ESA证书创建为了用在S/MIME签字上

目录

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**创建自已签署的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. 点击**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. 点击您创建的证书的超链接。
3. 点击**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：

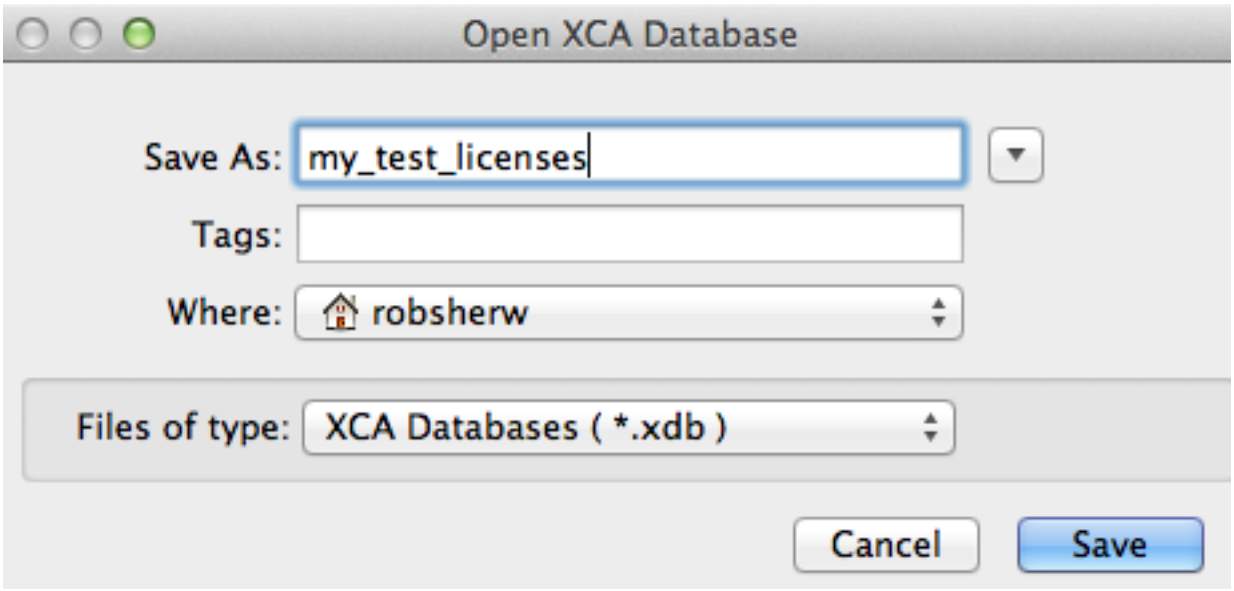
- 麦金塔操作系统(OSX) ：Sourceforge
- Microsoft Windows系统：Sourceforge

创建证书

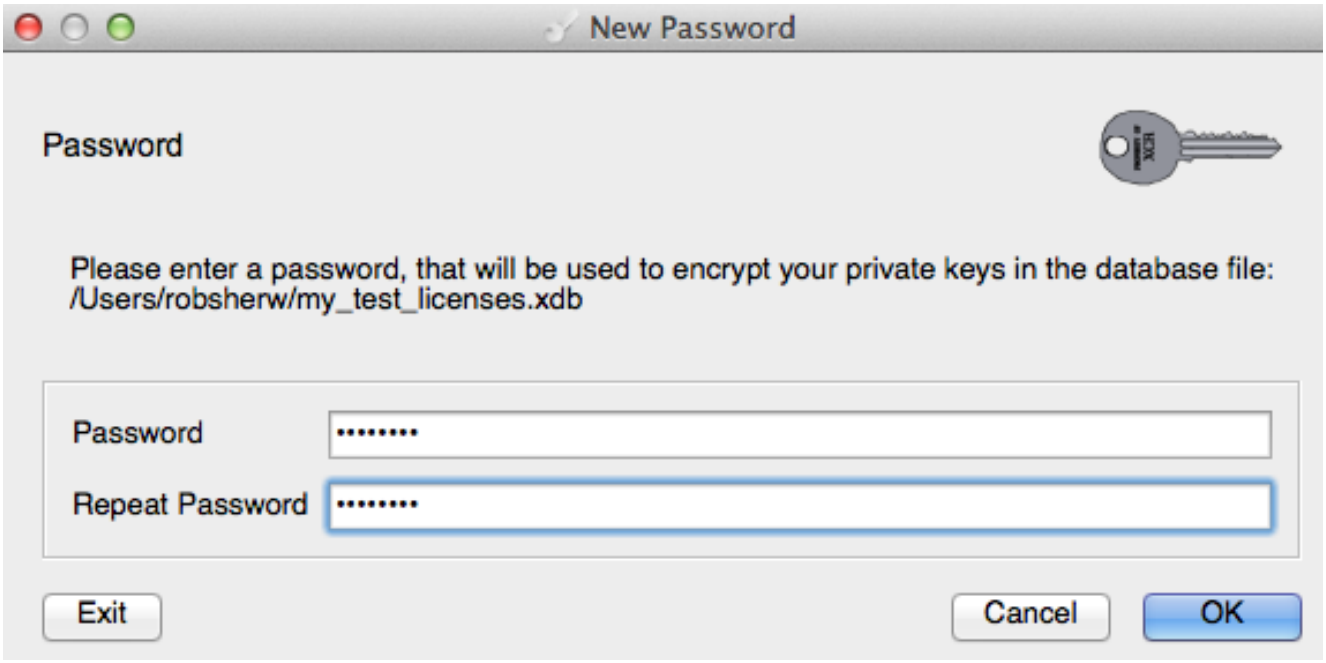
完成这些步骤为了创建S/MIME证书：

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**：



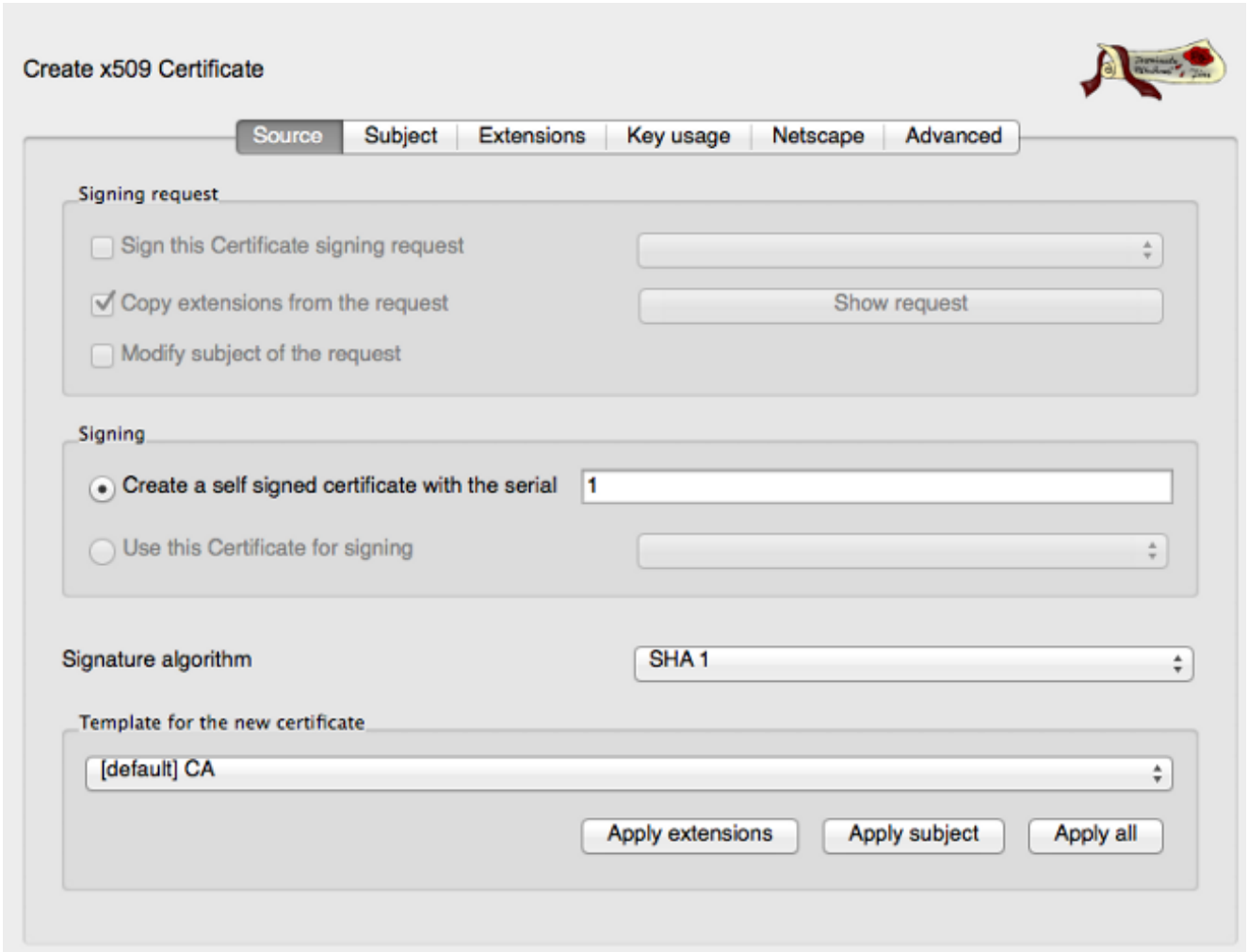
   Click **Save**.现在您必须输入关联对此数据库您的专用密钥的加密的一个密码。 此密码仅是为XCA数据库。



点击OK键为了完成数据库建立。

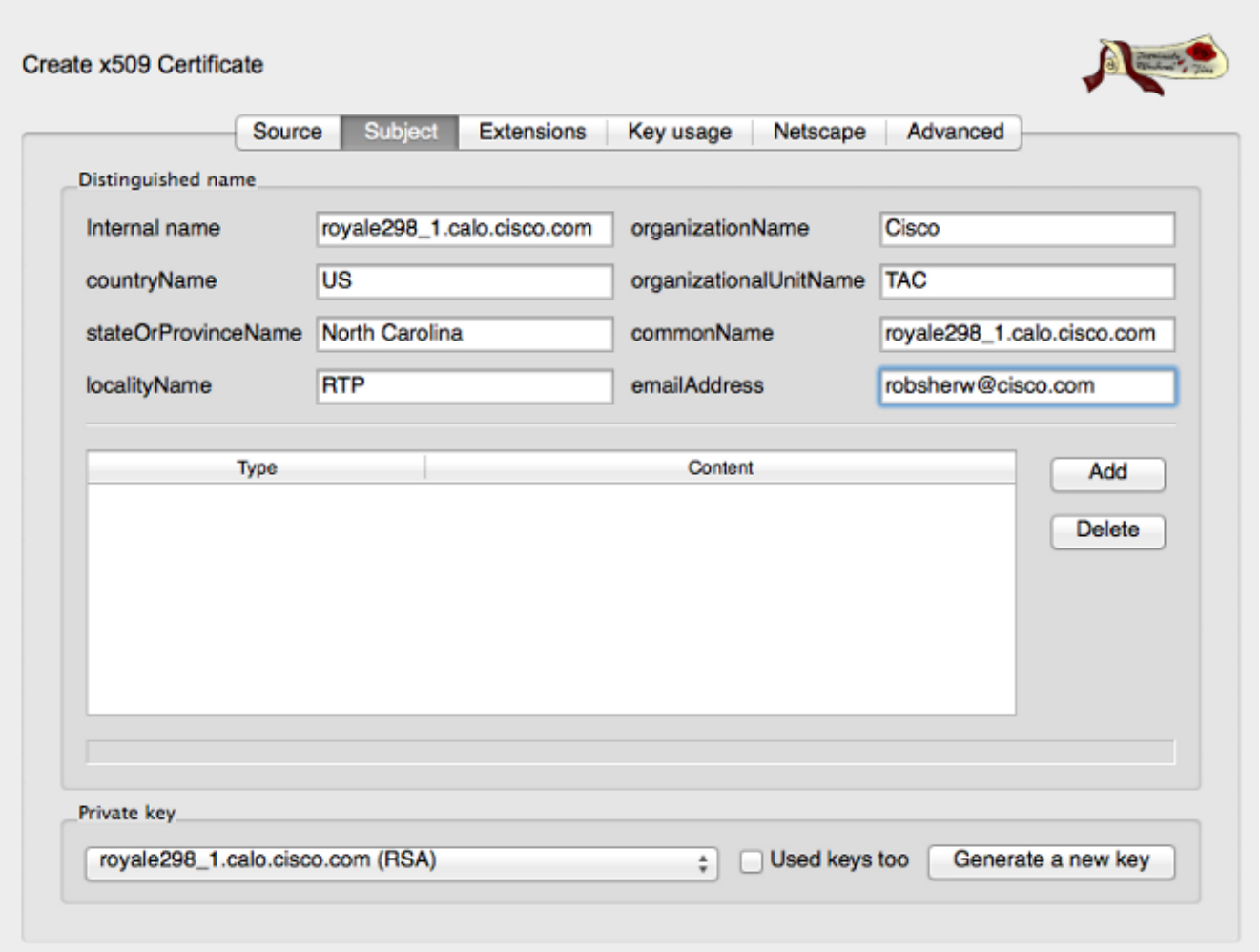
2. 从Certificates Tab，请选择**新证书，**并且*创建x509证书*屏幕出现。

因为可以使用，更改没有从来源选项卡要求默认值：



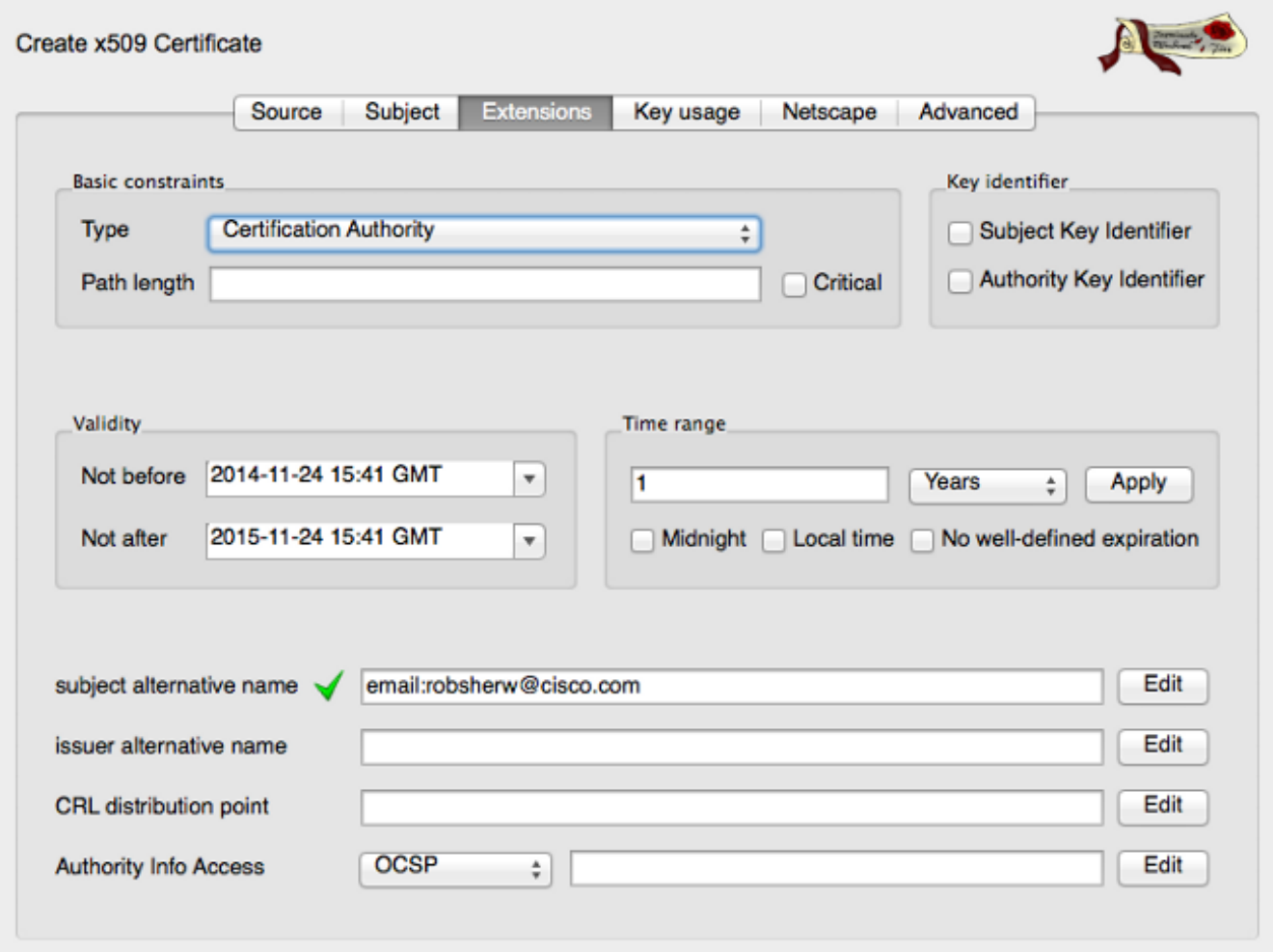
从附属的选项卡，请输入必填信息到辨别名称部分。 在专用密钥部分，请单击**生成新密钥**并

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。

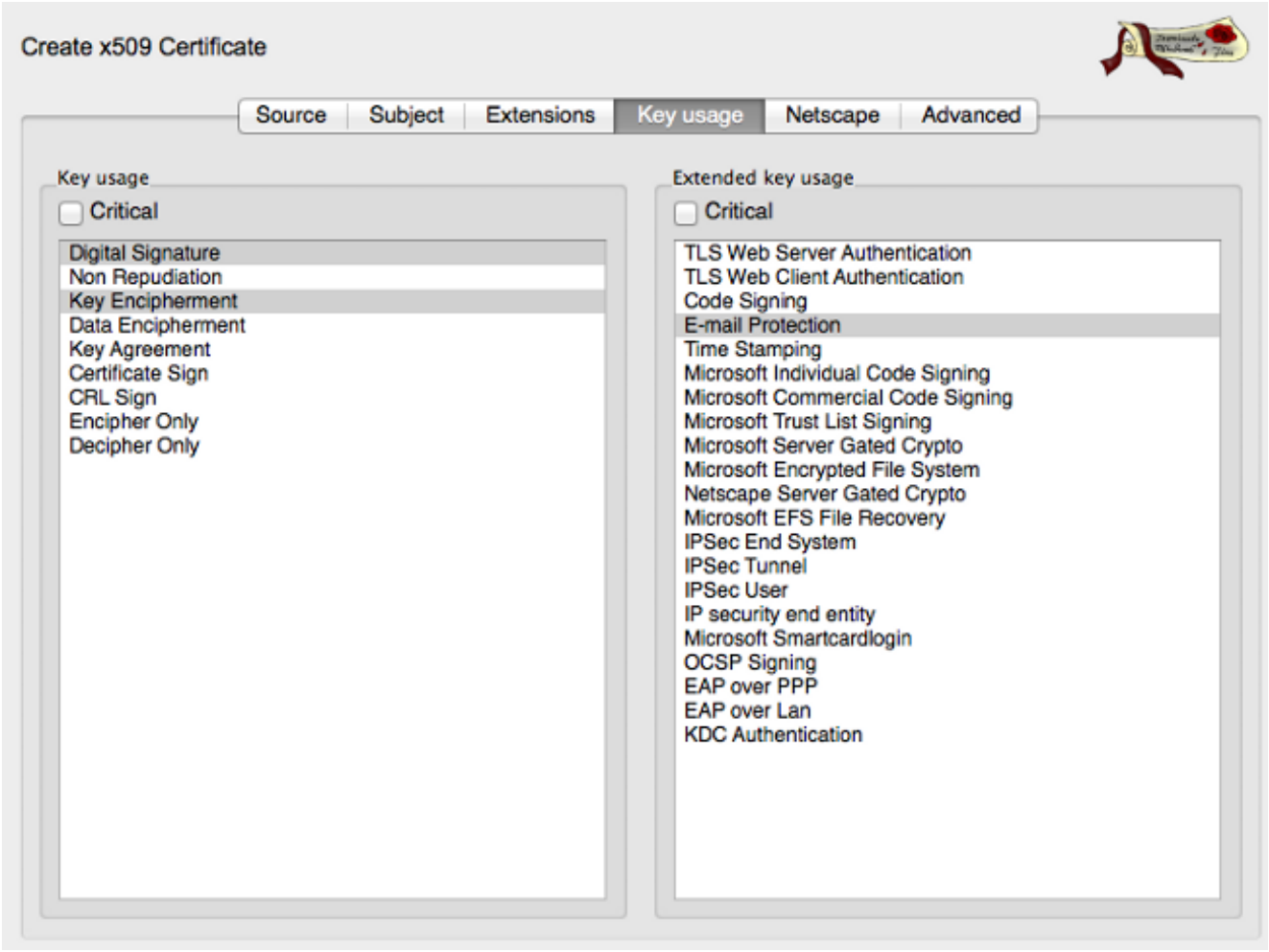


从扩展选项卡，在基本限制条件部分，为类型请选择**认证机关**。

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：



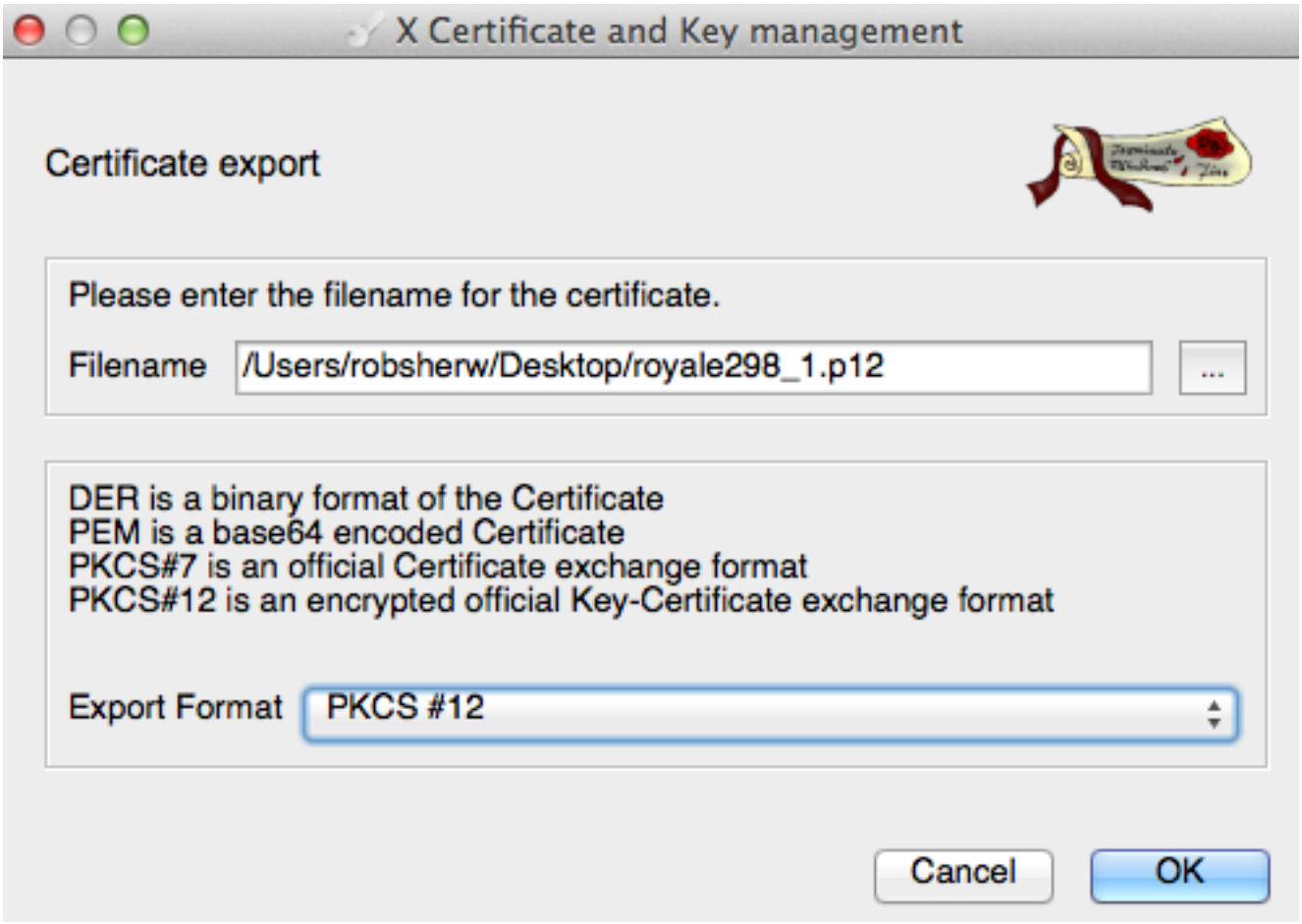
从密钥用法选项卡，在密钥用法部分，请突出显示**数字签名**和**密钥编码**。在延长的密钥用法部分，请突出显示**电子邮件保护**。这些是S/MIME的需要的元素：



3. 在底部的屏幕点击OK键，并且一个上推通知出现：

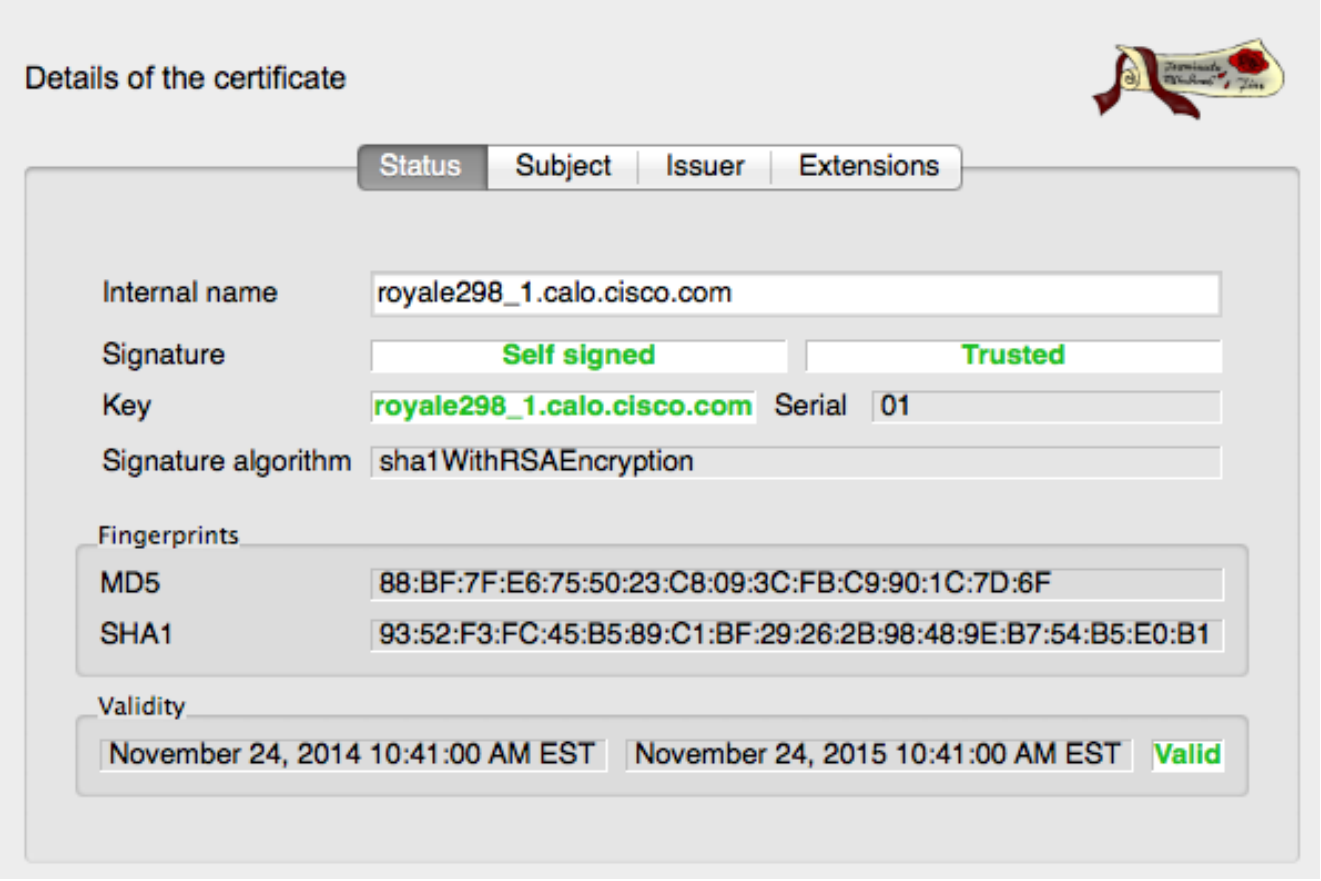
4. 您新建立的证书在证书选项卡当前出现。 点击证书为了突出显示它并且点击**出口**。选择证书应该保存的文件名、位置和出口格式。

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：

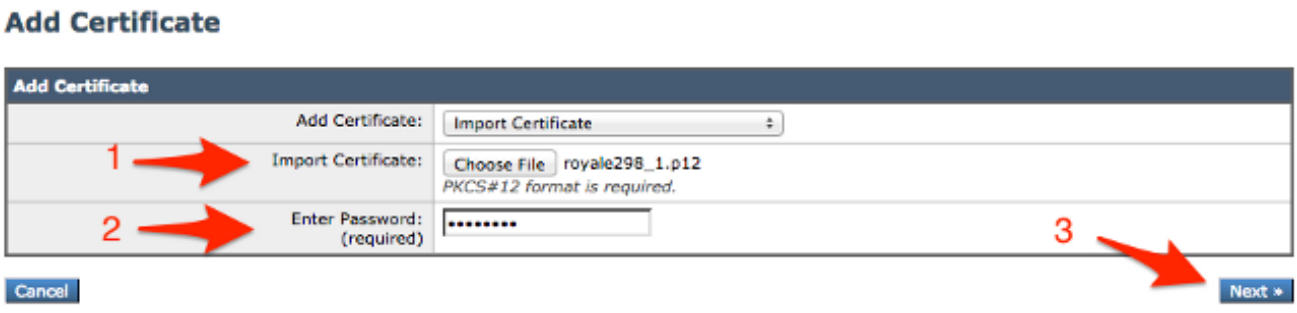


这时您的证书准备使用在您的ESA。

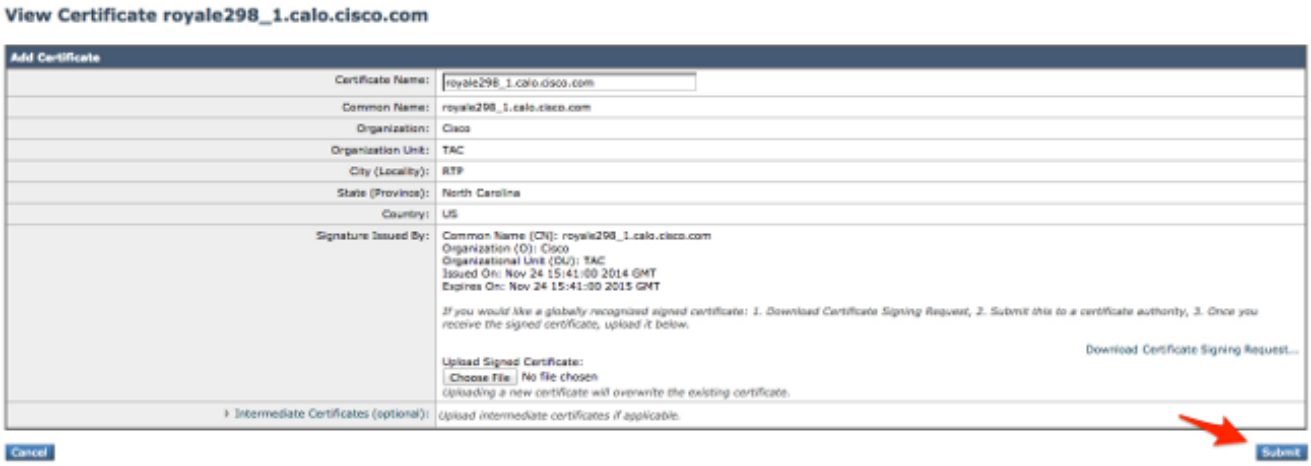
导入证书对ESA

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：



3. 查看证书并且单击**提交**为了确认您的更改：



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**：

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]