

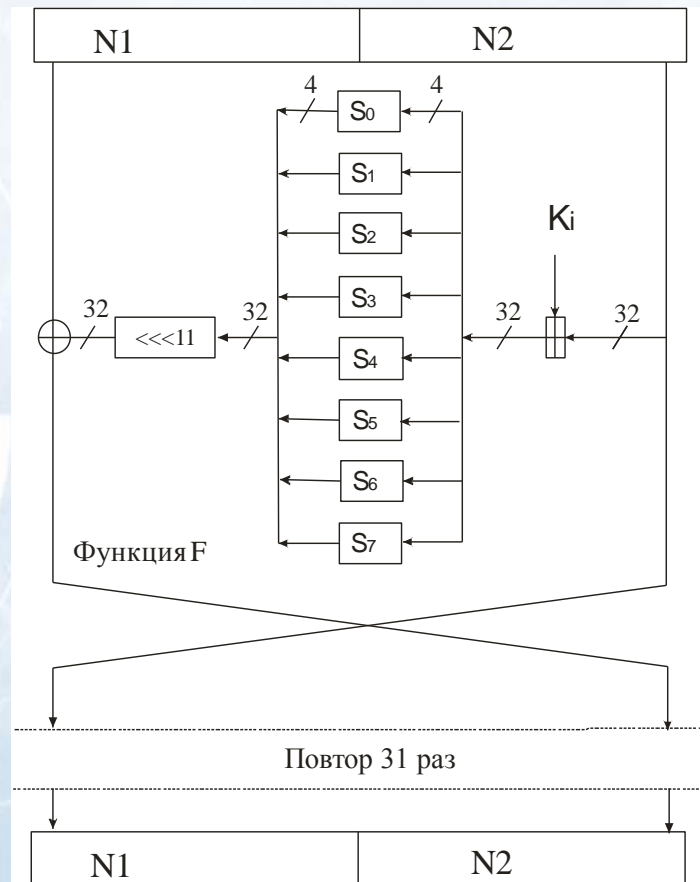


Введение в инфраструктуру открытых ключей



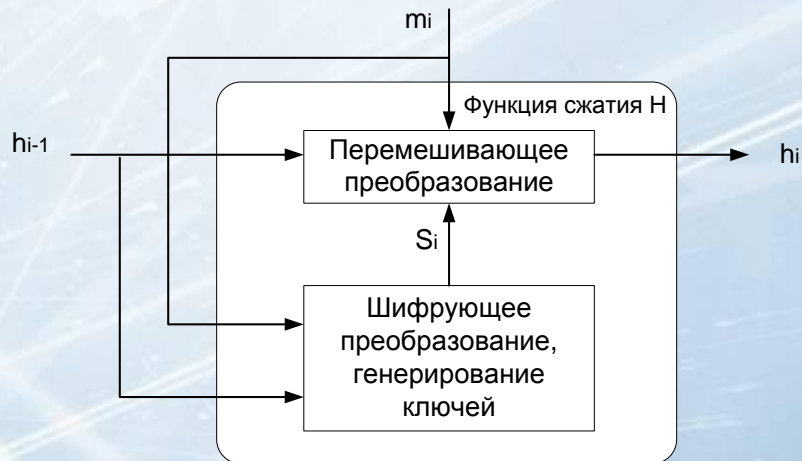
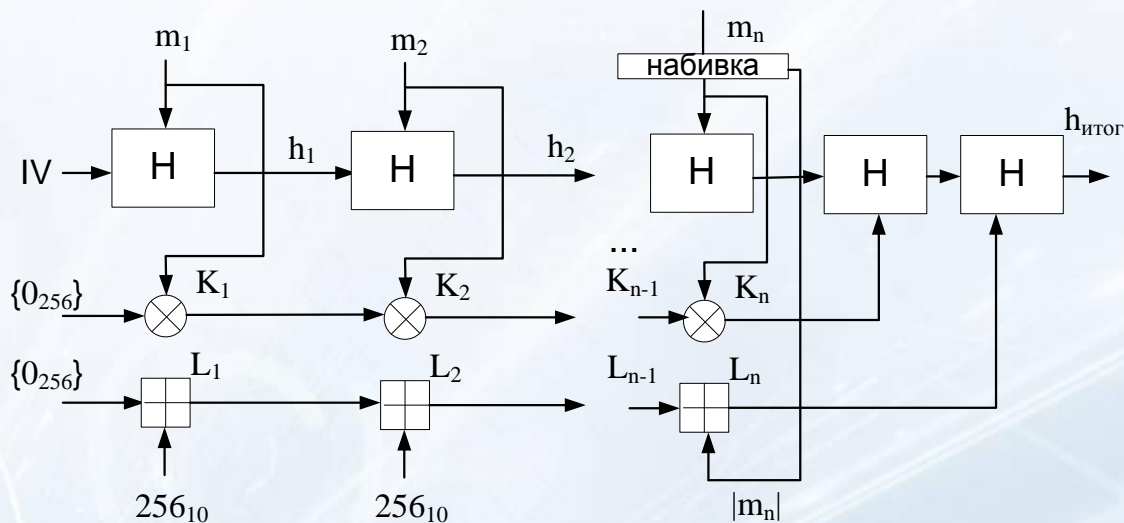
Симметричное шифрование

Для обеспечения конфиденциальности данных используется шифрование информации. В России в качестве национального стандарта используется алгоритм шифрования ГОСТ 28147-89.



 - сложение по модулю 2^{32}

ХЭШ-функция



ЭЦП

Подписание документа автором:



Проверка подписи получателем:



ФЗ N 63-ФЗ "Об электронной подписи"

от 6 апреля 2011 г.

Федеральный закон от 10 января 2002 года № 1-ФЗ "Об ЭЦП" признать утратившим силу с 1 июля 2012 года.

Типы подписей:

1. Простая (коды, пароли или иных средств для подтверждения факта формирования электронной подписи конкретным лицом)

2. Усиленная

- ❖ Неквалифицированная
- ❖ Квалифицированная

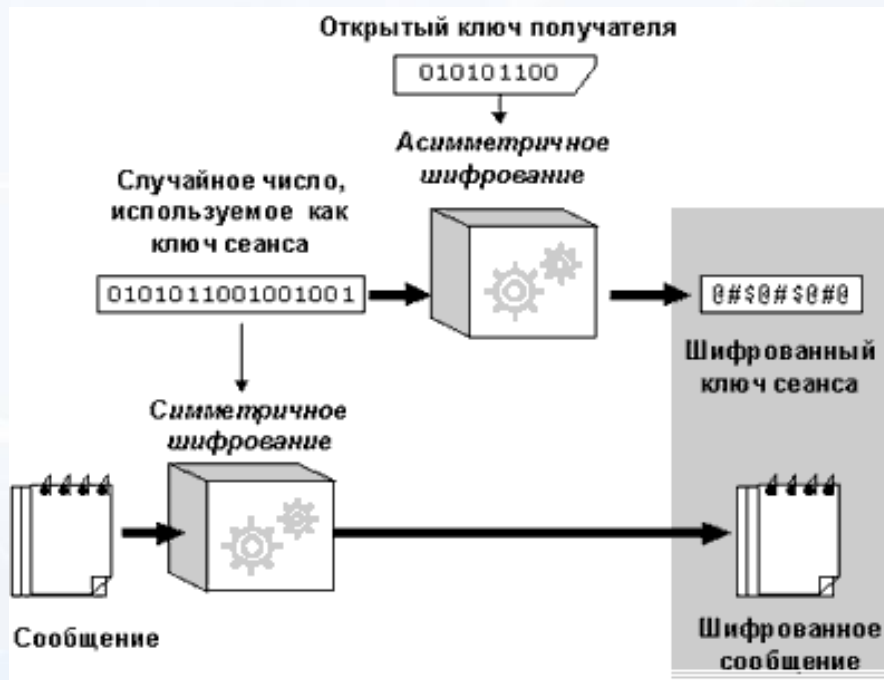
Неквалифицированная эл.подпись

- ❖ получена в результате криптографического преобразования информации с использованием ключа электронной подписи
- ❖ позволяет определить лицо, подписавшее электронный документ
- ❖ позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- ❖ создается с использованием средств электронной подписи.

Квалифицированная эл.подпись

- ❖ все признаки неквалифицированной эл.подписи
- ❖ ключ проверки эл.подписи указан в квалифицированном сертификате
- ❖ для создания и проверки эл.подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Электронный цифровой конверт



Распределение ключей

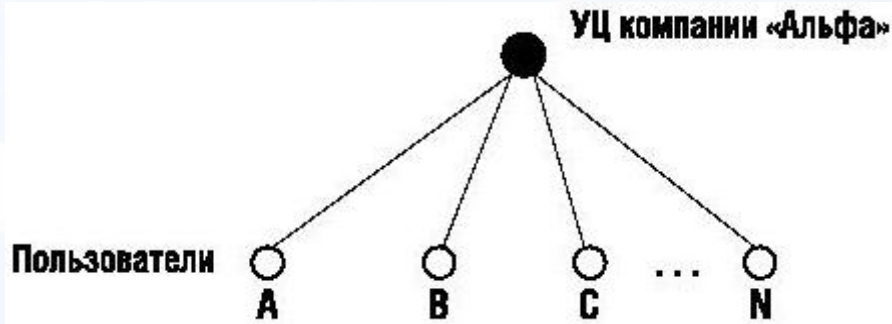
Необходимо исключить подмену на этапе пересылки открытых ключей, а также подтвердить правильность сведений о владельце.

Рассмотрим два варианта обмена :

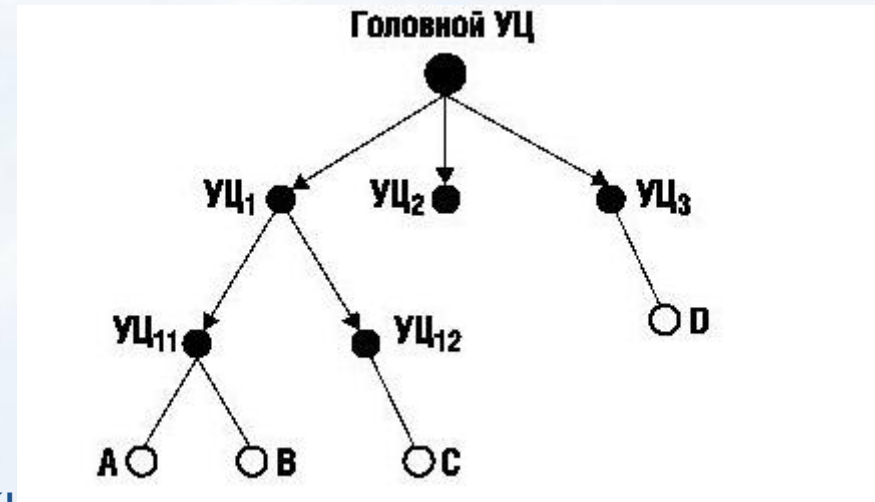
- Прямой обмен открытыми ключами
- Обмен открытыми ключами через удостоверяющий центр.

Архитектуры Public Key Infrastructure

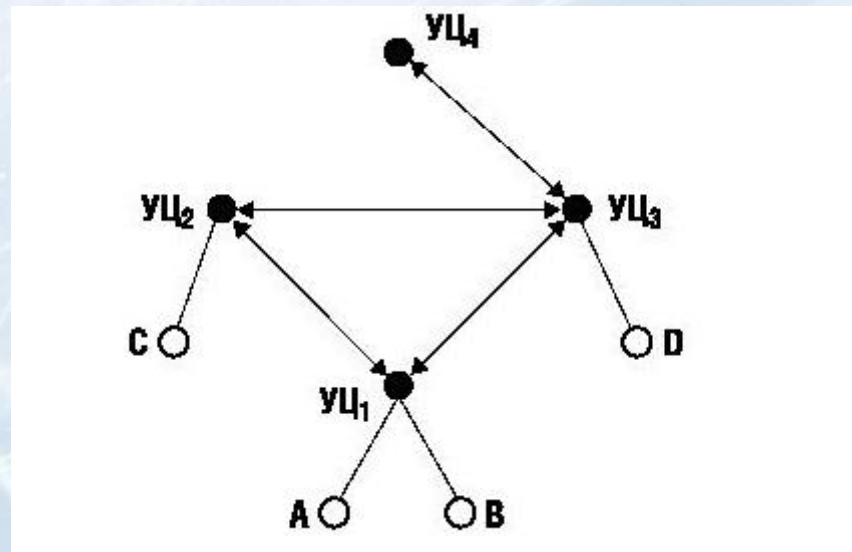
Одиночный УЦ



Иерархическая PKI

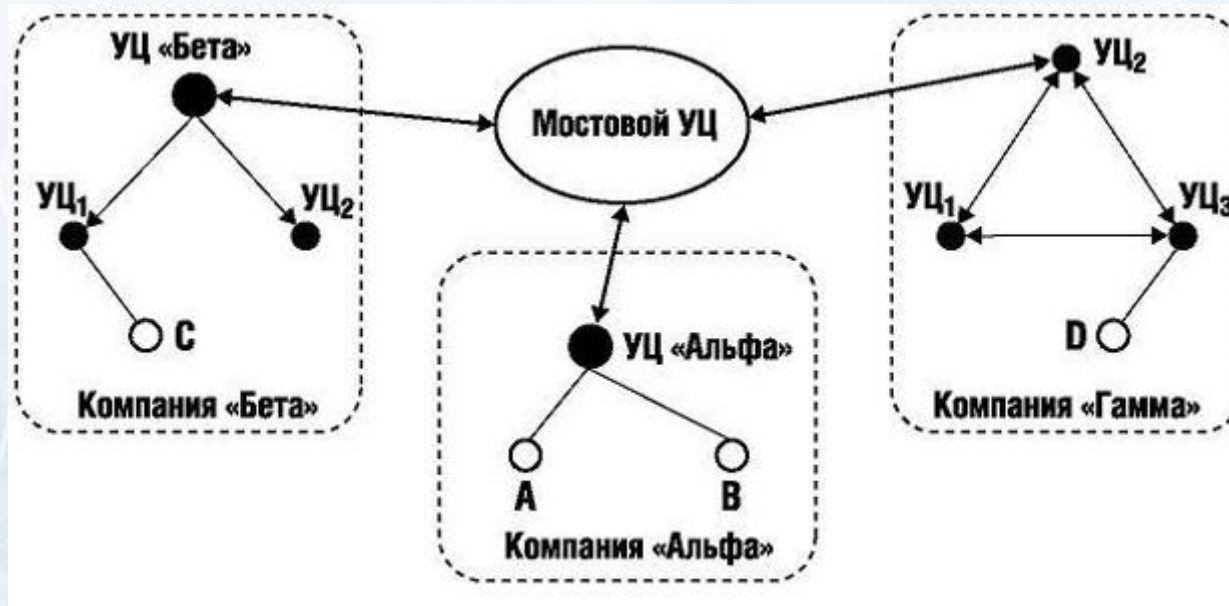


Сетевая PKI



Архитектуры РКІ (2)

Архитектура мостового УЦ



Стандарт X.509 версия 3

Version	Версия сертификата	3
Certificate Serial Number	Серийный номер сертификата	40:00:00:00:00:00:00:ab:38:1e:8b:e9:00:31:0c:60
Signature Algorithm Identifier	Идентификатор алгоритма ЭЦП	ГОСТ Р 34.10-94
Issuer X.500 Name	Имя Издателя сертификата	C=RU, ST=Moscow,O=PKI, CN=Certification Authority
Validity Period	Срок действия сертификата	Действителен с : Ноя 2 06:59:00 1999 GMT Действителен по : Ноя 6 06:59:00 2004 GMT
Subject X.500 Name	Имя Владельца сертификата	C=RU, ST=Moscow, O=PKI, CN=Sidorov
Subject Public Key Info	Открытый ключ Владельца	тип ключа: Открытый ключ ГОСТ длина ключа: 1024 значение: AF:ED:80:43.....
Issuer Unique ID version 2	Уникальный идентификатор Издателя	
Subject Unique ID version 2	Уникальный идентификатор Владельца	
type	critical	value
type	critical	value
type	critical	value
дополнения (только версия 3)		
CA Signature ЭЦП Центра Сертификации		

- Типы дополнений:
- ограничивающие
 - информационные



Программный комплекс «Верба-сертификат - МВ»

Удостоверяющий центр на базе программного комплекса «Верба»

Назначение

- ❖ Построение иерархической системы управления сертификатами (PKI)
- ❖ Обеспечение конфиденциальности, целостности информации и подтверждение авторства (ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94, ГОСТ 28147-89)

Состав

❖ Удостоверяющий центр:

- Центры сертификации (ЦС)
- Центры регистрации (ЦР)
- АРМ РКС

❖ Конечные пользователи:

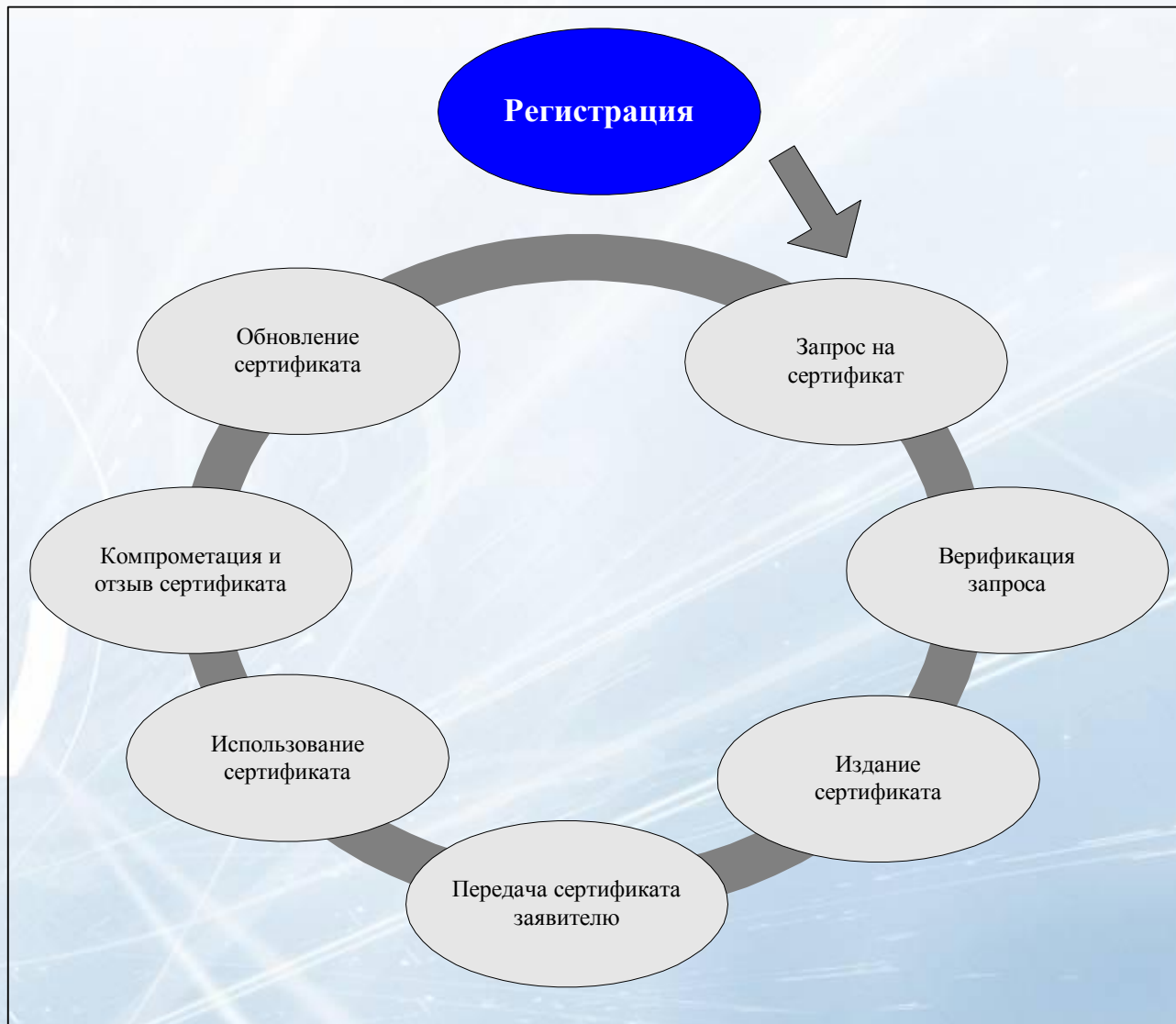
- «Верба- Сертификат МВ Клиент»
- ПО «Верба-файл»

Базовые объекты

системы «Верба-Сертификат МВ»

- ❖ сертификат (.cer)
- ❖ список отозванных сертификатов (COC) (.crl)
- ❖ запрос на сертификат (.pse)
- ❖ сертификат регистрации (.cer)
- ❖ сообщение о компрометации (.pse)
- ❖ упакованные данные (PKCS#7 и PKCS#10)

Жизненный цикл объектов





Центр Сертификации



Биологический датчик случайных чисел

Первоначальная инициализация датчика

Инициализация датчика случайных чисел

Вставьте ключевой носитель для инициализации ДСЧ в:

инициализационный считыватель авто

имя файла initrndm

< Назад Далее > Отмена

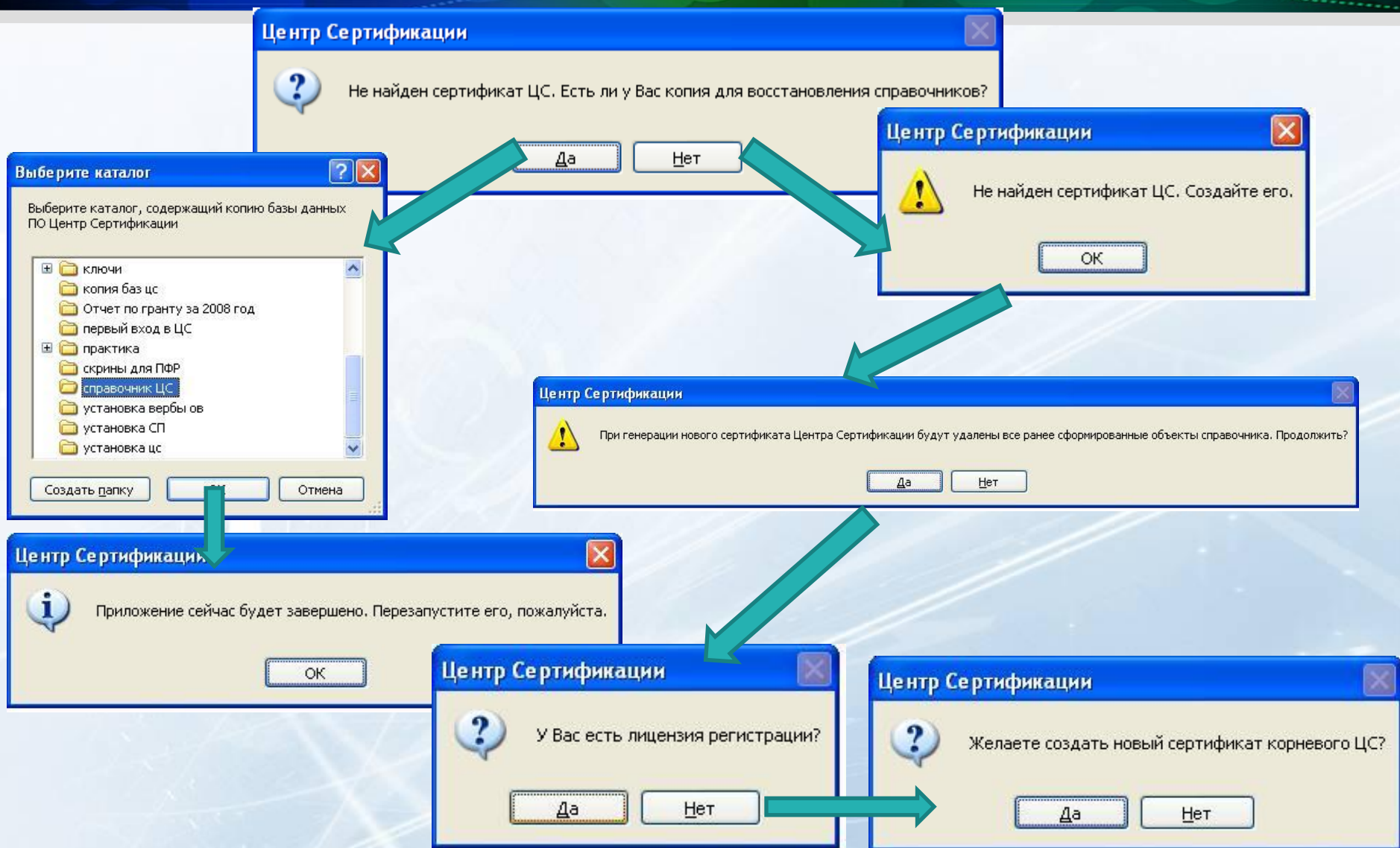
Биологический датчик случайных чисел

Нажимайте клавиши или двигайте мышью...

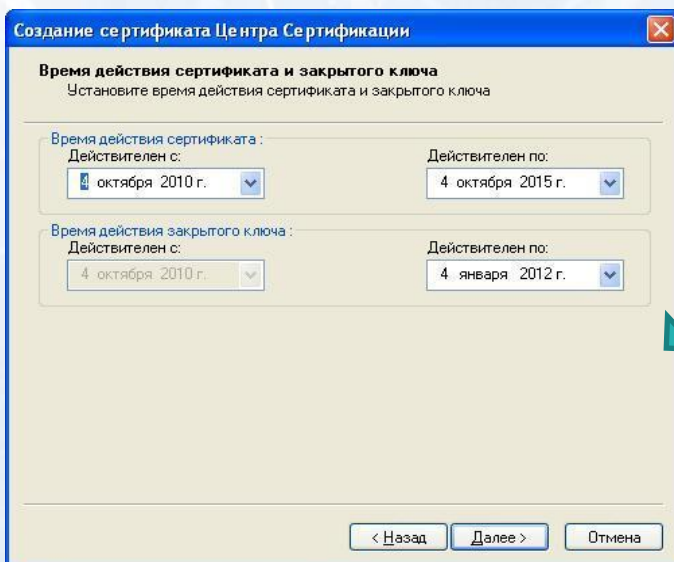
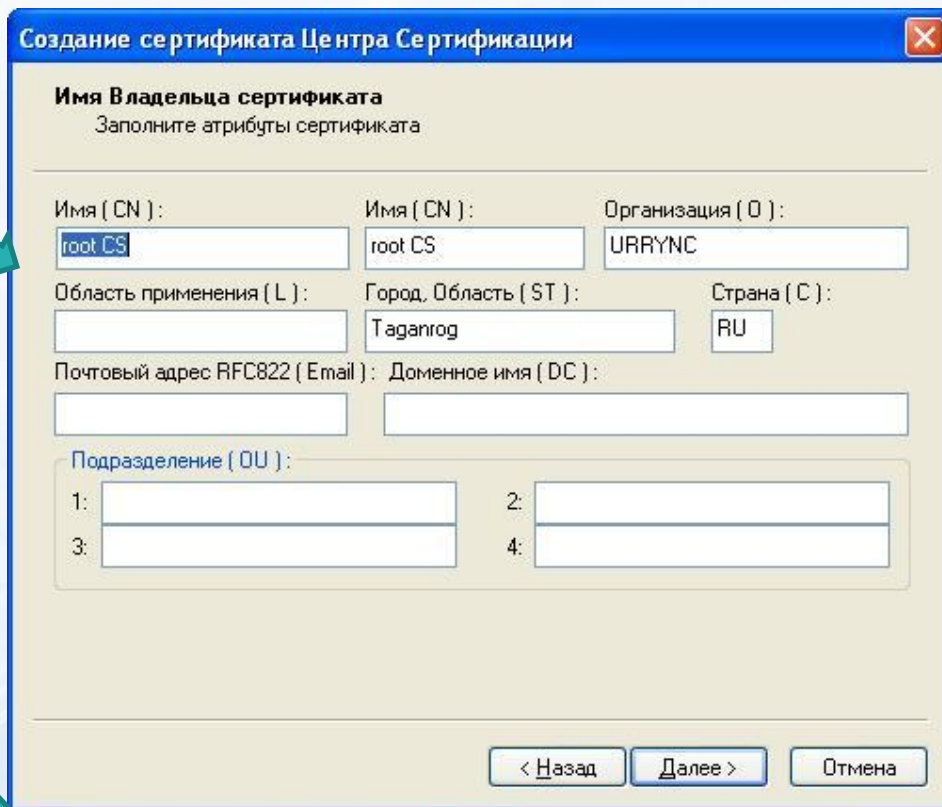
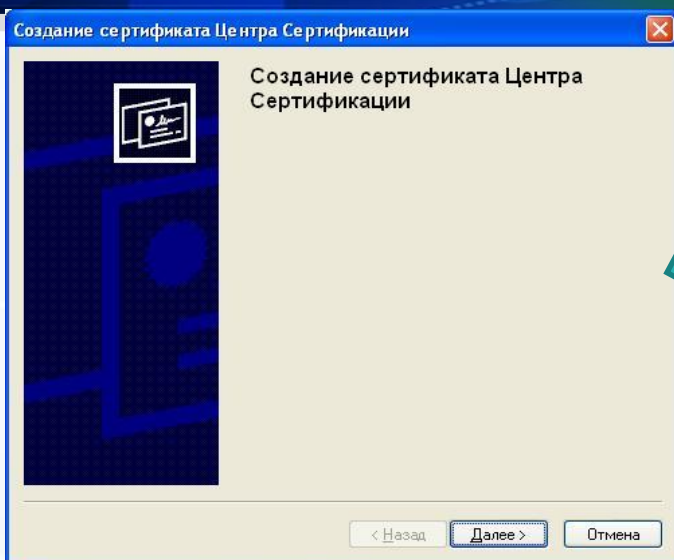
Alt +

Отказ

Первый запуск ЦС



Создание самоподписанного сертификата



Создание самоподписанного сертификата

Создание сертификата Центра Сертификации

Максимальное количество уровней иерархии
 Установите максимальное количество уровней иерархии

Максимальное количество уровней иерархии :

< Назад Далее >

Создание сертификата Центра Сертификации

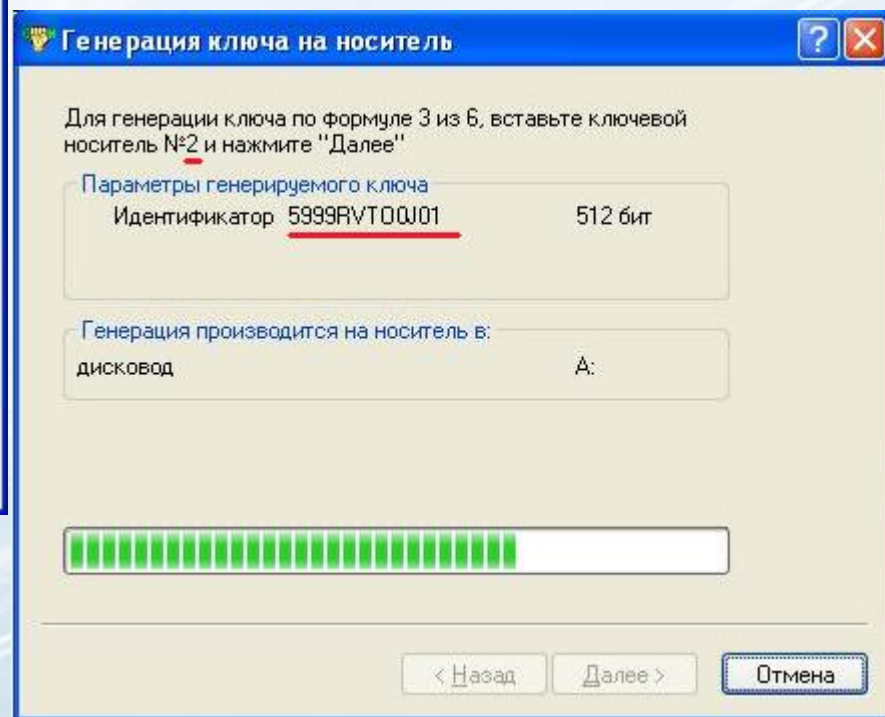
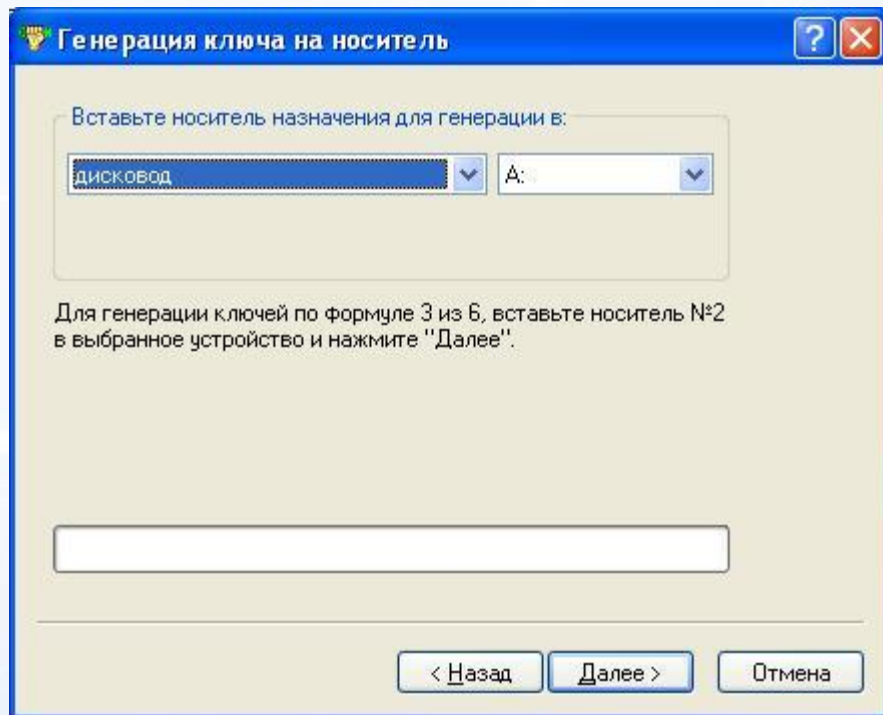
Задание альтернативного имени Владельца сертификата
 Заполните дополнительные сведения о Владельце сертификата

Параметр	Значение
email	marokat@gmail.com
DNS	
URL	
IP адрес	
Организация	URRYNC
Зарегистрированный Адрес	
Фамилия	Maro
Должность	mns
Номер Телефона	
Описание	
Номер Расчетного Счета	
Банковский Идентификационный Код	
Почтовый Адрес	
Адрес Exchange	
адрес Notes	

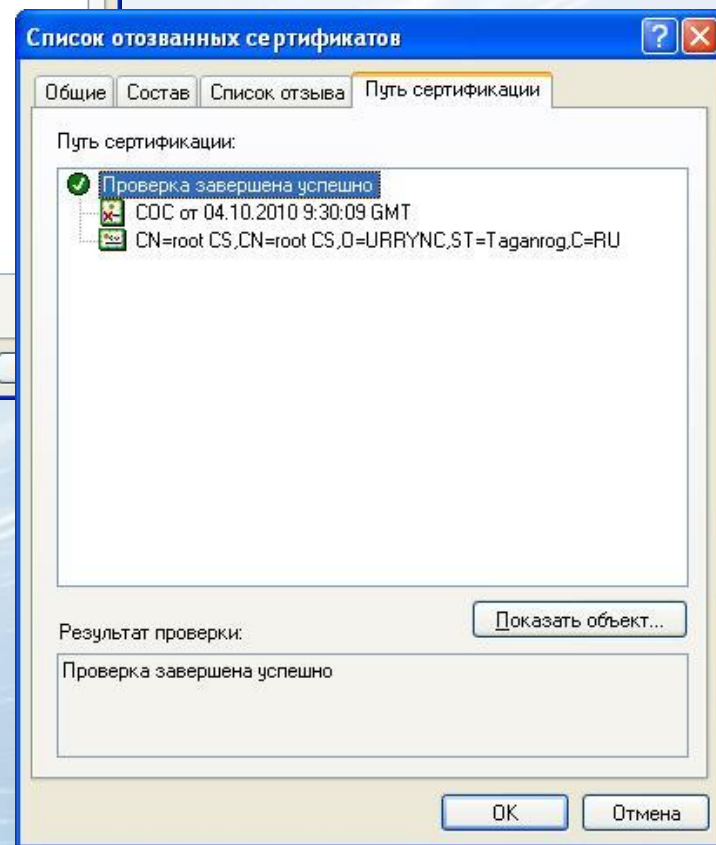
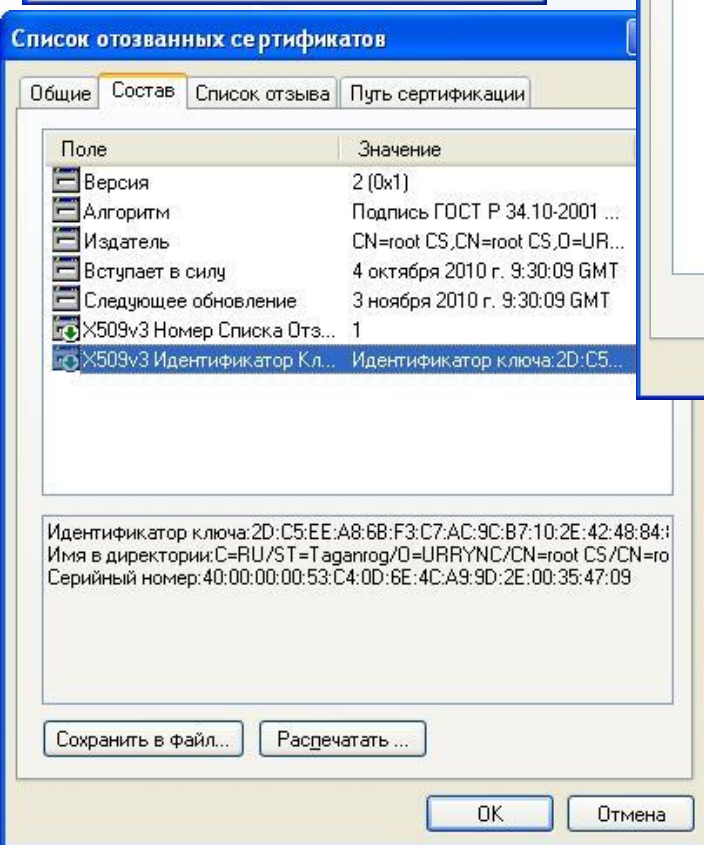
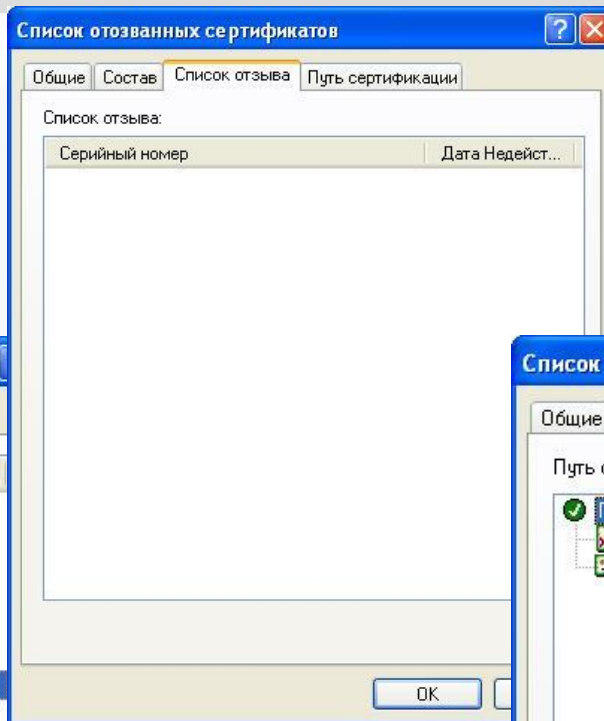
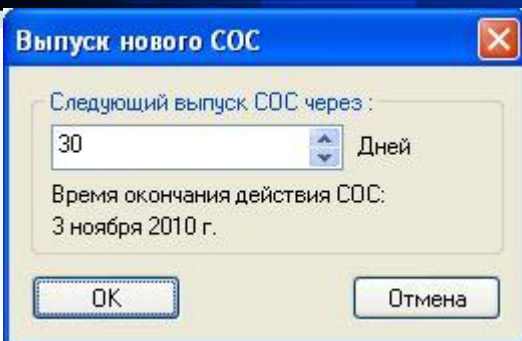
< Назад Готово Отмена

Сертификат ЦС печатается в двух экземплярах

Создание закрытых ключей ЦС



Формирование СОС ЦС



Интерфейс ЦС

Окно отображения разделов базы ЦС

Окно отображения объектов в разделах базы ЦС

Главное меню

Персональный справочник сертификатов
Содержит все сертификаты Центра Сертификации с неоконченным сроком действия
Защищен ЭЦП на ключе Центра Сертификации.

База регистрации ЦР
Содержит лицензии регистрации подчиненных ЦР

Шаблоны сертификатов
Содержит шаблоны для создания

База сертификации
Содержит запросы на получение сертификата от ЦР в виде PKCS#10
Содержит запросы на получение сертификата от абонентов, обработанные ЦР, в виде шаблонов сертификатов X.509
Все изданные ЦС сертификаты X.509

СООС
Содержит действующий в системе список отозванных сертификатов

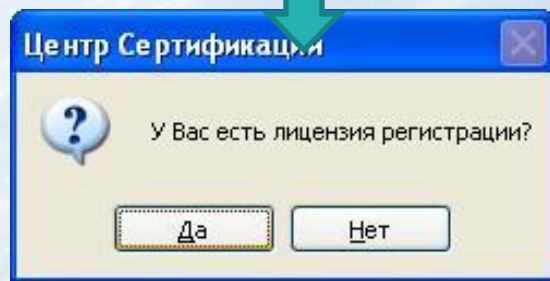
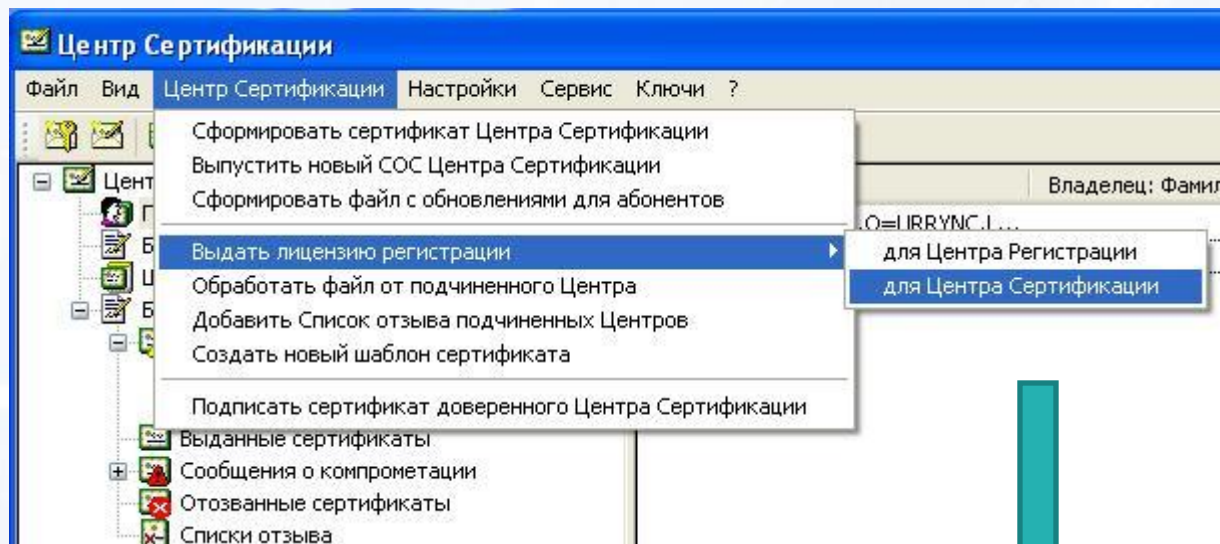
Запросы о компрометации
Содержит необработанные запросы (не включенные в список отозванных)
Содержит обработанные запросы, перечисленные в списке отозванных

Текущее время по Гринвичу

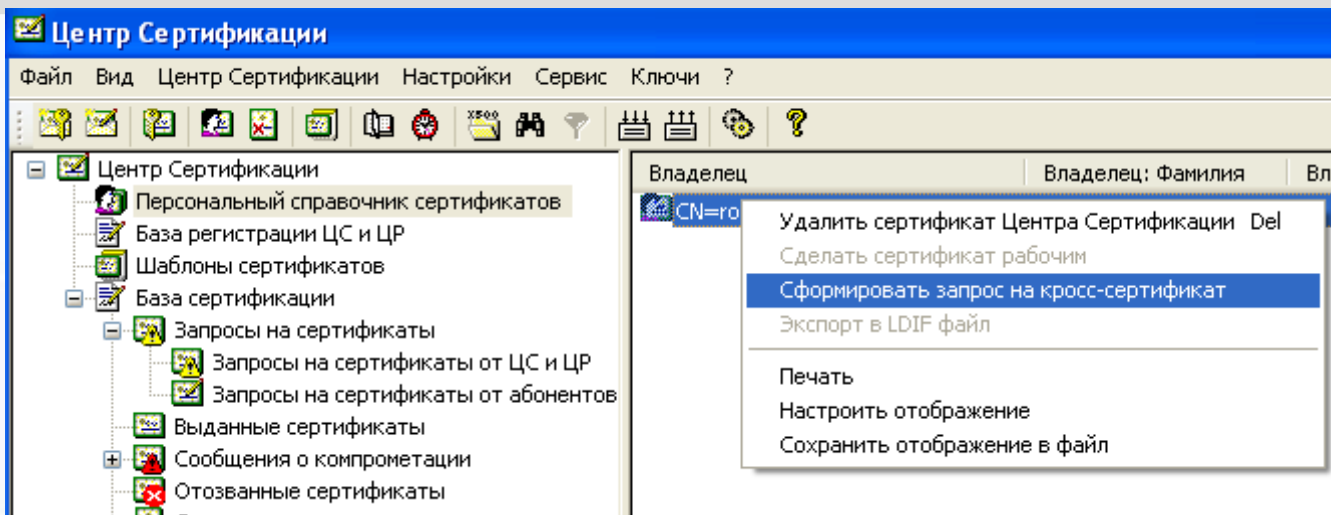
Владелец	Действ...	Де...
	24.03.2...	19...
	01.04.2...	19...
	23.09.2...	23...

[0 из 3] 17 июня 200

Регистрация подчиненного ЦС

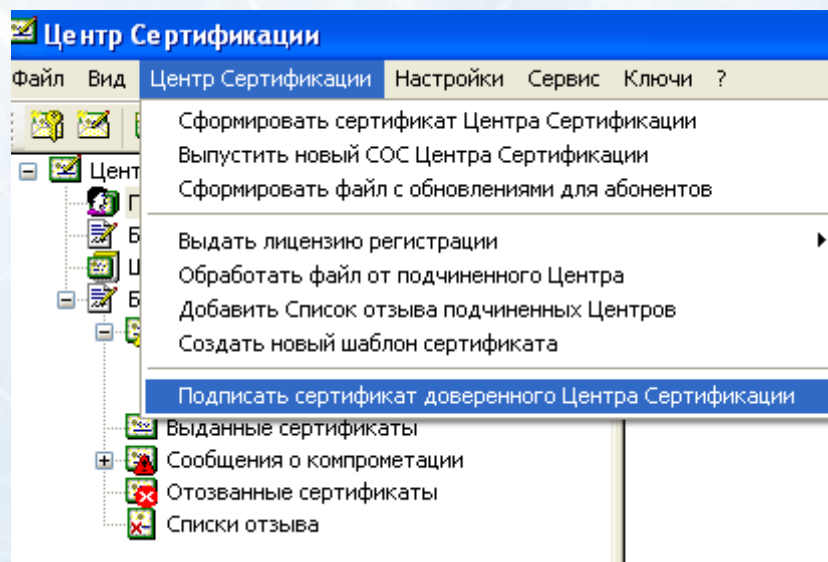


Установление доверия между ЦС



(.req)

ASN 1 .DER



(.pse) PKCS#7



Центр Регистрации

Интерфейс ЦР

The screenshot shows the 'Центр Регистрации' (Registration Center) software interface. The main window is titled 'Центр Регистрации' and contains a tree view on the left and a list of objects on the right. The tree view is organized as follows:

- Центр Регистрации
 - Персональный справочник сертификатов
 - Локальный справочник Центра Регистрации
 - Сертификаты регистрации
 - Запросы на сертификаты
 - Сертификаты
 - Сообщения о компрометации
 - СОС
 - База регистрации
 - Сертификаты регистрации
 - Запросы на сертификаты
 - Запросы на сертификаты от абонентов
 - Необработанные запросы на сертификаты от абонентов
 - Обработанные запросы на сертификаты от абонентов
 - Запросы отосланные в Центр Сертификации
 - Выданные сертификаты
 - Сообщения о компрометации
 - Запросы на отзыв сертификатов от абонентов
 - Запросы отосланные в Центр Сертификации
 - Отозванные сертификаты
 - Шаблоны сертификатов
 - Сетевые справочники сертификатов

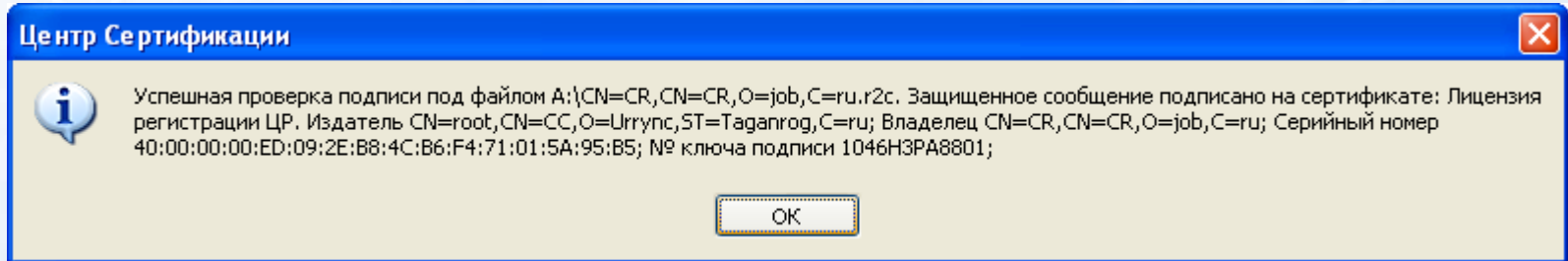
Four callout boxes on the right provide detailed information about specific sections:

- Персональный справочник сертификатов**
Содержит все сертификаты Центра
Сертификации с неоконченным сроком действия
- Локальный справочник ЦР**
Действующие сертификаты ЦР
Запросы на выпуск сертификатов ЦР
- База регистрации**
Сертификат регистрации абонентов
Запросы на выдачу сертификатов абонентов
Сертификаты абонентов
Сообщения о компрометации сертификатов
- Шаблоны сертификатов**
Содержит шаблоны для создания сертификатов регистрации

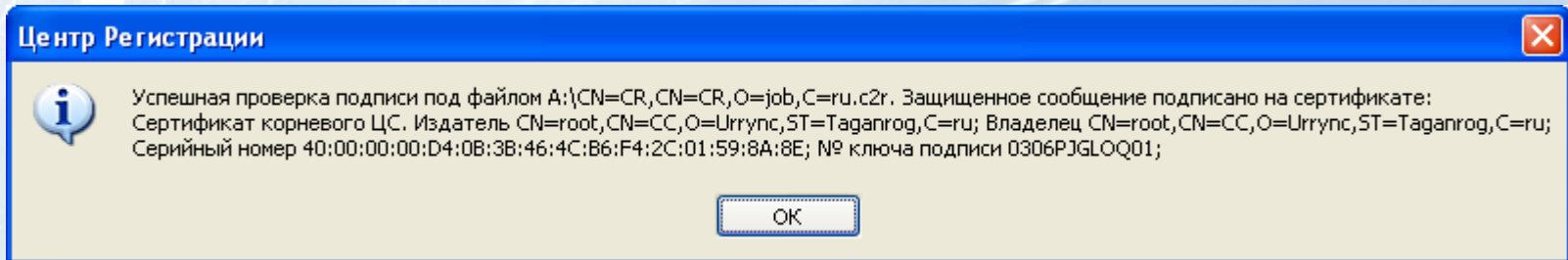
At the bottom of the window, there is a status bar showing 'Текущее время по Гринвичу' and the date '18 февраля 2005 г. 10:19:40 GMT'.

Создание сертификата ЦР

- ❖ ЦС: ЦС → Выдать лицензию регистрации → для ЦР
- ❖ ЦР: Вход по лицензии регистрации
- ❖ ЦР: ЦР → Сформировать запрос на сертификат ЦР (.r2c)
- ❖ ЦС: ЦС → Обработать файл от подчиненного центра



- ❖ ЦС: Создание сертификата и сохранение для ЦР (.c2r)
- ❖ ЦР: ЦР → Обработать файл из ЦС



Создание сертификата ЦР

Сертификат Центра Регистрации

Общие Состав Путь сертификации

Сертификат Центра Регистрации

Владелец: CN=CR,CN=CR,O=job,C=ru
Издатель: CN=root,CN=CC,O=Urrync,ST=Taganrog,C=ru

	Действителен с	Действителен по
Ключ:	14 октября 2010 г.	14 января 2012 г.
Сертификат:	14 октября 2010 г.	14 октября 2015 г.

Есть закрытый ключ этого сертификата

Экспорт ...

OK

Сертификат Центра Регистрации

Общие Состав Путь сертификации

Путь сертификации:

- ✓ Проверка завершена успешно
 - ✓ CN=CR,CN=CR,O=job,C=ru
 - ✗ СОС от 14.10.2010 12:14:41 GMT
 - ✓ CN=root,CN=CC,O=Urrync,ST=Taganrog,C=ru

Результат проверки: Показать объект...

Проверка завершена успешно

OK Отмена

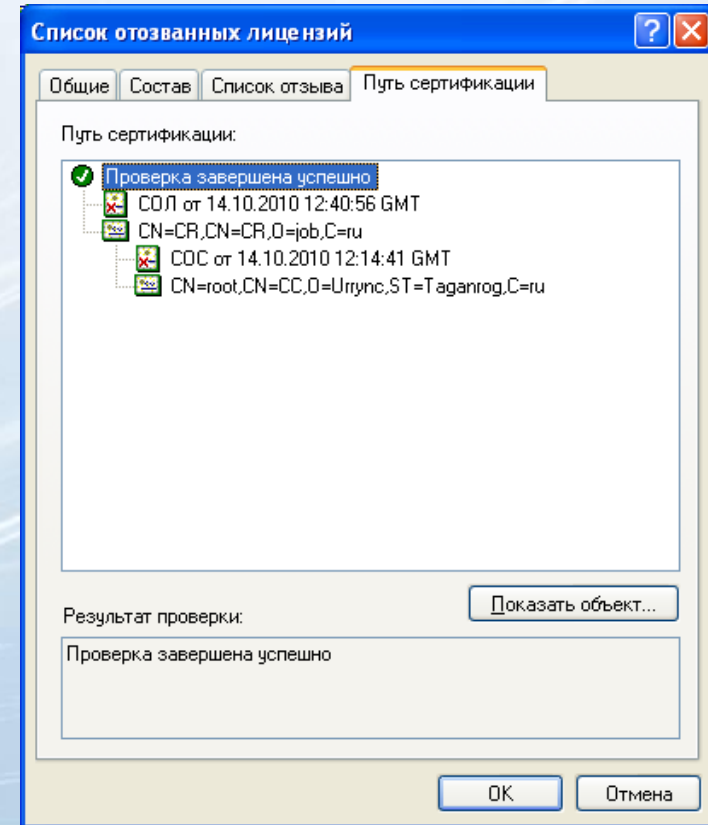
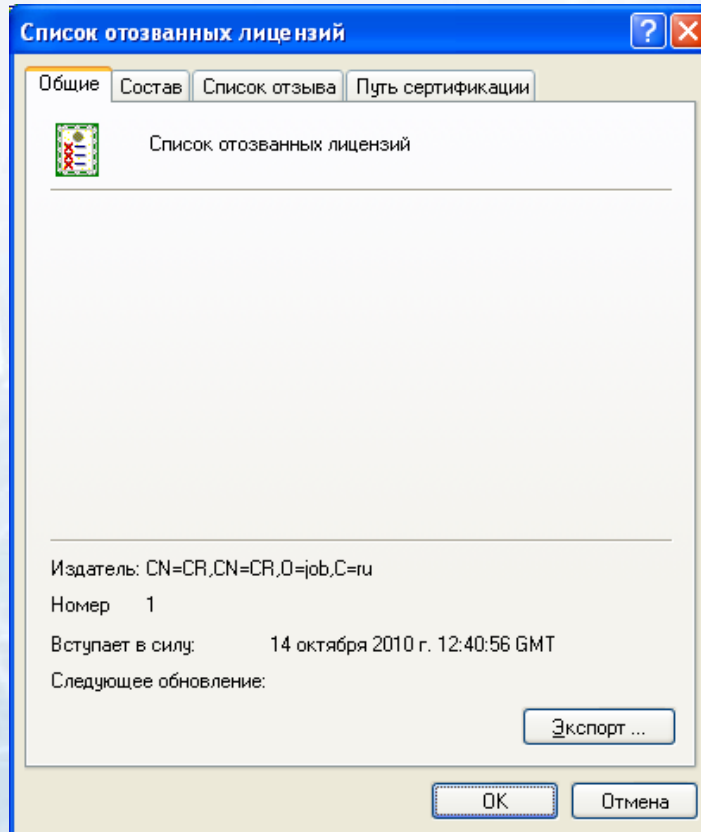
Центр Регистрации

ЦР работает в нормальном режиме.

OK

Импорт СОЛ ЦР в ЦС

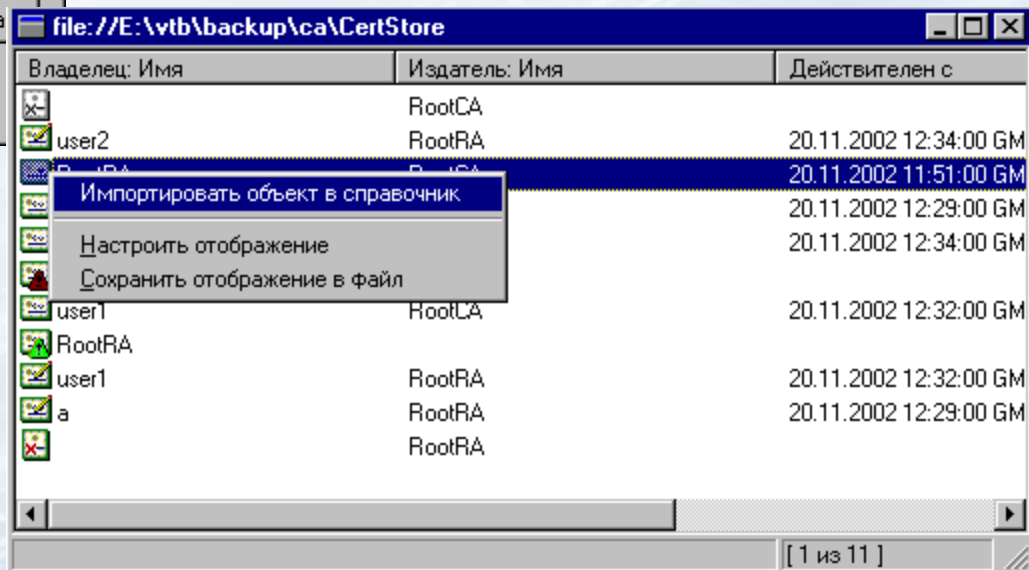
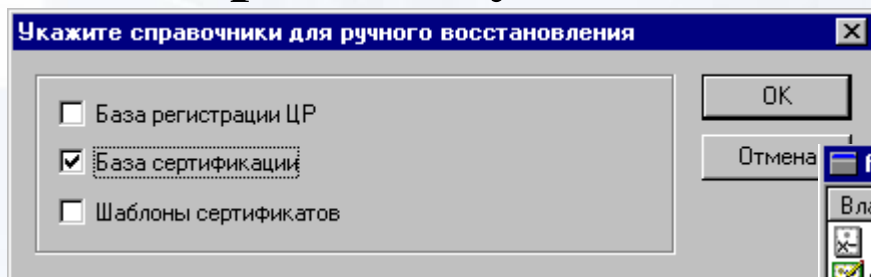
- ❖ ЦР: Списки отзыва → Экспорт в файл в DER кодировке (.crl)
- ❖ ЦС: ЦС → Добавить Список отзыва подчиненных Центров



Восстановление баз

Сервис → Восстановление справочников

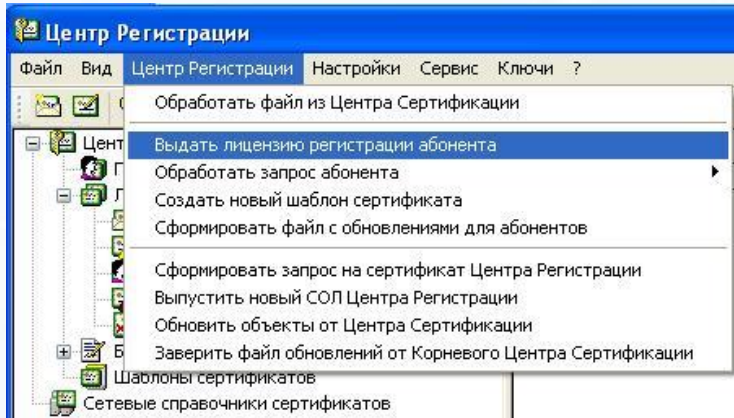
Сервис → Ручное восстановление справочников





Создание сертификатов пользователей

Регистрация пользователя



- Пользователь предоставляет:
- ❖ лист с образцами печати и личной подписи руководителя организации
 - ❖ копию Договора с администрацией системы
 - ❖ выписку из приказа о назначении администратора информационной безопасности организации

Создание новой лицензии регистрации

Наименование шаблона:

Имя Владельца сертификата
Заполните атрибуты сертификата

Имя (CN): user1 Имя (CN): user1 Организация (O): work

Область применения (L): Город, Область (ST): rostov Страна (C): ru

Почтовый адрес RFC822 (Email): Доменное имя (DC):

Подразделение (OU):

1: kaf 2: 3: 4:

Разрешить генерацию ключа шифрования. Ключ сформирован в ЦР

Время действия сертификата и закрытого ключа
Установите время действия сертификата и закрытого ключа

Время действия сертификата :
Действителен с: 15 октября 2010 г.

Действителен по: 15 октября 2020 г.

Время действия закрытого ключа :
Действителен с: 15 октября 2010 г.

Октябрь 2020 г.						
Пн	Вт	Ср	Чт	Пт	Сб	Вс
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8
☐ Сегодня: 15.10.2010						

Генерация ключей пользователем

Пользователь получает в ЦР:

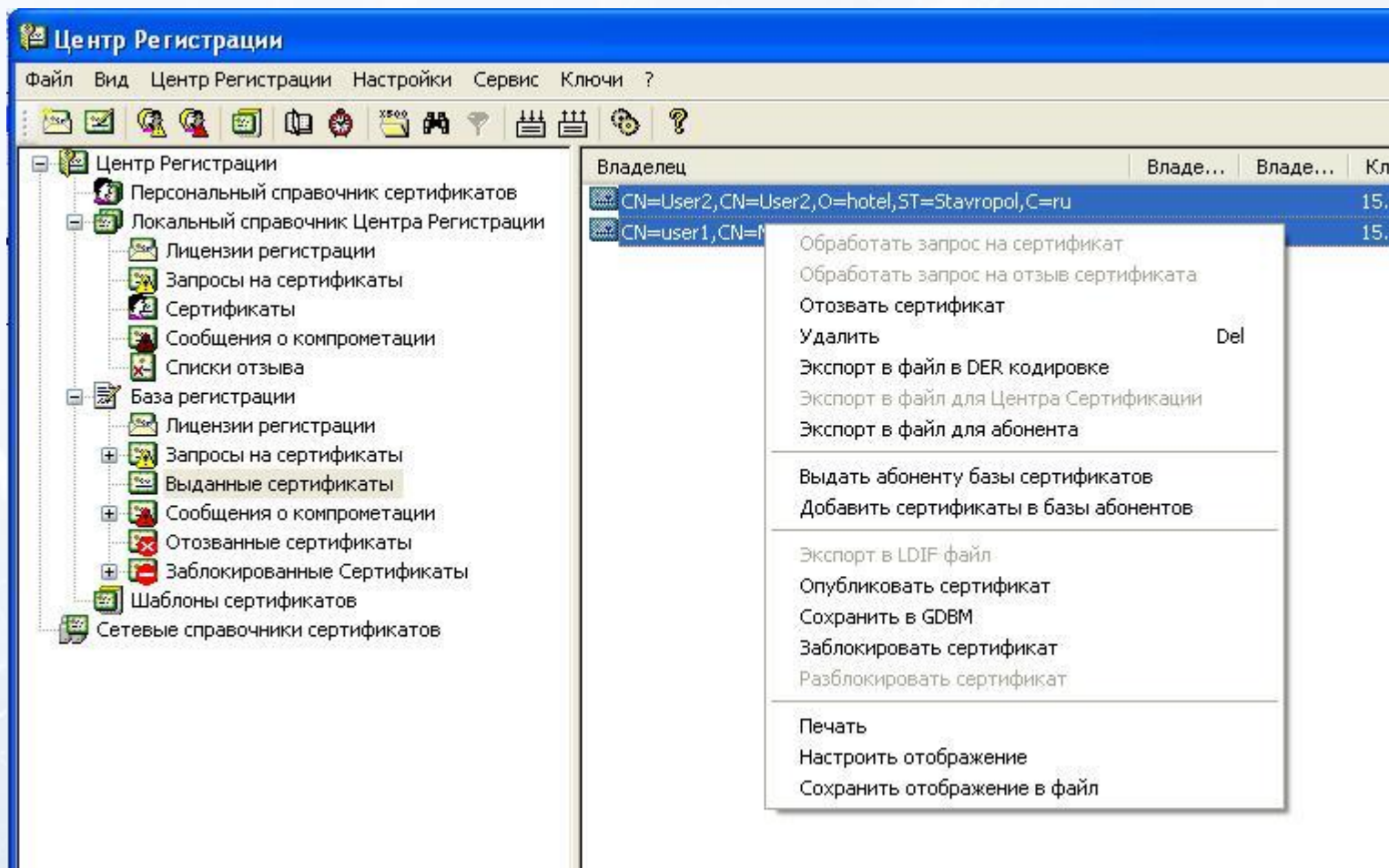
- ❖ Ключ регистрации
- ❖ Сертификат регистрации (сертификаты ЦС, ЦР и действующие СОС)
- ❖ Карточку оповещения о компрометации
- ❖ Копию заверенного бланка сертификата регистрации пользователя
- ❖ Копии заверенных бланков сертификатов ЦС и ЦР

Генерация ключей в ЦР

Пользователь получает:

- ❖ Закрытый ключ
- ❖ Сертификат открытого ключа
- ❖ Копии справочника
- ❖ Карточку оповещения о компрометации
- ❖ Копию заверенного бланка сертификата открытого ключа
- ❖ Копии заверенных бланков сертификатов ЦС и ЦР

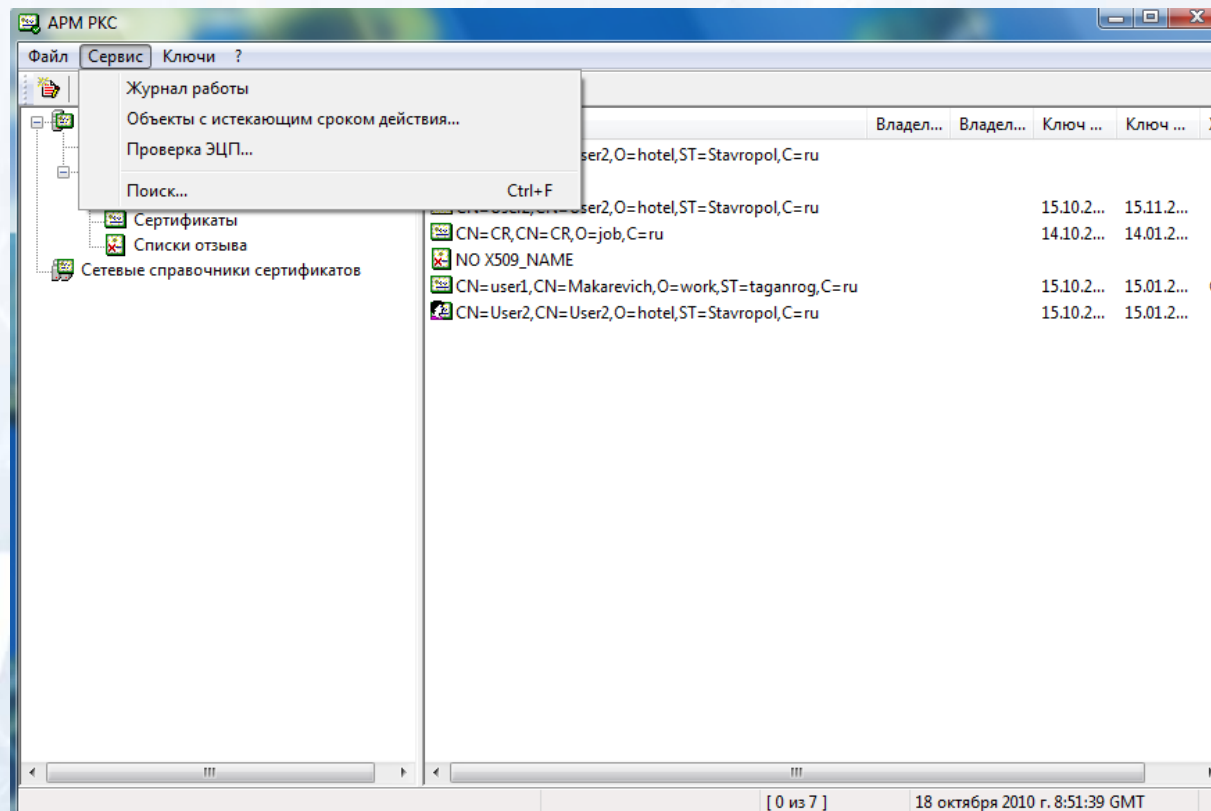
Создание обновлений для пользователей





АРМ «Разбора конфликтных ситуаций»

Интерфейс



Разбор конфликтной ситуации (1)

Мастер проверки ЭЦП

Выбор документа для проверки
Для проверки необходимо выбрать подписанный электронный документ

Введите имя файла, который содержит подписанный электронный документ

C:\Users\Катя\Desktop\OpenKeyCrypt.pdf.P7S

Данные в отдельном файле:

C:\Users\Катя\Desktop\OpenKeyCrypt.pdf

Мастер проверки ЭЦП

Опции проверки
Опции проверки позволяют задать параметры, которые будут использоваться при проверке подписи электронного документа

Проверить также:

- Только сертификат издателя
- Полную цепочку сертификатов

Выберите параметры проверки:

- Полная проверка
 - Проверять срок действия сертификата
 - Проверять на отзыв (присутствие в списке отозванных сертификатов)
 - Проверять срок действия списка отозванных сертификатов
 - Не учитывать время ЭЦП при проверке сертификата на отзыв
 - Проверять срок действия закрытого ключа сертификата

Текущее время (GMT): 18 октября 2010 г. 9:10:02 GMT

< Назад Далее > Отмена

Мастер проверки ЭЦП

Выбор справочников для поиска сертификатов и Списков Отзыва
Для выполнения проверки ЭЦП производится поиск сертификатов подписавших и построение цепочки до корневого ЦС

Использовать следующие справочники для поиска сертификатов и СОС:

- Настроенные справочники сертификатов
- А также следующие сертификаты и СОС:

Владелец
CN=root,CN=CC,O=Urrync,ST=Taganrog,...
CN=root,CN=CC,O=Urrync,ST=Taganrog,...

Добавить...
Добавить СОС ...
Удалить
Показать...

< Назад Далее > Отмена

Разбор конфликтной ситуации (2)

Мастер проверки ЭЦП

Результат проверки ЭЦП
При проверке ЭЦП проверяются ЭЦП и сертификаты подписавших в соответствии с опциями проверки

Проверка ЭЦП № 1 сообщения в формате PKCS#7 (всего 1 ЭЦП)
Результат проверки ЭЦП: **OK**
Результат проверки цепочки: OK

Показать...

Дата и время установки ЭЦП: 18 октября 2010 г. 9:03:05 GMT
Идентификация сертификата:
Издатель сертификата: CN=root,CN=CC,O=Urrync,ST=Taganrog,
Серийный номер сертификата: 40:00:00:00:F1:71:D1:C8:4C:B8:5B
Найден сертификат:
Владелец сертификата: CN=User2,CN=User2,O=hotel,ST=Stavrop

< Назад Далее >

Мастер проверки ЭЦП

Завершение работы мастера проверки ЭЦП документа

Работа мастера проверки ЭЦП документа завершена.

Опции и результаты проверки ЭЦП:

Дата и время формирования протокола: 18 октября 201
Имя файла с данными: C:\Users\Катя\Desktop\OpenKeyC
Имя файла с ЭЦП: C:\Users\Катя\Desktop\OpenKeyCrypt.
Результат проверки: Подпись верна.


Можно распечатать результат проверки ЭЦП. Для этого нажмите соответствующие кнопки:

Распечатать... Протокол...

Расширенная информация о сертификате ЭЦП
Для завершения нажмите кнопку "Готово"

Запустить мастер ещё раз

< Назад Готово Отмена

A decorative horizontal bar spanning the width of the slide. It features a central yellow-to-orange gradient with blue bokeh circles on either side. Dotted white lines and white arrowheads point towards the center of the bar.

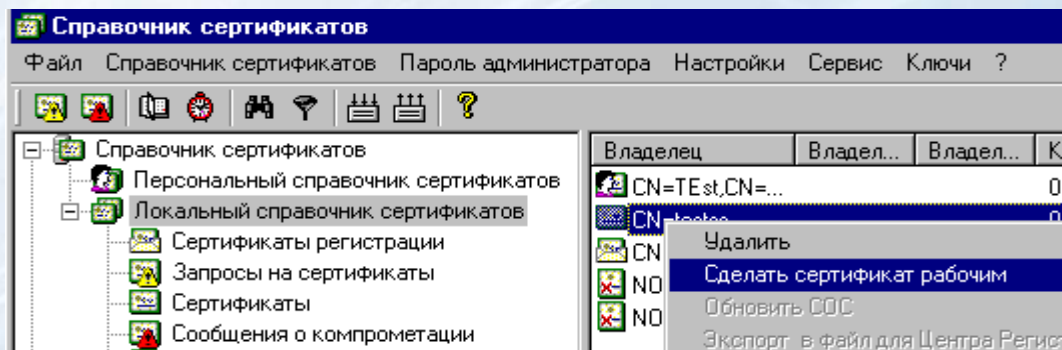
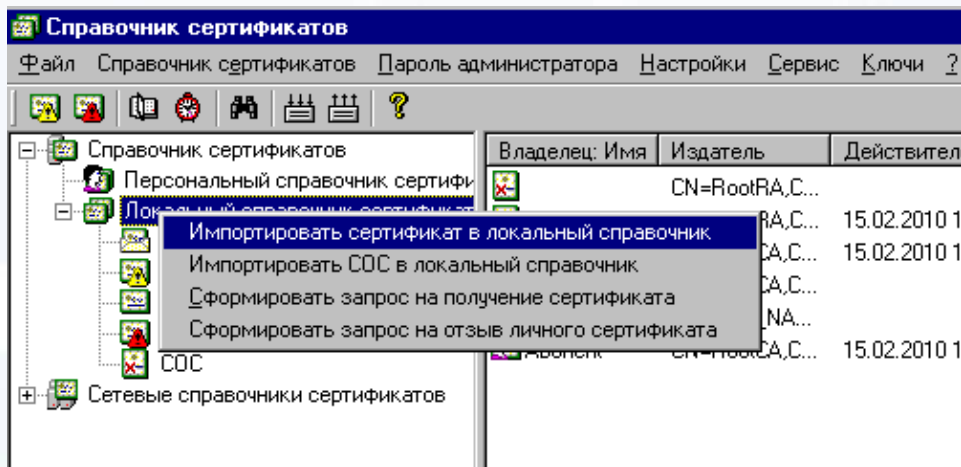
Верба-сертификат МВ Клиент

Поднятие справочника сертификатов

При первом запуске возможна настройка справочника сертификатов:

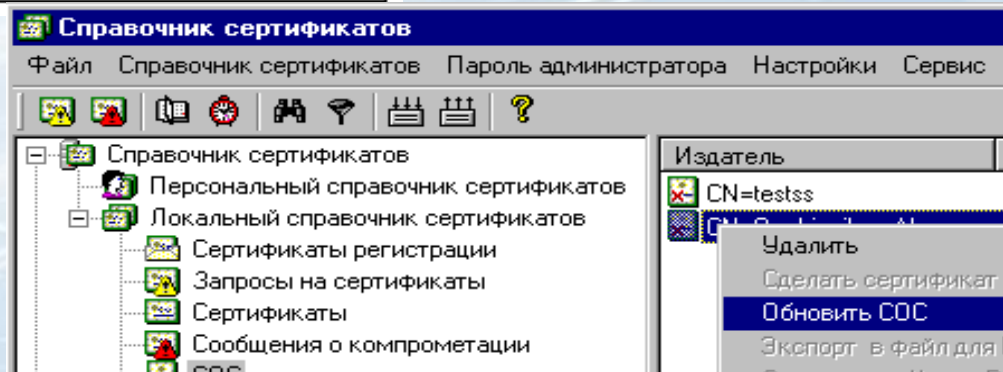
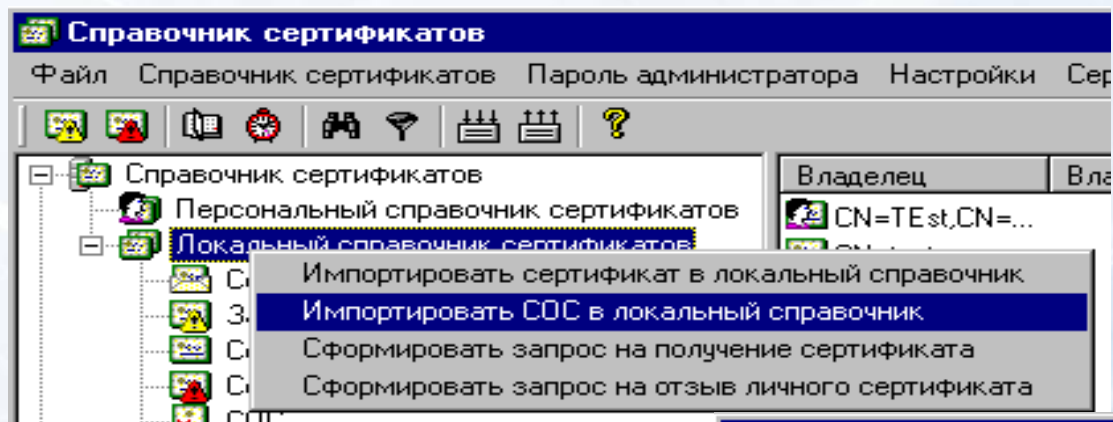
- ❖ По лицензии регистрации
- ❖ По копии баз справочника

Добавление сертификата

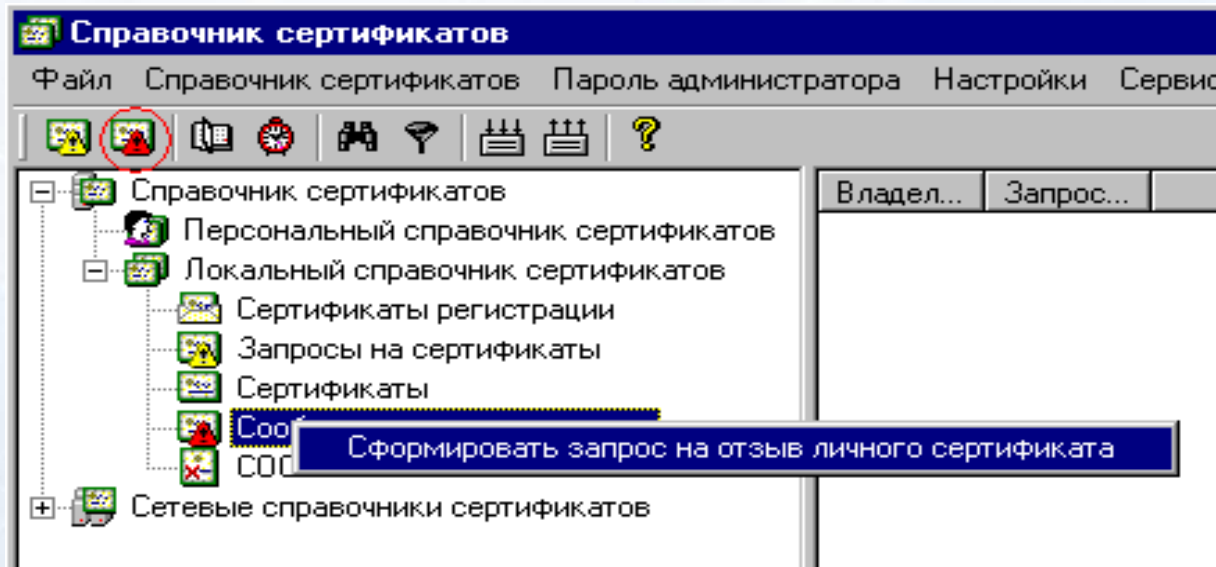


Обновление СОС

Добавление СОС из файла на внешнем носителе;
Обновление через файл с обновлениями;
Обновление СОС по сети, с использованием дополнения "Точка распространения СОС".



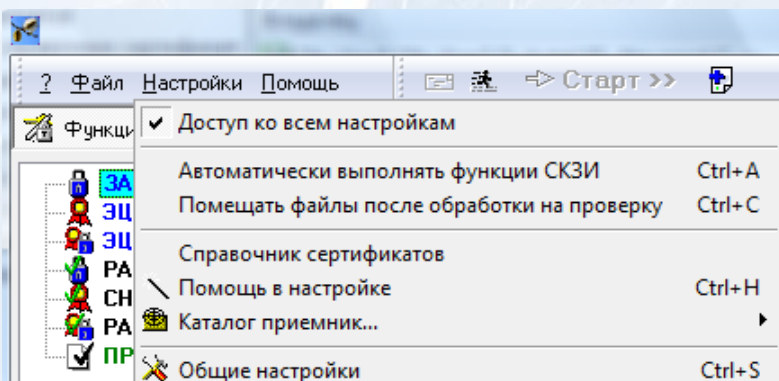
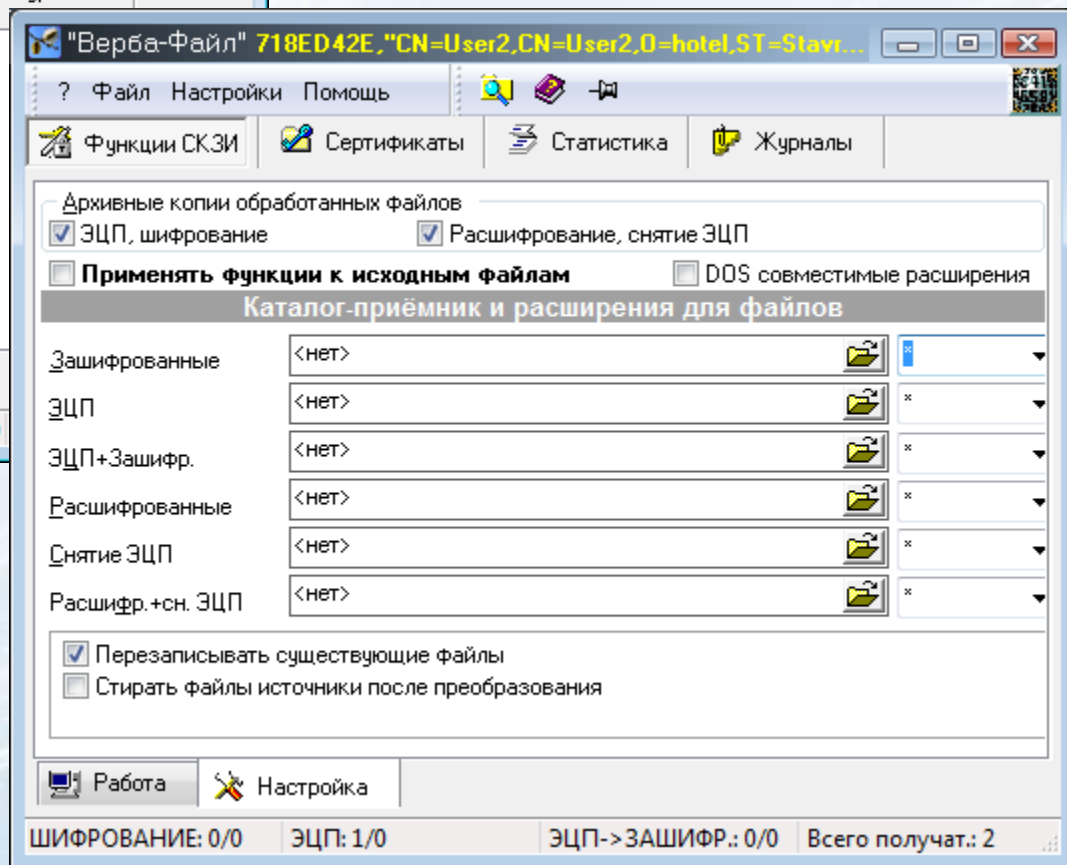
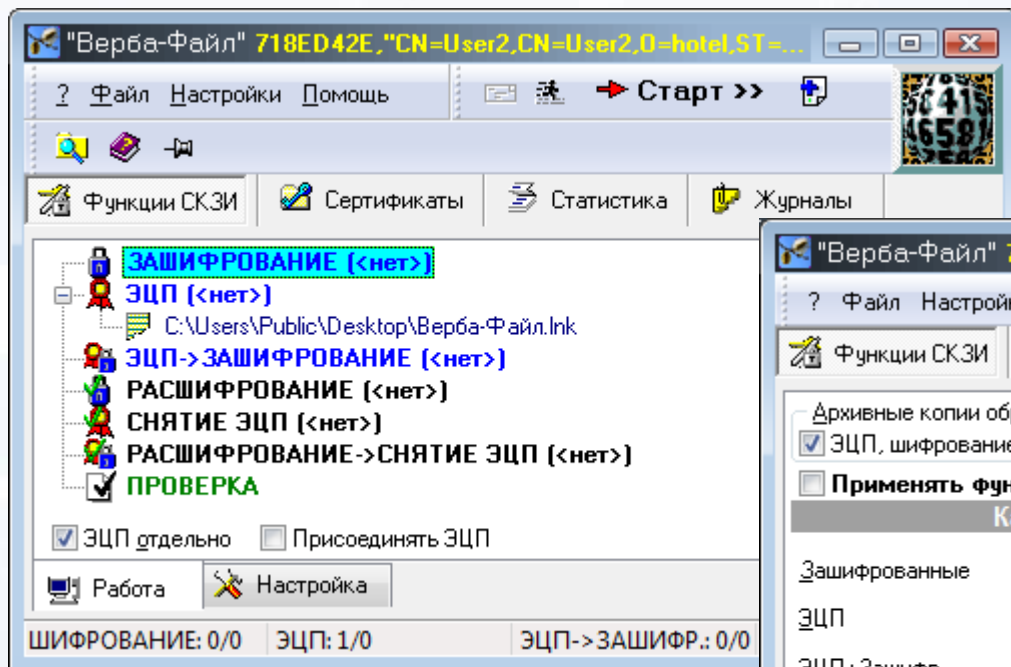
Отзыв сертификата



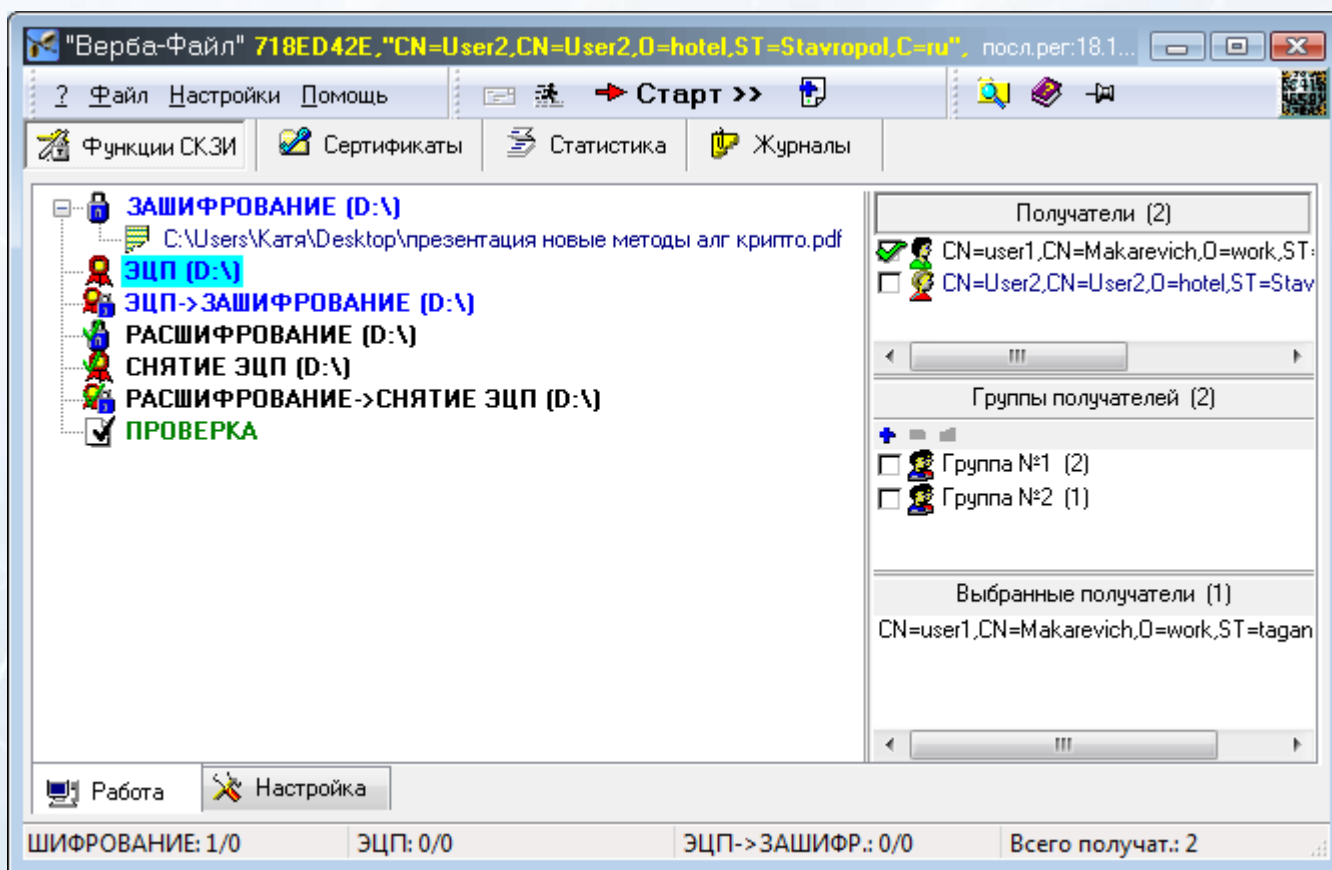


Верба-Файл

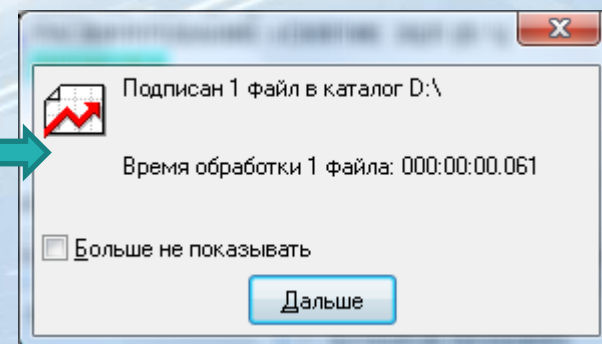
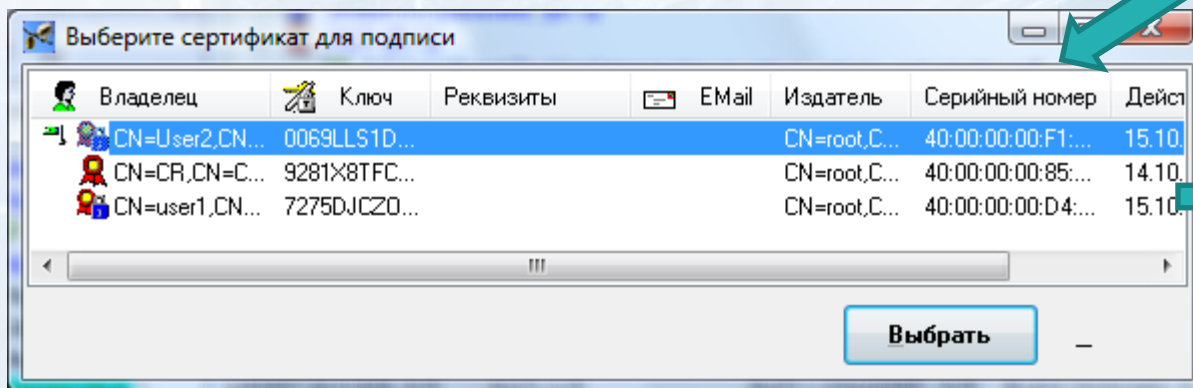
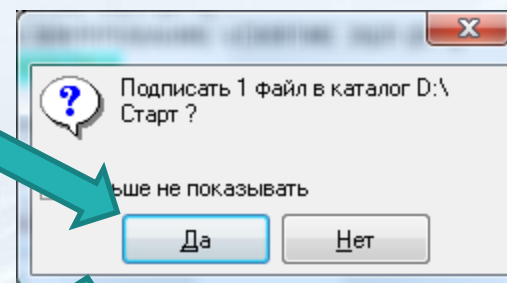
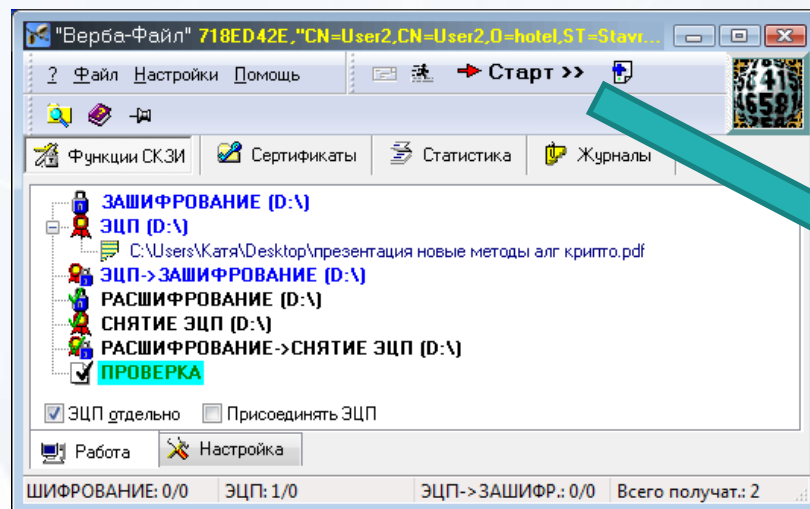
Интерфейс



Зашифрование



ЭЦП



Проверка

The screenshot displays the 'Verba-File' application window. The main pane shows a file explorer view of the 'D:\' drive, with a folder named 'ПРОВЕРКА' expanded to show a file 'C:\Users\Katyа\Desktop\GOCT_28147-89.htm.P7S'. This file has been scanned and found to contain two digital signatures (ЭЦП), both of which are verified (indicated by green checkmarks).

The verification report for the file is as follows:

Бланк проверки ЭЦП №1 Файл: C:\Users\Katyа\Desktop\GOCT_28147-89.htm.P7S

Бланк проверки ЭЦП файла

файл: C:\Users\Katyа\Desktop\GOCT_28147-89.htm.P7S
 Размер файла: 2,60 кбайт [2667 байт]
 ЭЦП отдельно, файл данных C:\Users\Katyа\Desktop\GOCT_28147-89.htm,
 Дата создания файла: 18 Октября 2010 г.
 Количество ЭЦП под файлом: 3
 Порядковый номер проверяемой ЭЦП: 1
 Серийный номер сертификата ключа ЭЦП: 40:00:00:00:D4:C5:97:96:4C:B8:57:6D:00:08:25:B1
 Дата и время простановки ЭЦП: 18.10.2010 11:33:34
 Результат проверки ЭЦП: Корректна

Данные о сертификате открытого ключа ЭЦП

Владелец: CN=user1,CN=Makarevich,O=work,ST=taganrog,C=ru
 Реквизиты:
 EMail:
 Издатель: CN=root,CN=CC,O=Urrync,ST=Taganrog,C=ru
 Серийный номер: 40:00:00:00:D4:C5:97:96:4C:B8:57:6D:00:08:25:B1
 Время начала действия сертификата: 15.10.2010 13:30:34
 Время конца действия сертификата: 14.10.2015 23:59:00

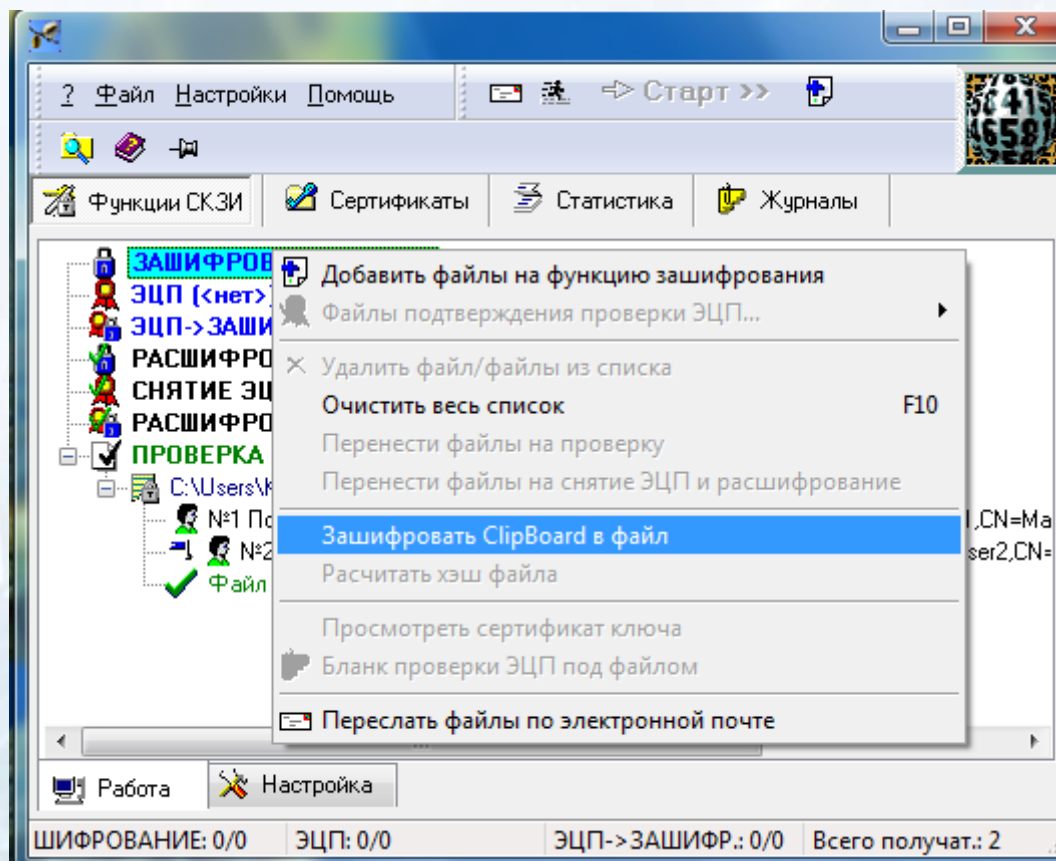
Дата проверки: 18 Октября 2010 г.

Подписи

Первой стороны _____ Второй стороны _____

Независимого эксперта _____

Шифрование содержимого буфера



ClipBoard.clp

Вычисление ХЭШ

The screenshot shows the 'Verba-File' application window. The title bar indicates the user is 'User2' on a system named 'hotel'. The interface includes a menu bar with 'Файл', 'Настройки', and 'Помощь'. Below the menu bar are tabs for 'Функции СКЗИ', 'Сертификаты', 'Статистика', and 'Журналы'. The main area displays a file explorer view of the 'D:\' drive, with a context menu open over a file named 'презентация новые методы алг крипто.pdf'. The menu options include 'Добавить файлы на функцию зашифрования', 'Удалить файл из списка', and 'Расчитать хэш файла'. A secondary window titled 'Получатели (2)' is also visible, showing a list of recipients.

The screenshot shows a small window titled 'Хэш файла "презентация новые методы алг крипто.pdf"'. It displays the calculated hash for the file. The window contains the following text:

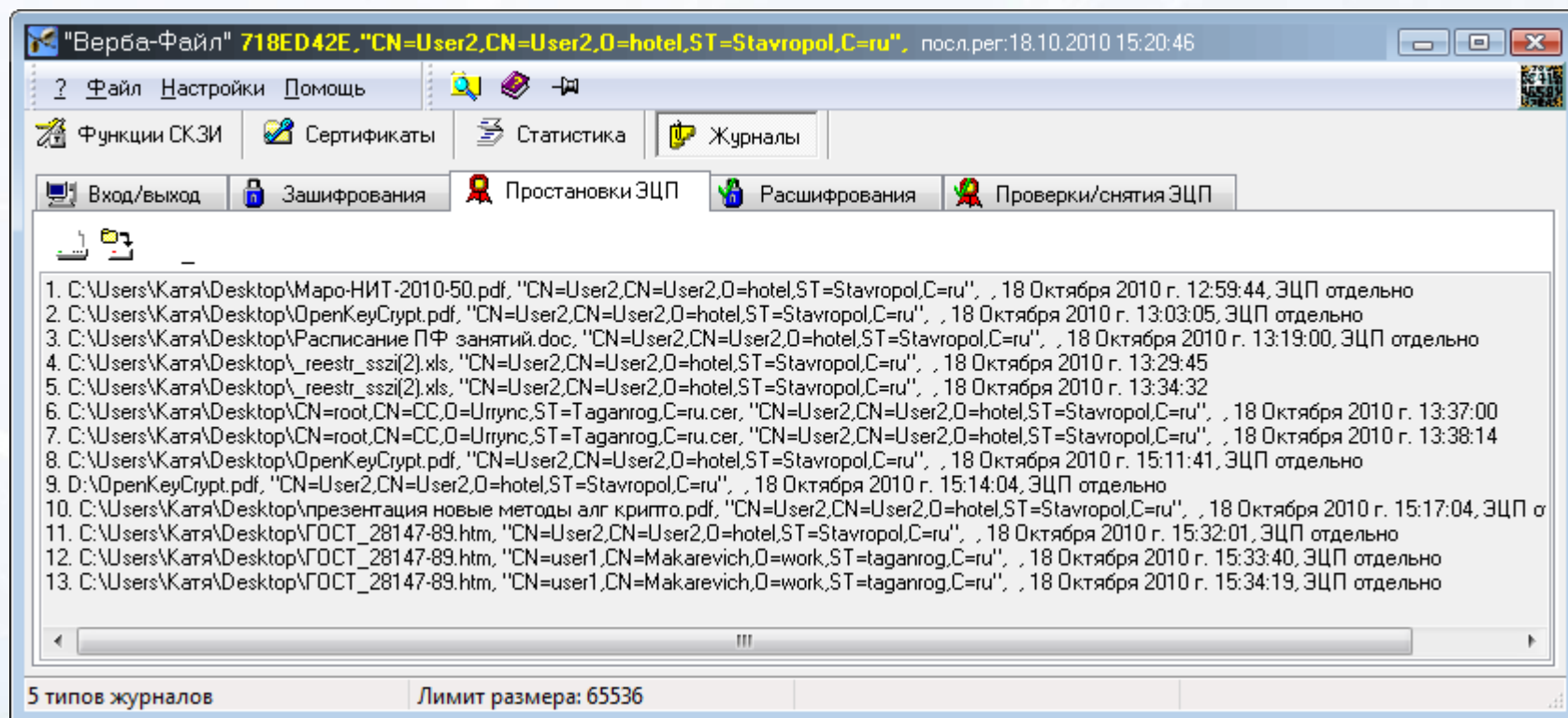
Функции СКЗИ "Верба-OW"
 Файл "C:\Users\Катя\Desktop\презентация новые методы алг крипто.pdf"

Хэш файла:

```

0-----7      8-----15
5B B1 91 23 7B 06 86 24 - 19 4F 2E 04 6C FD 84 07
20 30 23 AB FD 6F 87 0B - B3 20 13 1C 63 11 84 CF
    
```

Протоколирование



C:\«пользователь»\AppData\Roaming\MDPREI\Verba-File\JOU

Обработка командных скриптов

Команды:

TO <список ключей> — установить получателей зашифрованного файла

CRYPT <имя файла> или **ENCRYPT** <имя файла> — зашифровать файл

SIGN <имя файла> — подписать файл;

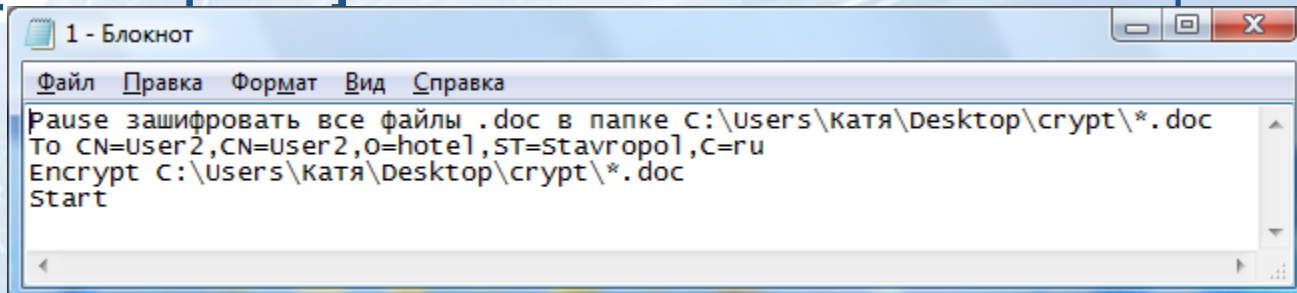
UNCRYPT <имя файла> или **DECRYPT** <имя файла> — расшифровать файл

UNSIGN <имя файла> — снять ЭЦП с файла с проверкой

START или **BEGIN** — начать процесс обработки

EXIT или **CLOSE** — закрыть программу

PAUSE [сообщение] — остановить выполнение скрипта



```
1 - Блокнот
Файл  Правка  Формат  Вид  Справка
Pause зашифровать все файлы .doc в папке C:\Users\катя\Desktop\crypt\*.doc
To CN=User2,CN=User2,O=hotel,ST=Stavropol,C=ru
Encrypt C:\Users\катя\Desktop\crypt\*.doc
Start
```



Вопросы?

**Южно-Российский региональный учебно-научный центр по
проблемам информационной безопасности ЮФУ**