

ESA证书创建为了用在S/MIME签字上

目录

[简介](#)

[背景信息](#)

[创建从ESA的S/MIME证书](#)

[创建从第三方应用的S/MIME证书](#)

[创建证书](#)

[导入证书对ESA](#)

[关联PEM证书](#)

[相关信息](#)

简介

为了便于测试本文描述如何创建证书与(S/MIME)签字在思科电子邮件安全工具(ESA)的安全/多媒体Internet邮件扩展。

背景信息

当您创建消息的一S/MIME证书签字时，必须符合在[RFC 5750](#)描述的要求：巩固/多媒体Internet邮件扩展(S/MIME)版本3.2 -证书处理。

创建从ESA的S/MIME证书

S/MIME自签名证书可以从ESA GUI创建：

1. 选择**网络>证书>Add证书...**
2. 从下拉列表，请选择**创建自己签署的S/MIME证书**
3. 填写相应的信息作为请求的。
4. 单击 **Next**。
5. 单击**提交**为了保存证书创建。
6. 单击**进行更改**为了保存对配置的更改。

为了使用证书和配置S/MIME公共密钥，您需要安排保存证书的复制在.pem格式的：

1. 选择**网络>证书**
2. 单击您创建的证书的超链接。
3. 单击**下载证书签名请求...**

这保存文件作为 *cert.pem*本地到您的计算机。 保存此为使用后在此条款的“关联PEM证书”部分。

创建从第三方应用的S/MIME证书

测试(或永久性)证书可以从ESA创建外部。对于此示例，X证书和密钥管理(XCA)是管理不对称密钥，例如Rivest沙米尔Addleman的应用程序(RSA)或数字签名算法(DSA)和打算是创建和签署的一小

Certificate Authority (CA)证书。它使用开放安全套接字协议层(Openssl)库密码操作。

Note:XCA是思科不支持的第三方应用。使用此应用程序仅提供管理为说明和方便S/MIME管理、测试和配置的。关于全面的详细信息和说明关于XCA，参考[XCA - X证书和密钥管理](#)文档。

您能下载XCA应用程序在这些位置之一：

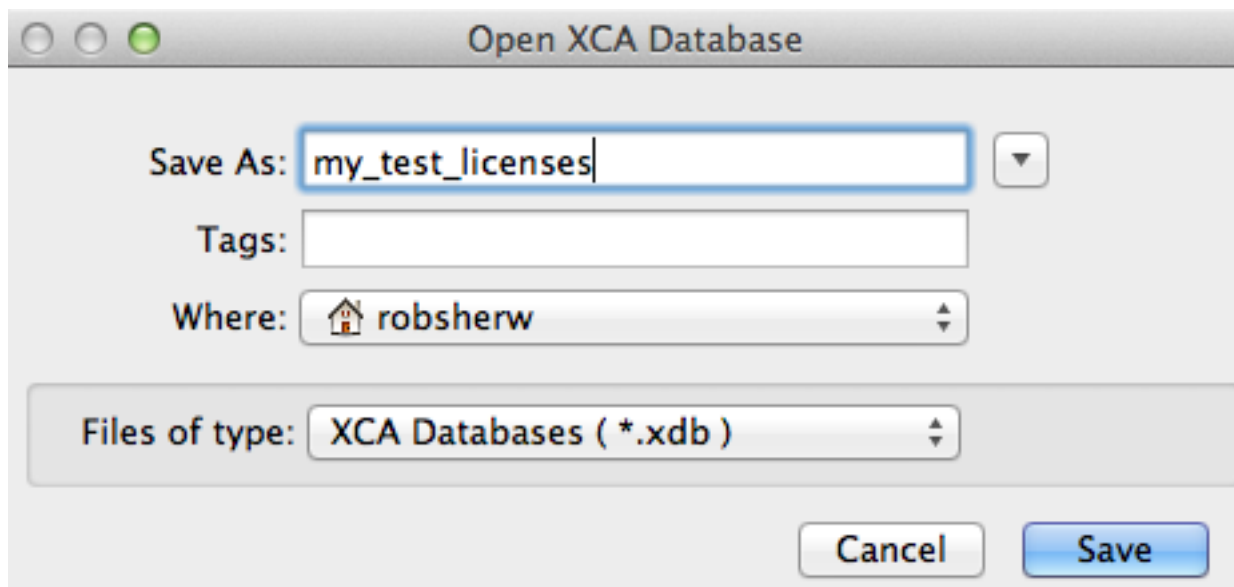
- 麦金塔操作系统(OSX)：[Sourceforge](#)
- Microsoft Windows系统：[Sourceforge](#)

创建证书

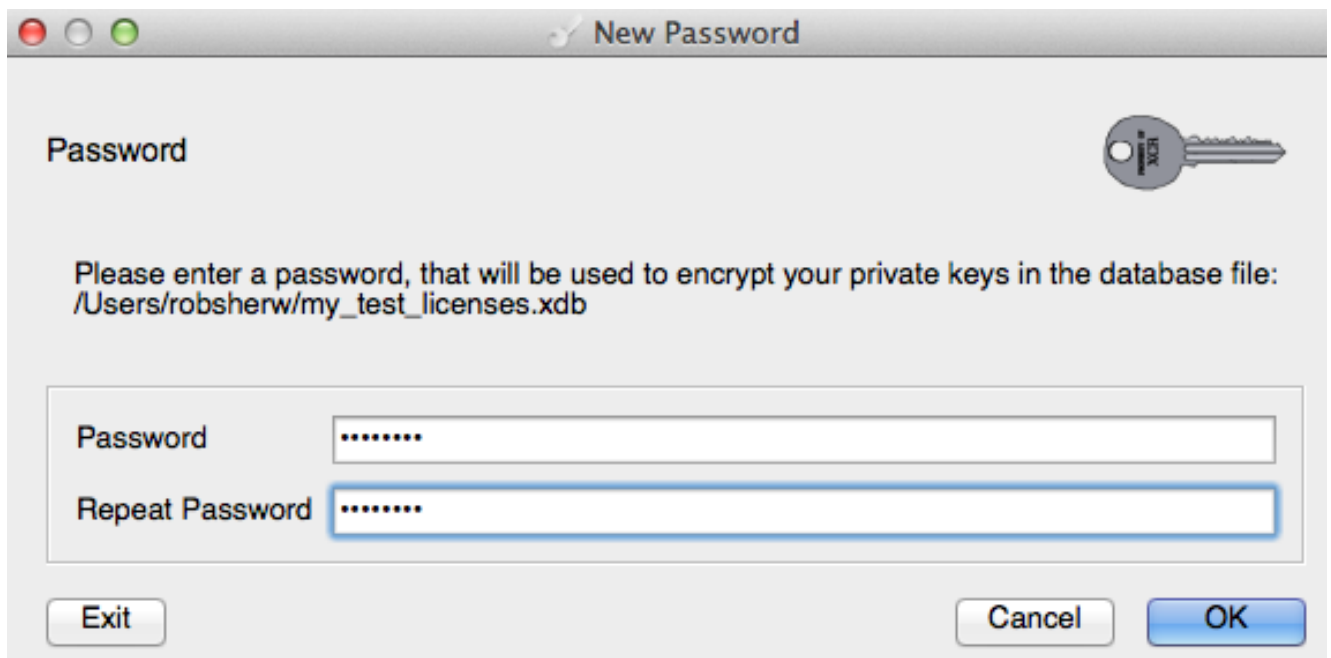
完成这些步骤为了创建S/MIME证书：

1. 如果一个已经存在，请使用XCA应用程序为了创建一个新的XCA数据库或打开一个当前XCA数据库。

从菜单栏，请选择File>新建的数据库>您的choice> <DB名称：



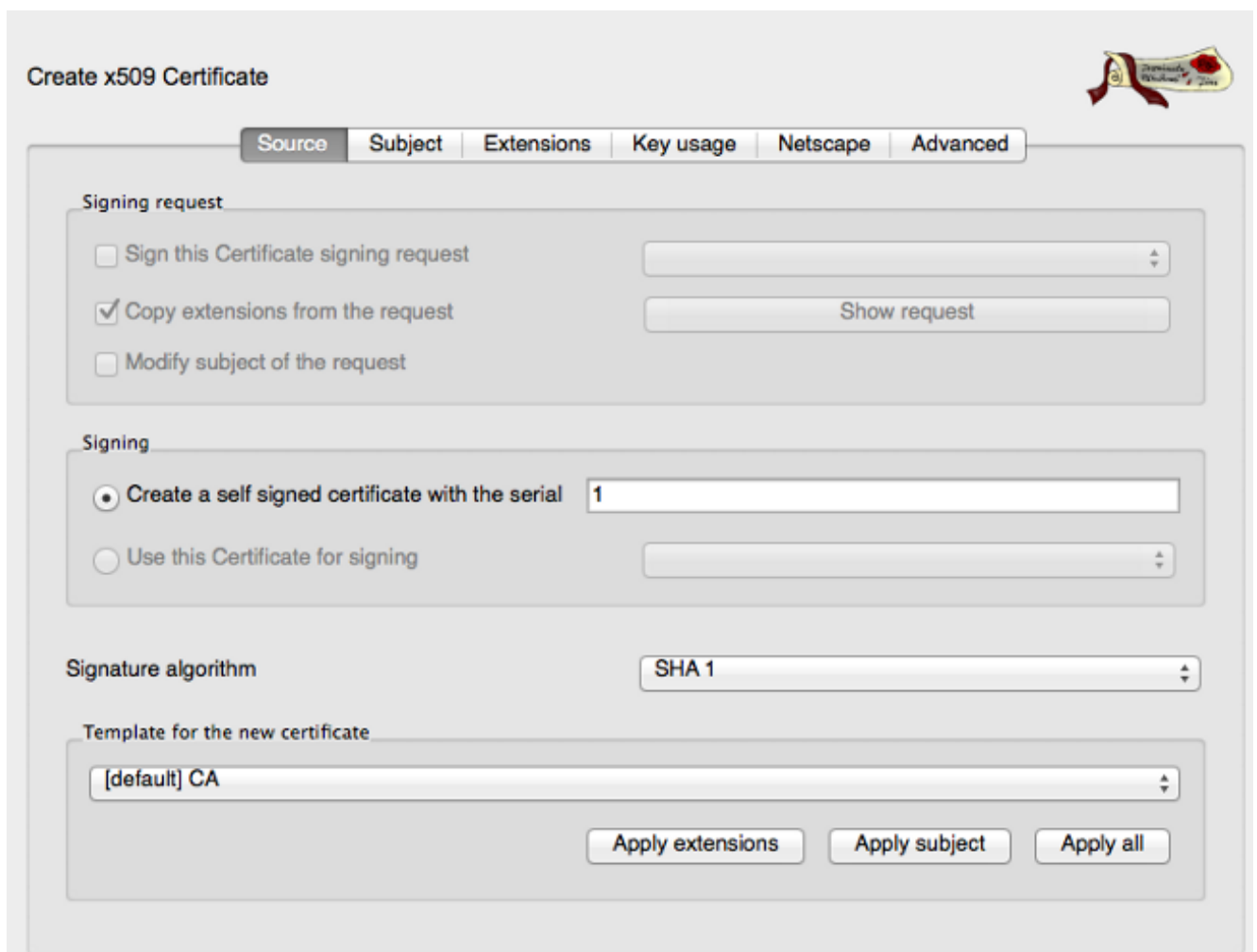
Click **Save**.现在您必须输入关联对此数据库您的专用密钥的加密的一个密码。此密码仅是为XCA数据库。



点击OK键为了完成数据库建立。

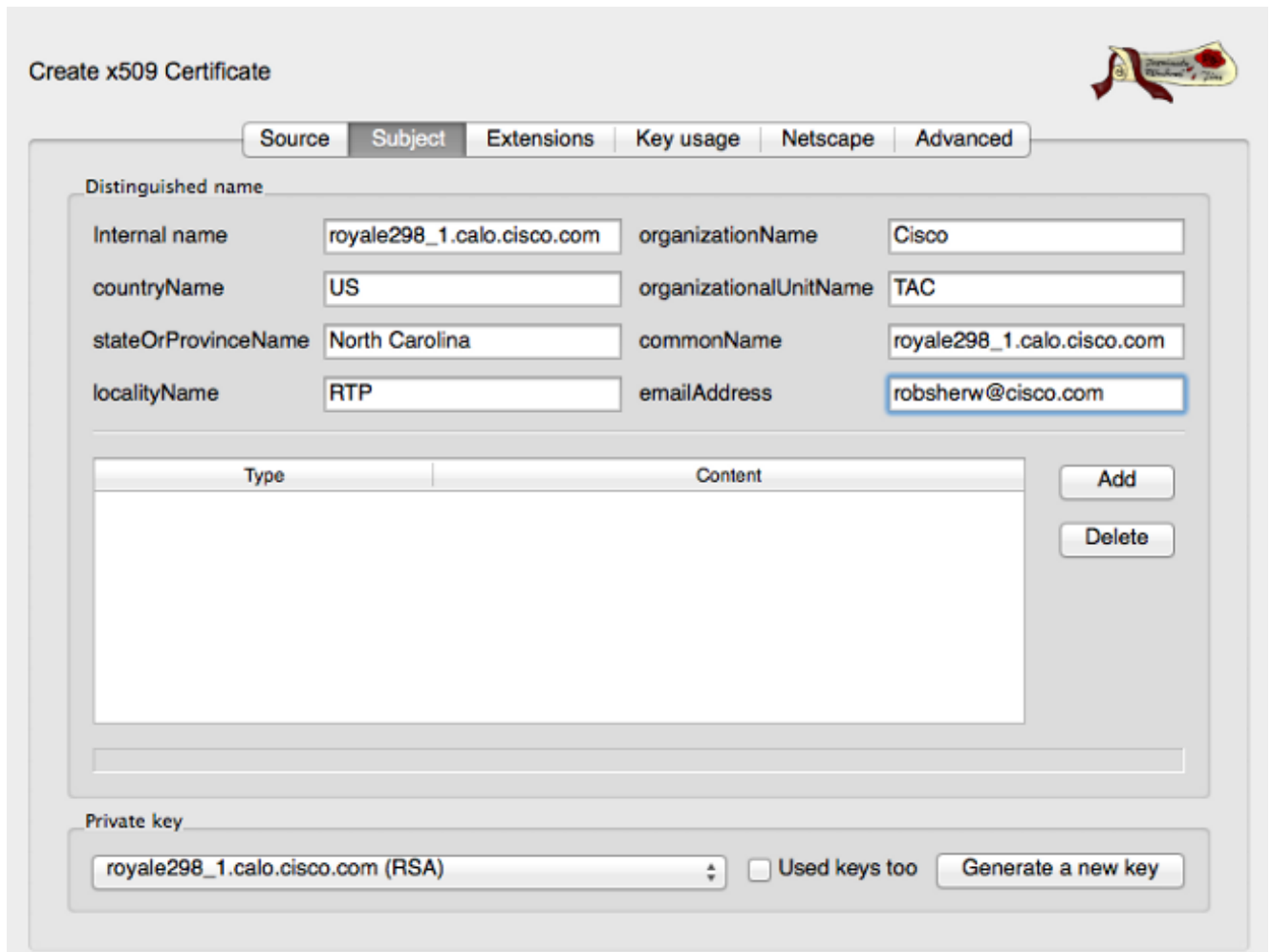
2. 从Certificates Tab，请选择**新证书**，并且**创建x509证书**屏幕出现。

因为可以使用，更改没有从来源选项卡要求默认值：



从附属的选项卡，请输入必填信息到辨别名称部分。在专用密钥部分，请单击**生成新密钥**并

且选择2048位或1024 keysize的位。单击**创建**为了生成专用密钥和连结它与此证书。



The screenshot shows the 'Create x509 Certificate' wizard 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 the fields is a table for extensions:


Type	Content
------	---------

Buttons for 'Add' and 'Delete' are located to the right of the table. At the bottom, the 'Private key' section shows a dropdown menu with 'royale298_1.calo.cisco.com (RSA)' selected, a checkbox for 'Used keys too', and a 'Generate a new key' button.

从扩展选项卡，在基本限制条件部分，为类型请选择**认证机关**。

Note:随后的证书签名请求(CSR)可以通过此CA签字类型设置对**不定义**。

在正确性部分，请根据您的需求(365天输入详细信息默认情况下)。您能选择添加一附属的替代方案名称(SAN)对于域名系统(DNS)，电子邮件地址和类似与使用**编辑按钮**该线路的。从SAN弹出窗口，请单击**添加**并且选择SAN类型和相关的内容。一旦完成，请单击**应用**为了应用这些更改，并且返回到扩展请选中窗口：

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

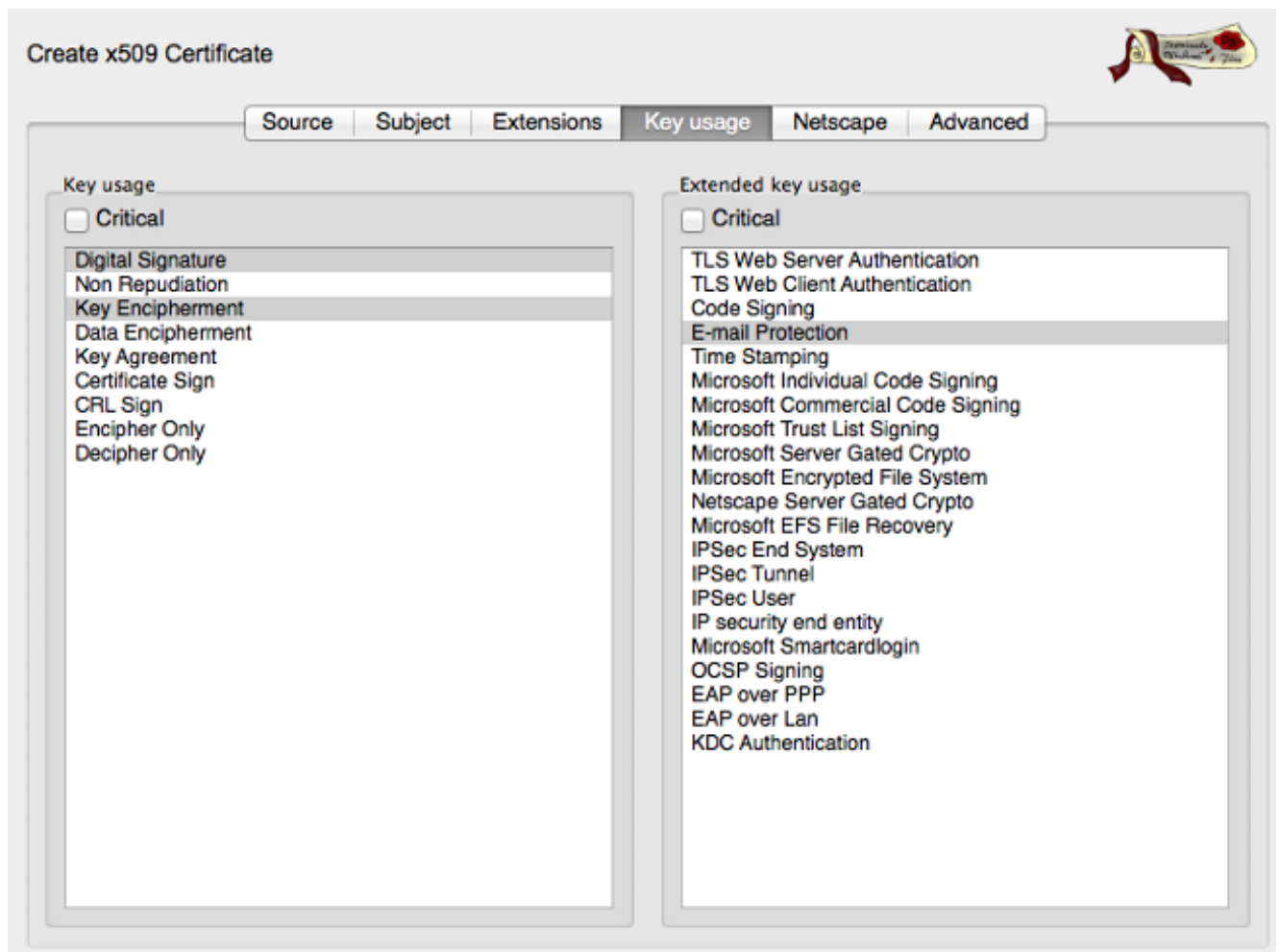
subject alternative name

issuer alternative name

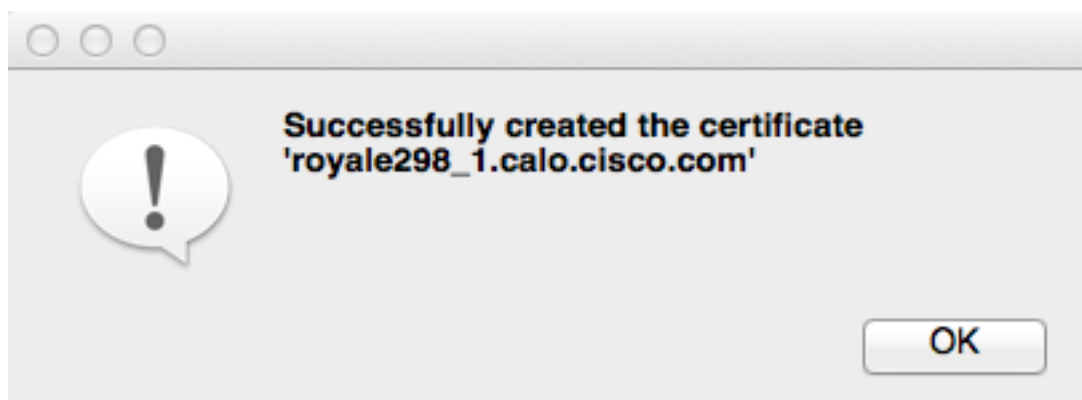
CRL distribution point

Authority Info Access

从密钥用法选项卡，在密钥用法部分，请突出显示**数字签名**和**密钥编码**。在延长的密钥用法部分，请突出显示**电子邮件保护**。这些是S/MIME的需要的元素：

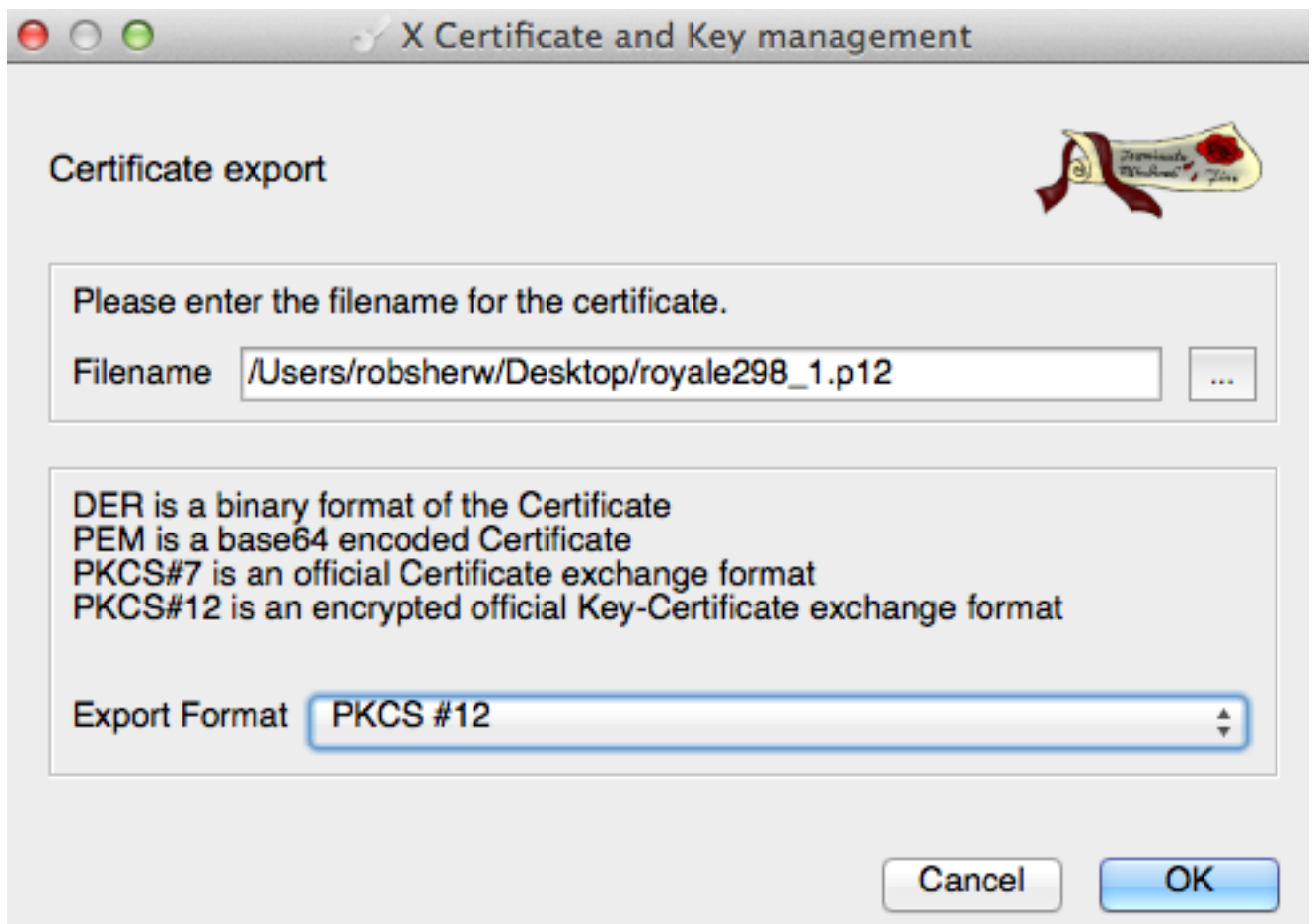


3. 在底部的屏幕点击OK键，并且一个上推通知出现：

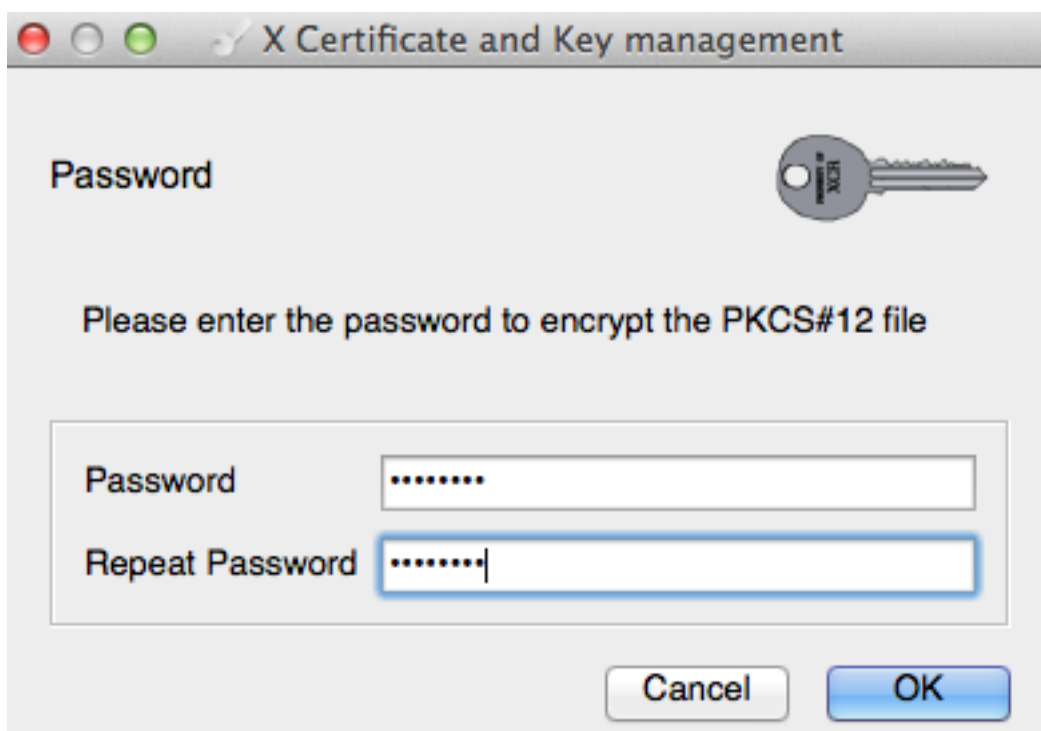


4. 您新建立的证书在证书选项卡当前出现。 点击证书为了突出显示它并且点击出口。选择证书应该保存的文件名、位置和出口格式。


Note:您应该导出您的在两PKCS12的证书和增强加密邮件(PEM)被格式化的证书。 PKCS12证书保存作为.p12被格式化的文件名。 PEM证书保存作为.crt被格式化的文件名。



点击OK键，并且您用PKCS12证书的加密密码提交，是需要的，当您导入在ESA上时的证书：



Note: 当您导出PEM格式化的证书时，没有提示对于密码，因为不是需要的。为了查看证书的详细信息，通过状态、主题、发布者和扩展选项卡单击证书和移动：

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

这时您的证书准备使用在您的ESA。

导入证书对ESA

如果创建一证书外部从ESA您必须导入它在您的ESA上。完成这些步骤为了导入证书：

1. 选择网络>证书>Add证书...>进口证明书。
2. 选择您在前面部分创建的PKCS12 (.p12)格式文件，输入关联对该证书的密码，并且其次单击：

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. 查看证书并且单击提交为了确认您的更改：

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>
	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>
Intermediate Certificates (optional):	<input type="checkbox"/> Upload intermediate certificates if applicable.

这时您的证书当前准备用于在您的ESA的S/MIME。

关联PEM证书

您必须当前添加您PEM格式化的证书到S/MIME公共密钥。完成这些步骤为了添加PEM格式化的证书：

1. 选择邮件策略> S/MIME公共密钥>Add公共密钥....
2. 输入名称，如所需求。
3. 打开在适当的文本编辑的PEM (.crt)被格式化的证书(例如Notepad++ [Windows/PC]或原子 [OSX])。
4. 复制内容从-----开始证书-----通过-----END证书-----。
5. 粘贴此内容到S/MIME公共密钥部分并且单击提交

Add S/MIME Public Key

Add Public Key	
Name:	royale298_1_public_key
S/MIME Public Key:	-----BEGIN CERTIFICATE----- MIIEA1CCAuqAAwIBAgIBATANBqkqkhiG9w0BAQUFADCBmIELMAkGA1UEBhMCVVMx FzAVBgNVBAAgTDk5xcnRoIENhcm9saW5hMQwwCgYDVQQHEwNSVFAxOjAMBgNVBAoT BUJNpc2NvMQwwCgYDVQQLEwNUQUxIzAhBgNVBAMMGnJveWFsZTI1SQF8xLmNhbg8u Y2IzY28uY29tMSEwHwYJKoZIhvcNAQkBFhJyb2JzaGVyY290b3Jlbn51b20wHhcN MTQxMTI0MTU0MTAwWncMTUxMTI0MTU0MTAwWjCBbmIEMAKGA1UEBhMCVVMx BgNVBAAgTDk5xcnRoIENhcm9saW5hMQwwCgYDVQQHEwNSVFAxOjAMBgNVBAoTBUJN pc2NvMQwwCgYDVQQLEwNUQUxIzAhBgNVBAMMGnJveWFsZTI1SQF8xLmNhbg8uY2Iz Y28uY29tMSEwHwYJKoZIhvcNAQkBFhJyb2JzaGVyY290b3Jlbn51b20wgaFIMAQG CSQGS1b3DQEBAAQAA4IBDwAwgEKAoIRAQDgEMocaf8ezvRTjCmBYMIQ12qEWTd ISA+LxwEgkDdmY+jMiRm1+nIBDDF1V9nw8PhD0Xs7UhK8r0m2aNcWdjaLY36Mh4d JjHTHNe/BCwxFXZVaCk9VfxrT5OpIRExtAfcZlvrXgkJ2YUkDZKE6huo4ZqY0Ib yTghWwMAF3oAsXRR+MTwQXj8fyaIy6Gee5QiaRtRwY+2+IKAtWiYuo9Blef2E 4MibfenRURkm5cUZZZrtUJIWe7JHuZCaOIvDjEdoMUcUSoZA5xG6a55ydfP4mG QCI9zmUc02nCcIaDd1cWhtv5x7pwi7wIavrdel2dfxLjNtCGne/CDfKNAgMBAAGj

6. 确认所有更改。这时您的S/MIME公共密钥为您的ESA当前设置。

相关信息

- [思科电子邮件安全工具最终用户指南](#)
- [思科电子邮件安全工具版本注释和一般信息](#)
- [技术支持和文档 - Cisco Systems](#)