importar el certificado:

1. Navegue al **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) [password field]

3 → [Next >]

[Cancel] [Next >]

3. Revise el certificado y el tecleo **somete** para confiar sus cambios:

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.

Cancel 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. Navegue para enviar la clave pública de las directivas > 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 Notepad++ o 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 **some**te:

Add S/MIME Public Key

Add Public Key	
Name:	royale298_1_public_key
S/MIME Public Key:	<pre>-----BEGIN CERTIFICATE----- MIIEAICCAsuqAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmIEMAKGA1UEBhMCVVMx FzAVBgNVBAGTDk5xcnRoIENhcj9saW5hMQwwCgYDVQQHEwNSVFAxOjAMBgNVBAoT BUUNoc2NwMQwwCgYDVQQLEwNUQUUMxIzAhBgNVBAMMGnJveWVsZTI1OEF8xLmNhbg8u Y2IzY28uY29tSEwHwYJKoZIhvcNAQkBFhJyb2JzaGVyY290BjA1UEBhMCVVMx MTQxMTI0MTU0MTAwW5hMQwwCgYDVQQHEwNSVFAxOjAMBgNVBAoTBUUNoc2Nw c2NwMQwwCgYDVQQLEwNUQUUMxIzAhBgNVBAMMGnJveWVsZTI1OEF8xLmNhbg8u Y2IzY28uY29tSEwHwYJKoZIhvcNAQkBFhJyb2JzaGVyY290BjA1UEBhMCVVMx CSsGSIb3DQEBAQUAA4IBDwAwgEKAAIBAQDgEMocaf8ezvRT/CmBYMIQ12qEWTd ISA+LxwEgkDdmY+jMiRm1+nIBDDF1V9nw8PhD0Xs7UhhK8r0m2qNcWdjaLY36Mh4d JjHTHNe/BCwxFXZVqCk9VfxrT50piRExtaAfcZlvrXgk2YUkDZKE6huo4ZqY0Ib yTghWwMAF3oAaXRR+MTwQXj8fyafy6Gee5QioRtRwY+2+IKAtWjYuu09Blef2E 4MibfenRUIRkm5cU2Z7ZrtUJIWe7JHuZCqDIvDjEdoMUcUSqZASxG6a55vdAFP4mG QCI9zmUc02nCcIaRd1cWhtv5x7pwi7wIvvrdej2dfxLJNrCGne/CDfKNAgMBAAGj -----</pre>

Cancel Submit

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

ESA.

Información Relacionada

- [AsyncOS 9.0 para el guía del usuario del correo electrónico](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)