Создание сертификата ESA для использования с подписанием S/MIME

Содержание

Введение

Этот документ описывает, как создать сертификаты для использования с Безопасными / Многоцелевыми расширениями почты в Интернете (S/MIME) , подписывающийся на Cisco Email Security Appliance (ESA).

Общие сведения

При создании сертификата S/MIME для подписания сообщения это должно удовлетворить требования, описанные в RFC 5750: Безопасные / Многоцелевые расширения почты в Интернете (S/MIME) Версия 3.2 - Обработка Сертификата.

Для этого процесса использование внешнего приложения требуется для генерации сертификата. X Сертификатов и Управление ключами (XCA) являются приложением , которое управляет асимметричными ключами, такими как алгоритм цифровой подписи райвеста шамира адлемана (RSA) или Алгоритм цифровой подписи (DSA), и предназначено, чтобы быть маленьким Центром сертификации (CA) для создания и подписания сертификатов. Это пользуется библиотекой Open Secure Sockets Layer (OpenSSL) для криптографических операций.

> **Примечание:** XCA является сторонним приложением, которое не поддерживается Cisco. Использование этого приложения предоставлено только для рисунка и простоты администрирования для администрирования S/MIME, тестирования и конфигурации. Для полного изложения и инструкций по XCA, обратитесь к XCA - X Сертификатов и документ управления ключами.

Можно загрузить приложение XCA в любом из этих местоположений:

- Операционные системы Macintosh (OSX): Sourceforge

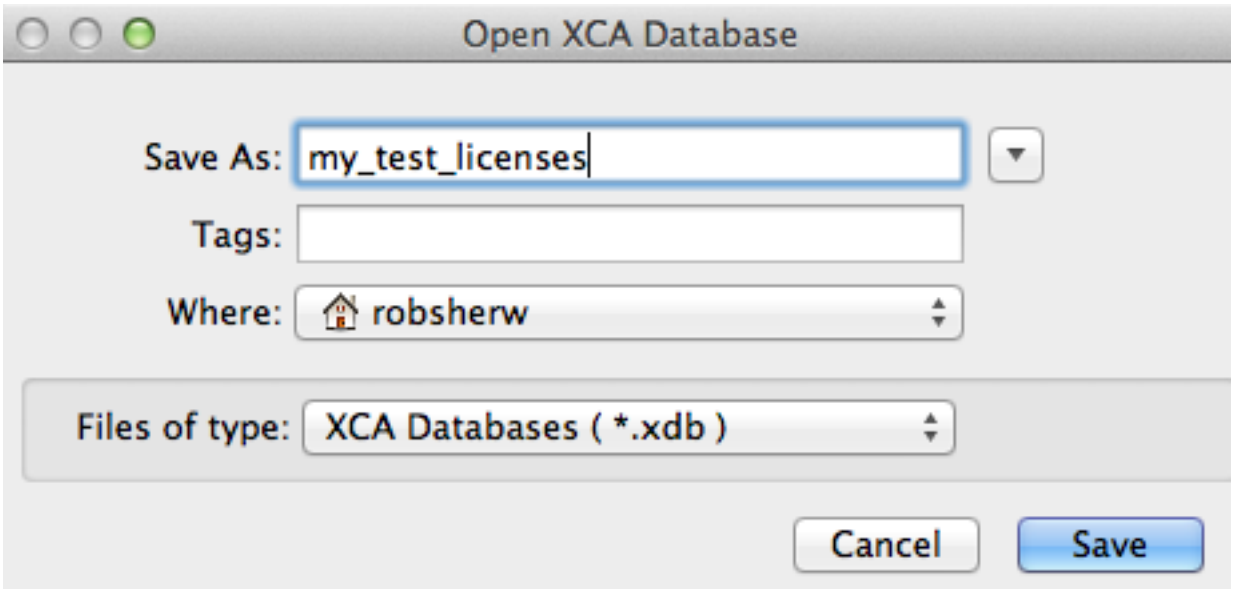
- Системы Microsoft Windows: Softpedia

Создайте сертификат

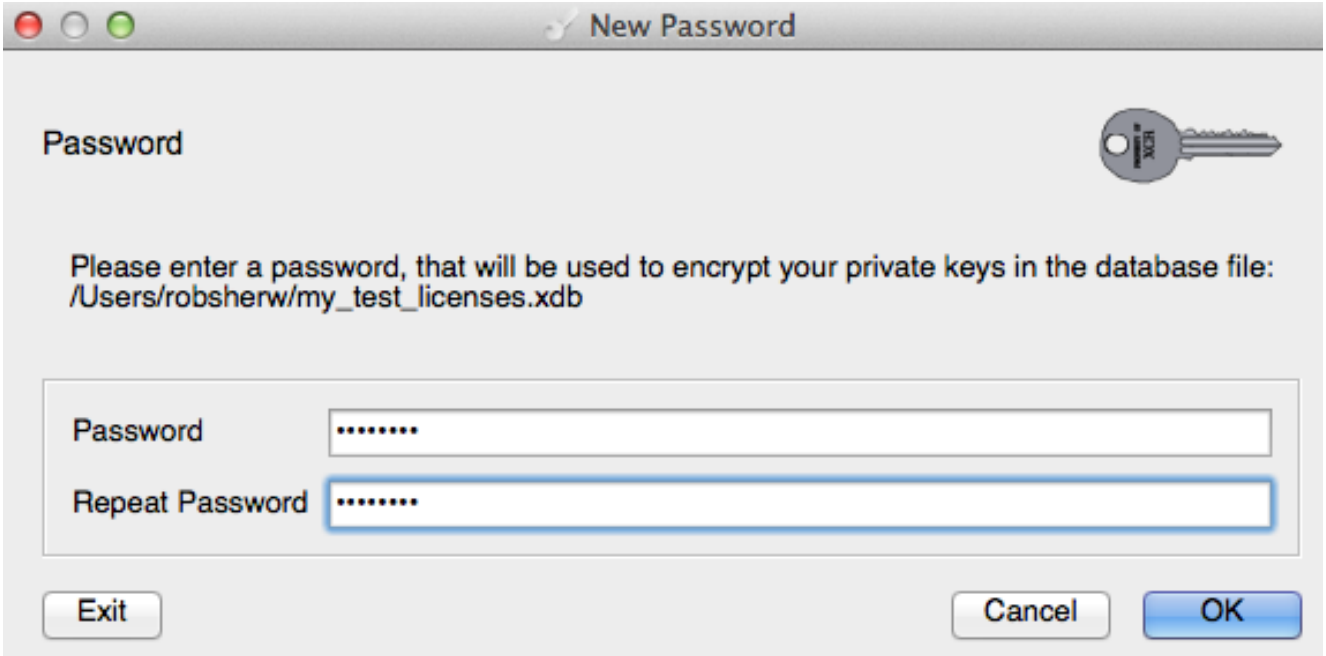
Выполните эти шаги для создания сертификата S/MIME:

1. Используйте приложение XCA, чтобы создать новую базу данных XCA или открыть текущую базу данных XCA, если вы уже существуете.

   От строки меню перейдите к **Файлу> Новая База данных> <название DB по Вашему выбору>**:



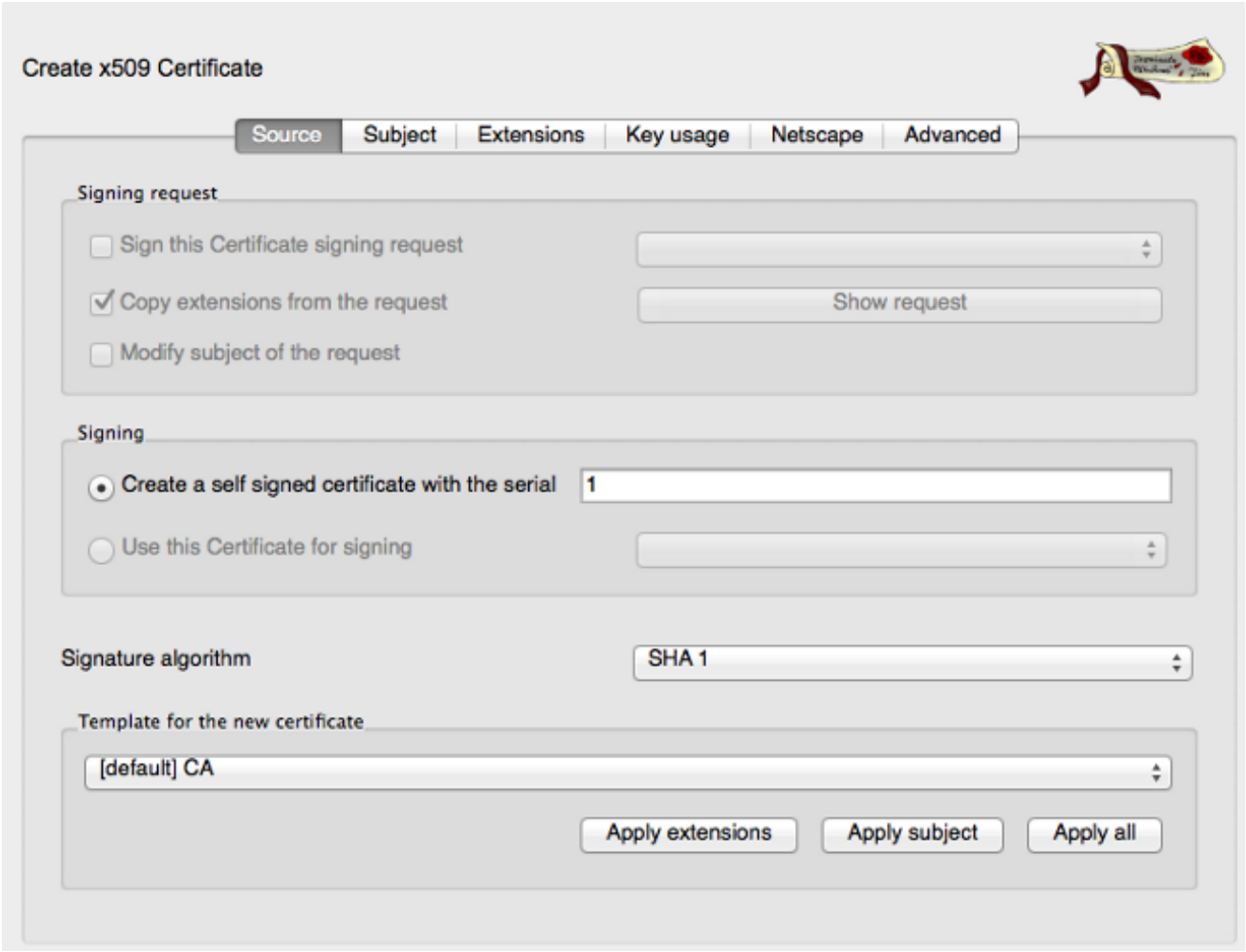
   Нажмите Save. Теперь необходимо ввести пароль для шифрования секретных ключей, которые привязаны к этой базе данных. Этот пароль только для базы данных XCA.



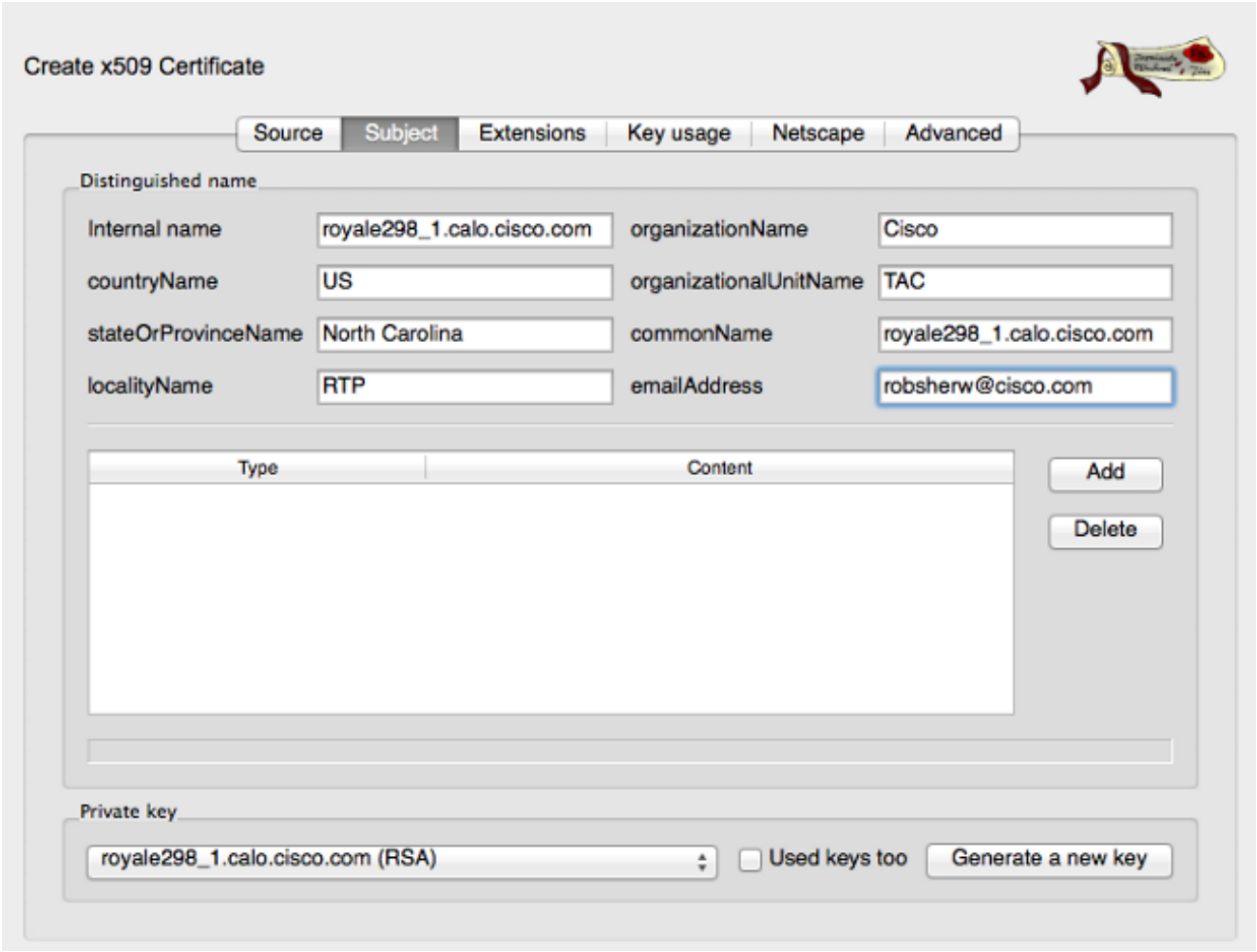
Нажмите **OK** для завершения создания базы данных.

2. От вкладки Certificates выберите **New Certificate**, и *экран Create x509 Certificate* появляется.

   Никакие изменения не требуются от вкладки Source, поскольку могут использоваться значения по умолчанию:

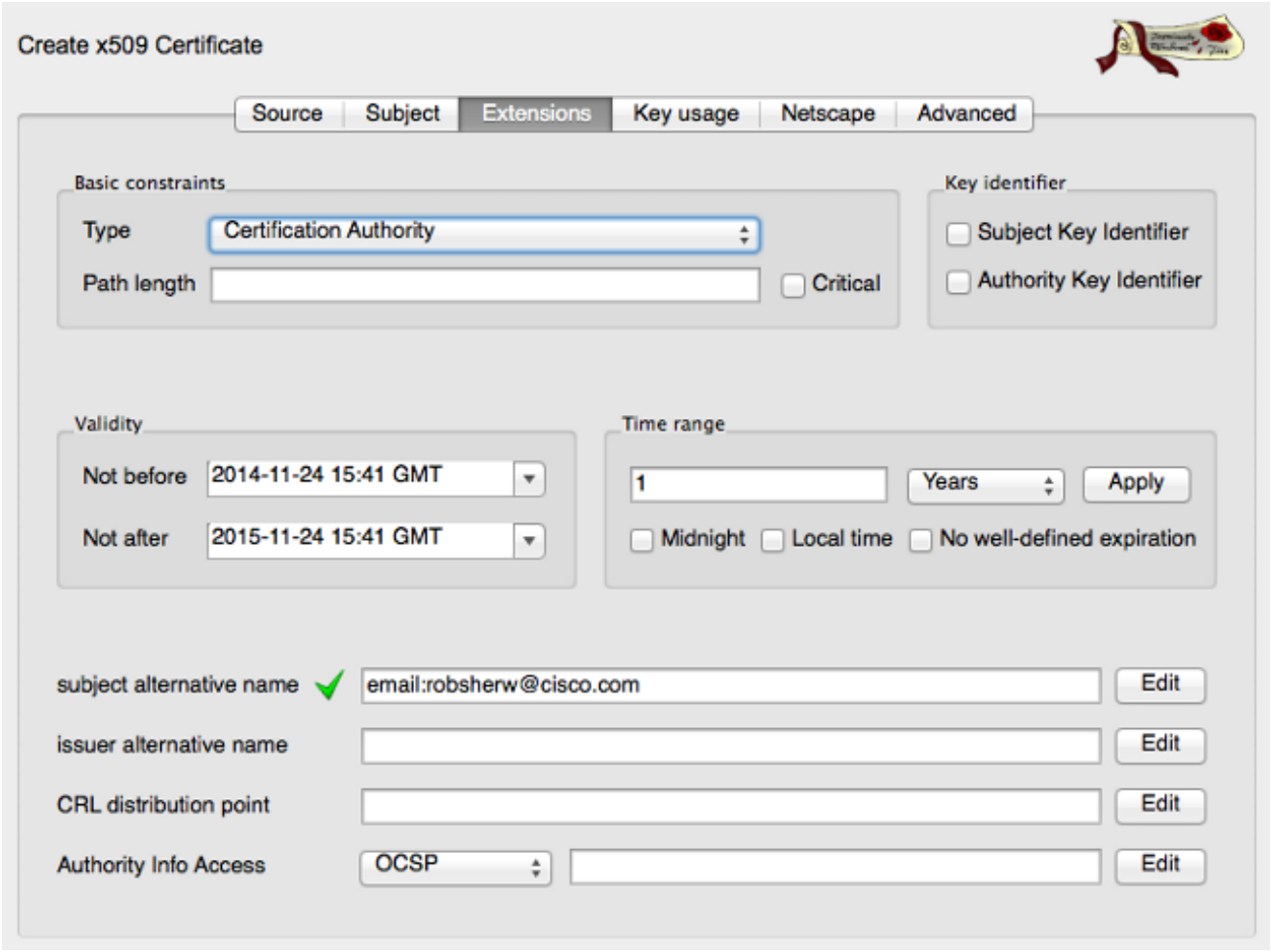


   От вкладки Subject введите необходимую информацию в раздел Составного имени. В разделе С закрытым ключом нажмите **Generate новый ключ** и выберите или **2048 битов** или **1024 бита** для размера ключа. Нажмите **Create**, чтобы генерировать Секретный ключ и привязать его к этому сертификату.

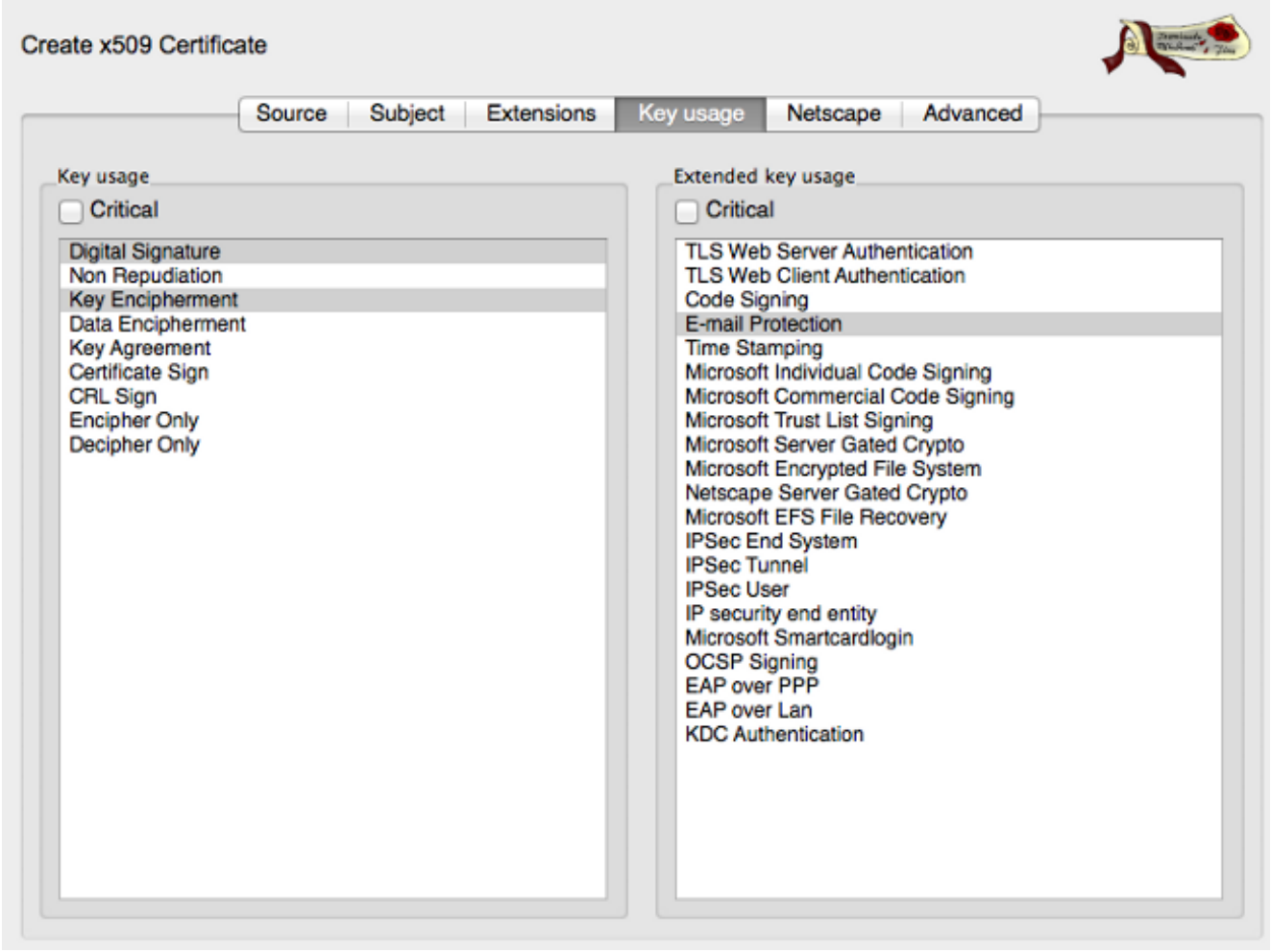


От вкладки Extensions, в разделе Основных ограничений, выбирают **Certificate Authority** для Типа.

Примечание: Последующие Запросы подписи сертификата (CSR) могут быть подписаны через этот CA с набором Типа к **Не Определенный**.
В разделе Законности введите подробные данные согласно своим требованиям (365 дней по умолчанию). Можно принять решение добавить альтернативное имя субъекта (SAN) для Системы доменных имен (DNS), адреса электронной почты, и похожий с использованием **кнопки Edit** для той линии. От всплывающего окна SAN **нажмите Add** и выберите SAN тип и привязанное содержание. После того, как завершенный, нажмите **Apply**, чтобы применить эти изменения и возвратиться к окну вкладки Extensions:



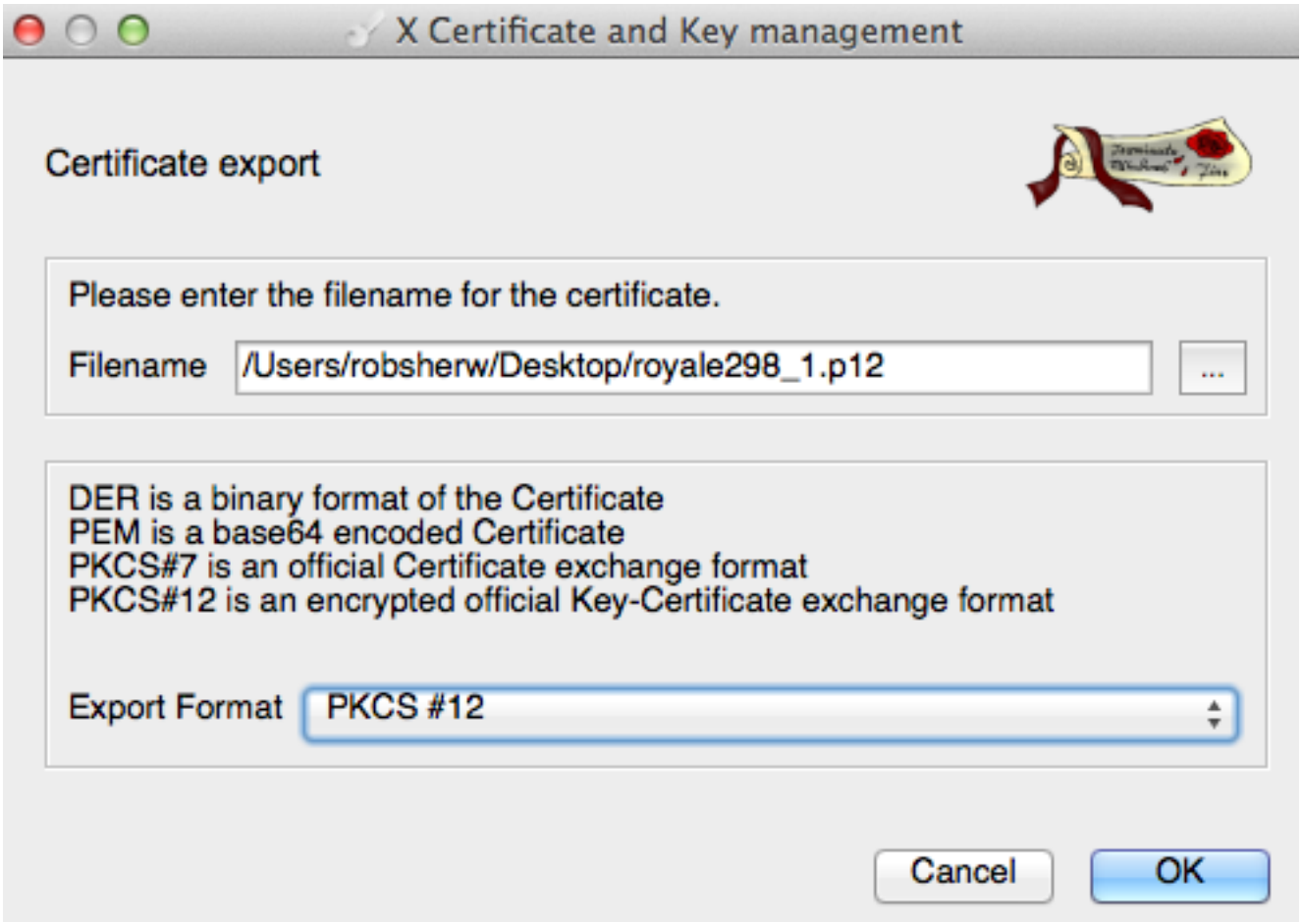
От Ключевой вкладки использования, в Ключевом разделе использования, **Цифровой подписи** выделения и **Ключевой Шифровке**. В Расширенном ключевом разделе использования выделите **Почтовую Защиту**. Это требуемые элементы для S/MIME:



3. Нажмите **OK** внизу экрана, и появляется всплывающее уведомление:

4. Ваш недавно созданный сертификат теперь появляется во вкладке Certificate. Нажмите сертификат, чтобы выделить его и нажать **Export**. Выберите имя файла, местоположение, к которому сертификат должен быть сохранен, и формат экспорта.

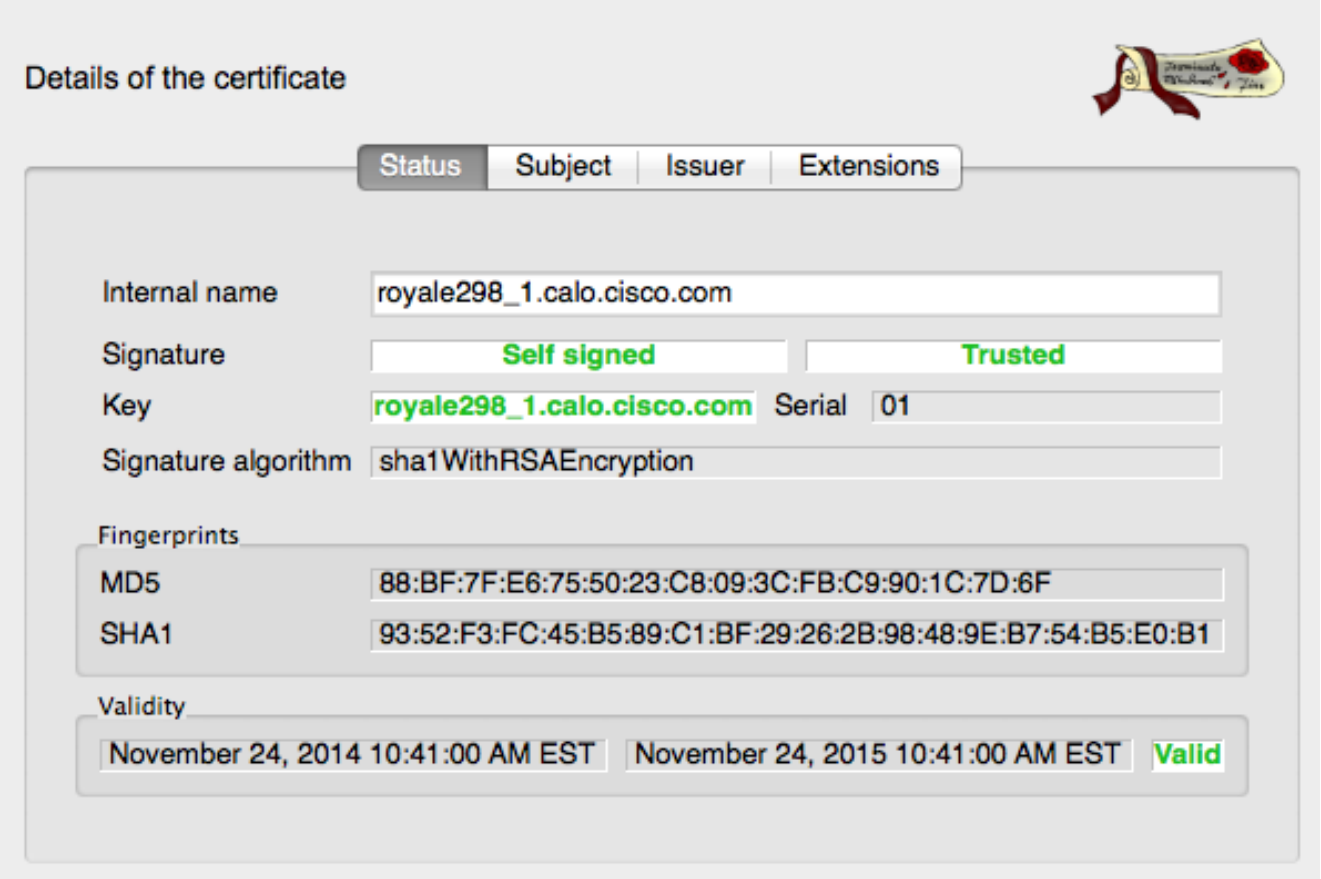
   Примечание: Необходимо экспортировать сертификат и в PKCS12 и в отформатированных сертификатах Privacy Enhanced Mail (PEM). Сертификат PKCS12 сохраняет, поскольку **.p12** отформатировал имя файла. Сертификат PEM сохраняет, поскольку **.crt** отформатировал имя файла.



Нажмите **OK**, и вам предоставляют пароль шифрования для сертификата PKCS12, который необходим, когда вы импортируете сертификат на ESA:

Примечание: Когда вы экспортируете отформатированный PEM сертификат, вам не предлагают для пароля, поскольку он не необходим.
Чтобы посмотреть детали сертификата, нажмите **Certificates** и переместитесь через

Статус, Предмет, Отправителя и вкладки Extensions:



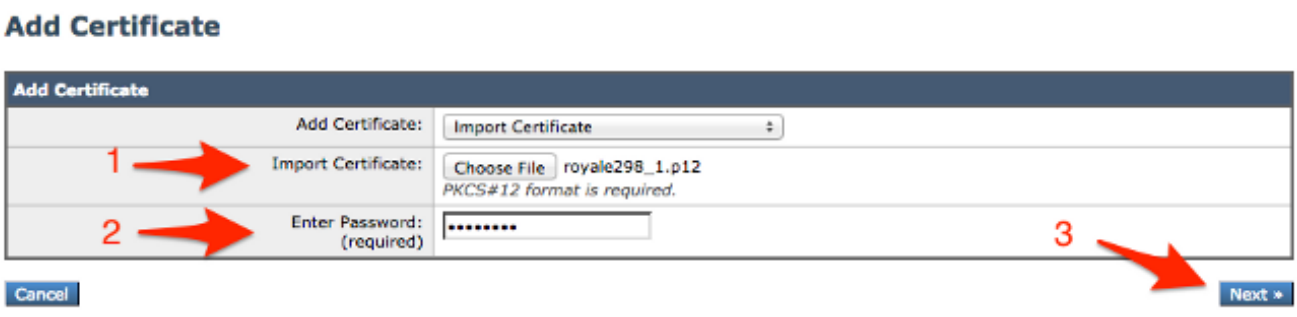
На этом этапе ваш сертификат готов использоваться на вашем ESA.

Импортируйте сертификат

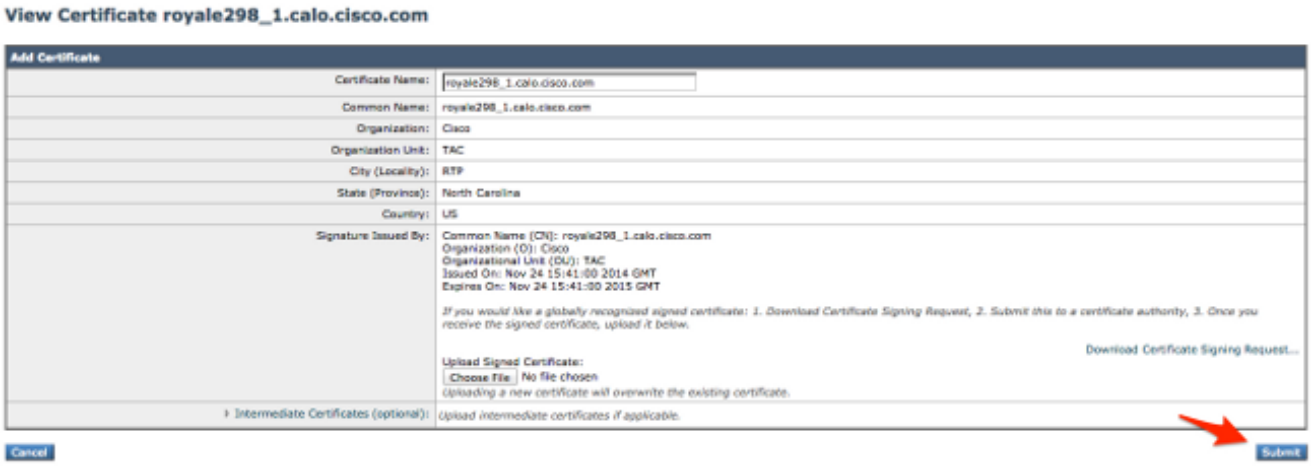
Теперь, когда сертификат создан, необходимо импортировать его на ESA. Выполните эти шаги для импорта сертификата:

1. Перейдите к **Сети>, Сертификаты> Добавляют Сертификат...> Сертификат импорта**.

2. Выберите PKCS12 (.p12) отформатированный файл, который вы создали в предыдущем разделе, введите пароль, который привязан к тому сертификату, и нажмите **Next**:



3. Рассмотрите сертификат и нажмите **Submit** для фиксации изменений:



На этом этапе ваш сертификат теперь готов использоваться для S/MIME на вашем ESA.

Привяжите сертификат PEM

Необходимо теперь добавить отформатированный PEM сертификат к Открытым ключам S/MIME. Выполните эти шаги для добавления отформатированного PEM сертификата:

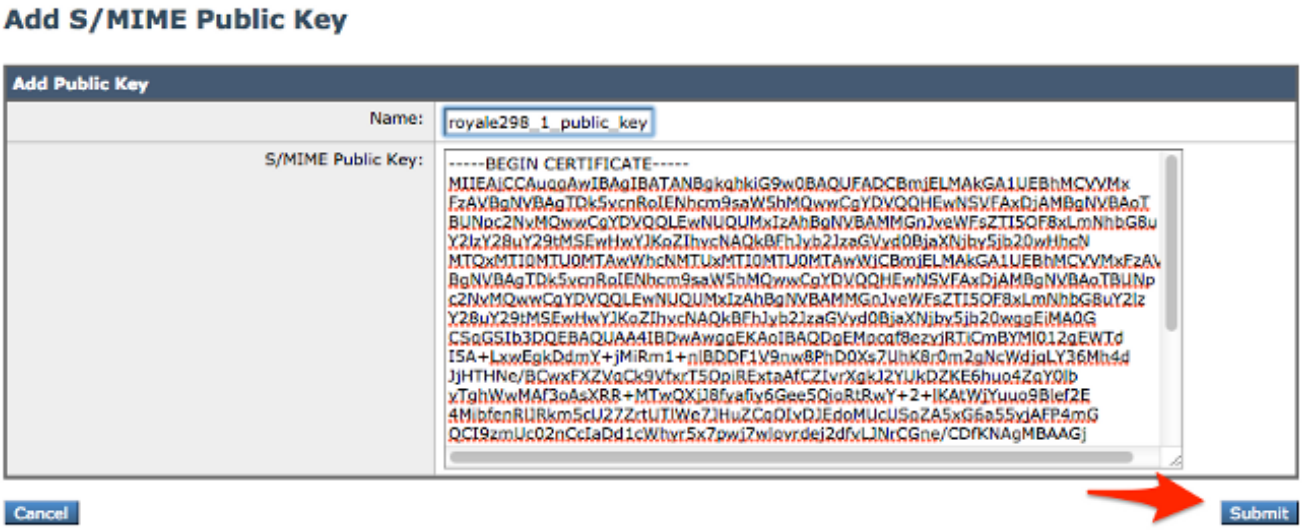
1. Перейдите для **Отправки по почте Политики>, Открытые ключи S/MIME> Добавляют Открытый ключ....**

2. Введите имя, как требуется.

3. Откройте PEM (.crt) отформатированный сертификат в соответствующем текстовом редакторе (таком как Блокнот ++ или Atom).

4. Скопируйте содержание с**-----СЕРТИФИКАТА BEGIN-----**через**-----КОНЕЧНЫЙ СЕРТИФИКАТ-----**.

5. Вставьте это содержание в раздел С открытым ключом S/MIME и нажмите **Submit**:



6. Передайте все изменения. На этом этапе ваш Открытый ключ S/MIME теперь установлен для вашего ESA.

Дополнительные сведения

- AsyncOS 9.0 для почтового руководства пользователя
- Cisco Systems – техническая поддержка и документация