

ЗАО «Сигнал-КОМ»

УТВЕРЖДЁН
ШКНР.00054-01 34 01-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
«NOTARY-PRO 2.8»

NOTARY-PRO
АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО
АДМИНИСТРАТОРА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Версия 2.8

Руководство администратора

ШКНР.00054-01 34 01
Листов 141

2019

АННОТАЦИЯ

Программно-аппаратный комплекс удостоверяющего центра «Notary-PRO 2.8» (далее – ПАК УЦ «Notary-PRO») предназначен для администрирования систем распределения криптографических ключей в соответствии с Рекомендациями ITU-T X.509, RFC 5280. С помощью средств ПАК УЦ «Notary-PRO» возможно построение как локальной, так и распределенной систем администрирования.

Настоящий документ содержит руководство администратора автоматизированного рабочего места администратора удостоверяющего центра.

СОДЕРЖАНИЕ

Аннотация	2
1. Общие сведения	6
1.1. Назначение программы	6
1.2. Список сокращений	7
1.3. Алгоритмы	7
1.4. Администратор УЦ	7
1.5. Схема работы Администратора УЦ	8
1.6. Сертификат ключа проверки электронной подписи	8
1.7. Уникальное имя	8
1.8. Расширения сертификатов	9
1.9. Запрос на создание сертификата ключа проверки ЭП	10
1.10. Список аннулированных сертификатов	10
1.11. Защита ключей удостоверяющего центра	11
1.11.1. Ключевой контейнер	11
1.11.2. Главный ключ удостоверяющего центра	12
1.11.3. Схема разделения секрета	12
2. Структура программы	14
2.1. Главное окно	14
2.1.1. Главное меню	14
2.1.2. Главная панель	18
2.1.3. Кнопочная панель	19
2.1.4. Информационная панель	19
2.2. Папки документов	20
2.2.1. Папка «Операторы РЦ»	20
2.2.2. Абонентские папки	20
2.2.3. Окно свойств абонентской папки	21
2.2.4. Папка «Абоненты»	24
2.2.5. Папка «Запросы»	24
2.2.6. Папка «Сертификаты»	25
2.3. Папка «Группы»	26
2.4. Папка «Списки отозванных сертификатов»	26
2.5. Папка «Ключи УЦ»	27
2.5.1. Папка «Параметры ключей»	27
2.6. Папка «Шаблоны администрирования»	28
2.7. Папка «Транзакции»	29
3. Действия Администратора	30
3.1. Установка параметров программы	30
3.1.1. Страница «Отображение данных»	30
3.1.2. Страница «Сертификаты»	30
3.1.3. Страница «Отправка уведомлений»	31
3.1.4. Страница «Списки отозванных сертификатов»	32
3.1.5. Страница «Криптография»	33
3.1.6. Страница «Трассировочный журнал»	34
3.1.7. Страница «Главный ключ»	34
3.1.8. Страница «Печать»	35
3.1.9. Страница «Источники данных»	35
3.1.10. Страница «Тип сертификата»	36
3.2. Шаблоны администрирования	37
3.2.1. Создание шаблона администрирования	37
3.2.2. Окно свойств шаблона администрирования	37
3.2.3. Удаление шаблона администрирования	40
3.3. Ключи УЦ	40
3.3.1. Параметры ключей	40
3.3.2. Окно свойств параметров ключей	40
3.3.3. Генерация ключа УЦ	43
3.3.4. Окно свойств ключа УЦ	44
3.3.5. Формирование сертификата УЦ	46
3.3.6. Экспорт ключа УЦ	50
3.3.7. Отзыв ключа УЦ	50
3.3.8. Восстановление ключа УЦ	50

3.3.9. Удаление ключа УЦ	51
3.4. Абоненты	51
3.4.1. Регистрация абонента	51
3.4.2. Окно свойств абонента	52
3.4.3. Удаление записи об абоненте	58
3.5. Запросы на сертификацию	58
3.5.1. Регистрация запроса	58
3.5.2. Окно свойств запроса	60
3.5.3. Создание связи «запрос-абонент»	65
3.5.4. Сертификация запроса	66
3.5.5. Отказ в сертификации запроса	69
3.5.6. Экспорт запроса	69
3.5.7. Удаление запроса	70
3.6. Сертификаты	70
3.6.1. Формирование сертификата	70
3.6.2. Окно свойств сертификата	70
3.6.3. Экспорт сертификата	76
3.6.4. Экспорт сертификатов абонента	76
3.6.5. Отзыв сертификата	77
3.6.6. Восстановление сертификата	78
3.6.7. Удаление сертификата	78
3.7. Списки отозванных сертификатов	79
3.7.1. Формирование списка отозванных сертификатов	79
3.7.2. Окно свойств списков отозванных сертификатов	81
3.7.3. Экспорт списка отозванных сертификатов	84
3.7.4. Удаление списка отозванных сертификатов	84
3.8. Автоматическая обработка запросов	84
3.8.1. Автоматическая обработка запросов из файловой системы	84
3.8.2. Автоматическая обработка запросов из Интернет	85
3.8.3. Автоматическая обработка запросов от Операторов РЦ	86
3.8.4. Ограничение при автоматической обработке СМС-запросов	87
3.8.5. Фильтрация при автоматической обработке запросов	88
3.9. Выборки	88
3.9.1. Создание выборки	88
3.9.2. Удаление выборки	89
3.9.3. Редактирование выборки	89
3.10. Дополнительные функции администрирования	89
3.10.1. Просмотр журнала событий	89
3.10.2. Резервное копирование базы данных	91
3.10.3. Изменение лицензии	92
3.10.4. Копирование ключевого носителя СКЗИ	93
3.10.5. Резервное копирование главного ключа	93
3.10.6. Переход к схеме разделения секрета	93
3.10.7. Настройка шаблонов печати документов	94
4. Настройка расширений сертификатов	96
4.1. Настройка списка расширений	96
4.2. Настройка расширения Basic Constraints (Основные ограничения)	97
4.3. Настройка расширения Subject Key Identifier (Идентификатор ключа владельца)	98
4.4. Настройка расширения Authority Key Identifier (Идентификатор ключа УЦ)	98
4.5. Настройка расширения Key Usage (Назначение ключа)	99
4.6. Настройка расширения Extended Key Usage (Расширенное использование ключа)	100
4.7. Настройка расширения Subject Alternative Name (Альтернативное имя владельца)	100
4.8. Настройка расширения Issuer Alternative Name (Альтернативное имя издателя)	101
4.9. Настройка расширения Certificate Policies (Сертификационные политики)	102
4.10. Настройка расширения CRL Distribution Points (Адрес списка отозванных сертификатов)	104
4.11. Настройка расширений Netscape	104
4.12. Настройка расширения Private Key Usage Period (Период действия закрытого ключа)	105
5. Взаимодействие с Операторами регистрационных центров	107
5.1. Регистрация имени Оператора	107
5.2. Назначение Оператору РЦ прав доступа к папкам документов	107
5.3. Установка свойств Оператора РЦ	108

5.4. Ограничение количества сертификатов, выпускаемых Операторами РЦ.....	109
5.5. Удаление записи об Операторе РЦ.....	110
5.6. Группы Операторов РЦ	110
5.6.1. Формирование группы	110
5.6.2. Редактирование свойств группы	110
5.6.3. Удаление группы	111
6. Взаимодействие с внешними УЦ.....	112
6.1. Иерархические отношения	112
6.1.1. Формирование запроса на создание сертификата ключа проверки УЦ.....	112
6.1.2. Импорт сертификата УЦ.....	113
6.2. Кросс-сертификация	114
6.2.1. Формирование и экспорт запроса на кросс-сертификат	114
6.2.2. Импорт запроса и выпуск кросс-сертификата	116
7. Создание квалифицированного сертификата	118
7.1. Шаблоны администрирования для квалифицированных сертификатов	118
7.2. Создание квалифицированного сертификата в ручном режиме	120
7.3. Импорт запроса на создание сертификата	120
7.4. Контроль атрибутов имени и расширений запроса.....	121
7.5. Выбор шаблона сертификации.....	123
7.6. Контроль атрибутов имени и расширений квалифицированного сертификата	124
7.7. Экспорт сертификата	126
Приложение 1. Оптимизация работы с БД большого объема	127
Приложение 2. Автоматизация публикации списка аннулированных сертификатов.....	135
Приложение 3. Изменение вида настроек расширенного использования ключа	138
Литература	140

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение программы

Удостоверяющий центр (УЦ) «Notary-PRO» предназначен для администрирования систем распределения криптографических ключей в соответствии с Рекомендациями ITU-T X.509 [18] и RFC 5280 [25].

УЦ «Notary-PRO» является центральным компонентом программно-аппаратного комплекса (ПАК) УЦ «Notary-PRO 2.8» [5], имеющего сертификат ФСБ России, устанавливающий соответствие ПАК УЦ требованиям ФСБ России к средствам удостоверяющего центра, утвержденным приказом ФСБ России от 27.12.2011 № 796, требованиям к информационной безопасности удостоверяющих центров, установленным для класса КС2, требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденным приказом ФСБ России от 27.12.2011 № 795, и подтверждающий возможность его использования для реализации функций удостоверяющего центра в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Настоящая версия УЦ «Notary-PRO» выполнена с использованием средства криптографической защиты информации (СКЗИ) «СADB 2.1» (вариант исполнения 2) [13] (далее – СКЗИ «СADB 2.1»), имеющего положительное заключение ФСБ России о соответствии нормативным криптографическим требованиям.

Удостоверяющий центр «Notary-PRO» обеспечивает выполнение следующих базовых функций, которые должны поддерживаться в соответствии с положениями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»:

- создание ключей ЭП и ключей проверки ЭП удостоверяющего центра (далее – ключи УЦ);
- создание корневых (самоподписанных) сертификатов ключей проверки ЭП удостоверяющего центра (далее – сертификаты УЦ);
- регистрацию пользователей УЦ (абонентов) – лиц (заявителей), обратившихся за получением сертификатов ключей проверки электронных подписей;
- прием, регистрацию и верификацию запросов на создание сертификатов ключей проверки ЭП пользователей;
- ручную и автоматическую обработку запросов на создание сертификатов ключей проверки ЭП;
- создание и выдачу сертификатов ключей проверки ЭП пользователей (далее – сертификаты);
- установку сроков действия сертификатов ключей проверки ЭП;
- обеспечение уникальности регистрационной информации пользователя, включаемой в атрибуты сертификата ключа проверки ЭП;
- обеспечение уникальности серийных номеров изготавливаемых сертификатов;
- обеспечение уникальности ключей проверки ЭП в составе выданных сертификатов;
- изготовление копий запросов и сертификатов ключей проверки ЭП на бумажном носителе;
- уведомление пользователей о выпуске запрошенных ими сертификатов;
- аннулирование сертификатов ключей проверки электронной подписи, а также приостановление и возобновление действия сертификатов;
- создание списков аннулированных сертификатов ключей проверки электронной подписи (CRL);
- ведение реестра выданных и аннулированных сертификатов ключей проверки электронной подписи;
- обеспечение актуальности информации, содержащейся в реестре сертификатов, и ее защита от несанкционированного доступа;
- публикацию сертификатов и списков отозванных сертификатов в общедоступных сетевых справочниках;

- формирование запросов на создание сертификатов ключей проверки ЭП УЦ в вышестоящем УЦ и кросс-сертификацию;
- взаимодействие с регистрационными центрами «Notary-PRO RA» [6].

Средства УЦ «Notary-PRO» предусматривают также возможность создания и обслуживания сертификатов ключей, предназначенных для ключевого обмена и шифрования симметричных ключей.

В режиме аккредитованного удостоверяющего центра УЦ «Notary-PRO» обеспечивает создание и обслуживание только квалифицированных сертификатов, выдаваемых по форме, утвержденной приказом ФСБ России от 27.12.2011 №795 [2].

1.2. Список сокращений

В настоящем документе используются следующие сокращения:

БД	- база данных
ДСЧ	- датчик случайных чисел
ИП	- индивидуальный предприниматель
ПАК	- программно-аппаратный комплекс
ПДСЧ	- программный датчик случайных чисел
ПО	- программное обеспечение
РЦ	- регистрационный центр
ОС	- операционная система
САС	- список аннулированных сертификатов
СОС	- список отозванных (аннулированных) сертификатов
СКЗИ	- средство криптографической защиты информации
СУБД	- система управления базой данных
УЦ	- удостоверяющий центр
ФДСЧ	- физический датчик случайных чисел
ЭВМ	- электронная вычислительная машина
ЭП	- электронная подпись
CA	- Certification Authority
CRL	- Certificate Revocation List
DER	- Distinguished Encode Rules
DN	- Distinguished Name (уникальное имя)
PEM	- Privacy Enhanced Mail
PKCS	- Public Key Cryptosystem
PSE	- Private Store Environment (ключевое хранилище)

1.3. Алгоритмы

Удостоверяющий центр «Notary-PRO» поддерживает следующие криптографические алгоритмы:

- ГОСТ Р 34.10-2012 - в соответствии с [7];
- ГОСТ Р 34.11-2012 - в соответствии с [8];
- ГОСТ Р 34.10-2001¹ - в соответствии с [9];
- ГОСТ Р 34.11-94 - в соответствии с [10].

1.4. Администратор УЦ

Администратор удостоверяющего центра (далее просто *Администратор*) - пользователь с особыми полномочиями. Он может генерировать ключи ЭП и формировать сертификаты ключей проверки ЭП удостоверяющего центра, формировать сертификаты пользователей (абонентов), выпускать списки отозванных сертификатов, назначать права Операторам регистрационных центров и др.

¹ Использование ГОСТ Р 34.10-2001 ограничено в соответствии с п. 3.6 Формуляра ШКНР.00054-01 30 01.

Запись об Администраторе создается при первой загрузке программы; этой записи по умолчанию присваивается регистрационный номер 1.

Эта запись не может быть удалена, однако, атрибуты записи могут быть отредактированы Администратором УЦ.

1.5. Схема работы Администратора УЦ

Администратор УЦ – уполномоченное лицо удостоверяющего центра, отвечающее выполнение следующих функций:

- создание ключей электронной подписи и сертификатов ключей проверки электронной подписи УЦ, их эксплуатацию, обновление и уничтожение;
- функционирование УЦ, обеспечивая выполнение набора услуг по регистрации запросов, созданию сертификатов ключей проверки ЭП пользователей УЦ;
- регистрацию Операторов регистрационных центров (РЦ) и назначение полномочий для Операторов РЦ;
- установку, конфигурирование, бесперебойную эксплуатацию и проведение профилактических работ программных и технических средств УЦ.

Общая схема работы Администратора УЦ выглядит следующим образом:

- Администратор УЦ генерирует ключ УЦ и формирует корневой сертификат УЦ;
- Администратор УЦ регистрирует абонентов (пользователей УЦ);
- пользователи формируют запросы на сертификацию и доставляют их Администратору УЦ заранее оговоренным способом;
- Администратор УЦ на основе запросов пользователей формирует сертификаты;
- Администратор УЦ периодически формирует списки отозванных сертификатов;
- сертификаты пользователей, сертификаты УЦ и списки отозванных сертификатов публикуются Администратором УЦ (рассылаются пользователям либо помещаются в общедоступный справочник).

1.6. Сертификат ключа проверки электронной подписи

Формат сертификатов ключей проверки ЭП, создаваемых и выдаваемых УЦ «Notary-PRO», соответствует Рекомендациям ITU-T X.509 [18], RFC 5280 [25].

Удостоверяющий центр создаёт сертификат ключа проверки ЭП пользователя путем заверения электронной подписью УЦ следующего набора данных:

- серийный номер сертификата;
- идентификатор алгоритма подписи;
- уникальное имя удостоверяющего центра;
- период годности сертификата;
- уникальное имя пользователя;
- информация о ключе проверки ЭП пользователя;
- расширения (дополнения) сертификата.

Каждый пользователь является владельцем одного или нескольких сертификатов, созданных и выданных удостоверяющим центром.

Пользователь может владеть сертификатами, полученными из разных удостоверяющих центров.

1.7. Уникальное имя

Уникальное имя (Distinguished Name в терминологии X.509) представляет собой набор атрибутов, совокупность которых, будучи включенной в сертификат, однозначно идентифицирует пользователя-владельца сертификата.

В удостоверяющем центре «Notary-PRO» для формирования уникальных имен используется следующий набор атрибутов:

Таблица 1

Имя атрибута	Атрибут X.520	Длина в байтах	Комментарии
Страна*	CountryName (C)	2	Код страны в Стандарте ISO3166 (для России: RU)
Область/район*	StateOrProvince Name (SP)	128	
Город/село*	LocalityName (L)	128	
Адрес	StreetAddress (STREET)	128	
Организация*	OrganizationName (O)	64	
Подразделение	OrganizationalUnitName (OU)	64	
Должность*	Title (T)	64	
Общее имя*	CommonName (CN)	64/1024	Значение после слеша соответствует максимальному размеру атрибута в квалифицированном сертификате
Фамилия*	Surname (SN)	40/1024	-"-
Приобретенное имя*	GivenName (G)	16/1024	-"-
Электронная почта	E-mail	64	
ИНН*		12	Идентификационный номер налогоплательщика
ОГРН*		13	Основной государственный регистрационный номер
ОГРНИП		15	ОГРН индивидуального предпринимателя
СНИЛС*		11	Страховой номер индивидуального лицевого счёта

Символом «*» в таблице помечены поля, обязательные для включения в квалифицированные сертификаты, изготавливаемые аккредитованным УЦ. Изготовление квалифицированных сертификатов обеспечивается настройками аккредитованного УЦ и правилами заполнения полей сертификата, приведенными в разделе 7 настоящего документа.

Состав и количество заполняемых полей в уникальном имени могут быть различными для разных пользователей. За достоверность и правильность информации, включаемой в уникальное имя, несет ответственность Администратор УЦ.

Атрибуты квалифицированного сертификата соответствуют требованиям приказа ФСБ России от 27.12.2011 № 795 и положениям «Извещения об использовании стандартных атрибутов имени commonName (общее имя), surname (фамилия), givenName (приобретенное имя) и дополнительных атрибутов имени поля «subject» в структуре квалифицированного сертификата ключа проверки электронной подписи» от 13.03.2013.

Программным комплексом «Notary-PRO» поддерживается уникальность имен лишь в контексте данного УЦ; при распределенном администрировании необходимо предпринимать меры по координации действий в части присвоения уникальных имен.

1.8. Расширения сертификатов

Удостоверяющий центр «Notary-PRO» поддерживает следующие расширения (дополнения) сертификатов в соответствии с [2] и [18] (символом «*» помечены расширения,

обязательные для включения в квалифицированные сертификаты, изготавливаемые аккредитованным УЦ; подробнее см. п. 7.4):

- основные ограничения (Basic Constraints);
- идентификатор ключа владельца (Subject Key Identifier);
- идентификатор ключа УЦ (Authority Key Identifier);
- альтернативное имя владельца (Subject Alternative Name);
- альтернативное имя издателя (Issuer Alternative Name);
- назначение ключа (Key Usage);
- расширенное использование ключа (Extended Key Usage);
- сертификационные политики (Certificate Policies);
- адрес списка аннулированных сертификатов (CRL Distribution Points);
- расширения Netscape в соответствии с [27];
- наименование средства ЭП владельца квалифицированного сертификата в соответствии с [2] (SubjectSignTool)*;
- средства ЭП и средства аккредитованного УЦ, использованные для создания квалифицированного сертификата, в соответствии с [2] (IssuerSignTool)*.

Если сертификат не включает расширений, то он соответствует Рекомендациям ITU-T X.509 v1 (1988 г.).

Любое расширение может быть помечено как критичное установкой флажка «Расширение критично» на соответствующей странице редактирования свойств расширения (см. п.4).

1.9. Запрос на создание сертификата ключа проверки ЭП

Сертификаты ключей проверки ЭП создаются удостоверяющим центром на основе ключей проверки ЭП пользователей. Ключи проверки ЭП доставляются Администратору УЦ в виде запросов на создание сертификатов ключей проверки ЭП (или просто запросов).

Запрос на создание сертификата формируется пользователем и представляет собой следующий набор информации:

- запрашиваемое имя;
- информацию о ключе проверки ЭП, включающую идентификатор алгоритма и собственно ключ проверки ЭП;
- расширения (необязательно).

Эта информация подписывается ключом ЭП пользователя, парным ключу проверки ЭП, включенному в запрос.

Запрашиваемое имя представляет собой набор атрибутов, подобный уникальному имени. Запрашиваемое имя формируется пользователем и может быть включено в сертификат в виде уникального имени только после проверки на достоверность.

Удостоверяющий центр «Notary-PRO» поддерживает запросы сертификатов в следующих форматах:

- PKCS #10 [22];
- СМС [32].
- MSIE (Microsoft Internet Explorer);
- SPKAC (Signed Public Key And Challenge).

1.10. Список аннулированных сертификатов

Сертификаты имеют период действия, однако любой сертификат может быть отозван (аннулирован) до истечения этого периода, если:

- соответствующий сертификату ключ ЭП пользователя скомпрометирован;
- пользователь-владелец сертификата больше не обслуживается данным удостоверяющим центром;
- действие сертификата временно приостановлено;

- скомпрометирован ключ удостоверяющего центра, использованный при формировании сертификата.

Удостоверяющий центр должен информировать пользователей об отозванных сертификатах. Для этой цели он поддерживает список отозванных (аннулированных) сертификатов или список отмены.

Список аннулированных сертификатов представляет собой блок информации, содержащий:

- идентификатор алгоритма подписи;
- уникальное имя удостоверяющего центра;
- период действия;
- список, представляющий собой последовательность пар: серийный номер сертификата, дата отмены.
- расширения (необязательно);
- электронную подпись УЦ.

Допустимо существование одновременно нескольких списков отмены, например, с перекрывающимися периодами или подписанных разными ключами удостоверяющего центра.

Для каждого сертификата УЦ должен всегда существовать список отозванных сертификатов.

1.11. Защита ключей удостоверяющего центра

Ключи ЭП удостоверяющего центра (ключи УЦ) являются критическими защищаемыми объектами. Для обеспечения защиты ключей УЦ используется ключевой контейнер, реализуемый в СКЗИ «CADB 2.1» (см. п. 1.11.1), и шифрование на главном ключе УЦ (см. п.1.11.2). В качестве вспомогательной меры защиты доступа к ключам УЦ может использоваться схема «разделения секрета» (см. п.1.11.3).

1.11.1. Ключевой контейнер

Ключи ЭП удостоверяющего центра «Notary-PRO» для алгоритма ГОСТ Р 34.10-2012 могут быть активизированы только при наличии ключевого контейнера формата СКЗИ «CADB 2.1» (PSE).

Ключевой контейнер СКЗИ «CADB 2.1» создается при первой загрузке программы.

Необходимо иметь резервную копию ключевого контейнера, ибо его утеря ведет к невозможности использования ключей УЦ. Процедура создания резервной копии ключевого контейнера описана в п. 3.10.4 настоящего руководства¹.

Формат и регламент хранения ключевых контейнеров СКЗИ «CADB 2.1» описаны в [14].

Для хранения ключевого контейнера СКЗИ «CADB 2.1» должны использоваться съемные ключевые носители из перечня, определенного в эксплуатационной документации на СКЗИ «CADB 2.1»:

- накопители на гибком магнитном диске (НГМД);
- сменные носители с интерфейсом USB;
- электронные ключи eToken производства ЗАО «Аладдин Р.Д.»;
- электронные ключи Rutoken производства ЗАО «Актив-софт».

Для использования электронных ключей необходимо установить пакет драйверов, который можно загрузить с сервера производителя.

При использовании электронных ключей для указания пути к файлу или каталогу необходимо использовать следующие префиксы:

- etoken:/ - для eToken
- rutoken:/ - для Rutoken

Ключи ЭП удостоверяющего центра, предназначенные для подписи сертификатов ключей проверки ЭП и списков отозванных (аннулированных) сертификатов, издаваемых удостоверяющим центром, не должны использоваться ни для каких иных целей.

¹ Недопустимо создание резервной копии ключевого контейнера средствами операционной системы.

1.11.2. Главный ключ удостоверяющего центра

Главный ключ УЦ (далее Главный ключ) используется в качестве дополнительной меры защиты ключей ЭП удостоверяющего центра, хранящихся в ключевом контейнере формата СКЗИ «CADB 2.1» (см. п. 1.11.1). Главный ключ служит для шифрования ключей ЭП удостоверяющего центра при их хранении в базе данных УЦ, а также для ограничения доступа к ряду привилегированных операций, выполняемых Администратором УЦ в процессе эксплуатации ПАК УЦ.

Главный ключ зашифрован на пароле, который запрашивается при загрузке программы, смене пароля главного ключа (см. п. 3.1.7), копировании ключевого носителя СКЗИ (см. п. 3.10.4), резервного копирования главного ключа (см. п.3.10.5), переходе на схему «с разделением секрета» (см. п. 3.10.6).

Главный ключ формируется при первой загрузке программы и хранится в файле. При формировании главного ключа Администратору необходимо задать каталог и имя файла для его хранения¹.

К паролю на Главный ключ предъявляются следующие требования:

- длина пароля должна составлять не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
- плановая смена пароля должна проводиться не реже одного раза в 6 месяцев.

В УЦ «Notary-PRO 2.8» реализован механизм контроля предельной даты использования пароля главного ключа. Дата плановой смены пароля устанавливается в момент смены пароля на основании параметра «Периодичность смены пароля, дней» и отображается в поле «Дата плановой смены пароля» на странице «Главный ключ» окна свойств параметров по умолчанию (см. п. 3.1.7).

После трёх попыток ввода неверного пароля к Главному ключу доступ к функциям УЦ по умолчанию блокируется на 60 сек. Интервал времени блокировки может быть изменен на странице «Главный ключ» окна свойств параметров по умолчанию, но должен составлять не менее 15 секунд. В случае действия блокировки, при входе в программу Администратор получит предупреждение (см. Рис. 1):

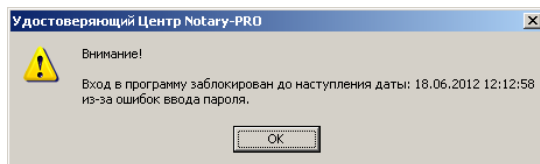


Рис. 1 Предупреждение о блокировке входа в программу

Необходимо иметь резервную копию файла главного ключа, ибо его утеря ведет к невозможности использования ключей УЦ.

Для загрузки программы Администратор может воспользоваться резервным файлом главного ключа, находящимся в каталоге (или на ключевом носителе), отличном от указанного в настройке программы. Для этого во время загрузки программы при запросе пароля к файлу главного ключа Администратор должен нажать клавишу <Esc> и в появившемся диалоге задать путь к резервной копии файла.

1.11.3. Схема разделения секрета

Для повышения уровня безопасности хранения и использования ключей УЦ в «Notary-PRO» реализована возможность перехода на пороговую схему «разделения секрета» (см. п. 3.10.6).

Данная схема предполагает деление главного ключа ключевого контейнера СКЗИ «CADB 2.1» (не путать с Главным ключом УЦ, см.п. 1.11.2) на несколько частей с последующим сохранением каждой из этих частей на отдельных ключевых носителях ответственных лиц – дежурных Администраторов УЦ (см.[15]).

¹ Рекомендуется хранить Главный ключ на съемном носителе.

При использовании схемы «разделения секрета» активация ключа электронной подписи УЦ при запуске ПО «Notary-PRO» произойдет только при одновременном предъявлении порогового количества частей разделенного ключевого контейнера.

В УЦ «Notary-PRO» реализована схема «разделения секрета» Шамира [35]. Настраиваемыми параметрами схемы «разделения секрета» являются: количество независимых частей и пороговое значение, соответствующее минимальному числу частей для обеспечения доступа к ключам УЦ. Рекомендуемые параметры схемы «разделения секрета» доступа к ключам УЦ – «3 из 5»; периодичность смены частей «разделенного секрета» - не реже одного раза в год.

Внеплановая смена частей «разделенного секрета» проводится при порче или утере ключевых носителей с частями ключевого контейнера, увольнении сотрудников, отвечающих за их хранение, и т.п.).

В режиме работы по схеме «с разделением секрета» блокируется возможность экспорта ключа УЦ из базы данных УЦ в файловую систему (см. п. 3.3.6).

Внимание! После перехода УЦ в режим функционирования по схеме «с разделением секрета» вернуться к первоначальной схеме будет невозможно.

2. СТРУКТУРА ПРОГРАММЫ

2.1. Главное окно

Главное окно программы (см. Рис. 2) содержит:

- главное меню (см. п. 2.1.1);
- главную панель (дерево с папками документов) (см. п. 2.1.2);
- кнопочную панель (см. п. 2.1.3);
- информационную панель (строку состояния) (см. п. 2.1.4);
- окна документов (папки документов) (см. п. 2.2);
- панель управления.

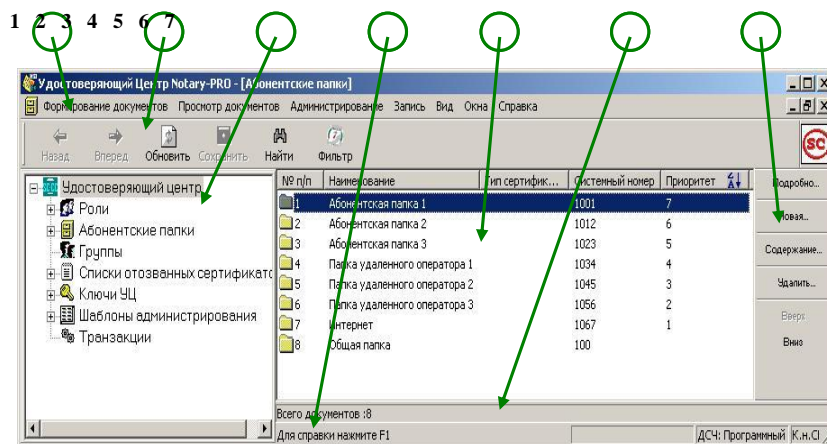


Рис. 2 Главное окно

1- Главное меню, 2- Кнопочная панель, 3-Главная панель, 4- Информационная панель, 5- Окно документов, 6- Информационная панель окна документов, 7- Панель управления.

Окно документов содержит записи из таблиц, локальную информационную панель с данными об общем числе записей в окне документов, а также Панель управления, содержащую кнопки для работы с отображаемыми документами.

2.1.1. Главное меню

Главное меню программы содержит следующие разделы:

- «Формирование документов» (см.п. 2.1.1.1);
- «Просмотр документов» (см.п. 2.1.1.2);
- «Администрирование» (см.п. 2.1.1.3);
- «Вид» (см.п. 2.1.1.4);
- «Справка» (см.п. 2.1.1.5);
- «Запись» (см.п. 2.1.1.6);
- «Окна» (см.п. 2.1.1.7).

Разделы «Запись» и «Окна» активны только в случае, если открыто хотя бы одно окно документов.

2.1.1.1. Раздел «Формирование документов»

Раздел «Формирование документов» содержит следующие пункты:

- «Регистрация нового абонента» - используется для регистрации в базе данных удостоверяющего центра нового абонента (пользователя); вызывает окно диалога, задающее атрибуты нового абонента (см. п. 3.4.1);
- «Запросы» - предназначен для импорта и обработки запросов абонентов удостоверяющего центра; содержит следующие подпункты:
 - ☐ «Импорт из файла» - используется для импорта запросов в базу данных удостоверяющего центра из файловой системы; вызывает диалог выбора файла запроса или группы файлов запросов с последующим вызовом диалога для настройки процедуры импорта (см. п. 3.5.1).
 - ☐ «Автоматическая обработка» - используется для настройки режимов автоматического импорта и обработки запросов:
 - «Из файловой системы...» - обеспечивает настройку процедуры автоматической обработки файлов запросов (см. п. 3.8.1);
 - «Из Интернет...» - обеспечивает настройку процедуры автоматической обработки запросов, полученных через Интернет (см. п. 3.8.2);
 - «От Операторов...» - обеспечивает настройку процедуры автоматической обработки запросов от Операторов регистрационных центров (см. п. 3.8.3).
- «Импорт сертификата» - используется для импорта сертификатов удостоверяющих центров; вызывает диалог выбора файла (см. п. 6.1.2);
- «Создание нового списка отмены» - используется для создания списка отозванных сертификатов; вызывает диалог для задания параметров нового списка отмены (см. п. 3.7.1);
- «Ключи УЦ» - используется для генерации, а также импорта ключей и параметров ключей удостоверяющего центра (см. п. 3.3.1); содержит следующие подпункты:
 - ☐ «Генерация нового ключа» - создание нового ключа УЦ в соответствии с заданными параметрами;
 - ☐ «Импорт ключа...» - обеспечивает загрузку ключей УЦ; вызывает мастер-диалог для загрузки ключа ЭП;
 - ☐ «Импорт параметров» - вызывает диалог для выбора файла с параметрами ключа УЦ;
 - ☐ «Копирование ключевого носителя СКЗИ» - обеспечивает резервное копирование ключевого носителя СКЗИ «CADB 2.1» (см.п. 3.10.4);
 - ☐ «Копирование главного ключа» - обеспечивает резервное копирование главного ключа (см. п. 3.10.5).
 - ☐ «Переход к схеме разделения секрета...» - обеспечивает переход к схеме разделения ключевого контейнера на несколько частей (см. 3.10.6).
- «Выход» - выход из программы.

2.1.1.2. Раздел «Просмотр документов»

Раздел «Просмотр документов» содержит следующие пункты:

- «Абоненты»:
 - ☐ «Несертифицированные...» - выводит окно, содержащее список абонентов удостоверяющего центра, не имеющих ни одного сертификата;
 - ☐ «Сертифицированные...» - выводит окно, содержащее список абонентов удостоверяющего центра, имеющих хотя бы один сертификат;
 - ☐ «Все...» - выводит окно, содержащее список всех абонентов удостоверяющего центра.
- «Запросы»:
 - ☐ «Несертифицированные...» - выводит окно, содержащее список несертифицированных запросов;
 - ☐ «Сертифицированные...» - выводит окно, содержащее список сертифицированных запросов;
 - ☐ «Все...» - выводит окно, содержащее список всех запросов, зарегистрированных удостоверяющим центром.

- «Сертификаты»:
 - ☐ «Действительные...» - выводит окно, содержащее список всех действительных сертификатов;
 - ☐ «Отозванные...» - выводит окно, содержащее список всех отозванных сертификатов;
 - ☐ «Просроченные...» - выводит окно, содержащее список всех сертификатов, период действия которых уже истек;
 - ☐ «Все...» - выводит окно, содержащее список всех сертификатов удостоверяющего центра.

Примечание: пункты меню «Абоненты», «Запросы» и «Сертификаты» отображают содержимое соответствующих папок системной Общей папки документов (см. п. 2.2.2).

- «Списки отмены»:
 - ☐ «Действующие...» - выводит окно, содержащее список всех действующих списков отмены, выпущенных удостоверяющим центром;
 - ☐ «Все...» - выводит окно, содержащее список всех списков отмены, выпущенных удостоверяющим центром.
- «Ключи УЦ»:
 - ☐ «Список ключей» - выводит окно, содержащее список всех ключей УЦ;
 - ☐ «Параметры ключей» - содержит следующие подпункты:
 - «Параметры ГОСТ Р 34.10-2012» - содержит параметры для ключей ГОСТ Р 34.10-2012 [7].
 - «Все параметры» - выводит окно, содержащее список всех параметров.

2.1.1.3. Раздел «Администрирование»

Раздел «Администрирование» содержит следующие пункты:

- «Шаблоны администрирования» - содержит следующие подпункты:
 - ☐ «Шаблоны Администратора УЦ» - выводит окно, содержащее список шаблонов администрирования, используемых при формировании сертификатов удостоверяющего центра;
 - ☐ «Шаблоны для абонентов» - выводит окно, содержащее список шаблонов администрирования, используемых при сертификации запросов абонентов удостоверяющего центра;
 - ☐ «Все шаблоны» - выводит окно, содержащее список всех шаблонов администрирования.
- «Установка параметров по умолчанию» - выводит многостраничный диалог для установки параметров настройки программы (см. п. 3.1);
- «Просмотр и настройка журнала событий» - выводит многостраничный диалог для просмотра записей и настройки журнала событий (см. п. 3.10.1);
- «Резервное копирование базы данных» - вызывает окно настройки режима резервного копирования базы данных удостоверяющего центра (см. п. 3.10.2);
- «Лицензия...» - вызывает отображение окна «Лицензия», содержащего параметры лицензионного соглашения (см. п. 3.10.3).

2.1.1.4. Раздел «Вид»

Раздел «Вид» содержит следующие пункты:

- «Главная панель» - переключатель отображения Главной панели;
- «Кнопочная панель» - переключатель отображения Кнопочной панели;
- «Информационная панель» - переключатель отображения Информационной панели.
- «Панель управления» - определяет расположение в окне документов Панели управления активного окна; содержит следующие переключатели:
 - ☐ «Сверху»;
 - ☐ «Снизу»;
 - ☐ «Слева»;

- ☐ «Справа».
- «Таблица» - предназначен для настройки внешнего вида активного окна документов; содержит следующие подпункты:
 - ☐ «Вид» - определяет способ отображения документов в активном окне:
 - «Значки»;
 - «Маленькие значки»;
 - «Список»;
 - «Развернутый список».
 - ☐ «Порядок столбцов» - предназначен для настройки порядка отображения полей окна документов (для развернутого списка).

2.1.1.5. Раздел «Справка»

Раздел «Справка» содержит следующие пункты:

- «Содержание» - служит для вызова справочной системы;
- «Указатель» - служит для вызова процедуры поиска справочного материала по ключевым словам;
- «О программе...» - выдает краткую справку о программе и лицензионном соглашении.

2.1.1.6. Раздел «Запись»

Раздел «Запись» содержит следующие пункты:

- «Подробно» - служит для вызова окна свойств документа, выделенного курсором;
- «Сохранить изменения» - сохраняет измененные параметры текущего документа в базе данных;
- «Найти» - вызывает диалог для задания параметров поиска записи в активном окне документов; поиск может осуществляться только по тому атрибуту, по которому в настоящий момент осуществляется сортировка записей активного окна;
- «Фильтр по дате» - вызывает диалог настройки дат, ограничивающих записи в папках «Абоненты», «Запросы», «Сертификаты»; при активном фильтре этот пункт меню помечен;
- «Печать» - вызывает диалог для загрузки текущего документа на печать; параметры печати документов задаются Администратором удостоверяющего центра в окне «Параметры по умолчанию» (см. п. 3.1);
- «Печать по шаблону» - предназначен для печати текущего документа по заранее подготовленному шаблону (см.п. 3.10.6).
- «Выделить все» - позволяет выделить все записи в открытом на данный момент окне.

2.1.1.7. Раздел «Окна»

Раздел «Окна» содержит следующие пункты:

- «Расположить друг над другом» - определяет способ каскадного расположения окон документов на экране;
- «Расположить рядом» - определяет способ расстановки окон документов на экране, при котором окна находятся рядом, не перекрывая друг друга;
- «Упорядочить значки» - служит для упорядочивания (расстановки в линию) заголовков свернутых окон документов;
- «Закрыть все...» - служит для закрытия всех окон документов;
- «Переместить окно свойств в центр экрана» - предназначен для центрирования активного окна свойств в случае переноса его за границы видимой области экрана.

Кроме того, раздел «Окна» содержит список всех открытых в текущий момент окон документов.

2.1.2. Главная панель

Главная панель программы (см. Рис. 3) представлена в виде дерева, узлами которого являются папки документов. Главная панель обеспечивает удобный и быстрый доступ к окнам документов, отфильтрованным по заранее установленным правилам.

Администратор удостоверяющего центра может создавать новые папки (наборы данных) (см. п. 2.2.2), устанавливая для них собственные правила фильтрации документов (3.9).

Состав Главной панели при первом запуске программы включает только системные папки (см. Рис. 3), которые не могут быть удалены и имена которых не могут быть изменены:

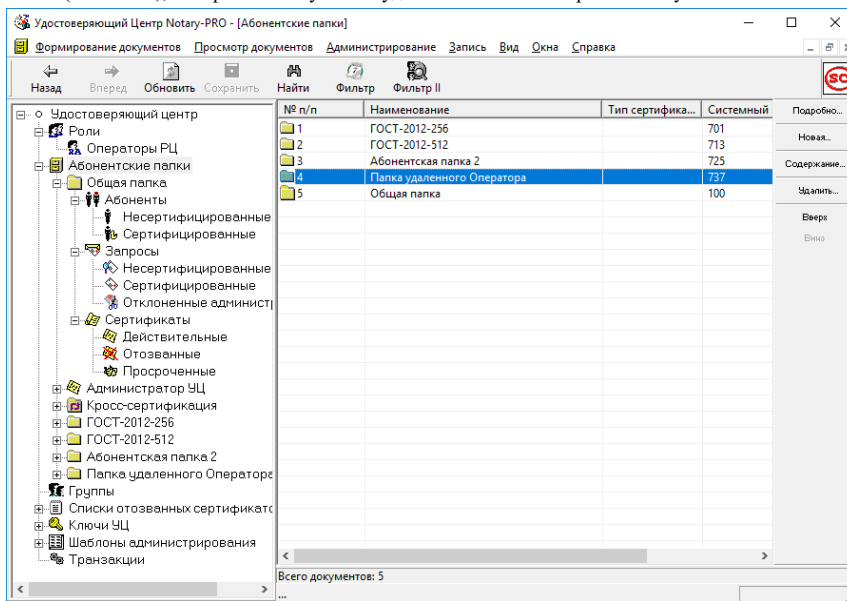


Рис. 3 Состав Главной панели при первом запуске программы.

- «Роли» - перечень папок, содержащих записи о пользователях, которым Администратор УЦ частично делегировал свои полномочия, доверив выполнение некоторых функций администрирования; каждой папке данной категории соответствует определенный набор административных функций, определяющих роль, назначенную группе пользователей, объединяемых данной папкой; в текущей версии поддерживается только одна ролевая функция:
 - «Операторы РЦ» - данная папка содержит записи об Операторах регистрационных центров (см. п. 5.1).
- «Абонентские папки» - перечень папок, каждая из которых (кроме системной папки «Кросс-сертификация» включает фиксированный набор документов УЦ:
 - «Абоненты» (см.п. 2.2.4);
 - «Запросы» (см.п. 2.2.5);
 - «Сертификаты (см.п. 2.2.6).

При первом запуске программы в перечне абонентских папок содержатся только три системные папки:

- «Общая папка» - в ней отображаются все документы удостоверяющего центра;
- «Администратор УЦ» - в ней отображаются только документы Администратора удостоверяющего центра;
- «Кросс-сертификация» - включает фиксированный набор документов, относящихся к процедуре кросс-сертификации (см.п. 6.2):
 - «Субъекты кросс-сертификации»;
 - «Запросы для кросс-сертификации»;

- «Кросс-сертификаты»;
в дальнейшем набор абонентских папок может быть расширен Администратором УЦ (см.п. 2.2.2).
 - «Группы» - папка, в которой содержится информация об установленных квотах выпуска сертификатов для различных групп Операторов регистрационных центров (см.п. 2.3).
 - «Списки отозванных сертификатов» - папка содержит перечень всех списков отозванных сертификатов (см. п. 2.4), выпущенных удостоверяющим центром, а также папку:
 - «Действующие» - содержит только списки отозванных сертификатов, период действия которых еще не истек.
 - «Ключи УЦ» - папка содержит список ключей удостоверяющего центра (см. п. 2.5), а также папку:
 - «Параметры ключей» (см. п. 2.5.1) - содержит список параметров ключей УЦ.
 - «Шаблоны администрирования» - папка содержит список шаблонов администрирования удостоверяющего центра (см. п.2.6), а также папки:
 - «Шаблоны Администратора УЦ» - список шаблонов администрирования для сертификатов УЦ;
 - «Шаблоны для абонентов» - список шаблонов администрирования для сертификатов абонентов.
 - «Транзакции» - папка содержит записи обо всех операциях с запросами на сертификаты, проводимых в удостоверяющем центре (см. п. 2.7).
- Отображение Главной панели может быть отключено из главного меню (см. п. 2.1.1.4).

2.1.3. Кнопочная панель

Кнопочная панель главного окна программы (см. п. 2.1) содержит следующий набор кнопок:

- «Назад» - активизация предыдущего окна документов из очереди открытых окон;
- «Вперед» - активизация следующего окна документов из очереди открытых окон;
- «Обновить» - обновление данных в активном окне документов (повторное считывание из базы данных);
- «Сохранить» - сохранение измененных данных в активном окне документов (запись в базу данных);
- «Найти» - поиск документа в активном окне;
- «Фильтр» - вызывает диалог настройки дат, ограничивающих количество записей в папках «Абоненты», «Запросы», «Сертификаты». При активном фильтре эта кнопка утоплена.

Отображение кнопочной панели может быть отключено из главного меню (см. п. 2.1.1.4).

2.1.4. Информационная панель

Информационная панель главного окна программы (см. п. 2.1) содержит вспомогательную информацию:

- подсказку о названии процедуры, которая будет выполняться при нажатии левой клавиши мыши;
- маркеры «WEB» или «OPER» с информацией о времени последнего сканирования таблиц буферной БД приложения «Notary-PRO Web Pages» и таблиц запросов на сертификацию, поступивших от Операторов РЦ, соответственно;
- маркер «ДСЧ» с указанием типа используемого в настоящий момент датчика случайных чисел (см. п. **Ошибка! Источник ссылки не найден.**);
- маркер «PSE» с информацией об используемом ключевом носителе СКЗИ «CADB 2.1» (см.п. 1.11.1).

Отображение строки состояния может быть отключено из главного меню (см. п. 2.1.1.4).

2.2. Папки документов

2.2.1. Папка «Операторы РЦ»

В папке «Операторы РЦ» (см. Рис. 4) отображается список уникальных имен Операторов регистрационных центров.

Панель управления окна «Операторы РЦ» содержит следующий набор кнопок:

- «Подробнее...» - вызывает окно с отображением атрибутов Оператора РЦ (см. п. 5.2);
- «Новый...» - вызывает окно для регистрации имени Оператора регистрационного центра (см. п. 5.1);
- «Удалить...» - используется для удаления записи об Операторе РЦ (см. п. 5.5);
- «Доступ к папкам...» - используется для назначения Оператору РЦ прав доступа к документам (см. п. 5.2).

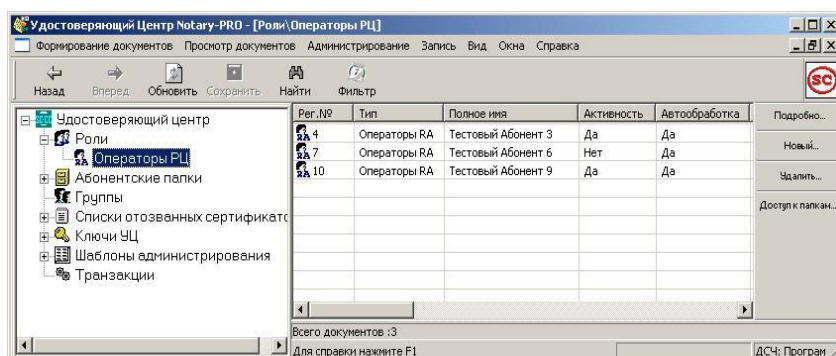


Рис. 4 Папка документов «Операторы РЦ»

2.2.2. Абонентские папки

Окно «Абонентские папки» (см. Рис. 5) отображает информацию о системных папках («Общая папка», «Администратор УЦ», «Кросс-сертификация») и абонентских папках, созданных Администратором удостоверяющего центра.

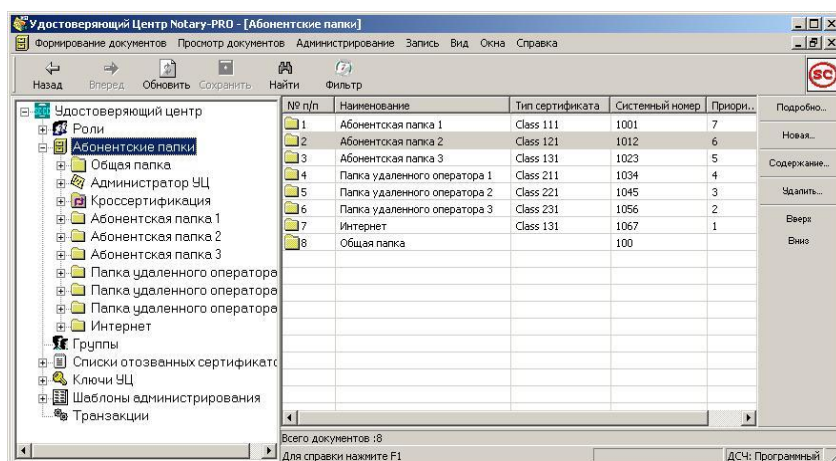


Рис. 5 Окно «Абонентские папки»

Панель управления данного окна содержит следующий набор кнопок:

- «Подробнее...» - открывает страницы свойств абонентской папки, выделенной курсором (см. п. 2.2.3);

- «Новая...» - вызывает окно диалога создания новой абонентской папки;
- «Содержание...» - вызывает окно диалога для просмотра содержимого папки (списка абонентов, входящих в папку), а также для изменения содержимого абонентской папки;
- «Удалить...» - удаляет выделенную курсором абонентскую папку; при этом документы, входящие в папку, из базы данных не удаляются.
- «Вверх» - служит для увеличения приоритета абонентской папки;
- «Вниз» - служит для уменьшения приоритета абонентской папки.

Кнопки «Вверх» и «Вниз» активизированы только в случае наличия не менее трех абонентских папок и сортировки записей в окне по значению поля «Приоритет».

Приоритеты абонентских папок используются при автоматической обработке запросов, в процессе поиска папки с атрибутами совпадающими с атрибутами из обрабатываемого запроса (см. пп.3.8.1, 3.8.2).

Каждая папка, входящая в перечень «Абонентские папки» включает обязательный стандартный набор папок документов:

- «Абоненты» (см.п. 2.2.4);
- «Запросы» (см.п. 2.2.5);
- «Сертификаты» (см.п. 2.2.6).

В Общей папке отображаются все записи соответствующего типа.

Для каждого типа документов Администратор может создавать собственные наборы данных – выборки (см.п. 3.9).

2.2.3. Окно свойств абонентской папки

Вызывается по кнопке «Подробнее...» Панели управления; представляет собой многостраничный диалог.

2.2.3.1. Страница «Параметры»

Страница «Параметры» (см. Рис. 6) содержит следующие атрибуты абонентской папки:

Палка ' Абонентская папка 2'

Параметры | Шаблон имени | Заметки

Наименование: Абонентская папка 2

Системный номер: 737

Шаблон администрирования №: 8 [x] [] -->

☐ Автоматическая сертификация запросов разрешена

☐ Автоматическая отправка сертификатов на LDAP

Условия отбора

Разрешенные алгоритмы и длина ключей в запросах

☒ ГОСТ Р 34.10-2012 (256 бит) от 256 до 256

☐ ГОСТ Р 34.10-2012 (512 бит) от 512 до 512

Разрешенный тип сертификатов: [dropdown] Сброс

Рис. 6 Страница «Параметры» окна свойств папки документов

- «Наименование» - имя папки;
- «Системный номер» - номер папки, который присваивается программой удостоверяющего центра;
- «Шаблон администрирования» - для каждой папки может быть установлен шаблон администрирования, в соответствии с которым будет производиться сертификация запросов; если шаблон администрирования для папки не установлен, используется шаблон «Общей папки»;
- «Автоматическая сертификация запросов разрешена» - разрешает автоматическую сертификацию запросов в соответствии с правилами, описанными в п. 3.8¹;
- «Автоматическая отправка сертификатов на LDAP» - разрешает автоматическую публикацию сертификатов и списков отозванных сертификатов в сетевом справочнике;
- «Разрешенные алгоритмы и длина ключей в запросах» - фильтры по параметрам ключа проверки ЭП, в соответствии с которыми абоненты, регистрируемые в процессе автоматической обработки запросов, помещаются в нужную абонентскую папку;
- «Разрешенный тип сертификатов» - фильтр по типам сертификатов, в соответствии с которым абоненты, регистрируемые в процессе автоматической обработки запросов, помещаются в нужную абонентскую папку; данное поле может принимать пустое значение либо значение из списка зарегистрированных в УЦ типов сертификатов, например:
 - ☐ Class 0

¹ При автоматической сертификации запросов новый абонент будет зарегистрирован только в том случае, если импортируемый запрос самоподписан и в базе данных Удостоверяющего центра нет ни одного сертификата с уникальным именем, совпадающим с атрибутами имени в запросе.

- ❑ Class 1
- ❑ Class 2
- ❑ Class 3.

Примечание. Тип сертификата может передаваться в УЦ вместе с запросом на сертификат в качестве дополнительного признака, определяющего в совокупности с атрибутами запроса выбор профиля (шаблона) сертификации. Регистрация типов сертификатов и их интерпретация определяется действующей Сертификационной политикой удостоверяющего центра и выполняется Администратором УЦ путем редактирования файла crt_cls_lst.ini, расположенного в каталоге запуска программы.

2.2.3.2. Страница «Шаблон имени»

Страница «Шаблон имени» (см. Рис. 7) содержит шаблон с атрибутами уникального имени, по которому абоненты, регистрируемые в процессе автоматической обработки запросов, помещаются в нужную абонентскую папку.

Примечание: в полях шаблона имени допускается использование масок с символом «*», означающим, что на месте размещения «*» в запрашиваемом имени может располагаться произвольный набор символов. В маске допускается также использование символа «?», означающего, что на этой позиции в запрашиваемом имени может располагаться любой одиночный символ.

Атрибуты уникального имени	
Полное имя	×
Организация	×
Подразделение	×
Должность	×
Страна	×
Город село	×
Область район	×
Электронная почта	×
ИНН	✗
ОГРН	✗
СНИЛС	✗
Фамилия	×
Имя Отчество	×
Адрес	×
Почтовый адрес	×
Неструктурированное имя	×
Псевдоним	×
Серийный номер	×
ОГРНИП	✗
КП ФСС	×
РНС ФСС	×

Рис. 7 Страница «Шаблон имени» окна свойств папки документов

2.2.3.3. Страница «Заметки»

Страница «Заметки» содержит комментарии Администратора.

2.2.4. Папка «Абоненты»

В папке «Абоненты» (см. Рис. 8), входящей в стандартный набор документов любой абонентской папки, отображается список абонентов данной папки (для «Общей папки» - список всех абонентов удостоверяющего центра) .

Панель управления окна «Абоненты» содержит следующий набор кнопок:

- «Подробнее...» - открывает окно свойств записи, выделенной курсором (см. п. 3.4.2);
- «Новый...» - вызывает окно регистрации нового абонента (см. п. 3.4.1);
- «Удалить...» - удаляет из базы данных запись об абоненте (см. п. 3.4.3);
- «Экспорт...» - экспортирует все действительные сертификаты абонента, все сертификаты УЦ, необходимые для проверки сертификатов абонента, и все действующие списки отмены (см. п. 3.6.4).

Папка «Абоненты» содержит следующие стандартные разделы:

- «Несертифицированные» - содержит список записей об абонентах, не имеющих ни одного сертификата;
- «Сертифицированные» - содержит список записей об абонентах, имеющих хотя бы один сертификат.

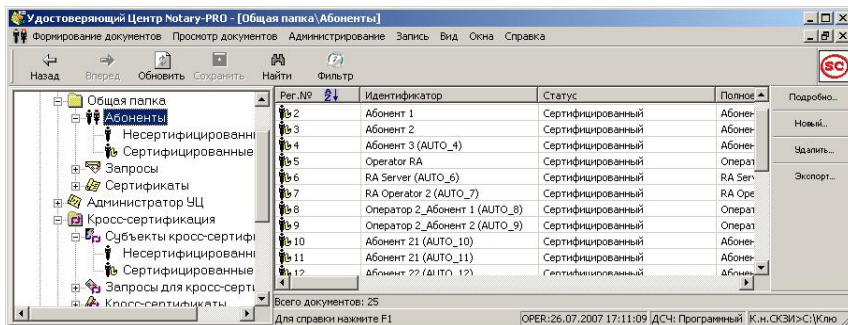


Рис. 8 Папка документов «Абоненты»

2.2.5. Папка «Запросы»

В папке «Запросы» (см. Рис. 9), входящей в стандартный набор документов любой абонентской папки, отображается список запросов, принадлежащих абонентам данной папки (для «Общей папки» – список всех запросов).

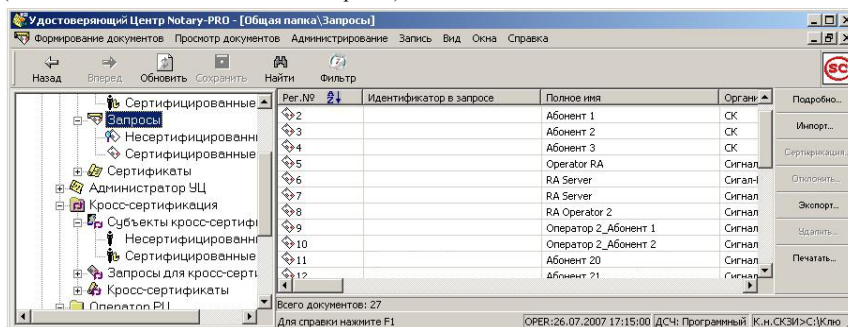


Рис. 9 Папка документов «Запросы»

Панель управления окна папки «Запросы» содержит следующий набор кнопок:

- «Подробнее...» - открывает окно свойств запроса, выделенного курсором (см. п. 3.5.2);
- «Импорт...» - вызывает окно диалога для выбора файла(ов) запроса(ов) (см.п. 3.5.1);
- «Сертификация...» - вызывает окно диалога создания сертификата (см.п. 3.5.4);

- «Отклонить...» - позволяет Администратору УЦ запретить сертификацию запроса с указанием причины запрета (см. п. 3.5.5);
- «Экспорт...» - вызывает окно диалога для задания имени файла для сохранения запроса, выделенного курсором (см. п. 3.5.6);
- «Удалить...» - удаляет из базы данных запрос, выделенный курсором (см. п. 3.5.7);
- «Печатать...» - вызывает окно диалога для загрузки на печать текста запроса, выделенного курсором.

Папка «Запросы» содержит следующий обязательный стандартный набор папок:

- «Несертифицированные» - содержит список запросов, для которых еще не выпущен сертификат;
- «Сертифицированные» - содержит список запросов, для которых уже создан сертификат.

2.2.6. Папка «Сертификаты»

В папке «Сертификаты» (см. Рис. 10), входящей в стандартный набор документов любой абонентской папки, отображается список сертификатов, сформированных для абонентов данной папки (для «Общей папки» - список всех сертификатов).

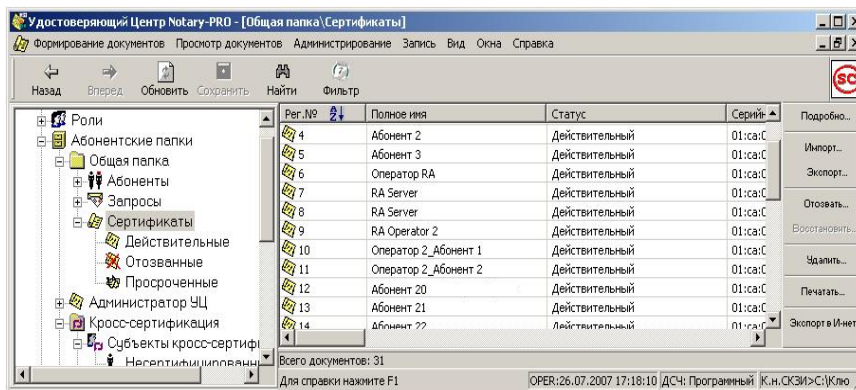


Рис. 10 Папка документов «Сертификаты»

Панель управления окна папки «Сертификаты» содержит следующий набор кнопок:

- «Подробнее...» - отображает окно свойств сертификата, выделенного курсором (см. п. 3.6.2);
- «Импорт...» - вызывает окно диалога для выбора имени файла сертификата (см. п. 6.1.2);
- «Экспорт...» - вызывает окно диалога для задания имени файла, в который будет экспортирован сертификат (см. п. 3.6.3); допускается экспорт сразу нескольких сертификатов, помеченных курсором;
- «Отозвать...» - вызывает процедуру отзыва сертификата (см. п. 3.6.5);
- «Восстановить...» - вызывает процедуру восстановления действительного статуса отозванного ранее сертификата (см. п. 3.6.6);
- «Удалить...» - удаляет из базы данных сертификат, выделенный курсором (см. п. 3.6.7);
- «Печатать...» - вызывает окно диалога для загрузки на печать сертификата, выделенного курсором;
- «Экспорт в И-нет...» - вызывает процедуру экспорта сертификата в базу данных приложения «Notary-PRO Web Pages» для доставки удаленному абоненту (см. п. 3.8.2).

Папка «Сертификаты» содержит следующий обязательный стандартный набор папок:

- «Действительные» - содержит список записей о действительных сертификатах;
- «Отозванные» - содержит список отозванных сертификатов;
- «Просроченные» - содержит список сертификатов, период действия которых истек.

2.3. Папка «Группы»

В данной папке отображается список всех групп Операторов РЦ, с указанием для каждой группы установленной квоты на выпуск сертификатов всеми Операторами данной группы и количества уже выпущенных ими сертификатов на данный момент времени (см. Рис. 11).

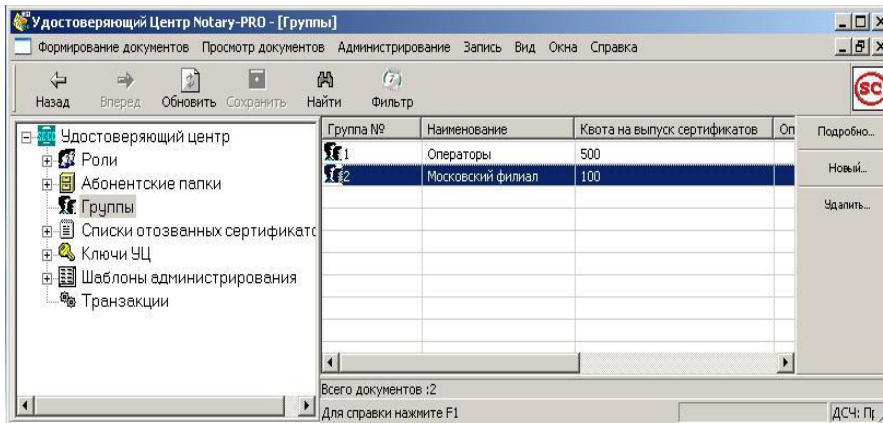


Рис. 11 Папка документов «Группы»

Панель управления окна папки «Группы» содержит следующий набор кнопок:

- «Подробнее...» - открывает окно свойств группы, выделенной курсором (см.п. 5.6.2);
- «Новый...» - вызывает процедуру создания новой записи в папке «Группы» (см.п. 5.6.1);
- «Удалить...» - удаляет из базы группу, выделенную курсором (см.п. 5.6.3).

2.4. Папка «Списки отозванных сертификатов»

В данной папке отображаются списки отозванных сертификатов, сформированные удостоверяющим центром (см. Рис. 12).

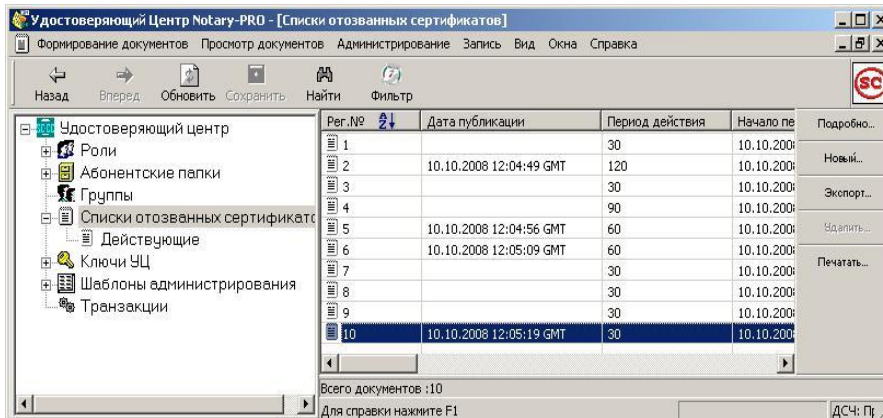


Рис. 12 Папка документов «Списки отозванных сертификатов»

Панель управления окна папки «Списки отозванных сертификатов» содержит следующий набор кнопок:

- «Подробнее...» - открывает окно свойств списка отозванных сертификатов, выделенного курсором (см.п. 3.7.2);
- «Новый...» - вызывает процедуру формирования нового списка отозванных сертификатов (см.п. 3.7.1);

- «Экспорт...» - вызывает окно диалога для задания имени файла, в который будет экспортирован список отозванных сертификатов (см.п. 3.7.3);
- «Удалить...» - удаляет из базы данных список отозванных сертификатов, выделенный курсором (см.п. 3.7.4);
- «Печатать...» - вызывает окно диалога для загрузки на печать списка отозванных сертификатов, выделенного курсором.

Папка «Списки отозванных сертификатов» содержит следующий обязательный стандартный набор папок:

- «Действующие» - включает перечень списков отозванных сертификатов, период действия которых еще не истек.

2.5. Папка «Ключи УЦ»

В данной папке отображается список ключей удостоверяющего центра (см. Рис. 13).

Панель управления окна папки «Ключи УЦ» содержит следующий набор кнопок:

- «Подробнее...» - открывает окно свойств ключа УЦ, выделенного курсором (см. п. 3.3.4);
- «Новый...» - вызывает процедуру формирования нового ключа УЦ (см. п. 3.3.3);
- «Импорт...» - вызывает окно диалога импорта файла ключа УЦ;
- «Сертификация...» - вызывает диалог формирования сертификата ключа проверки ЭП УЦ (см. п. 3.3.5);
- «Экспорт...» - вызывает окно диалога для задания имени файла, в который будет экспортирован ключ УЦ, выделенный курсором (см. п. 3.3.6);
- «Создать запрос» - вызывает окно диалога для задания параметров запроса сертификата (см. п. 3.3.5.1);
- «Отозвать...» - вызывает процедуру отзыва ключа УЦ (см. п. 3.3.7);
- «Восстановить...» - вызывает процедуру восстановления действительного статуса отозванного ранее ключа УЦ (см. п. 3.3.8);
- «Удалить...» - удаляет из базы данных ключ УЦ, выделенный курсором (см. п. 3.3.9);
- «Печатать...» - вызывает окно диалога для загрузки на печать ключа УЦ, выделенного курсором.

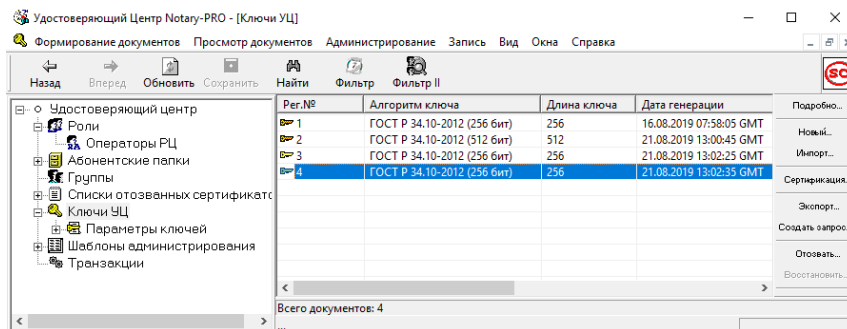


Рис. 13 Папка документов «Ключи УЦ»

2.5.1. Папка «Параметры ключей»

В папке «Параметры ключей» отображается список долговременных параметров, на основе которых генерируются ключи УЦ (см. Рис. 14).

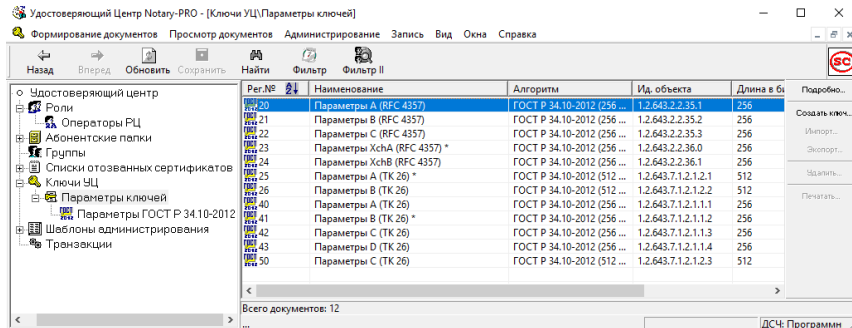


Рис. 14 Папка документов «Параметры ключей»

Панель управления окна папки «Параметры ключей» содержит следующий набор кнопок:

- «Подробнее...» - открывает страницы свойств параметров ключей, выделенных курсором (см. п.3.3.2);
- «Создать ключ» - вызывает процедуру создания ключа на основе параметров, выделенных курсором (см. п. 3.3.3);
- «Экспорт...» - вызывает окно диалога для задания имени файла, в который будут экспортированы параметры ключей;
- «Печатать...» - вызывает окно диалога для загрузки на печать параметров ключей, выделенных курсором; данная опция недоступна для параметров ключей ГОСТ Р 34.10-2001, приведенных в RFC 4357 [23], и параметров ключей ГОСТ Р 34.10-2012 [7].

Папка «Параметры ключей» содержит список зарегистрированных параметров ключей ГОСТ Р 34.10-2012 [7].

2.6. Папка «Шаблоны администрирования»

В данной папке отображается список шаблонов администрирования (см. Рис. 15).

Панель управления окна папки «Шаблоны администрирования» содержит следующий набор кнопок:

- «Подробнее...» - отображает окно свойств шаблона администрирования, выделенного курсором (см. п. 3.2.2);
- «Создать...» - вызывает процедуру создания нового шаблона администрирования (см. п. 3.2.1);
- «Удалить...» - удаляет из базы данных шаблон администрирования, выделенный курсором (см. п. 0).

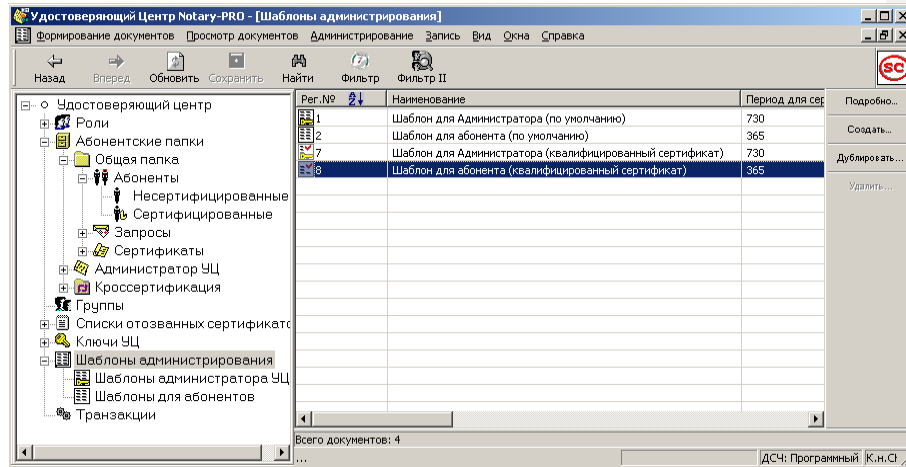


Рис. 15 Папка документов «Шаблоны администрирования»

Папка «Шаблоны администрирования» содержит следующие стандартные разделы:

- «Шаблоны Администратора УЦ» - содержит список шаблонов администрирования для сертификатов УЦ;
- «Шаблоны для абонентов» - содержит список шаблонов администрирования для сертификатов абонентов УЦ.

2.7. Папка «Транзакции»

В данной папке отображаются транзакции успешно обработанных запросов на сертификаты.

Область документов папки «Транзакции» разделяется на два окна (см. Рис. 16):

- в верхнем окне документов отображается список всех транзакций по обработке запросов в УЦ;
- в нижнем окне документов при нажатии на кнопку «Подробнее...» Панели управления окна «Транзакции» отображается информация о транзакции, выделенной курсором в верхнем окне документов.

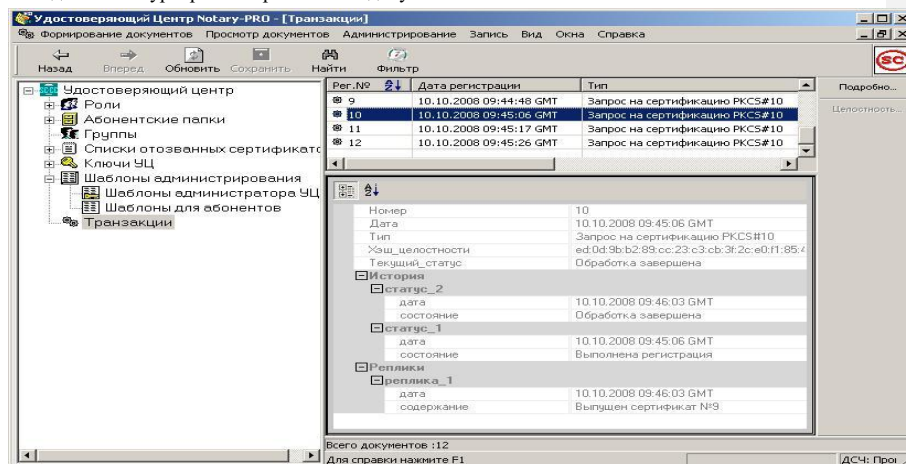


Рис. 16 Папка документов «Транзакции»

3. ДЕЙСТВИЯ АДМИНИСТРАТОРА

3.1. Установка параметров программы

Окно настроек параметров по умолчанию вызывается из главного меню, пункт «Администрирование/Установка параметров по умолчанию» и представляет собой многостраничный диалог.

3.1.1. Страница «Отображение данных»

Страница «Отображение данных» (см. Рис. 17) служит для настройки общих параметров отображения окон документов, а также настройки формата даты и времени. Здесь же настраиваются параметры фильтрации документов по дате регистрации.

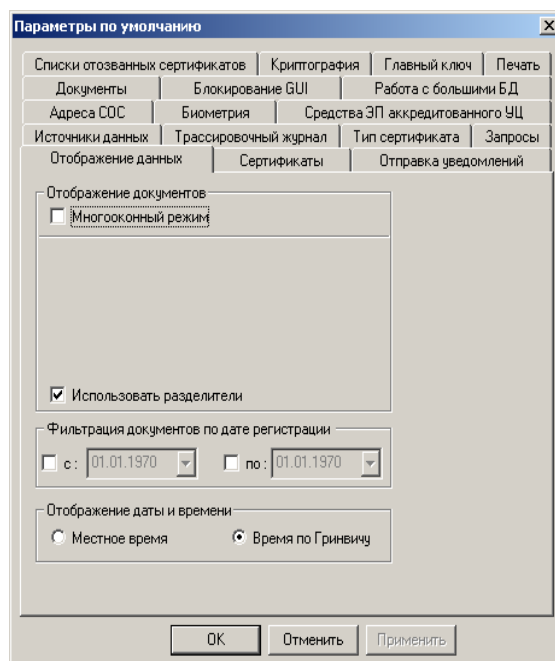


Рис. 17 Страница «Отображение данных» окна свойств параметров по умолчанию

Флажок «Многооконный режим» управляет отображением окон документов: при включенном флажке каждая папка документов отображается в отдельном окне.

Флажок «Использовать разделители» управляет отображением сетки в окнах документов.

«Фильтрация документов...» действует на папки «Абоненты», «Запросы» и «Сертификаты».

3.1.2. Страница «Сертификаты»

Страница «Сертификаты» (см. Рис. 18) предназначена для выбора рабочих сертификатов, а также установки дежурного сертификата УЦ.

Для поддерживаемых удостоверяющим центром алгоритмов ГОСТ Р 34.10-2001¹ и ГОСТ Р 34.10-2012 Администратором может быть назначен рабочий сертификат. С помощью рабочих сертификатов УЦ формируются сертификаты абонентов, если только в шаблоне администрирования не указан другой сертификат для подписи (см. п. 3.2.2.1).

¹ Использование ГОСТ Р 34.10-2001 ограничено в соответствии с п. 3.6 Формуляра ШКНР.00036-01 30 01.

Одному из рабочих сертификатов УЦ должен быть присвоен статус «Дежурный». Дежурный сертификат используется по умолчанию для формирования сертификатов абонентов в случае, если для соответствующего алгоритма не определен рабочий сертификат, либо в шаблоне администрирования не указан другой сертификат УЦ.

Смена дежурного и рабочих сертификатов может быть произведена в любой момент времени и фиксируется в журнале событий.

Кроме того, на этой странице можно установить интервал предупреждения об истечении периода действия сертификатов УЦ, а также установить срок хранения сертификатов в базе данных УЦ.

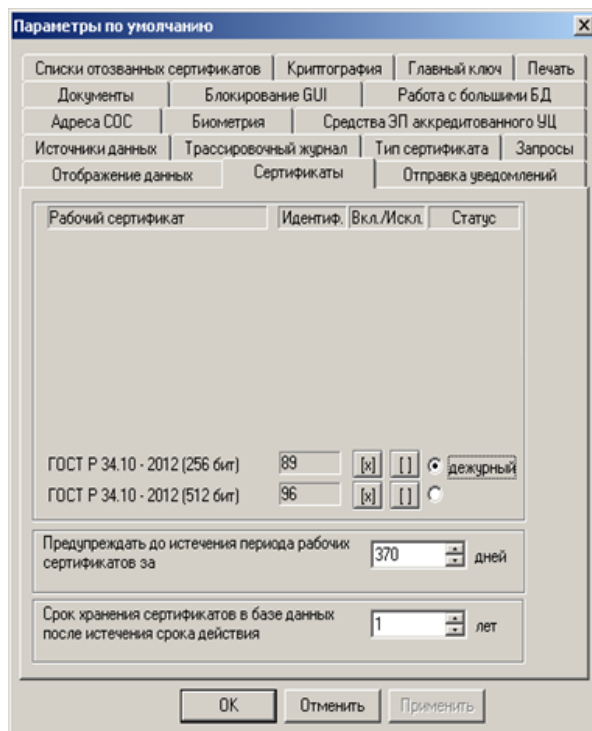


Рис. 18 Страница «Сертификаты» окна свойств параметров по умолчанию

3.1.3. Страница «Отправка уведомлений»

Страница «Отправка уведомлений» (см. Рис. 19) предназначена для управления процессом рассылки удостоверяющим центром почтовых уведомлений.

Удостоверяющий центр поддерживает возможность автоматической отправки абонентам уведомлений о регистрации поступающих запросов сертификатов (либо уведомлений об ошибках, произошедших при регистрации запросов).

Для отправки уведомления в запросе должно быть заполнено поле «Электронная почта», значение которого будет использовано в качестве адреса получателя уведомления.

Автоматическая отправка уведомления о регистрации запроса (см. п. 3.5.1) будет осуществляться только в том случае, если запрос импортирован из файловой системы (в ручном или автоматическом режимах). В случае, если запрос доставлен через Web-интерфейс, отправка уведомления будет осуществляться средствами приложения «Notary-PRO Web Pages».

При успешной регистрации запроса в качестве текста отправляемого сообщения будет использовано содержимое файла *BodyCompleteReqMail.txt*, а в качестве темы - содержимое файла *SubjectCompleteReqMail.txt*.

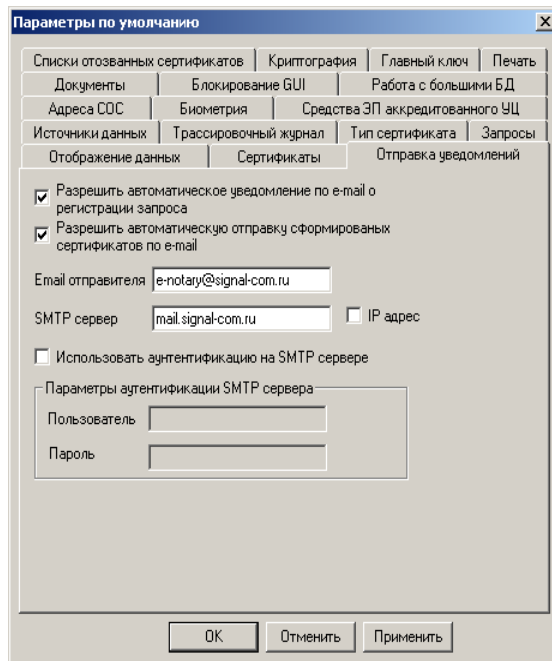


Рис. 19 Страница «Отправка уведомлений» окна свойств параметров по умолчанию

Если в ходе регистрации запроса произошла ошибка, то в качестве текста уведомления будет использовано содержимое файла *BodyErrorAddReqMail.txt*, а в качестве темы - содержимое файла *SubjectErrorAddReqMail.txt*.

Перечисленные файлы должны быть расположены в рабочем каталоге удостоверяющего центра «Notary-PRO».

Удостоверяющий центр поддерживает возможность автоматической отправки абонентам сформированных сертификатов.

Автоматическая отправка сформированного сертификата абонента будет осуществляться только в том случае, если в уникальном имени заполнено поле «Электронная почта».

Вместе с сертификатом абонента отправляется также соответствующая цепочка сертификатов УЦ и все необходимые списки отозванных сертификатов.

Если сертификация запроса прошла успешно, в качестве текста отправляемого сообщения будет использовано содержимое файла *BodyCertificationMail.txt*, а в качестве темы - содержимое файла *SubjectCertificationMail.txt*

Если в ходе сертификации запроса произошла ошибка, то в качестве текста уведомления будет использовано содержимое файла *BodyErrorCreateCertReqMail.txt*, а в качестве темы - содержимое файла *SubjectErrorCreateCertReqMail.txt*.

Перечисленные файлы должны быть расположены в рабочем каталоге удостоверяющего центра «Notary-PRO».

3.1.4. Страница «Списки отозванных сертификатов»

Страница «Списки отозванных сертификатов» (см. Рис. 20) служит для:

- установки периода действия списков отозванных сертификатов, используемого по умолчанию;
- задания параметров по организации планового формирования списков отозванных сертификатов в автоматическом режиме.

The screenshot shows a dialog box titled "Параметры по умолчанию" (Parameters by default). It has a tabbed interface with the following tabs: "Документы", "Блокирование GUI", "Работа с большими БД", "Адреса СОС", "Биометрия", "Средства ЭП аккредитованного УЦ", "Источники данных", "Трассировочный журнал", "Тип сертификата", "Запросы", "Отображение данных", "Сертификаты", "Отправка уведомлений", "Списки отозванных сертификатов", "Криптография", "Главный ключ", and "Печать". The "Списки отозванных сертификатов" (Lists of revoked certificates) tab is selected. It contains the following settings:

- "Период действия (дней)" (Validity period in days): 3
- ☒ "Плановое формирование списков отозванных сертификатов" (Scheduled formation of lists of revoked certificates)
 - "Дата и время начала формирования" (Start date and time of formation): 17.07.2014 20:42:02
 - "Периодичность" (Periodicity) table:

дни	часы	минуты
1	0	1
 - "Дата и время последней публикации" (Last publication date and time): 16.07.2014 12:41:02
 - Buttons: [] and "Выполнить сейчас ..." (Execute now ...)
- ☒ "Экспресс-формирование списков отозванных сертификатов" (Express formation of lists of revoked certificates)
 - "Интервал обработки запросов на отзыв/восстановление сертификатов (минуты)" (Interval for processing requests for revocation/restoration of certificates in minutes): 5

Buttons at the bottom: "ОК", "Отменить", "Применить".

Рис. 20 Страница «Списки отозванных сертификатов» окна свойств параметров по умолчанию

3.1.5. Страница «Криптография»

Страница «Криптография» (см. Рис. 21) служит для установки алгоритмов хэширования, используемых по умолчанию, для поддерживаемых асимметричных криптоалгоритмов ГОСТ.

The screenshot shows the same dialog box, but with the "Криптография" (Cryptography) tab selected. It contains the following settings:

- "Алгоритмы хэширования" (Hashing algorithms) section:
 - "Для ГОСТ Р 34.10-2012 (256 бит)" (For GOST R 34.10-2012 (256 bits)): ГОСТ Р 34.11-2012 (256 бит)
 - "Для ГОСТ Р 34.10-2012 (512 бит)" (For GOST R 34.10-2012 (512 bits)): ГОСТ Р 34.11-2012 (512 бит)

Buttons at the bottom: "ОК", "Отменить", "Применить".

Рис. 21 Страница «Криптография» окна свойств параметров по умолчанию

3.1.6. Страница «Трассировочный журнал»

Страница «Трассировочный журнал» (см. Рис. 22) служит для установки настроек журнала событий удостоверяющего центра.

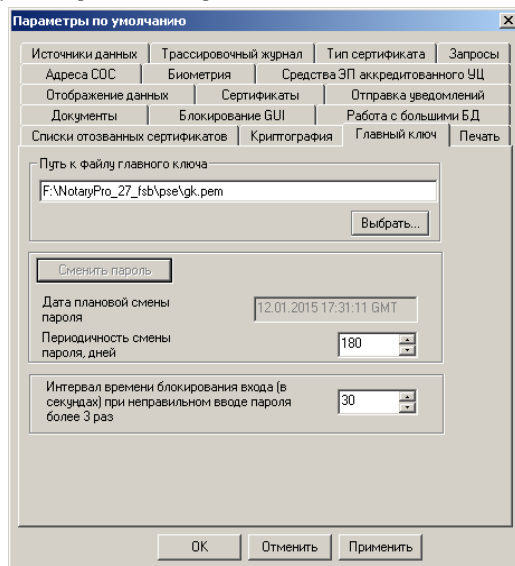


Рис. 22 Страница «Трассировочный журнал» окна свойств параметров по умолчанию

3.1.7. Страница «Главный ключ»

Страница «Главный ключ» (см. Рис. 23) используется для:

- установки пути к файлу главного ключа;
- смены пароля доступа к файлу главного ключа.

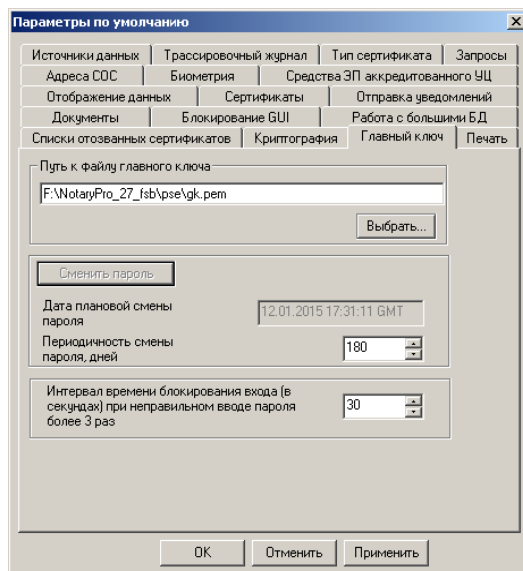


Рис. 23 Страница «Главный ключ» окна свойств параметров по умолчанию

Требования к паролю на главный ключ приводятся в п.1.11.2.

Периодичность смены пароля определяется параметром «Периодичность смены пароля, дней». Следующая дата смены пароля вычисляется при очередной смене пароля и отображается в поле «Дата плановой смены пароля».

В УЦ реализована возможность блокировки доступа к ресурсам УЦ: при неправильном вводе пароля более трех раз последующие попытки ввода пароля будут запрещены в течение периода времени (в секундах), который задается в поле «Интервал времени блокирования входа...».

3.1.8. Страница «Печать»

Страница «Печать» (см. Рис. 24) предназначена для настройки параметров печати документов удостоверяющего центра:

- параметров страницы;
- выбора шрифта, используемого при печати.

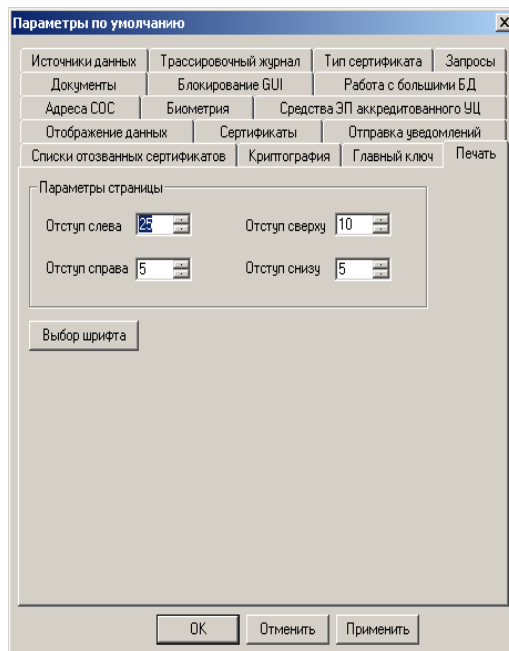


Рис. 24 Страница «Печать» окна свойств параметров по умолчанию

3.1.9. Страница «Источники данных»

Страница «Источники данных» (см. Рис. 25) предназначена для установки таймаута выполнения запросов к базе данных УЦ.

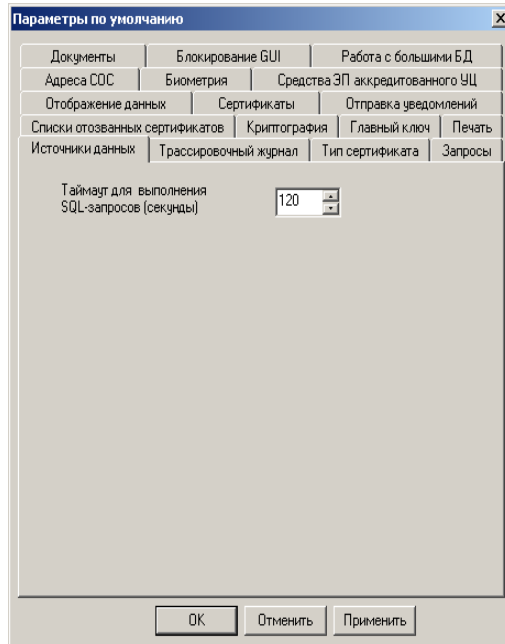


Рис. 25 Страница «Источники данных» окна свойств параметров по умолчанию

3.1.10. Страница «Тип сертификата»

Параметр «Тип сертификата» является вспомогательным идентификатором, который может передаваться в УЦ вместе с запросом на сертификат, расширяя перечень атрибутов запроса, обеспечивающих возможность более тонкой настройки фильтрации запросов по папкам с различными профилями (шаблонами) сертификации (см.п. 2.2.3.1).

Данный параметр используется также для автоматического разрешения коллизии имен, которая может возникать при обработке в УЦ запросов, имеющих одинаковые запрашиваемые имена, но поступающие из разных источников, обслуживающих разные прикладные системы с индивидуальными шаблонами сертификации: коллизия имен в рамках данного УЦ разрешается добавлением к атрибутам запроса типа сертификата.

Назначение типов сертификатов и их интерпретация определяется действующей Сертификационной политикой удостоверяющего Центра и устанавливается Администратором УЦ путем редактирования файла `crt_cls.lst.ini`, расположенного в каталоге запуска программы.

Например, Администратор УЦ может назначить тип сертификата в соответствии с типом той прикладной системы, в которой он будет использоваться: тип сертификата «Class 0» – для системы «Банк-Клиент», «Class 1» - для системы «Интернет-Банкинг», «Class 3» - для системы «Интернет-Брокер» и т.д.

Страница «Тип сертификата» (см. Рис. 26) предназначена для настройки способа присвоения параметра «Тип сертификата» при обработке регистрируемых запросов, выполняемой Администратором УЦ в ручном режиме:

- при установленной опции «Указать при ручной регистрации нового абонента» окно для выбора типа сертификата будет открываться при регистрации нового абонента (см.п.3.4.1);
- при установленной опции «Указать при ручной регистрации запроса» окно для выбора типа сертификата будет открываться при регистрации запроса (см. п.3.5.1).

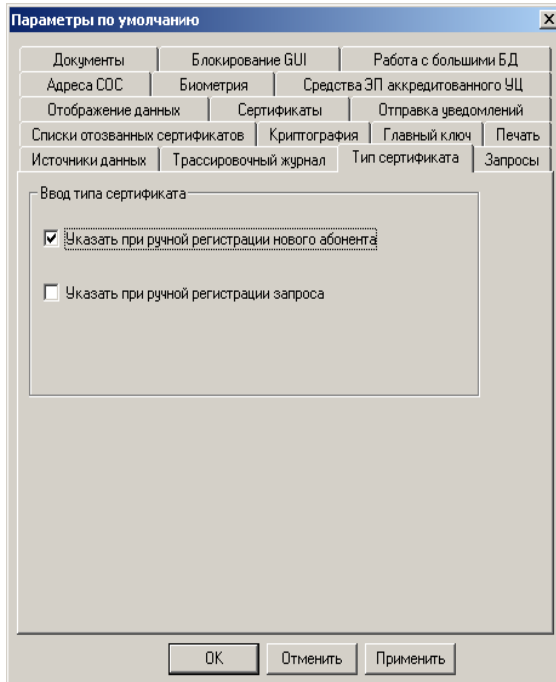


Рис. 26 Страница «Тип сертификата» окна свойств параметров по умолчанию

3.2. Шаблоны администрирования

Шаблоны администрирования используются для хранения значений параметров сертификации.

Шаблоны администрирования подразделяются на две категории:

- шаблоны для абонентов (используются при сертификации запросов);
- шаблоны Администратора УЦ (используются при сертификации ключей УЦ).

Шаблон администрирования может быть назначен для папки либо индивидуально для абонента.

3.2.1. Создание шаблона администрирования

Для создания нового шаблона администрирования необходимо:

- находясь в папке «Шаблоны администрирования», на Панели управления окна данной папки нажать кнопку «Создать...»;
- в окне диалога ввести имя нового шаблона;
- параметры нового шаблона наследуются из шаблона, который в момент нажатия кнопки «Создать...» был активным;
- на страницах свойств шаблона настроить параметры нового шаблона и сохранить изменения.

3.2.2. Окно свойств шаблона администрирования

Вызывается по кнопке «Подробнее...» Панели управления; представляет собой многостраничный диалог.

3.2.2.1. Страница «Параметры»

Страница «Параметры» (см. Рис. 27) содержит следующие атрибуты шаблона администрирования:

Рис. 27 Страница «Параметры» окна свойств шаблона администрирования

- «Наименование» - имя шаблона администрирования;
- «Период действия сертификата (дней)» - задает значение по умолчанию для периода действия создаваемых сертификатов (в сутках);
- «Номер сертификата УЦ» - номер сертификата УЦ, который будет использован при создании сертификатов;
- «Имя в сертификате» - указывает, какое имя включать в сертификат по умолчанию: из запроса или из регистрационной записи абонента;
- «Кодировка символов» - задает тип кодировки атрибутов уникального имени (ANSI, Unicode или UTF8).

3.2.2.2. Страница «Расширения»

Страница «Расширения» (см. Рис. 28) содержит список расширений, включаемых по умолчанию в сертификат, создаваемый по данному шаблону.

По кнопке «Добавить» можно добавить расширения, по кнопке «Удалить» - удалить.

Выделив курсором конкретное расширение и нажав кнопку «Подробнее...», можно отредактировать свойства расширения.

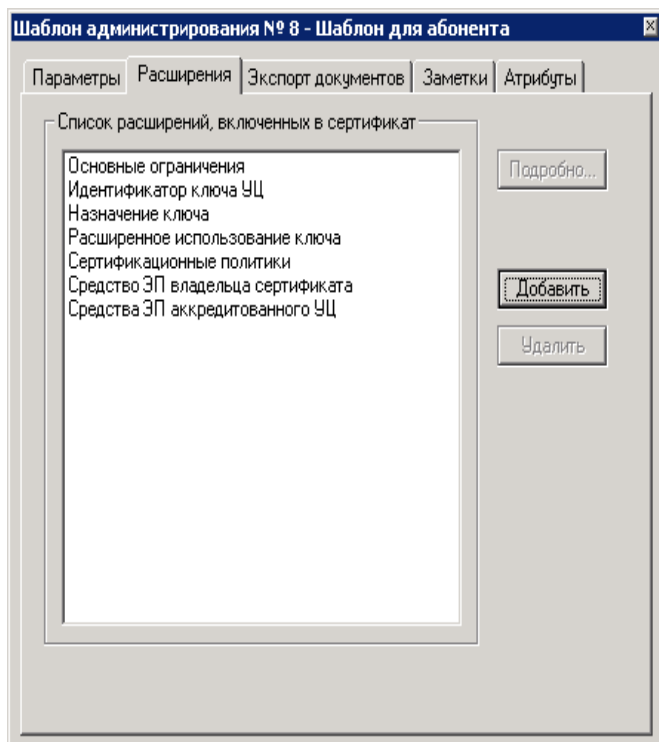


Рис. 28 Страница «Расширения» окна свойств шаблона администрирования
Действия Администратора по настройке расширений подробно описаны в п.4.

3.2.2.3. Страница «Экспорт документов»

Страница «Экспорт документов» (см. Рис. 29) содержит следующие атрибуты:

- «Формат экспорта запросов» - может быть следующим:
 - ☐ PEM (текстовый);
 - ☐ DER (бинарный).

При выборе формата PEM можно установить флаг включения текстового заголовка.

- «Формат экспорта сертификатов» - может быть следующим:
 - ☐ PEM (текстовый);
 - ☐ DER (бинарный);
 - ☐ PFX (PKCS #12, в соответствии с [26]);
 - ☐ P7B (PKCS #7, в соответствии с [20]).

При выборе формата PEM можно установить флаг включения текстового заголовка.

В разделе «Префикс имени файла» Администратор может назначить различные значения для префиксов, подставляемых в имена файлов экспортируемых сертификатов абонентов и сертификатов УЦ. При установленной опции «подставить Полное Имя абонента при экспорте в файл» к префиксу в имени файла сертификата добавляется значение атрибута «Полное имя» (Common Name) из состава сертификата.

- «Формат экспорта списков отмены» - может быть следующим:
 - ☐ PEM (текстовый);
 - ☐ CRL (бинарный).

При выборе формата PEM можно установить флаг включения текстового заголовка.

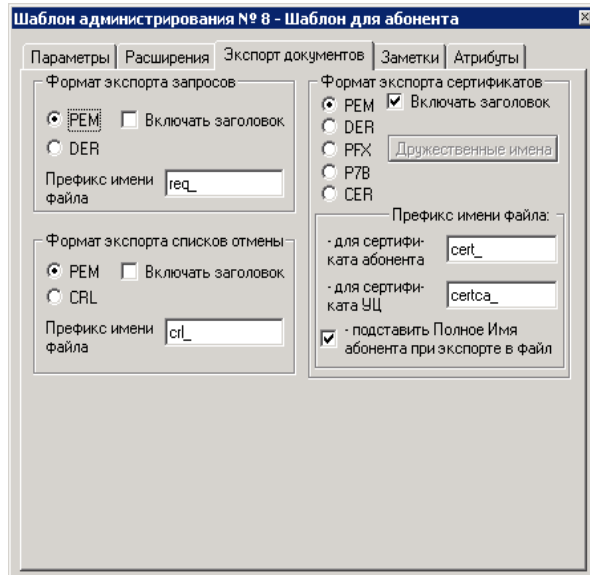


Рис. 29 Страница «Экспорт документов» окна свойств шаблона администрирования

3.2.2.4. Страница «Заметки»

Страница «Заметки» содержит комментарии администратора.

3.2.2.5. Страница «Атрибуты»

Страница «Атрибуты» содержит не редактируемый упорядоченный список атрибутов, определяющий их порядок следования в сертификате, изготовленном по данному шаблону. Требуемый порядок следования атрибутов задается специализированными мастер-шаблонами, которые не подлежат удалению.

3.2.3. Удаление шаблона администрирования

Для удаления шаблона администрирования необходимо, находясь в папке «Шаблоны администрирования», выделить нужный шаблон курсором и на Панели управления окна данной папки нажать кнопку «Удалить...».

Нельзя удалить системный мастер-шаблон и шаблон, на который имеется ссылка в свойствах зарегистрированного абонента или абонентской папки.

3.3. Ключи УЦ

3.3.1. Параметры ключей

Для алгоритма ГОСТ Р 34.10-2001¹ и ГОСТ Р 34.10-2012 ключи УЦ генерируются на основе долговременных параметров ключей, которые регистрируются в базе данных УЦ. Для каждого из указанных алгоритмов имеется хотя бы по одному набору параметров, используемых по умолчанию.

Параметры алгоритмов ГОСТ Р 34.10-2001[23] и ГОСТ Р 34.10-2012 [7] сведены в отдельные группы (см. п. 2.5.1) .

3.3.2. Окно свойств параметров ключей

Вызывается по кнопке «Подробнее...» Панели управления; представляет собой многостраничный диалог.

¹ Использование ГОСТ Р 34.10-2001 ограничено в соответствии с п. 3.6 Формуляра ШКНР.00036-01 30 01.

3.3.2.1. Страница «Главная»

Страница «Главная» (см. Рис. 30) содержит следующие атрибуты параметров ключа:

- «Ид. объекта» - стандартный идентификатор объекта для параметра (OID);
- «Алгоритм» - алгоритм параметров ключа;
- «Длина в битах» - длина параметров ключа;
- «Дата регистрации» - дата регистрации параметров ключа.

Параметры ключей. Рег.№ 20

Главная | Ключи УЦ | Текст | Заметки

Наименование
параметры цифровой подписи А: ГОСТ Р 34.10-2012 (256 бит)

Ид. объекта
1.2.643.2.2.35.1

Алгоритм
ГОСТ Р 34.10-2012 (256 бит)

Длина в битах
256

Дата регистрации
02.09.2013 10:47:20 GMT

Рис. 30 Страница «Главная» окна свойств параметров ключа УЦ

3.3.2.2. Страница «Ключи УЦ»

Страница «Ключи УЦ» (см. Рис. 31) содержит список ключей УЦ, созданных на основе данных параметров.

При нажатии кнопки «Подробнее...» на экран выводится окно свойств выделенного ключа УЦ (окно свойств параметров ключа остается активным).

При нажатии кнопки «Перейти...» выводится окно свойств выделенного ключа УЦ (окно свойств ключа становится активным, окно свойств параметров ключа закрывается).

При нажатии кнопки «Отдельное окно» создается новая выборка (см. п. 3.9), содержащая записи, отображаемые в настоящем окне.

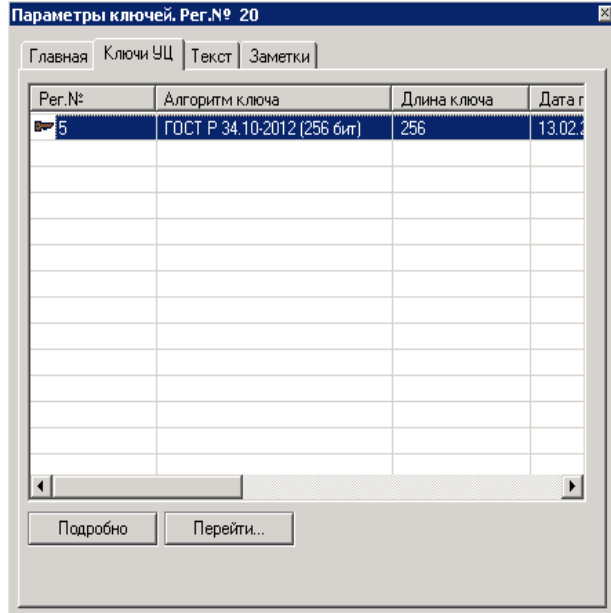


Рис. 31 Страница «Ключи УЦ» окна свойств параметров ключа УЦ

3.3.2.3. Страница «Текст»

Страница «Текст» (см. Рис. 32) содержит текст параметров ключей (пример для ключей ГОСТ Р 34.10-2001 (SC) с параметрами NIST (см. п.2.8.2 [33]).

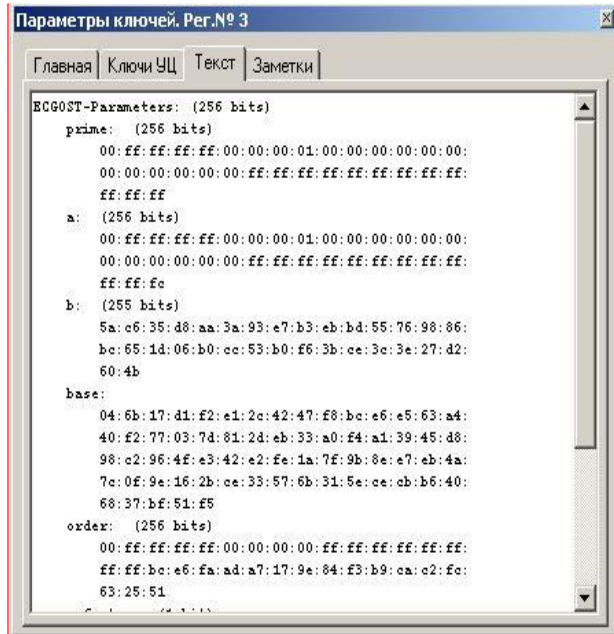


Рис. 32 Страница «Текст» окна свойств параметров ключа УЦ

Примечание [t1]:

Примечание [t2]:

3.3.2.4. Страница «Заметки»

Страница «Заметки» содержит комментарии администратора.

3.3.3. Генерация ключа УЦ

Для генерации новой пары ключей УЦ необходимо в Главном меню программы выбрать пункт «Формирование документов/Ключи УЦ/Генерация нового ключа» или, находясь в папке «Ключи УЦ», на Панели управления окна данной папки нажать кнопку «Новый».

В появившемся окне выбора параметров ключей (см. Рис. 33) Администратор должен выполнить следующие действия:

- выбрать один из поддерживаемых программой двухключевых алгоритмов из выпадающего списка «Алгоритм ключа»:
 - ГОСТ Р 34.10-2012
- выбрать параметры ключей из выпадающего списка; выбор производится из списка зарегистрированных параметров (см. п. 3.3.1);
- нажать кнопку «Создать ключ»;

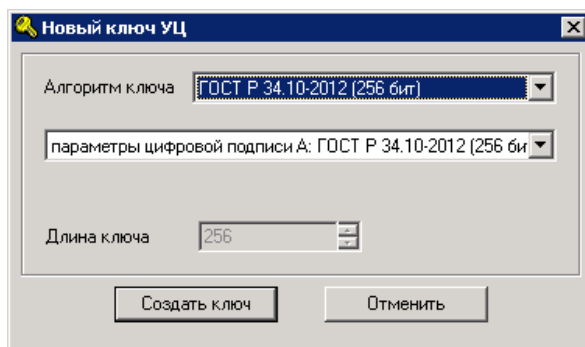


Рис. 33 Диалог выбора параметров новой пары ключей

- дождаться конца процесса генерации (см. Рис. 34); процедура генерации ключа может занять от нескольких секунд до нескольких минут, в зависимости от выбранного алгоритма, длины ключа и быстродействия компьютера; процесс генерации может быть прерван в любой момент нажатием кнопки «Отмена».

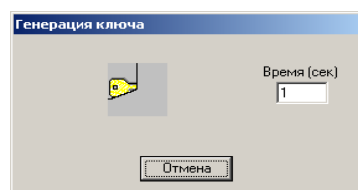


Рис. 34 Диалог генерации ключей

Для алгоритма ГОСТ Р 34.10-2012 предусмотрена также возможность генерации новой пары ключей на основе долговременных параметров ключей, зарегистрированных в базе данных УЦ (см.п. 3.3.1).

При этом для генерации ключей необходимо, находясь в папке «Ключи УЦ/Параметры ключей», нажать кнопку «Создать ключ...» на Панели управления.

После окончания процесса генерации ключа Администратор получает возможность:

- просмотреть подробную информацию о новом ключе (см.п. 3.3.4);
- сформировать сертификат УЦ для нового ключа (см. п. 3.3.5);
- сформировать запрос сертификата для нового ключа (см. п. 3.3.5.1);
- экспортировать ключ УЦ в файловую систему (см.п. 3.3.6).

3.3.4. Окно свойств ключа УЦ

Вызывается по кнопке «Подробнее...» Панели управления; представляет собой многостраничный диалог.

3.3.4.1. Страница «Параметры»

Страница «Параметры» (см. Рис. 35) содержит следующие атрибуты ключа УЦ:

- «Алгоритм ключа» - идентификатор алгоритма;
- «Длина ключа» - длина ключа;
- «Дата генерации» - дата генерации ключа;
- «Дата отмены» - дата отмены ключа (если он был отменен);
- «Номер параметров ключа» - регистрационный номер параметров ключа, на основе которых был создан данный ключ;
- «Путь к ключевому носителю СКЗИ» - путь к ключевому контейнеру формата СКЗИ «CADB 2.1».

Ключ УЦ № 14 - Рабочий

Параметры | Сертификаты | Запросы | Текст | Заметки

Алгоритм ключа: ГОСТ Р 34.10-2012 (256 бит)

Длина ключа: 256

Дата генерации: 01.10.2015 11:23:08

Дата отмены:

Номер параметров ключа: 20 ... -->

Путь к ключевому носителю СКЗИ: Изменить

Рис. 35 Страница «Параметры» окна свойств ключа УЦ

3.3.4.2. Страница «Сертификаты»

Страница «Сертификаты» (см. Рис. 36) содержит список сертификатов УЦ, соответствующих данному ключу УЦ.

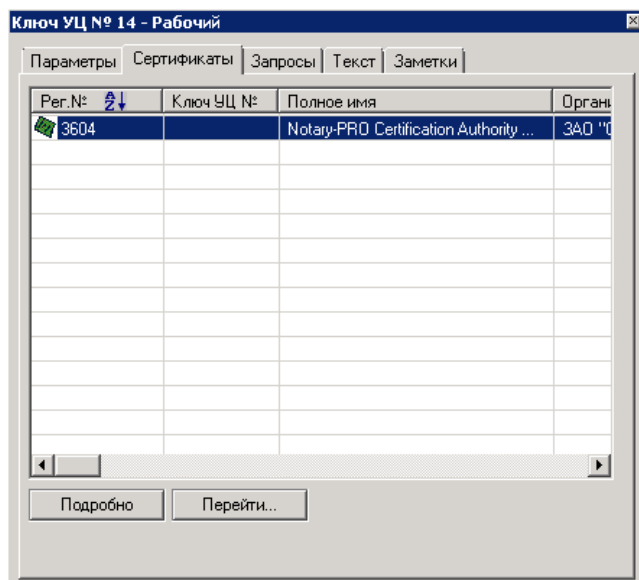


Рис. 36 Страница «Сертификаты» окна свойств ключа УЦ

При нажатии кнопки «Подробнее...» на экран выводится окно свойств выделенного сертификата УЦ (окно свойств ключа остается активным).

При нажатии кнопки «Перейти» выводится окно свойств выделенного сертификата УЦ (окно свойств сертификата становится активным, окно свойств ключа закрывается).

При нажатии кнопки «Отдельное окно» создается новая выборка (см. п. 3.9), содержащая записи, отображаемые в настоящем окне.

3.3.4.3. Страница «Запросы»

Страница «Запросы» (см. Рис. 37) содержит список запросов на сертификацию, сформированных для данного ключа УЦ.

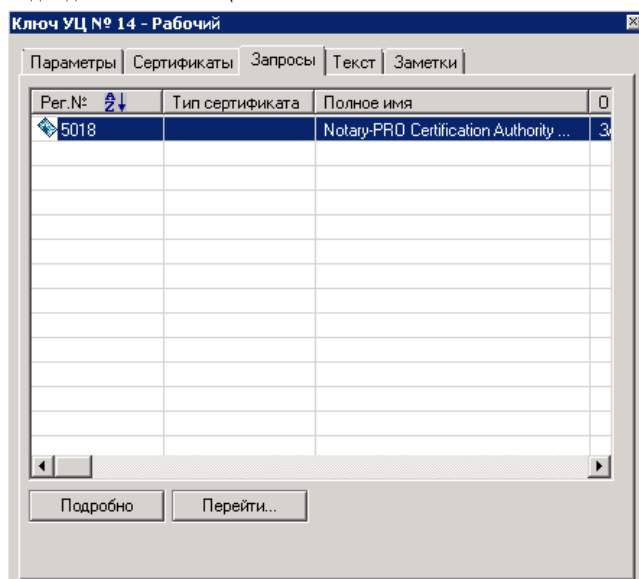


Рис. 37 Страница «Запросы» окна свойств ключа УЦ

При нажатии кнопки «Подробнее...» на экран выводится окно свойств выделенного запроса УЦ (окно свойств ключа остается активным).

При нажатии кнопки «Перейти» выводится окно свойств выделенного запроса УЦ (окно свойств запроса становится активным, окно свойств ключа закрывается).

При нажатии кнопки «Отдельное окно» создается новая выборка (см. п. 3.9), содержащая записи, отображаемые в настоящем окне.

3.3.4.4. Страница «Текст»

Страница «Текст» (см. Рис. 38) содержит текст ключа УЦ (в зашифрованном виде).

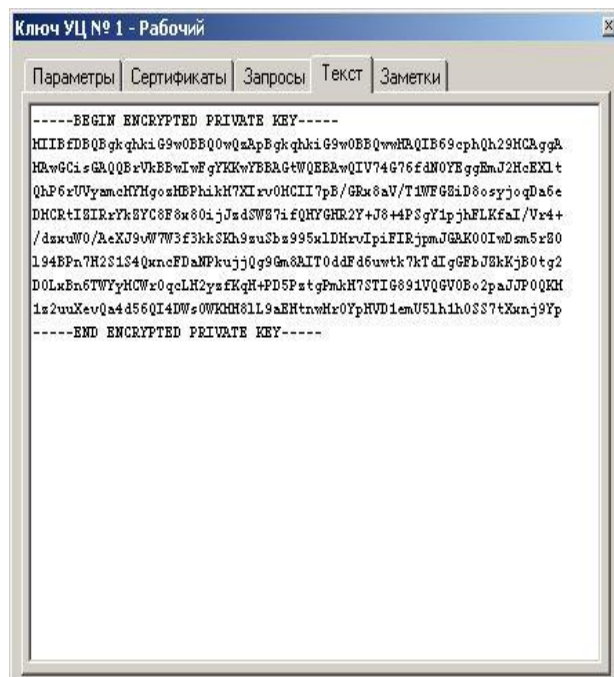


Рис. 38 Страница «Текст» окна свойств ключа УЦ

3.3.4.5. Страница «Заметки»

Страница «Заметки» содержит комментарии Администратора.

3.3.5. Формирование сертификата УЦ

На каждый ключ УЦ может быть выпущено произвольное число сертификатов.

Для формирования сертификата УЦ необходимо:

- находясь в папке «Ключи УЦ», выделить курсором нужный ключ;
- на Панели управления окна данной папки нажать кнопку «Сертификация...».

При этом Администратору выдается многостраничное окно с параметрами сертификации.

После ввода всех необходимых параметров необходимо нажать кнопку «Создать».

3.3.5.1. Страница «Шаблоны»

Страница «Шаблоны» (см. Рис. 39) предназначена для выбора шаблона администрирования, в соответствии с которым будет сформирован сертификат УЦ. Подробнее о настройке шаблонов администрирования см. п. 3.2.

Для формирования сертификата достаточно нажать кнопку «Создать». Однако перед этим Администратор может установить значения параметров сертификата, отличные от параметров шаблона

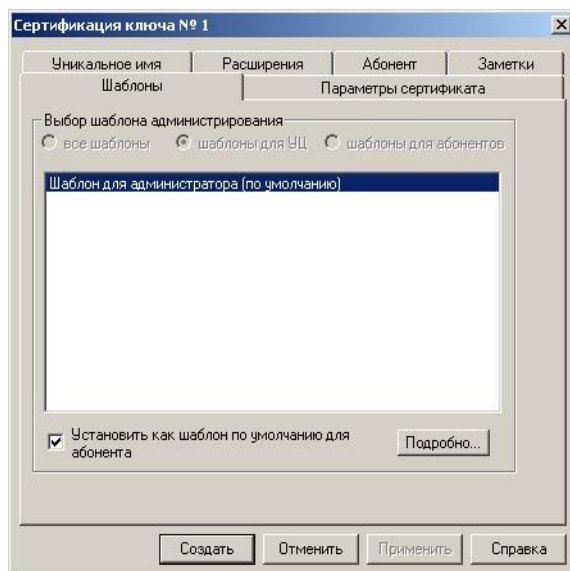


Рис. 39 Страница «Шаблоны» окна свойств параметров сертификации ключа УЦ

3.3.5.2. Страница «Параметры сертификата»

На странице «Параметры сертификата» (см. Рис. 40) Администратору предоставляется возможность:

The screenshot shows a software window titled 'Сертификация ключа № 14'. It has several tabs: 'Расширения', 'Абонент', 'Заметки', 'Биометрические данные', 'Шаблоны', 'Параметры сертификата' (which is active), and 'Уникальное имя'. The 'Параметры сертификата' tab contains the following fields and controls:

- 'Период действия (дней)': a numeric input field with the value '730'.
- 'Начало периода': a date dropdown menu showing '21 августа 2019 г.'.
- 'Конец периода': a date dropdown menu showing '20 августа 2021 г.'.
- 'Алгоритм открытого ключа': a dropdown menu showing 'ГОСТ Р 34.10-2012 (256 бит)'.
- 'Длина ключа в битах': a numeric input field with the value '256'.
- 'Подписать сертификатом УЦ №': a text input field followed by a browse button ('...').
- Two checkboxes:
 - ☒ 'Включить расширения'
 - ☐ 'Сохранить как рабочий сертификат'

At the bottom of the window are two buttons: 'Создать' and 'Отменить'.

Рис. 40 Страница «Параметры сертификата» окна свойств параметров сертификации ключа УЦ

- установить период действия сертификата УЦ либо установить даты начала и окончания периода действия сертификата;
- изменить сертификат удостоверяющего центра, используемый при формировании сертификата (если формируется незамоподписанный сертификат УЦ);
- Администратору предоставляется возможность сделать новый сертификат рабочим сертификатом УЦ (см.п. 3.1.2).

3.3.5.3. Страница «Уникальное имя»

На странице «Уникальное имя» (см. Рис. 41) Администратор может установить атрибуты уникального имени, которое будет включено в новый сертификат УЦ.

The screenshot shows a window titled 'Сертификация ключа № 4'. It has four tabs: 'Расширения', 'Абонент', 'Заметки', and 'Биометрические данные'. The 'Уникальное имя' sub-tab is active, showing a list of attributes for a unique name. The attributes and their values are:

Атрибуты уникального имени	
Полное имя	Удостоверяющий центр Notary-PI
Организация	ЗАО "Сигнал-KOM"
Подразделение	Удостоверяющий центр
Должность	x
Страна	RU
Город село	Москва
Область район	77 г. Москва
Электронная почта	sa@signal-com.ru
ИНН	00771402893
ОГРН	1027700239863
СНИЛС	x
Фамилия	x
Имя Отчество	x
Адрес	x
Почтовый адрес	x
Неструктурированное имя	x
Псевдоним	x
Серийный номер	x
Описание	x

Below the list, there are three radio buttons: 'Имя из запроса' (unselected), 'Как у абонента' (selected), and 'Выбрать из списка имен'. At the bottom are 'Создать' and 'Отменить' buttons.

Рис. 41 Страница «Уникальное имя» окна свойств параметров сертификации ключа УЦ

3.3.5.4. Страница «Расширения»

На странице «Расширения» (см. Рис. 42) Администратору предоставляется возможность настроить параметры расширений сертификата.

Действия Администратора по настройке расширений подробно описаны в п. 4.

The screenshot shows a window titled 'Сертификация ключа № 1'. It has four tabs: 'Шаблоны', 'Параметры сертификата', 'Уникальное имя', and 'Расширения'. The 'Расширения' sub-tab is active, showing a list of extensions included in the certificate. The list contains:

- Основные ограничения
- Идентификатор ключа
- Флаги использования ключа

There are three buttons on the right: 'Подробнее...', 'Добавить', and 'Удалить'. At the bottom are 'Создать', 'Отменить', 'Применить', and 'Справка' buttons.

Рис. 42 Страница «Расширения» окна свойств параметров сертификации ключа УЦ

3.3.5.5. Страница «Абонент»

Страница «Абонент» (см. Рис. 43) содержит данные об Администраторе.

Сертификация ключа № 4

Шаблоны | Параметры сертификата | Уникальное имя

Расширения | Абонент | Заметки | Биометрические данные

Рег. №: 1 | Идентификатор: Notary-PRO v.2.7

Атрибуты уникального имени

Полное имя	Удостоверяющий центр Notary-PF
Организация	ЗАО "Сигнал-КОМ"
Подразделение	Удостоверяющий центр
Должность	x
Страна	RU
Город село	Москва
Область район	77 г. Москва
Электронная почта	sa@signal-com.ru
ИНН	007714028893
ОГРН	1027700239863
СНИЛС	x
Фамилия	x
Имя Отчество	x
Адрес	x
Почтовый адрес	x
Неструктурированное имя	x
Псевдоним	x
Сериальный номер	x

Создать | Отменить

Рис. 43 Страница «Абонент» окна свойств параметров сертификации ключа УЦ

3.3.5.6. Страница «Заметки»

Страница «Заметки» хранит комментарии Администратора.

3.3.6. Экспорт ключа УЦ

Ключ УЦ может быть экспортирован из базы данных УЦ в файловую систему.

Для экспорта ключа УЦ необходимо:

- находясь в папке «Ключи УЦ», выделить курсором нужный ключ;
- на Панели управления окна данной папки нажать кнопку «Экспорт...»;
- указать имя файла для сохранения ключа;
- ввести пароль для шифрования ключа.

После перехода УЦ в режим работы по схеме «с разделением секрета» (см. п. 1.11.3) возможность экспорта ключа УЦ в файловую систему блокируется.

3.3.7. Отзыв ключа УЦ

Процедура отзыва ключа УЦ выполняется при компрометации этого ключа.

Для отзыва ключа УЦ необходимо:

- находясь в папке «Ключи УЦ», выделить курсором нужный ключ;
- на Панели управления окна данной папки нажать кнопку «Отозвать...».

При отмене ключа УЦ отменяются также:

- все сертификаты УЦ, выпущенные для этого ключа;
- все сертификаты абонентов, выпущенные с использованием отозванных сертификатов УЦ (только после подтверждения Администратора).

Отозванный ключ может быть в дальнейшем восстановлен (см. п. 3.3.8).

3.3.8. Восстановление ключа УЦ

Отозванный ранее ключ может быть восстановлен Администратором.

Для восстановления отозванного ключа УЦ необходимо:

- находясь в папке «Ключи УЦ», выделить курсором нужный ключ;
- на Панели управления окна данной папки нажать кнопку «Восстановить...».

3.3.9. Удаление ключа УЦ

Для удаления ключа УЦ необходимо, находясь в папке «Ключи УЦ», выделить курсором нужный ключ и на Панели управления окна данной папки нажать кнопку «Удалить».

Перед удалением ключа УЦ необходимо удалить:

- все сертификаты УЦ, сформированные для этого ключа;
- все запросы, сформированные для этого ключа.

3.4. Абоненты

3.4.1. Регистрация абонента

Для регистрации нового абонента необходимо:

- в Главном меню программы выбрать пункт «Формирование документов/Регистрация нового абонента»;
- или в абонентских папках Главной панели выбрать папку «Абоненты» и на Панели управления окна данной папки нажать кнопку «Новый» (см. п. 2.2.2).

В появившемся окне регистрации нового абонента (см. Рис. 44) нужно заполнить необходимые поля и нажать кнопку «Сохранить».

Рис. 44 Окно регистрации нового абонента

Единственным обязательным для заполнения полем является поле «Идентификатор»; идентификатор должен быть уникальным.

Остальные поля составляют группу атрибутов, образующих в совокупности имя абонента, уникальное в контексте данного УЦ. Эти атрибуты включаются по умолчанию в сертификаты абонента.

Идентификатор, уникальное имя и другие атрибуты абонента могут быть в дальнейшем изменены Администратором.

Если в настройках установки типа сертификата задана опция «Указать при ручной регистрации нового запроса» (см.п. 3.1.10), открывается окно (см. Рис. 45), в котором необходимо выделить нужный тип сертификата и нажать кнопку «Выбрать». В результате, к контексту идентификатора абонента добавится идентификатор типа сертификата, указывающий на то, что уникальное имя абонента является составным. Это означает, что при автоматической регистрации запросов к данному абоненту смогут «привязаться» только запросы с аналогичным запрашиваемым именем и таким же значением параметра «Тип сертификата».

При создании записи о новом абоненте параметры уникального имени заполняются данными из шаблона имени абонентской папки, в которой создается новая запись (см.п. 2.2.3.2).

Если процедура регистрации нового абонента была вызвана из «Общей папки» поля новой записи заполняются атрибутами абонента, выделенного курсором.

Состав и количество заполняемых полей атрибутов абонента определяются Администратором и могут быть различными для разных абонентов.

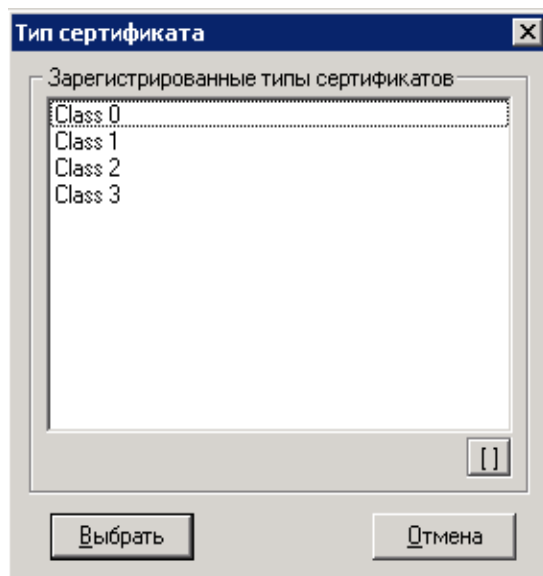


Рис. 45 Окно выбора типа сертификата

3.4.2. Окно свойств абонента

Вызывается по кнопке «Подробнее...» Панели управления; представляет собой многостраничный диалог.

3.4.2.1. Страница «Параметры»

Страница «Параметры» (см. Рис. 46) содержит следующие атрибуты абонента:

Абонент № 2 - Сертифицированный

Заметки | Документы | Справочные атрибуты | Доступ к субъекту

Параметры | Список имен | Сертификаты | Запросы | Специальные атрибуты

Идентификатор: Открытое акционерное общество "Организация" (AU)

⊖ Атрибуты уникального имени

Полное имя	Открытое акционерное общество
Организация	ОАО "Организация"
Подразделение	Дирекция
Должность	Генеральный директор
Страна	RU
Город село	Москва
Область район	77 г. Москва
Электронная почта	mail@organisation.ru
ИНН	001234567894
ОГРН	1027700239863
СНИЛС	
Фамилия	Фамилия
Имя Отчество	Имя Отчество
Адрес	"
Почтовый адрес	"
Неструктурированное имя	"
Псевдоним	"

Дата регистрации: 13.02.2014 13:22:08 GMT

Рис. 46 Страница «Параметры» окна свойств абонента

- «Идентификатор» - уникальный идентификатор абонента в базе данных удостоверяющего центра;
- Атрибуты абонента (уникальный набор);
- «Дата регистрации» - дата создания записи.

3.4.2.2. Страница «Список имен»

Страница «Список имен» (см. Рис. 47) содержит список уникальных имен абонента, включенных в сформированные удостоверяющим центром сертификаты абонента.

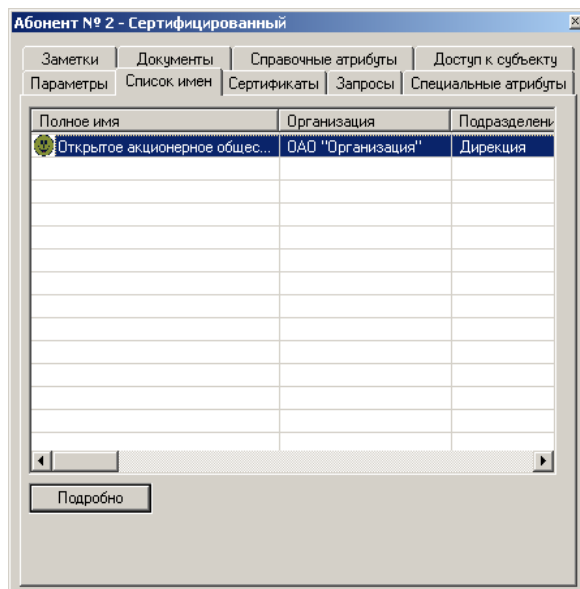


Рис. 47 Страница «Список имен» окна свойств абонента

При нажатии кнопки «Подробнее...» выделенное курсором уникальное имя выводится в форме просмотра (см. Рис. 48).

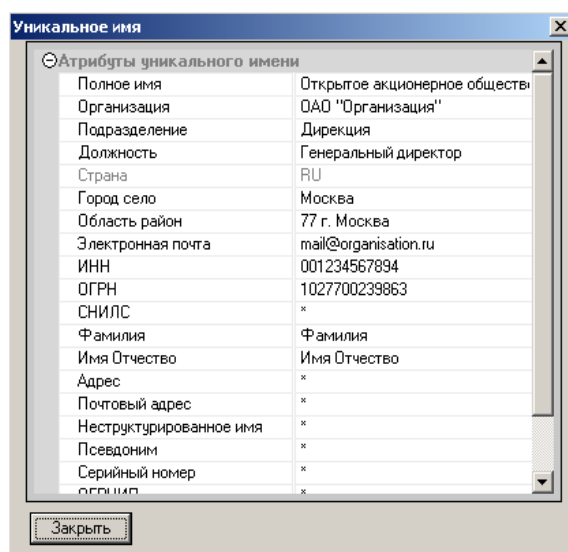


Рис. 48 Форма просмотра уникального имени

3.4.2.3. Страница «Сертификаты»

Страница «Сертификаты» (см. Рис. 49) содержит список сертификатов данного абонента.

При нажатии кнопки «Подробнее...» на экран выводится окно свойств выделенного сертификата абонента (окно свойств абонента остается активным).

При нажатии кнопки «Перейти...» выводится окно свойств выделенного сертификата (окно свойств сертификата становится активным, окно свойств абонента закрывается).

При нажатии кнопки «Отдельное окно» создается новая выборка (см. п. 3.9), содержащая сертификаты данного абонента.

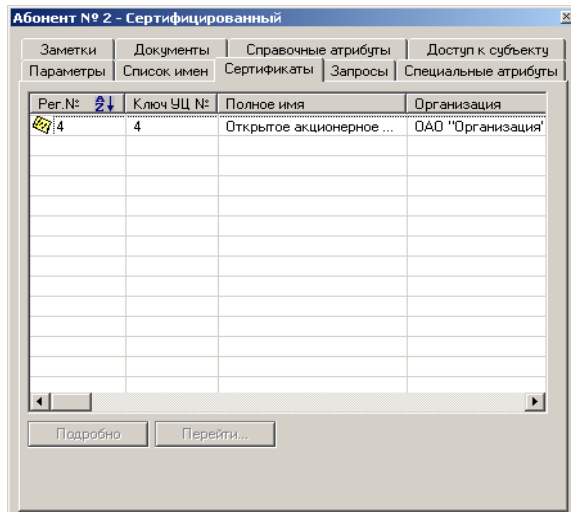


Рис. 49 Страница «Сертификаты» окна свойств абонента

3.4.2.4. Страница «Запросы»

Страница «Запросы» (см. Рис. 50) содержит список запросов данного абонента.

При нажатии кнопки «Подробнее...» на экран выводится окно свойств выделенного запроса (окно свойств абонента остается активным).

При нажатии кнопки «Перейти...» выводится окно свойств выделенного запроса (окно свойств запроса становится активным, окно свойств абонента закрывается).

При нажатии кнопки «Отдельное окно» создается новая выборка (см. п. 3.9), содержащая запросы данного абонента.

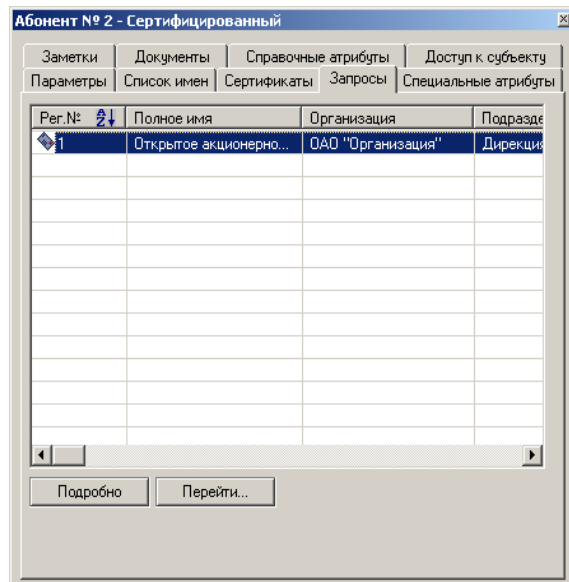


Рис. 50 Страница «Запросы» окна свойств абонента

3.4.2.5. Страница «Специальные атрибуты»

Страница «Специальные атрибуты» (см. Рис. 51) содержит следующую информацию:

- «Почтовый адрес» - почтовый адрес абонента;
- «Телефоны» - контактные телефоны абонента;
- «Факс» - номер факса абонента;
- кнопки доступа к аварийному паролю абонента:
 - ☐ кнопка «Проверить» - Администратор может проверить текущий аварийный пароль абонента (например, при передаче пароля абонентом по телефону);
 - ☐ кнопка «Сменить» - Администратор может сменить текущий аварийный пароль данного абонента;
- «Альтернативное имя» - установив флаг использования альтернативного имени абонента, Администратор может задать атрибуты дополнительного имени по кнопке «Редактировать»; дополнительное имя включается в сертификаты данного абонента в виде расширения Subject Alternative Name (см. п. 4.7); если флаг использования альтернативного имени абонента был установлен, но ни один атрибут дополнительного имени задан не был, то при закрытии окна свойств абонента данный флаг будет сброшен;
- «Шаблон администрирования» - каждому абоненту удостоверяющего центра может быть назначен индивидуальный шаблон администрирования (см. п. 3.1), по которому будет производиться сертификация запросов данного абонента, независимо от шаблона администрирования, установленного для папки, в которой находится запись об абоненте;
- «Абонентская папка» - отображает имя абонентской папки; запись об абоненте может быть перемещена Администратором в другую абонентскую папку (нажатием кнопки [x]);
- «Роль» - Администратор может назначить любому абоненту административную роль: в настоящей версии УЦ - только роль Оператора регистрационного центра (см. п. 5);
- «Группа» - для каждого абонента, являющегося Оператором регистрационного центра, Администратор УЦ может установить членство в одной из групп Операторов РЦ, зарегистрированной в базе данных УЦ; для каждой группы Операторов РЦ Администратором УЦ может быть назначено ограничение (квота) на общее количество

сертификатов, которое разрешается выпустить всем Операторам данной группы (см. п. 5.4).

The screenshot shows a window titled 'Абонент № 4437 - Сертифицированный'. It has a tabbed interface with tabs: 'Заметки', 'Документы', 'Справочные атрибуты', 'Доступ к субъекту', 'Параметры', 'Список имен', 'Сертификаты', 'Запросы', and 'Специальные атрибуты'. The 'Специальные атрибуты' tab is active. It contains several input fields and buttons: 'Почтовый адрес', 'Телефоны', 'Факс', 'Аварийный пароль' with 'Проверить...' and 'Сменить...' buttons, a checkbox for 'Альтернативное имя в' with a 'Редактировать...' button, 'Шаблон администрирования №' with a value of 24 and buttons '[x]', '[]', and '-->', 'Абонентская папка' with a value of 'ГОСТ-2012 256 бит' and buttons '[x]', '[]', and '-->', a 'Роль' dropdown menu set to '-- Нет --', and a 'Группа' field with a value of 0 and buttons '[x]' and '[]'.

Рис. 51 Страница «Специальные атрибуты» окна свойств абонента

3.4.2.6. Страница «Заметки»

Страница «Заметки» содержит комментарии Администратора.

3.4.2.7. Страница «Документы»

Страница «Документы» (см. Рис. 52) окна свойств абонента содержит список файлов-документов произвольного формата, хранящихся в базе данных УЦ и имеющих отношение к данному абоненту, в частности, электронная или отсканированная бумажная копия договора о присоединении абонента к регламенту УЦ.

При нажатии кнопки «Добавить...» выводится окно выбора файла, который необходимо сохранить в базе данных УЦ и ассоциировать с данным абонентом.

При нажатии кнопки «Открыть» для просмотра и редактирования будет открыт файл, выделенный курсором из приведенного списка. Приложение, с помощью которого будет открыт файл, выбирается автоматически в соответствии с настройками операционной системы.

При нажатии кнопки «Свойства...» выводится окно свойств выделенного файла.

При нажатии кнопки «Удалить» выделенный файл будет удален из базы данных УЦ.

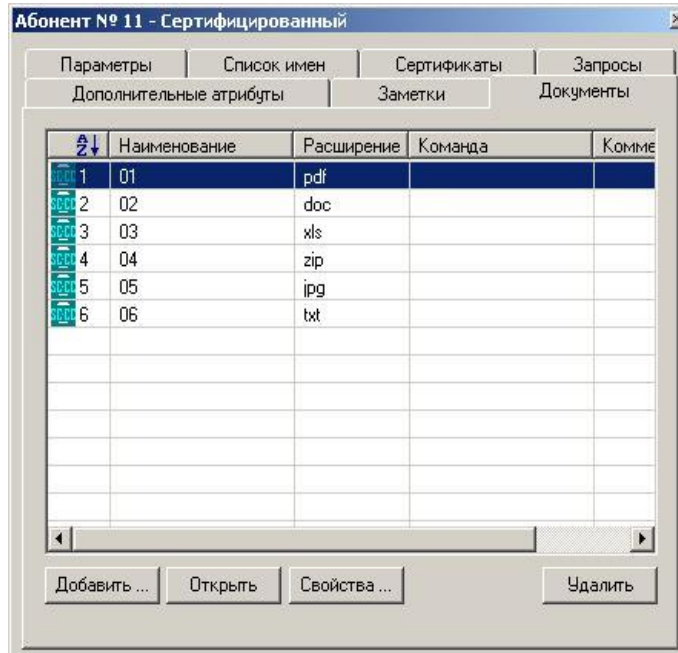


Рис. 52 Страница «Документы» окна свойств абонента

3.4.3. Удаление записи об абоненте

Для удаления записи об абоненте необходимо:

- в Главной панели перейти в папку «Абоненты»;
- выделить курсором нужного абонента;
- на Панели управления окна данной папки нажать кнопку «Удалить» (см. п. 2.2.2).

Нельзя удалить:

- абонента, который является Администратором;
- абонента, для которого в базе данных УЦ зарегистрированы сертификаты и/или запросы; сначала необходимо удалить все сертификаты и запросы абонента.

3.5. Запросы на сертификацию

3.5.1. Регистрация запроса

Для регистрации нового запроса сертификата (или группы запросов) необходимо:

- в Главном меню программы выбрать пункт «Формирование документов/Запросы/Импорт из файла» или в абонентских папках Главной панели выбрать папку «Запросы» и нажать кнопку «Импорт...» на Панели управления окна данной папки;
- задать имя файла, содержащего запрос сертификата или пометить группу файлов запросов в браузере выбрать нужный файл запроса и нажать «ОК»;
- если в настройках установки типа сертификата задана опция «Указать при ручной регистрации запроса» (см. п. 3.1.10), открывается окно «Тип сертификата» (см. Рис. 53), в котором надо выделить нужный тип сертификата и нажать кнопку «Выбрать»; если импортируемому запросу не ставится в соответствие параметр «Тип сертификата», необходимо нажать кнопку «Отмена»; данное окно не появляется, если опция «Указать при ручной регистрации запроса» не установлена;

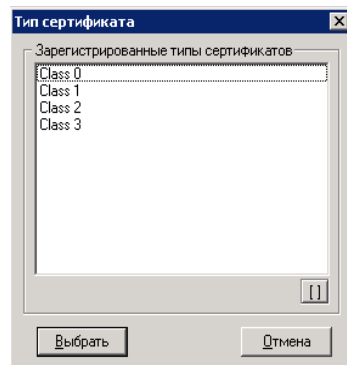


Рис. 53 Окно выбора типа сертификата

- в открывшемся окне «Импорт запросов из файловой системы» (см. Рис. 54) с параметрами импорта запроса заполнить необходимые поля:

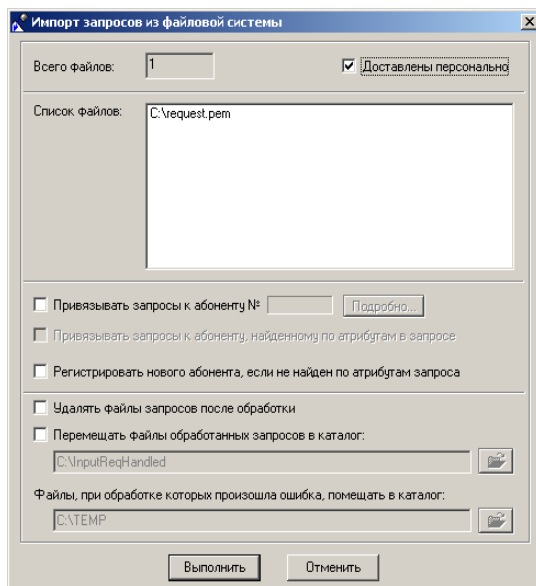


Рис. 54 Окно параметров импорта запроса

- ☐ указать способ доставки запроса (запросов): персонально или иным способом;
- ☐ выбрать абонента, с которым должен быть ассоциирован импортируемый запрос (по кнопке «Подробно»);
- ☐ при наличии установленного признака «Доставлены персонально» указать, разрешается ли автоматическая регистрация нового абонента, если атрибуты запрашиваемого уникального имени в запросе не соответствуют атрибутам имени ни одного из зарегистрированных абонентов;
- ☐ определить действия над файлом запроса (или группой файлов) после регистрации: переместить в заданный каталог либо удалить;
- ☐ указать каталог, в который следует перемещать файлы запросов, при обработке которых произошла ошибка.

Если при импорте запроса не был указан абонент, которому принадлежит запрос, зарегистрированный запрос не может быть сертифицирован до тех пор, пока не будет выполнена процедура установления связи «запрос-абонент» (см. п. 3.5.3).

3.5.2. Окно свойств запроса

Вызывается по кнопке «Подробнее...» Панели управления; представляет собой многостраничный диалог.

3.5.2.1. Страница «Параметры»

Страница «Параметры» (см. Рис. 55) содержит следующие атрибуты запроса:

Запрос № 17 - Сертифицированный

Параметры | Запрашиваемое имя | Абонент | Текст | Заметки | Документы

Регистрация

Дата: 26.02.2014 08:23:28 GMT Оператор №: []

Способ доставки: Персонально [] []

Тип PKCS#10 Тип запрашиваемого сертификата

Самоподписан: Да Проверен сертификатом №: []

Алгоритм открытого ключа: ГОСТ Р 34.10-2012 (256 бит)

Длина ключа: 256

Сертификация

Номер сертификата: 31 Оператор №: []

Свертка MD5: 02:e8:ed:a7:d3:f3:48:95:91:3a:1b:ae:b1:1c:ed:e0

Свертка SHA-1: cd:dd:dc:06:30:29:6f:d1:f1:33:0a:a7:71:b3:1d:6a:7d:b3:36:21

Свертка ГОСТ: a4:24:90:4c:ed:d9:6d:8c:93:cf:d0:cd:79:60:89:3b:2b:56:71:9a:c6:92:37:59:f7:5c:89:71:62:61:d4:f2

Рис. 55 Страница «Параметры» окна свойств запроса

- «Дата регистрации» - дата регистрации запроса (дата записи запроса в базу данных);
- «Способ доставки» - информационное поле, содержащее краткое описание способа доставки запроса в удостоверяющий центр; атрибут «Способ доставки» может иметь следующие значения:
 - ☐ «Интернет» – запрос получен из БД приложения «Notary-PRO Web Pages»;
 - ☐ «Файловая система» - запрос получен посредством импорта из файловой системы;
 - ☐ «Персонально» - запрос доставлен лично абонентом; при этом в окне импорта запросов из файловой системы Администратором был выставлен флаг «Доставлены персонально» (см.п. 3.5.1);
 - ☐ «Не определен» - только для запросов УЦ.
- «Оператор №» - отображает идентификатор Оператора РЦ, который *зарегистрировал* запрос; если значение отсутствует - запрос зарегистрирован Администратором УЦ;
- «Тип запроса» - возможные значения:
 - ☐ PKCS#10;
 - ☐ CMC (PKCS#10);
 - ☐ SPKAC (Netscape/Mozilla/Opera);;
- «Тип запрашиваемого сертификата» - тип сертификата, переданный в УЦ вместе с запросом в качестве дополнительного признака, определяющего в совокупности с атрибутами запроса выбор профиля (шаблона) сертификации (см. п. 2.2.3.1); данное поле содержит пустое значение либо значение из списка зарегистрированных в УЦ типов сертификатов, например:
 - ☐ Class 0
 - ☐ Class 1

□ Class 2

Примечание. Тип сертификата может передаваться в УЦ вместе с запросом в качестве дополнительного признака, определяющего в совокупности с атрибутами запроса выбор профиля (шаблона) сертификации. Назначение типов сертификатов и их интерпретация определяется действующей Сертификационной политикой удостоверяющего центра и устанавливается Администратором УЦ путем редактирования файла crt_cls.lst.ini из каталога запуска программы.

- «Самоподписан» - флаг, сообщающий Администратору о том, что запрос был подписан ключом ЭП, парным ключу проверки ЭП, включенному в запрос;
- «Проверен сертификатом №» - номер сертификата абонента, которым был проверен запрос;
- «Алгоритм ключа проверки ЭП» - алгоритм ключа проверки ЭП, включенного в запрос;
- «Длина ключа» - длина ключа проверки ЭП, включенного в запрос;
- «Номер сертификата» - номер сертификата, сформированного на основе данного запроса;
- «Оператор №» - отображает идентификатор Оператора РЦ, который *сертифицировал* запрос; если значение отсутствует - запрос сертифицирован Администратором УЦ;
- «Свертка MD5» - значение хэш-функции запроса, вычисленное по алгоритму MD5;
- «Свертка SHA-1» - значение хэш-функции запроса, вычисленное по алгоритму SHA-1;
- «Свертка ГОСТ» - значение хэш-функции запроса, вычисленное по алгоритму ГОСТ Р 34.11-94 [10].

3.5.2.2. Страница «Запрашиваемое имя»

Страница «Запрашиваемое имя» (см. Рис. 56) содержит следующие атрибуты:

- «Идентификатор в запросе» - значение атрибута Unstructured Name (см. [20]);
- Атрибуты запрашиваемого имени (см. п. 1.7);
- «Пароль в запросе» - значение атрибута Challenge Password (см. [20]).

Запрос № 1 - Сертифицированный

Параметры | **Запрашиваемое имя** | Абонент | Текст | Заметки | Документы

Идентификатор в запросе

⊖ Атрибуты уникального имени

Полное имя	Открытое акционерное общество
Организация	ОАО "Организация"
Подразделение	Дирекция
Должность	Генеральный директор
Страна	RU
Город село	Москва
Область район	77 г. Москва
Электронная почта	mail@organisation.ru
ИНН	001234567894
ОГРН	1234567890123
СНИЛС	*
Фамилия	Фамилия
Имя Отчество	Имя Отчество
Адрес	*
Почтовый адрес	*
Неструктурированное имя	*
Псевдоним	*

Пароль в запросе

Рис. 56 Страница «Запрашиваемое имя» окна свойств запроса

3.5.2.3. Страница «Абонент»

Страница «Абонент» (см. Рис. 57) содержит следующие атрибуты запроса:

- «Регистр.№» - регистрационный номер абонента, которому принадлежит запрос;
- «Идентификатор» - идентификатор абонента;
- Атрибуты абонента;
- Кнопки:
 - «Поиск...» - поиск абонента по атрибутам запрашиваемого имени;
 - «Выбрать...» - выбор абонента из списка зарегистрированных абонентов удостоверяющего центра;
 - «Очистить...» - удаление связи «запрос-абонент»;
 - «Создать...» - регистрация нового абонента по атрибутам запрашиваемого имени;
 - «Подробно...» - просмотр атрибутов абонента в форме просмотра свойств абонента (см.п. 3.4.2);
 - «Перейти...» - переход в папку «Абоненты» текущей абонентской папки с позиционированием на записи об абоненте.

Регистр.№	Идентификатор	Открытое акционерное
2		

⊖ Атрибуты уникального имени

Полное имя	Открытое акционерное общество
Организация	ОАО "Организация"
Подразделение	Дирекция
Должность	Генеральный директор
Страна	RU
Город село	Москва
Область район	77 г. Москва
Электронная почта	mail@organisation.ru
ИНН	001234567894
ОГРН	1027700239863
СНИЛС	
Фамилия	Фамилия
Имя Отчество	Имя Отчество
Адрес	*
Почтовый адрес	*
Неструктурированное имя	*
Псевдоним	*

Поиск... Выбрать... Очистить... Создать... Подробно Перейти...

Рис. 57 Страница «Абонент» окна свойств запроса

3.5.2.4. Страница «Текст»

Страница «Текст» (см. Рис. 58) содержит текст запроса.

Запрос № 4963 - Сертифицированный

Параметры Запрашиваемое имя Абонент **Текст** Заметки Документы

```

Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: C=RU, CN=Test 1000002
  Subject Public Key Info:
    Public Key Algorithm: id-ec26-gost3410-12-256
  (1.2.643.7.1.1.1.1.1)
    Public Key:
      pub:
        f8:f0:dc:50:1d:2f:20:5d:17:36:79:a8:cb:ff:c6:
        0f:c0:c9:47:04:10:3b:59:72:d5:bd:a4:12:4e:7a:
        81:f3:1d:13:9e:ac:89:ac:5d:8d:54:af:da:b8:
        86:e6:67:05:18:c3:4e:ad:9b:ac:76:73:af:b4:ca:
        bb:a4:b8:f9
      Parameters: 0 ID: 1.2.643.2.2.36.0
    Attributes:
      a0:00
      Signature Algorithm: id-ec26-signwithdigest-gost3410-12-256
      (1.2.643.7.1.1.3.2)
      15:97:8b:6a:0b:8e:a5:54:43:ac:c0:6f:e5:dd:c0:3f:d6:56:
      c4:05:86:12:c3:ad:5a:b7:ce:c2:a0:ac:a4:16:37:96:d8:
      46:3d:19:b2:6f:4d:a4:7f:22:40:75:fd:4b:25:c2:ea:3d:6f:
      4d:f7:fd:a9:e1:8c:06:35:9b:22
-----BEGIN CERTIFICATE REQUEST-----
MIHIMIIGRAgEAMCICsAUBGNVBAVTAlJUMRMwEQYDUQDDApiz28tc6k1221uMGYw
  
```

Рис. 58 Страница «Текст» окна свойств запроса

3.5.2.5. Страница «Заметки»

Страница «Заметки» (см. Рис. 59) содержит комментарии Администратора и диагностические сообщения программы, полученные в ходе обработки запроса. Перечень наиболее часто используемых комментариев Администратор может сформировать через редактируемый файл Notary3m_Comment.ini, расположенный в каталоге запуска программы УЦ.

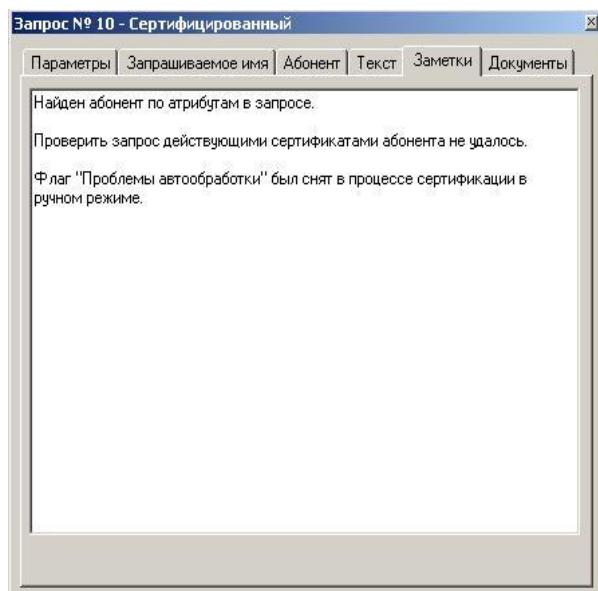


Рис. 59 Страница «Заметки» окна свойств запроса

3.5.2.6. Страница «Документы»

Страница «Документы» (см. Рис. 60) содержит список файлов, относящихся к данному запросу и хранящиеся в базе данных УЦ, в частности, отсканированные бумажные копии запросов, заверенные собственноручной подписью абонента и Администратора УЦ.

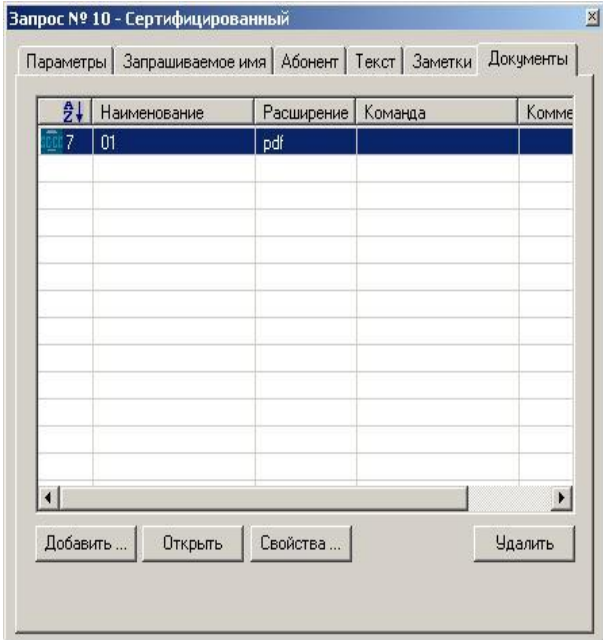


Рис. 60 Страница «Документы» окна свойств запроса

3.5.3. Создание связи «запрос-абонент»

Любой запрос может быть сертифицирован только после того, как установлена логическая связь «запрос-абонент» (после «привязки» запроса к абоненту).

Связь «запрос-абонент» может быть установлена следующим образом:

- находясь в окне «Запросы» («Запросы/Несертифицированные») абонентской папки, выделить курсором нужный запрос и, нажав кнопку «Подробнее...», войти в окно с параметрами запроса;
- в окне с параметрами запроса перейти на страницу «Абонент» и воспользоваться одной из перечисленных ниже кнопок:
 - ☐ при нажатии кнопки «Выбрать...» Администратору предоставляется возможность привязки запроса к одному из абонентов удостоверяющего центра (см. Рис. 61);
 - ☐ при нажатии кнопки «Поиск...» производится автоматический поиск абонента с атрибутами имени, идентичными атрибутам запрашиваемого имени;
 - ☐ при нажатии кнопки «Создать...» регистрируется новый абонент с атрибутами запрашиваемого имени.

В процессе создания связи «запрос-абонент» программа пытается проверить запрос одним из действующих сертификатов абонента. В случае отрицательного результата выдается предупреждение о том, что запрос будет привязан без проверки.

Связь «запрос-абонент» может быть в дальнейшем (но не после сертификации) удалена нажатием кнопки «Очистить» (см. п.3.5.2.3).

Аналогичные действия по созданию связи «запрос-абонент» могут быть выполнены непосредственно в ходе сертификации запроса (см. п. 3.5.4).

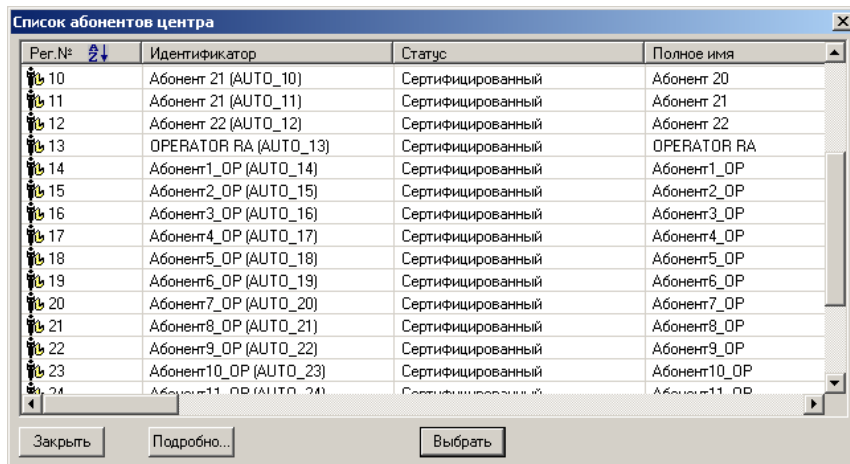


Рис. 61 Окно выбора абонента в создании связи «запрос-абонент»

3.5.4. Сертификация запроса

Сертификация запроса может быть выполнена двумя способами:

1. Из папки «Абоненты»

- в абонентских папках Главной панели выбрать папку «Абоненты» (либо «Абоненты/Несертифицированные»);
- выделить курсором нужного абонента и нажать кнопку «Подробнее»;
- перейти на страницу «Запросы»;
- выделить курсором нужный запрос и нажать кнопку «Перейти» или «Отдельное окно»;
- на Панели управления появившегося окна с параметрами запроса нажать кнопку «Сертификация...» (см. п. 2.2.5).

2. Из папки «Запросы»

- в любой абонентской папке Главной панели открыть папку «Запросы» (либо «Запросы/Несертифицированные»);
- выделить курсором нужный запрос;
- на Панели управления окна данной папки нажать кнопку «Сертификация...» (см. п. 2.2.5).

Примечание 1. Необходимым условием сертификации является наличие логической связи «запрос-абонент» (см.п. 3.5.3).

Примечание 2. Повторная сертификация сертифицированных ранее ключей абонентов возможна только после подтверждения Администратором.

После нажатия кнопки «Сертификация...» Администратору выдается многостраничный диалог с параметрами сертификации (см. пп.3.5.4.1- 3.5.4.6).

3.5.4.1. Страница «Шаблоны»

Страница «Шаблоны» (см. Рис. 62) предназначена для выбора шаблона администрирования, в соответствии с которым будет сформирован сертификат. Подробнее о настройке шаблонов администрирования см. п. 3.1.

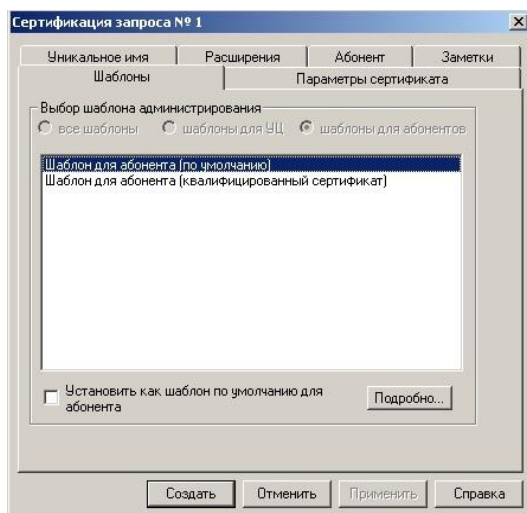


Рис. 62 Страница «Шаблоны» окна с параметрами сертификации запроса

Для формирования сертификата достаточно нажать кнопку «Создать». Однако, перед этим Администратор может установить значения параметров сертификата, отличные от параметров шаблона.

3.5.4.2. Страница «Параметры сертификата»

На странице «Параметры сертификата» (см. Рис. 63) Администратору предоставляется возможность:

- установить период действия сертификата либо установить даты начала и окончания периода действия сертификата;
- изменить сертификат удостоверяющего центра, используемый при формировании сертификата.

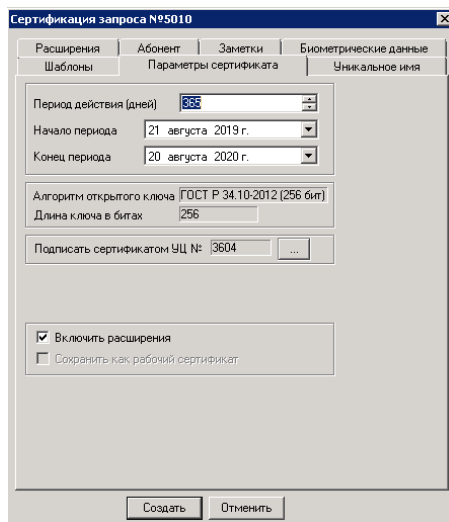


Рис. 63 Страница «Параметры сертификата» окна с параметрами сертификации запроса

3.5.4.3. Страница «Уникальное имя»

На странице «Уникальное имя» (см. Рис. 64) Администратор может установить атрибуты уникального имени абонента, которое будет включено в новый сертификат.

Переключатель «Имя из запроса» / «Как у абонента» служит для установки атрибутов уникального имени в значения из запроса и из регистрационной записи абонента соответственно. По умолчанию переключатель устанавливается в значение, заданное в шаблоне администрирования (см.п. 3.2.2.1).

The screenshot shows a window titled 'Сертификация запроса №1' with a tabbed interface. The 'Уникальное имя' tab is active. It contains several text input fields for personal and organizational data: 'Полное имя' (Testovyy Abonent), 'Организация' (ЗАО Сигнал-КОМ), 'Подразделение', 'Должность', 'Город/село' (Москва), 'Область/район', 'Страна' (Россия), and 'Электронная почта' (abonent-test@mail.ru). Below these fields are two radio buttons: 'Имя из запроса' (unselected) and 'Как у абонента' (selected), along with a 'Выбрать из списка имен' button. At the bottom are 'Создать', 'Отменить', and 'Применить' buttons.

Рис. 64 Страница «Уникальное имя» окна с параметрами сертификации запроса

3.5.4.4. Страница «Расширения»

На странице «Расширения» (см. Рис. 65) Администратору предоставляется возможность настроить параметры расширений сертификата.

The screenshot shows the same window with the 'Расширения' tab active. It features a list box titled 'Список расширений, включенных в сертификат' containing five items: 'Идентификатор ключа владельца' (selected), 'Идентификатор ключа УЦ', 'Расширенное использование ключа', 'Назначение ключа', and 'Адрес списка отмены'. To the right of the list are buttons for 'Подробнее...', 'Добавить', and 'Удалить'. The bottom buttons 'Создать', 'Отменить', and 'Применить' are also visible.

Рис. 65 Страница «Расширения» окна с параметрами сертификации запроса

Действия Администратора по настройке расширений подробно описаны в п.4.

3.5.4.5. Страница «Абонент»

Страница «Абонент» (см. Рис. 66) содержит данные об абоненте, которому принадлежит сертификат.

Сертификация запроса №1

Шаблоны | Параметры сертификата

Уникальное имя | Расширения | Абонент | Заметки

Рег. №: 2 | Идентификатор: Тестовый Абонент (AUTO_2):

Полное имя: Тестовый Абонент

Организация: ЗАО Сигнал-КОМ

Подразделение:

Должность:

Город/село: Москва

Область/район:

Страна: Россия

Электронная почта: abonent-test@mail.ru

Создать | Отменить | Применить

Рис. 66 Страница «Абонент» окна с параметрами сертификации запроса

3.5.4.6. Страница «Заметки»

Страница «Заметки» содержит комментарии Администратора УЦ.

3.5.5. Отказ в сертификации запроса

Если Администратора УЦ по каким-либо причинам отклоняет сертификацию запроса (например, при работе с запросами от Операторов РЦ, для которых не установлен режим автоматической сертификации), то он должен проделать следующие действия:

- в абонентских папках Главной панели выбрать папку «Запросы» (либо «Запросы/Несертифицированные»);
- выделить курсором нужный запрос и нажать кнопку «Отклонить...»;
- в появившемся окне (см. Рис. 67) указать причину, по которой данный запрос не был сертифицирован, и нажать кнопку «ОК».

Укажите причину для отклонения запроса

Причина: Нет достоверной информации, подтверждающей личнос

ОК | Отмена

Рис. 67 Окно ввода причины отклонения запроса

3.5.6. Экспорт запроса

Любой запрос может быть экспортирован из базы данных УЦ в файловую систему.

Для экспорта запроса необходимо:

- в абонентских папках Главной панели выбрать папку «Запросы»;

- выделить курсором нужный запрос;
- на Панели управления окна данной папки нажать кнопку «Экспорт...» (см. п. 2.2.5).

Формат экспорта запросов задается на странице «Экспорт документов» окна свойств шаблона администрирования данного абонента (см. п. 3.2.2.3).

3.5.7. Удаление запроса

Любой несертифицированный запрос можно удалить в любое время. Если запрос сертифицирован, то удалить его можно только после удаления соответствующего сертификата.

Для удаления запроса необходимо:

- в абонентских папках Главной панели выбрать папку «Запросы»;
- выделить курсором нужный запрос;
- на Панели управления окна данной папки нажать кнопку «Удалить...» (см. п. 2.2.5).

3.6. Сертификаты

3.6.1. Формирование сертификата

Смотри п. 3.5.4 «Сертификация запроса».

3.6.2. Окно свойств сертификата

3.6.2.1. Страница «Параметры»

Страница «Параметры» (см. Рис. 68) содержит следующие атрибуты сертификата:

- «Серийный номер» - уникальный серийный номер сертификата;
- «Дата регистрации» - дата регистрации (создания) сертификата;
- «Период действия сертификата» - период действия сертификата в сутках;
- «Начало периода действия» - дата начала периода действия сертификата;
- «Окончание периода действия» - дата окончания периода действия сертификата;
- «Версия сертификата» - версия согласно X.509;
- «Алгоритм подписи» - алгоритм электронной подписи сертификата;
- «Кодировка символов» - кодировка национальных символов в сертификате (возможные значения: ANSI, Unicode, UTF8);
- «Алгоритм открытого ключа» - алгоритм ключа проверки ЭП абонента;
- «Длина ключа» - длина ключа проверки ЭП абонента;
- «Дата публикации» - дата экспорта сертификата (в виде файла и/или на LDAP);
- «Дата отмены» - даты отмены сертификата (если он был отменен).

Расширения	Текст	Свертки	Заметки
Документы		Биометрические данные	
Параметры	Уникальное имя	Администратор	Сертификационный путь
Серийный номер: 01:dd:01:12:01:08:01:03			
Дата регистрации: 26.02.2014 08:29:56 GMT			
Период действия сертификата (дней): 7303			
Начало периода действия: 26.02.2014 08:29:14 GMT			
Окончание периода действия: 24.02.2034 08:29:14 GMT			
Версия сертификата: 3		Кодировка символов: UTF8	
Алгоритм подписи: ГОСТ Р 34.10-2012 (256 бит)			
Алгоритм открытого ключа: ГОСТ Р 34.10-2012 (256 бит)			
Длина ключа: 256			
Дата публикации: 26.02.2014 08:37:43 GMT			
Дата отзыва:			

Рис. 68 Страница «Параметры» окна свойств сертификата

3.6.2.2. Страница «Уникальное имя»

Страница «Уникальное имя» (см. Рис. 69) содержит следующие атрибуты сертификата:

- Атрибуты уникального имени (см. п. 1.7);
- «Абонент №» - регистрационный номер абонента, которому принадлежит сертификат;
- «Запрос №» - регистрационный номер запроса, на основании которого выпущен сертификат.

The screenshot shows a software window titled 'Сертификат № 11 - Действительный'. It has a tabbed interface with the following tabs: 'Расширения', 'Текст', 'Свертки', 'Заметки', 'Документы', 'Параметры', 'Уникальное имя' (selected), 'Администратор', and 'Сертификационный путь'. The 'Уникальное имя' tab contains several text input fields with the following values: 'Полное имя' (Тестовый Абонент 10), 'Организация' (ЗАО Сигнал-КОМ), 'Подразделение' (empty), 'Должность' (empty), 'Город/село' (Москва), 'Область/район' (empty), 'Страна' (Россия), and 'Электронная почта' (abonent-test 10@mail.ru). At the bottom, there are two groups of controls: 'Абонент №' with a value of 11 and 'Запрос №' with a value of 10. Each group includes a text box, an ellipsis button (...), and a right-pointing arrow button (→).

Рис. 69 Страница «Уникальное имя» окна свойств сертификата

3.6.2.3. Страница «Администратор»

Страница «Администратор» (см. Рис. 70) содержит атрибуты сертификата Администратора, с помощью которого заверен сертификат абонента:

- «Ключ УЦ №» - регистрационный номер ключа УЦ, которым был подписан сертификат;
- «Сертификат УЦ №» - регистрационный номер сертификата УЦ, которым был подписан данный сертификат;
- Атрибуты уникального имени Администратора, включенного в сертификат (см. п. 1.7).

При нажатии кнопки «Подробнее» на экран выводится окно свойств Администратора УЦ (окно свойств сертификата остается активным).

При нажатии кнопки «Перейти...» выводится окно свойств Администратора УЦ (окно свойств сертификата закрывается).

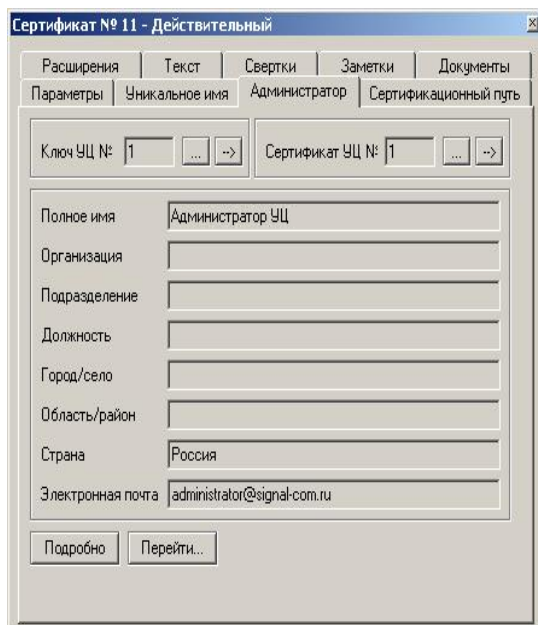


Рис. 70 Страница «Администратор» окна свойств сертификата

3.6.2.4. Страница «Сертификационный путь»

Страница «Сертификационный путь» (см. Рис. 71) содержит цепочку сертификатов, представленную в виде упорядоченного списка:

- первым в списке расположен самоподписанный сертификат корневого удостоверяющего центра;
- последним – сертификат абонента.

При нажатии кнопки «Подробнее...» на экран выводится окно свойств сертификата, выделенного курсором (окно свойств сертификата остается активным).

При нажатии кнопки «Перейти» выводится окно свойств сертификата, выделенного курсором (текущее окно свойств закрывается).



Страница «Расширения» (см. Рис. 72) содержит список расширений, включенных в сертификат.



По кнопке «Подробнее...» можно посмотреть настройки каждого из расширений. Действия Администратора по настройке расширений подробно описаны в п.4.

3.6.2.6. Страница «Текст»

Страница «Текст» (см. Рис. 73) содержит текст сертификата.

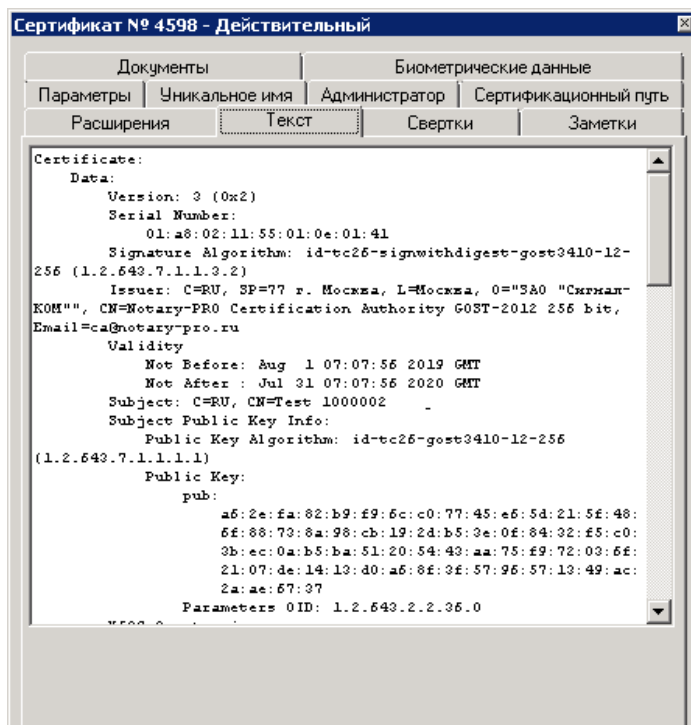


Рис. 73 Страница «Текст» окна свойств сертификата

3.6.2.7. Страница «Свертки»

Страница «Свертки» (см. Рис. 74) содержит:

- «Свертка MD5» - значение хэш-функции MD5;
- «Свертка SHA-1» - значение хэш-функции SHA-1;
- «Свертка ГОСТ» - значение хэш-функции сертификата, вычисленное по алгоритму ГОСТ Р 34.11-94 [10].

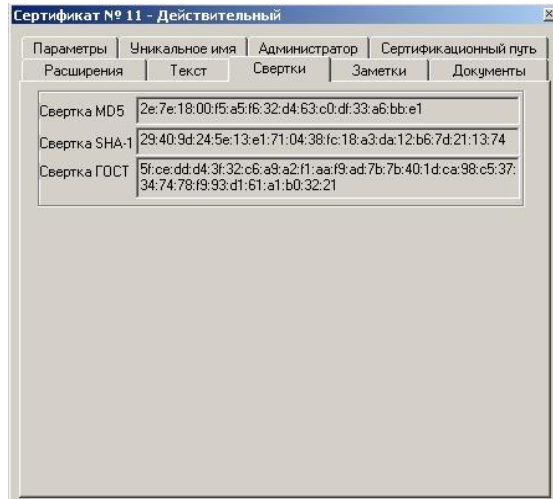


Рис. 74 Страница «Свертки» окна свойств сертификата

3.6.2.8. Страница «Заметки»

Страница «Заметки» содержит комментарии Администратора.

3.6.2.9. Страница «Документы»

Страница «Документы» содержит список файлов, ассоциируемых с данным сертификатом и хранящихся в базе данных УЦ, в частности, отсканированные бумажные копии сертификатов, заверенные собственноручной подписью абонента и Администратора УЦ.

3.6.3. Экспорт сертификата

Любой сертификат может быть экспортирован из базы данных УЦ в файловую систему. Если сертификат был экспортирован хотя бы один раз, он не может быть удален из базы данных до тех пор, пока не истечет срок его хранения в базе данных. Срок хранения задается на странице «Сертификаты» окна «Параметры по умолчанию» (см. п. 3.1.2).

Для экспорта сертификата необходимо:

- в абонентских папках Главной панели выбрать папку «Сертификаты»;
- выделить курсором нужный сертификат;
- на панели управления окна данной папки нажать кнопку «Экспорт...»;
- при этом выдается запрос имени файла для сохранения сертификата.

Формат экспорта сертификатов задается на странице «Экспорт документов» окна свойств шаблона администрирования (см.п. 3.2.2.3).

3.6.4. Экспорт сертификатов абонента

Для экспорта всех сертификатов абонента необходимо:

- в абонентских папках выбрать папку «Абоненты»;
- выделить курсором нужного абонента;
- на Панели управления нажать кнопку «Экспорт...»;
- при этом выдается запрос имени каталога для сохранения данных.

Наряду с сертификатами абонента производится экспорт всех необходимых сертификатов УЦ, а также экспорт всех действующих на данный момент списков отмены.

3.6.5. Отзыв сертификата

Для отзыва сертификата необходимо:

- в абонентских папках Главной панели выбрать папку «Сертификаты» (либо «Действительные сертификаты»);
- выделить курсором нужный сертификат;
- на Панели управления окна папки нажать кнопку «Отозвать...»;
- в открывшемся окне (см. Рис. 75) указать курсором причину отзыва сертификата и нажать кнопку «Выбрать».

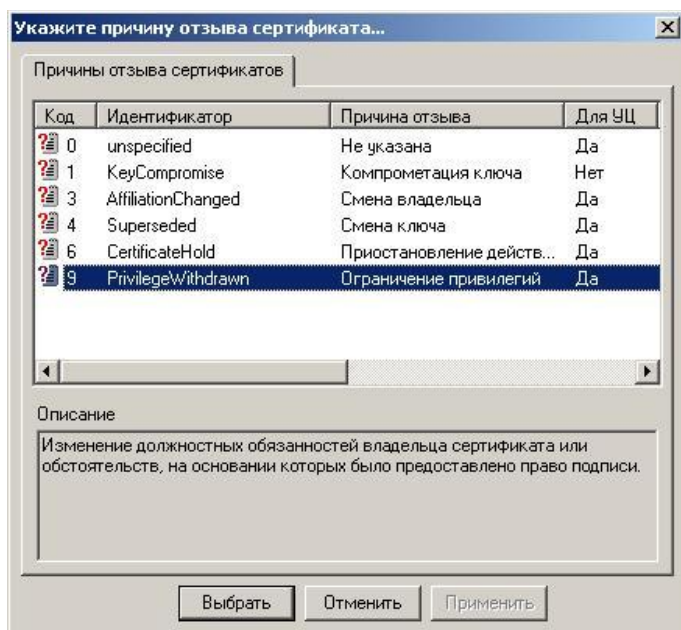


Рис. 75 Окно выбора причины отзыва сертификата

Перечень возможных причин отзыва сертификата в удостоверяющем центре «Notary-PRO» приводится в следующей таблице:

Таблица 2

Код	Идентификатор	Причина отзыва	Для УЦ	Для пользователя	Восстановление	Описание
0	Unspecified	Не указана	Да	Да	Нет	Отзыв сертификата без указания причины отзыва. Не рекомендуется для использования.
1	KeyCompromise	Компрометация ключа	Нет	Да	Нет	Компрометация ключа ЭП владельца сертификата (утра, раскрытие, искажение ключа, утеря ключа с последующим обнаружением, факт или подозрение того, что ключ стал известен другим лицам, нарушение правил хранения ключа ЭП).
2	CACompromise	Компрометация	Да	Нет	Нет	Компрометация ключа ЭП УЦ. При отзыве сертификата УЦ могут

Код	Идентификатор	Причина отзыва	Для УЦ	Для пользователя	Восстановление	Описание
		ключа УЦ				быть отозваны все сертификаты, выпущенные с его помощью.
3	AffiliationChanged	Смена владельца	Да	Да	Нет	Изменение сведений, указанных в сертификате (увольнение с работы, перевод на другую должность, смена персональных данных владельца сертификата, выявление ошибок в реквизитах).
4	Superseded	Смена ключа	Да	Да	Нет	Физическая порча ключевого носителя, невозможность воспроизведения пароля к ключу.
5	CessationOfOperation	Прекращение работы УЦ	Да	Нет	Нет	Прекращение деятельности УЦ. Устанавливает запрет для сертификата УЦ на выпуск новых сертификатов пользователей, разрешая только выпуск списков отозванных сертификатов.
6	CertificateHold	Приостановление действия	Да	Да	Да	Приостановление действия сертификата при подозрении на компрометацию того ключа ЭП (до выяснения обстоятельств). Приостановленный сертификат позднее может быть восстановлен или отозван с указанием другой причины.
9	PrivilegeWithdrawn	Ограничение привилегий	Да	Да	Нет	Изменение должностных обязанностей владельца сертификата или обстоятельств, на основании которых было предоставлено право подписи.

После отмены сертификата должен быть выпущен новый список отозванных сертификатов (см. п. 3.7.1).

Если отзываемый сертификат является сертификатом УЦ, то при его отзыве могут быть отозваны также все сертификаты абонентов, изготовленные с использованием данного сертификата УЦ.

3.6.6. Восстановление сертификата

Отозванный ранее сертификат абонента может быть восстановлен только в том случае, если в качестве причины его отзыва было указано «Приостановление действия» (см. п. 3.6.5).

Отозванный сертификат УЦ может быть восстановлен, если не отозван парный ему ключ УЦ.

Для восстановления отозванного ранее сертификата необходимо:

- в абонентских папках Главной панели выбрать папку «Сертификаты»;
- выделить курсором нужный сертификат;
- на Панели управления окна папки нажать кнопку «Восстановить...».

Если отозванный сертификат является сертификатом УЦ, и при его отзыве были отозваны также все абонентские сертификаты, изготовленные с его помощью, то при восстановлении сертификата УЦ каждый из абонентских сертификатов может быть восстановлен вышеописанным способом.

3.6.7. Удаление сертификата

Для удаления сертификата необходимо:

- в абонентских папках Главной панели выбрать папку «Сертификаты»;
- выделить курсором нужный сертификат;
- на Панели управления окна данной папки нажать кнопку «Удалить...».

Нельзя удалить:

- опубликованный (т.е. когда-либо экспортированный) сертификат до истечения срока его хранения в базе данных удостоверяющего центра;
- сертификат, включенный в список отозванных сертификатов, до истечения срока его хранения в базе данных удостоверяющего центра;
- сертификат УЦ, с помощью которого изготовлен хотя бы один сертификат;
- сертификат, на который есть ссылки в других документах (например, сертификат, которым был проверен зарегистрированный запрос). При удалении такого сертификата сообщается причина, по которой нельзя удалить сертификат, и предоставляется возможность просмотра списка документов, имеющих ссылки на данный сертификат.

При удалении сертификата абонента может удаляться соответствующий ему запрос (после подтверждения Администратора). Если запрос не удален, то он может быть повторно сертифицирован.

3.7. Списки отозванных сертификатов

3.7.1. Формирование списка отозванных сертификатов

Формирование списка отозванных сертификатов может быть:

- плановым, производимым по истечении периода действующего списка;
- экстренным, при отмене сертификата (или нескольких сертификатов).

Для формирования списка отозванных сертификатов необходимо в Главном меню программы выбрать пункт «Формирование документов/Создание нового списка отмены» или, находясь в папке «Списки отозванных сертификатов», на Панели управления окна данной папки нажать кнопку «Новый».

В появившемся многостраничном окне Администратор получает возможность:

- установить период действия списка отмены (см. Рис. 76); период устанавливается в сутках; максимально возможная величина периода определяется числом целых суток и часов до истечения периода сертификата УЦ;

Новый список отмены

Параметры | Сертификаты | Заметки

Период действия (дней) 5

Начало периода 21 августа 2019 г.

Конец периода 26 августа 2019 г.

Алгоритм хэширования ГОСТ Р 34.11-2012 (256 бит)

Рабочий сертификат для подписи 3604

Выпуск нескольких списков одновременно Нет

Создать Отменить

Рис. 76 Диалог формирования нового списка отозванных сертификатов

- пометить сертификат УЦ, которым должен быть подписан новый список отмены; при необходимости указать несколько сертификатов УЦ (см. Рис. 77); в этом случае при нажатии кнопки «Создать» будет сформировано несколько списков отмены, подписанных разными сертификатами УЦ;
- просмотреть список отзываемых сертификатов (см. Рис. 78); кнопка «Подробнее» позволяет просмотреть информацию о каждом из отзываемых сертификатов.

Списки отозванных сертификатов должны своевременно публиковаться Администратором УЦ.

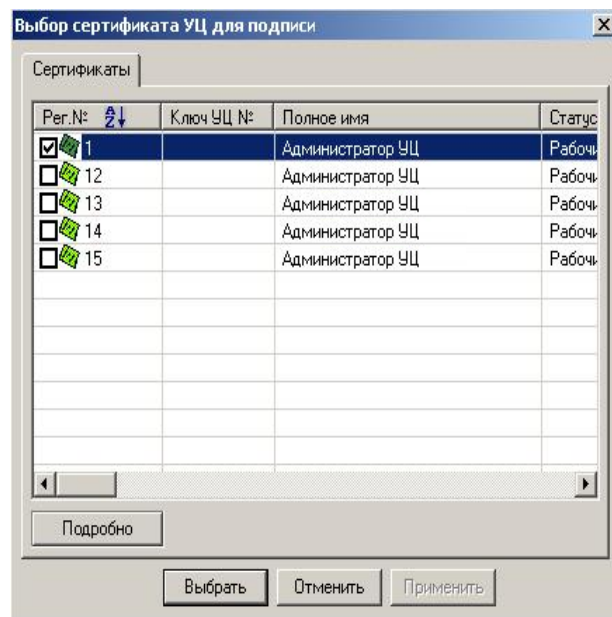


Рис. 77 Окно выбора сертификатов УЦ

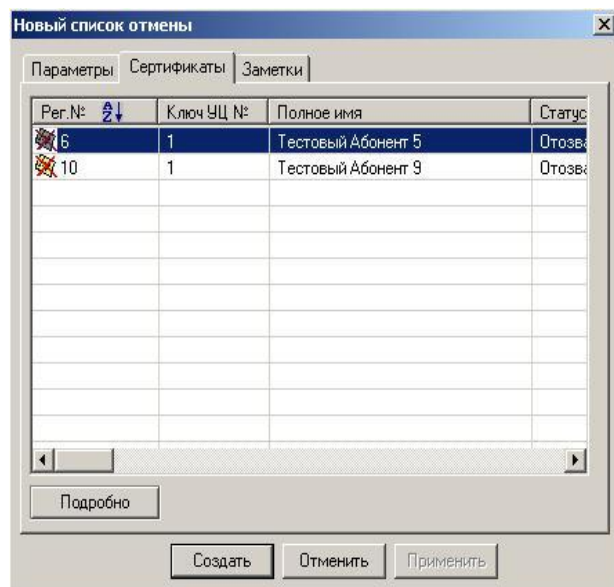


Рис. 78 Список отозванных сертификатов

3.7.2. Окно свойств списков отозванных сертификатов

3.7.2.1. Страница «Параметры»

Страница «Параметры» (см. Рис. 79) содержит следующие атрибуты списка отозванных сертификатов:

- «Период действия» - период действия списка в днях;
- «Начало периода» - дата начала периода действия списка отозванных сертификатов;
- «Конец периода» - дата окончания периода действия списка отозванных сертификатов;
- «Подписан ключом №» - регистрационный номер ключа УЦ, которым был подписан список отозванных сертификатов;
- «Сертификат СА» - регистрационный номер сертификата УЦ;
- «Алгоритм подписи» - алгоритм электронной подписи УЦ;
- «Свертка MD5» - значение хэш-функции MD5;
- «Свертка SHA-1» - значение хэш-функции SHA-1;
- «Свертка ГОСТ» - значение хэш-функции списка отозванных сертификатов, вычисленное по алгоритму ГОСТ Р 34.11-94 [10].

The screenshot shows a window titled 'Список отозванных сертификатов № 101 - Действующий'. It has four tabs: 'Параметры' (selected), 'Сертификаты', 'Текст', and 'Заметки'. The 'Параметры' tab contains several input fields and a table of hashes.

Период действия (дней)	30
Начало периода	14.08.2014 09:37:17 GMT
Конец периода	13.09.2014 09:37:17 GMT
Дата публикации	20.08.2014 13:30:01 GMT
№ списка	0

Подписан ключом №	23	[icon]	-->
Сертификат УЦ	89	[icon]	-->
Алгоритм подписи	ГОСТ Р 34.10-2012 (256 бит)		

Свертка MD5	c1:b4:d3:8a:c7:76:d5:b1:62:7d:c8:4c:37:9e:c7:3c
Свертка SHA-1	f3:39:d6:de:f4:22:17:e1:e5:1d:ae:46:44:13:bf:8d:67:37:a3:00
Свертка ГОСТ	ef:cb:9b:b8:1f:17:2b:f9:6a:08:9e:60:d4:fc:de:59:dd:3c:c2:41:04:8e:4b:23:bb:a3:53:b8:48:ef:63:26

Рис. 79 Страница «Параметры» окна свойств списка отозванных сертификатов

3.7.2.2. Страница «Сертификаты»

Страница «Сертификаты» (см. Рис. 80) содержит список сертификатов, вошедших в данный список отозванных сертификатов.

При нажатии кнопки «Подробнее» на экран выводится окно свойств сертификата, выделенного курсором (текущее окно свойств остается активным).

При нажатии кнопки «Перейти...» выводится окно свойств сертификата, выделенного курсором (текущее окно свойств закрывается).

При нажатии кнопки «Отдельное окно» создается новая выборка (см. п. 3.9), содержащая записи, отображаемые в настоящем окне.

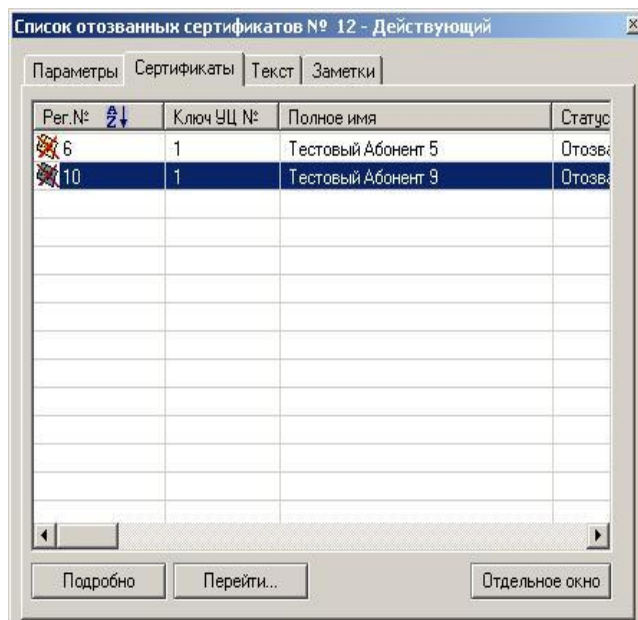


Рис. 80 Страница «Сертификаты» окна свойств списка отозванных сертификатов

3.7.2.3. Страница «Текст»

Страница «Текст» (см. Рис. 81) содержит текст списка отозванных сертификатов.

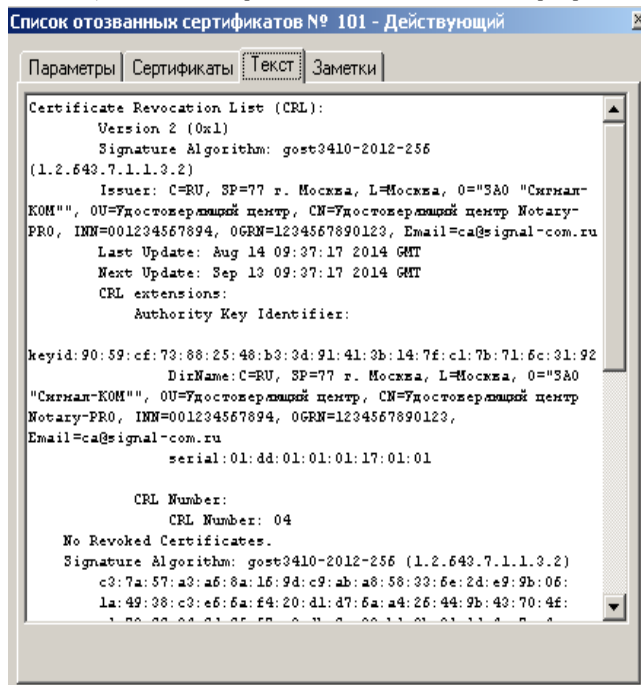


Рис. 81 Страница «Текст» окна свойств списка отозванных сертификатов

3.7.2.4. Страница «Заметки»

Страница «Заметки» содержит комментарии Администратора.

3.7.3. Экспорт списка отозванных сертификатов

Любой список отозванных сертификатов может быть экспортирован из базы данных УЦ в файловую систему. Для экспорта списка отозванных сертификатов необходимо:

- находясь в папке «Списки отозванных сертификатов», выделить курсором нужную запись;
- на Панели управления окна данной папки нажать кнопку «Экспорт...»;
- при этом выдается запрос имени файла для сохранения списка отмены.

Если список отозванных сертификатов был экспортирован, он не может быть удален из базы данных до истечения периода его действия.

3.7.4. Удаление списка отозванных сертификатов

Для удаления списка отозванных сертификатов необходимо:

- находясь в папке «Списки отозванных сертификатов», выделить курсором нужную запись;
- на панели управления окна данной папки нажать кнопку «Удалить...».

Нельзя удалить опубликованный (т.е. когда-либо экспортированный) список отозванных сертификатов до истечения периода его действия.

3.8. Автоматическая обработка запросов

3.8.1. Автоматическая обработка запросов из файловой системы

В программе удостоверяющего центра реализована возможность автоматической обработки запросов, импортируемых из файловой системы. Для настройки режима автоматической обработки Администратору УЦ необходимо:

- выбрать пункт главного меню «Формирование документов/Запросы/ Автоматическая обработка/Из файловой системы»
- в окне диалога (см. Рис. 82) установить параметры обработки:
 - ☐ указать каталог, из которого будут импортироваться запросы сертификатов;
 - ☐ установить флаг регистрации новых абонентов, если при автоматической обработке запросов разрешается регистрировать новых абонентов с атрибутами имени, взятыми из запроса¹;
 - ☐ задать каталог, куда будет экспортирован файл нового сертификата, если при автоматической обработке запросов разрешается автоматическое формирование сертификатов (см. п. 2.2.3.1);
 - ☐ при необходимости установить флаг экспорта только сертификатов абонентов (без цепочки сертификатов УЦ и списков отозванных сертификатов);
 - ☐ определить тип действия над файлом запроса после обработки: удалять или перемещать в специально выбранный каталог;
 - ☐ установить интервал опроса каталога с импортируемыми запросами (в секундах).

При установленном флаге «Автоматическая обработка включена» обработка запускается сразу после выхода из окна диалога по клавише «ОК».

Если во время автоматической обработки запроса возникли какие-либо проблемы, Администратор может получить более подробную информацию об ошибке на странице «Заметки» в окне свойств запроса (см.п. 3.5.2.5).

¹ Новый абонент будет зарегистрирован только в том случае, если импортируемый запрос самоподписан и в базе данных Удостоверяющего центра нет ни одного сертификата с уникальным именем, совпадающим с атрибутами имени в запросе.

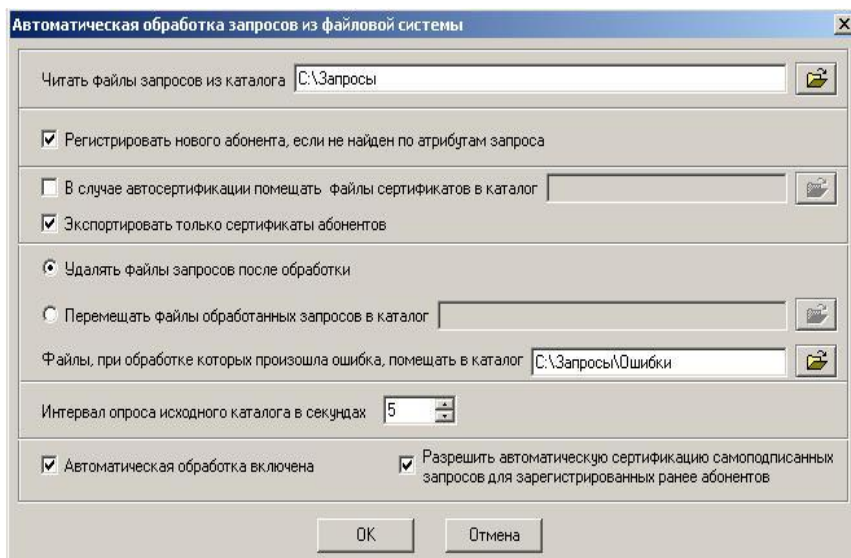


Рис. 82 Диалог установки параметров автоматической обработки запросов из файловой системы

Новые абоненты, которые регистрируются в процессе автообработки запросов, автоматически регистрируются в системной «Общей папке» и затем могут быть перемещены в одну из зарегистрированных абонентских папок в соответствии со следующим алгоритмом:

- программа удостоверяющего центра ищет абонентскую папку с атрибутами, совпадающими с атрибутами из обрабатываемого запроса (шаблон уникального имени, разрешенные криптоалгоритмы и длина ключей в запросах, разрешенный тип сертификатов);
- если такая папка найдена, запись о новом абоненте помещается в эту папку; поиск ведется в порядке убывания значения поля «Приоритет» абонентских папок.

3.8.2. Автоматическая обработка запросов из Интернет

В программе удостоверяющего центра реализована возможность автоматической обработки запросов, импортируемых из базы данных (буферная БД или база данных Интернет) приложения «Notary-PRO Web Pages» [12]. Для настройки режима автоматической обработки Администратору УЦ необходимо:

- выбрать пункт главного меню «Формирование документов/Запросы/Автоматическая обработка/Из Интернет»;
- в окне диалога (см. Рис. 83) установить параметры автообработки:
 - ☐ установить флаг регистрации новых абонентов, если при автоматической обработке запросов разрешается регистрировать новых абонентов с атрибутами имени, взятыми из запроса¹;
 - ☐ указать абонентскую папку, куда будут помещаться записи о новых абонентах (при необходимости);
 - ☐ установить интервал опроса базы данных Интернет приложения «Notary-PRO Web Pages»;
 - ☐ опция «Хранить записи...» позволяет производить периодическое автоматическое удаление записей из таблиц базы данных Интернет, в которой временно хранятся запросы пользователей, поступивших на обработку через Интернет; в той же базе хранятся сертификаты, которые пользователь может получить через Web-интерфейс;

¹ Новый абонент будет зарегистрирован только в том случае, если импортируемый запрос самоподписан и в базе данных Удостоверяющего центра нет ни одного сертификата с уникальным именем, совпадающим с атрибутами имени в запросе.

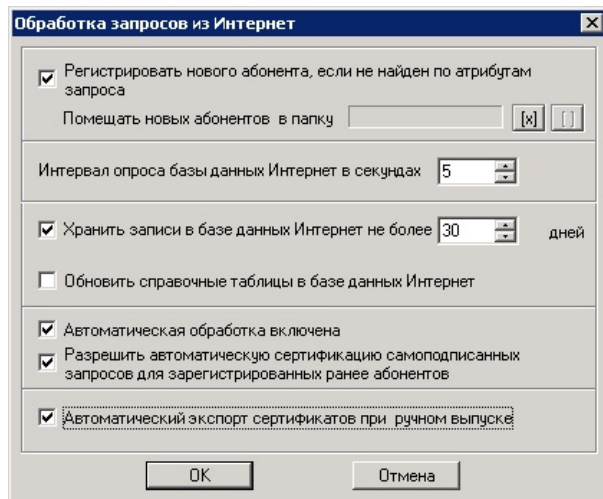


Рис. 83 Диалог установки параметров автоматической обработки запросов из Интернет

- ☐ при необходимости установить флаг обновления справочных таблиц (таблицы со списками действительных сертификатов УЦ) в базе данных Интернет.

При установленном флаге «Автоматическая обработка включена» автообработка запускается сразу после выхода из окна диалога по клавише «ОК».

Запросы, полученные из базы данных Интернет приложения «Notary-PRO Web Pages», могут автоматически сертифицироваться после регистрации, если в свойствах соответствующей папки установлен флаг «Автоматическая сертификация разрешена» (см. п. 2.2.3.1).

Процедура поиска абонентской папки для новых абонентов при автоматической обработке запросов из Интернет ничем не отличаются от аналогичной процедуры при автоматической обработке запросов из файловой системы (см.п. 3.8.1).

При ручной сертификации запросов, импортированных из базы данных Интернет, допускается использование настройки «Автоматический экспорт сертификатов при ручном выпуске» (см. Рис. 83). Следует иметь в виду, что установка режима автоматического экспорта сертификатов в Интернет лишает Администратора УЦ возможности просмотра созданного сертификата и его удаления.

3.8.3. Автоматическая обработка запросов от Операторов РЦ

В программе удостоверяющего центра реализована возможность автоматической обработки запросов абонентов, зарегистрированных Операторами регистрационных центров (см. п. 5).

Автоматическая обработка запросов от Операторов регистрационных центров настраивается по команде главного меню «Формирование документов/Запросы/Автоматическая обработка/От Операторов...»

Настройка сводится к установке следующих параметров в появляющемся диалоге (см. Рис. 84):

- «Интервал между вызовами процедуры обработки Запросов на Сертификацию...» - указывается интервал времени в секундах;
- «Предельное количество Запросов на сертификацию, обрабатываемое за один вызов ...» - используется для уменьшения времени реакции программы при обработке большого числа запросов.

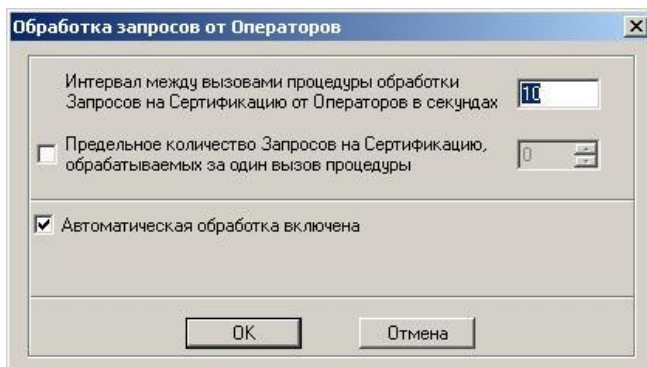


Рис. 84 Диалог установки параметров автоматической обработки запросов от Операторов РЦ

При установленном флаге «Автоматическая обработка включена» автообработка запускается сразу после выхода из окна диалога по клавише «ОК».

3.8.4. Ограничение при автоматической обработке СМС-запросов

В текущей версии программы по умолчанию *запрещен* автоматический выпуск сертификатов на основе СМС-запросов при несовпадении атрибутов полного имени в запросе с атрибутами абонента (например, при смене атрибутов абонента в результате изменения должности). Обработка подобных запросов становится возможной только в ручном режиме.

Для того чтобы отменить действующее ограничение, необходимо снять отметку с элемента управления «Запретить автоматическую сертификацию при изменении атрибутов уникального имени», как это показано на Рис. 85.

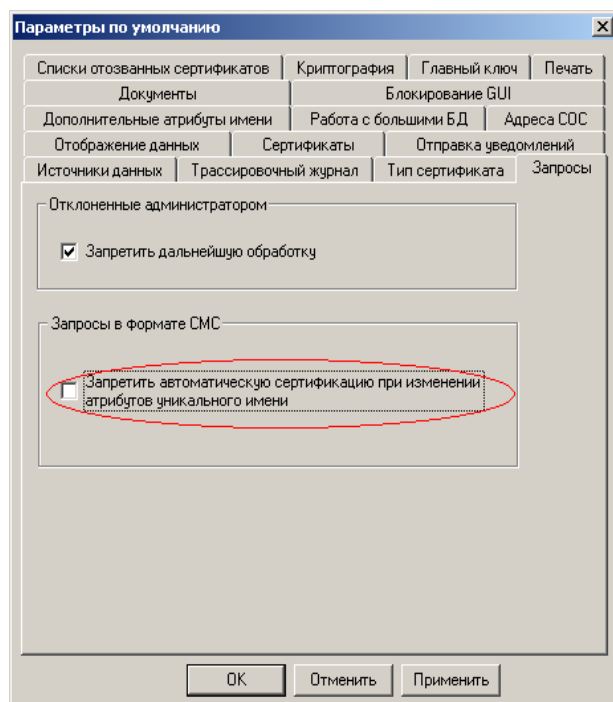


Рис. 85 Снятие ограничения на автоматическую сертификацию СМС-запросов

3.8.5. Фильтрация при автоматической обработке запросов

В УЦ «Notary-PRO» запрещается автоматическая сертификация запросов, если выполняется хотя бы одно из перечисленных ниже условий:

- владелец ключа не аутентифицирован (запрос не был доставлен лично владельцем и при этом не проверен ни одним из его действующих сертификатов);
- обладание секретным ключом не доказано (запрос не содержит корректную ЭП, которая может быть проверена при помощи открытого ключа, содержащегося в запросе);
- атрибуты имени в запросе (subject) не соответствуют текущим регистрационным данным абонента.

Запросы, не удовлетворяющие данным критериям («сомнительные» запросы), подлежат только ручной обработке.

При ручной сертификации любого запроса всегда выполняется проверка по указанным выше критериям и в случае появления «сомнительного» запроса Администратор получит предупреждение, как на Рис. 86.

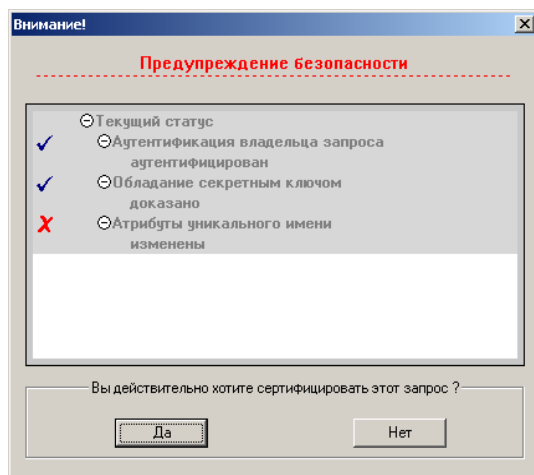


Рис. 86 Предупреждение при сертификации запроса

Решение о сертификации подобного запроса принимает Администратор. При отказе от сертификации запроса рекомендуется завершить его обработку и выполнить процедуру отклонения запроса с указанием причины.

3.9. Выборки

3.9.1. Создание выборки

Для каждого стандартного набора данных (см. описание папок/окон документов), можно создать произвольную выборку данных. По сути, создание пользовательского набора данных сводится к созданию подмножества записей на основе уже существующего набора данных в базе данных удостоверяющего центра. Процедура создания пользовательского набора данных включает следующие действия:

- в Главной панели выбрать папку документов, на основе которой будет создаваться выборка;
- нажать правую клавишу мыши на выделенной папке; в появившемся меню выбрать пункт «Создать выборку»;
- в окне диалога (см. Рис. 87) следует:
 - ввести имя нового набора данных в поле «Наименование выборки»;
 - с помощью панели со списком атрибутов запроса сформировать новую строку запроса, которая при нажатии кнопки «Добавить» добавляется в текст запроса;

повторить этот пункт необходимое число раз, пока вы не получите нужное условие новой выборки;

Примечание: нажатием кнопки «Очистить» можно удалить последнюю строку из условия выборки.

- ☐ установить флаг «Сохранить выборку в базе данных», чтобы выборка сохранилась при последующих запусках программы;
- ☐ нажать кнопку «ОК»; при этом будет создано окно с новым набором данных.

Рис. 87 Диалог создания выборки на примере создания набора сертификатов, опубликованных за последние сутки

3.9.2. Удаление выборки

Для удаления выборки следует нажать правую клавишу мыши на выбранном пользовательском наборе данных и в появившемся меню выбрать пункт «Удалить».

3.9.3. Редактирование выборки

Для редактирования выборки следует нажать правую клавишу мыши на выбранном наборе данных и в появившемся меню выбрать пункт «Параметры выборки».

3.10. Дополнительные функции администрирования

3.10.1. Просмотр журнала событий

Окно «Журнал событий» вызывается из главного меню, пункт «Администрирование/Просмотр и настройка журнала событий» и представляет собой двухстраничное окно.

Первая страница «Журнала событий» (см. Рис. 88) содержит записи об основных действиях Администратора либо о событиях, произошедших в процессе автоматической обработки запросов, а также об ошибках программы.

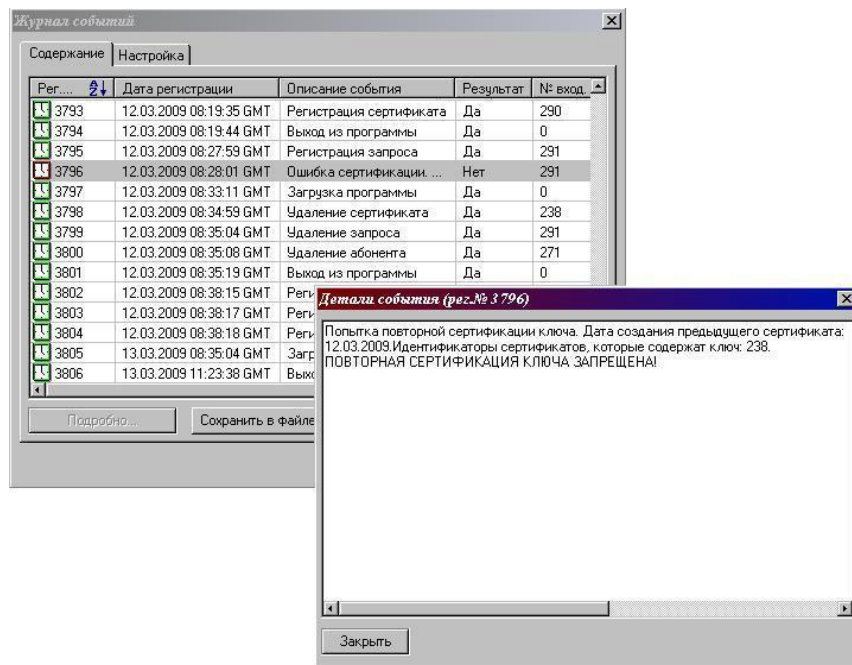


Рис. 88 Страница «Содержание» окна свойств журнала событий

Информация «Журнала событий» отображается в виде таблицы следующего формата:

Таблица 3

Наименование поля	Содержание
Рег.№	Регистрационный номер записи; присваивается автоматически; не может быть изменен.
Дата регистрации	Время формирования записи в журнале событий.
Описание события	Краткое описание события.
Результат	Успешный/неуспешный результат обработки события
Тип события	Код события.
Оператор	Идентификатор Оператора, который зарегистрировал документ.

По нажатию кнопки «Подробнее...» на экран выводится окно, содержащее комментарий либо уточнение к текущей записи.

Копирование журнала в текстовый файл осуществляется нажатием кнопки «Сохранить в файле...». При этом требуется задать каталог и имя файла для сохранения.

Записи в журнале событий накапливаются неограниченно. Журнал может быть очищен нажатием кнопки «Очистить сейчас», расположенной на странице «Настройка» (см. Рис. 89). При очистке журнала сохраняются записи за несколько последних дней, число которых указано в настройке «Журнала событий»:

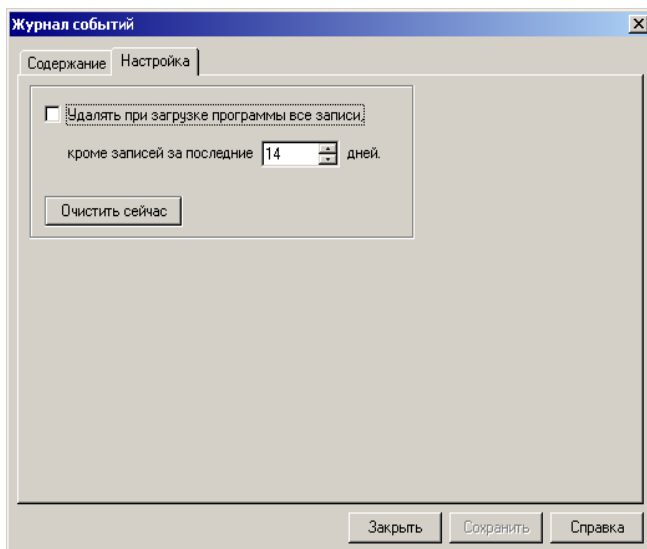


Рис. 89 Страница «Настройка» окна свойств журнала событий

Администратор удостоверяющего центра может установить флаг «Удалять при загрузке программы все записи», обеспечивающий автоматическую очистку журнала событий при загрузке программы.

3.10.2. Резервное копирование базы данных

Возможность резервного копирования базы данных удостоверяющего центра средствами самих СУБД (Microsoft SQL Server или Oracle) описана в разделе **Ошибка! Источник ссылки не найден.** настоящего Руководства.

Резервное копирование базы данных удостоверяющего центра встроенными средствами УЦ реализовано только для СУБД Microsoft SQL Server (либо MSDE).

Окно «Резервное копирование базы данных» (см. Рис. 90) вызывается из главного меню, пункт «Администрирование/Резервное копирование базы данных», и содержит следующие элементы:

- текстовое поле, в котором задается путь к каталогу, предназначенному для хранения файлов копий базы данных;
- поле для задания числа одновременно хранимых копий;
- кнопка «Создать резервную копию...» для принудительного создания резервной копии базы данных удостоверяющего центра;
- флаг инициализации режима автоматического резервного копирования;
- параметры режима автоматического резервного копирования:
 - ☐ событие, используемое для инициализации процедуры резервного копирования в автоматическом режиме (запуск программы или выход из программы);
 - ☐ периодичность создания резервных копий в автоматическом режиме.

Файлы с копиями базы данных удостоверяющего центра сохраняются в выбранном каталоге на том компьютере, на котором установлена база данных удостоверяющего центра.

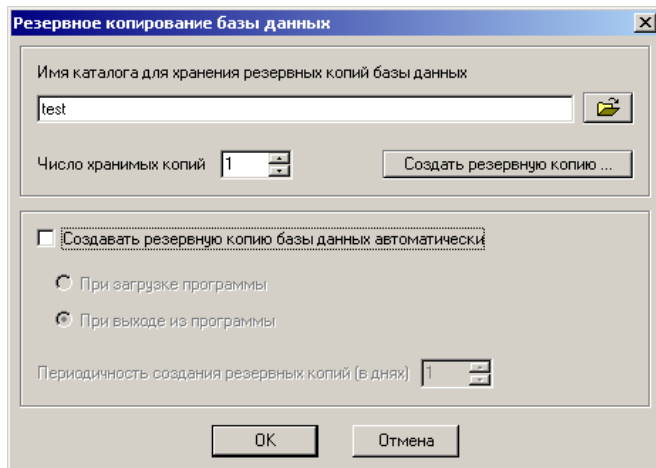


Рис. 90 Окно резервного копирования БД УЦ

Примечание. Имена файлов с копиями базы данных формируются по следующему правилу: к фиксированной части имени – «Сору» добавляется текущая дата в формате «ГГГГММДД», где ГГГГ - текущий год; ММ - текущий месяц; ДД - текущий день. Все файлы копий базы данных удостоверяющего центра имеют расширение «n3m». Имена файлов с копиями баз данных менять не рекомендуется.

Восстановление базы данных до состояния, в котором база данных находилась на момент создания резервной копии, осуществляется с помощью стандартных средств СУБД.

3.10.3. Изменение лицензии

Окно «Лицензия» (см. Рис. 91) вызывается из главного меню, пункт «Администрирование/Лицензия...», и содержит следующую информацию:

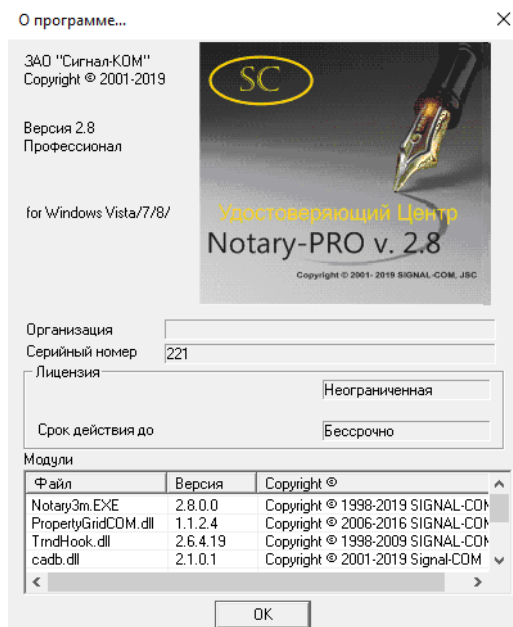


Рис. 91 Окно «Лицензия»

- наименование организации;
- уникальный серийный номер программного обеспечения;
- размер лицензии (конкретное число, либо «Неограниченная»); под размером лицензии подразумевается количество уникальных имен (см. п. 1.7), которые могут быть зарегистрированы программой;
- количество уникальных имен, которые уже зарегистрированы программой на данный момент времени;
- срок истечения лицензионного соглашения (конкретная дата, либо «Бессрочно»).

Параметры лицензионного соглашения могут быть изменены удаленно. Для этого Администратор удостоверяющего центра должен получить от поставщика программного обеспечения «Notary-PRO» специальный одноразовый пароль. Пароль может быть получен любым способом (по телефону, факсимильной связи, электронной почте и т.п.).

В нижней части окна имеется поле для ввода пароля на изменение лицензии. После ввода пароля следует нажать кнопку «Изменить...». В случае успешного выполнения операции под заголовком «Новые параметры» будут отображены новые параметры лицензионного соглашения.

Программа не позволяет повторно использовать пароль на изменение лицензии.

3.10.4. Копирование ключевого носителя СКЗИ

Для того, чтобы выполнить резервное копирование ключевого носителя СКЗИ «CADB 2.1», необходимо воспользоваться командой главного меню «Формирование документов/Ключи УЦ/Копирование ключевого носителя СКЗИ».

После выбора этого пункта меню требуется установить ключевой носитель в считывающее устройство и ввести пароль для доступа к Главному ключу. Если пароль введен правильно, появляется диалог «Резервное копирование ключевого носителя СКЗИ». Далее требуется указать путь к каталогу для резервной копии.

3.10.5. Резервное копирование главного ключа

Для того, чтобы выполнить резервное копирование главного ключа, необходимо воспользоваться командой главного меню «Формирование документов/Ключи УЦ/Копирование главного ключа».

После выбора этого пункта меню требуется ввести пароль для доступа к Главному ключу. Если пароль введен правильно, в появившемся диалоге необходимо указать расположение резервной копии главного ключа.

3.10.6. Переход к схеме разделения секрета

Для того чтобы перейти на работу по схеме «с разделением секрета» (см. п.1.11.3), необходимо в Главной панели установить курсор на папку «Ключи УЦ» и воспользоваться командой главного меню «Формирование документов/Ключи УЦ/Переход к схеме разделения секрета...».

После запрошенного ввода пароля к Главному ключу УЦ в открывшемся окне диалога (см. Рис. 92) следует выбрать схему разделения секрета:

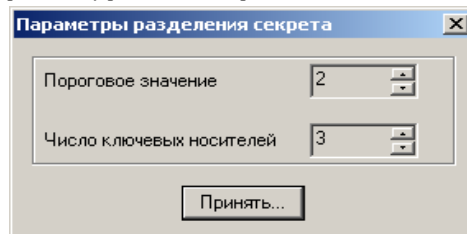


Рис. 92 Окно настройки параметров схемы «с разделением секрета»

- параметр «Пороговое значение» задает количество ключевых носителей, одновременное предъявление которых необходимо для доступа к ключам УЦ;

- параметр «Число ключевых носителей» задает количество частей, на которое будет разделен исходный ключевой носитель.

Рекомендуемые параметры схемы «разделения секрета» приведены в п. 1.11.3.

После нажатия кнопки «Принять» появляется диалоговое окно (см. Рис. 93), в котором необходимо указать тип нового ключевого носителя СКЗИ и путь к каталогу нового ключевого носителя.

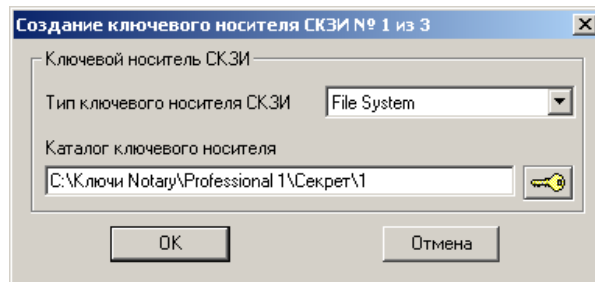


Рис. 93 Окно создания нового ключевого носителя

Данную процедуру необходимо повторить столько раз, сколько ключевых носителей было задано в окне настройки параметров схемы «с разделением секрета».

После того, как будут созданы все ключевые носители, необходимо перезапустить ПО удостоверяющего центра.

Обновление частей разделенного секрета аналогично процедуре первоначального «разделения секрета», описанной выше, но активация обновления возможна только после предъявления порогового количества частей действующего разделенного ключевого контейнера.

3.10.7. Настройка шаблонов печати документов

Шаблон печати документа представляет собой текстовый файл с расширением .tpl, в состав которого включаются управляющие слова, заменяемые при печати соответствующими значениями из текущего документа. Список поддерживаемых управляющих слов приведен в следующей таблице:

Таблица 4

Версия документа:	[!VERSION!]
Серийный номер документа:	[!SERIALNUM!]
Дата начала периода действия документа:	[!NOTBEFORE!]
Дата окончания периода действия документа:	[!NOTAFTER!]
Уникальное имя владельца документа	
Полное имя:	[!SUB_DN_CN!]
Организация:	[!SUB_DN_O!]
Подразделение:	[!SUB_DN_OU!]
Должность:	[!SUB_DN_T!]
Город:	[!SUB_DN_L!]
Область:	[!SUB_DN_SP!]
Страна:	[!SUB_DN_C!]
Адрес электронной почты:	[!SUB_DN_EMAIL!]

Уникальное имя издателя документа	
Полное имя:	[!ISS_DN_CN!]
Организация:	[!ISS_DN_O!]
Подразделение:	[!ISS_DN_OU!]
Должность:	[!ISS_DN_T!]
Город/село:	[!ISS_DN_L!]
Область:	[!ISS_DN_SP!]
Страна:	[!ISS_DN_C!]
Адрес электронной почты:	[!ISS_DN_EMAIL!]
Ключ проверки ЭП владельца документа:	[!PUB_KEY!]
Расширения в сертификате:	[!EXTENSIONS!]
Подпись издателя документа:	[!SIGN!]
Текст документа:	[!TEXT!]
Документ в формате PEM:	[!BODY!]
Значение хэш-функции ГОСТ:	[!FP_GOST!]
Значение хэш-функции MD5:	[!FP_MD5!]
Значение хэш-функции SHA-1:	[!FP_SHA1!]

4. НАСТРОЙКА РАСШИРЕНИЙ СЕРТИФИКАТОВ

4.1. Настройка списка расширений

Настройка списка расширений производится на странице «Расширения», которая доступна в нескольких диалогах и окнах свойств:

- окно свойств шаблона администрирования (см. п. 3.2);
- диалоговое окно параметров сертификации ключа УЦ (см. п. 3.3.5);
- диалоговое окно параметров сертификации запроса (см. п. 3.5.4);
- окно свойств сертификата (см. п. 3.6.2);
- диалоговое окно формирования запроса для ключа УЦ (см. п. 6.1).

Любое расширение может быть помечено как критичное установкой флажка «Расширение критично» на соответствующей странице редактирования свойств расширения.

Пример страницы «Расширения» приведен на Рис. 94. Расширения, перечисленные в списке, будут включены в сертификат.

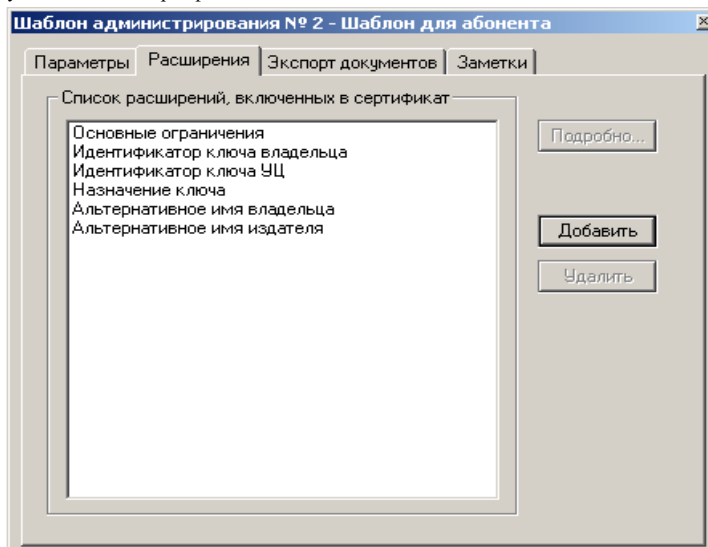


Рис. 94 Страница «Расширения» окна сертификации запроса

По кнопке «Подробнее...» вызывается окно редактирования свойств конкретного расширения. При выделении в списке нескольких расширений вызывается многостраничный диалог, позволяющий редактировать сразу несколько расширений.

Кнопка «Удалить» приводит к исключению выделенного расширения из списка включаемых в сертификат.

Кнопка «Добавить...» вызывает диалог (см. Рис. 95), позволяющий управлять списком расширений.

Кнопка «Добавить» добавляет выбранные в левом списке расширения в список включаемых в сертификат.

Кнопка «Удалить» удаляет выбранные в правом списке расширения из списка включаемых в сертификат.

Кнопки «Добавить все...» и «Удалить все...» позволяют добавлять и удалять сразу весь список.

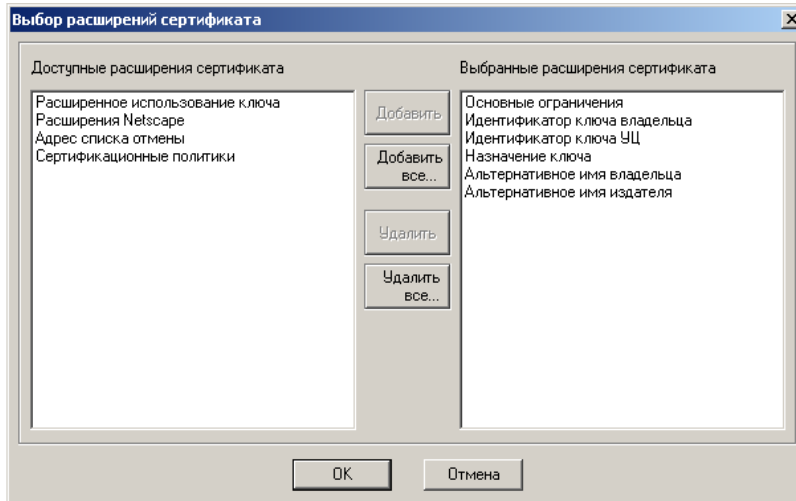


Рис. 95 Окно редактирования списка расширений

4.2. Настройка расширения Basic Constraints (Основные ограничения)

Настройка расширения Basic Constraints (Основные ограничения) производится на странице «Основные ограничения» окна «Расширения сертификата» (см. Рис. 96).

Флажок «Администратор» служит признаком принадлежности сертификата Администратору УЦ: для сертификатов УЦ флажок должен быть установлен, для остальных сертификатов – сброшен.

Длина сертификационного пути – целое значение, указывающее максимальную длину сертификационного пути; имеет значение только для сертификатов УЦ: значение 0 означает, что с помощью данного сертификата УЦ могут выпускаться только сертификаты конечных пользователей; флажок «Без ограничений» снимает всякие ограничения на длину сертификационного пути для данного сертификата УЦ.

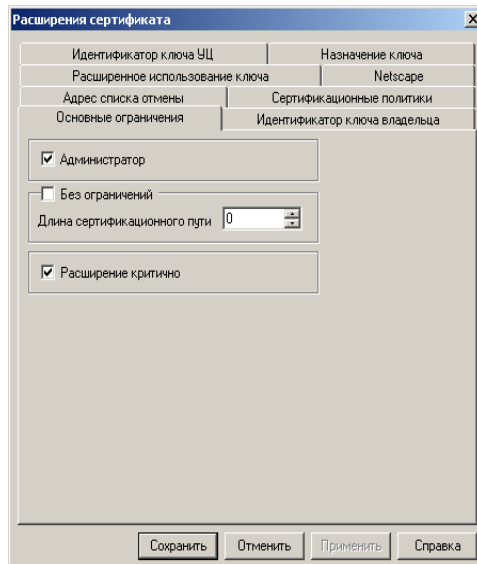


Рис. 96 Страница редактирования расширения Basic Constraints

4.3. Настройка расширения Subject Key Identifier (Идентификатор ключа владельца)

Настройка расширения Subject Key Identifier (Идентификатор ключа владельца) производится на странице «Идентификатор ключа владельца» окна «Расширения сертификата» (см. Рис. 97).

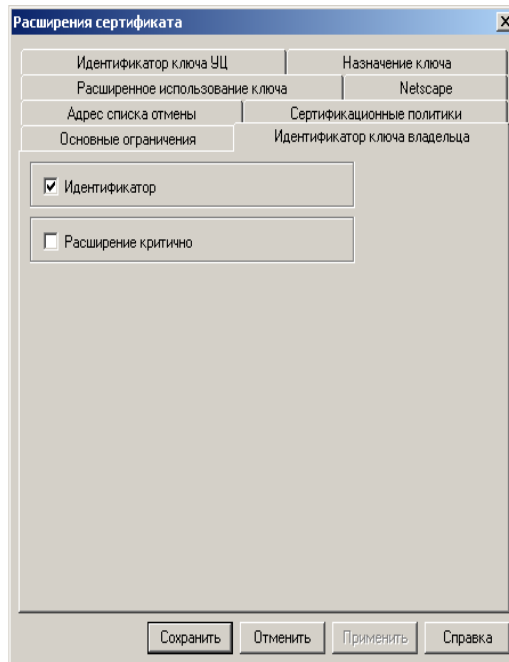


Рис. 97 Страница редактирования расширения Subject Key Identifier

Установленный флажок «Идентификатор» служит признаком необходимости включения идентификатора ключа проверки ЭП владельца в сертификат.

По умолчанию флажок установлен.

4.4. Настройка расширения Authority Key Identifier (Идентификатор ключа УЦ)

Настройка расширения Authority Key Identifier (Идентификатор ключа УЦ) производится на странице «Идентификатор ключа УЦ» окна «Расширения сертификата» (см. Рис. 98).

Флажок «Идентификатор» служит признаком необходимости включения идентификатора ключа проверки ЭП УЦ в выпускаемый сертификат.

Флажок «Уникальное имя и серийный номер» служит признаком необходимости включения уникального имени УЦ и серийного номера сертификата УЦ в выпускаемый сертификат.

Хотя бы один из флажков должен быть всегда установлен. Допустима установка обоих флажков. Рекомендуется использование только флажка «Идентификатор».

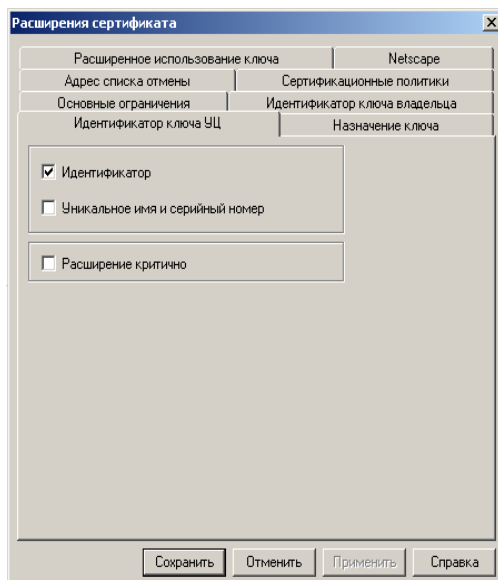


Рис. 98 Страница редактирования расширения Authority Key Identifier

4.5. Настройка расширения Key Usage (Назначение ключа)

Настройка расширения Key Usage (Назначение ключа) производится на странице «Назначение ключа» окна «Расширения сертификата» (см. Рис. 99).

Необходимо поставить флаги в полях, соответствующих назначению данного сертификата¹. Хотя бы один из флажков должен быть установлен.

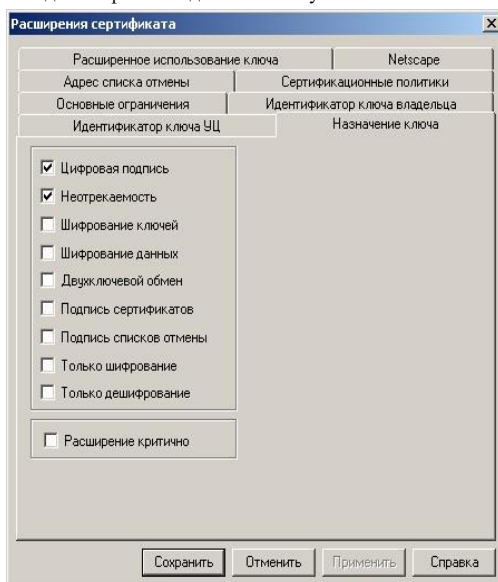


Рис. 99 Страница редактирования расширения Key Usage

¹ В версии «Notary-PRO Standard» поля «Подпись сертификатов» и «Подпись списков отмены» недоступны для редактирования.

4.6. Настройка расширения Extended Key Usage (Расширенное использование ключа)

Настройка расширения Extended Key Usage (Расширенное использование ключа) производится на странице «Расширенное использование ключа» окна «Расширения сертификата» (см. Рис. 100).

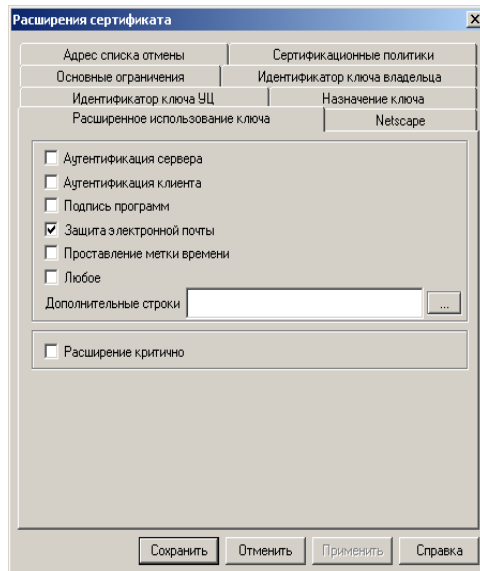


Рис. 100 Страница редактирования расширения Extended Key Usage

Необходимо поставить флаги в полях, соответствующих назначению данного сертификата. Хотя бы один из флагов должен быть установлен. Помимо стандартных назначений сертификата, через кнопку редактирования поля «Дополнительные строки» могут быть добавлены произвольные идентификаторы (см. Рис. 101). Идентификаторы должны быть записаны в десятично-точечном представлении.

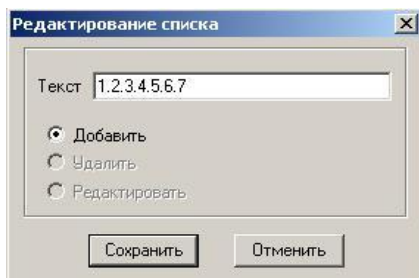


Рис. 101 Страница редактирования идентификатора, включаемого в расширение Extended Key Usage

Список идентификаторов объектов, включаемых в «Расширенное использование ключа» может быть заполнен из внешнего списка идентификаторов объектов (OID) (см. Приложение 3. Изменение вида настроек расширенного использования ключа).

4.7. Настройка расширения Subject Alternative Name (Альтернативное имя владельца)

Настройка расширения Subject Alternative Name (Альтернативное имя владельца) является индивидуальной для каждого абонента, поэтому настройка данного расширения через общие шаблоны администрирования недоступна. В шаблонах можно задать лишь наличие

данного расширения в сертификате (см. п. 3.2.2.2). Настройку расширения Subject Alternative Name следует производить непосредственно в окне свойств абонента (до сертификации запросов). Для этого необходимо:

- в папке «Абоненты» соответствующей абонентской папки выделить курсором нужного абонента и нажать кнопку «Подробнее...» на Панели управления;
- в открывшемся окне свойств абонента перейти на страницу «Дополнительные атрибуты»;
- установить флаг в поле «Альтернативное имя» (см. п. 3.4.2.5) и нажать кнопку «Редактировать...»;
- в открывшемся окне настройки расширения Subject Alternative Name (см. Рис. 102) осуществляется ввод (редактирование) параметров:

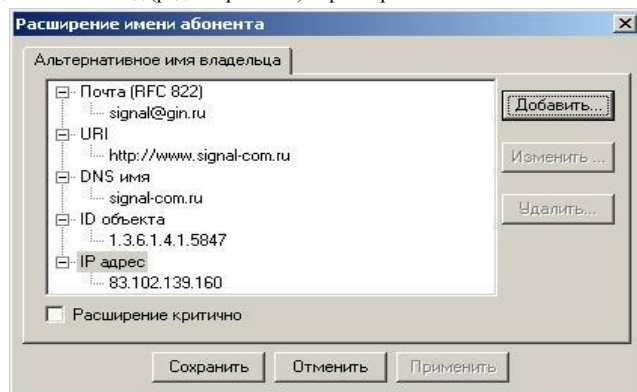


Рис. 102 Окно редактирования расширения Subject Alternative Name

Добавление новых значений осуществляется выбором соответствующего узла дерева имен с последующим нажатием кнопки «Добавить...». В появившемся диалоге (см. Рис. 103) необходимо ввести новое значение.



Рис. 103 Окно редактирования адреса электронной почты, включаемого в расширение Subject Alternative Name

Редактирование значений осуществляется выбором конкретного значения с последующим нажатием кнопки «Изменить...». В появившемся диалоге (см. Рис. 103) необходимо изменить текущее значение.

Удаление значений осуществляется выбором конкретного значения с последующим нажатием кнопки «Удалить...».

После окончания ввода всех необходимых данных нажмите кнопку «Сохранить».

Расширение Subject Alternative Name (Альтернативное имя владельца) при сертификации запроса будет попадать в сертификат абонента только в том случае, если данное расширение присутствует в шаблоне администрирования (см. п. 3.2.2.2) и одновременно установлен флаг в поле «Альтернативное имя» на странице «Дополнительные атрибуты» окна свойств абонента (см. п. 3.4.2.5).

4.8. Настройка расширения Issuer Alternative Name (Альтернативное имя издателя)

Настройка расширения Issuer Alternative Name (Альтернативное имя издателя) через общие шаблоны администрирования недоступна. В шаблонах можно задать лишь наличие данного расширения в сертификате (см. п. 3.2.2.2). Настройку расширения Issuer Alternative Name следует производить непосредственно в окне свойств абонента Администратор УЦ

(абонент с регистрационным номером 1), находящегося в папке «Администратор УЦ/Абоненты».

Порядок настройки расширения Issuer Alternative Name аналогичен порядку настройки расширения Subject Alternative Name (см. п. 3.4.2.5).

4.9. Настройка расширения Certificate Policies (Сертификационные политики)

Настройка расширения Certificate Policies (Сертификационные политики) производится на странице «Сертификационные политики» окна «Расширения сертификата» (см. Рис. 104).

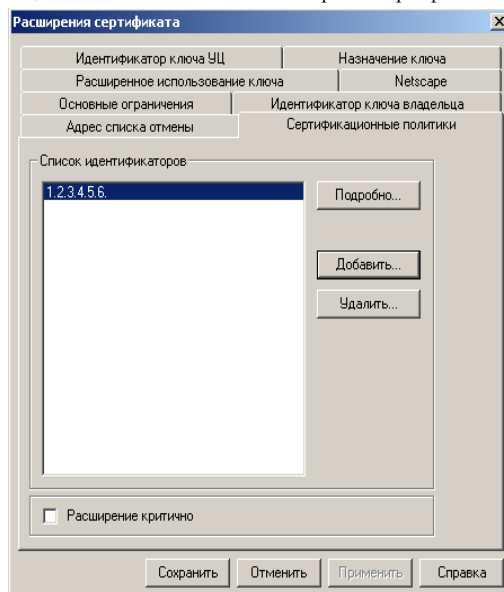


Рис. 104 Страница редактирования расширения Certificate Policies

Добавление новых значений осуществляется нажатием кнопки «Добавить...». В появившемся диалоге (см. Рис. 105) необходимо настроить необходимые поля.

Редактирование значений осуществляется выбором конкретного значения с последующим нажатием кнопки «Подробнее...». В появившемся диалоге (см. Рис. 105) необходимо отредактировать нужные поля.

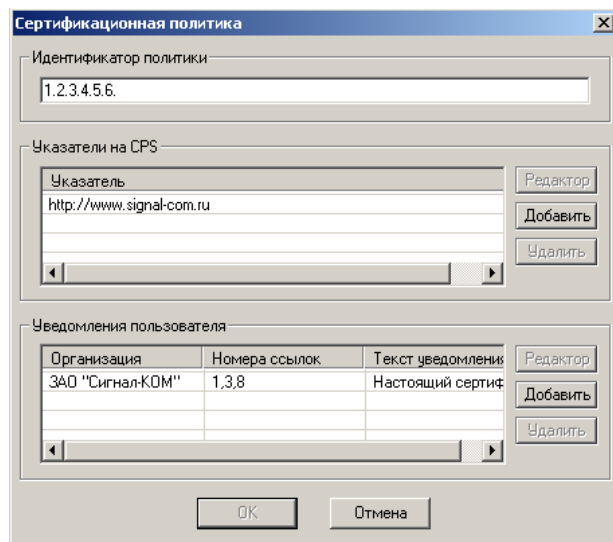


Рис. 105 Окно редактирования сертификационной политики, включаемой в расширение Certificate Policies

Удаление значений осуществляется выбором конкретного значения с последующим нажатием кнопки «Удалить...».

Поле «Идентификатор политики» является обязательным для заполнения и должно содержать OID сертификационной политики в десятично-точечном представлении.

Помимо собственно идентификатора, расширение, описывающее сертификационную политику, может содержать квалификаторы: указатели на CPS и/или уведомления пользователя.

Список «Указатели на CPS» содержит адреса (URI), по которым доступен документ, описывающий регламент работы УЦ. Для управления списком предназначены 3 кнопки справа от списка: «Добавить», «Редактор» и «Удалить». Диалог формирования нового значения указателя приведен на Рис. 106.



Рис. 106 Окно формирования нового указателя на CPS

Список «Уведомления пользователя» содержит уведомления об использовании сертификата. Для управления списком предназначены 3 кнопки справа от списка: «Добавить», «Редактор» и «Удалить». Диалог формирования нового уведомления пользователя приведен на Рис. 107.

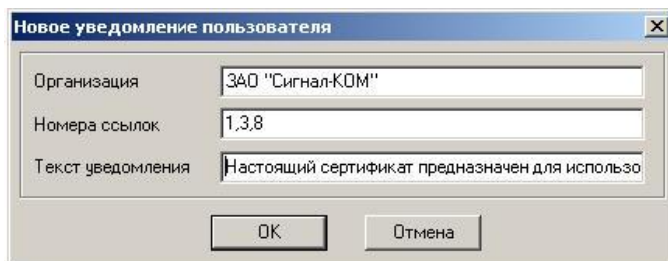


Рис. 107 Окно формирования нового уведомления пользователя

В диалоге формирования нового уведомления пользователя необходимо заполнить либо поля «Организация» и «Номера ссылок», либо поле «Текст уведомления», либо все три поля. Подробнее об использовании уведомлений пользователя в качестве квалификаторов сертификационной политики см. RFC 5280 [19].

4.10. Настройка расширения CRL Distribution Points (Адрес списка отозванных сертификатов)

Настройка расширения CRL Distribution Points (Адрес списка отозванных сертификатов) производится на странице «Адрес списка отмены» окна «Расширения сертификата» (см. Рис. 108).

Добавление, редактирование и удаление значений осуществляется аналогично описанному в п. 4.7.

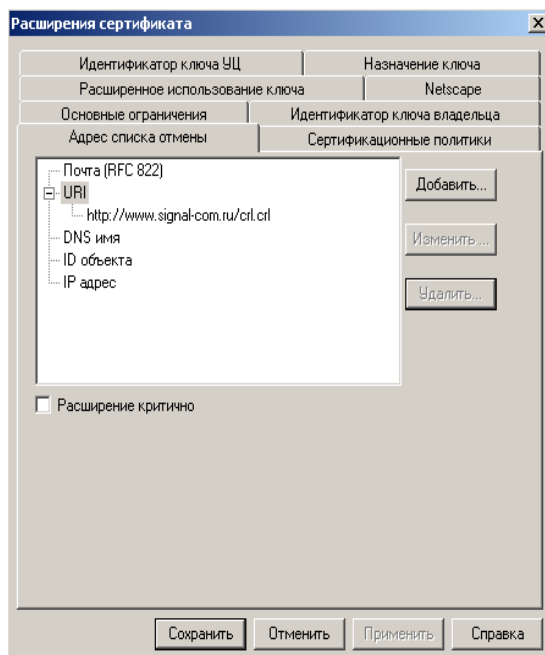


Рис. 108 Страница редактирования расширения CRL Distribution Points

4.11. Настройка расширений Netscape

Настройка расширений Netscape производится на странице «Netscape» окна «Расширения сертификата» (см. Рис. 109).

В окне настройки расширения необходимо поставить флажки или ввести необходимые параметры в соответствующие поля. Хотя бы один флажок должен быть установлен, либо хотя бы одно поле должно быть заполнено.

Рис. 109 Страница редактирования расширений Netscape

4.12. Настройка расширения Private Key Usage Period (Период действия закрытого ключа)

Настройка расширения Private Key Usage Period (Период действия закрытого ключа) производится на странице «Период действия закрытого ключа» окна «Расширения сертификата» (см. Рис. 110). В окне настройки расширения необходимо установить период (в днях).

Расширения сертификата

Идентификатор ключа УЦ	Назначение ключа
Расширенное использование ключа	Netscape Адрес списка отмены
Сертификационные политики	Справочные атрибуты субъекта
Доступ к субъекту	Доступ к издателю Имя_шаблона_администратора
Основные ограничения	Идентификатор ключа владельца
Признак_доверия_службе_OCSP	Период действия закрытого ключа

⊖ Период действия закрытого ключа

OID	2.5.29.16
Период в днях	365

Добавить...

Удалить...

Сохранить

Отменить

Рис. 110 Страница редактирования расширения Private Key Usage Period

5. ВЗАИМОДЕЙСТВИЕ С ОПЕРАТОРАМИ РЕГИСТРАЦИОННЫХ ЦЕНТРОВ

5.1. Регистрация имени Оператора

Для обеспечения доступа Оператора регистрационного центра к БД удостоверяющего центра Администратор должен выполнить следующие действия:

- зарегистрировать нового абонента (см. п. 3.4.1) и назначить ему роль «Оператор RA» (см. п. 3.4.2.5);
- зарегистрировать запрос на сертификацию от абонента из предыдущего пункта (см. п. 3.5.1) и создать сертификат (см. п. 3.5.4);
- зарегистрировать имя Оператора регистрационного центра (см. п. 5.1);
- разрешить Оператору доступ к необходимым папкам документов (см. п. 5.2);
- при необходимости включить режим автоматической обработки запросов от Операторов РЦ (см. п. 3.8.3);
- при необходимости установить для Операторов РЦ квоту на выпуск сертификатов (см. п. 5.4).

Для создания новой записи об Операторе РЦ необходимо:

- открыть в Главной панели папку документов «Роли/Операторы РЦ»;
- на Панели управления окна данной папки нажать кнопку «Новый»;
- в появившемся окне (см. Рис. 111) необходимо отметить требуемую запись и закрыть окно нажатием кнопки «Выбрать»; при этом в окне папки «Операторы РЦ» появится новая запись.

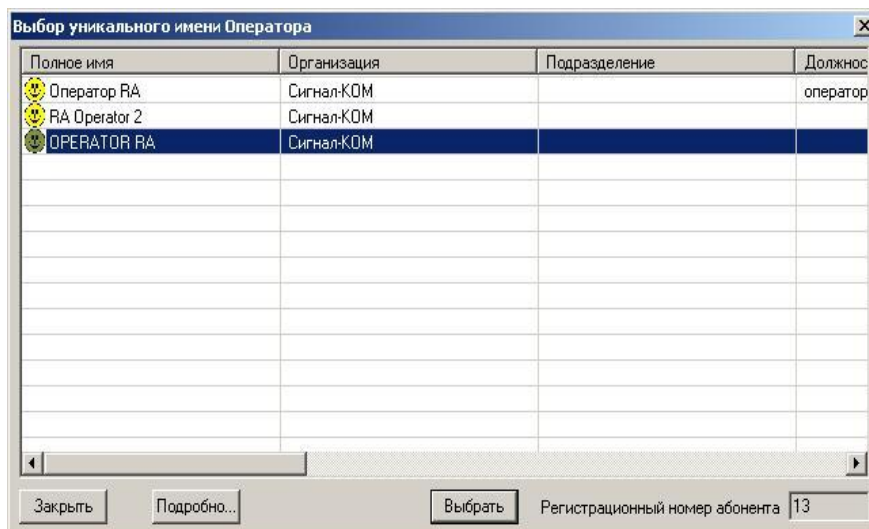


Рис. 111 Окно выбора уникального имени Оператора

5.2. Назначение Оператору РЦ прав доступа к папкам документов

Чтобы разрешить Оператору РЦ доступ к необходимым папкам документов, Администратор должен:

- выбрать нужного Оператора в окне папки «Роли/Операторы РЦ» и нажать кнопку «Доступ к папкам...» в Панели управления;
- в появившемся окне (см. Рис. 112) отметить папки, которые будут доступны данному Оператору РЦ; для назначения доступа к папке «Общая» необходимо нажать кнопку «Показать все» и пометить папку галочкой;
- нажать кнопку «Сохранить» и закрыть окно нажатием кнопки «Закрыть».

Все изменения будут доступны для Оператора только после перезагрузки модуля «Notary-PRO RA» [6].

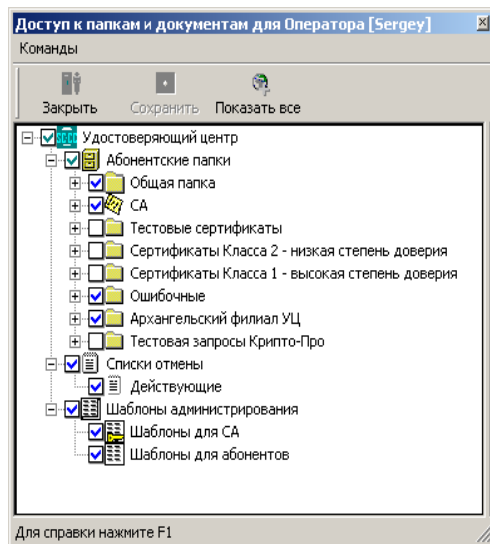


Рис. 112 Окно назначения Оператору РЦ прав доступа к папкам документов УЦ

5.3. Установка свойств Оператора РЦ

Доступ к свойствам Оператора регистрационного центра можно получить по нажатию кнопки «Подробнее...» на Панели управления в окне папки «Роли/Операторы РЦ».

В появившемся диалоговом окне с названием «Свойства Оператора №...» (см. Рис. 113) Администратор может выбрать рабочий сертификат, который будет использоваться для аутентификации Оператора при его подключении к УЦ (к серверу РЦ).

Выбор нужного сертификата производится по кнопке выбора «[x]» на странице «Свойства Оператора». Если в поле редактирования «Рабочий сертификат Оператора» установить значение «0», Оператор сможет использовать для доступа к Серверу регистрационного центра любой из своих сертификатов.

Установка флажка «Работа разрешена» разрешает работу Оператора регистрационного центра.

Установка флажка «Автоматическая обработка запросов разрешена» задает режим автоматической обработки запросов, регистрируемых Оператором.

Установка флажка «Редактирование шаблонов для абонентов» позволяет Оператору редактировать шаблоны администрирования или оперативно изменять параметры сертификации запроса непосредственно в процессе его обработки.

Установка флажка «Сертификация всех доступных запросов» позволяет Оператору отправлять на сертификацию все запросы, находящиеся в доступных для него папках, даже если они были зарегистрированы другими Операторами или импортированы через Интернет.

Администратор может сохранить свой комментарий, заполнив поле редактирования «Комментарий».

The screenshot shows a window titled 'Свойства Оператора № 10'. It has two tabs: 'Свойства оператора' and 'Параметры'. The 'Параметры' tab is active. It contains the following fields and controls:

- Имя: Тестовый Абонент 9
- Тип: Операторы РА
- Рабочий сертификат Оператора: 0, with buttons [x], [], and -->
- Checkboxes:
 - ☒ Работа разрешена
 - ☒ Автоматическая обработка запросов
 - ☐ Редактирование шаблонов для абонентов
 - ☒ Сертификация всех доступных запросов
- Комментарий: (empty text area)

Рис. 113 Страница «Свойства Оператора» окна свойств Оператора РЦ

Страница свойств «Параметры» (см. Рис. 114) содержит идентификатор и параметры уникального имени Оператора РЦ.

The screenshot shows the same window as Figure 113, but with the 'Параметры' tab selected. It contains the following fields and controls:

- Идентификатор: Тестовый Абонент 9 (AUTO_10):[Class 1]
- Полное имя: Тестовый Абонент 9
- Организация: ЗАО Сигнал-КОМ
- Подразделение: (empty)
- Должность: (empty)
- Город/село: Москва
- Область/район: (empty)
- Страна: Россия (dropdown menu)
- Электронная почта: abonent-test 9@mail.ru
- Дата регистрации: 10.10.2008 09:45:18 GMT

Рис. 114 Страница «Параметры» окна свойств Оператора РЦ

5.4. Ограничение количества сертификатов, выпускаемых Операторами РЦ

Администратор УЦ может контролировать объем выданных сертификатов, устанавливая Операторам РЦ квоту (ограничение) на количество выпускаемых ими сертификатов. Для этого необходимо либо зарегистрировать данного Оператора РЦ в одной из уже существующих групп, для которой установлены соответствующие ограничения, либо создать для Оператора РЦ новую группу (см. п. 5.6.1).

Для регистрации Оператора РЦ в группе необходимо выполнить следующие действия:

- в соответствующей абонентской папке в разделе «Абоненты» выделить курсором запись, соответствующую данному Оператору РЦ, и нажать кнопку «Подробнее...» на Панели управления;
- в открывшемся окне свойств абонента перейти на страницу «Дополнительные атрибуты» (см. п. 3.4.2.5);
- в поле «Группа» выбрать из списка всех зарегистрированных в базе данных УЦ групп Операторов нужную группу.
- Процедура просмотра или редактирования свойств группы описана в п. 5.6.2.

5.5. Удаление записи об Операторе РЦ

Запись об Операторе регистрационного центра удаляется нажатием кнопки «Удалить...» Панели управления окна папки «Роли/Операторы РЦ» после выбора необходимой записи.

Запись не может быть удалена, пока существует хотя бы один запрос, зарегистрированный данным Оператором.

5.6. Группы Операторов РЦ

5.6.1. Формирование группы

Для формирования новой группы Операторов РЦ Администратору УЦ необходимо:

- находясь в папке «Группы», на Панели управления окна данной папки нажать кнопку «Новый...»;
- в появившемся окне (см. Рис. 115) ввести имя новой группы Операторов в поле «Наименование»;
- при необходимости установить флажок «Ограничение на выпуск сертификатов» и определить общее количество сертификатов (квоту), которое разрешено выпустить всем Операторам РЦ, зарегистрированным в данной группе; в окне «выпущено» отображается количество сертификатов, уже выпущенное данной группой операторов к настоящему моменту;
- в поле «Описание» при необходимости занести свои комментарии;
- нажать кнопку «ОК».

В окне папки «Группы» появится новая запись.

Рис. 115 Окно свойств группы Операторов РЦ

5.6.2. Редактирование свойств группы

Для просмотра или редактирования свойств группы Операторов РЦ необходимо в окне папки «Группы» выделить курсором нужную запись, нажать кнопку «Подробнее...» и в открывшемся окне свойств группы (см. Рис. 115) отредактировать необходимые значения.

Следует иметь в виду, что если установленное значение поля «Ограничение на выпуск сертификатов» будет меньше или равно количеству уже выпущенных сертификатов, попытка выпуска новых сертификатов любым из Операторов данной группы будет блокироваться.

5.6.3. Удаление группы

Для того чтобы удалить группу Операторов РЦ, необходимо в окне папки «Группы» выделить курсором соответствующую запись и нажать кнопку «Удалить...».

Запись не может быть удалена, если Операторами данной группы выпущен хотя бы один сертификат.

6. ВЗАИМОДЕЙСТВИЕ С ВНЕШНИМИ УЦ

Между различными удостоверяющими центрами могут устанавливаться доверительные отношения следующих типов:

- иерархические (см. п.6.1) – УЦ верхнего уровня (головной УЦ) является издателем сертификатов для всех УЦ нижнего уровня (подчиненных УЦ), для которых эти сертификаты являются сертификатами авторитета;
- равноправные (см. п.6.2) – каждый УЦ помимо собственного сертификата авторитета является владельцем кросс-сертификатов, число которых равно числу УЦ, с которыми он имеет доверительные отношения.

УЦ «Notary-PRO» позволяет реализовать обе схемы взаимодействия между несколькими удостоверяющими Центрами.

6.1. Иерархические отношения

6.1.1. Формирование запроса на создание сертификата ключа проверки УЦ¹

Запросы на создание сертификата ключа проверки УЦ формируются с целью получения сертификата в другом удостоверяющем центре (при установлении иерархических отношений). Такие запросы не могут быть сертифицированы в локальном УЦ, а могут быть лишь экспортированы (см. п. 3.5.6).

Для формирования запроса Администратору необходимо:

- находясь в папке «Ключи УЦ», нажать кнопку «Создать запрос...»;
- на странице «Уникальное имя» диалогового окна установить атрибуты запрашиваемого имени, пользуясь полями редактирования или кнопкой «Выбрать из списка имен», предназначенной для выбора имени из списка уникальных имен, принадлежащих Администратору УЦ (см. Рис. 116);

The image shows a Windows-style dialog box titled 'Параметры запроса УЦ' (Parameters of the request to the CA). It has two tabs: 'Уникальное имя' (Unique name) and 'Расширения' (Extensions). The 'Уникальное имя' tab is active, showing several text input fields for personal and organizational data. The fields are: 'Полное имя' (Full name) with 'Удостоверяющий Центр' (Certifying Center), 'Организация' (Organization) with 'ЗАО Сигнал-КОМ', 'Подразделение' (Department) which is empty, 'Должность' (Position) with 'Администратор безопасности' (Security Administrator), 'Город/село' (City/village) with 'Москва' (Moscow), 'Область/район' (Region/district) which is empty, 'Страна' (Country) with a dropdown menu showing 'Россия' (Russia) and a small '...' button, and 'Электронная почта' (Email) which is empty. Below these fields is a button labeled 'Выбрать из списка имен' (Select from list of names). At the bottom of the dialog are four buttons: 'Создать' (Create), 'Отменить' (Cancel), 'Применить' (Apply), and 'Справка' (Help).

Рис. 116 Страница «Уникальное имя» окна формирования запроса для ключа УЦ

- на странице «Расширения» диалогового окна задать параметры расширений запрашиваемого сертификата (см. Рис. 117); действия Администратора по настройке расширений подробно описаны в п. 4;

- нажать кнопку «Создать».

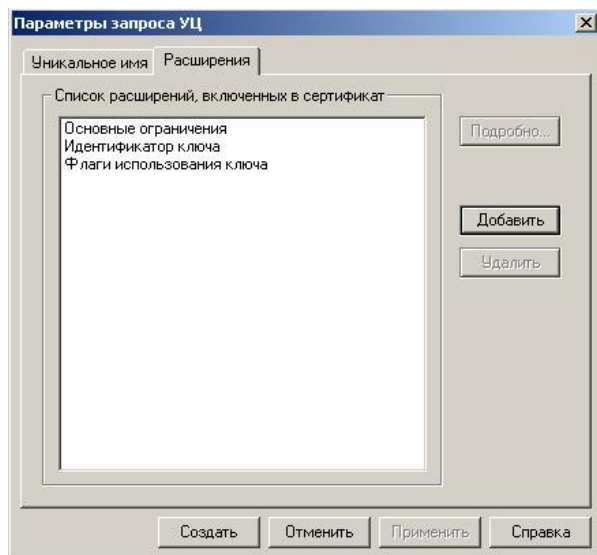


Рис. 117 Страница «Расширения» окна формирования запроса для ключа УЦ

На каждый ключ УЦ может быть выпущено произвольное число запросов.

6.1.2. Импорт сертификата УЦ

При установлении иерархических сертификационных отношений между удостоверяющими центрами ключ УЦ может быть сертифицирован в вышестоящем УЦ. Для этого Администратор УЦ должен создать запрос (см. п.6.1.1), экспортировать его в файл (см. п.3.5.6) и передать в вышестоящий УЦ.

После сертификации запроса в вышестоящем УЦ в базу данных локального УЦ импортируется цепочка сертификатов в следующем порядке:

- сначала - самоподписанный сертификат корневого УЦ;
- затем - сертификаты промежуточных (если таковые имеются) УЦ;
- и в конце – импортируемый сертификат УЦ.

Если импортируемый сертификат не может быть проверен, регистрация такого сертификата будет запрещена.

Для импорта сертификата необходимо:

- в Главное меню программы выбрать пункт «Формирование документов/Импорт сертификата» или в абонентских папках Главной панели выбрать папку «Сертификаты»;
- нажать кнопку «Импорт...» на Панели управления окна данной папки (см. п. 2.2.6);
- в открывшемся окне диалога выбрать файл импортируемого сертификата.

6.2. Кросс-сертификация

Функции выпуска кросс-сертификатов и запросов для кросс-сертификации доступны через папку «Кросс-сертификация» Главной Панели (см. Рис. 118).

Папка «Кросс-сертификация» содержит следующие разделы:

- «Субъекты кросс-сертификации» - раскрывает список абонентов, который дополняется новым элементом после регистрации запроса на выпуск кросс-сертификата; данный раздел является полным аналогом в части управления (см. п. 2.2.4) и набора свойств (см. п. 3.4.2), что и раздел «Абоненты» абонентских папок;
- «Запросы для кросс-сертификации» - показывает список запросов на выпуск кросс-сертификатов; в список включены как запросы, сформированные данным УЦ, так и запросы от других УЦ, зарегистрированные данным УЦ; данный раздел является полным аналогом в части управления (см. п. 2.2.5) и набора свойств (см. п. 3.5.2), что и раздел «Запросы» абонентских папок;
- «Кросс-сертификаты» - аналог раздела «Сертификаты» абонентских папок, раскрывает список кросс-сертификатов, выпущенных данным УЦ; данный раздел является полным аналогом в части управления (см. п. 2.2.6) и набора свойств (см. п. 3.6.2), что и раздел «Сертификаты» абонентских папок.

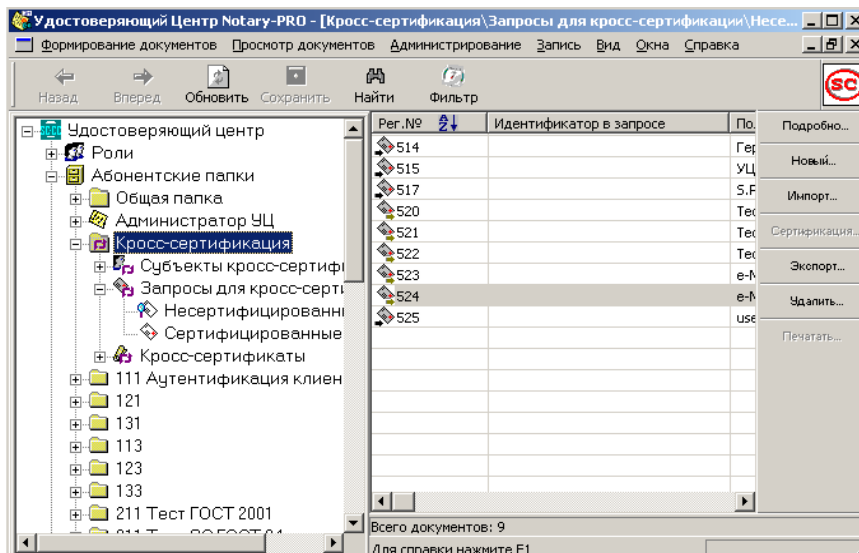


Рис. 118 Папка «Кросс-сертификация» Главной Панели

6.2.1. Формирование и экспорт запроса на кросс-сертификат

Для выпуска запроса на кросс-сертификат Администратор должен открыть раздел «Кросс-сертификация \ «Запросы для кросс-сертификации» и нажать кнопку «Новый...» на Панели управления. В появившемся окне диалога «Выбор сертификата УЦ» (см. Рис. 119) Администратор должен выделить один из сертификатов УЦ и нажать кнопку «Выбрать». Атрибуты указанного сертификата (уникальное имя и необходимый набор расширений) будут включены в формируемый запрос. После выбора сертификата УЦ возможна корректировка длины сертификационного пути (см. Рис. 120).

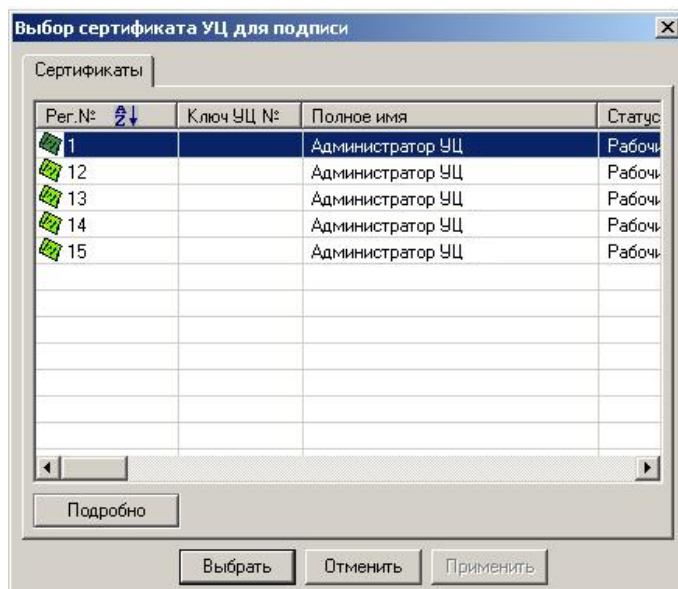


Рис. 119 Выбор сертификата УЦ для выпуска запроса на кросс-сертификацию

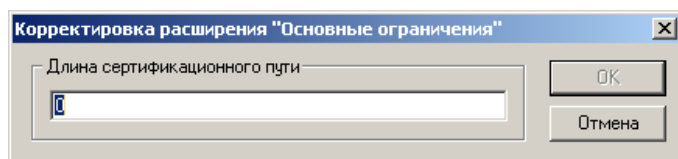



Рис. 120 Диалог корректировки длины сертификационного пути расширения «Основные ограничения».

Если корректировка длины сертификационного пути не требуется, в диалоговом окне «Корректировка расширения «Основные ограничения»» необходимо нажать кнопку «Отмена». Кнопка «ОК» становится активной только после ввода нового значения в поле «Длина сертификационного пути».

Свойства сформированного запроса на кросс-сертификат можно контролировать при помощи многостраничного диалога свойств, представленного на Рис. 121.

Созданный запрос на кросс-сертификат помечается значком . Ссылка на сертификат УЦ, на основе которого создан запрос на кросс-сертификат, отображается на странице «Параметры» окна свойств запроса в поле «Исходный сертификат УЦ» (см. Рис. 121).

Экспорт запроса на кросс-сертификацию выполняется с помощью нажатия кнопки «Экспорт» панели управления (см. Рис. 118). В появившемся диалоге необходимо выбрать имя файла для сохранения запроса.

Проверенный, кросс, исходящий

Параметры		Запрашиваемое имя		Абонент		Текст		Заметки	
Регистрация									
Дата		12.11.2014 16:15:02		Оператор №:					
Способ доставки		Не определен				...			
Тип PKCS#10		Тип запрашиваемого сертификата							
Самоподписан Да		Проверен сертификатом №:							
Алгоритм открытого ключа		ГОСТ Р 34.10-2012 (256 бит)		Исходный сертификат УЦ					
Длина ключа		256		223		...			
Сертификация									
Номер сертификата				Оператор №:					
				
Свертка MD5		59fc:38:46:e3:31:3b:a0f5:16:33:cc:19:67:c9:55							
Свертка SHA-1		ab:96:b2:7b:4d:2f:8e:89:66:f6:cd:5c:46:1c:66:b9:ed:ba:10:81							
Свертка ГОСТ		79:a4:2b:9a:06:61:7:89:24:f7:58:c5:2e:0f:11:ca:93:1b:ca:9d:88:82:e9:31:b8:b0:9c:ed:b4:f0:39:66							

Рис. 121 Свойства запроса на кросс-сертификацию

6.2.2. Импорт запроса и выпуск кросс-сертификата

Для регистрации запроса, полученного из другого УЦ и предназначенного для кросс-сертификации, Администратор должен открыть раздел «Запросы для кросс-сертификации» Главной Панели и выполнить команду «Импорт...».

После выбора файла запроса, в появившемся окне диалога «Импорт запросов из файловой системы» (см. Рис. 122), необходимо выполнить следующие настройки:

- установить флажок «Доставлены персонально»;
- установить флажок «Регистрировать нового абонента, если не найден по атрибутам в запросе».

Импорт запросов из файловой системы

Всего файлов: 1 ☒ Доставлены персонально

Список файлов: C:\request.pem

☐ Привязывать запросы к абоненту №: Подробно...

☐ Привязывать запросы к абоненту, найденному по атрибутам в запросе

☒ Регистрировать нового абонента, если не найден по атрибутам запроса


☐ Удалять файлы запросов после обработки

☐ Перемещать файлы обработанных запросов в каталог: C:\TEMP

Файлы, при обработке которых произошла ошибка, помещать в каталог: C:\TEMP1

Выполнить Отменить

Рис. 122 Окно диалога «Импорт запросов из файловой системы»

При нажатии на кнопку «Выполнить», в разделе «Запросы для кросс-сертификации /Несертифицированные» появится новая запись, помеченная значком .

Для выпуска кросс-сертификата Администратор должен, находясь в разделе «Запросы для кросс-сертификации» Главной Панели, выполнить команду «Сертификация...».

Основные свойства выпускаемого кросс-сертификата задаются на странице «Параметры сертификата» многостраничного диалога «Сертификация запроса» (см. Рис. 123).

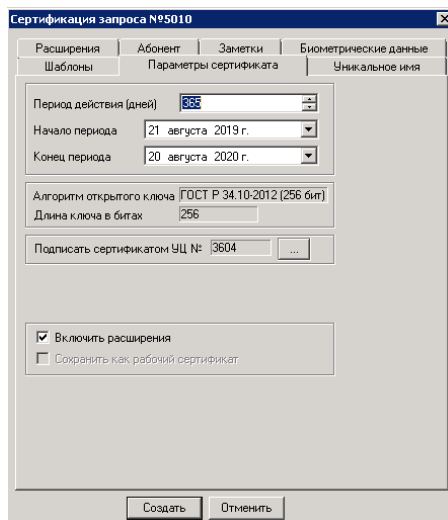



Рис. 123 Диалог «Сертификация запроса»

При нажатии на кнопку «Создать» в разделе «Кросс-сертификаты/Действительные» будет зарегистрирована новая запись, помеченная значком .

Экспорт кросс-сертификата выполняется с помощью нажатия кнопки «Экспорт» панели управления (см. Рис. 118). В появившемся диалоге необходимо выбрать имя файла для сохранения сертификата.

7. СОЗДАНИЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА

В ПАК УЦ «Notary-PRO 2.8» реализована возможность создания и выдачи из готовления квалифицированных сертификатов ключа проверки электронной подписи (далее – квалифицированные сертификаты) в соответствии с положениями Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи» [1] и «Требованиями к форме квалифицированного сертификата ключа проверки электронной подписи», утвержденными приказом ФСБ России от 27.12.2011 № 795 [2].

При установке программного обеспечения УЦ «Notary-PRO 2.8», предназначенного для создания и выдачи квалифицированных сертификатов ключей проверки ЭП, должен быть задан режим «Аккредитованный УЦ» (см. п. **Ошибка! Источник ссылки не найден.**).

Примечание [t3]:

Удостоверяющий центр «Notary-PRO» в режиме функционирования «Аккредитованный УЦ» поддерживает следующие криптографические алгоритмы:

- ГОСТ Р 34.10-2012 - в соответствии с [7];
- ГОСТ Р 34.11-2012 - в соответствии с [8].

Атрибуты квалифицированного сертификата ключа проверки ЭП, созданные в режиме «Аккредитованный УЦ», соответствуют требованиям приказа ФСБ России от 27.12.2011 № 795 и положениям «Извещения об использовании стандартных атрибутов имени commonName (общее имя), surname (фамилия), givenName (приобретенное имя) и дополнительных атрибутов имени поля «subject» в структуре квалифицированного сертификата ключа проверки электронной подписи» от 13.03.2013

Внимание! Аккредитованный удостоверяющий центр создаёт только квалифицированные сертификаты ключей проверки электронной подписи.

7.1. Шаблоны администрирования для квалифицированных сертификатов

Для выпуска квалифицированных сертификатов в УЦ «Notary-PRO» предусмотрены специальные предустановленные шаблоны администрирования (для Администратора УЦ и для абонентов) с пометкой «квалифицированный сертификат», которые могут быть сдублированы, но не могут быть удалены (см. Рис. 124).

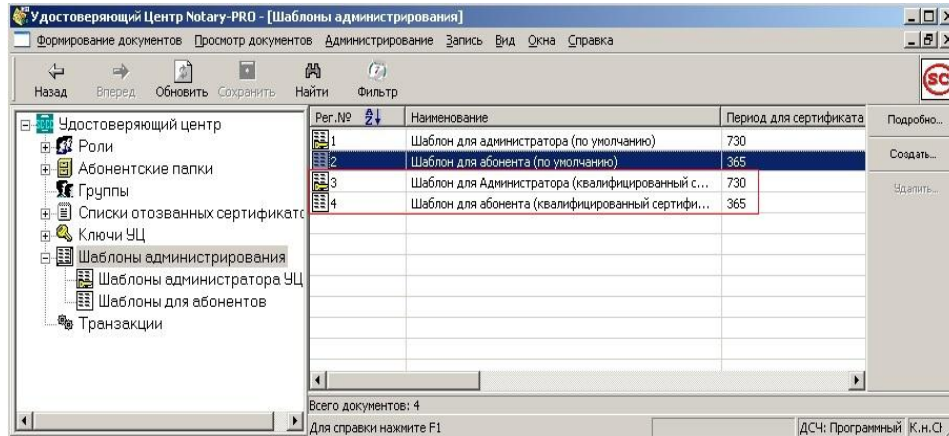


Рис. 124 Шаблоны администрирования для квалифицированных сертификатов
(выделены рамкой)

Указанные специальные шаблоны обеспечивают формирование необходимых расширений квалифицированного сертификата в момент его выпуска в соответствии со списком, приведенным на Рис. 125.

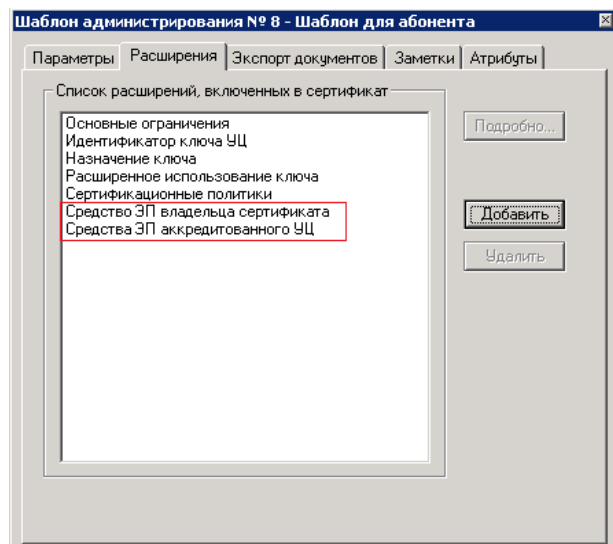


Рис. 125 Расширения для квалифицированного сертификата

Текстовые данные для заполнения расширения «Средства ЭП аккредитованного УЦ» квалифицированного сертификата (IssuerSignTool в соответствии с [2]) копируются из полей формы реквизитов, расположенных на странице «Средства ЭП аккредитованного УЦ» окна «Параметры по умолчанию» (см. Рис. 126).

Параметры по умолчанию

Списки отозванных сертификатов	Криптография	Главный ключ	Печать
Источники данных	Трассировочный журнал	Тип сертификата	Документы
Блокирование GUI	Работа с большими БД	Адреса СОС	
Отображение данных	Сертификаты	Отправка уведомлений	
Биометрия	Средства ЭП аккредитованного УЦ		

☒ Аккредитованный УЦ

Наименование средства ЭП в составе УЦ
СКЗИ "CADB 2.1"

Наименование средства УЦ
ПАК УЦ "Notary-PRO" v.2.8

Реквизиты документа ФСБ России о подтверждении соответствия средства ЭП
Заключение № 149/3/2/2-1868 от 14.08.2019

Реквизиты документа ФСБ России о подтверждении соответствия средства УЦ
Заключение № 149/7/1/1-1-1-1 от 14.08.2019

OK Отменить Применить

Рис. 126 Реквизиты для формирования расширения «Средства ЭП аккредитованного УЦ»

При формировании расширения «Средство ЭП владельца сертификата» (subjectSignTool в соответствии с [2]) необходимые текстовые данные копируются непосредственно из запроса на квалифицированный сертификат.

В режиме автоматической обработки и сертификации запросов, в случае отсутствия в запросе на квалифицированный сертификат расширения subjectSignTool сертификация запроса блокируется, а в случае отсутствия указания на класс средств ЭП в certificatePolicies, автоматически вставляется значение KC1.

При ручной обработке запросов, в случае отсутствия в запросе на квалифицированный сертификат расширения subjectSignTool выдается диалоговое окно, позволяющее Администратору УЦ задать нужное значение subjectSignTool, а в случае отсутствия указания на класс средств ЭП в certificatePolicies, по умолчанию вставляется значение KC1, но на этапе сертификации Администратором УЦ может быть установлено необходимое значение класса защиты через шаблон администрирования для квалифицированных сертификатов.

7.2. Создание квалифицированного сертификата в ручном режиме

Ручной режим обработки запроса на изготовление квалифицированного сертификата позволяет Администратору УЦ контролировать все этапы процесса сертификации и параметры квалифицированного сертификата, удалять ошибочные сертификаты и экспортировать успешно изготовленные.

Администратор УЦ имеет возможность вносить любые дополнительные критические параметры самостоятельно, а также задерживать выпуск квалифицированного сертификата до завершения процедуры сверки его параметров с данными из подтверждающих документов.

7.3. Импорт запроса на создание сертификата

Импорт файла запроса сертификата осуществляется с помощью диалогов:

- «Выбор файла запроса» (см. Рис. 127)
- «Импорт запросов из файловой системы» с контролем уникального имени (см. Рис. 128).

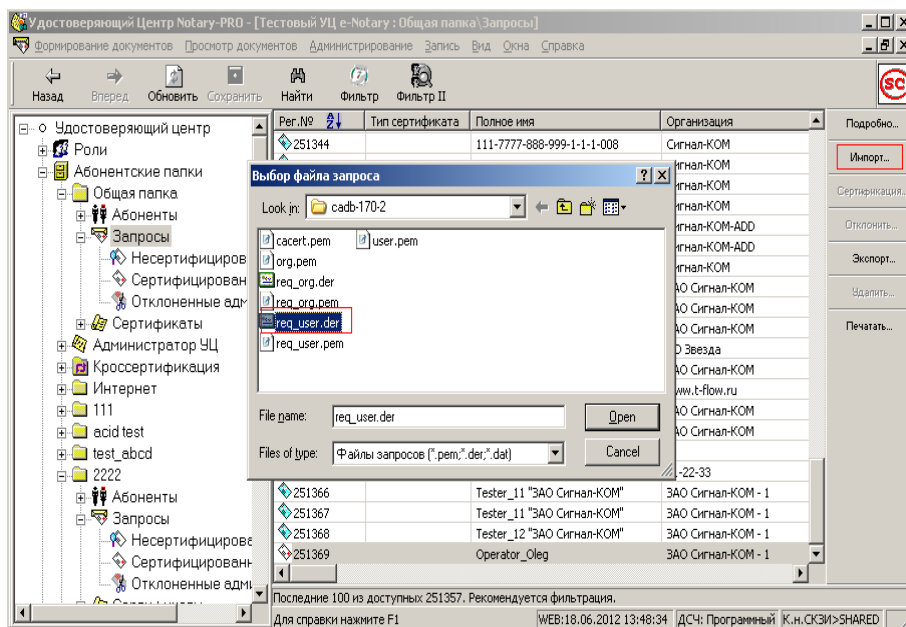


Рис. 127 Импорт файла запроса на сертификацию

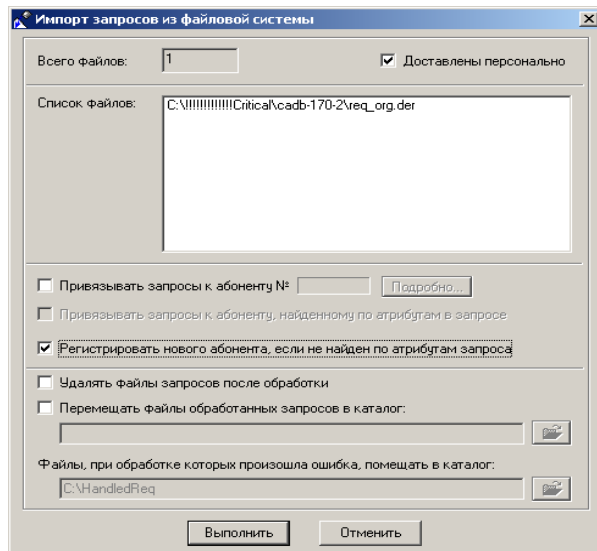


Рис. 128 Диалог импорта запроса с контролем уникального имени

Импорт запроса завершается созданием в БД удостоверяющего центра учетной записи запроса на сертификат.

7.4. Контроль атрибутов имени и расширений запроса

Каждая учетная запись запроса имеет диалог свойств, включающий страницы «Запрашиваемое имя» и «Абонент». Администратор УЦ может контролировать и изменять атрибуты уникального имени запроса через параметры страницы «Абонент» диалога свойств запроса (см. Рис. 129).

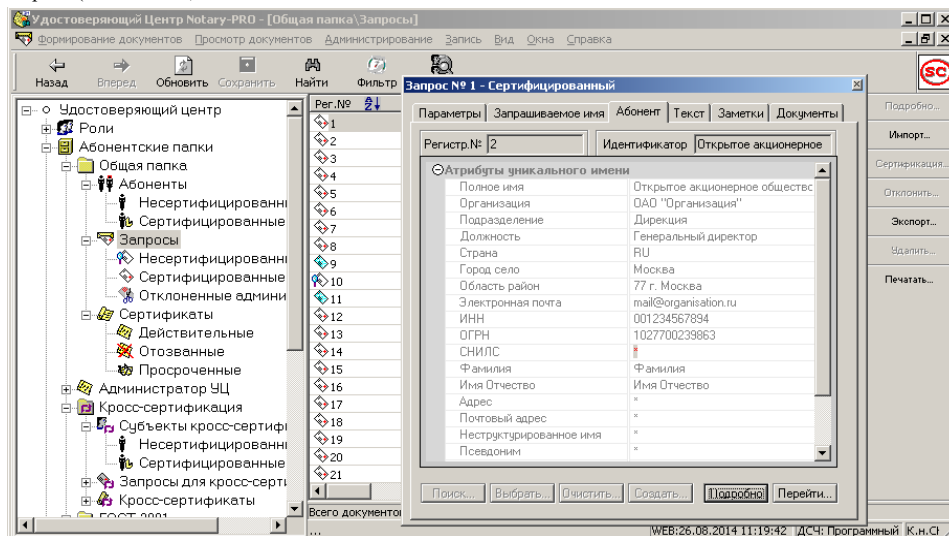


Рис. 129 Учетная запись импортированного запроса и атрибуты уникального имени

В соответствии с требованиями [1, 2, 16, 17] Администратор аккредитованного УЦ должен придерживаться следующих правил назначения атрибутов уникального имени в квалифицированных сертификатах юридических лиц (ЮЛ), физических лиц (ФЛ) и индивидуальных предпринимателей (ИП):

Таблица 5

Имя атрибута	Тип сертификата	Содержание
Страна (Country Name)	ЮЛ	адрес места регистрации юридического лица в соответствии с учредительными документами;
Область/район (State or Province Name)	ФЛ	адрес места регистрации физического лица (название улицы и номер дома)
Город/село (Locality Name)	ИП	указываются по желанию владельца сертификата)
Адрес (StreetAddress)		
Организация (OrganizationName)	ЮЛ	полное или сокращенное наименование юридического лица
Подразделение (OrganizationUnit Name)	ЮЛ	наименование подразделения, в котором работает уполномоченный представитель юридического лица (указывается по желанию)
Должность (Title)	ЮЛ	должность уполномоченного представителя юридического лица
Общее имя (Common Name)	ФЛ	фамилия, имя и отчество (если имеется) физического лица – владельца сертификата, как они указаны в документе, удостоверяющем личность
	ИП	полное наименование юридического лица, как оно указано в уставных документах юридического лица
Фамилия (Surname)	ФЛ	фамилия владельца сертификата, как она указана в документе, удостоверяющем личность (опциональный атрибут)
	ИП	фамилия уполномоченного представителя, действующего от имени юридического лица на основании учредительных документов юридического лица или доверенности
Приобретённое имя (Given Name)	ФЛ	имя и отчество (если имеется) владельца сертификата, как они указаны в документе, удостоверяющем личность (опциональный атрибут)
	ИП	имя и отчество (если имеется) уполномоченного представителя, действующего от имени юридического лица на основании учредительных документов юридического лица или доверенности
ИНН (INN)	ЮЛ	индивидуальный номер налогоплательщика – юридического лица; значение атрибута должно содержать 2 лидирующих нуля перед ИНН юридического лица
	ФЛ	индивидуальный номер налогоплательщика – физического лица
ОГРН (OGRN)	ЮЛ	основной государственный регистрационный номер юридического лица
ОГРНИП (OGRNIP)	ИП	основной государственный регистрационный номер индивидуального предпринимателя (в настоящее время не используется)
СНИЛС (SNILS)	ЮЛ	страховой номер индивидуального лицевого счёта государственного пенсионного страхования для физического лица или уполномоченного представителя, действующего от имени юридического лица
	ФЛ	
	ИП	

Запрос на изготовление квалифицированного сертификата должен содержать расширение «Средство ЭП владельца сертификата» и идентификаторы сертификационной политики, определяющие класс ЭП в соответствии с [2]. Содержимое расширений и сертификационных политик запроса на квалифицированный сертификат можно контролировать с помощью страницы «Текст» диалога свойств запроса по каждой учетной записи (см. Рис. 130).

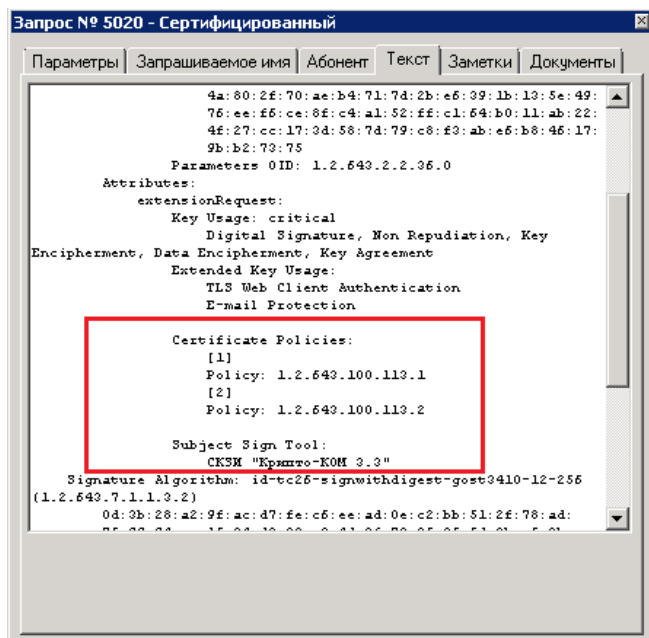


Рис. 130 Контроль расширения «Средство ЭП владельца сертификата» и элементов политики

7.5. Выбор шаблона сертификации

Для изготовления квалифицированного сертификата необходимо указать запрос и выбрать «Шаблон для абонента (квалифицированный сертификат)» из общего списка шаблонов (см. Рис. 131), который становится доступным при нажатии кнопки «Сертификация» на боковой кнопочной панели окна программы.

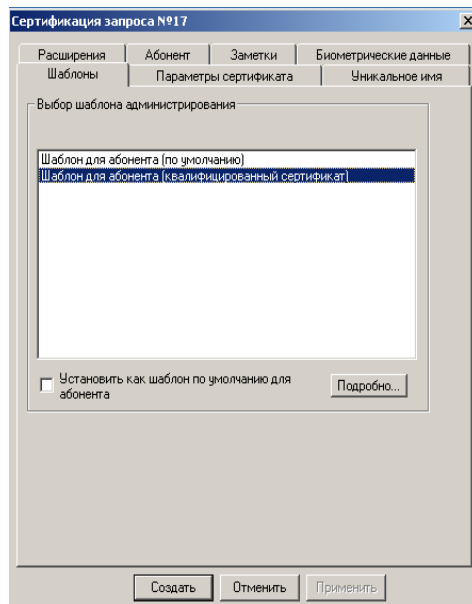


Рис. 131 Выбор шаблона абонента для создания квалифицированного сертификата

На странице «Расширения» при правильном выборе шаблона администрирования должны присутствовать записи «Средство ЭП владельца сертификата» и «Средства ЭП аккредитованного УЦ» (см. Рис. 132). Только в этом случае в сертификат будут включены все необходимые расширения и элементы политик квалифицированного сертификата.

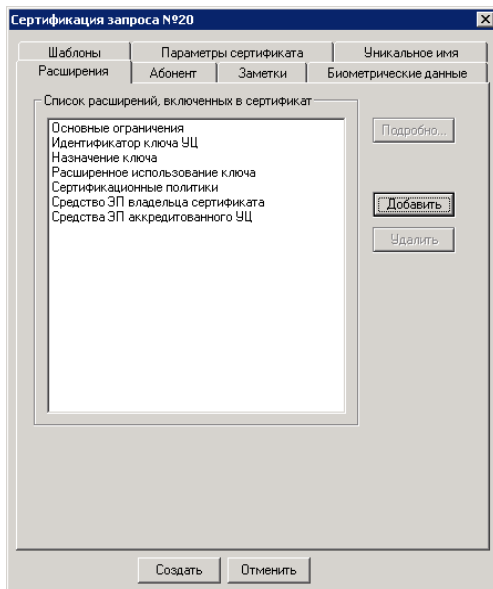


Рис. 132 Расширения квалифицированного сертификата

После завершения диалога при нажатии кнопки «Создать» должна появиться новая учетная запись сертификата.

7.6. Контроль атрибутов имени и расширений квалифицированного сертификата

Администратор УЦ может контролировать содержимое выпущенных квалифицированных сертификатов при помощи диалога свойств учетной записи раздела «Сертификаты». Список расширений сертификата доступен на странице «Расширения» данного диалога (см. Рис. 133).

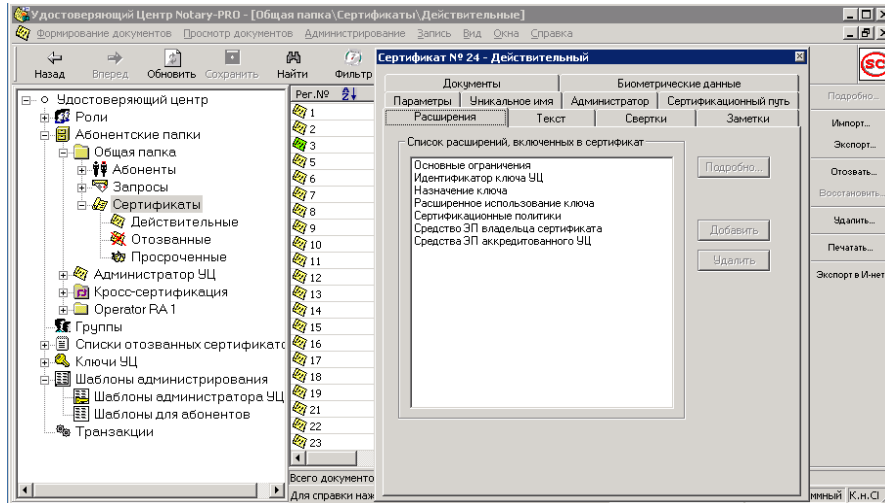


Рис. 133 Список расширений, включенных в квалифицированный сертификат

Страница «Текст» содержит представление квалифицированного сертификата в текстовом виде (см. пример на Рис. 134).

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      01:a8:02:11:56:01:0e:01:42
    Signature Algorithm: id-tc26-signwithdigest-gost3410-12-256 (1.2.643.7.1.1.3.2)
    Issuer: C=RU, SP=77 р. Москва, L=Москва, O="ЗАО "Сигнал-КОМ"", CN=Notary-PRO
    Certification Authority GOST-2012 256 bit, Email=ca@notary-pro.ru
    Validity
      Not Before: Aug 21 14:48:03 2019 GMT
      Not After : Aug 20 14:48:03 2020 GMT
    Subject: INN=007726728755, C=RU, CN=Сертификат для ЭДО, SNILS=07557100665
    Subject Public Key Info:
      Public Key Algorithm: id-tc26-gost3410-12-256 (1.2.643.7.1.1.1.1)
      Public Key:
        pub:
          aa:2d:4a:da:b5:19:14:76:e0:7d:88:40:52:b9:9e:
          4a:80:2f:70:ae:b4:71:7d:2b:e6:39:1b:13:5e:49:
          76:ee:f6:ce:8f:c4:a1:52:ff:c1:64:b0:11:ab:22:
          4f:27:cc:17:3d:58:7d:79:c8:f3:ab:e6:b8:46:17:
          9b:b2:73:75
          Parameters OID: 1.2.643.2.2.36.0
    X509v3 extensions:
      Basic Constraints: critical
      CA:FALSE
      Authority Key Identifier:
        keyid:97:2e:70:4a:92:76:82:dc:95:6a:c3:ad:6c:08:30:3a:0c:96:2d:38
        DirName:C=RU, SP=77 р. Москва, L=Москва, O="ЗАО "Сигнал-КОМ"", CN=Notary-PRO
      Certification Authority GOST-2012 256 bit, Email=ca@notary-pro.ru
      serial:01:dd:01:01:01:0e:01:01
      CRL Distribution Points:
        Distribution Point:
          Full Name:
            URI: http://www.e-notary.ru/crl_test/ca_3604.crl
      PKIX Authority Info Access:
        Access Method: OCSP
        Access Location:
          URI: http://ocsptest.e-notary.ru
      Subject Sign Tool:
        СКЗИ "Крипто-КОМ 3.3"
      Certificate Policies:
        [1]
        Policy: 1.2.643.100.113.1
        [2]
        Policy: 1.2.643.100.113.2
```

```

Issuer Sign Tool:
  signTool: CKЗИ "CADB 2.1"
  cATool: ПАК УЦ "Notary-PRO" v.2.8
  signToolCert: Заключение № 149/3/2/2-1868 от 14.08.2019
  cAToolCert: Заключение № 149/7/1/1-??? от ???.2019

Extended Key Usage:
  TLS Web Client Authentication
  E-mail Protection

Key Usage: critical
  Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment,
Key Agreement
Signature Algorithm: id-tc26-signwithdigest-gost3410-12-256 (1.2.643.7.1.1.3.2)
b6:1c:47:42:00:13:13:f6:79:41:6b:26:48:e8:92:ac:7a:51:
56:cd:c3:04:7a:b9:61:15:36:f7:05:1e:6f:0a:3b:cf:2c:78:
c0:af:2a:49:ac:0f:e4:d2:ee:03:51:c1:55:c4:93:dc:10:1a:
c3:cd:7d:34:c6:21:c1:b4:52:2a
  
```

Рис. 134 Фрагмент текстового представления квалифицированного сертификата

7.7. Экспорт сертификата

Квалифицированный сертификат, зарегистрированный в БД УЦ «Notary-PRO» после тщательной проверки и верификации документов владельца подписи, может быть передан владельцу только после операции экспорта в файл или в сетевой справочник сертификатов (см. Рис. 135).

Следует иметь ввиду, что учетная запись сертификата после его экспорта не может быть удалена из БД УЦ. И, напротив, учетная запись еще не экспортированного сертификата может быть удалена в случае обнаружения неточностей или ошибок.

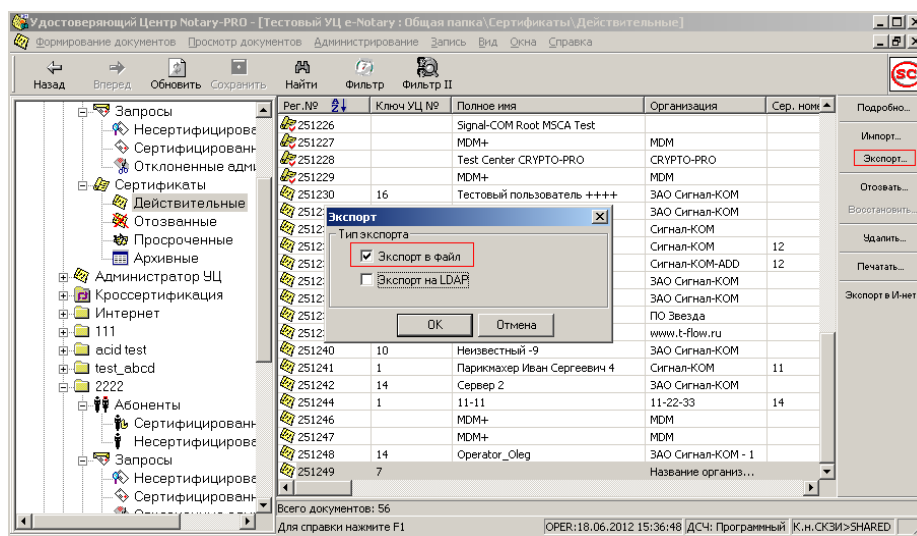


Рис. 135 Экспорт квалифицированного сертификата проверки подписи в файл

ПРИЛОЖЕНИЕ 1. ОПТИМИЗАЦИЯ РАБОТЫ С БД БОЛЬШОГО ОБЪЁМА

Настоящее Приложение описывает необходимые действия Администратора удостоверяющего центра в случае, если количество записей превышает значение 100 000 зарегистрированных уникальных имен, а общий размер БД УЦ превышает 4ГБ. Достижение порогового значения размера характеризуется резким падением производительности и увеличением времени отклика системы при выполнении ряда операций администрирования УЦ. При этих условиях рекомендуется использовать режимы ограничения размера выборок и расширенной фильтрации, которые доступны в версии АРМ Администратора УЦ 2.6.8.x и более поздних.

Для уменьшения времени реакции системы при работе с БД большого размера Администратор УЦ должен отметить визуальный элемент «Ограничивать количество записей в выборках» (см. Рис. 136). При этом появится возможность выбора опций «отображать первые» или «отображать последние» N записей, где число N принимает значения от 100 до 5000. Значение по умолчанию для числа записей в выборках – 100, что соответствует самому малому времени реакции при выборе значений из диапазона. Опция «отображать последние» всегда обеспечивает доступ Администратора к подмножеству всех последних записей.

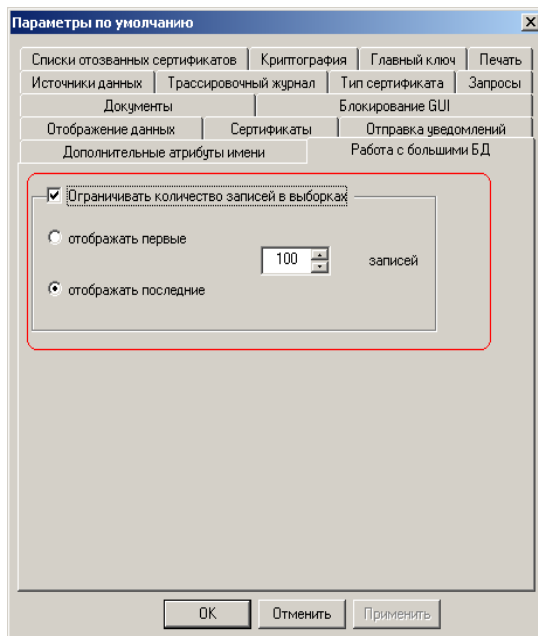


Рис. 136 Установка режима ограничения размера выборки

Снятие отметки с пункта «Ограничивать количество записей в выборках» может быть полезным и при малом количестве записей в БД УЦ.

Установка режима ограничения размера выборки влияет на отображение данных в следующих типах представлений (см. Таблица 6):

Таблица 6 Действие ограничения на размер выборки для различных представлений данных

Тип представления	Степень влияния	Комментарий
Абоненты	Ограничение, действующее для всех папок	Актуально для подтипов: - все, - несертифицированные, - сертифицированные
Запросы	Ограничение, действующее для всех папок	Актуально для подтипов: - все, - несертифицированные, - сертифицированные, - отклоненные Администратором.
Сертификаты	Ограничение, действующее для всех папок	Актуально для подтипов: - все, - действительные, - отозванные, - просроченные
Списки отозванных сертификатов	Ограничение	Актуально для подтипов: - все, - действительные
Ключи	Ограничение	
Шаблоны администрирования	Ограничение	Актуально для подтипов: - все, - для Администратора, - для пользователей
Журнал событий	Ограничение	
Транзакции	Ограничение	
Объекты-выборки	Ограничение, действующее для всех папок	
Объекты-ссылки	Без ограничения	

Внимание! Ограничение действует как дополнительный фильтр, критерием отбора которого является число записей от начала выборки или от конца. При этом некоторые записи могут оказаться «за пределами» выборки. Об этом сигнализирует предупреждение-подсказка «Действует ограничение по числу записей! Используйте фильтрацию» (см. Рис. 137). Информация в нижней части окна представления «Последние (первые) N из доступных M», позволяет судить о полноте полученного подмножества по отношению к множеству отобранных записей (см. Рис. 138).

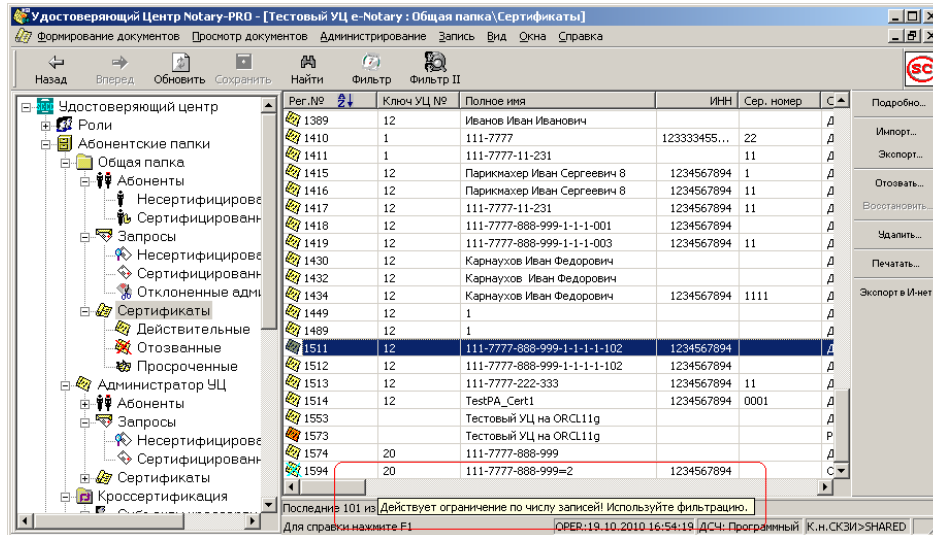


Рис. 137 Всплывающее предупреждение о действии ограничения на размер выборки

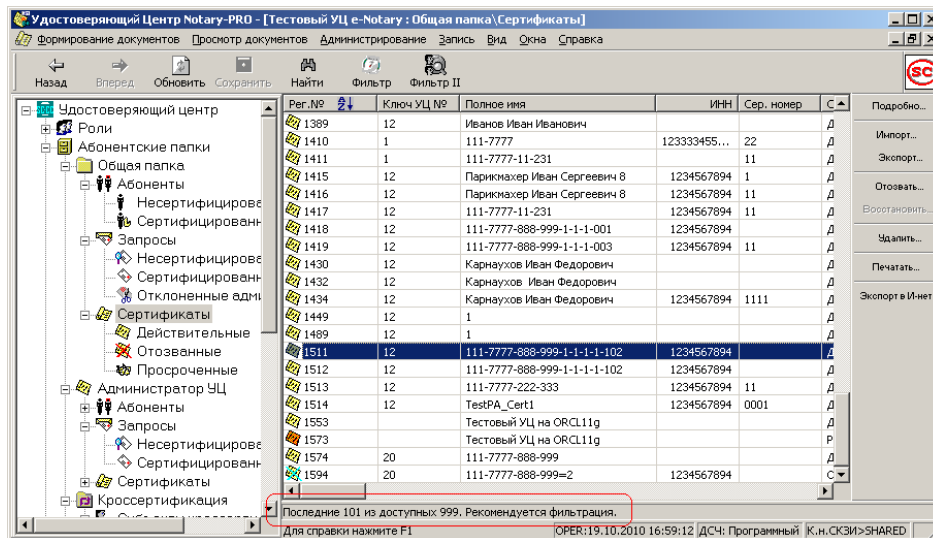


Рис. 138 Информационная строка об ограничении числа записей в представлении данных

При работе с представлениями данных, которые организованы по принципу ограничения числа записей, предусмотрен комплексный фильтр по атрибутам уникального имени, который может комбинироваться с фильтром по дате регистрации объектов (учетная запись абонента, запрос, сертификат, список отмены, событие из журнала событий).

Комплексный фильтр по атрибутам уникального имени активируется при помощи кнопки на главной панели с названием «Фильтр II» (см. Рис. 139).

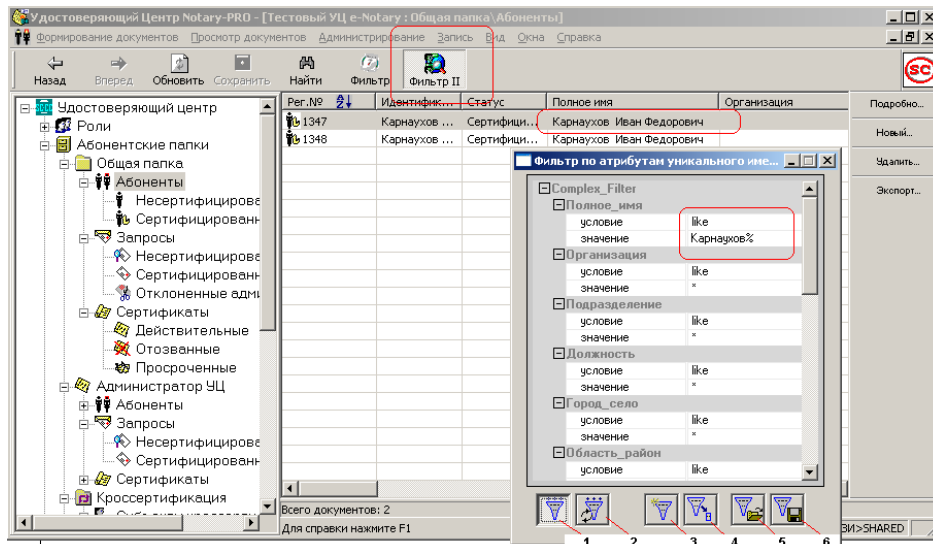


Рис. 139 Работа с комплексным фильтром по атрибутам уникального имени. Цифрами обозначены кнопки фильтра: 1- активировать; 2-активировать обновленное условие; 3- создать новый фильтр; 4- компактная форма фильтра; 5-загрузить условие, сохраненное ранее; 6- сохранить условие.

Фильтр, представляет собой немодальное диалоговое окно с настраиваемыми размерами. Положение и содержимое окна фильтра сохраняется между сессиями. Новый фильтр вызывается через нажатие кнопки 3. Далее вводится необходимое число атрибутов, включающих условие сравнение и маску. Фильтр активируется нажатием кнопки 1. Условие фильтрации может быть изменено. Измененное условие активируется нажатием кнопки 2. Кнопка 4 делает представление фильтра компактным (см. Рис. 140). Нажатием кнопок 5 и 6 выполняются операции сохранения и загрузки. При эффективной фильтрации число записей в представлении сокращается, что ускоряет их анализ.



Рис. 140 Компактная форма фильтра

При снятии фильтра возможна ситуация, когда отмеченная в представлении запись (на Рис. 141- запись с идентификатором 1347) останется за пределами выборки из-за действия ограничения на ее размер. Об этом сигнализирует сообщение «Запись с идентификатором не может быть показана, так как находится вне границ выборки». Если Администратору важна

текущая запись, то может быть создан объект-ссылка, который представляет собой выборку, содержащую только эту запись. Для этого на вопрос «Создать ссылку в отдельном окне ?» необходимо ответить утвердительно.

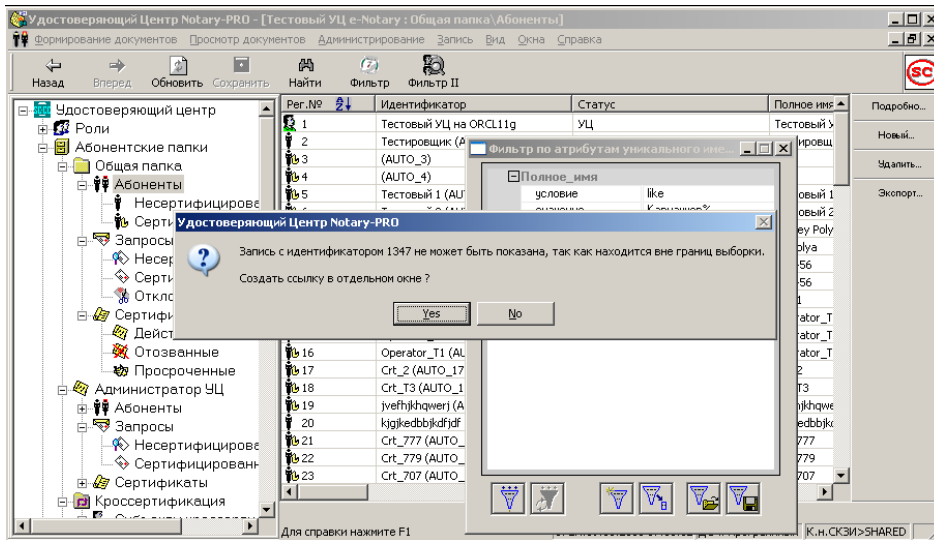


Рис. 141 Создание объекта-ссылки

После завершения операции создается новая ссылка, которая размещается в соответствующей родительской папке (см. Рис. 142). Каждая ссылка имеет уникальный идентификатор и сохраняется до конца сессии.

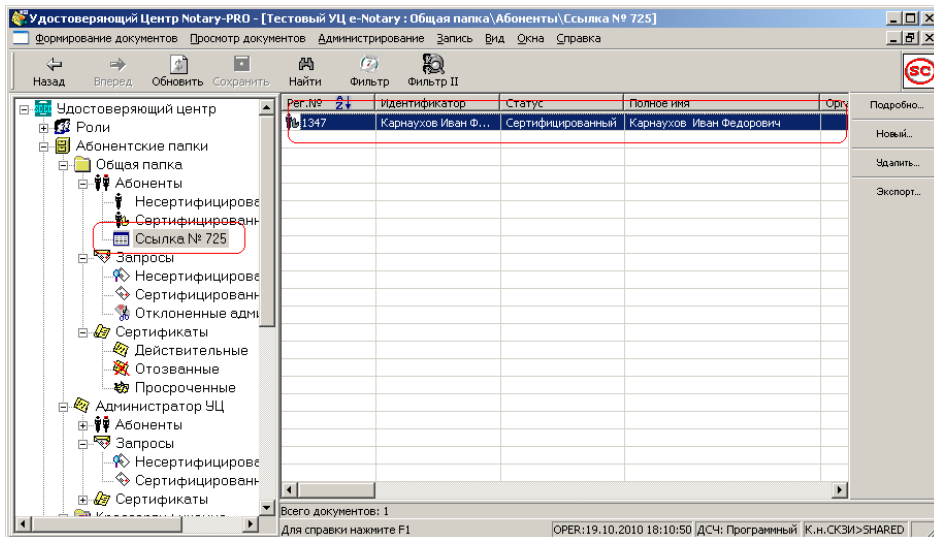


Рис. 142 Отображение объекта-ссылки в главной панели

Комбинированный фильтр по дате регистрации объекта и по атрибутам уникального имени позволяет еще в большей степени упростить процедуру поиска. На Рис. 143 показана установка комбинированного фильтра.

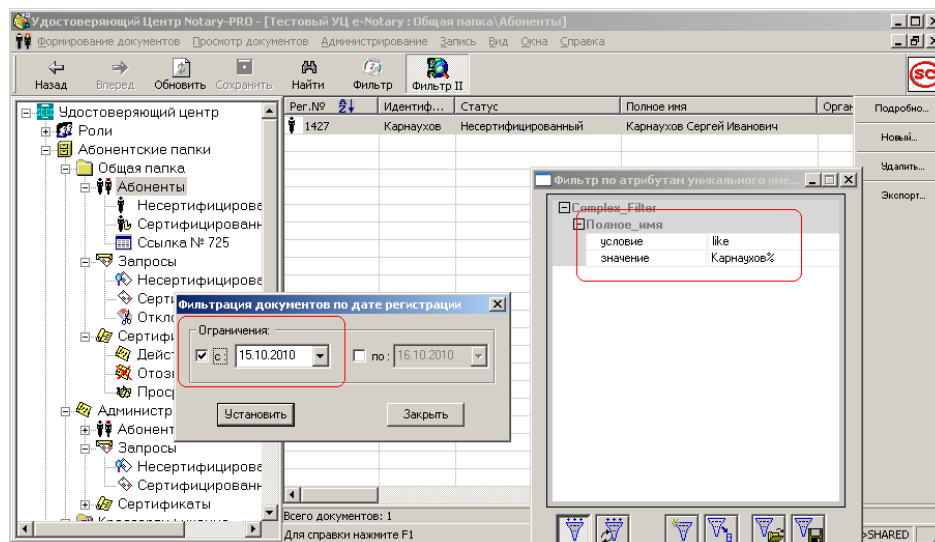


Рис. 143 Установка комбинированного фильтра по дате регистрации и по атрибутам уникального имени

Фильтр по дате и комплексный фильтр по атрибуту уникального имени оказывают различное действие в зависимости от представлений (см. Таблица 7).

Таблица 7. Возможность создания комбинированного фильтра: (+) – чувствителен, (-) – безразличен.

Тип представления	Фильтр по атрибуту уникального имени	Фильтр по дате	Комментарий
Абоненты	+	+	Актуально для всех папок
Запросы	+	+	Актуально для всех папок
Сертификаты	+	+	Актуально для всех папок
Списки отозванных сертификатов	-	+	
Ключи	-	-	
Шаблоны администрирования	-	-	
Журнал событий	-	+	
Транзакции	-	+	
Объекты-выборки	-	+	Актуально для всех папок
Объекты-ссылки	-	-	Актуально для всех папок

Установка фильтра по дате для журнала событий (см. Рис. 144) позволяет упростить его анализ, особенно в том случае, когда журнал не очищается.

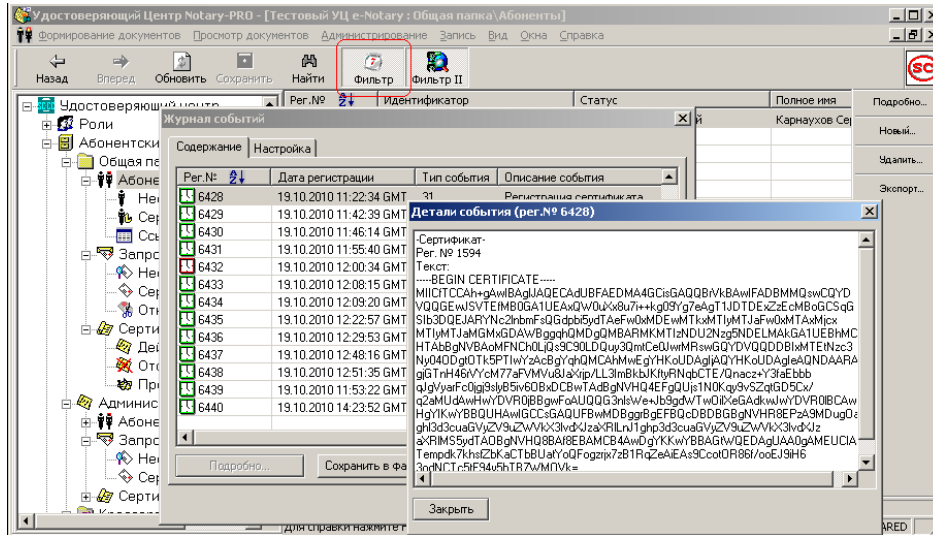


Рис. 144 Фильтрация журнала событий по времени

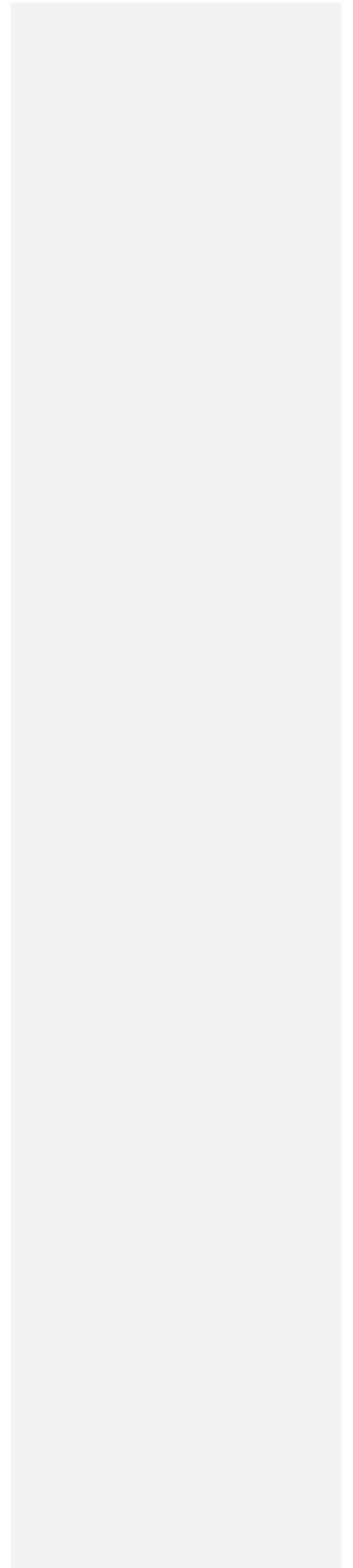
Эффективное использование ограничений и фильтров базируется на анализе достаточности ресурсов SQL – сервера (MSSQL Server 2000/2005/2008, Oracle 9.2/10g/11g). Для оценки достаточности ресурсов Oracle следует изучить статистику выполнения запроса:

```
DECLARE
MAINTABLE VARCHAR2(200);
KEY_FIELD VARCHAR2(200);
ORDER_FIELD VARCHAR2(200);
SQL_CLAUSE VARCHAR2(200);
USE_DESC NUMBER;
ROWS_NUMBER NUMBER;
BEGIN
MAINTABLE := 'Subscribers';
KEY_FIELD := 'SUB_RecID';
ORDER_FIELD := 'UNI_FullName';
SQL_CLAUSE := 'FROM Subscribers, VW_UniqueNames, Countries, TreeNodes WHERE
SUB_RecID = UNI_SUB_RecID (+) AND UNI_IsBase IS NOT NULL AND UNI_COU_ShortName
= COU_ShortName (+) AND SUB_FOL_NodeID = TRE_NodeID (+)';
USE_DESC := 0;
ROWS_NUMBER := 1000; -- Ограничение на число записей в выборке ...

PROC_GETINDICATORRSET_M(
MAINTABLE => MAINTABLE,
KEY_FIELD => KEY_FIELD,
ORDER_FIELD => ORDER_FIELD,
SQL_CLAUSE => SQL_CLAUSE,
USE_DESC => USE_DESC,
ROWS_NUMBER => ROWS_NUMBER
);
END;
```

134
ШКНР.00054-01 34 01

Если время исполнения приведенного скрипта превышает 1.2 секунды, необходимо расширение ОЗУ на машине, где развернут Oracle.



ПРИЛОЖЕНИЕ 2. АВТОМАТИЗАЦИЯ ПУБЛИКАЦИИ СПИСКА АННУЛИРОВАННЫХ СЕРТИФИКАТОВ

При экспорте списков аннулированных сертификатов (САС) используется модель отображений, которая множеству указанных точек распространения CRL (расширение сертификата CDP¹) ставит в соответствие имя ресурса, обеспечивающего физическое хранение действующего САС - файл, каталог, отдельные поля записей БД. К этим объектам хранения актуальных САС пользователи могут обращаться через файловый интерфейс или с помощью протоколов HTTP, FTP, LDAP и пр.

Следует учитывать, что одна задекларированная точка распространения списка отозванных сертификата (CDP), из соображений надежности доступа, может быть сохранена на нескольких различных физических носителях.

Для описания подобной модели отображений используется список правил, который формируется в определенной последовательности при помощи окна модального диалога «Параметры экспорта Списков Отозванных Сертификатов» (Рис. 146). Активация диалога осуществляется нажатием кнопки «Настроить» на странице «Адреса СОС» в окне настроек УЦ «Параметры по умолчанию» (Рис. 145).

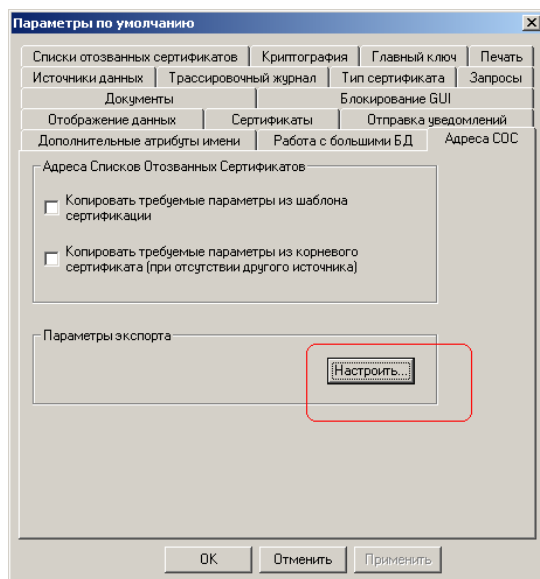


Рис. 145 Страница для настройки параметров расширенного экспорта СОС

Диалог «Параметры экспорта Списков Отозванных Сертификатов» масштабируется для удобства работы с длинными строками. Основным элементом диалога являются карты расширенного экспорта, каждая из которых ассоциируется с определенным типом точки распространения списка отозванных сертификатов (CDP). Для выбора нужной карты необходимо выбрать одну из закладок (см. Рис. 146):

- Точки URI;
- Точки DNS;
- Точки EMAIL;
- Точки IP;
- Точки RID.

¹ Расширение CRL Distribution Points в составе сертификатов x.509

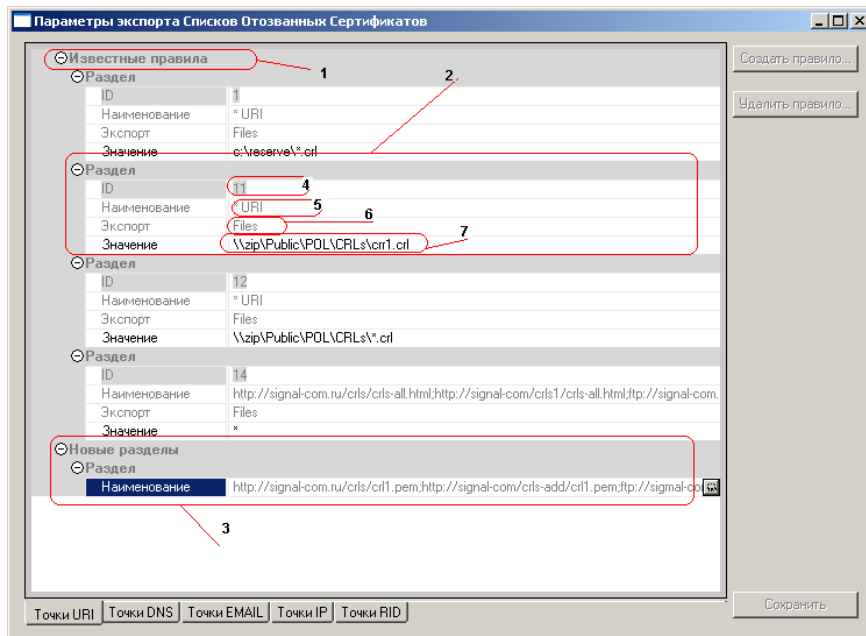


Рис. 146 Карта расширенного экспорта СОС. 1- множество актуальных правил; 2 - заголовок одного из правил расширенного экспорта СОС; 3 - множество точек распространения СОС, для которых не сформулированы правила отображения. Структура актуального правила: 4 – внутренний идентификатор, 5 - наименование точки распространения СОС; 6- тип расширенного экспорта; 7- локальный или сетевой ресурс, где обеспечивается хранение СОС

Как видно из Рис. 146, карта содержит две основные категории:

- «Известные правила»;
- «Новые разделы».

Категория «Известные правила» содержит набор действующих правил, которые выполняются в данный момент времени.

Категория «Новые разделы» содержит «материал» для создания новых правил в категории «Известные правила».

Чтобы исключить искажения имени точки распространения списка отозванных сертификатов (CDP), все новые записи в категории «Известные правила» формируются только на основе дублирования некоторого прототипа. Для создания (удаления) правила курсор должен быть установлен на строчку карты с наименованием «Раздел».

Создание правила возможно только после активации кнопки «Создать правило». Удаление правила из карты осуществляется с помощью кнопки «Удалить правило».

При создании нового правила категории копируется строка «Наименование» (3). Идентификатор записи «ID» (4) является внутренним значением и требуется только для задания ссылки при отладке. Значение параметра «Экспорт» (6) выбирается из списка возможных вариантов¹. Строка «Значение» (7) содержит имя ресурса, где будет физически сохранен экспортируемый СОС².

На Рис. 146 приводится пример правил заполнения карты расширенного экспорта.

- ✓ Правило с идентификатором ID = 1 содержит наименование по умолчанию «* URI». Правила, содержащие такое наименование, используются для экспорта любого СОС, точка распространения которого (URI) указана в расширении CDP сертификатов, изданных в УЦ. Символ (*) означает «любой» URI.

¹ В текущей версии доступен только вариант файлового интерфейса «Files»

² Указанный строковый параметр должен быть задан корректно.

В соответствии с установленным правилом 1, новый список отозванных сертификатов при выпуске должен быть помещен в физическое хранилище **c:\reserve*.crl**. Звездочка указывает на то, что для файла СОС, размещаемого в хранилище, будет использоваться сформированное по шаблону УЦ имя, содержащее постоянную строковую часть и текущий номер списка. При экспорте СОС в хранилище учитывается расширение файла, указанное в параметре «Значение». Расширение **«.crl»** обеспечивает экспорт СОС в бинарном формате, расширение **«.pem»** - в формате BASE64, а расширение **«.txt»** - в формате **«.pem»** с текстовым заголовком.

Таким образом, правило 1 позволяет создать архив всех выпущенных в УЦ списков отозванных сертификатов, точки распространения которых указаны в расширении CDP сертификатов, изданных этим же УЦ.

- ✓ Правило с идентификатором ID = 11 аналогично правилу 1, но созданный СОС должен экспортироваться в виде файла **crl1.crl** в сетевой каталог [\\zip\Public\POL\CRLs\crl1.crl](#).
- ✓ Правило с идентификатором ID = 12 обеспечивает поддержание архива всех выпущенных СОС (точки распространения которых указаны в расширении CDP изданных сертификатов), но в сетевом каталоге [\\zip\Public\POL\CRLs](#).
- ✓ Формирование правила с идентификатором ID = 14 не закончено, т.к. параметр «Значение» содержит значок «*», означающий, что данное правило игнорируется менеджером экспорта СОС и может рассматриваться в качестве сохраняемого шаблона.

Режим автоматического включения адреса точки распространения СОС в расширение CDP формируемого сертификата пользователя управляется двумя флажками (см. Рис. 145):

- «Копировать требуемые параметры из шаблона сертификации» (Флаг А);
- «Копировать требуемые параметры из корневого сертификата (при отсутствии другого источника)» (Флаг В).

Возможные варианты установки приведены в Таблица 8.

Таблица 8. Настройка для добавления CDP в сертификаты пользователей

№	Флаг А	Флаг В	Результат
1	-	-	Совместимость с предыдущими версиями АРМ Администратора УЦ
2	+	-	Установка расширения только на основе шаблонов.
3	+	+	«Смешанный» режим. Если расширение установлено шаблоном, оно имеет приоритет. Если расширение в шаблоне не задано, будет перенесено из сертификата авторитета.
4	-	+	Установка расширения в подчиненном сертификате только на основе копирования расширения из сертификата авторитета.

В текущей версии программы реализована функция автоматического экспорта СОС в режиме их планового выпуска по расписанию и/или выпуска в экспресс-режиме.

ПРИЛОЖЕНИЕ 3. ИЗМЕНЕНИЕ ВИДА НАСТРОЕК РАСШИРЕННОГО ИСПОЛЬЗОВАНИЯ КЛЮЧА

Список идентификаторов объектов, включаемых в «Расширенное использование ключа» расширения сертификата X.509 (см. п. 4.6), может быть заполнен из внешнего списка идентификаторов объектов (OID).

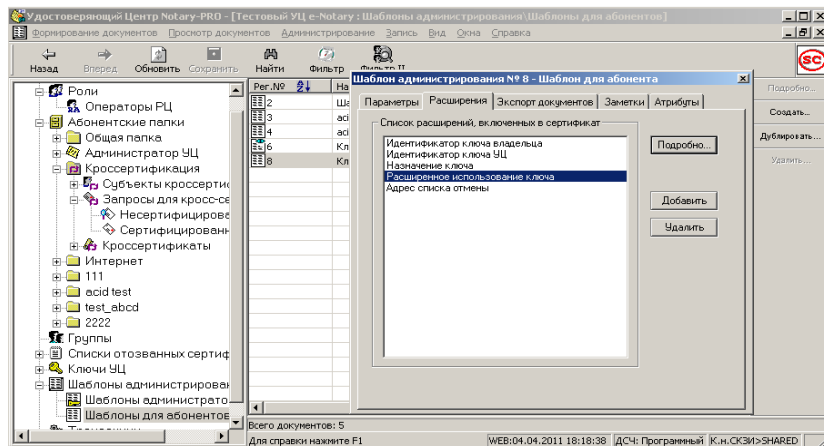


Рис. 147 Выбор расширения «Расширенное использование ключа» для редактирования

Расширение может быть отредактировано как на стадии формирования или редактирования шаблона (см. Рис. 147), так и непосредственно при ручном выпуске сертификата, которое допускает изменения расширений «на лету».

Редактирование расширения выполняется при помощи диалог «Расширенное использование ключа», как показано на Рис. 148. Команда, активируемая кнопкой «Добавить из списка...», открывает диалог для выбора необходимого набора идентификаторов объектов из списка в диалоге «Идентификаторы объектов (OID)».

Выбор группы осуществляется с помощью отметки нужных элементов. Копирование завершается нажатием кнопки «Выбрать».

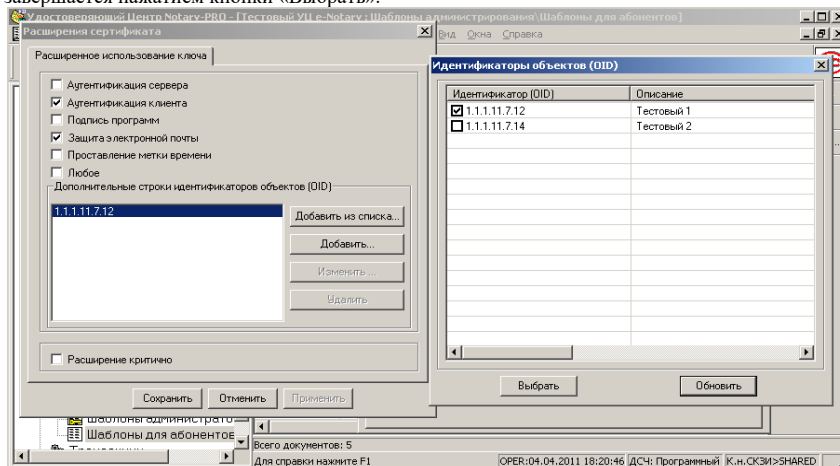


Рис. 148 Диалог «Расширенное использование ключа» и подчиненный диалог «Идентификаторы объектов (OID)»

Список идентификаторов может быть задан с помощью файла конфигурации ECU_OIDs.ini. Этот файл содержит строки идентификаторов и связанных комментариев. Ниже приведён пример конфигурационного файла ECU_OIDs.ini:

```
[OIDS_LIST]
LIST_SIZE=2
:
DEF_OID_DESCR_0=Тестовый 1
DEF_OID_0=1.1.1.11.7.12
DEF_OID_DESCR_1=Тестовый 2
DEF_OID_1=1.1.1.11.7.14
```

ЛИТЕРАТУРА

1. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
2. Требования к форме квалифицированного сертификата ключа проверки электронной подписи. Приложение к приказу ФСБ России от 27.12.2011 № 795.
3. Требования к средствам электронной подписи. Приложение к приказу ФСБ России от 27.12.2011 № 796.
4. Требования к средствам удостоверяющего центра. Приложение к приказу ФСБ России от 27.12.2011 № 796.
5. ПАК УЦ Notary-PRO 2.8. Формуляр. ШКНР.00054-01 30 01. Сигнал-КОМ, 2019.
6. Notary-PRO RA. Автоматизированное рабочее место оператора регистрационного центра. Руководство оператора. ШКНР.00054-01 34 02. Сигнал-КОМ, 2019.
7. ГОСТ Р 34.10-2012. Информационная технология Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
8. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.
9. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
10. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.
11. Notary-PRO RA Server. Сервер регистрационного центра. Руководство системного программиста. ШКНР.00054-01 32 03. Сигнал-КОМ, 2019.
12. Notary-PRO Web Pages. Веб-приложение удостоверяющего центра. Руководство системного программиста. ШКНР.00054-01 32 06. Сигнал-КОМ, 2019.
13. СКЗИ «CADB 2.1». Формуляр. ШКНР.00053-01 30 01. Сигнал-КОМ, 2019.
14. СКЗИ «CADB 2.1». Подсистема управления ключевой информацией. Общее описание. ШКНР.00053-01 31 01. Сигнал-КОМ, 2019.
15. ПАК УЦ Notary-PRO 2.8. Типовой регламент. ШКНР.00054-01 90 02. Сигнал-КОМ, 2019.
16. Приказ ФНС России от 8.04.2013 № ММ-7-4/142@ «Порядок применения квалифицированных сертификатов ключей проверки электронных подписей в информационных системах ФНС России».
17. Приказ ФНС России от 29.06.2012 № ММВ-7-6/465@ «Об утверждении формата описи документов, направляемых в налоговый орган в электронном виде по телекоммуникационным каналам связи».
18. ITU-T Recommendation X.509, «Information Technology - Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks», August 2005.
19. R.Rivest, The MD5 Message-Digest Algorithm, RFC 1321, April 1992.
20. B.Kaliski, «PKCS #7: Cryptographic Message Syntax Version 1.5», RFC 2315, March 1998.
21. M.Nystrom, B.Kaliski, «PKCS #9: Selected Object Classes and Attribute Types Version 2.0», RFC 2985, November 2000.
22. M.Nystrom, B.Kaliski, «PKCS #10: Certification Request Syntax Specification Version 1.7», RFC 2986, November 2000.
23. V.Popov, I.Kurepkin, S.Leontiev, «Additional cryptographic algorithms for use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 algorithms», RFC 4357, January 2006.
24. S.Leontiev, D.Shefanovski, «Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile», RFC 4491, May 2006.
25. D.Cooper, S.Santesson, S.Farrell, S.Boeyen, R.Housley, W. Polk, «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», RFC 5280, May 2008.
26. RSA Laboratories, «PKCS #12: Personal Information Exchange Syntax Standard version 1.0», June 24, 1999.
27. Netscape Certificate Extensions Communicator 4.0 Version.
28. Oracle9i Backup and Recovery Concepts. Release 2 (9.2)

29. Sam R. Alapati, «Expert Oracle Database 10g Administration», Apress, 2005.
30. B. Woody, «Administrator's Guide to SQL Server 2005», 2006.
31. Е. Мамаев, «Microsoft SQL Server 2000. Наиболее полное руководство», БХВ-Петербург, 2005.
32. RFC 5272. J. Schaad, M. Myers, «Certificate Management Messages over CMS (CMC)», 2008.
33. SEC 2: Recommended Elliptic Curve Domain Parameters. September 20, 2000. Version 1.0. Certicom Research.
34. FIPS 186-2, Digital Signature Standard. Federal Information Processing Standards Publication 186-2, 2000. Available from: <http://csrc.nist.gov/>
35. Adi Shamir, How to share a secret. Communications of the ACM, 1979.
36. Р 1323565.1.024-2019. Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов. Федеральное агентство по техническому регулированию и метрологии, 2019.
37. Р 1323565.1.023-2018. «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509». Федеральное агентство по техническому регулированию и метрологии, 2018.