

# Criação do certificado ESA para o uso com assinatura S/MIME

## Índice

[Introdução](#)

[Informações de Apoio](#)

[Crie o certificado S/MIME do ESA](#)

[Crie o certificado S/MIME do aplicativo de terceiros](#)

[Crie um certificado](#)

[Importe um certificado ao ESA](#)

[Associe um certificado PEM](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve como criar Certificados para propósitos testando com o seguro/Multipurpose Internet Mail Extension (S/MIME) que assina na ferramenta de segurança do email de Cisco (ESA).

## Informações de Apoio

Quando você cria um certificado S/MIME para a mensagem que assina, deve cumprir as exigências descritas no [RFC 5750](#): Fixe/versão 3.2 dos Multipurpose Internet Mail Extension (S/MIME) - Certificate a manipulação.

## Crie o certificado S/MIME do ESA

Os certificados auto-assinados S/MIME podem ser criados do ESA GUI:

1. Escolha **certificado do > Add da rede > dos Certificados...**
2. O da lista de drop-down, escolha **criam o certificado Auto-assinado S/MIME**
3. Preencha a informação apropriada como pedido.
4. Clique em Next.
5. O clique **submete-se** a fim salvar a criação do certificado.
6. O clique **compromete mudanças** a fim salvar mudanças à configuração.

A fim usar o certificado e configurar chaves públicas S/MIME, você precisa de ter salvar uma cópia do certificado no formato do .pem:

1. Escolha a **rede > os Certificados**
2. Clique o hiperlink para o certificado que você apenas criou.
3. Clique a **solicitação de assinatura de certificado da transferência...**

Isto salvar o arquivo como *cert.pem localmente* a seu computador. Salvar isto para o uso mais tarde seção “associado no certificado PEM” deste artigo.

## Crie o certificado S/MIME do aplicativo de terceiros

Certificados o teste (ou permanent) podem ser criados externamente do ESA também. Para este exemplo, o certificado X e o gerenciamento chave (XCA) são um aplicativo que controle chaves assimétricas, tais como Rivest-Shamir-Addleman (RSA) ou o Digital Signature Algorithm (DSA), e são pretendidos ser um Certificate Authority (CA) pequeno para a criação e a assinatura dos Certificados. Usa a biblioteca aberta do secure sockets layer (OpenSSL) para as operações criptográficas.

**Note:** O XCA é um aplicativo de terceiros que não seja apoiado por Cisco. O uso deste aplicativo é fornecido somente para a ilustração e a facilidade da administração para a administração, testes, e configuração S/MIME. Para detalhes completos e instruções no XCA, refira o [XCA - certificado X](#) e documento do [gerenciamento chave](#).

Você pode transferir o aplicativo XCA em qualquer um destes lugar:

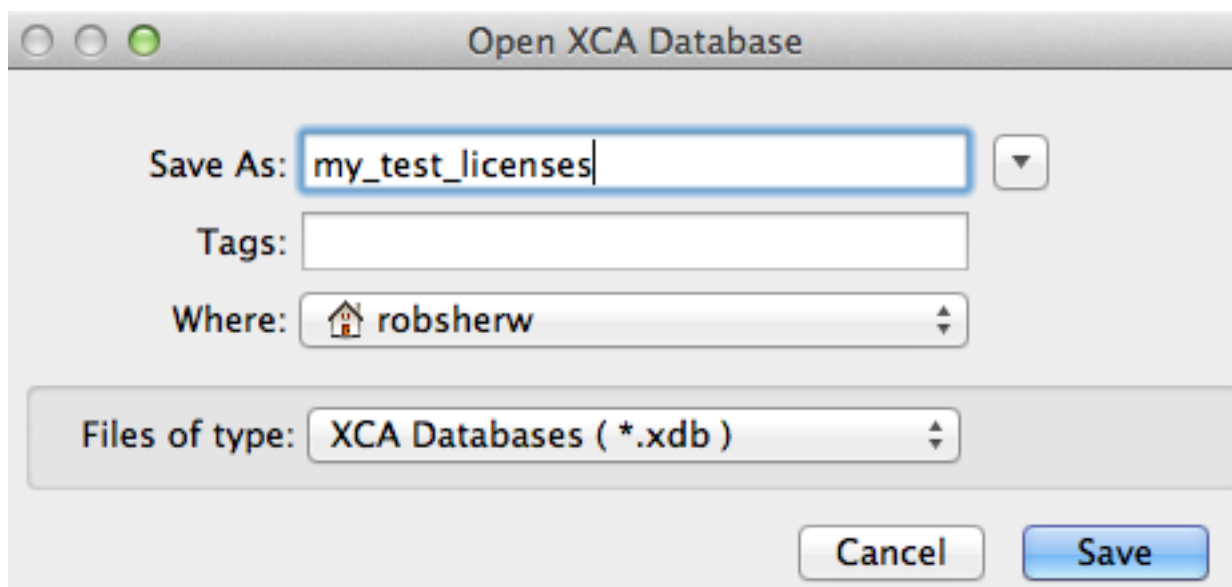
- Sistemas operacionais de Macintosh (OSX): [Sourceforge](#)
- Sistemas de Microsoft Windows: [Sourceforge](#)

### Crie um certificado

Termine estas etapas a fim criar um certificado S/MIME:

1. Use o aplicativo XCA a fim criar um base de dados novo XCA ou abrir um base de dados atual XCA, se um já existe.

Da barra de menus, escolha o **arquivo > base de dados novo > nome <DB de seu choice>**:



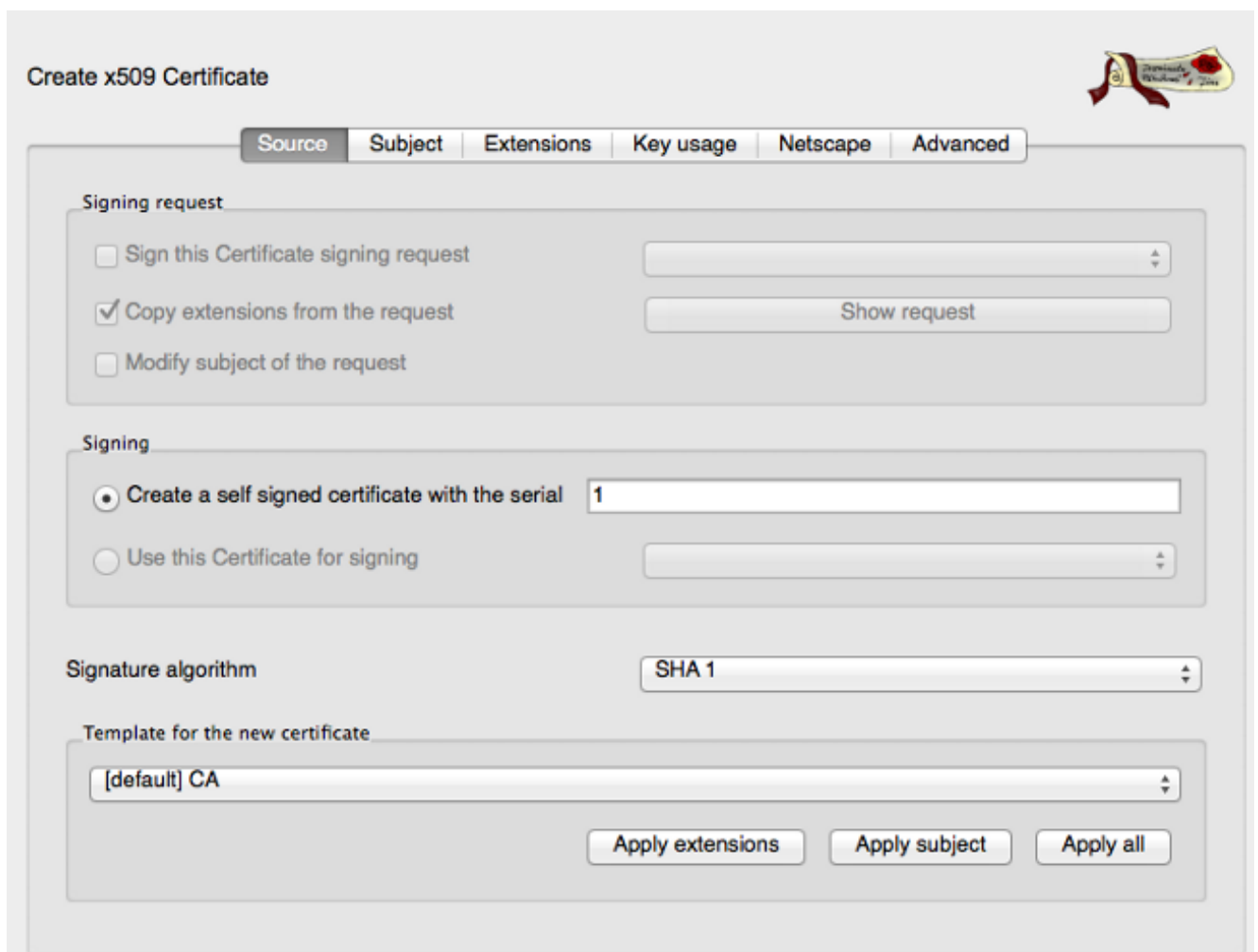
Click **Save**. Agora você deve incorporar uma senha para a criptografia de suas chaves privadas que são associadas a este base de dados. Esta senha é somente para o base de dados XCA.



**APROVAÇÃO** do clique a fim terminar a criação de base de dados.

2. Dos Certificados catalogue, escolha o **certificado novo** e a tela do *certificado da criação x509* aparece.

Nenhuma mudança é exigida da aba da fonte, porque os valores padrão podem ser usados:



Da aba sujeita, incorpore a informação requerida na seção do nome destacado. Na seção da chave privada, o clique **gerencie uma chave nova** e escolha **2048 o bit** ou o **bit 1024** para o keysize. Clique **criam** a fim gerar a chave privada e associá-la com este certificado.

The screenshot shows the 'Create x509 Certificate' interface with the 'Subject' tab selected. The 'Distinguished name' section contains the following fields:

|                     |                            |                        |                            |
|---------------------|----------------------------|------------------------|----------------------------|
| 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         |

Below these fields is a table for extensions with columns 'Type' and 'Content', and 'Add' and 'Delete' buttons. The 'Private key' section shows a dropdown menu with 'royale298\_1.calo.cisco.com (RSA)', a checkbox for 'Used keys too', and a 'Generate a new key' button.

Da aba dos Ramais, na seção básica das limitações, escolha o **Certificate Authority** para o tipo.

**Note:** As solicitações de assinatura de certificado subsequentes (CSR) podem ser assinadas através deste CA com o tipo grupo ao **não definido**.

Na seção da validade, entre os detalhes conforme suas exigências (365 dias à revelia). Você pode escolher adicionar um nome alternativo sujeito (SAN) para o Domain Name System (DNS), o endereço email, e o similar com o uso do **botão Edit** para essa linha. Da janela pop-up SAN, o clique **adiciona** e escolhe o tipo SAN e o índice associado. Uma vez que terminado, o clique **aplica-se** a fim aplicar estas mudanças e para retornar aos Ramais catalogue o indicador:

## 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

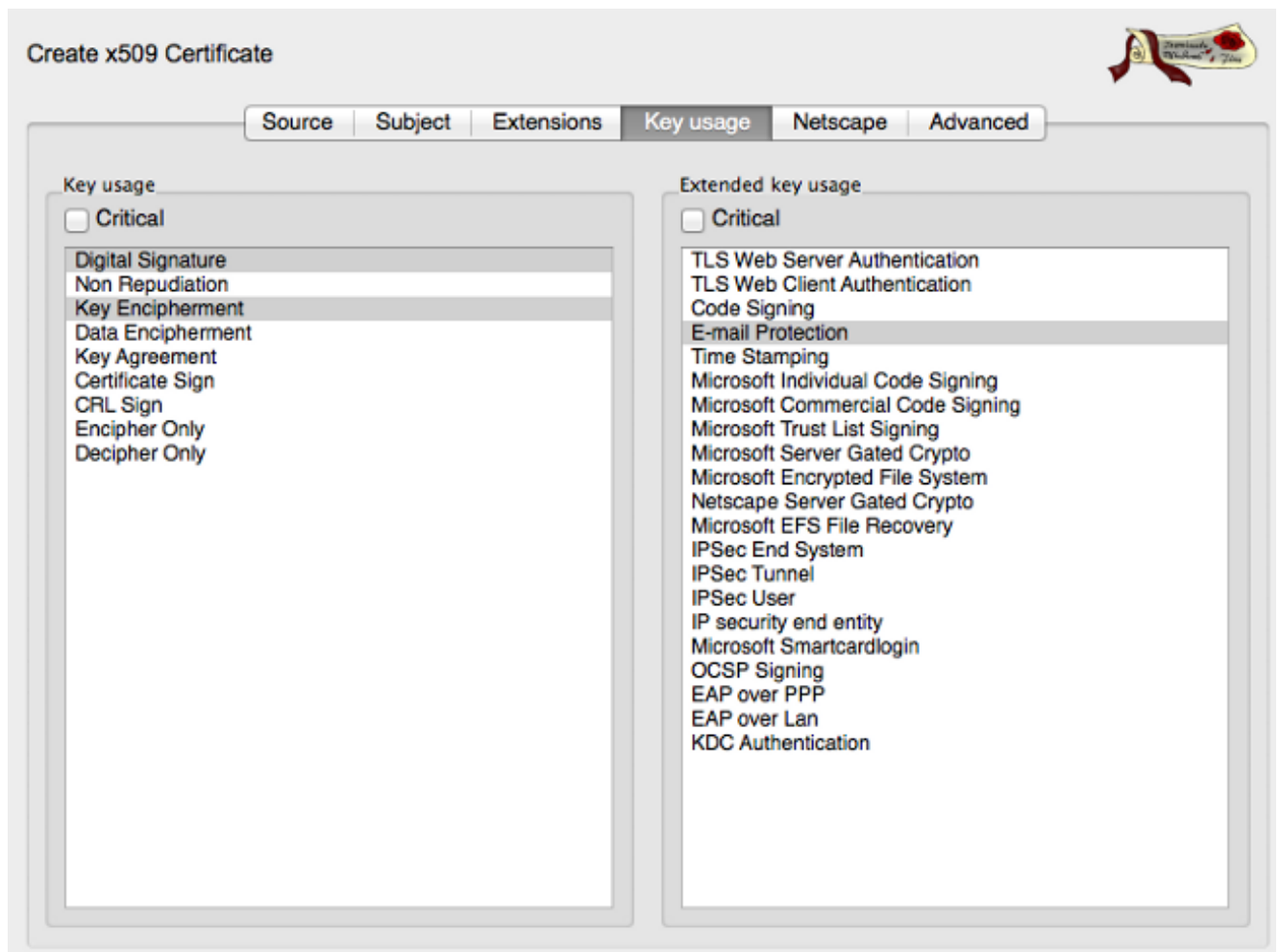
subject alternative name

issuer alternative name

CRL distribution point

Authority Info Access

Da aba chave do uso, na seção chave do uso, destaque a **assinatura digital** e a **cifragem da chave**. Na seção chave prolongada do uso, destaque a **proteção do email**. Estes são os elementos exigidos para S/MIME:

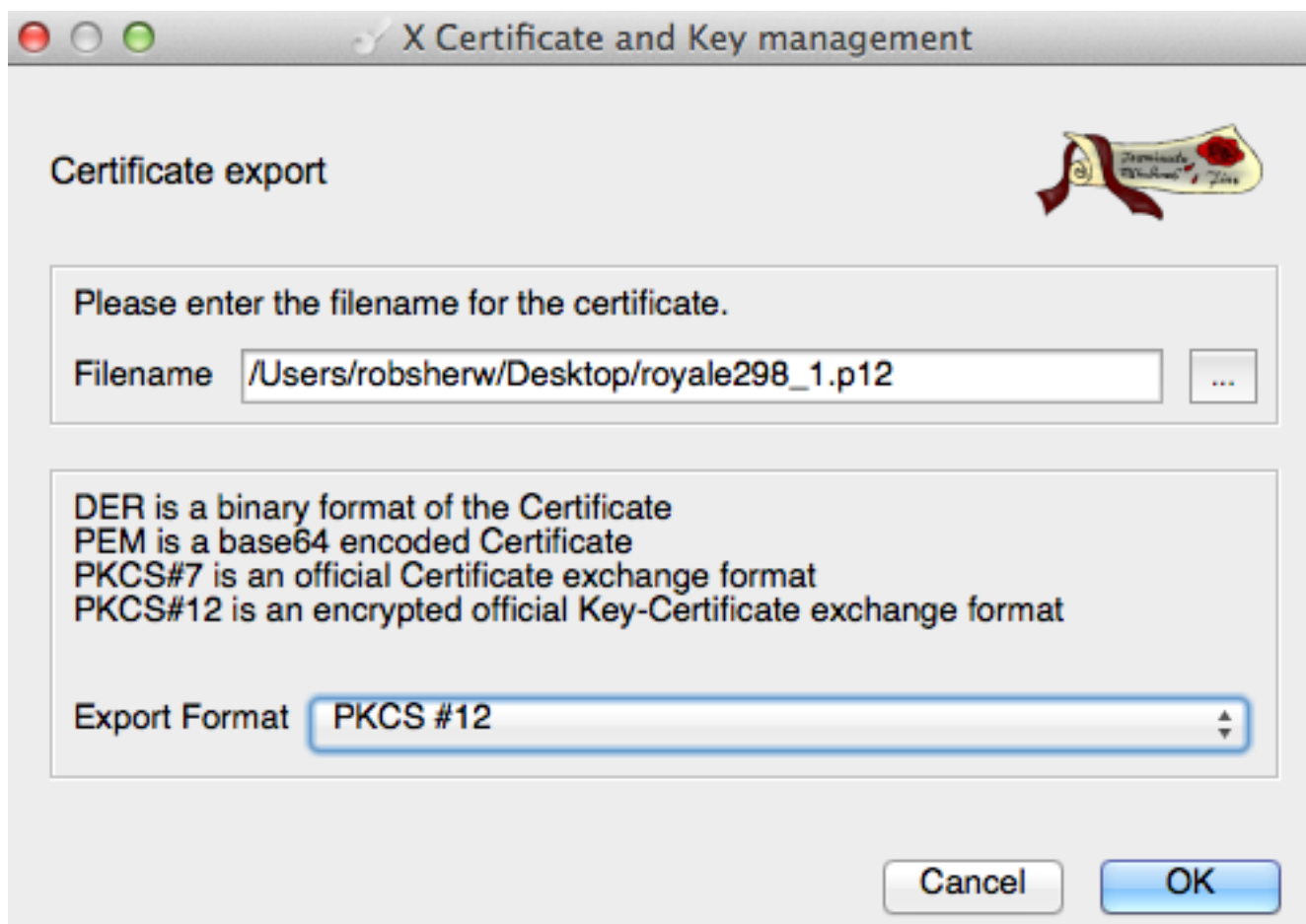


3. A **APROVAÇÃO** do clique na parte inferior da tela e de uma notificação do PNF-acima aparece:

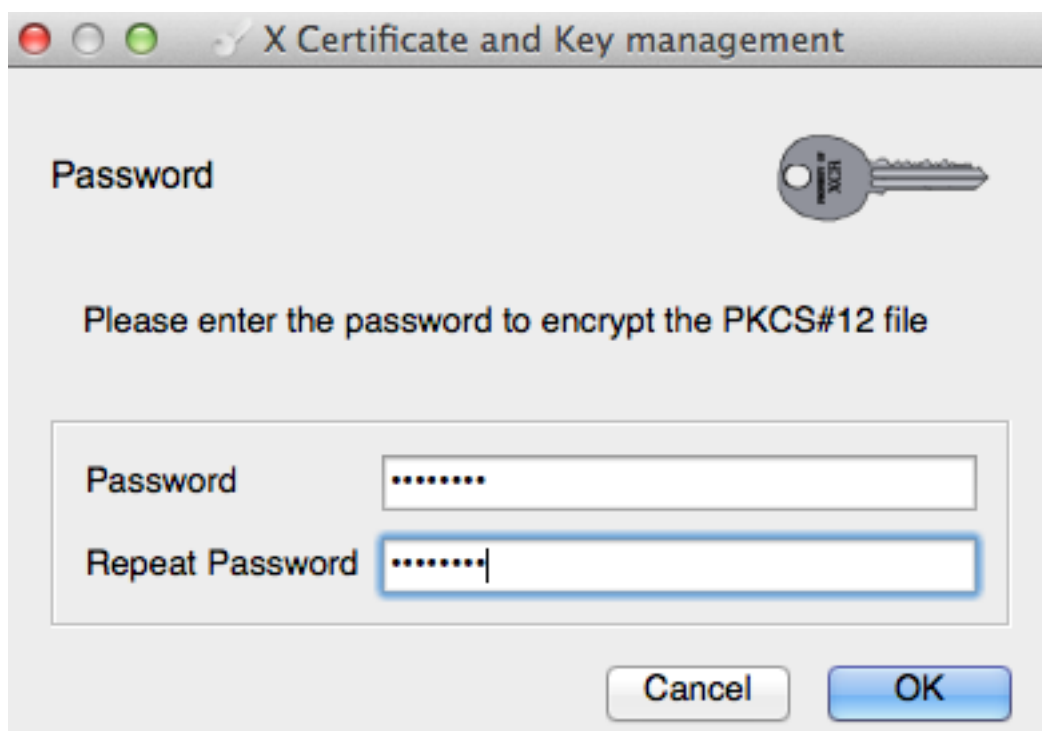


4. Seu certificado recém-criado aparece agora na aba do certificado. Clique o certificado a fim destacar o e a **exportação** do clique. Selecione o nome de arquivo, o lugar a que o certificado deve ser salvar, e o formato da exportação.

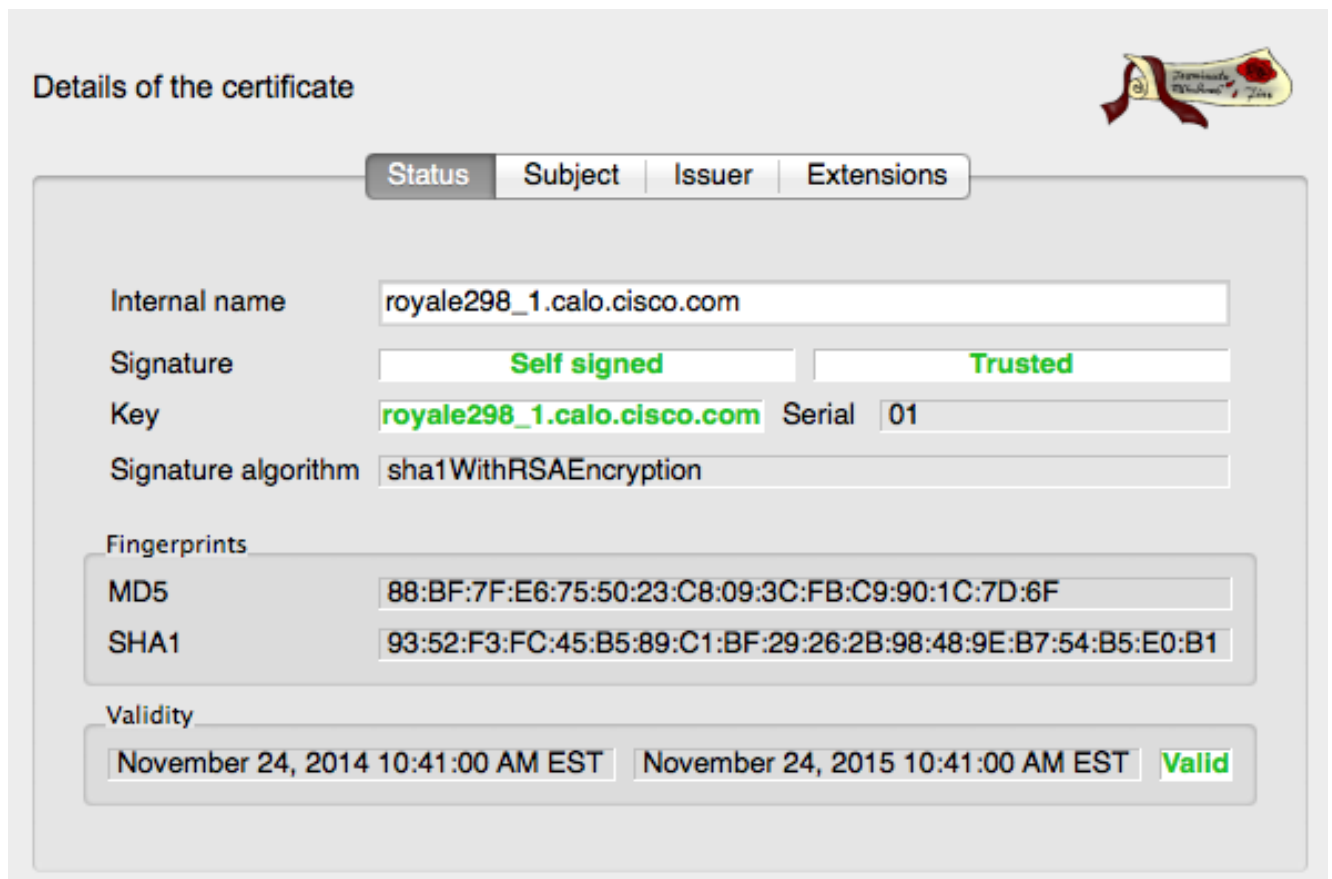
**Note:** Você deve exportar seu certificado em ambo o PKCS12 e Certificados formatados do Privacy Enhanced Mail (PEM). O certificado do PKCS12 salvar como um nome de arquivo formatado **.p12**. O certificado PEM salvar como um nome de arquivo formatado **.crt**.



A **APROVAÇÃO** e você do clique são apresentado com a senha da criptografia para o certificado do PKCS12, que é precisado quando você importa o certificado no ESA:



**Note:** Quando você exporta o certificado PEM-formatado, você não está alertado para uma senha, porque não é precisada. A fim ver os detalhes do certificado, clique **Certificados** e movimento através das abas do estado, do assunto, do expedidor, e dos Ramais:



Neste momento seu certificado está pronto para ser usado em seu ESA.

## Importe um certificado ao ESA

Se você criou um certificado externamente do ESA você deve importá-lo em seu ESA. Termine estas etapas a fim importar o certificado:

1. Escolha **certificado do > Add da rede > dos Certificados... > certificado de importação.**
2. Escolha o arquivo formatado do PKCS12 (.p12) que você criou na seção anterior, incorporam a senha que é associada a esse certificado, e clicam-na **em seguida:**

### Add Certificate

3. Reveja o certificado e o clique **submete-se** a fim comprometer suas mudanças:



## 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<br>Organization (O): Cisco<br>Organizational Unit (OU): TAC<br>Issued On: Nov 24 15:41:00 2014 GMT<br>Expires On: Nov 24 15:41:00 2015 GMT<br><br><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> |
|                                       | <a href="#">Download Certificate Signing Request...</a>  |
| Upload Signed Certificate:            | <input type="button" value="Choose File"/> No file chosen<br><small>Uploading a new certificate will overwrite the existing certificate.</small>   |
| Intermediate Certificates (optional): | <input type="checkbox"/> Upload intermediate certificates if applicable.   |

Neste momento seu certificado está agora pronto para ser usado para S/MIME em seu ESA.

## Associe um certificado PEM

Você deve agora adicionar seu certificado PEM-formatado às chaves públicas S/MIME. Termine estas etapas a fim adicionar o certificado PEM-formatado:

1. Escolha a chave pública do > Add das políticas do correio > das chaves públicas S/MIME....
2. Dê entrada com o nome, como necessário.
3. Abra o certificado formatado PEM (.crt) em um editor de texto apropriado (tal como o [Windows/PC] Notepad++ ou o [OSX] do átomo).
4. Copie o índice de -----COMECE O CERTIFICADO----- através -----CERTIFICADO DA EXTREMIDADE-----.
5. Cole este índice na seção da chave pública S/MIME e o clique **submete-se**:

### Add S/MIME Public Key

| Add Public Key     |   |
|--------------------|---|
| Name:              | royale298_1 public key  |
| S/MIME Public Key: | <pre>-----BEGIN CERTIFICATE----- MIIEAICCAsAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmIEMAKGALUEBhMCVVMx FzAVBgNVBAgTDk5xcnRoIENhcm9saW5hMQwwCgYDVQQHEwNSVFAxDMBAgNVBAoT BUlNpY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2Nv Y2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2Nv Y2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2Nv MTQxMTI0MTU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0MTU0 BgNVBAgTDk5xcnRoIENhcm9saW5hMQwwCgYDVQQHEwNSVFAxDMBAgNVBAoT BUlNpY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2Nv Y2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2Nv Y2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2NvY2Nv CSaGSIB3DQEBAQAIAAIBDWAwqEKAAoIBAQAQEMocaf8ezvRTICmBYMIQ12aEWTd ISA+LxxEgkDdmY+jMIRm1+nIBDDF1V9nw8PhD0Xs7UhhK8r0m2aNCWdjaLY36Mh4d JJHTHNe/BCwxFXZVaCk9Vfxt5DpiRExtaAfcZlvrXgkJ2YUkDZKE6huo4ZqY0Ib yTghWwMAF3oAaXRR+MTwQXJ38fvafv6Gee5QioRtRwY+2+IKAtWjYuuo9Blef2E 4MibfenRlIRkm5cU2ZZrtUjWeZjHuZCgDIvDJEdoMUcUsaZA5xG6a55yAfp4mG QCI9zmUc02nCcIaDd1cWthr5x7owi7wlvvrdej2dfvLjNtCGne/CDfKNAGMBAAGj -----</pre> |

6. Comprometa todas as mudanças. Sua chave pública S/MIME é ajustada neste momento agora para seu ESA.

## Informações Relacionadas

- [Cisco envia por correio eletrônico guias do utilizador final da ferramenta de segurança](#)
- [Cisco envia por correio eletrônico Release Note e informação geral da ferramenta de](#)

segurança

- Suporte Técnico e Documentação - Cisco Systems