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

Contenido

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

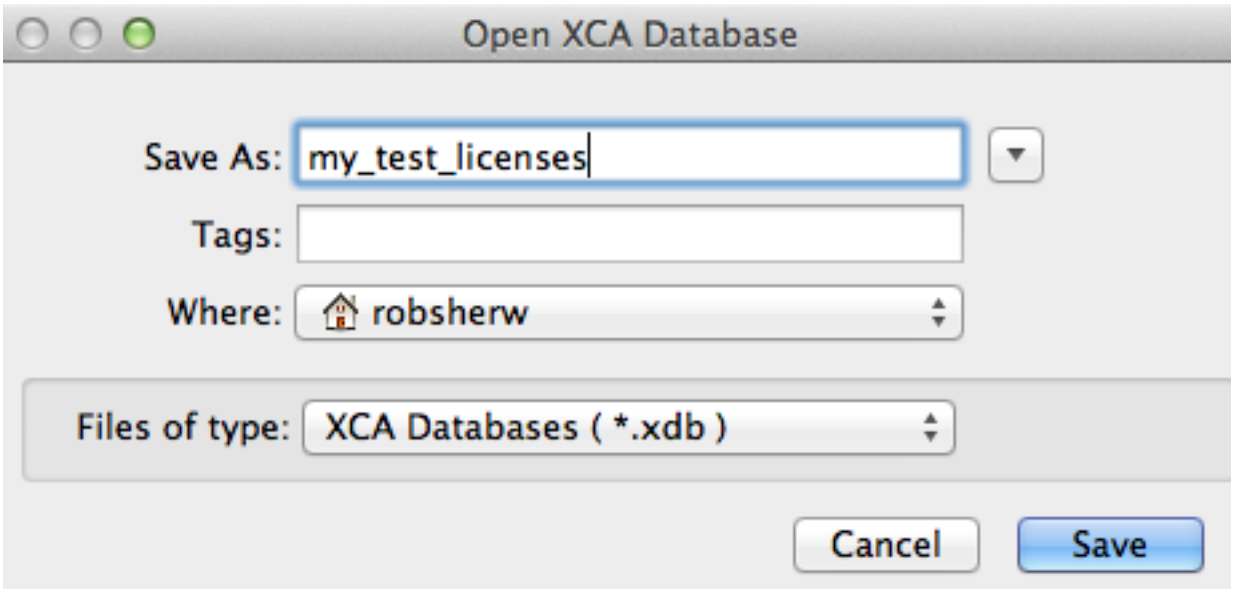
- Sistemas de Microsoft Windows: Softpedia

Cree un certificado

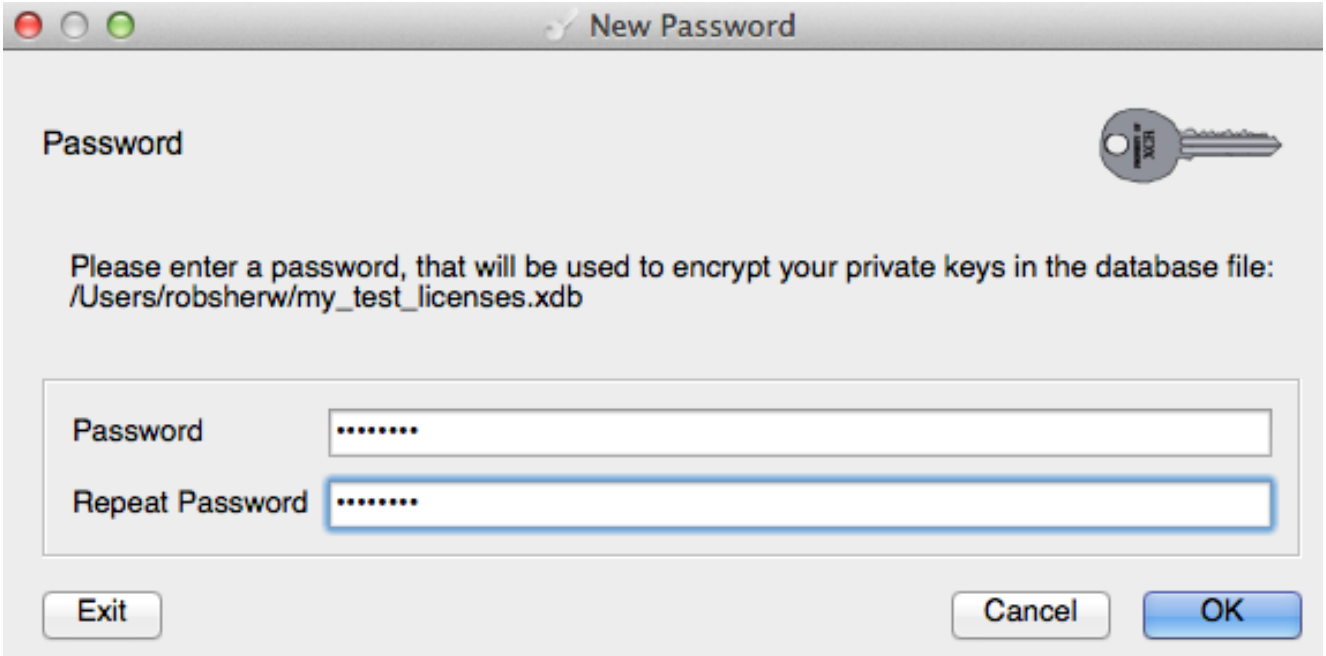
Complete estos pasos para crear un certificado S/MIME:

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 clasifiar > nueva base de datos > nombre <DB de su choice>**:



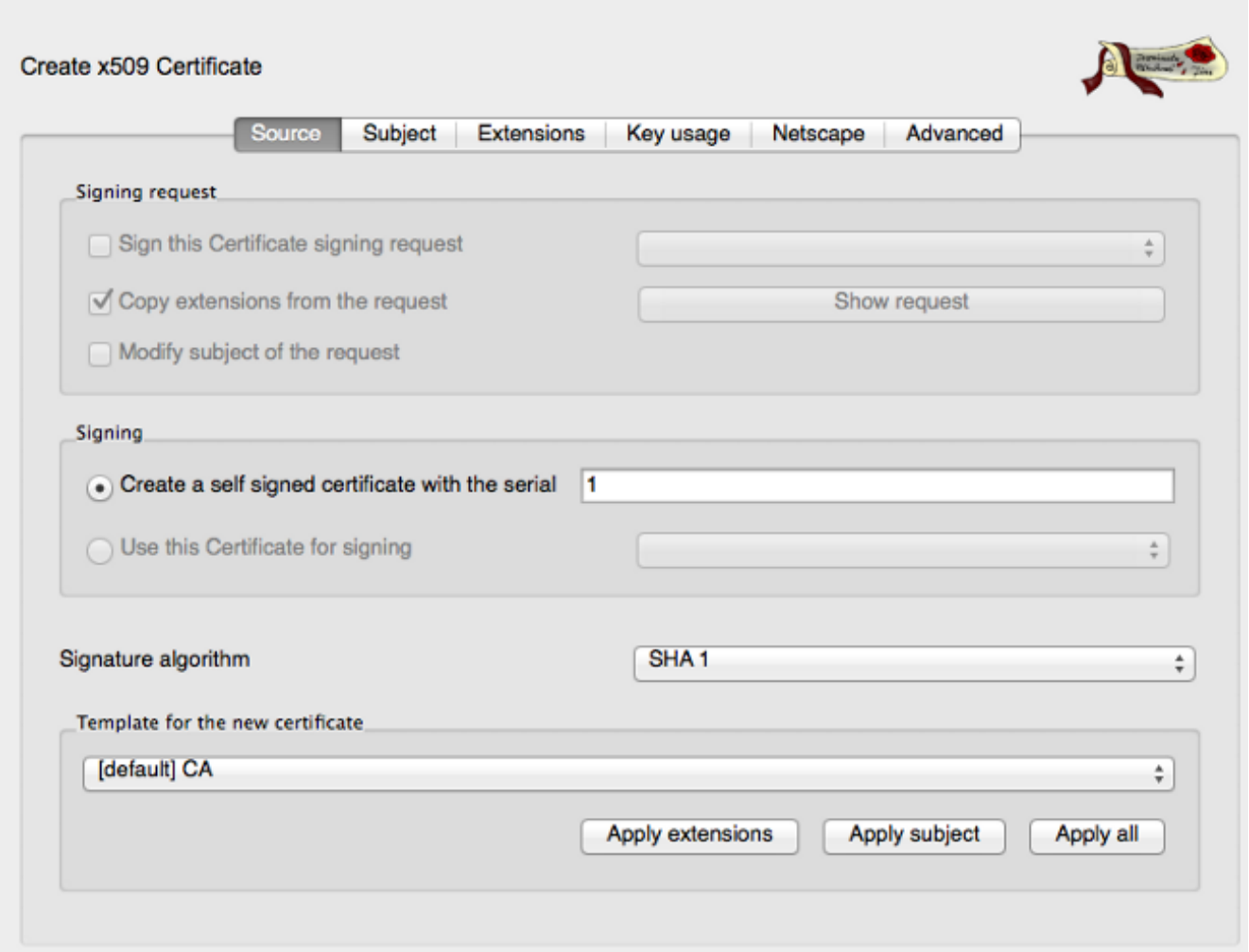
   Haga clic en Save (Guardar). Ahora usted debe ingresar una contraseña para el cifrado de sus claves privadas que se asocien a esta base de datos. Esta contraseña está solamente para la base de datos XCA.



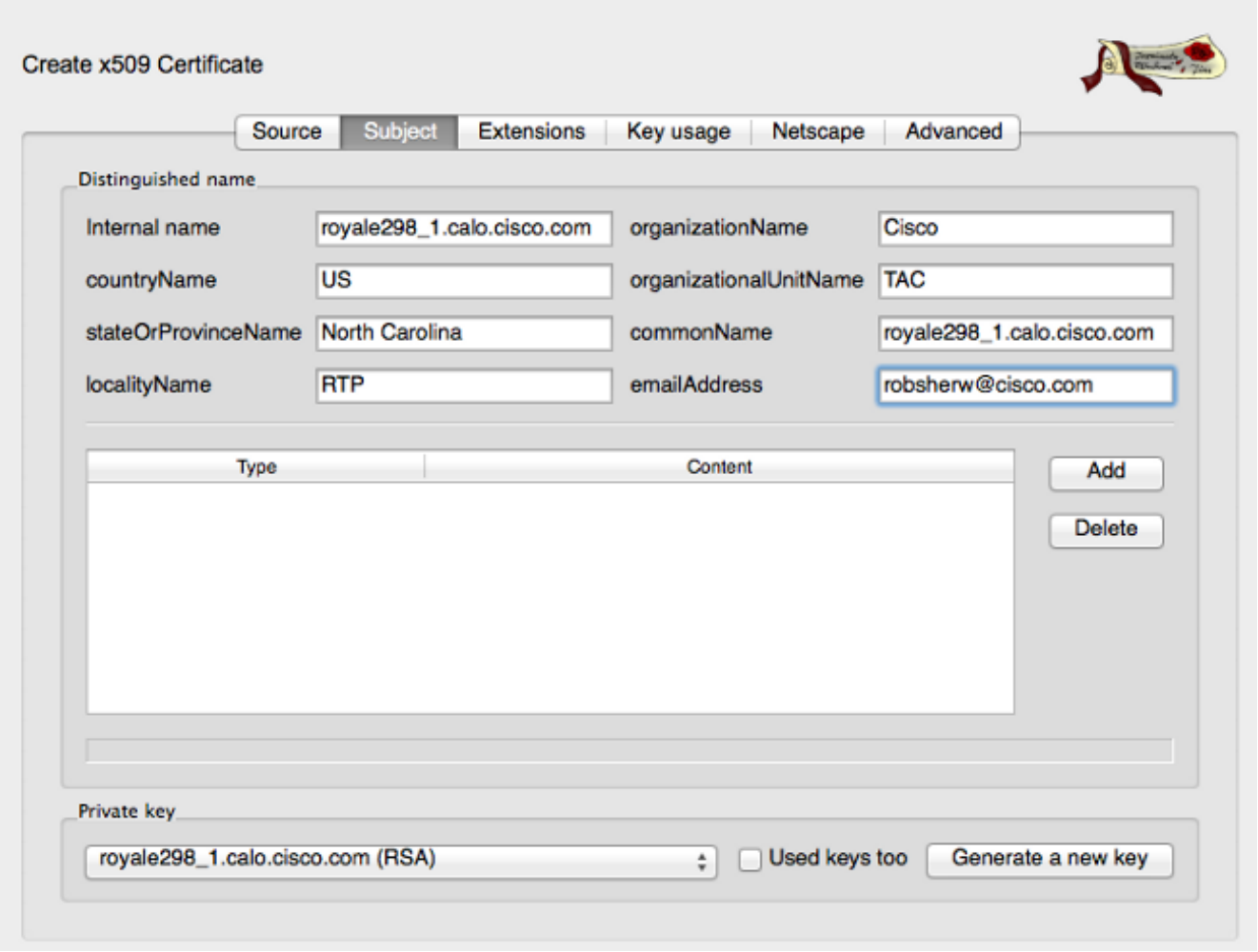
Haga Click en OK para acabar la creación de la base de datos.

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

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

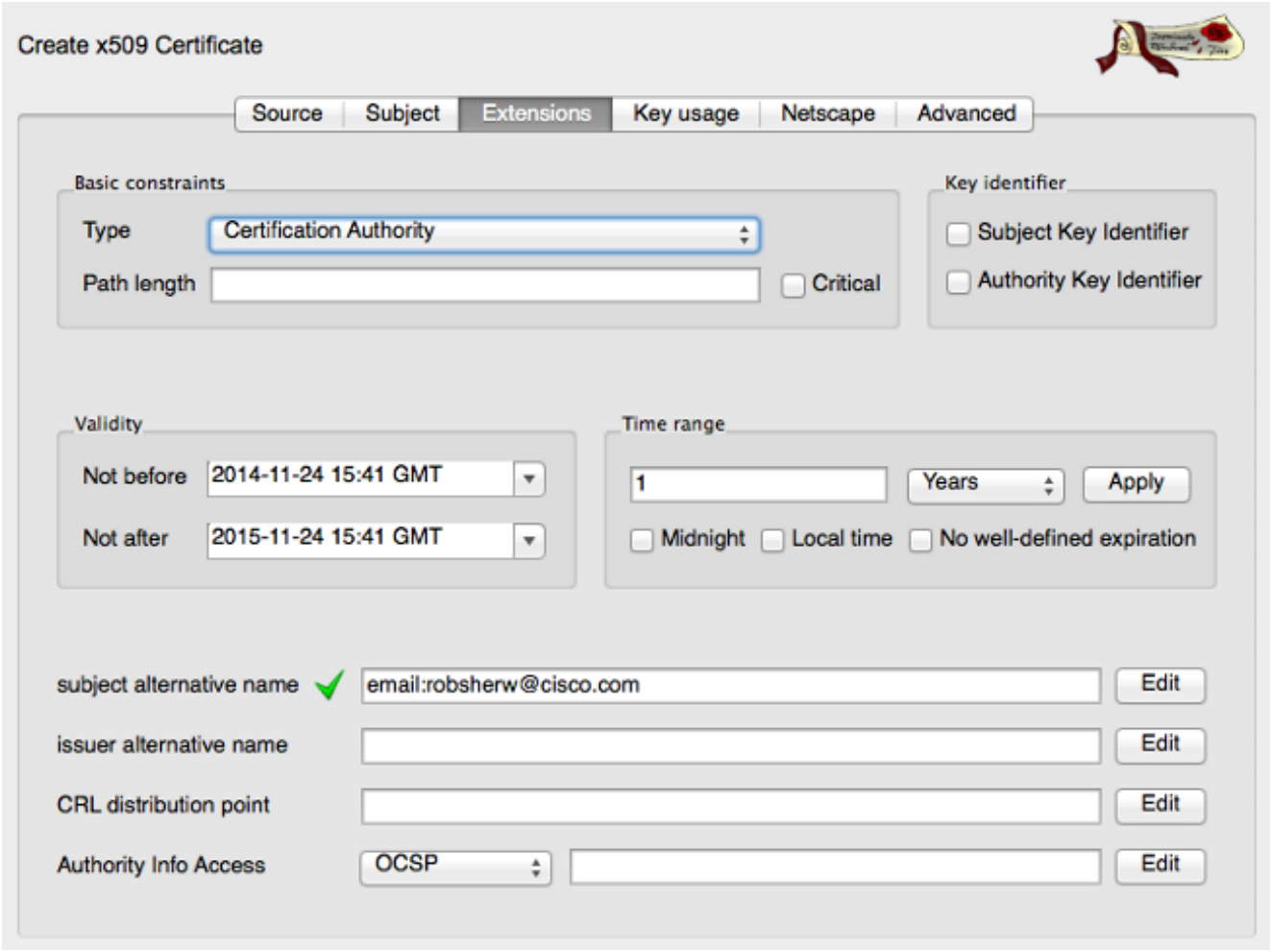


   De la lengueta sujeta, ingrese la Información requerida en la sección del nombre distintivo. En la sección de la clave privada, el tecleo **genera una nueva clave** y elige **2048 el bit** o el **bit 1024** para el keysize. Haga clic **crean** para generar la clave privada y asociarla a este certificado.

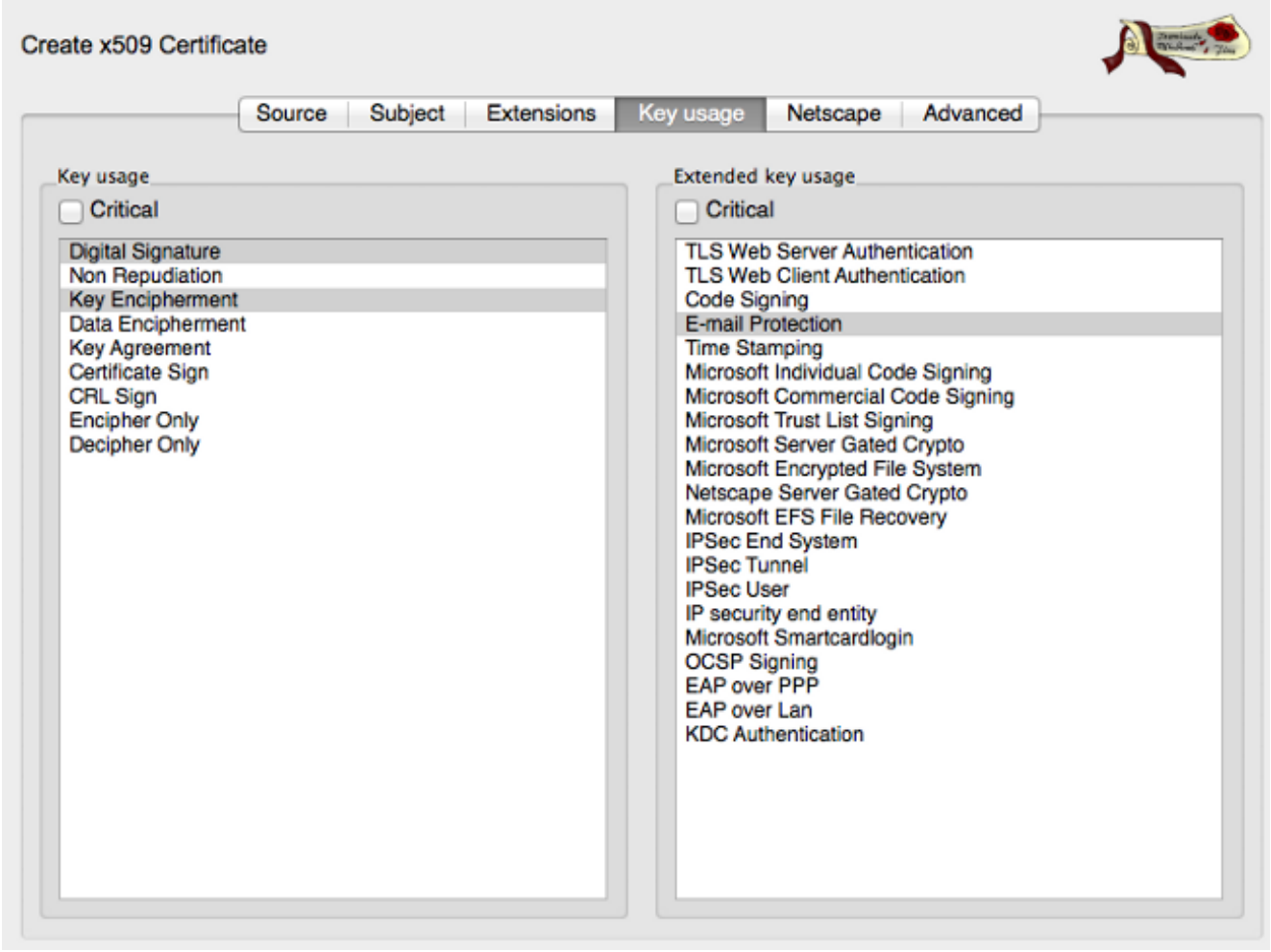


De la lengueta de las Extensiones, en la sección básica de los apremios, seleccione el **Certificate Authority** para el tipo.

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:



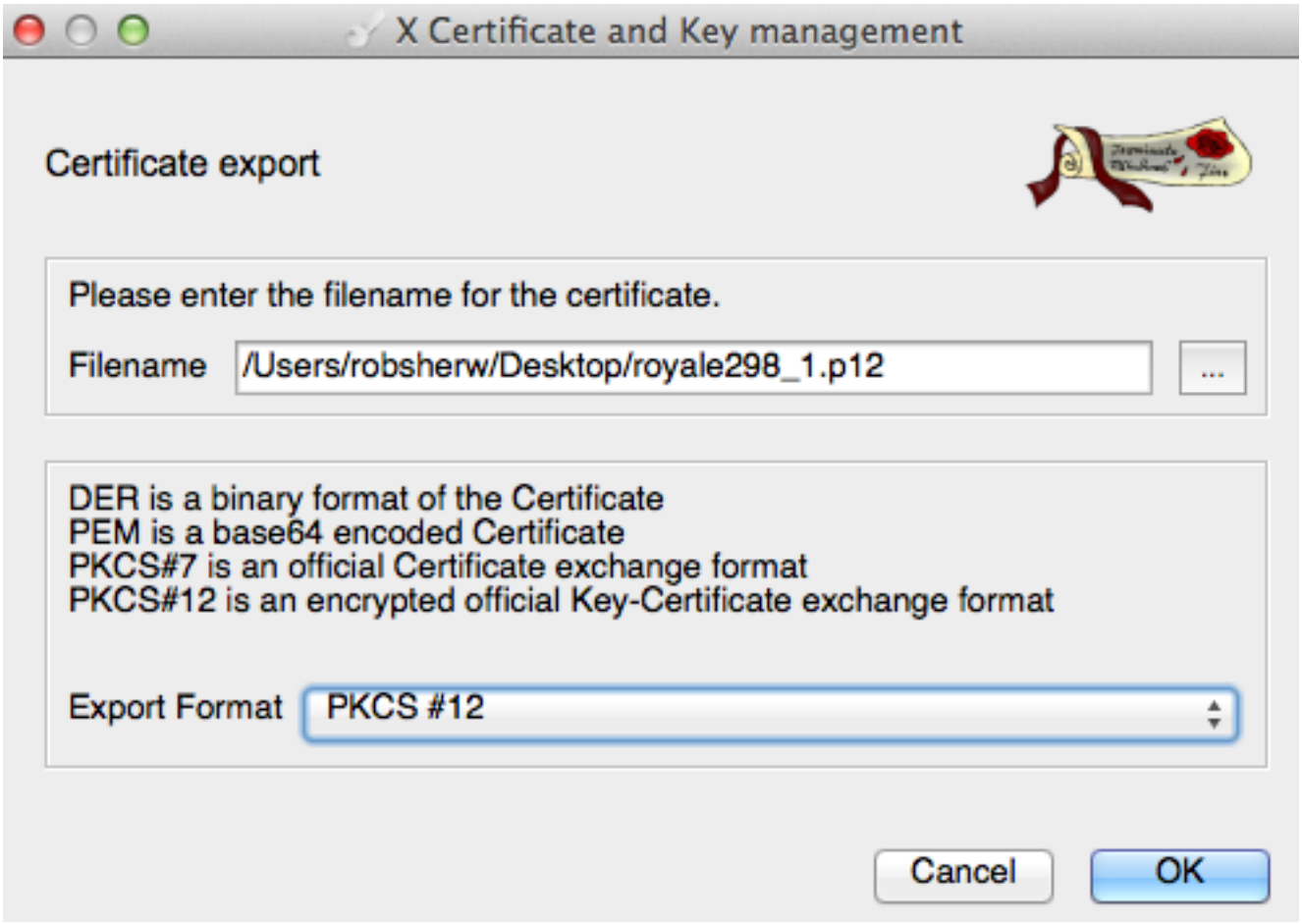
De la lengueta dominante del uso, en la sección dominante del uso, resalte la **firma digital** y la **estenografía de la clave**. En la sección dominante extendida del uso, resalte la **protección del email**. Éstos son los elementos requeridos para S/MIME:



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 tecleo de cuadro del certificado el certificado para resaltar lo y la **exportación del** tecleo. Seleccione el nombre de fichero, la ubicación a los cuales el certificado debe ser guardado, y el formato de la exportación.

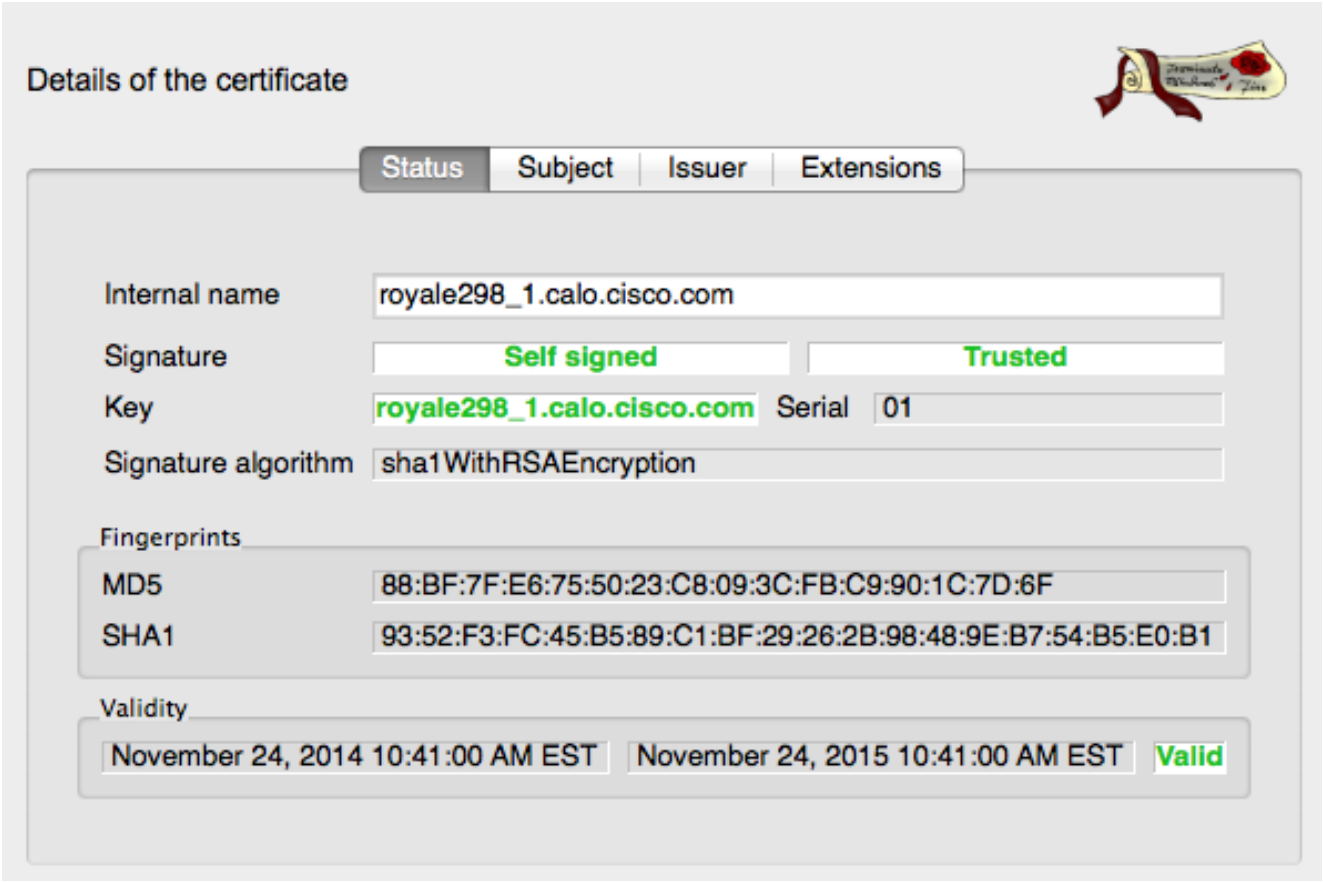
   Nota: Usted debe exportar su certificado en ambo PKCS12 y Certificados formatados Privacy Enhanced Mail (PEM). El certificado del PKCS12 guarda como nombre del archivo formatado **.p12**. El certificado PEM guarda como nombre del archivo formatado **.crt**.



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:

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:



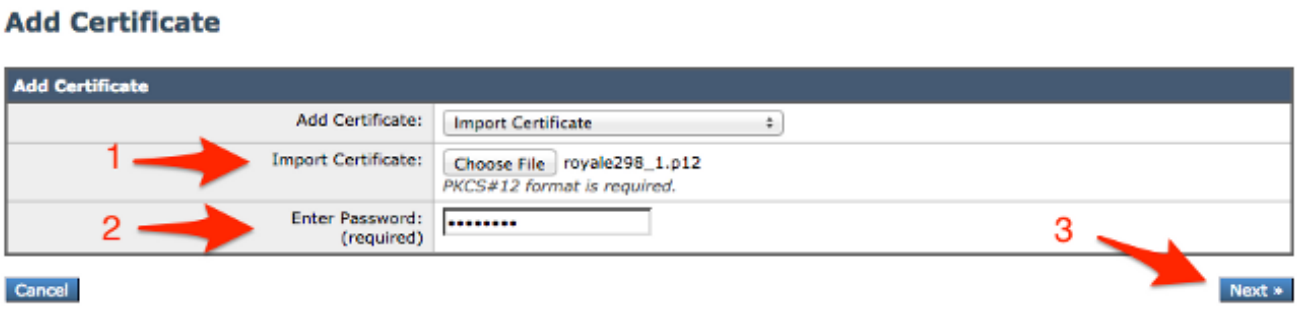
En este momento su certificado está listo para ser utilizado en su ESA.

Importe un certificado

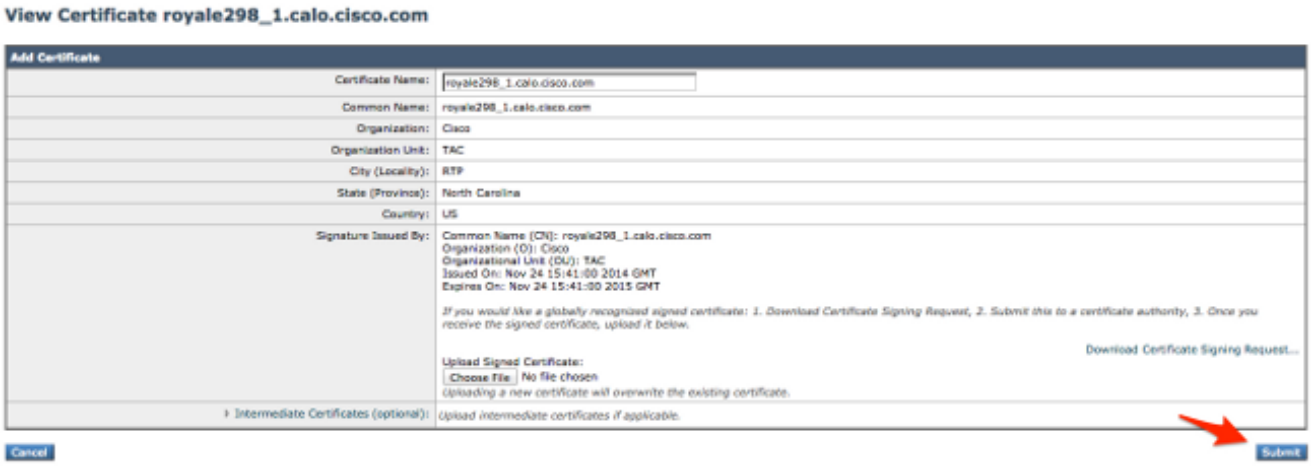
Ahora que se crea el certificado, usted debe importarlo sobre su ESA. Complete estos pasos para importar el certificado:

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**:



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



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 **-----COMIENCE EL CERTIFICADO-----** por **-----CERTIFICADO DEL EXTREMO-----**.

5. Pegue este contenido en la sección de la clave pública S/MIME y el tecleo **somete**:

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