AMB Group

Центр Защиты Ресурсов Информационных Систем

ЦЕЗАРИС

Инфраструктура открытых ключей

Инструкция по эксплуатации

Редакция 1.0

АННОТАЦИЯ

Данный документ содержит описание криптопровайдера **"*CESARIS Cryptographic Service Provider* ©"**, который входит в состав проекта **Центр Защиты Ресурсов Информационных Систем (ЦЕЗАРІС).**

Документ предназначен для пользователей и прикладных программистов, разрабатывающих собственные приложения.

СОДЕРЖАНИЕ

1. Описание криптопровайдера CESARIS-CSP

Разработчик: АМБ-групп.
Криптопровайдер: ***"CESARIS Cryptographic Service Provider ©"***
Сокращенное название: ***"CESARIS CSP"***

1.1. Назначение

CESARIS-CSP (**далее - Криптопровайдер**) предназначен для:

- наложения и проверки электронной цифровой подписи (ЭЦП) на электронных документах при обмене ими между пользователями, в соответствии с отечественными стандартами ГОСТ 34.311-95, ГОСТ 34.310-95 и ДСТУ 4145-2002;
- обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования, в соответствии с ГОСТ 28147-89;
- контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированного изменения или от нарушения правильности функционирования;
- управления ключевыми элементами системы в соответствии с регламентом средств защиты.

1.2.Основные характеристики

Длина ключей электронной цифровой подписи:

- 512, 1024 бита при использовании алгоритма ГОСТ 34.310-95;
- 163 - 431 бит при использовании алгоритма ДСТУ 4145-2002 и полиномиального базиса;
- 173 - 431 бит при использовании алгоритма ДСТУ 4145-2002 и оптимального нормального базиса.

Длина ключей, используемых при шифровании:

- симметричный ключ - 256 бит при использовании алгоритма ГОСТ 28147-89;
- ассиметричное шифрование – 1024 - 4096 бит на базе алгоритма RSA.

Хеширование:

- длина значения хэш-функции по ГОСТ 34.311-95 – 256 бит.

Типы ключевых носителей:

- файл (на любом носителе);
- USB E-Token (производитель Aladdin Knowledge Systems Ltd, http://www.aladdin.com);
- смарт-карты ASECard Crypto с ридером ASEDrive IIIe (производитель Athena, www.athena-scs.com);
- смарт-карты Axalto CyberFlex, Axalto CryptoFlex с ридерами Reflex та E-gate (производитель Axalto Inc, http://www.axalto.com);
- смарт-карты GemPlus (производитель GemPlus, http://www.gemplus.com);
- USB-токены MiniKey, смарт-карты PrivateCard (производитель Algorithmic Research, http://www.arx.com);
- JAVA-смарт-карты (производитель Oberthur Card Systems, www.oberthurcs.com).

1.3. Реализуемые алгоритмы

Алгоритм выработки значения хэш-функции реализован в соответствии с требованиями ГОСТ 34.311-95 "Информационная технология. Криптографическая защита информации. Функция хеширования".

Алгоритмы формирования и проверки ЭЦП реализованы в соответствии с требованиями:

- ГОСТ 34.310-95 "Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма ";
- ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння"

Алгоритм зашифрования/расшифрования данных реализован в соответствии с требованиями ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".

При генерации закрытых и открытых ключей обеспечена возможность генерации с различными параметрами p, q, a в соответствии с ГОСТ 34.310-95.

При выработке значения хэш-функции и шифровании обеспечена возможность использования различных узлов замены в соответствии с ГОСТ 34.311-95 и ГОСТ 28147-89.

1.4. Состав программного обеспечения

Криптопровайдер представляет собой набор библиотек, зарегистрированных в операционной системе (ОС):

- csrs804csp.dll, csrs804ex.dll – криптопровайдер ГОСТ 34.310-95 & RSA;
- csrs805csp.dll, csrs805ex.dll – криптопровайдер ДСТУ 4145-2002 (полиномиальный базис) & RSA;
- csrs806csp.dll, csrs806ex.dll – криптопровайдер ДСТУ 4145-2002 (полиномиальный базис) & ECDH;
- csrs807csp.dll, csrs807ex.dll – криптопровайдер ДСТУ 4145-2002 (оптимальный нормальный базис) & RSA;
- csrs808csp.dll, csrs808ex.dll – криптопровайдер ДСТУ 4145-2002 (оптимальный нормальный базис) & ECDH;
- cesarisstore.dll – модуль хранилища;
- cesaris_dispatch.dll, cesaris_virtual.dll – модули поддержки работы с носителями с использованием интерфейса PKCS#11.
- cesaris_file.dll - модуль поддержки файловых носителей;
- cesaris_aladdin.dll - модуль поддержки носителей Aladdin;
- cesaris_athena.dll - модуль поддержки носителей Athena;
- cesaris_axalto.dll - модуль поддержки носителей Axalto;
- cesaris_gemplus.dll - модуль поддержки носителей GemPlus;
- cesaris_oberthur.dll - модуль поддержки носителей Oberthur Card Systems;
- cesaris_ikey.dll - модуль поддержки носителей iKey SafeNet;
- cesaris_arl.dll - модуль поддержки носителей Algorithmic Research;
- cesaristsp.dll – COM-объект для работы с TimeStamp;
- cesariscfg.cpl – элемент панели управления Windows.

Криптопровайдер подписан цифровой подписью компании Microsoft, а указанные библиотеки регистрируются в операционной системе (ОС) Windows пользователя.

В состав инсталляционного пакета Криптопровайдера также входит утилита работы с носителями ключевой информации «Менеджер PKCS#11» описанная в п.3.1.

Операционные системы

CESARIS CSP функционирует в следующих операционных системах:

- Windows 2000;
- Windows XP;
- Windows Server 2003.

2. Инсталляция криптопровайдера

Для установки криптопровайдера пользователь должен иметь **права администратора** на компьютере.

1. Запустить инсталляционный пакет (рис.2-1) и выбрать язык общения при инсталляции.

2. Выбрать тип установки и рабочий каталог.

Тип *"Стандартная"* предусматривает инсталляцию на компьютер пяти криптопровайдеров (ГОСТ 34.310-95 и ДСТУ 4145-2002), модулей PKCS#11, поддержку файлового носителя ключей, а также документации.

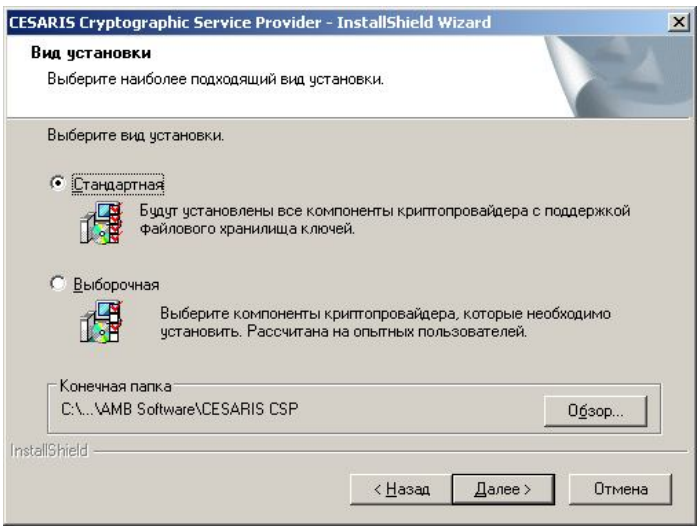


Рис.2-1

3. В случае необходимости дополнительно установить (или исключить) компоненты выберите тип установки *"Выборочная"*. При этом вы сможете добавить поддержку работы с другими доступными носителями ключей. Также в рабочий каталог записываются примеры использования криптопровайдера на языке С.

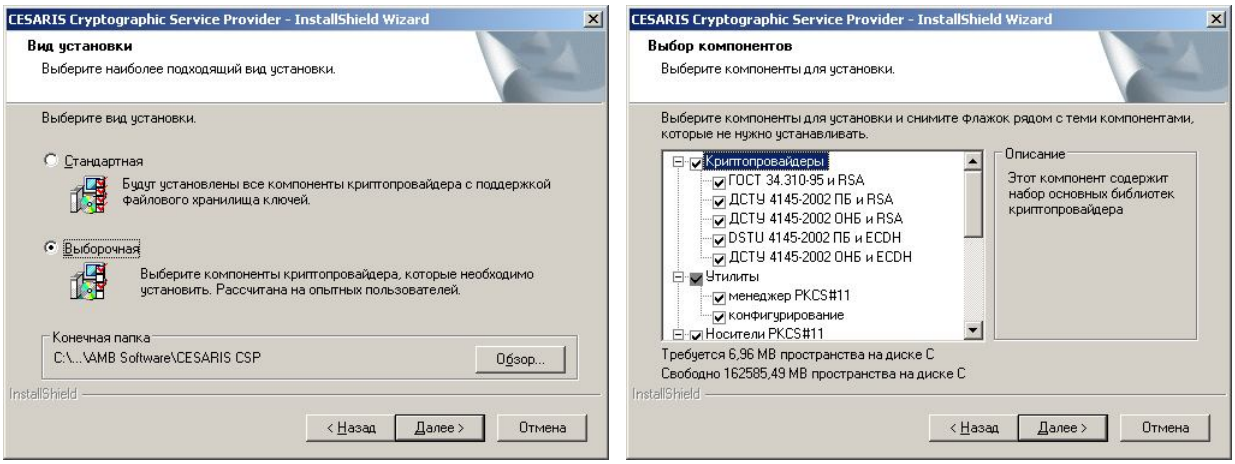


Рис.2-2

4. После установки компонентов появится запрос (рис.2-3) создать новый файловый носитель на диске (если его поддержка устанавливалась). Вы можете отказаться, если такой уже создан.

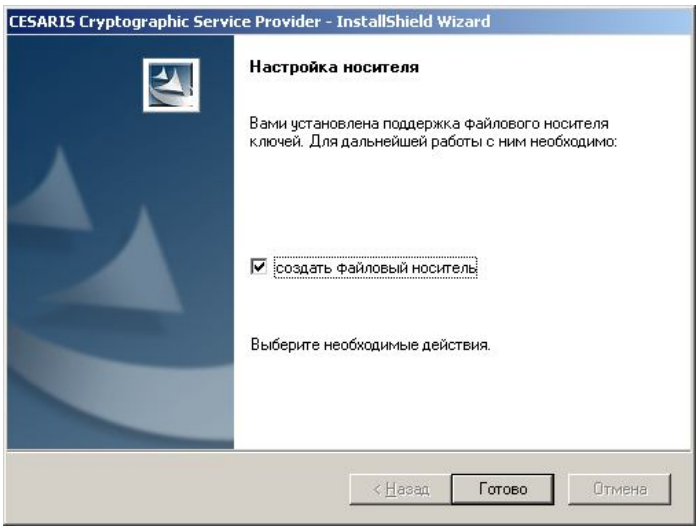


Рис.2-3

5. Запускается утилита настройки криптопровайдера.

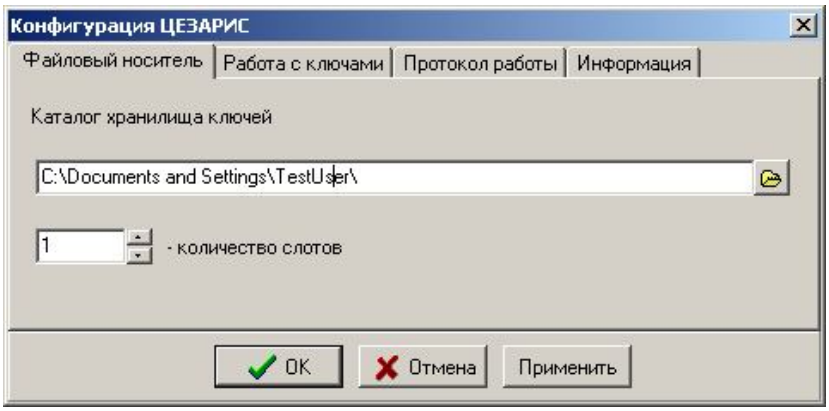
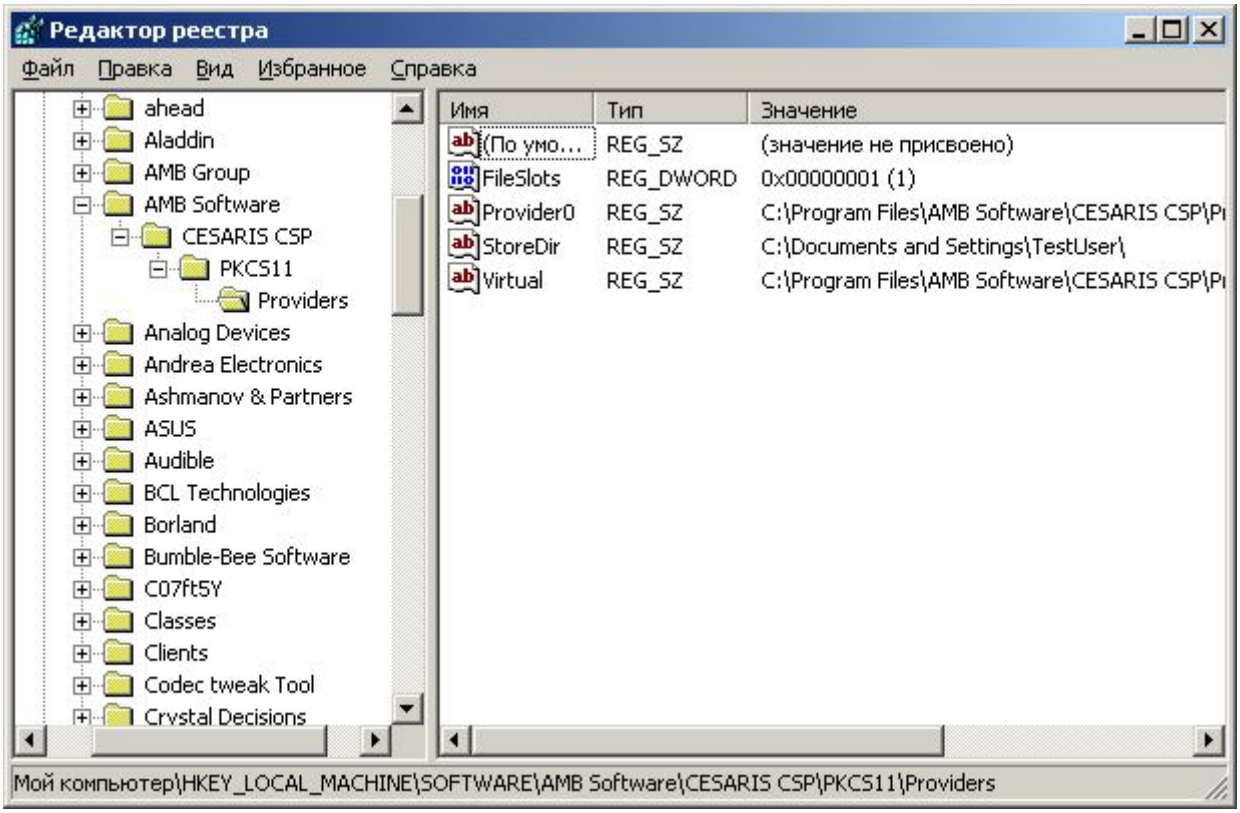


Рис.2-4

Настройка файлового носителя (рис.2-4) заключается в выборе каталога, где будут размещаться ключевые файлы token*.dat, и их количества (количества слотов). По умолчанию, установлен рабочий каталог текущего пользователя и один слот.

Имя каталога сохраняется в ключах реестра:
- HKEY_CURRENT_USER\Software\ABM Software\CESARIS CSP\PKCS11\ Providers\StoreDir;
- HKEY_LOCAL_MACHINE\ Software\ ABM Software\CESARIS CSP \PKCS11\Providers\StoreDir.

Количество файлов (слотов) сохраняется в ключе реестра:
- HKEY_LOCAL_MACHINE\ Software\ ABM Software\CESARIS CSP \PKCS11\Providers\ FileSlots.



В случае установки на сервер необходимо выбрать каталог, доступный для чтения-записи серверному процессу.

Кроме настройки файлового носителя утилита позволяет:

- установить временную задержку запроса пароля ключа (рис.2-5).

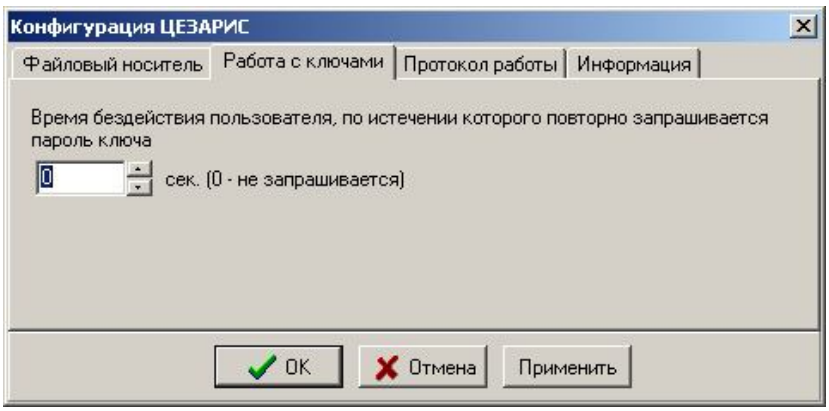


Рис.2-5

- включить/отключить протоколирование (рис.2-6). Этот режим рекомендуется только на стадии отладки программного обеспечения.

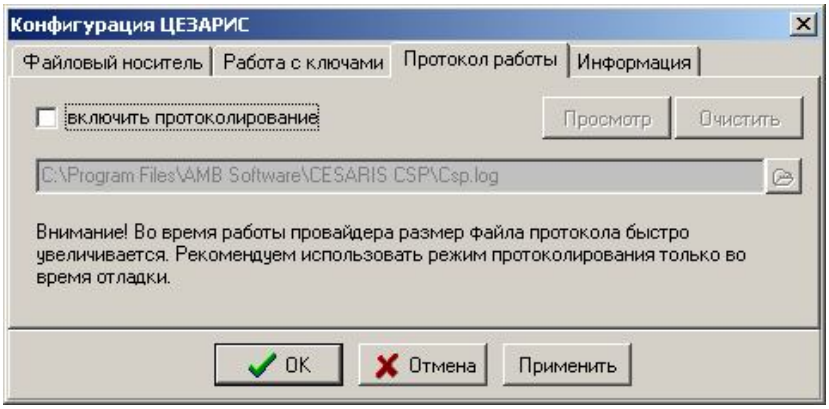


Рис.2-6

- просмотреть список установленных криптопровайдеров (рис.2-7)

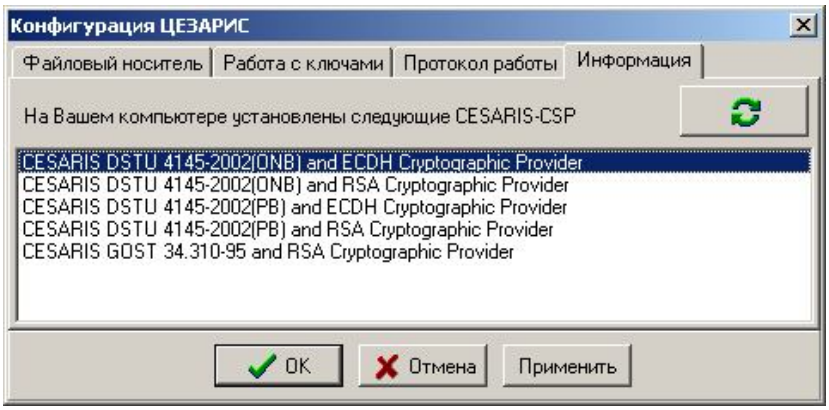


Рис.2-7

6. Если вы выбрали опцию создания файлового носителя (рис.2-3), после настройки криптопровайдера запустится соответствующая утилита (рис.2-8)

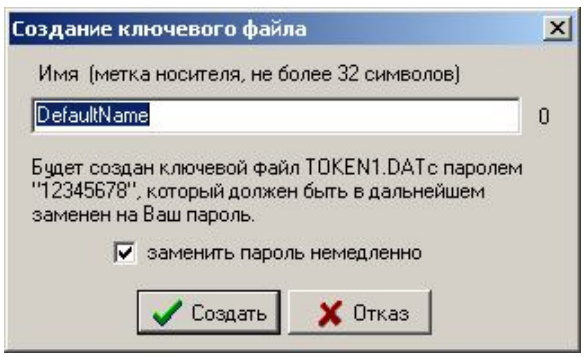


Рис.2-8

При создании файлового носителя необходимо выбрать метку носителя, а также установить *собственный пароль* для работы с ключами.

По умолчанию выбирается имя текущего пользователя. Можно изменить значение метки на любое другое, но не более 32 символов.

Если хотите установить свой пароль сразу после создания файлового носителя, необходимо выбрать опцию *"заменить пароль немедленно"*.

После нажатия кнопки *"Создать"* проверяется наличие в каталоге раннее созданного файла. При этом выдается предупреждение, что файл уже существует, и запрос подтвердить (или отказаться от процедуры) создания нового файла (рис.2-9).

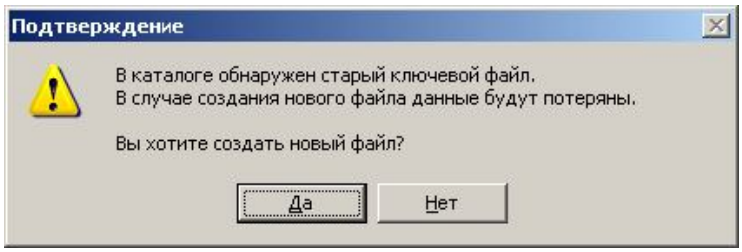


Рис.2-9

В случае подтверждения будет создан файл с начальным паролем "12345678" и появится запрос ввода нового пароля (ПИНа) (рис.2-10).

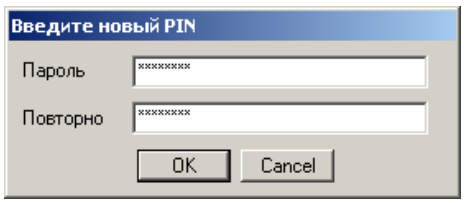


Рис.2-10

Ограничения:
Длина пароля от 6 до 255 символов.

Пароль не должен содержать двух одинаковых символов подряд или три одинаковых символа во всей строке. Также не допускается использование последовательностей клавиш раскладки клавиатуры для составления пароля (типа - qwerty).

В случае ошибки во время смены пароля файл останется с начальным паролем "12345678".

7. Провайдер готов к работе.

3. Использование утилит

В комплект инсталляционного пакета криптопровайдера входят утилиты для создания файлового носителя (токена) и работы с объектами на подключенных устройствах, поддерживающих API-интерфейс PKCS#11.

Работа с утилитой создания файлового носителя описана в разделе 2.

3.1. Менеджер PKCS#11

Менеджер используется для инициализации носителей (токенов), смены паролей и просмотра/удаления объектов. Описание интерфейса PKCS#11 дано в [2].

Общий вид окна утилиты показан на рисунке 3-1.

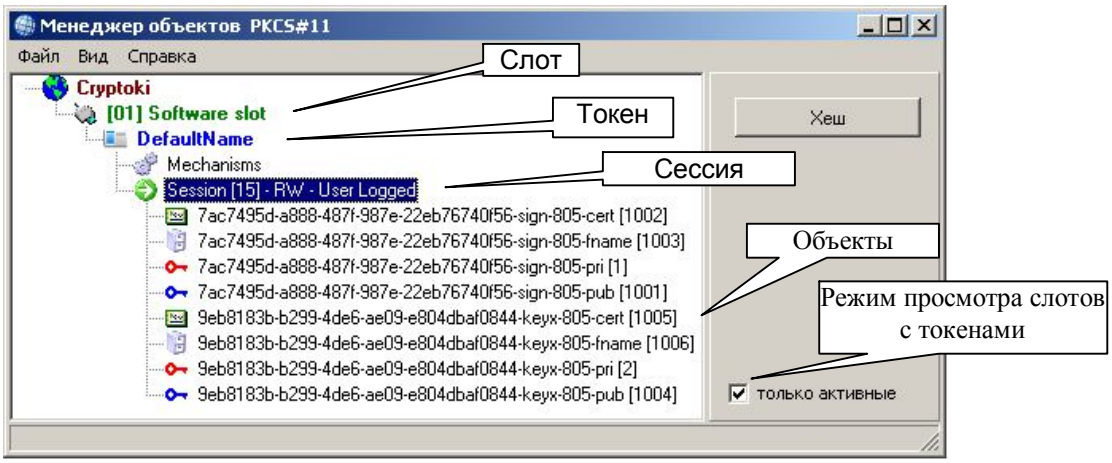


Рис.3-1

Каждый узел дерева имеет собственное меню, которое соответствует перечню функций интерфейса PKCS#11 для данного класса.

В качестве примера на рисунке 3-2 показано меню сессии.

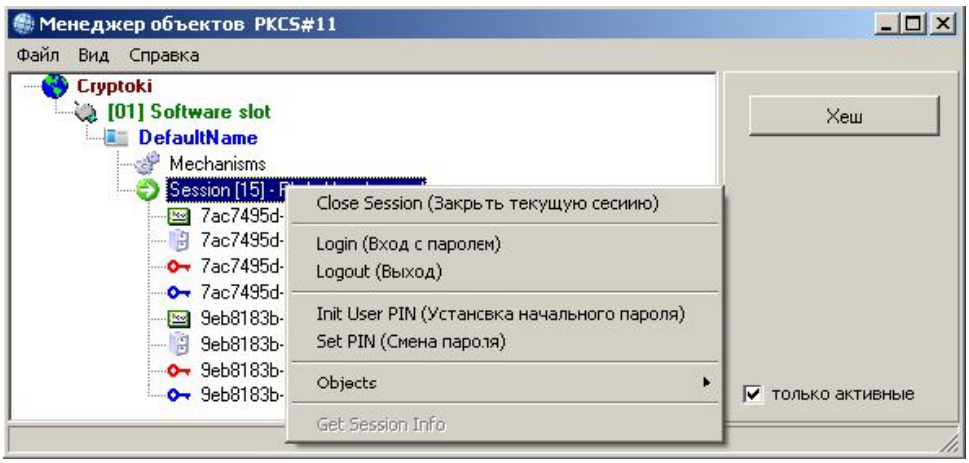


Рис.3-2

3.1.1. Инициализация токена

Инициализация токена производится:

- во время создания нового файла ключей (для неактивного слота меню – *"Создать токен"*);
- при необходимости очистить данные и пароли в существующем токене.

Процедура выполняется в 2 этапа:

1 этап инициализация токена с установкой пароля администратора (Security Officer, SO)

2 этап установка начального пароля доступа для пользователя (User).

Для инициализации токена необходимо выполнить пункт меню активного токена *"Init Token"* или пункт меню неактивного слота *"Create Token"*. При этом вводится метка токена (до 32 символов) и пароль администратора (SO PIN).

Для установки начального пароля пользователя необходимо двойным щелчком (или через меню токена *"Open RW-session"*) открыть RW-сессию (Read-Write, для чтения и записи) и выполнить пункт меню сессии "Init User PIN". При этом вводится пароль администратора и новый пароль пользователя.

3.1.2. Аутентификация (login)

При открытии дерева объектов пользователь получает доступ на просмотр и удаление общедоступных (public) объектов. При этом сессия содержит надпись *"Not logged"* и иконку красного цвета.

Для получения доступа к приватным объектам необходимо выполнить пункт меню сессии *"Login"*, выбрать тип пользователя и ввести пароль. После успешной проверки пароля сессия будет содержать надпись *"USER logged" ("SO logged")* и иконку зеленого цвета.

В случае аутентификации в качестве SO доступ к приватным объектам будет заблокирован. Данный тип пользователя необходим только для проведения начальной установки пароля пользователя.

3.1.3. Смена пароля доступа

Для смены пароля необходимо провести аутентификацию (*"Login"*) и выполнить пункт меню сессии *"Set PIN"*.

3.1.4. Просмотр свойств объектов

Просмотр свойств объекта производится с помощью двойного щелчка мышкой или через меню объекта (рис. 3-3).

Окно свойств (атрибутов, ATTRIBUTES) объекта показывает заголовок, размер объекта и общие атрибуты для всех объектов PKCS#11:

- CKA_CLASS – класс объекта;
- CKA_LABEL – метка объекта
- CKA_TOKEN – признак того, что объект сохранен на токене (не сессионный);
- CKA_PRIVATE – доступ к объекту только после аутентификации;
- CKA_MODIFIABLE – разрешение модификации объекта.

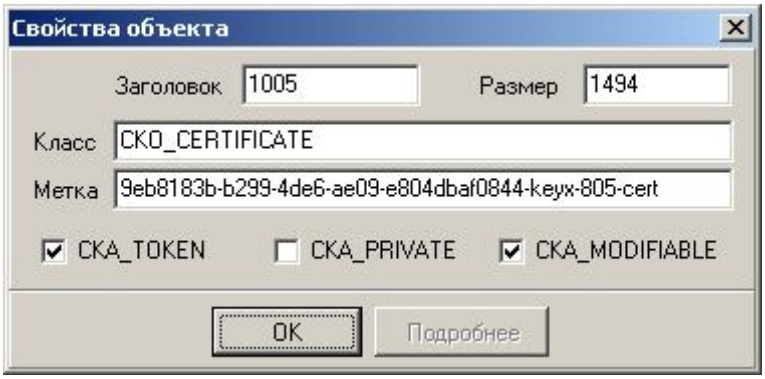


Рис.3-3

Для объектов типа СЕРТИФИКАТ (CKO_CERTIFICATE[1]) в меню есть дополнительный пункт *"View X.509 certificate"* (рис.3-4) для просмотра содержания сертификата средствами ОС Windows.

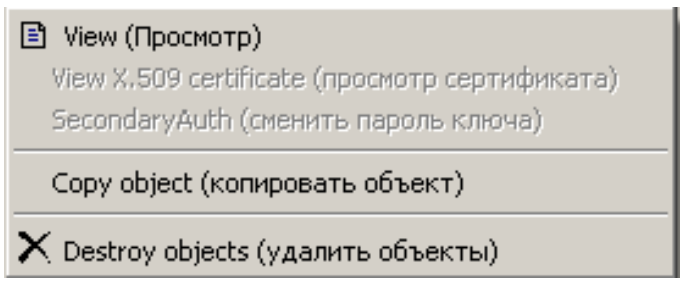


рис.3-4

3.1.5. Копирование объектов

Копирование выполняется только для объектов типа CKO_DATA с помощью пункта меню "Copy object" (рис.3-4).

После этого объект можно вставить на любой токен, выполнив пункт меню сессии "Objects/Insert object".

3.1.6. Удаление объектов

Удаление одного или нескольких объектов выполняется с помощью пункта меню "Destroy objects" (рис.3-4) или кнопкой Del.

Возможно удаление сразу нескольких выделенных в дереве объектов.

3.1.7. Дублирование ключей и сертификатов

Дублирование ключей предназначено для обеспечения возможности возобновления работы с ключами в случае утери оригиналов вследствие выхода из строя носителя или оборудования, за исключением случаев компрометации ключей. Дублирование ключей предусмотрено службой дублирования ключей ЦСК и является обязательной процедурой для ключей Центра сертификации в соответствии с Общим описанием ЦСК и Инструкциями по обращению с ключевыми данными.

[1] типы объектов согласно PKCS#11

Копии ключей создаются в защищенном виде по стандарту PKCS#12 на контролируемых носителях. Экспорт и импорт сертификатов а также, при необходимости, персональных ключей и других связанных объектов (открытый ключ, дружественное имя) на резервные носители выполняется средствами утилиты «Менеджер PKCS#11».

1) Экспорт сертификатов и ключей из хранилища операционной системы Windows.

Выполняется стандартными средствами ВЕБ-броузера, который поддерживает работу с сертификатами формата X.509, например Internet Explorer версий 5 и старше по пути: Tools-> Internet options-> Contetnt-> Certificates, кнопкой «Экспорт» на выбранном сертификате:

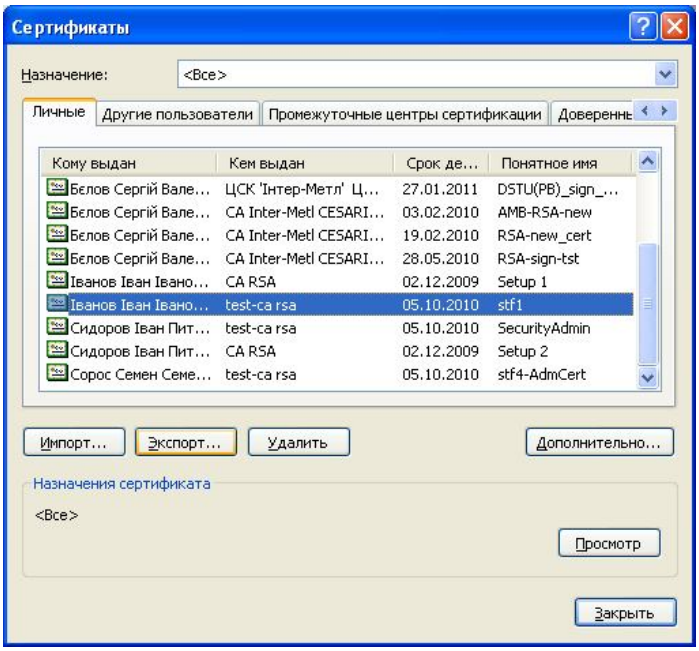


Рис.3.5

Далее следует выполнить действия, предложенные «Мастером экспорта сертификатов».

Экспорт сертификата происходит в любой заданный файл без пароля, для экспорта сертификата вместе с персональным ключом

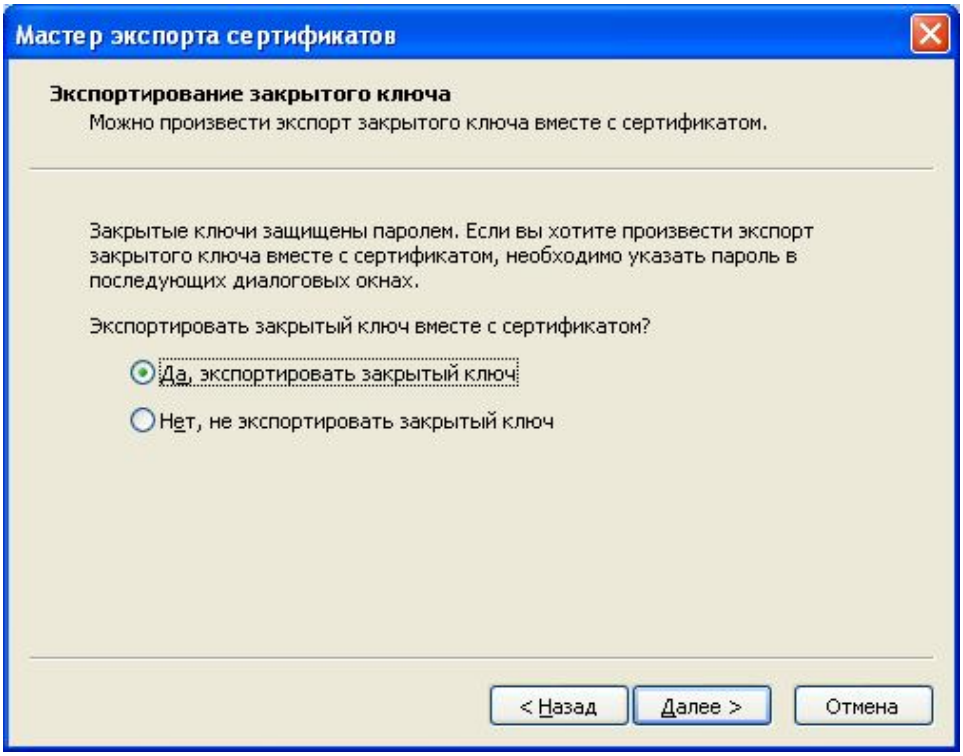


Рис.3.6

лицо - владелец сертификата обязательно задает пароль (не менее 6 символов) и результирующий файл (.pfx) будет зашифрован на этом пароле (рис. 3.7-1 ? 3.7-3):

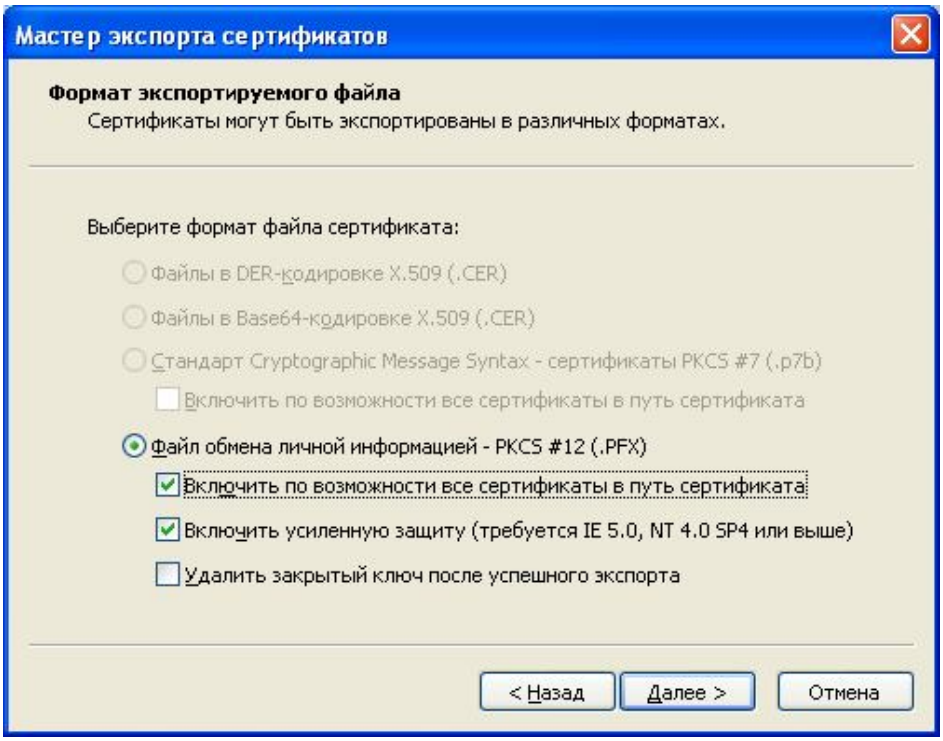


Рис.3.7-1

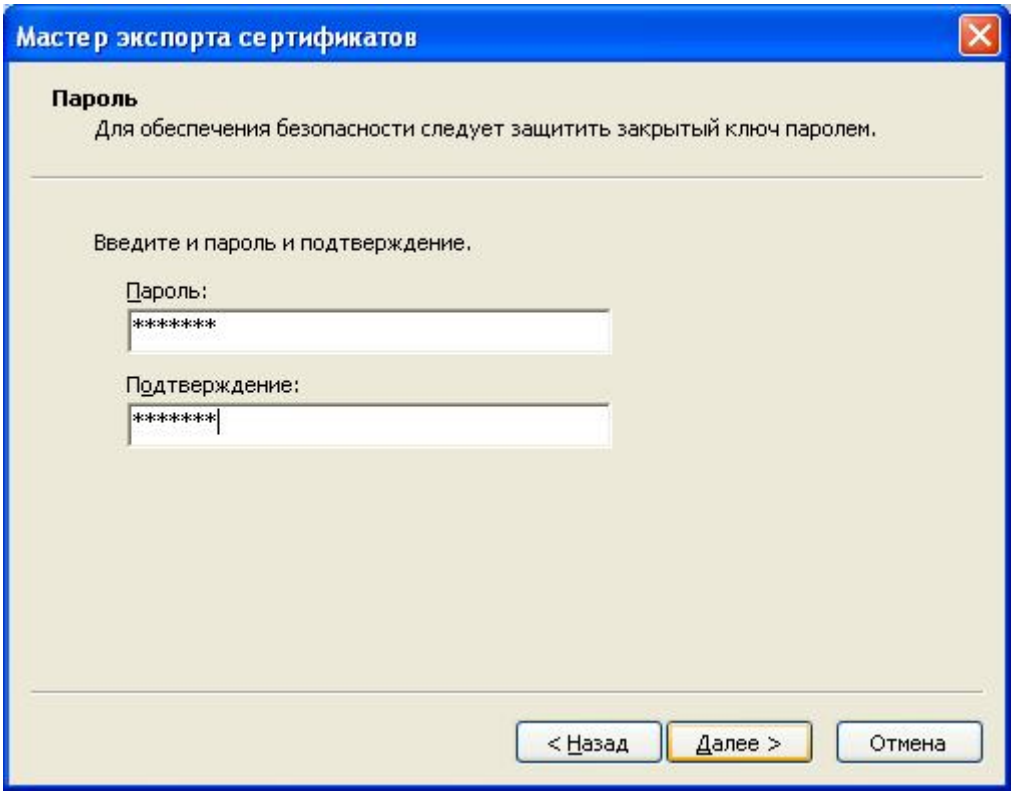


Рис.3.7-2

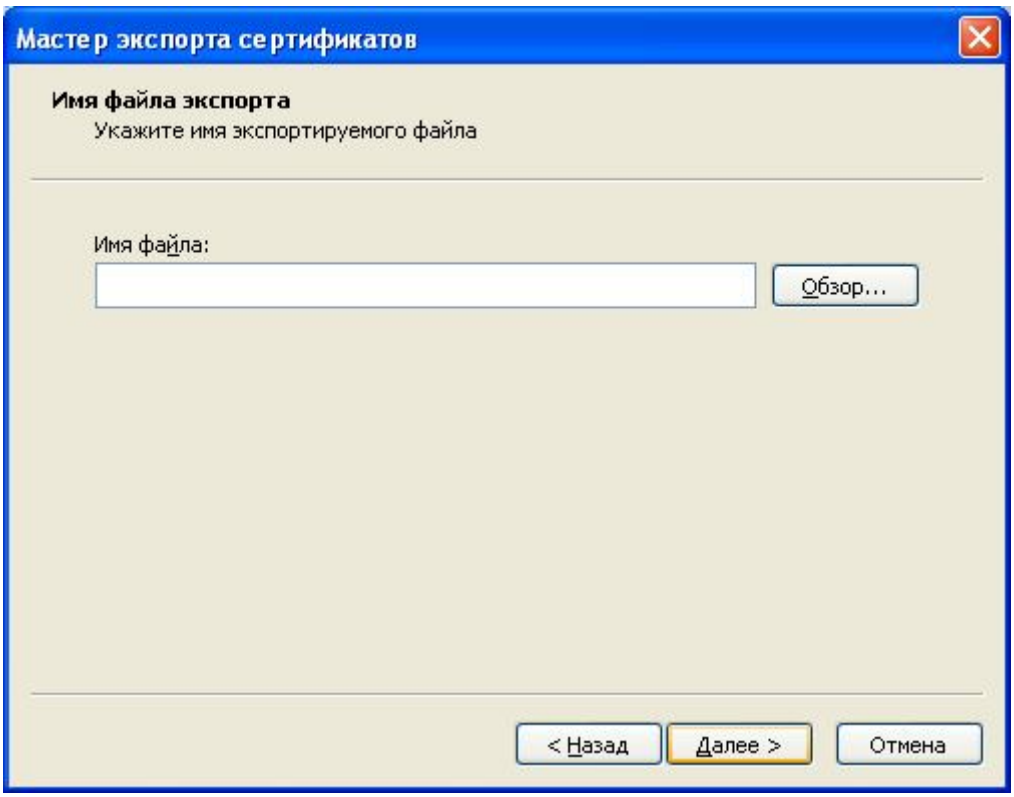


Рис.3.7-3

В дальнейшем для использования экспортированного сертификата и личного ключа необходимые данные устанавливаются на компьютер из полученного файла формата PKCS#12 с расширением .PFX с помощью того же «Мастера экспорта сертификатов».

2) Экспорт сертификатов и ключей с одной смарт-карточки на другую

Для экспорта сертификата из защищенного носителя, которым является смарт-карта или файловый токен, на другой носитель (смарт–карту, файловый токен), необходимо в окне менеджера PKCS#11 (далее - менеджер), который входит в состав инсталляции криптопровайдера, выделить необходимый для экспорта элемент - сертификат и нажать на нем правой клавишей мыши и далее в контекстном меню выбрать пункт “Export to SIM”:

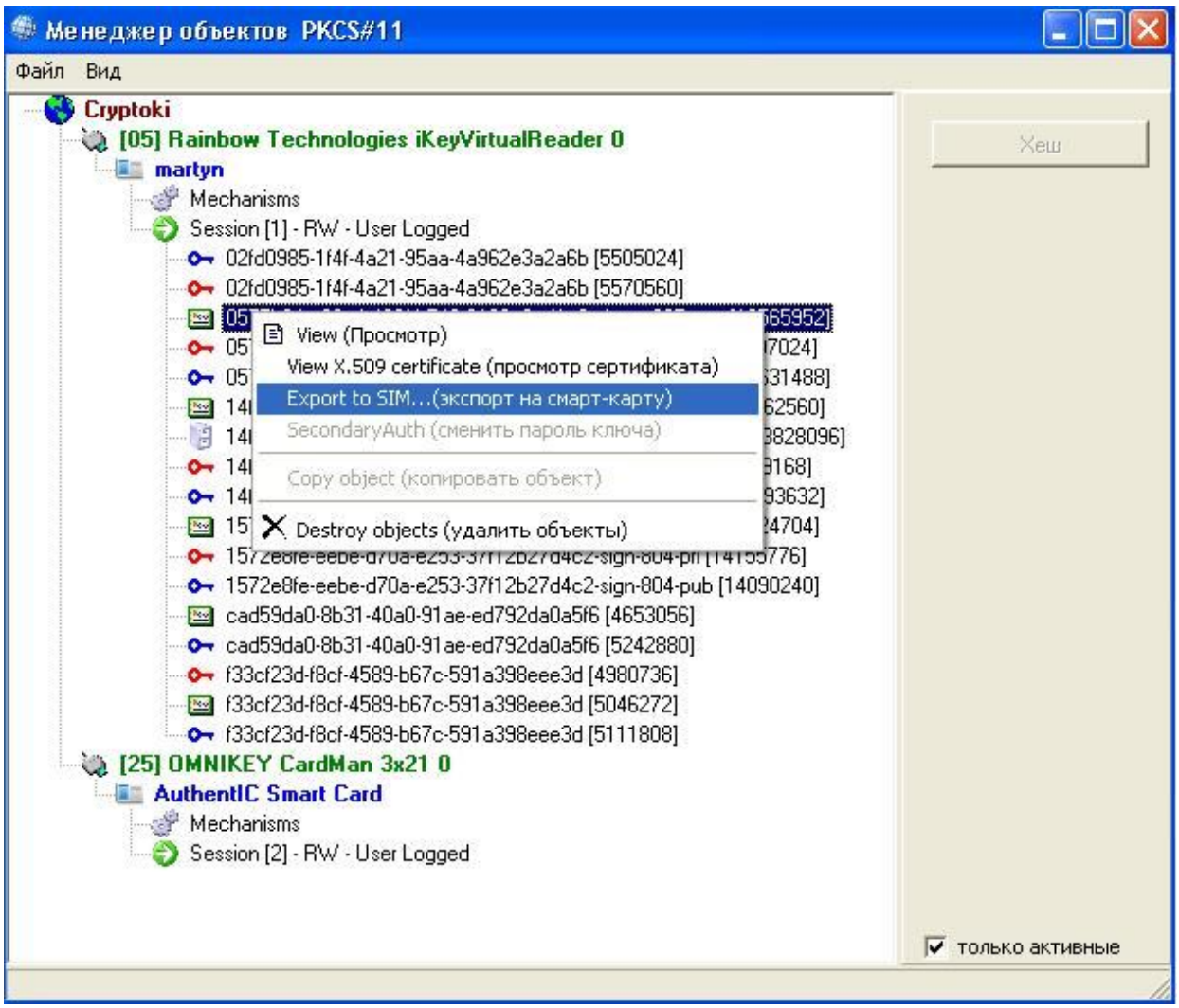


Рис.3.8

Примечание: для выполнения экспорта оба носителя должны быть включены и выполнен вход по доступу к ним с использованием соответствующего персонального пароля (см. далее).

После чего будет предложено выбрать смарт-карту, на которую будет скопирована ключевая информация (карта-приемник должна быть установлена в другом ридере смарт-карточек):

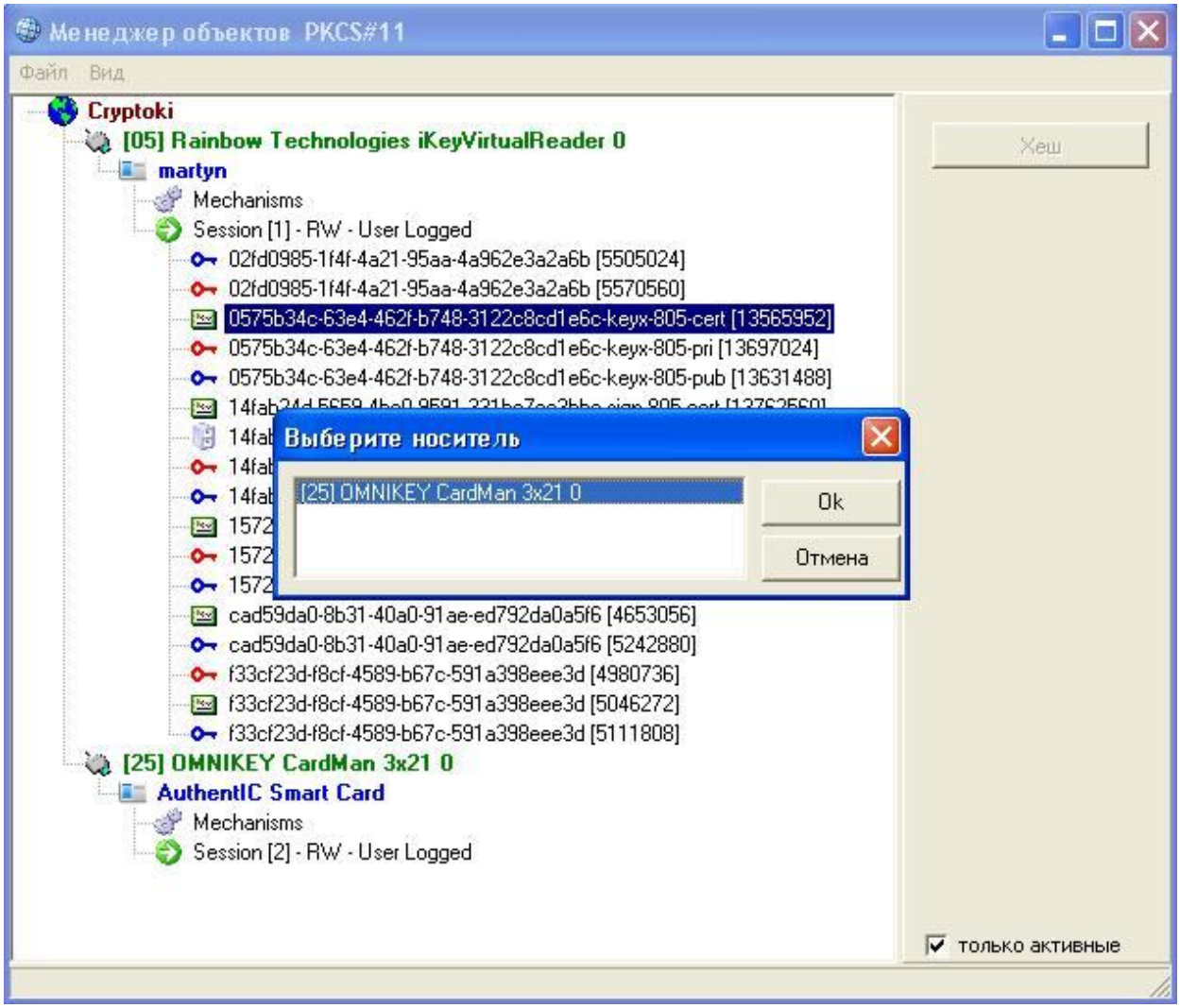


Рис.3.9

После нажатия «Ок» выполняется экспорт ключевой информации и в результате вместе с сертификатом будут экспортированы все связанные с ним объекты (public key, private key, friendly name) .

В том случае, если для смарт-карты, которая является первичным источником (носителем) ключевой информации, не был выполнен вход с паролем, экспорт персонального ключа будет невозможен, о чем пользователь будет предупрежден:

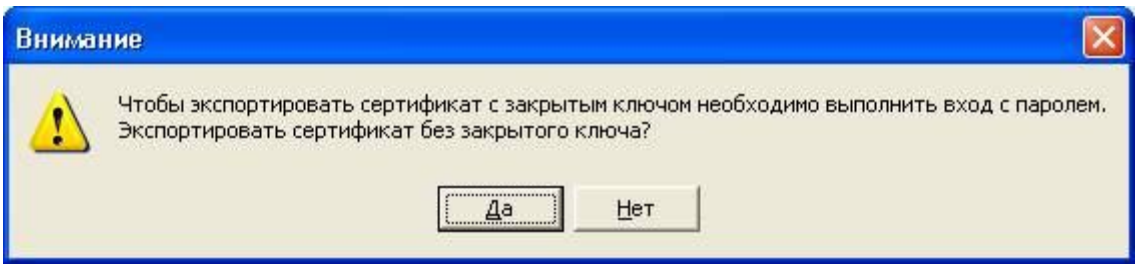


Рис.3.10

Если при этом выбрать «Да», то будут экспортированы все объекты, связанные с выбранным сертификатом, кроме персонального ключа, при выборе «Нет» - экспорт не будет выполняться.

Если пользователь выполнил вход с паролем на носитель, который является «источником», а для носителя-«приемника» выполнен вход без пароля, то для продолжения экспорта будет выведено приглашение ввести пароль доступа к смарт-карте приемника:

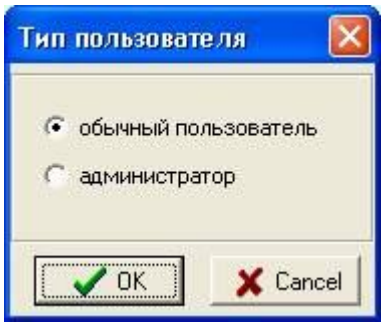


Рис.3.11

Необходимо выбрать «обычный пользователь». Для входа с правами «администратор» необходимо знать административный пароль смарт-карточки.

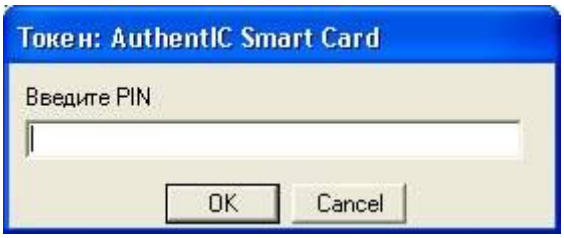


Рис.3.12

После ввода правильного пароля выделенный сертификат и все его объекты будут экспортированы на новый носитель.

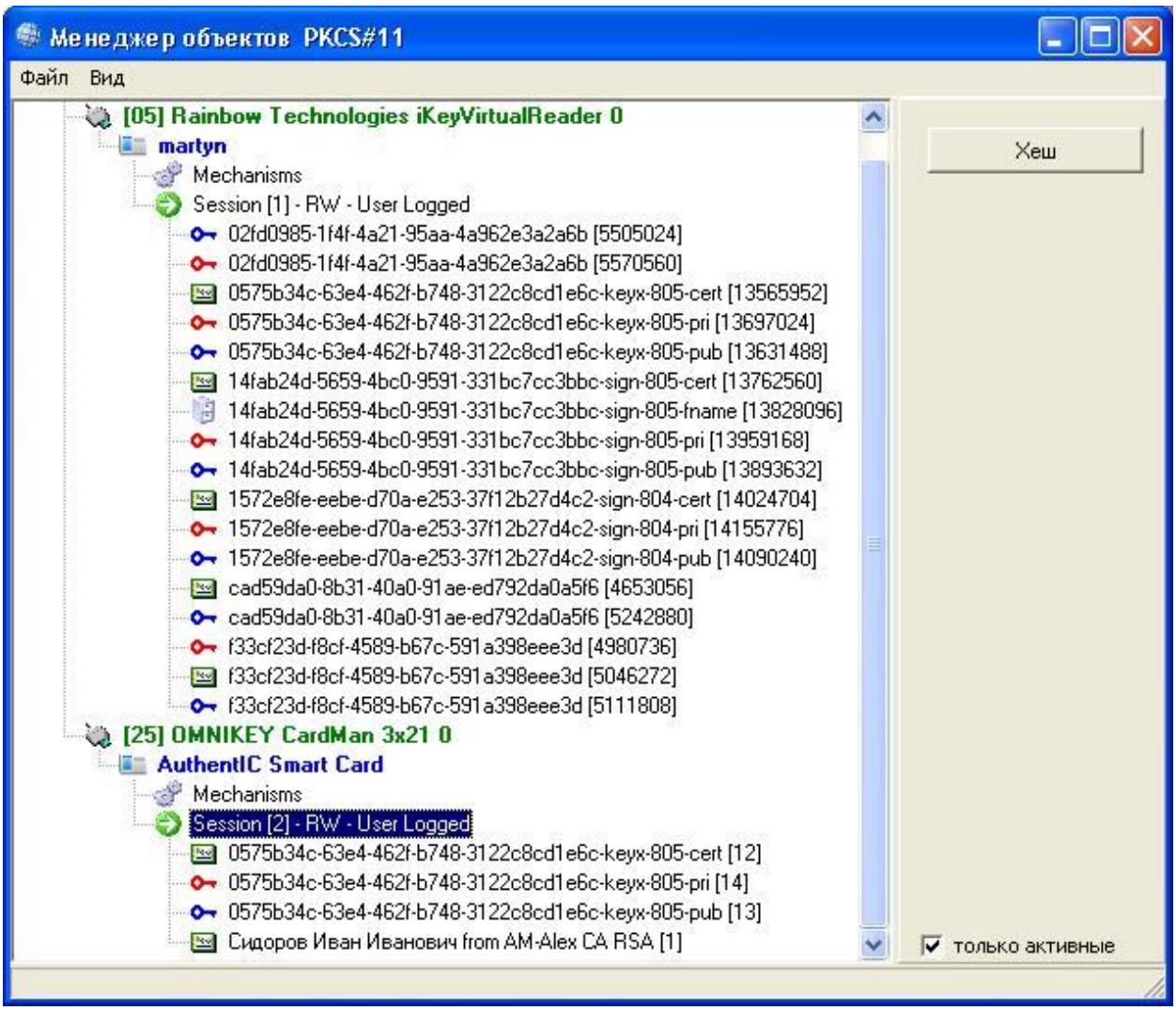


Рис.3.13

Если при выполнении экспорта менеджер обнаружит, что объект с таким идентификатором-меткой уже существует на приемнике, будет выведено предупреждение:

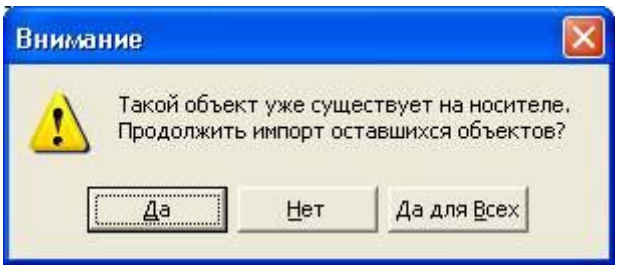


Рис.3.14

Если выбор «Да» - импорт такого объекта, дубликат которого уже существует на носителе, будет пропущен и будет выполнен импорт оставшихся объектов. Если будет далее снова найден дубликат, будет выведено такое же окно. Для того, чтобы избежать появления этого диалогового окна, необходимо выбрать «Да для всех», в этом случае все найденные дубликаты будут игнорироваться без появления диалогового окна. Выбор кнопки «Нет» останавливает импорт.

Аналогично вышеуказанному описанию дублирования ключевой иінформации со смарт-карточки на другую, выполняется дублирование из файлового токена на смарт-карточку и наоборот (пример на рис. 3.15):

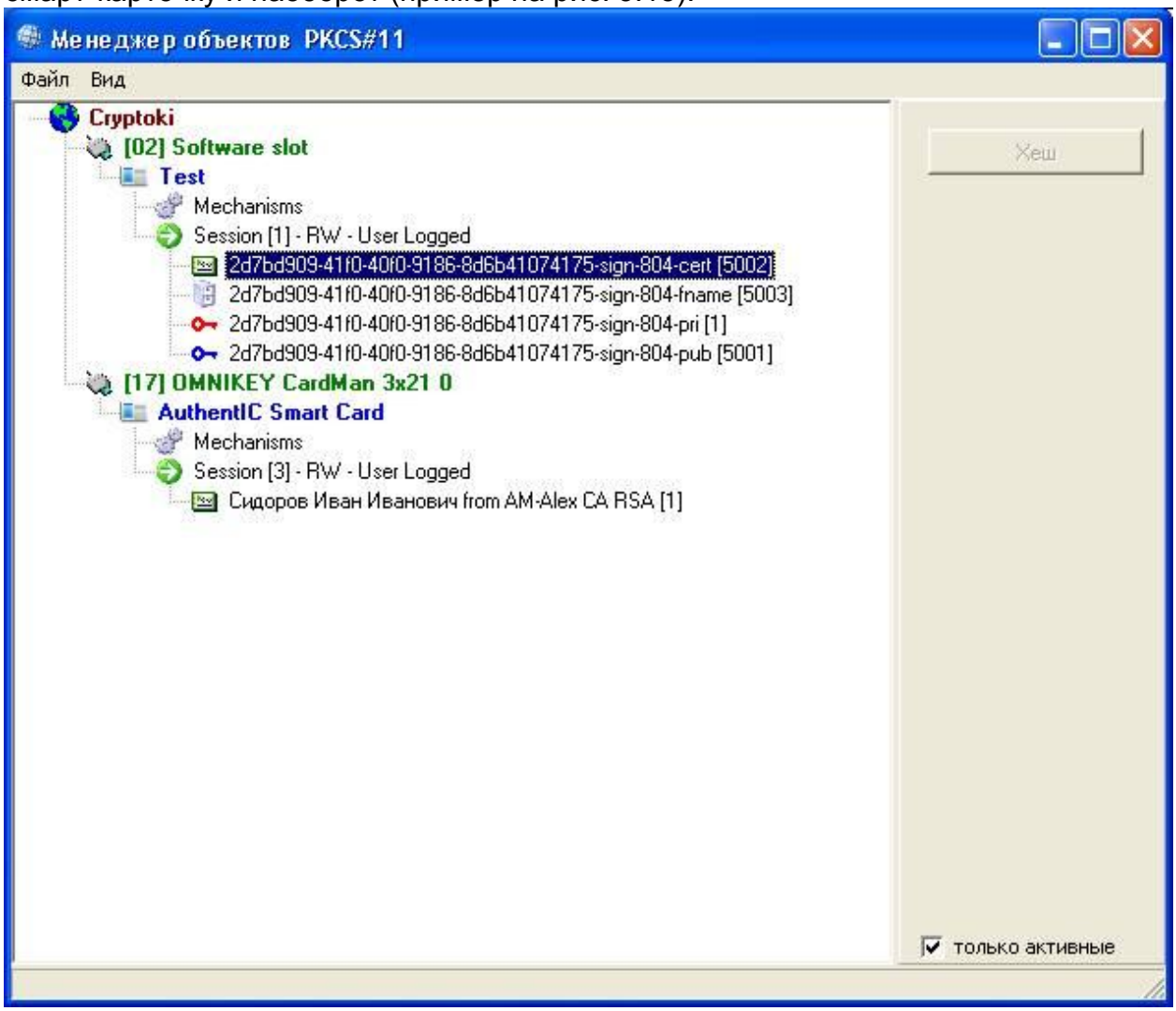


Рис.3.15

Последующее использование полученного дубликата носителя ключевой информации регламентируется соответствующими Инструкциями и Регламентом ЦСК «Цезарис».

3.1.8. Соглашение по названиям (меткам) объектов

Криптопровайдер работает с виртуальными контейнерами ключей. Контейнер может содержать два типа ключевых пар: AT_SIGNATURE – для подписи, AT_KEYEXCHANGE – для обмена симметричными ключами шифрования.

Кроме того, в контейнер помещаются сертификаты соответствующих ключевых пар и объекты с дружественными именами сертификатов (friendly name)[2].

Для работы криптопровайдера метка объекта должна содержать:

- имя контейнера ключей – как правило, в формате GUID;
- назначение контейнера ключей:
  "sign" – подпись;
  "keyx" – распределение ключей.

[2] если они указаны для соответствующих сертификатов

- тип провайдера:
  "804" – ГОСТ 34.310-95 и RSA;
  "805" – ДСТУ 4145-2002 (полиномиальный базис) и RSA;
  "806" – ДСТУ 4145-2002 (полиномиальный базис) и ECDH;
  "807" – ДСТУ 4145-2002 (оптимальный нормальный базис) и RSA;
  "808" – ДСТУ 4145-2002 (оптимальный нормальный базис) и ECDH.
- тип объекта:
  "pri" – объекта CKO_PRIVATEKEY, приватный ключ;
  "pub" – объект CKO_PUBLICKEY, открытый ключ;
  "cert" – объект CKO_CERTIFICATE, сертификат;
  "fname" – объект CKO_DATA, дружественное имя сертификата).

Рекомендуемая литература

1. А.Щербаков, А.Домашев "Прикладная криптография. Использование и синтез криптографических интерфейсов". Москва: Русская редакция, 2003.
2. RSA Laboratories. PKCS#11: Cryptographic Token Interface Standard.
3. ГОСТ 34.311-95 "Информационная технология. Криптографическая защита информации. Функция хеширования".
4. ГОСТ 34.310-95 "Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма ";
5. ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння"
6. ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".
7. RSA Laboratories. PKCS#1: RSA Cryptography Standard.