ООО «ЛИССИ-Софт»

Программный комплекс «Fox-XCA»

Руководство администратора

RU.ЛСАФ.00005-01 34 01

Москва 2013

Содержание

Аннотация

Настоящий документ содержит руководство администратора по работе с программным комплексом «Fox-XCA».

В документе описаны возможности комплекса и интерфейс администратора.

1 Общее описание

1.1 Назначение

ПК «Fox-XCA» предназначен для создания, обработки и хранения заявок на издание или аннулирование сертификатов ключей проверки электронной подписи (ЭП), издания сертификатов Удостоверяющего центра, издания списков аннулированных сертификатов (CAC), ведения базы сертификатов.

ПК «Fox-XCA» реализует следующие основные функции:

- генерация ключевых пар (ГОСТ Р 34.10-2012, ГОСТ Р 34.10-2001, RSA, DSA);
- формирование и хранение запросов на сертификаты в формате PKCS#10;
- выдача и переиздание сертификатов;
- формирование списков аннулированных сертификатов;
- импорт и экспорт ключевых пар, запросов, сертификатов, цепочек сертификатов, списков аннулированных сертификатов в форматах DER, BER, PEM, PKCS#12;

ПК «Fox-XCA» в качестве криптоядра использует сертифицированное средство криптографической защиты информации (СКЗИ) – программную библиотеку защиты информации «СКЗИ «ЛИРССЛ», реализующее следующие криптографические алгоритмы:

- шифрование данных по ГОСТ 28147-89 в режимах простой замены, гаммирования, гаммирования с обратной связью и в режиме сцепления блоков;
- контроль целостности данных посредством вычисления имитовставки по ГОСТ 28147-89;
- вычисление значения хэш-функции в соответствии с ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012;
- вычисление и проверку электронной подписи (ЭП) в соответствии с ГОСТ Р 34.10-2012, ГОСТ Р 34.10-2001.

ПК «Fox-XCA» функционирует под управлением ОС Linux или MS Windows

1.2 Интерфейс администратора ПК «Fox-XCA»

Интерфейс администратора предназначен для формирования сертификатов ключей проверки ЭП, списков аннулированных сертификатов, ведения базы данных сертификатов и списков аннулированных сертификатов, создания запросов на издание или аннулирование сертификатов, формирования заявок на изменение статуса сертификатов.

Через интерфейс администратора выполняется обработка запросов на создание ключей и сертификатов, управление статусом уже выпущенных сертификатов, ведение базы данных сертификатов (от принятия заявки на создание до аннулирования).

Интерфейс администратора обеспечивает:

- выпуск заверенных на ключе ЭП УЦ сертификатов ключей проверки ЭП пользователей;
- формирование списков действительных и аннулированных сертификатов;
- защиту от несанкционированного доступа к данным;

- совместимость форматов изданных сертификатов с рекомендациями X.509 версии 3 (RFC 3280);
- формирование заявки на сертификат в формате PKCS#10;
- формирование запросов на отзыв сертификатов ключей проверки ЭП;
- формирование запросов на приостановление/возобновление действия сертификатов ключей проверки ЭП;
- экспорт сертификатов, запросов на сертификаты, ключевых пар, CAC;
- импорт сертификатов, запросов на сертификаты, ключевых пар, CAC.

2 Установка ПК «Fox-XCA»

2.1 Установка в ОС MS Windows

Для установки ПК «Fox-XCA» в ОС MS Windows необходимо запустить инсталлятор Fox-XCA-Setup.exe и следовать инструкциям мастера установки.

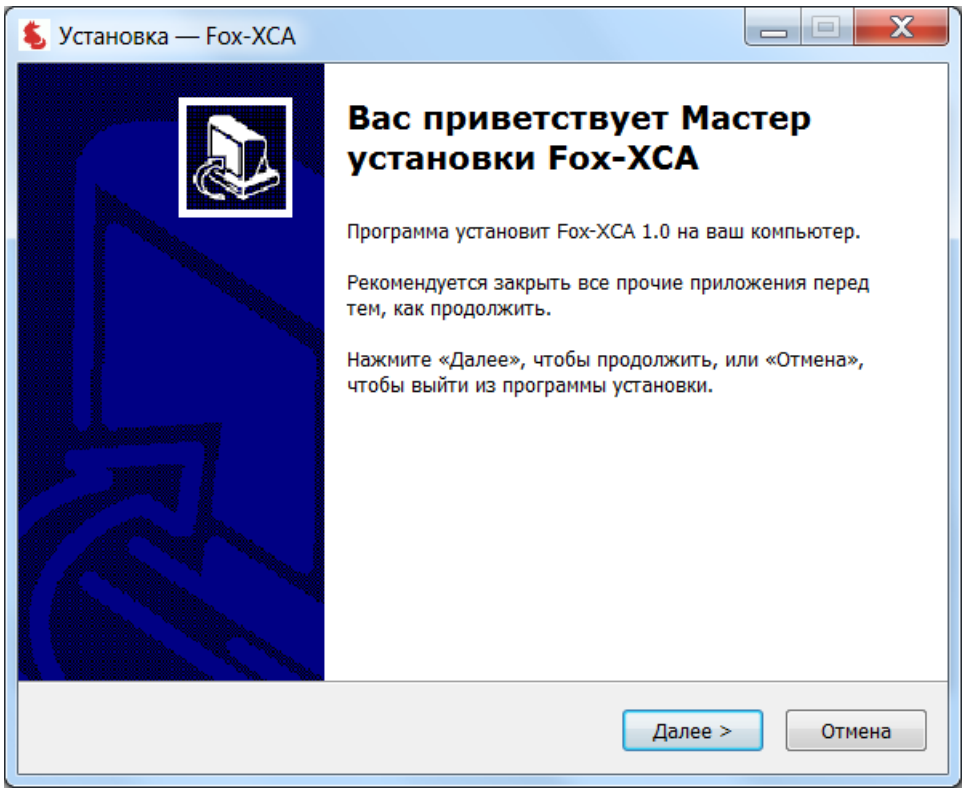

Рис. 1: Окно мастера установки «Fox-XCA»

2.2 Установка в ОС Linux

Для установки ПК «Fox-XCA» в ОС Linux необходимо от имени суперпользователя ***root*** запустить инсталлятор командой
#sh ./foxxca_install.sh
и следовать инструкциям мастера установки.

2.3 Инициализация установленной системы

После установки системы и до того, как вы сможете ее использовать, необходимо провести инициализацию.

Инициализация ПК «Fox-XCA» производится через интерфейс администратора.

Для входа в интерфейс администратора необходимо запустить ПК «Fox-XCA», выбрав соответствующий пункт меню:

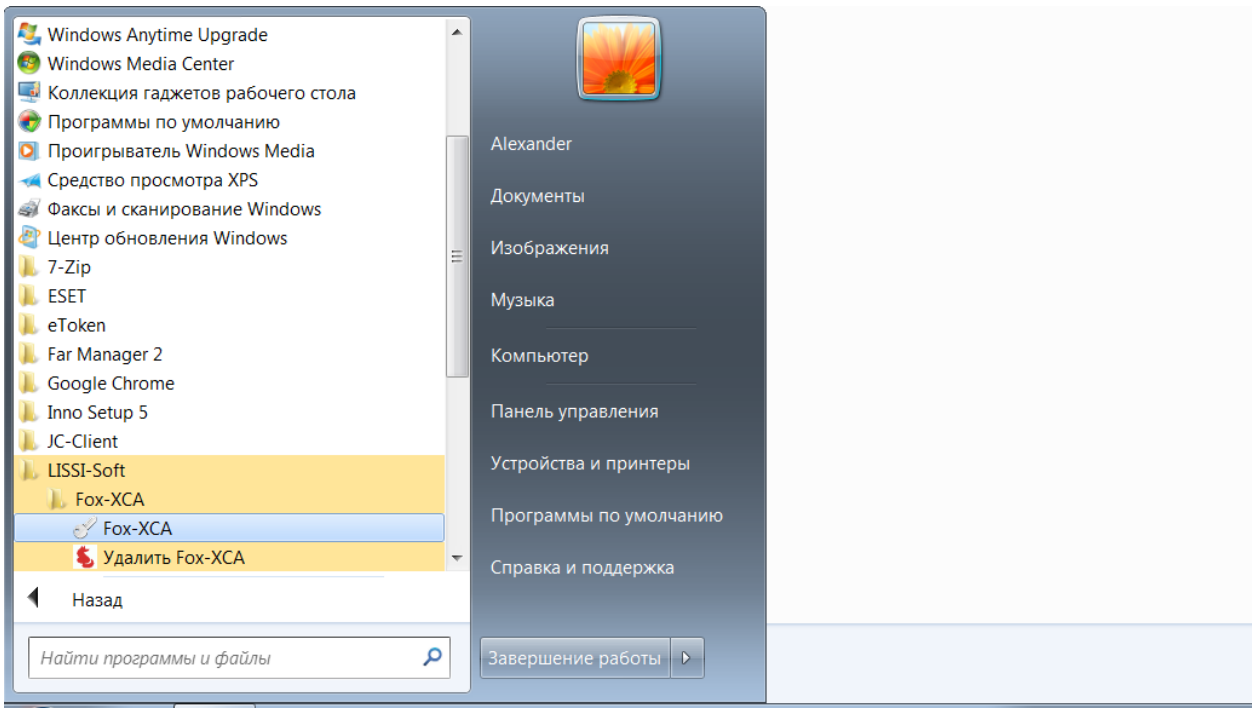

Рис. 2: Ярлык запуска ПК «Fox-XCA»

Инициализация проводится в 2 этапа:

- создание базы данных;
- создание самоподписанного сертификата УЦ.

Этап 1

После запуска ПК «Fox-XCA» появится главное окно интерфейса администратора.

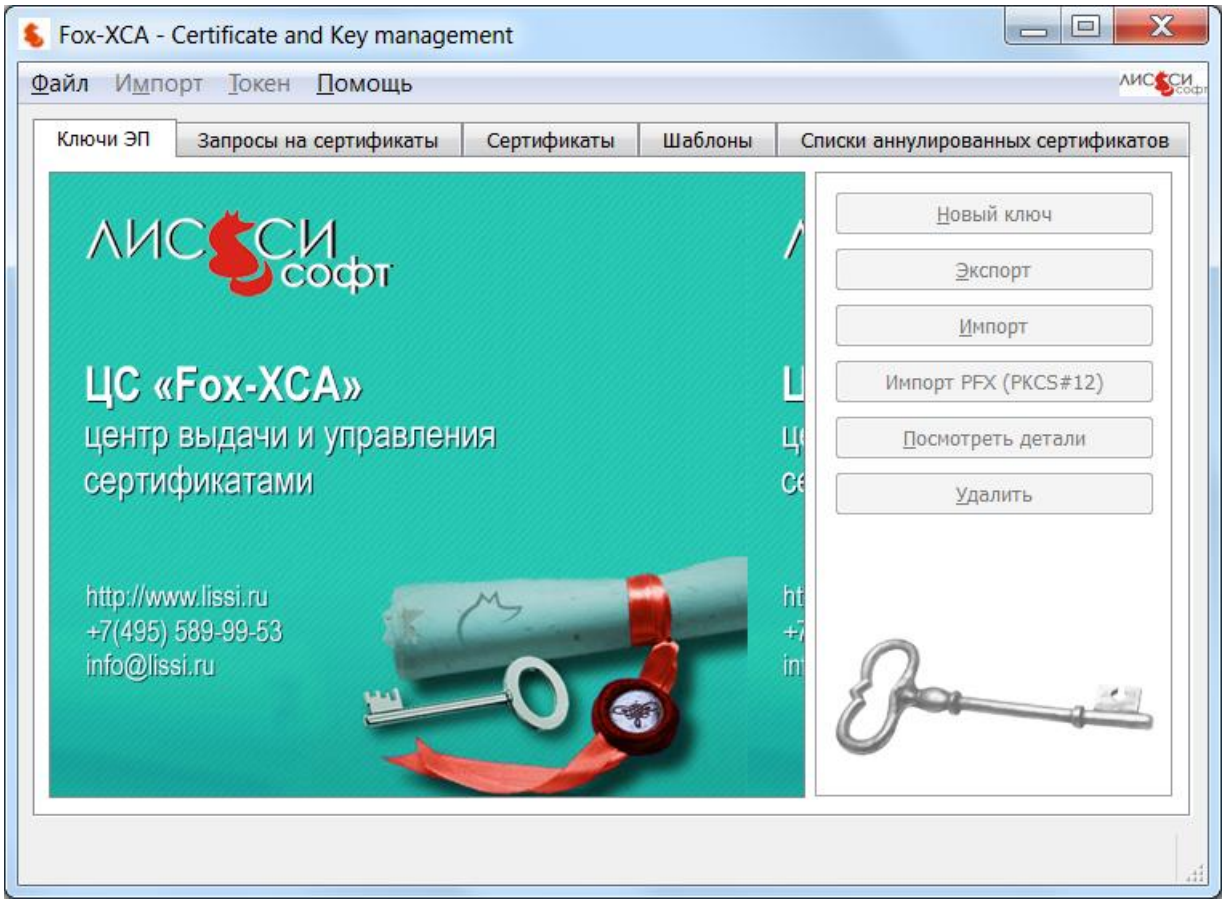

Рис. 3: Главное окно интерфейса администратора

Далее необходимо выбрать пункт меню «Файл→Новая база данных», после чего откроется диалоговое окно создания новой базы данных.

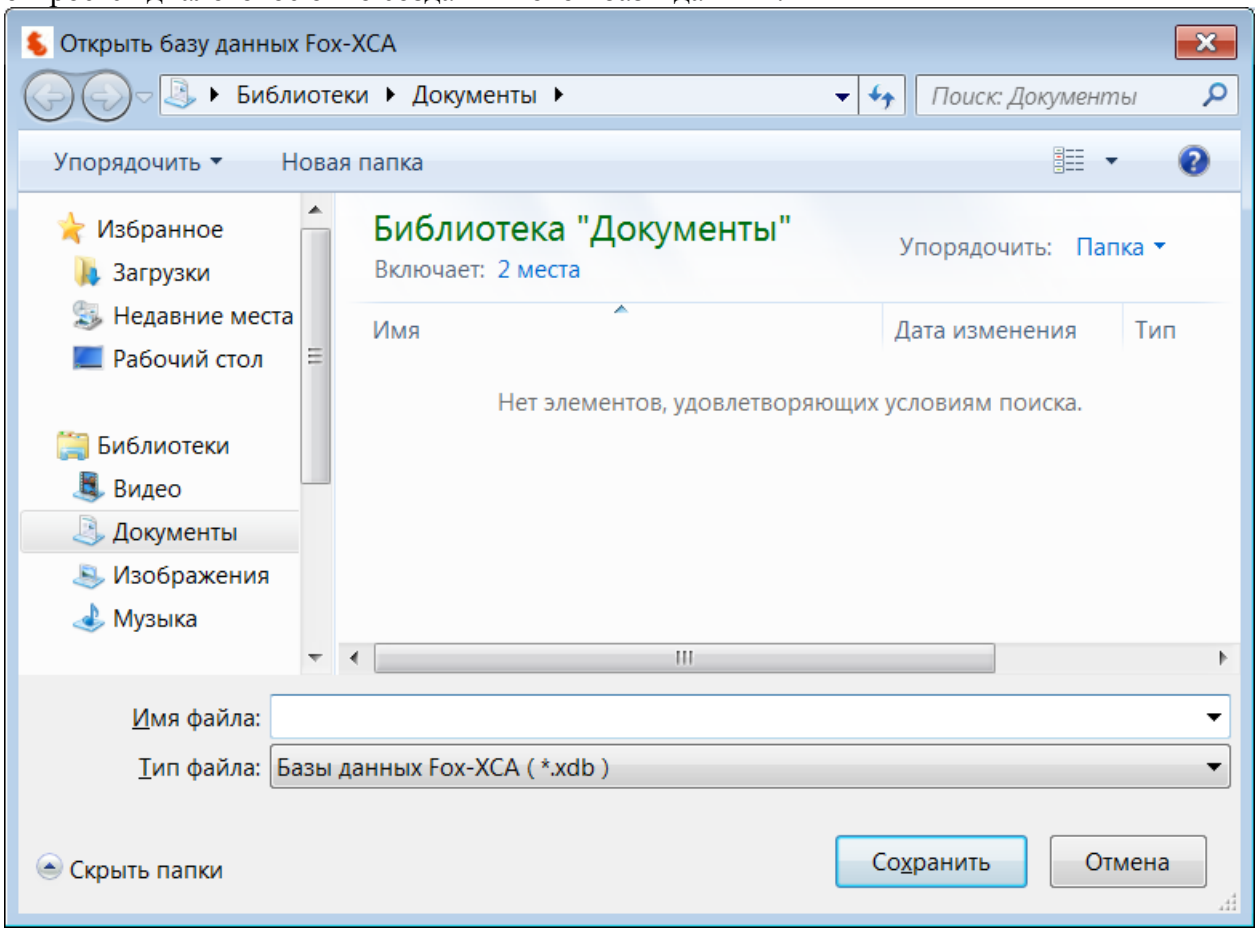

Рис. 4: Диалог создания новой БД

В появившемся диалоге необходимо задать путь и имя файла новой БД и нажать кнопку «Сохранить».

После этого необходимо задать пароль на новую БД.

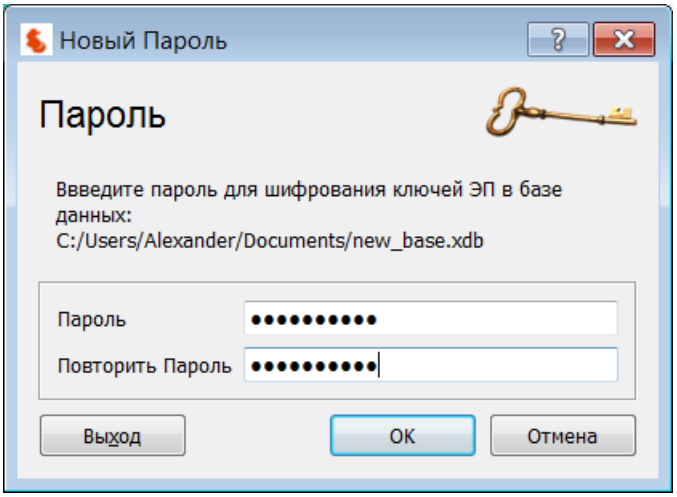

Рис. 5: Диалог задания пароля на новую БД

После этого появится окно интерфейса администратора с открытой вкладкой «Ключи ЭП».

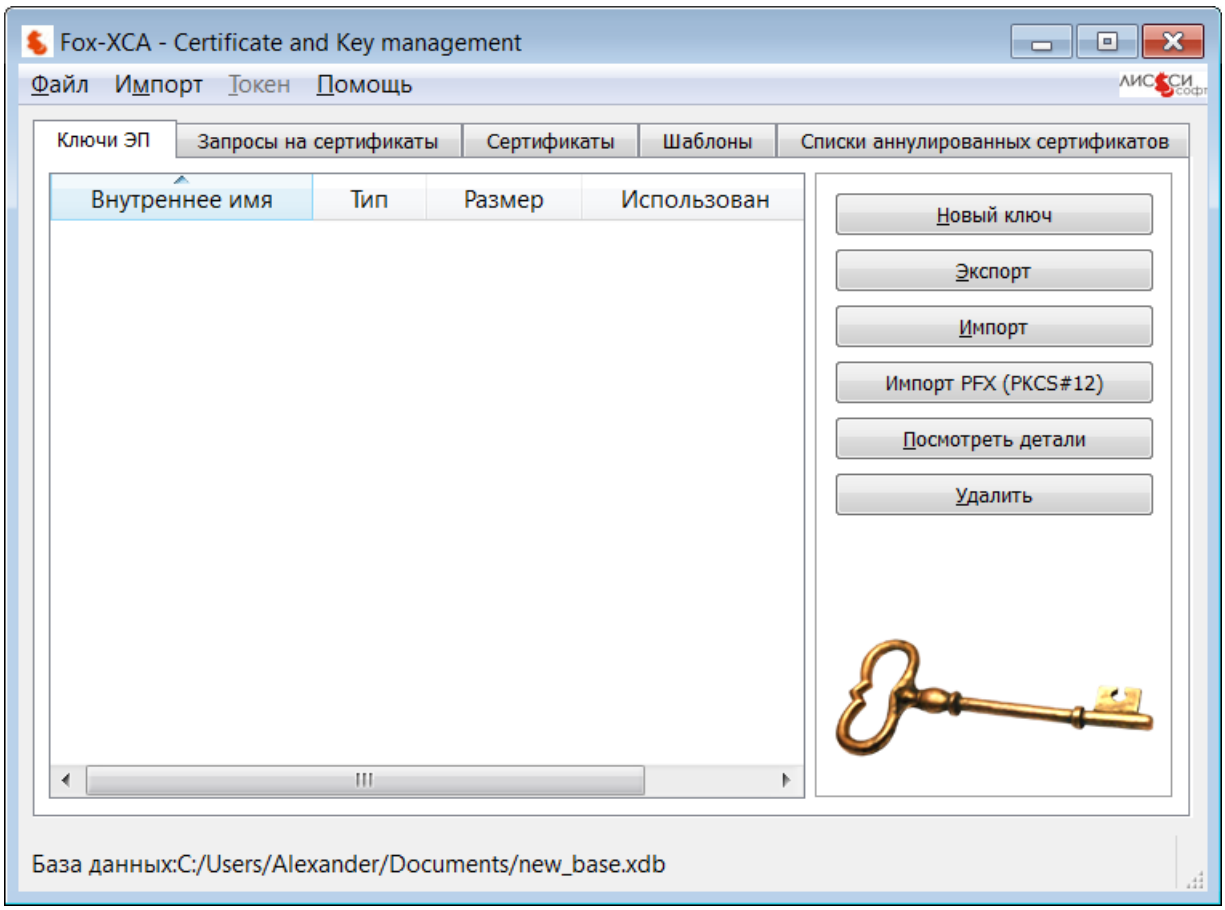

Рис. 6: Вкладка «Ключи ЭП» интерфейса администратора

На этом первый этап инициализации завершен.

Этап 2

Для создания самоподписанного сертификата УЦ необходимо выполнить следующие действия:

- сформировать новый ключ ЭП;
- создать новый запрос на сертификат;
- создать сертификат УЦ.

Для создания нового ключа ЭП необходимо нажать на кнопку «Новый ключ» во вкладке «Ключи ЭП» (рис. 6) и заполнить появившуюся форму (рис. 7), в которой следует задать имя ключа, выбрать используемый алгоритм и, если это необходимо, длину ключа.

Имя ключа должно начинаться с буквы.

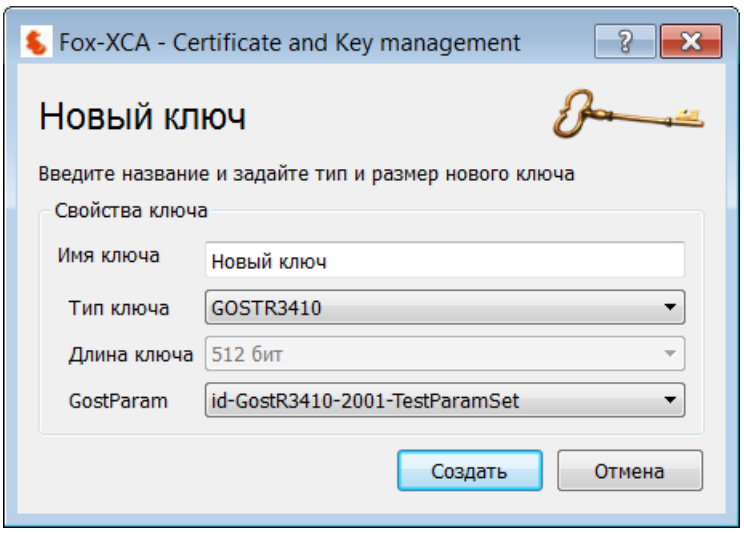

Рис. 7: Диалоговое окно «Новый ключ»

Затем необходимо создать новый запрос на сертификат. Для этого необходимо нажать кнопку «Новый запрос» во вкладке «Запросы на сертификаты» (рис. 8).

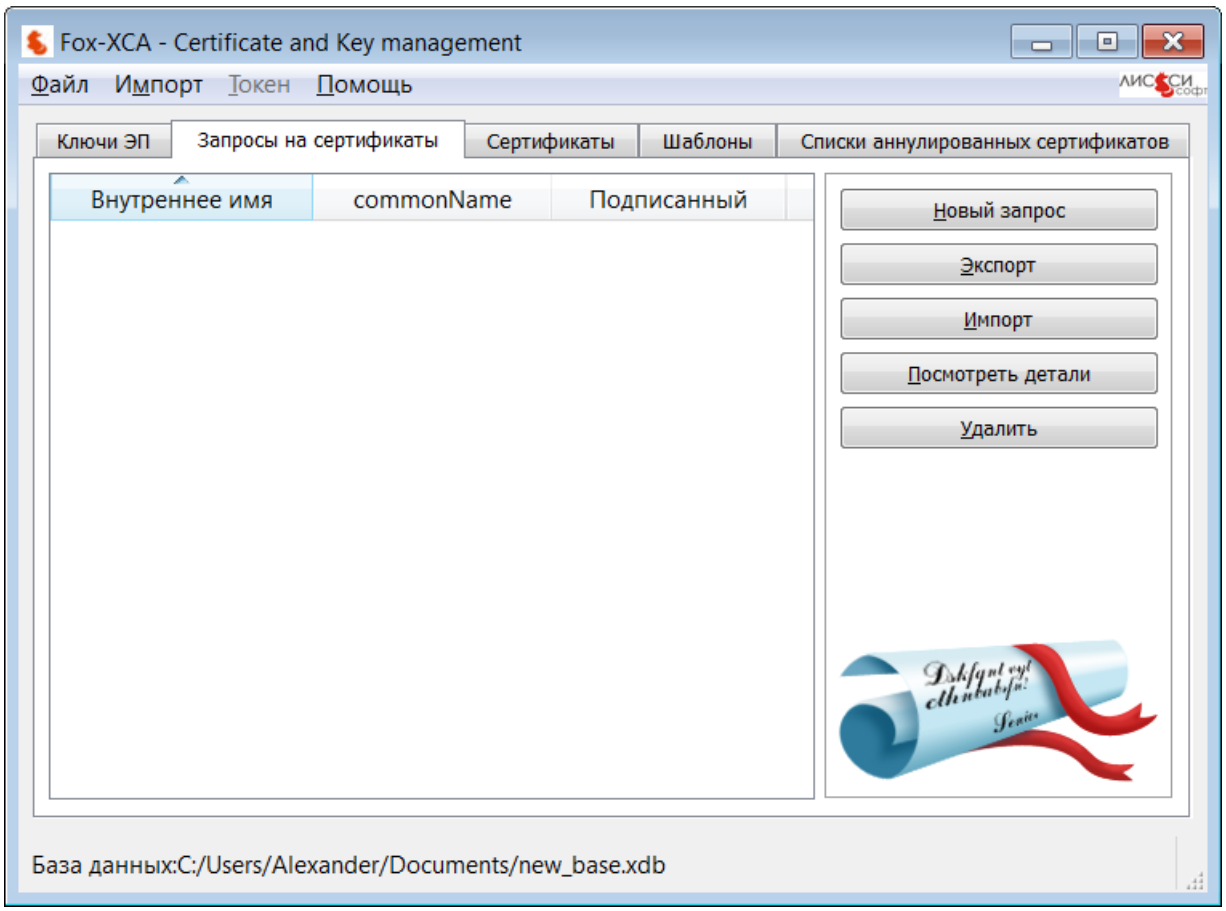

Рис. 8: Вкладка «Запросы на сертификаты» интерфейса администратора

В открывшемся диалоговом окне необходимо задать следующие параметры:

- во вкладке «Владелец» заполнить поля в разделе «Отличительное имя»;
- во вкладке «Расширения» задать тип основных ограничений «Центр Сертификации» и отметить флаг «Критичное»;

- во вкладке «Область применения ключа» выбрать в качестве применения ключа «Подписывание сертификатов» и «Подписывание списка отзыва (CRL)» и отметить флаг «Критичное».

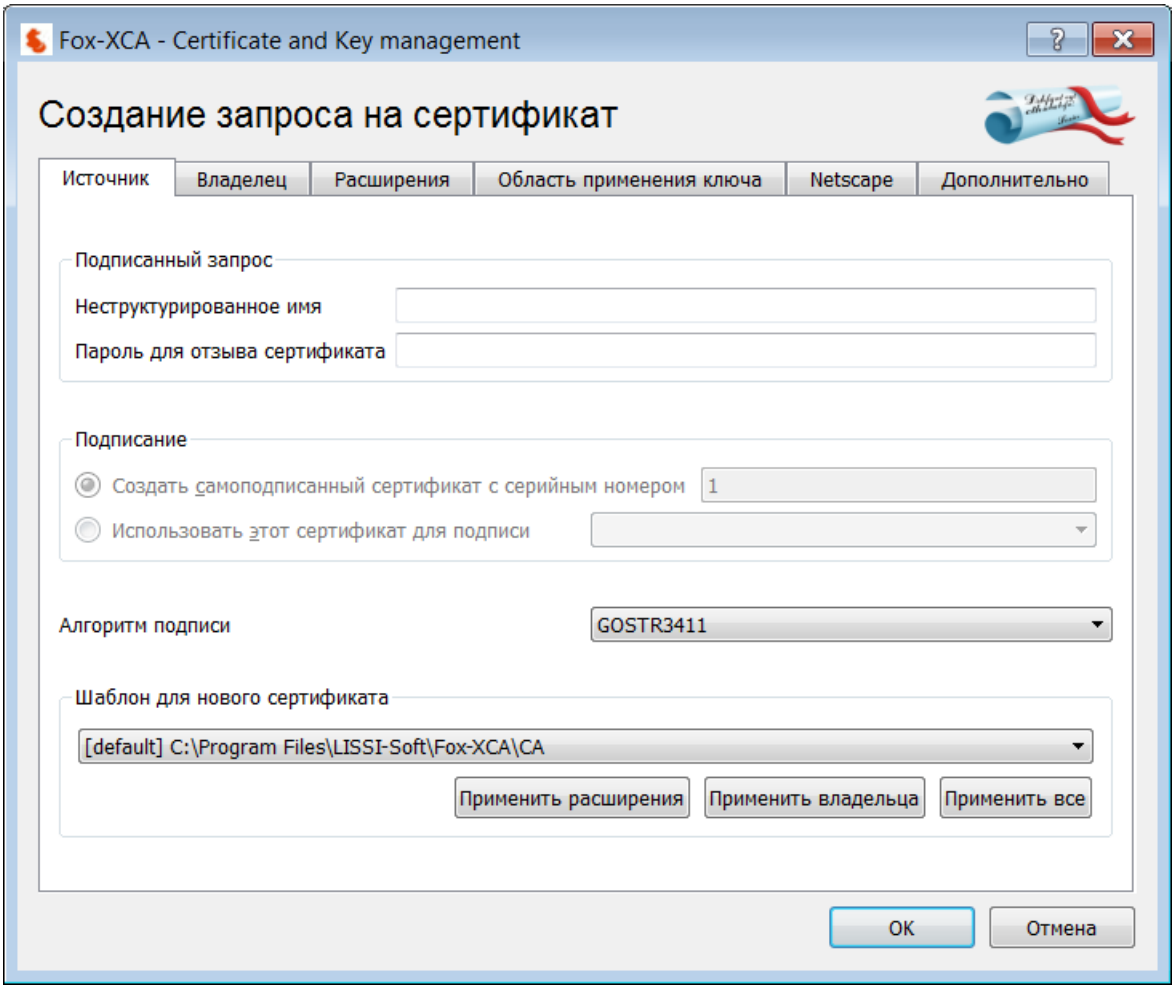

Рис. 9: Диалоговое окно «Создание запроса на сертификат»

Более подробно о параметрах и полях запроса на сертификат рассказывается в пункте 3.4.

После задания всех параметров необходимо нажать кнопку «OK».

Для создания сертификата УЦ необходимо нажать на кнопку «Новый сертификат» во вкладке «Сертификаты» (рис. 10).

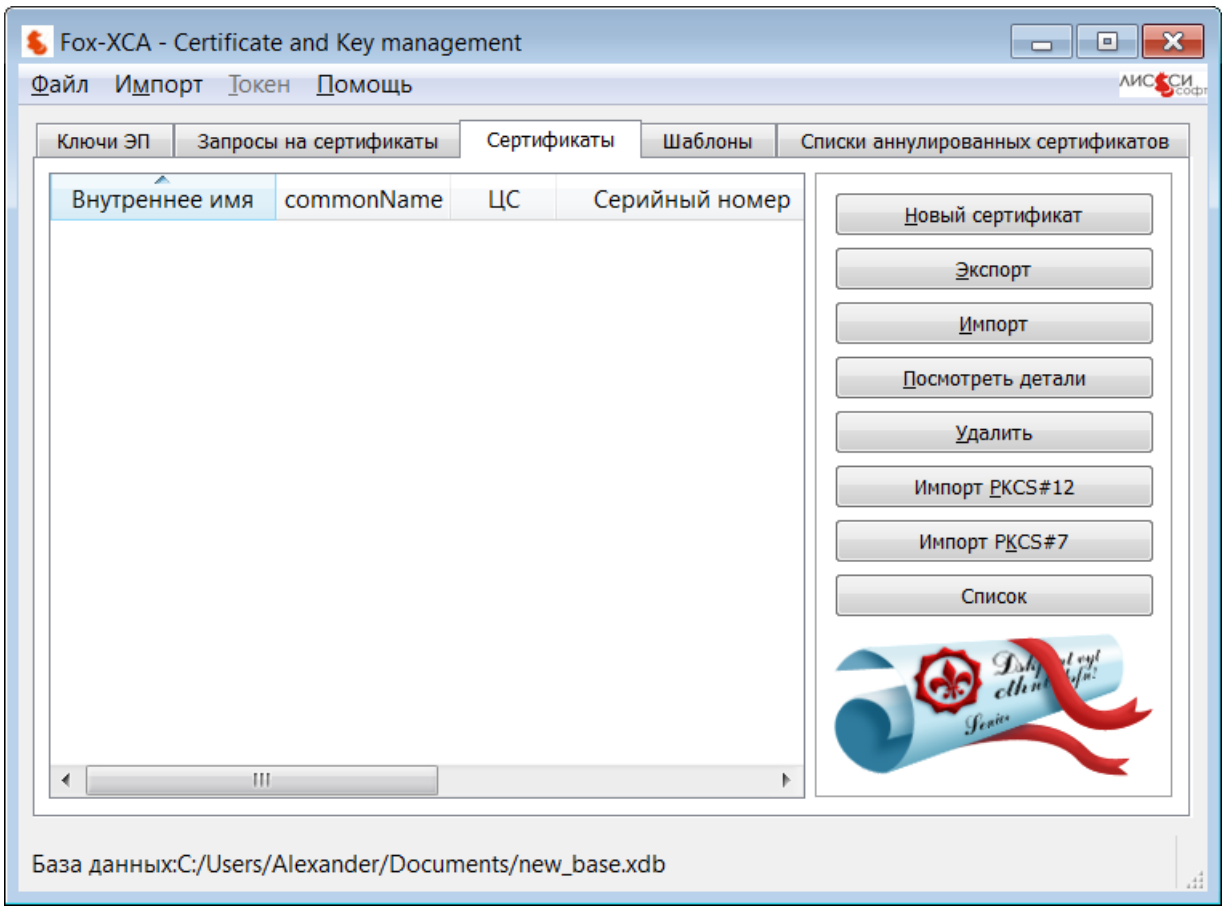

Рис. 10: Вкладка «Сертификаты» интерфейса администратора

После этого появится диалоговое окно создания сертификата.

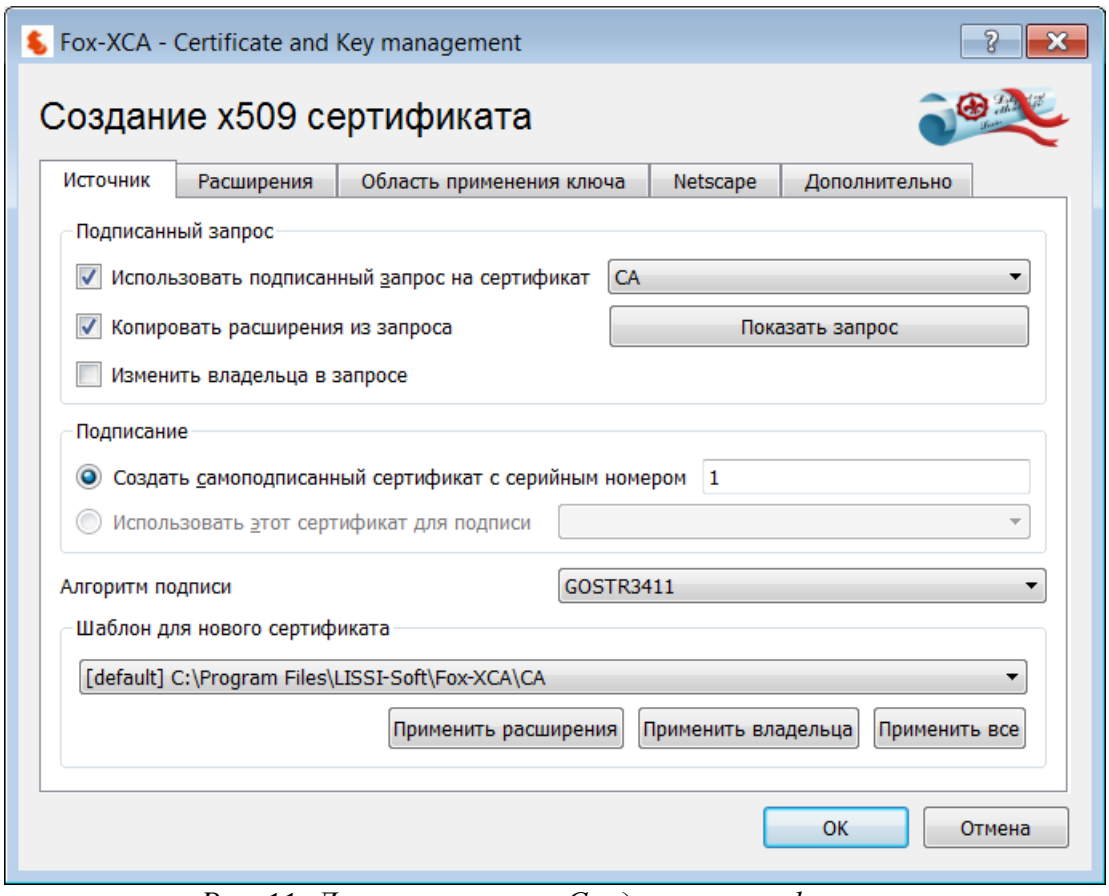

Рис. 11: Диалоговое окно «Создание сертификата»

В появившемся окне необходимо отметить флаг «Использовать подписанный запрос на сертификат», и выбрать в выпадающем списке ранее созданный запрос.

После этого необходимо нажать кнопку «ОК» для создания сертификата.

3 Интерфейс администратора

3.1 Общие операции

Многие операции в ПК «Fox-XCA» применимы ко всем объектам, будь то ключи, сертификаты, запросы на сертификаты или списки отозванных сертификатов. Именно такие операции описаны в этом разделе.

3.1.1 Импорт объектов

Импорт объекта может быть произведен как с помощью кнопки «Импорт», находящейся справа, так и с помощью контекстного меню, которое появляется при нажатии правой клавиши мыши на объекте. Функция импорта достаточно интеллектуальна - она пробует разобрать содержимое файла, используя все известные форматы, независимо от расширения файла. Список известных форматов:

- **Ключи** - PEM закрытый ключ, PEM открытый ключ, DER закрытый ключ, DER открытый ключ, PKCS#8 закрытый ключ;
- **Запросы на сертификаты** - DER запрос, PEM запрос, Netscape SPKAC запрос;
- **Сертификаты** - DER сертификат, PEM сертификат (PKCS#12 и PKCS#7 сертификаты должны импортироваться с помощью дополнительных кнопок, потому что эти форматы могут содержать более одного сертификата и ключа).

После выбора имени файла, ПК «Fox-XCA» попробует все известные форматы для данного типа объектов и, в случае неудачи, выведет сообщение об ошибке. Также существует возможность выбирать сразу несколько файлов с помощью клавиши SHIFT.

Кроме того, с помощью меню **«Импорт»** можно загрузить объект из файла. Помимо обычных функции импорта, в этом меню есть функция импорта PEM-файла. Так как формат PEM содержит описание объекта, который в нем находится, то с помощью этой функции вы можете загрузить объект из PEM-файла, будь то ключ, список отозванных сертификатов, сертификат или запрос на сертификат. Функция импорта PEM-файлов сама определит, к какому типу относится объект, и загрузит его.

Когда загружается более одного объекта, все загружаемые объекты отображаются в окне мульти-импорта. Когда происходит импорт PKCS#7 или PKC#12, все импортируемые объекты также отображаются в окне мульти-импорта. В этом окне вы можете просмотреть объекты и решить - импортировать их или нет.

После загрузки объектов, ПК «Fox-XCA» ищет в своей базе данных этот объект. Если такой объект уже существует в базе, выводится сообщение, в котором указывается имя этого объекта в базе.

3.1.2 Детальная информация об объекте

Окно с детальной информации об объекте можно открыть, два раза кликнув мышкой на объекте, с помощью контекстного меню или с помощью кнопки «Просмотреть детали», находящейся справа. В этом окне можно, два раза кликнув на имени сертификата издателя или на имени соответствующего ключа, посмотреть детальную информацию о них.

3.1.3 Переименование объекта

Объект может быть переименован с помощью контекстного меню или с помощью нажатия клавиши <F2>. Если при переименовании объекта выяснится, что такое имя в базе уже есть, ПК «Fox-XCA» добавит к имени «_01», чтобы сохранить уникальность имен в базе.

3.1.4 Уничтожение объектов

Объекты могут быть уничтожены с помощью кнопки «Уничтожить» или с помощью контекстного меню. Если вы удаляете сертификат, созданный с помощью ПК «Fox-XCA», вам будет выдано предупреждение. Дело в том, что вы не сможете отозвать удаленный сертификат. Таким образом, удаляйте только те сертификаты, выданные вами, которые вы не экспортировали. Запросы на сертификаты можно удалять сразу после издания сертификатов, так как запрос можно восстановить из сертификата с помощью функции экспорта сертификата в запрос. Но это возможно, только если у вас есть закрытый ключ для данного сертификата. Для удаления можно выбирать сразу несколько объектов.

3.2 Управление закрытыми ключами

3.2.1 Создание

Перед созданием закрытого ключа необходимо перейти на вкладку «Ключи ЭП» интерфейса администратора.

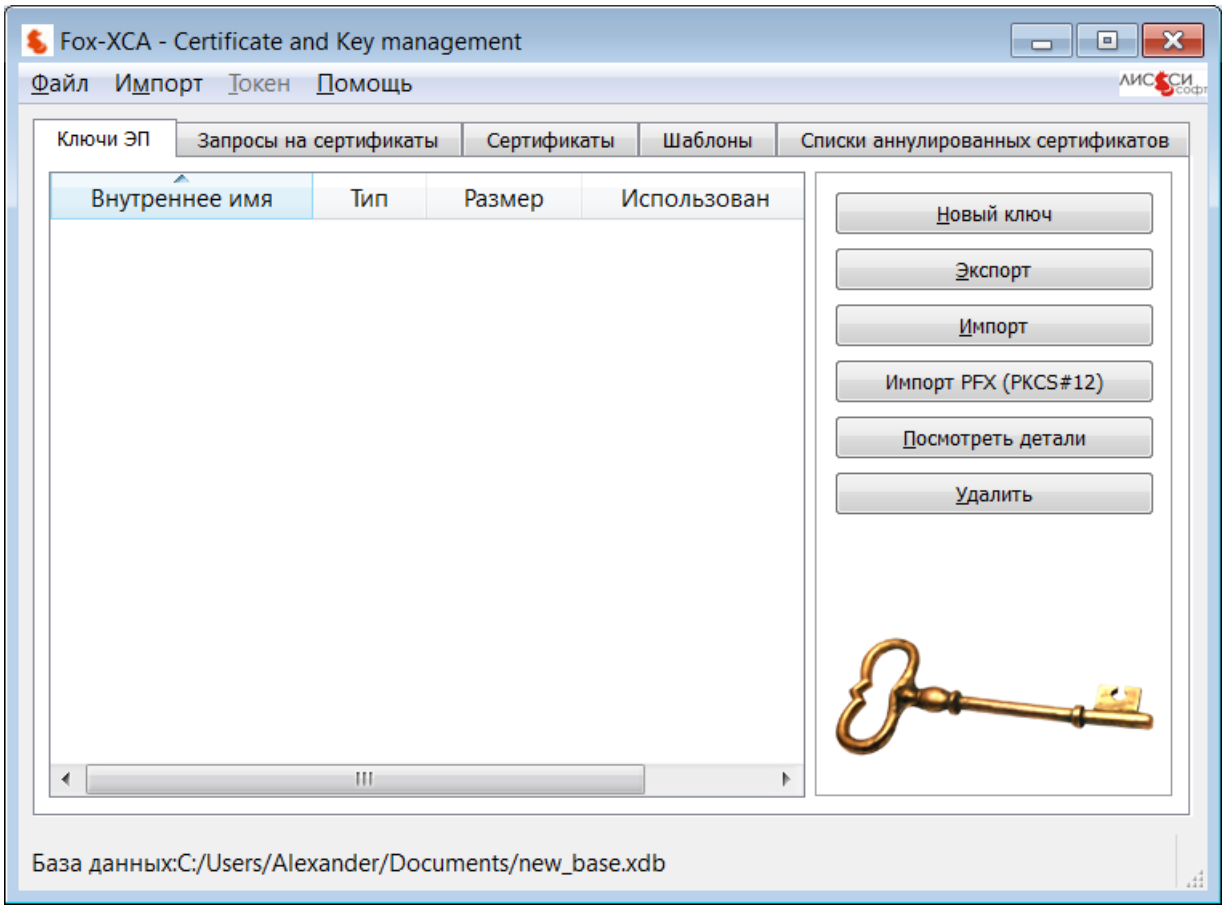

Рис. 12: Вкладка «Ключи ЭП» интерфейса администратора

Для создания нового закрытого ключа необходимо нажать на кнопку «Новый ключ» и заполнить появившуюся форму (рис. 13), в которой следует задать имя ключа, выбрать используемый алгоритм и, если это необходимо, длину ключа (только для алгоритмов RSA и DSA).

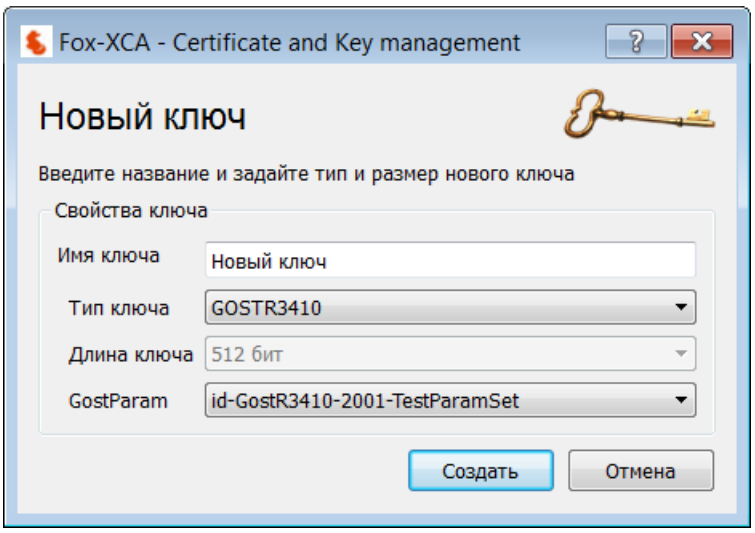

Рис. 13: Диалоговое окно «Новый ключ»

3.2.2 Экспорт

Ключи можно экспортировать, выбрав нужный ключ в списке и нажав кнопку «Экспорт», или с помощью контекстного меню. После этого появится диалоговое окно экспорта ключа.

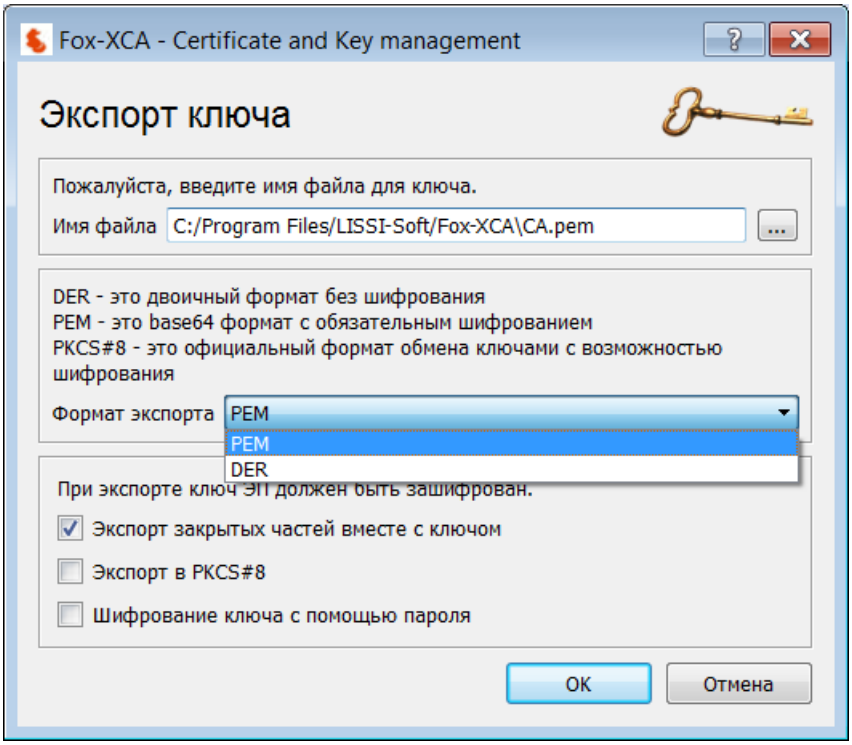

Рис. 14: Диалоговое окно «Экспорт ключа»

В нем задаются:

- имя файла;
- формат (DER, PEM);
- экспортировать также закрытый ключ;
- экспорт в PKCS#8;
- необходимость шифрования ключа с использованием пароля.

Имя файла формируется из внутреннего имени ключа плюс pem, der или pk8 суффикс. Когда меняется формат экспорта, суффикс также меняется. Только форматы PKCS#8 или PEM могут быть зашифрованы, потому что формат DER (хотя он может быть зашифрован) не поддерживает возможности задать параметры шифрования. Конечно, шифрование не имеет значения, если вы экспортируете только открытый ключ.

3.3 Управление запросами на сертификат

Запрос на сертификат описан в стандарте PKCS#10. Он используется для передачи Удостоверяющему центру всей необходимой информации для издания сертификата, но не содержит ключ ЭП. В запросе содержится вся персональная информация, ваш ключ проверки ЭП и расширения для сертификата.

Запросы в формате Netscape SPKAC нельзя создать или экспортировать, но их можно импортировать и подписывать. Такие запросы помечаются в таблице как SPKAC и им задается иконка «Netscape».

3.3.1 Создание

Для создания нового запроса на сертификат необходимо нажать на кнопку «Новый запрос» во вкладке «Запросы на сертификаты».

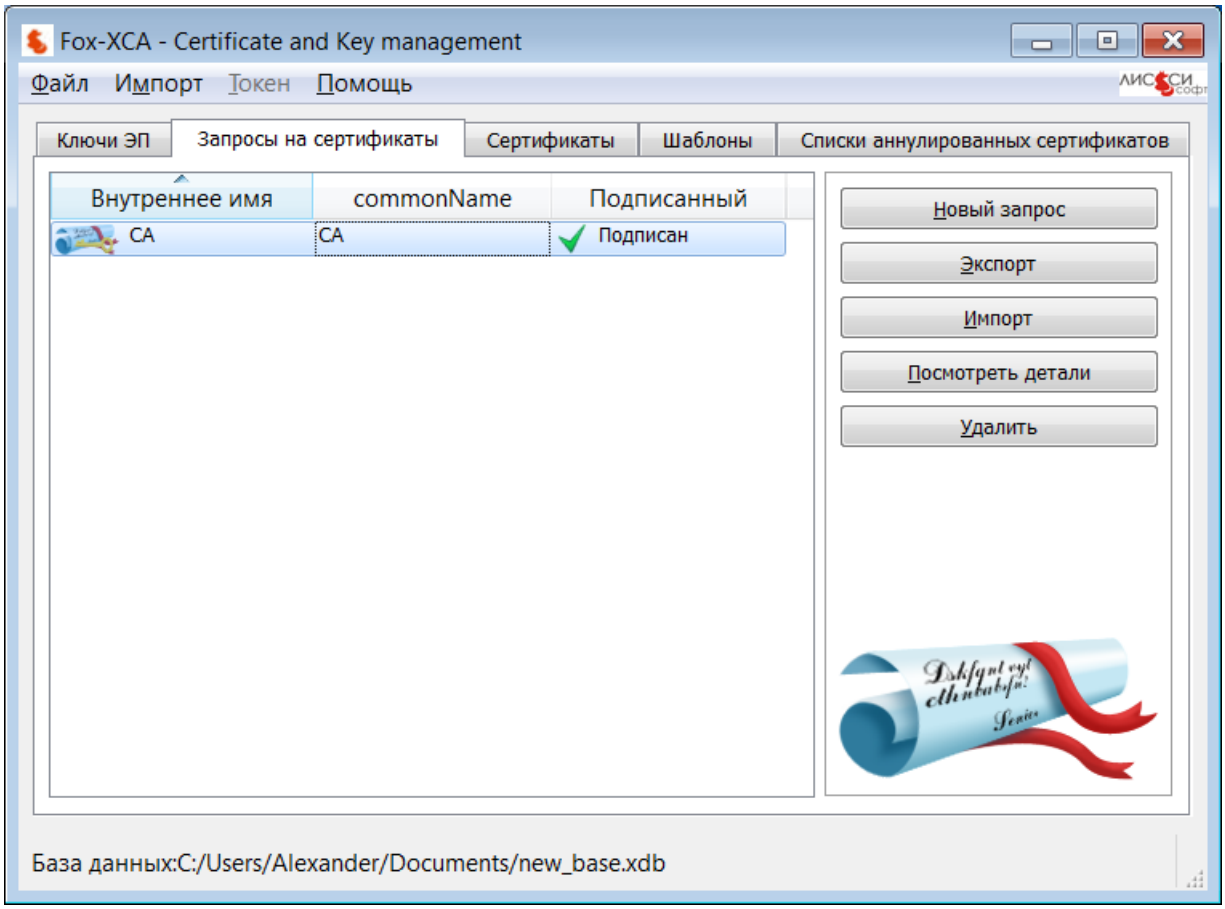

Рис. 15: Вкладка «Запросы на сертификаты» интерфейса администратора

Откроется окно создания запроса на сертификат, где вы можете ввести всю необходимую информацию для создания нового запроса (см. главу 3.4.2).

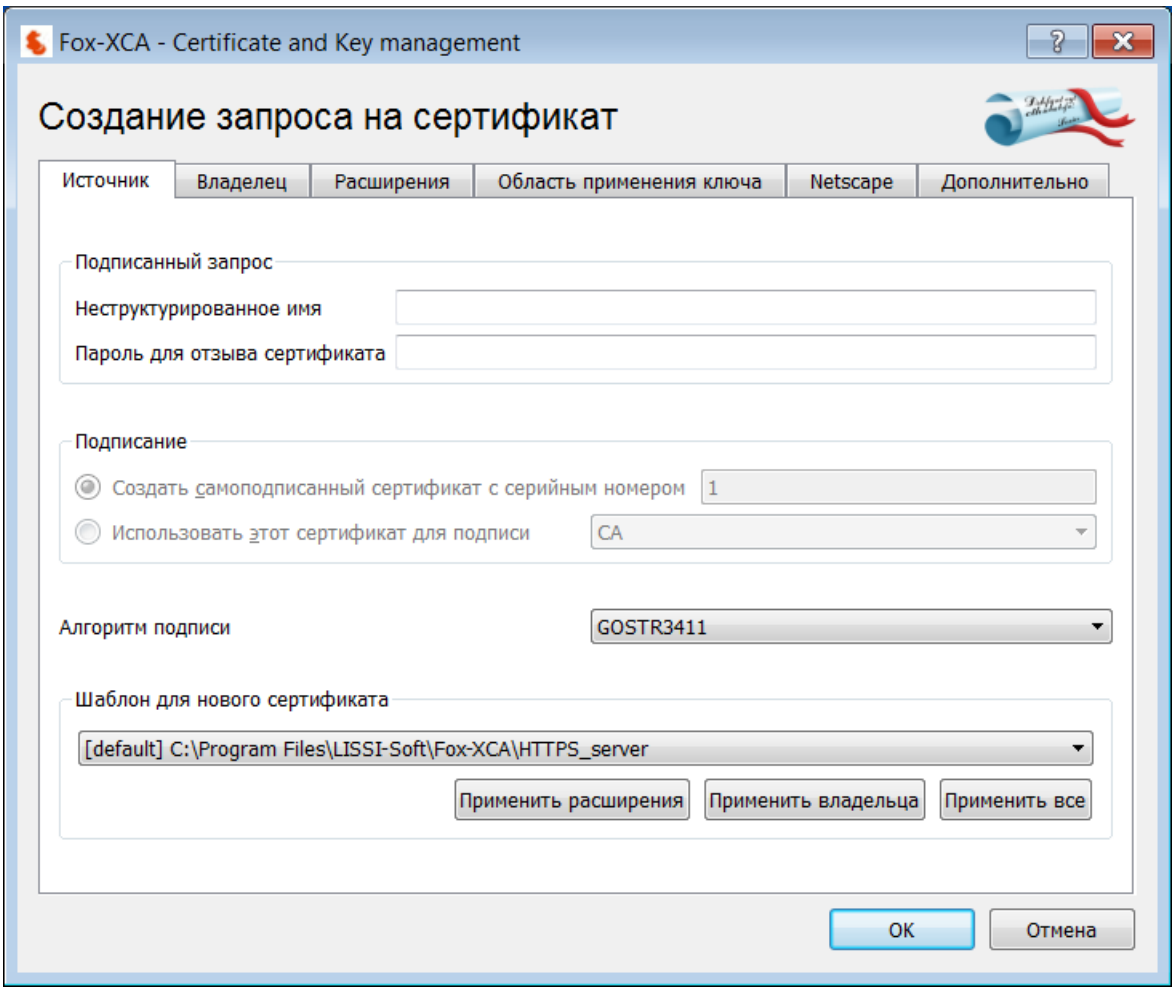

Рис. 16: Диалоговое окно «Создание запроса на сертификат»

Вкладка «Источник»

Единственным отличием при создании запроса на сертификат от собственно создания сертификата являются поля «Неструктурированное имя» и «Пароль для отзыва сертификата» во вкладке «Источник».

Неструктурированное имя – имя или имена владельца сертификата в виде неструктурированной ASCII строки (интерпретация данных имен определяется издателем сертификата). Это поле является не обязательным.

Пароль для отзыва сертификата – пароль, по которому впоследствии можно будет отозвать сертификат.

Также можно сформировать запрос на сертификат из уже существующего сертификата с помощью пункта контекстного меню сертификата (Экспорт→Запрос). Этот пункт меню доступен только тогда, когда в базе есть ключ ЭП от этого сертификата. В этом случае вся необходимая информация копируется из сертификата, и «Мастер создания запросов» не используется.

3.3.2 Экспорт

Запрос может быть экспортирован с помощью кнопки «Экспорт» или через контекстное меню. Имя и формат файла могут быть выбраны в появившемся окне.

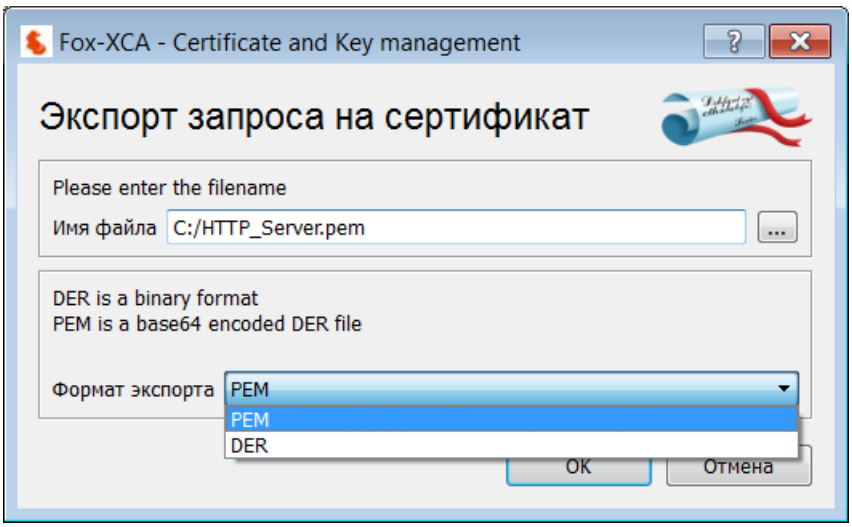

Рис. 17: Диалоговое окно экспорта запроса на сертификат

3.4 Управление сертификатами

3.4.1 Просмотр

Все сертификаты в базе отображаются во вкладке «Сертификаты» в виде древовидной структуры, отражающей цепочку сертификации. Если сертификат является сертификатом УЦ, и есть несколько сертификатов, выданных этим УЦ, то выданные сертификаты будут отображаться после нажатия на символ «плюс» слева от имени сертификата УЦ.

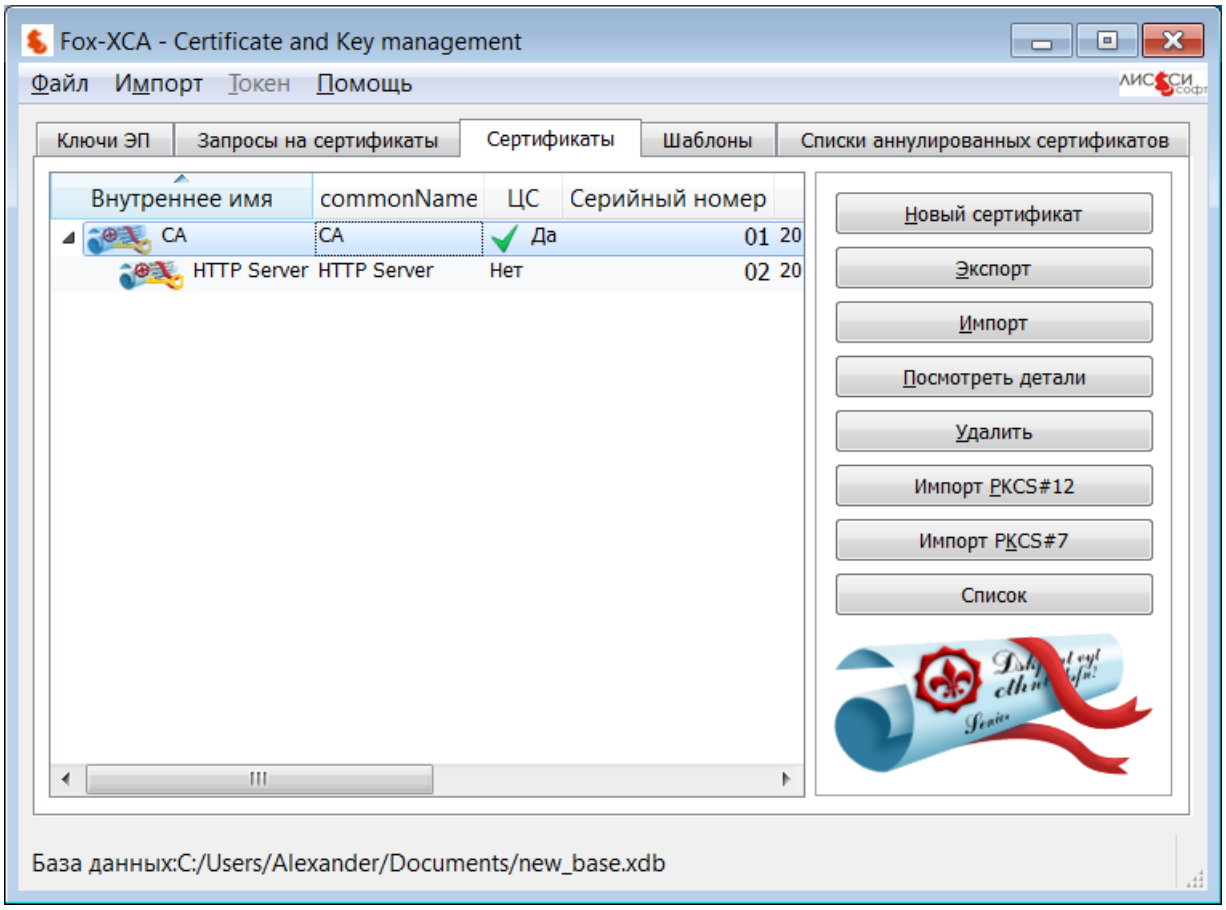

Рис. 18: Вкладка «Сертификаты» интерфейса администратора

3.4.2 Создание

Чтобы создать сертификат необходимо перейти на вкладку «Сертификаты» в интерфейсе администратора и нажать кнопку «Новый сертификат». Появится диалоговое окно создания сертификата.

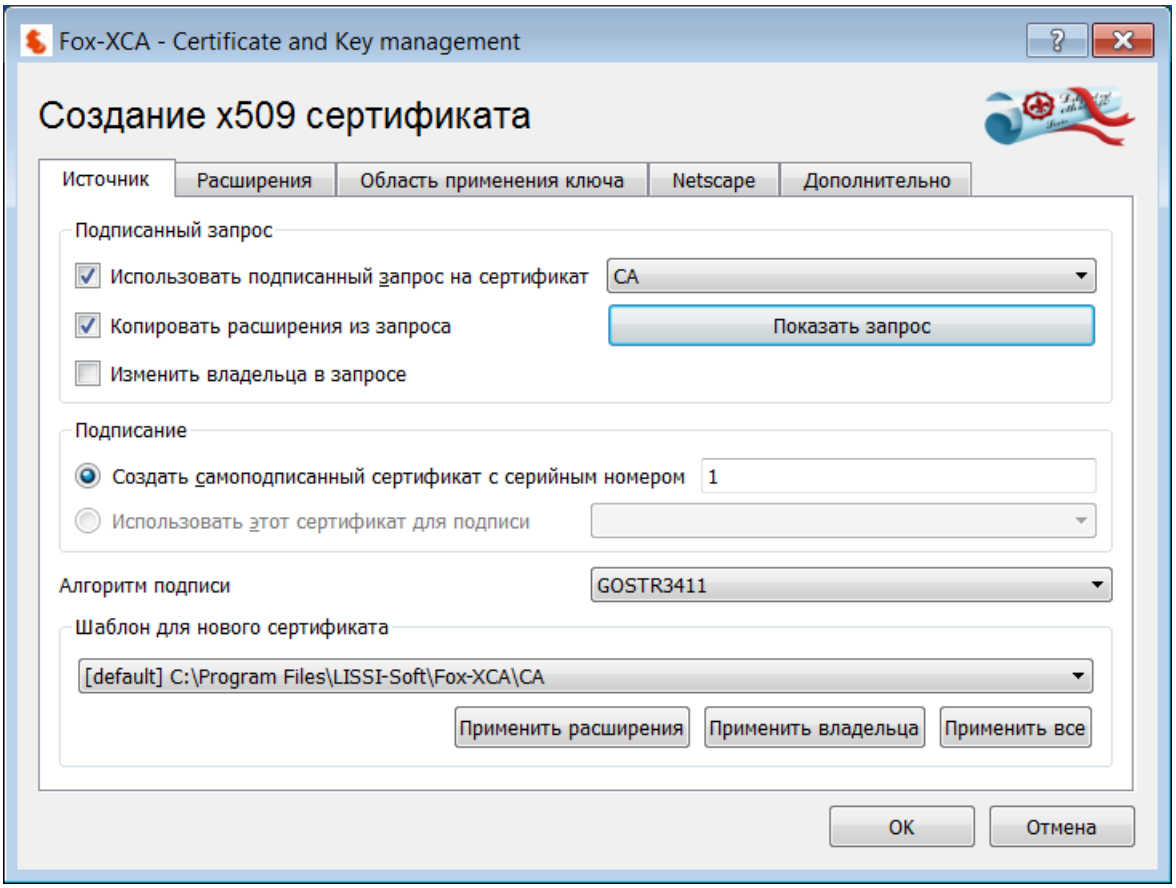

Рис. 19: Диалоговое окно «Создание сертификата»

Вкладка «Источник»

Подписанный запрос

Если сертификат создается из запроса с помощью сертификата УЦ или из запроса создается самоподписанный сертификат, запрос можно выбрать здесь. В случае создания самоподписанного сертификата, в базе должен быть ключ ЭП, соответствующий данному запросу.

Флаг «Копировать расширения из запроса» позволяет использовать заданные в запросе расширения в создаваемом сертификате.

Подписание

Здесь можно выбрать, будет ли создан самоподписанный сертификат или будет создан обычный сертификат с помощью выбранного из списка сертификата УЦ. В выпадающем меню отображаются только те сертификаты УЦ, для которых доступен ключ ЭП.

Алгоритм подписи

Обычно следует использовать SHA256 или выше, но так как старые версии Windows (включая XP) не могут с ними работать, пользователям Windows следует использовать либо SHA1, либо GOSTR3411 в случае использования ключей, созданных с использованием алгоритма ГОСТ Р 34.10-2001.

Шаблоны

Поля сертификата могут быть заполнены из шаблона, для этого необходимо выбрать шаблон из списка и нажать кнопку «Применить» (подробную информацию о шаблонах см. в пункте 3.5).

Вкладка «Владелец»

Эта вкладка не появляется, если подписывается запрос на сертификат, потому что запрос содержит всю необходимую информацию, вводимую на этой вкладке.

Отличительное имя

В этом блоке могут быть введены все персональные данные - страна, имя, адрес электронной почты и т.д. Необходимым полем является только «Внутреннее имя». Поле «Код страны» должно быть либо пустым, либо содержать две латинские буквы; например RU для России. Если вы создаете сертификат для SSL-сервера, в поле «Общее имя» вам следует вписать DNS-имя сервера.

Другие редко используемые поля персональных данных могут быть выбраны в выпадающем меню. В сертификат добавятся только те поля, которые были добавлены с помощью кнопки «Добавить». Любые поля могут быть добавлены сколько угодно раз. Это редко используется, но это возможно.

Ключ ЭП

Ключи можно сгенерировать прямо в этом окне «на лету» с помощью кнопки «Создать новый ключ». Сгенерированный ключ будет добавлен в базу, даже если впоследствии создание сертификата или запроса будет отменено. Выпадающее меню содержит только те ключи, которые еще не были использованы в других запросах или сертификатах. Чтобы использовать уже использованные ключи поставьте галочку «Отображать уже использованные ключи». Список ключей недоступен, если создается или изменяется шаблон.

Вкладка «Расширения»

Следующие 3 вкладки содержат все возможные поля расширений для сертификата.

Основные ограничения

Если задан тип «Центр Сертификации», сертификат будет определяться ПК «Fox-XCA» и другими приложениями как сертификат УЦ. Сертификаты серверов и сертификаты для электронной почты должны иметь значение этого поля «Конечный пользователь» (строго рекомендуется) или вообще не содержать этого поля («Не определен»).

Параметр «Длина пути» задает максимально допустимое количество сертификатов УЦ, которые могут быть в одной цепочке с данным сертификатом. Поэтому если параметр «Длина пути» будет равен «0», он может быть использован только для подписи сертификатов конечных пользователей, но не дополнительных сертификатов УЦ.

Флаг «Критичное» (здесь и далее)

Сообщает приложению, использующему сертификат, может ли оно игнорировать данный тип расширения. Если расширение задано как критичное, а приложение не распознает данный тип расширения, приложение должно отвергнуть сертификат. С другой стороны, если расширение определено как некритичное, а приложение не распознает данный тип расширения, приложение без опасений может игнорировать расширение и использовать сертификат.

Идентификатор ключа

Идентификатор ключа владельца

Это расширение используется для различения многочисленных ключей подписи сертификатов одного и того же владельца сертификата. Владелец предоставляет уникальный идентификатор ключа либо предоставляет указатель на другой сертификат, который может удостоверять ключ издателя. RFC 2459 обязывает использовать это поле для всех подписываемых УЦ сертификатов, а также рекомендует применять его для конечных пользователей.

Идентификатор ключа ЦС

Это расширение используется для различения многочисленных ключей подписи сертификатов одного и того же УЦ. УЦ предоставляет уникальный идентификатор ключа или предоставляет указатель на другой сертификат, который может удостоверить ключ издателя. RFC 2459 обязывает использовать это поле для любого сертификата, который не является самоподписанным.

Период действия

Это поле содержит два значения типа дата/время: «Не раньше» и «Не позже». Эти значения определяют период, на протяжении которого данный сертификат считается действительным, если не будет отозван.

Поле «Не раньше» выставляется на текущие дату и время операционной системы, а поле «Не позже» выставляется на текущие дату и время плюс определенный период времени.

Для шаблонов заданные даты и время не сохраняются, так как от них нет никакой пользы. Зато сохраняется «Временной диапазон» и он автоматически применяется, когда выбран шаблон. Применение периода времени означает, что «Не раньше» выставляется в «сейчас», а «Не позже» выставляется в «сейчас + период времени». Если галочка «Полночь» выставлена, обе даты будут приведены к 12 часам ночи.

Альтернативное имя владельца

Это расширение задает одно или несколько альтернативных форм имен, связанных с владельцем данного сертификата. Использование данного поля дает возможность поддерживать различные приложения, которые используют свои собственные формы имен, включая различные программы для работы с электронной почтой, средства электронного обмена данными и IPSec.

Альтернативными именами могут выступать:

- Email – адрес email;
- URI - унифицированный идентификатор ресурса;
- DNS – имя домена Internet;
- RID - registered ID: OBJECT IDENTIFIER;
- IP - IP адрес;
- otherName.

IP адрес может быть задан как в формате IPv4, так и в формате IPv6.

Поле **otherName** может включать данные, ассоциированные с OID. В этом случае сначала записывается OID и через двоеточие после него записывается значение в формате ASN1_generate_nconf(3).

Альтернативное имя издателя

Это расширение задает одно или несколько альтернативных форм имен, связанных с издателем данного сертификата. Как и для расширения «Альтернативное имя

владельца», использование этого поля позволяет обеспечить поддержку различными приложениями.

Точка распространения CAC

Это расширение задает *унифицированный идентификатор ресурса (URI)* для указания местоположения структуры CAC, содержащей информацию об отмене данного сертификата. Может быть задано несколько URI.

Способ доступ к информации УЦ

Это расширение предоставляет информацию о том, как получить доступ к некоторой информации, относящейся к УЦ.

Возможен выбор:

- OCSP – Online Certificate Status Protocol, онлайновый протокол состояния сертификата – протокол, используемый для проверки статуса сертификатов X.509;
- Издатель сертификата УЦ.

Для этих объектов можно задать такие же параметры, как и для «Альтернативного имени владельца», кроме «otherName».

Вкладка «Область применения ключа»

Применение ключа

Это расширение применяется для задания ограничений на операции, которые могут выполняться с открытым ключом в составе этого сертификата. К таким операциям относятся:

- Цифровая подпись (Digital Signature)
- Неотрекаемость (Non Repudiation)
- Шифрование ключей (Key Encipherment)
- Шифрование данных (Data Encipherment)
- Согласование ключей (Key Agreement)
- Подписывание сертификатов (Certificate Sign)
- Подписывание CAC (CRL Sign)
- Только шифрование (Encipher Only)
- Только расшифровка (Decipher Only)

Это поле может быть помечено как критичное или как некритичное. Если оно помечено как критичное, открытый ключ в составе этого сертификата может использоваться только по своему назначению. В противном случае будет иметь место нарушение политики УЦ. RFC 2459 рекомендует устанавливать флаг критичности при использовании данного расширения.

Расширенная область применения ключа

Это расширение может быть использовано в дополнение или вместо расширения «Область применения ключа», чтобы определить одно или несколько применений открытого ключа, который удостоверяет данный сертификат. Это расширение дает возможность сертификату взаимодействовать с различными протоколами и приложениями. Допустимые значения:

- TLS Web Server Authentication;
- TLS Web Client Authentication;
- Code Signing;

- E-mail Protection;
- Time Stamping;
- Microsoft Individual Code Signing;
- Microsoft Commercial Code Signing;
- Microsoft Trust List Signing;
- Microsoft Server Gated Crypto;
- Microsoft Encrypted File System;
- Netscape Server Gated Crypto;
- Microsoft EFS File Recovery;
- IPSec End System;
- IPSec Tunnel;
- IPSec User;
- IP security and entity;
- Smart Card Logon.

RFC 2459 указывает, что это поле может быть помечено как критичное или некритичное.

Вкладка «Netscape»

Данные расширения не стандартные, специфичны для продуктов компании Netscape и в основном устаревшие. Их использование на данный момент не имеет смысла.

Это расширение, состоящее из списка флагов. Оно использовалось для задания применения сертификата. На данный момент вместо него используются расширения «Основные ограничения», «Идентификатор ключа» и «Дополнительные применения ключа». Допустимые значения:

- SSL клиент (SSL Client)
- SSL сервер (SSL Server)
- S/MIME
- Подпись объектов (Object Signing)
- SSL УЦ (SSL CA)
- S/MIME УЦ (S/MIME CA)
- УЦ подписи объектов (Object Signing CA)

Остальные поля - это строковые расширения, содержащие информацию, которая будет отображена некоторыми браузерами при просмотре сертификата:

- Базовый URL (Base URL)
- URL отзыва (Revocation URL)
- URL УЦ отзыва (Ca Revocation URL)
- URL обновления сертификата (Certificate Renewal URL)
- URL политики УЦ (Ca Policy URL)
- Имя SSL сервера (SSL server name)
- Комментарий (Comment)

После ввода всех необходимых данных необходимо нажать кнопку «ОК» для сохранения сертификата.

3.4.3 Экспорт

Сертификат может быть экспортирован с помощью кнопки «Экспорт» или через контекстное меню. Имя и формат файла могут быть выбраны в появившемся окне.

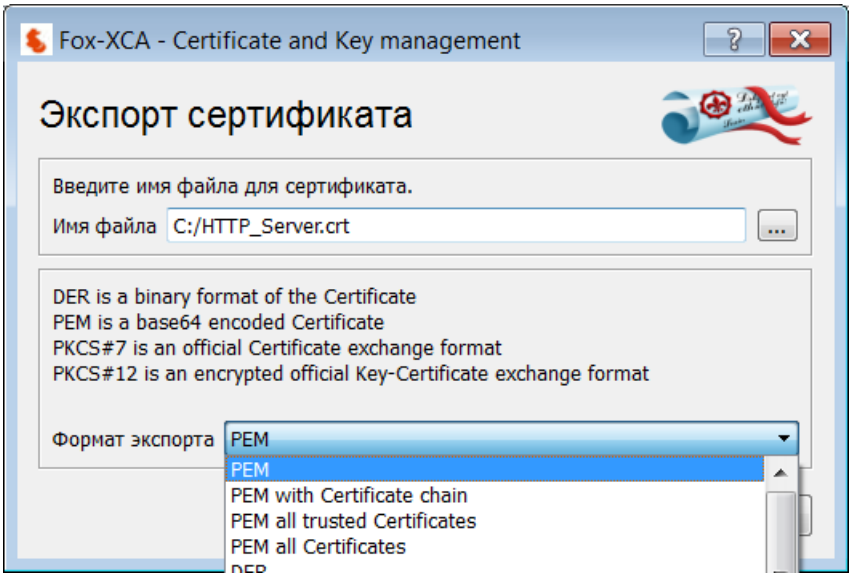

Рис. 20: Диалоговое окно экспорта сертификата

Возможные форматы экспорта сертификата:

- PEM
- PEM с цепочкой сертификатов
- PEM все доверенные сертификаты
- PEM все сертификаты
- DER
- PKCS #7 с цепочкой сертификатов
- PKCS #7 все доверенные сертификаты
- PKCS #7 все сертификаты
- PKCS#12
- PKCS#12 с цепочкой сертификатов
- PEM сертификат + ключ
- PEM сертификат + PKCS8 ключ

3.5 Создание и использование шаблонов

Для облегчения заполнения запросов на сертификат можно создать шаблон запроса, включив в него неизменяемую (или редко изменяемую) информацию, а затем на основе созданных шаблонов быстро создавать новые запросы и издавать сертификаты.

3.5.1 Создание

Для создания шаблона необходимо нажать на кнопку «Новый шаблон» во вкладке «Шаблоны» интерфейса администратора. Появится диалоговое окно выбора начального шаблона.

В этом окне можно выбрать имеющийся шаблон, на основе которого будет создан новый.

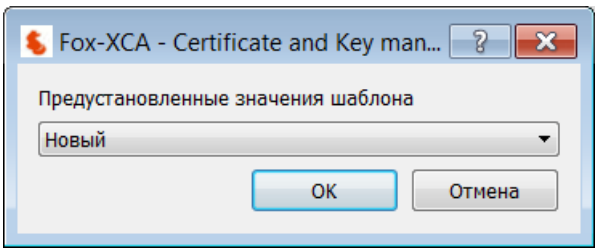

Рис. 21: Диалоговое окно выбора начального шаблона

После выбора появится окно создания нового шаблона.

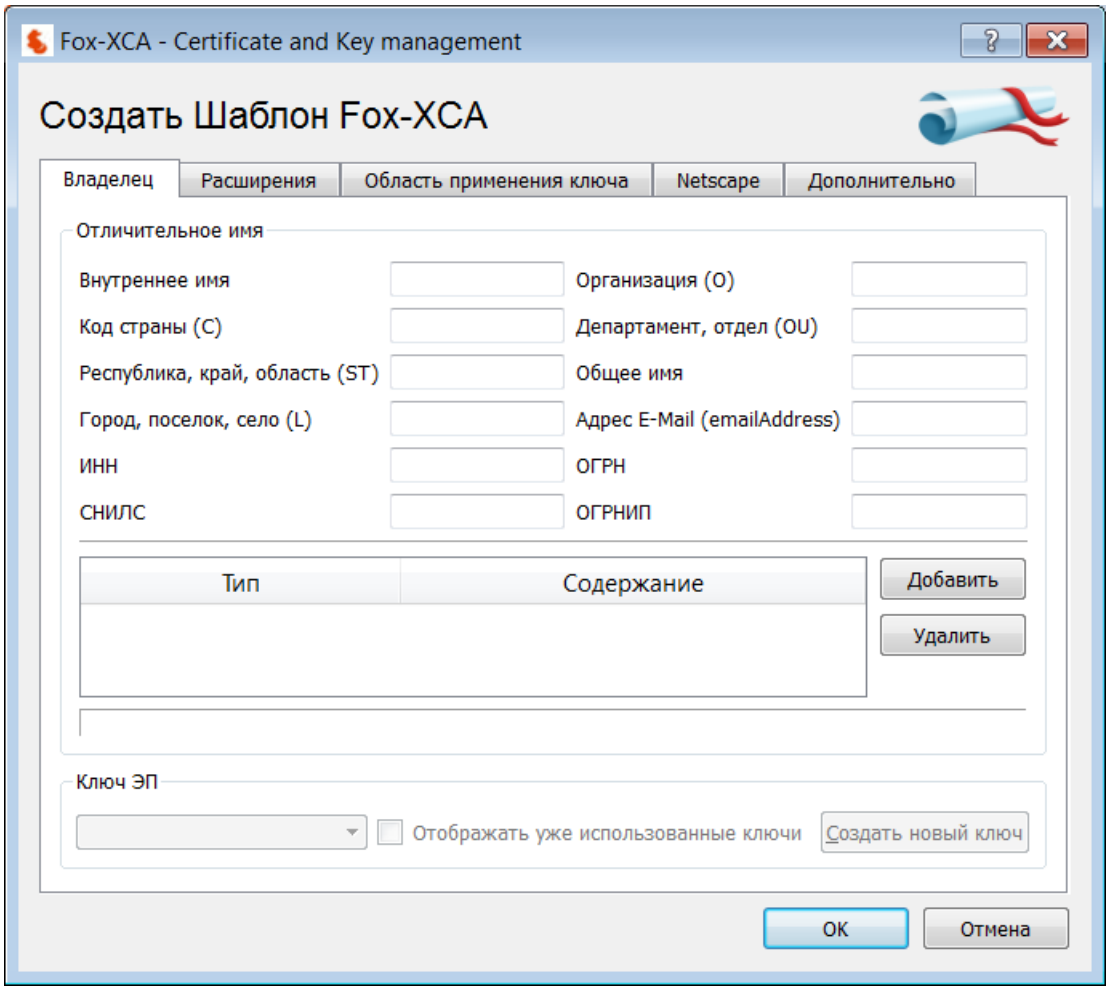

Рис. 22: Диалоговое окно создания нового шаблона

Создание шаблона аналогично созданию сертификата или запроса на сертификат за исключением вкладки «Источник».

3.5.2 Экспорт

Шаблон может быть экспортирован с помощью кнопки «Экспорт» или через контекстное меню. Имя файла может быть выбрано в появившемся окне.

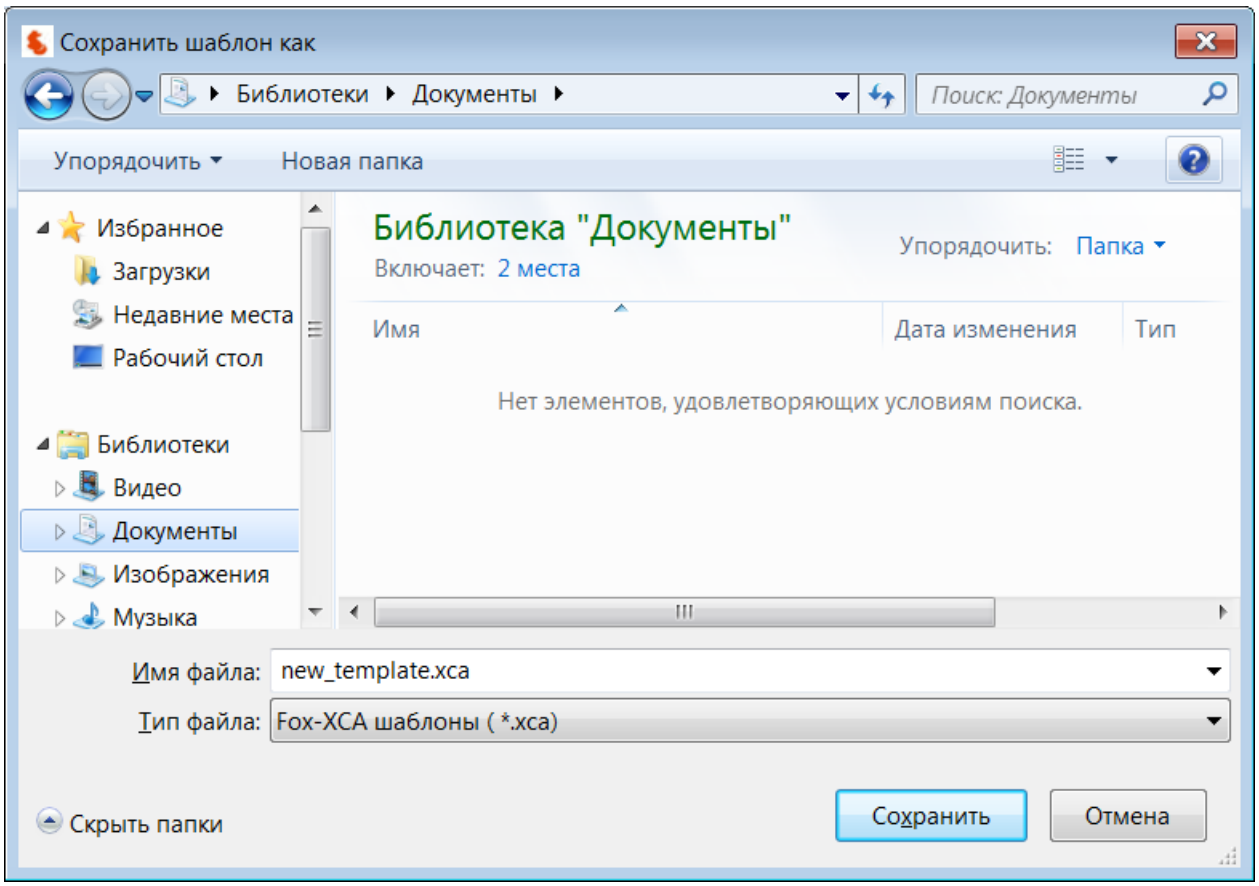

Рис. 23: Диалоговое окно экспорта шаблона

3.6 Аннулирование, восстановление и переиздание сертификатов

Все сертификаты издаются с ограниченным периодом действия. Однако может случиться такая ситуация, когда сертификат не следует использовать или он становится недействительным до истечения даты «Не позднее» в сертификате. В этом случае УЦ следует аннулировать сертификат путем добавления сертификата в список аннулированных сертификатов.

3.6.1 Аннулирование

Сертификат может быть аннулирован, только если в базе есть и сертификат, и ключ ЭП издателя.

Чтобы аннулировать сертификат, необходимо вызвать пункт «Аннулировать» из контекстного меню сертификата.

Сертификат будет помечен как аннулированный, и дата отзыва будет сохранена в базе вместе с сертификатом.

3.6.2 Восстановление

Чтобы восстановить действие сертификата, необходимо вызвать пункт «Восстановить» из контекстного меню аннулированного сертификата.

3.6.3 Обновление

Сертификат может быть обновлен, только если в базе есть ключ ЭП издателя. Обновление заключается в создании копии сертификата с продленным сроком действия.

Чтобы обновить сертификат, необходимо вызвать пункт «Обновить» из контекстного меню сертификата.

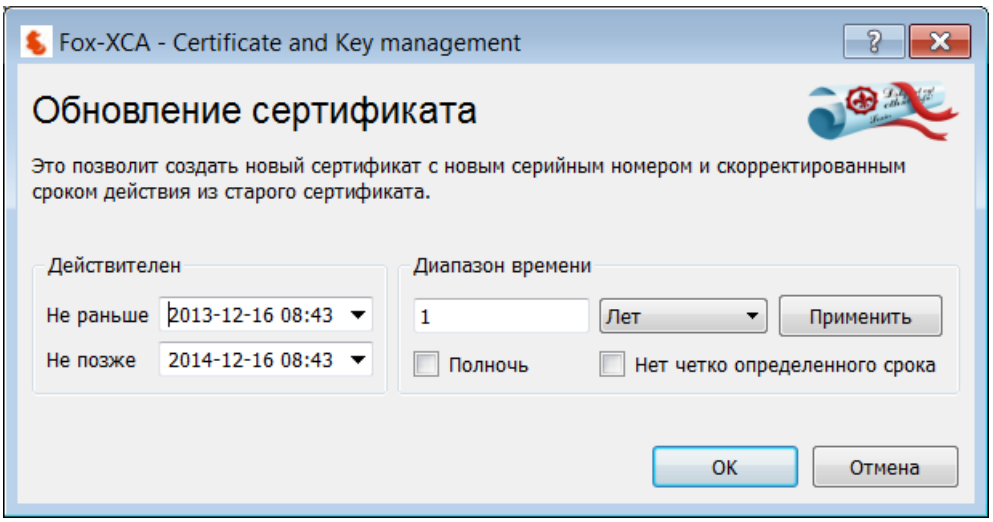

Рис. 24: Диалог переиздания сертификата

В появившемся диалоговом окне переиздания сертификата задать новый период действия сертификата и нажать кнопку «ОК».

3.7 Управление списками аннулированных сертификатов

3.7.1 Формирование

В ПК «Fox-XCA» сформировать список аннулированных сертификатов можно с помощью контекстного меню сертификата ЦС (ЦС→Создание CRL).

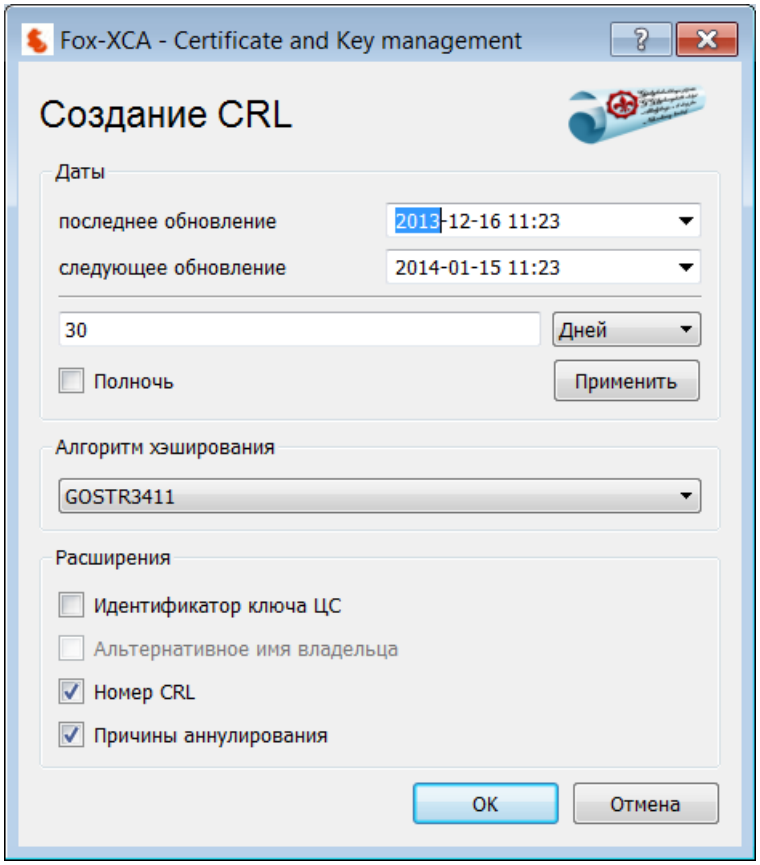

Рис. 25: Диалоговое окно создания списка аннулированных сертификатов

Функция создания CAC генерирует новый список аннулированных сертификатов, собирая информацию обо всех аннулированных сертификатах и даты их аннулирования.

Расширения

Идентификатор ключа ЦС

Это расширение может быть использовано для дифференциации многочисленных ключей подписи списка аннулированных сертификатов, принадлежащих данному УЦ. Это поле содержит уникальный идентификатор ключа (идентификатор ключа субъекта в сертификате автора подписи списка аннулированных сертификатов). Использование этого поля в соответствии с RFC 2459 является обязательным.

Альтернативное имя владельца

Это расширение связывает одно или несколько альтернативных имен с эмитентом списка аннулированных сертификатов. RFC 2459 указывает, что если в поле владельца сертификата не задано отличительное имя, должно присутствовать одно или несколько альтернативных имен.

3.7.2 Экспорт

CAC может быть экспортирован с помощью кнопки «Экспорт» или через контекстное меню. Имя и формат файла могут быть выбраны в появившемся окне.

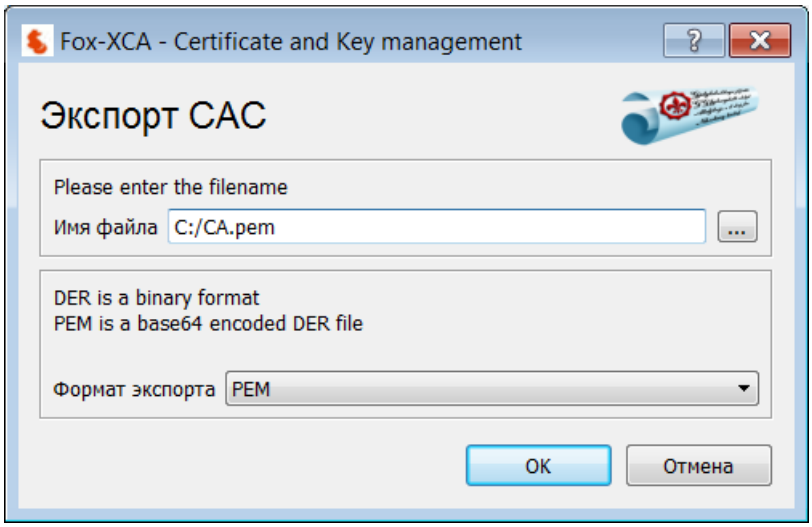

Рис. 26: Диалоговое окно экспорта списка отозванных сертификатов

3.8 Специальные функции УЦ

Контекстное меню сертификата ЦС содержит подменю ЦС, с помощью которого можно выполнять следующие действия - редактировать свойства данного УЦ или создавать список отозванных сертификатов (см. пункт 4.9).

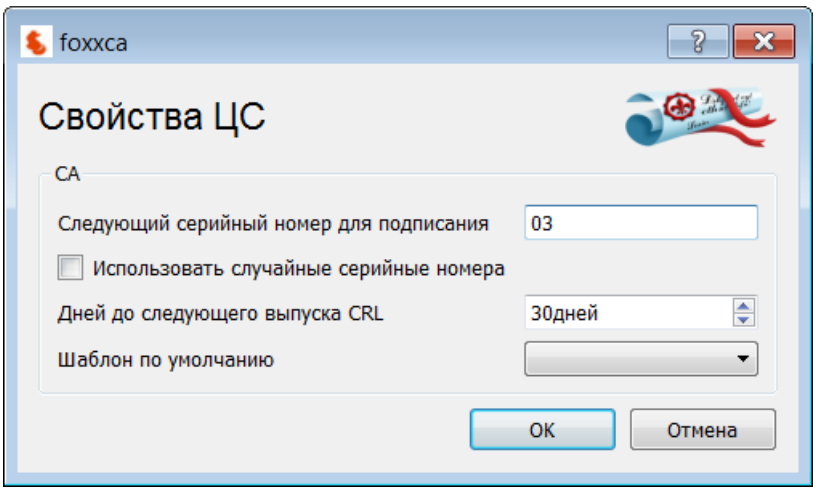

Рис. 27: Диалоговое окно свойств УЦ

В свойствах УЦ может задаваться:

- следующий серийный номер для подписания - серийный номер следующего сертификата, который будет издан данным УЦ;
- количество дней до издания очередного списка аннулированных сертификатов;
- шаблон по умолчанию для издаваемых сертификатов.

3.9 Опции ПК «Fox-XCA»

Окно настройки опций можно открыть с помощью меню "Файл→Опции". Все опции сохраняются в базе и не зависят от реестра операционной системы или конфигурационных файлов.

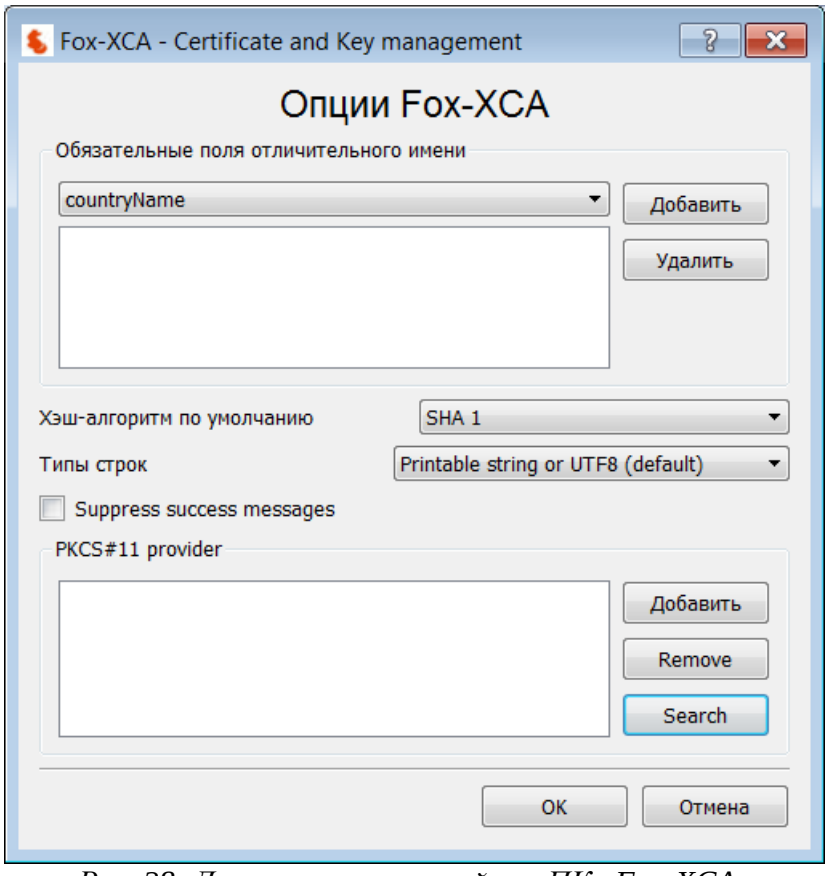

Рис. 28: Диалоговое окно свойств ПК «Fox-XCA»

3.9.1 Обязательные поля отличительного имени

Можно создать список обязательных полей отличительного имени, чтобы получать уведомление, если при создании сертификата одно из этих полей осталось пустым. Этот список не задействован при создании и редактировании шаблонов, потому что шаблон может иметь поля, которые должны заполняться в процессе издания сертификата.

3.9.2 Опции работы со строками

Эти опции применяются ко всем строкам, которые будут преобразованы в ASN1 строки.

- **PKIX только UTF8 (RFC2459)** - все типы строк будут выбраны в соответствии с RFC2459 для записей, опубликованных после 2004 года, что означает, что почти все поля отличительного имени будут конвертированы в UTF8.
- **Не использовать BMP строки** - все строки, содержащие не печатаемые символы, будут рассматриваться как ошибочные.
- **PKIX рекомендации в RFC2459** - все типы строк будут выбраны, как описано в RFC2459.
- **Автоматическое определение** - все типы строк будут выбраны в соответствии с RFC2459 для записей, опубликованных после 2004 года, что означает, что почти все поля отличительного имени будут конвертированы в UTF8.

3.9.3 Хэш-алгоритм по умолчанию

Старые версии Windows (включая Windows XP) не могут оперировать SHA256 и SHA512.

Эта опция позволяет выставить алгоритм хэш-функции по умолчанию:

- MD2
- MD5
- SHA1
- SHA256
- SHA512
- GOST4311

3.10 Идентификаторы объектов (OID’ы)

Частные OID'ы, списки OID'ов для отличительного имени или для расширенного использования ключа могут быть добавлены в перечисленные ниже файлы:

- **oids.txt** - дополнительные OID'ы
- **eku.txt** - список OID'ов ExtendedKeyUsage
- **dn.txt** - список OID'ов DistinguishedName
- **aia.txt** - список OID'ов AuthorityInformationAccess

Пути поиска этих файлов описаны ниже:

Unix

- PREFIX/share/xca/
- PREFIX обычно /usr или /usr/local
- /etc/xca/
- $HOME/xca/

Windows

- Директория инсталляции (Например: C:\Program Files\LISSI-Soft\Fox-XCA)

Все OID'ы не являющиеся официальными, но принадлежащие вашей компании или организации могут быть добавлены в файл oids.txt. Все возможные местонахождения файла oids.txt просматриваются и все найденные файлы загружаются. Таким образом инсталлятор добавляет свои файлы в «/usr/share/xca», Администратор кладет свои файлы в «/etc/xca» , а пользователь в «$HOME/xca».

Формат этих файлов такой: «OID:короткое имя:длинное имя»

Пробелы в начале, в конце и между колонок игнорируются, как и текст в конце строки. Строки, начинающиеся с символа «#», игнорируются.

Файлы, содержащие списки OID'ов, (eku.txt, dn.txt, aia.txt) обрабатываются по-другому - используется только первый найденный файл. Формат этих файлов - одна запись на одну строку. Запись может содержать либо числовое представление OID'да , например 1.3.6.1.5.5.8.2.2, либо короткое имя, например «iKEIntermediate», либо длинное имя – «IP security end entity». Строки, начинающиеся с символа «#», игнорируются. Если эти файлы содержат новые неофициальные OID'ы, они должны быть описаны в одном из файлов oids.txt.

4 Резервное копирование и восстановление БД ПК «Fox-XCA»

Резервное копирование производится путем копирования файла рабочей БД на внешний носитель.

Восстановление БД производится путем копирования БД с носителя, содержащего резервную копию на компьютер с установленным ПК «Fox-XCA».