Извлечение ключа из токена с неизвлекаемым ключом

Довольно часто при оформлении сертификатов ключей электронной подписи можно наблюдать навязчивый пиар токенов с неизвлекаемым ключом. Продавцы из удостоверяющих центров уверяют, что, купив у них СКЗИ КриптоПРО CSP и токен с неизвлекаемым ключом (Рутокен ЭЦП или JaCarta ГОСТ), мы получим сертифицированные СКЗИ, обеспечивающие 100%-ную защиту от кражи ключей с токена. Но так ли это на самом деле? Для ответа на этот вопрос проведем простой эксперимент…

Конфигурация тестового стенда

Соберем тестовый стенд с конфигурацией, типовой для машин, участвующих в электронном документообороте (ЭДО):

1. ОС MS Windows 7 SP1
2. СКЗИ КриптоПРО CSP 3.9.8423
3. Драйверы Рутокен для Windows (x86 и x64). Версия: v.4.1.0.0 от 20.06.2016, WHQL-certified
4. Единый Клиент JaCarta и JaCarta SecurLogon. Версия 2.9.0 сборка 1531
5. КриптоАРМ Стандарт Плюс 5. Версия 5.2.0.8847.

Для тестирования будут использоваться токены с неизвлекамым ключом:

1. Рутокен ЭЦП. Версия 19.02.14.00 (02)
2. JaCarta ГОСТ. Номер модели JC001-2.F09 v2.1

Методика тестирования

Смоделируем типовой процесс подготовки Администратором информационной безопасности ключевых документов для организации ЭДО:

1. генерируется контейнер закрытого ключа и запрос на сертификат открытого ключа;
2. после прохождения в удостоверяющем центре процедуры сертификации из запроса получается сертификат;

3. сертификат в совокупности с контейнером закрытого ключа образует готовую для использования ключевую информацию. Данную ключевую информацию, записанную на носителе, будем называть исходным ключевым документом;

4. с исходного ключевого документа изготавливаются копии, которые записываются на отчуждаемые носители (далее будем называть их рабочими ключевыми документами) и передаются уполномоченным пользователям;

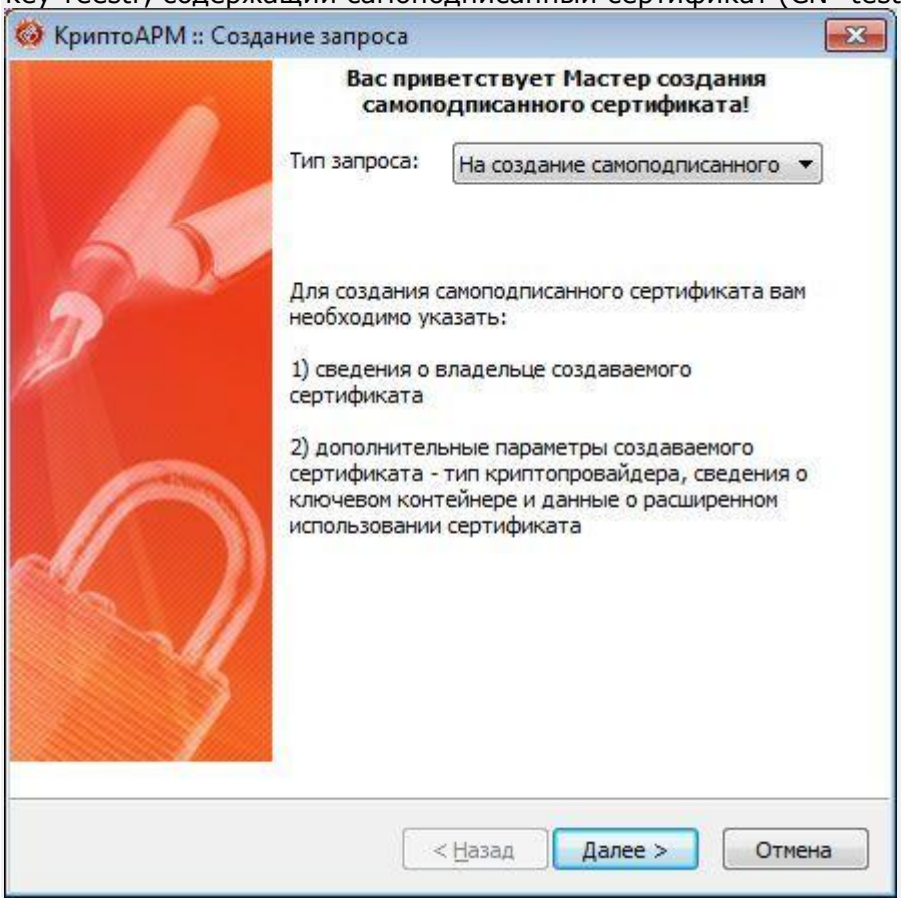
5. после изготовления необходимого количества рабочих ключевых документов исходный ключевой документ уничтожается или депонируется на хранение в орган криптографической защиты информации.

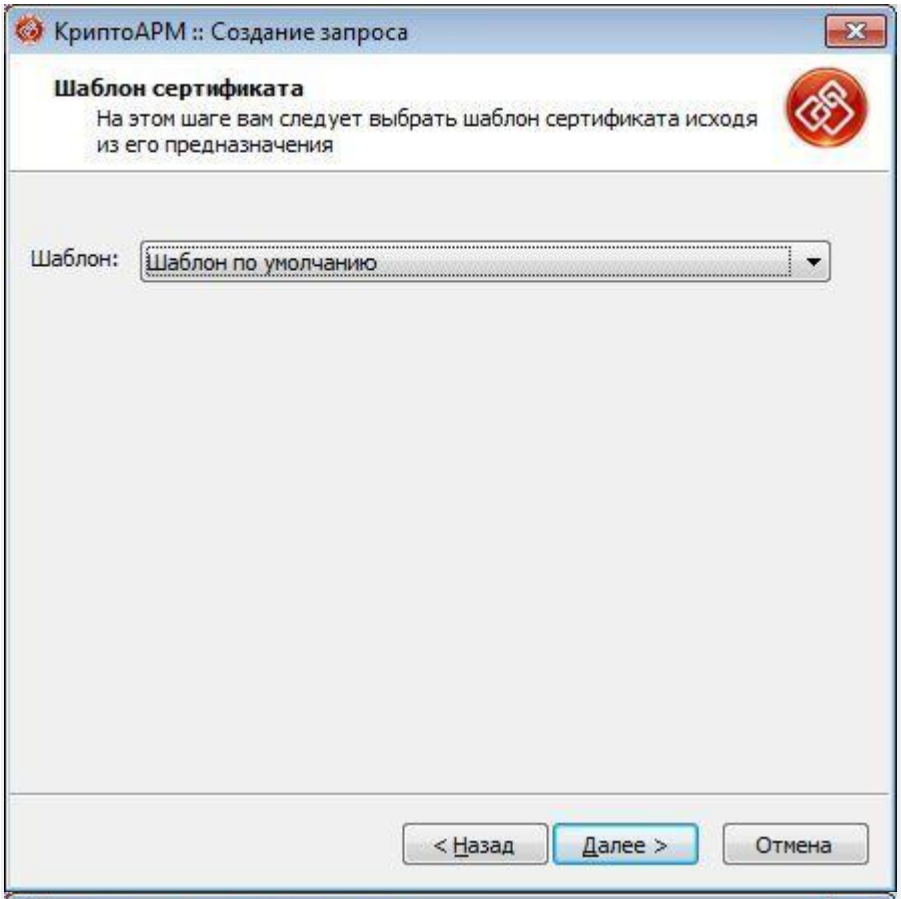
В нашем случае мы не будем пользоваться услугами центров сертификации, а сгенерируем ключевой контейнер с самоподписанным сертификатом и разместим его в реестре компьютера (АРМа генерации ключевой информации), это и будет *исходный ключевой документ*. Затем скопируем ключевую информацию на Рутокен ЭЦП и JaCarta ГОСТ, изготовив *рабочие ключевые документы*. После этого уничтожим *исходный ключевой документ*, удалив из реестра ключевой контейнер. И, наконец, попробуем скопировать ключевую информацию с рабочих ключевых документов обратно в реестр.

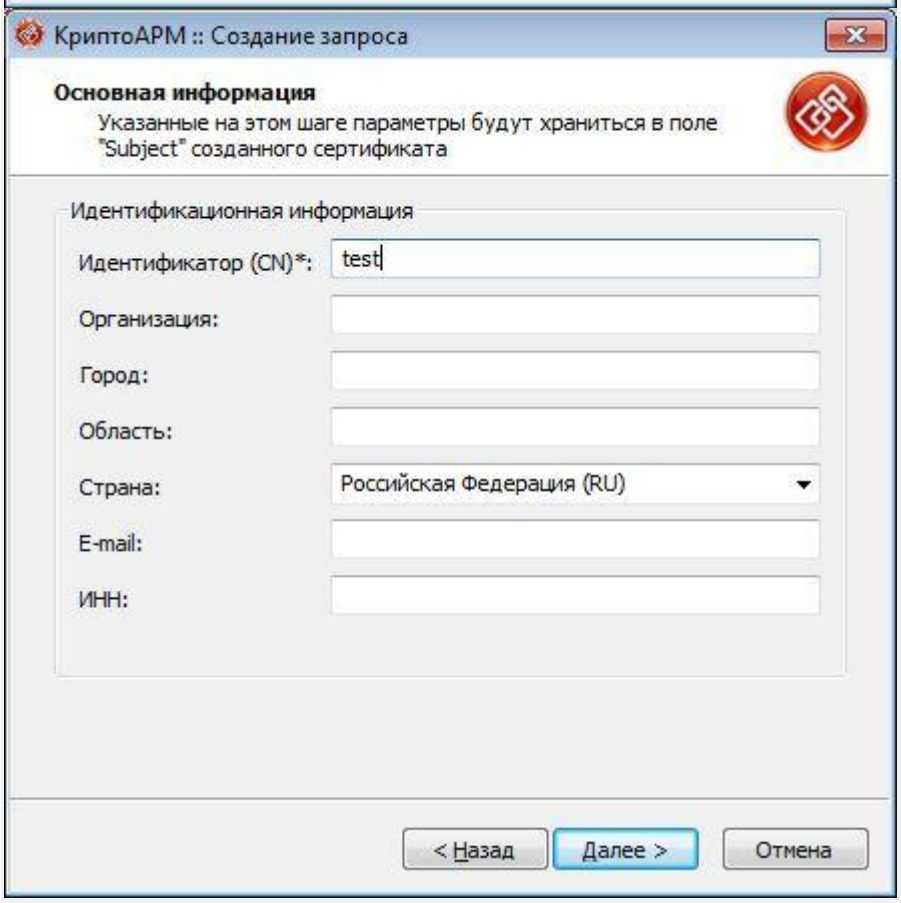
Проведение тестирования

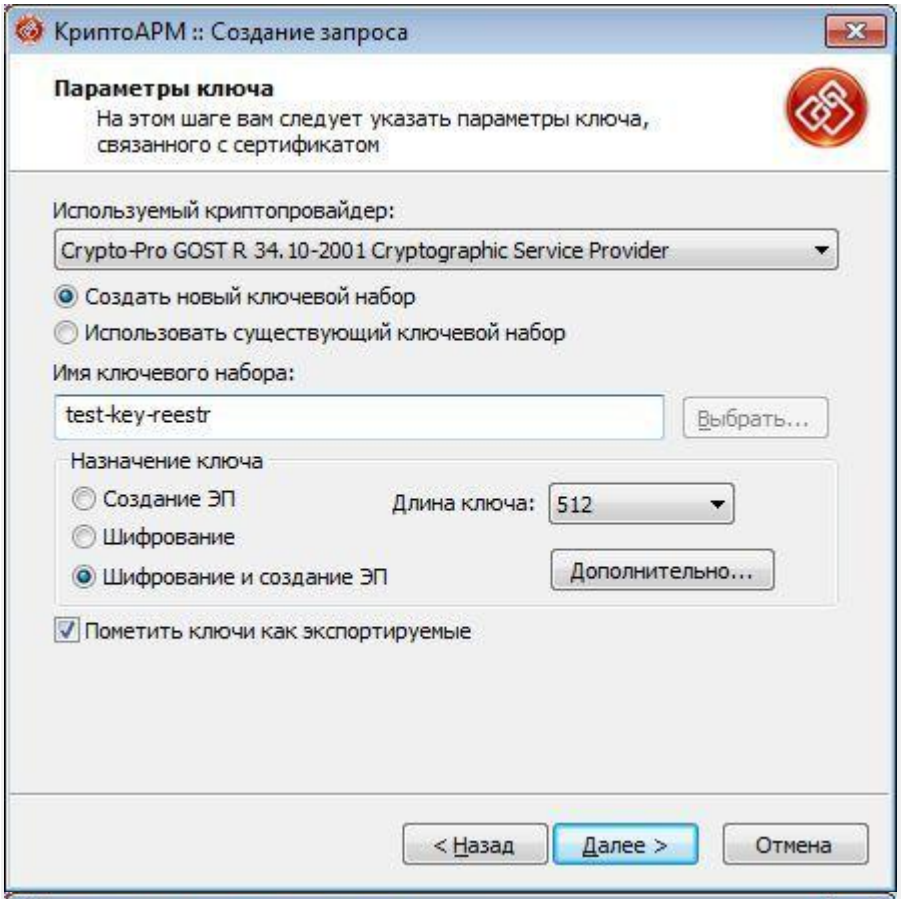
1. Создадим *исходный ключевой документ*.

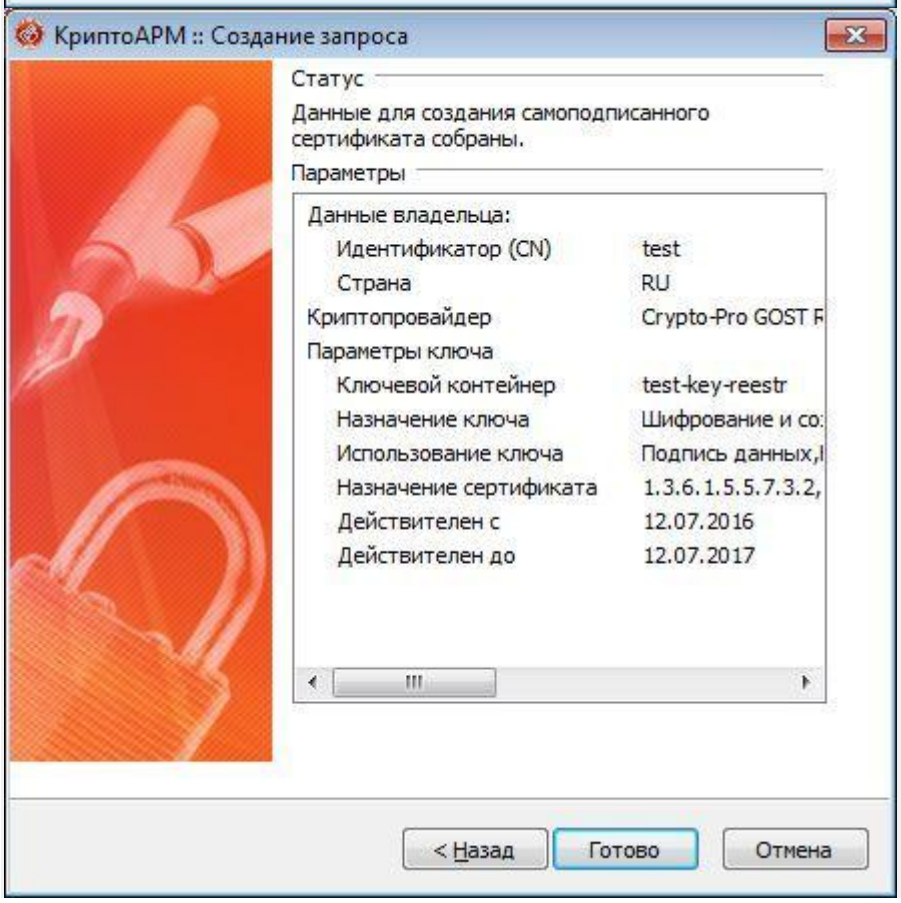
Для этого с помощью КриптоАРМ создадим в реестре контейнер закрытого ключа test-key-reestr, содержащий самоподписанный сертификат (CN=test)

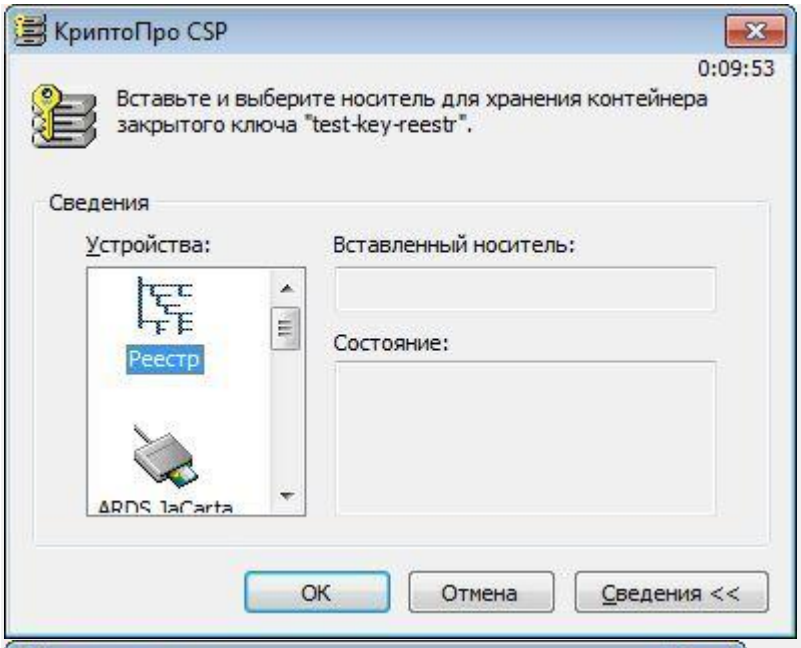


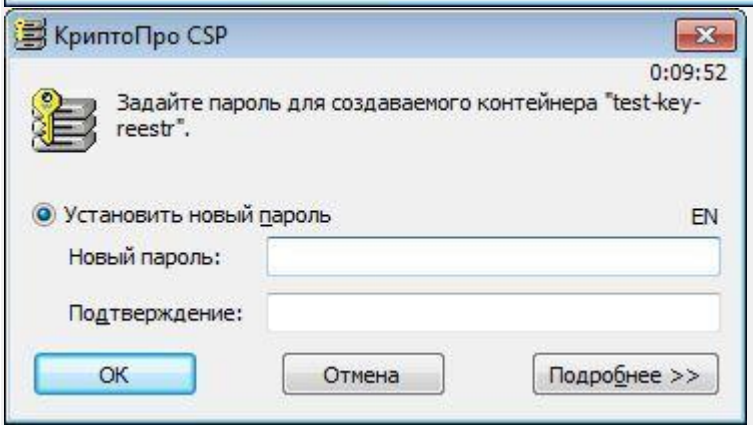

КриптоАРМ :: Создание запроса
Шаблон сертификата
На этом шаге вам следует выбрать шаблон сертификата исходя из его предназначения
Шаблон:
Шаблон по умолчанию
< Назад
Далее >
Отмена

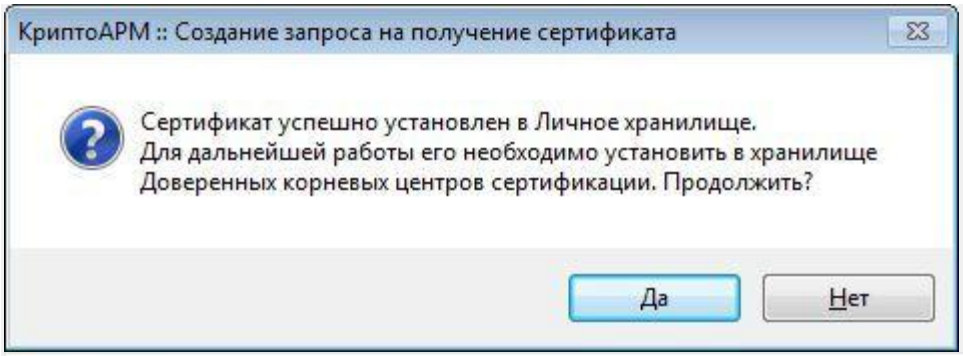

КриптоАРМ :: Создание запроса
Основная информация
Указанные на этом шаге параметры будут храниться в поле "Subject" созданного сертификата
Идентификационная информация
Идентификатор (CN)*:
test
Организация:
Город:
Область:
Страна:
Российская Федерация (RU)
E-mail:
ИНН:
< Назад
Далее >
Отмена

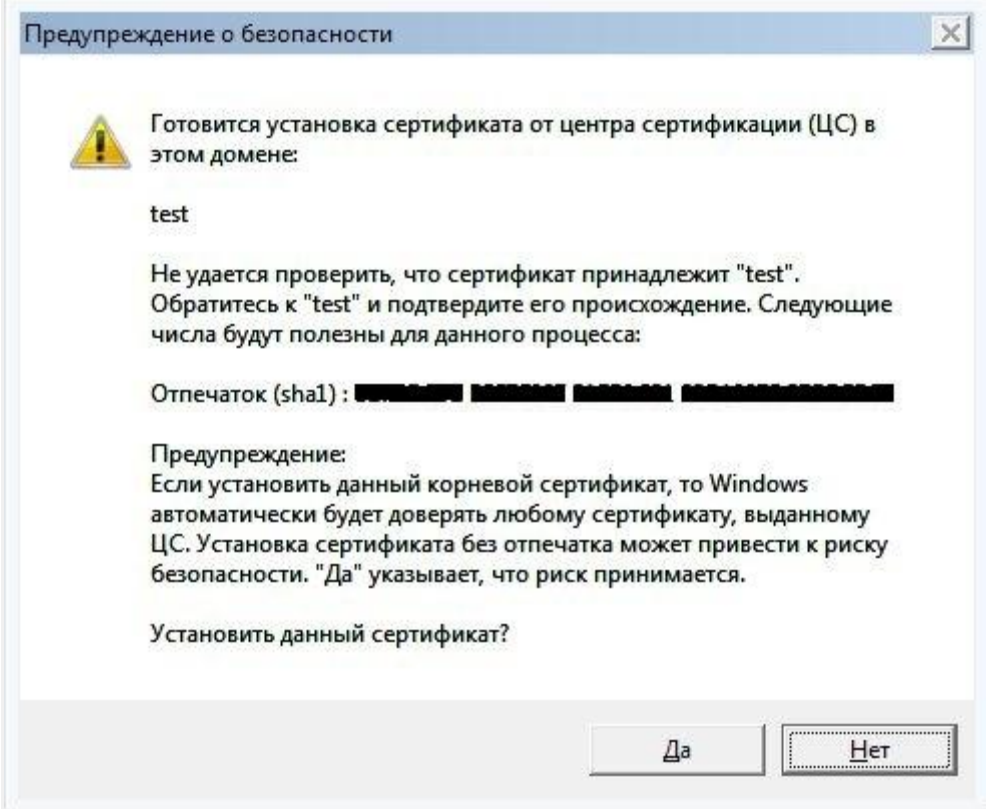

КриптоАРМ :: Создание запроса
Параметры ключа
На этом шаге вам следует указать параметры ключа, связанного с сертификатом
Используемый криптопровайдер:
Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
Создать новый ключевой набор
Использовать существующий ключевой набор
Имя ключевого набора:
test-key-reestr
Выбрать...
Назначение ключа
Создание ЭП
Длина ключа: 512
Шифрование
Шифрование и создание ЭП
Дополнительно...
Пометить ключи как экспортируемые
< Назад
Далее >
Отмена


КриптоАРМ :: Создание запроса
Статус
Данные для создания самоподписанного сертификата собраны.
Параметры
Данные владельца:
Идентификатор (CN) test
Страна RU
Криптопровайдер Crypto-Pro GOST R
Параметры ключа
Ключевой контейнер test-key-reestr
Назначение ключа Шифрование и со
Использование ключа Подпись данных,
Назначение сертификата 1.3.6.1.5.5.7.3.2,
Действителен с 12.07.2016
Действителен до 12.07.2017
< Назад
Готово
Отмена


КриптоПро CSP
0:09:53
Вставьте и выберите носитель для хранения контейнера закрытого ключа "test-key-reestr".
Сведения
Устройства:
Вставленный носитель:
Реестр
Состояние:
OK
Отмена
Сведения <<

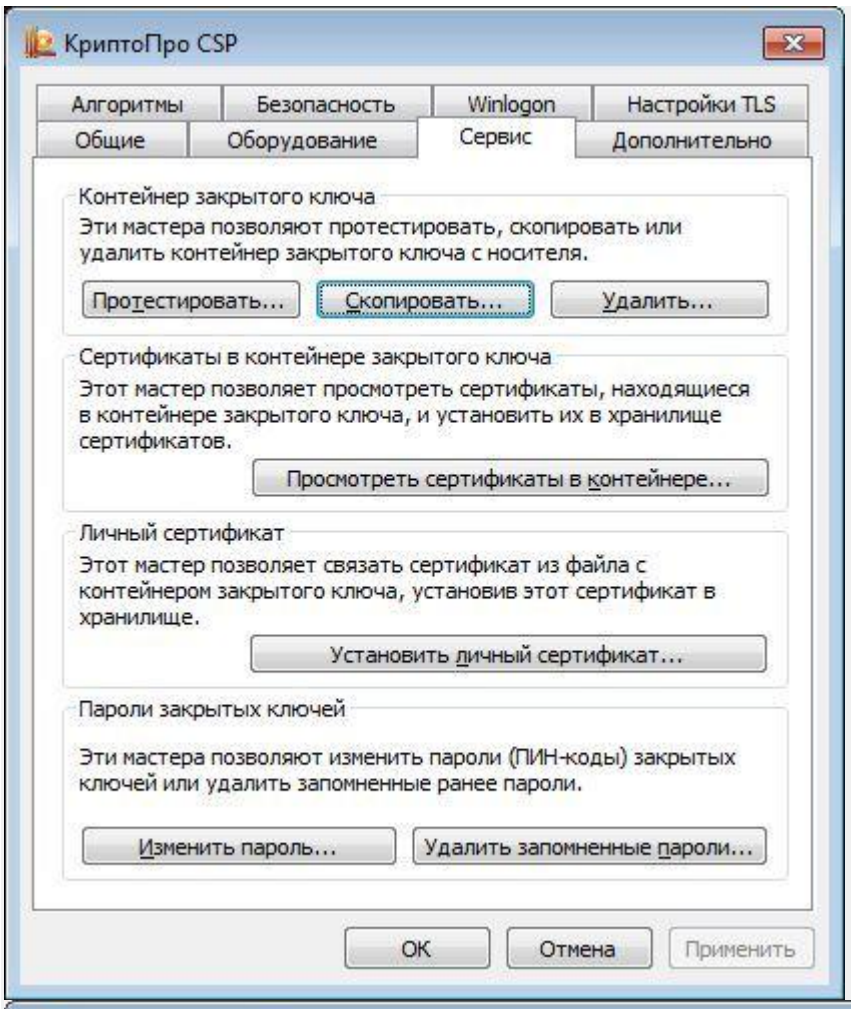

КриптоПро CSP
0:09:52
Задайте пароль для создаваемого контейнера "test-key-reestr".
Установить новый пароль
EN
Новый пароль:
Подтверждение:
OK
Отмена
Подробнее >>

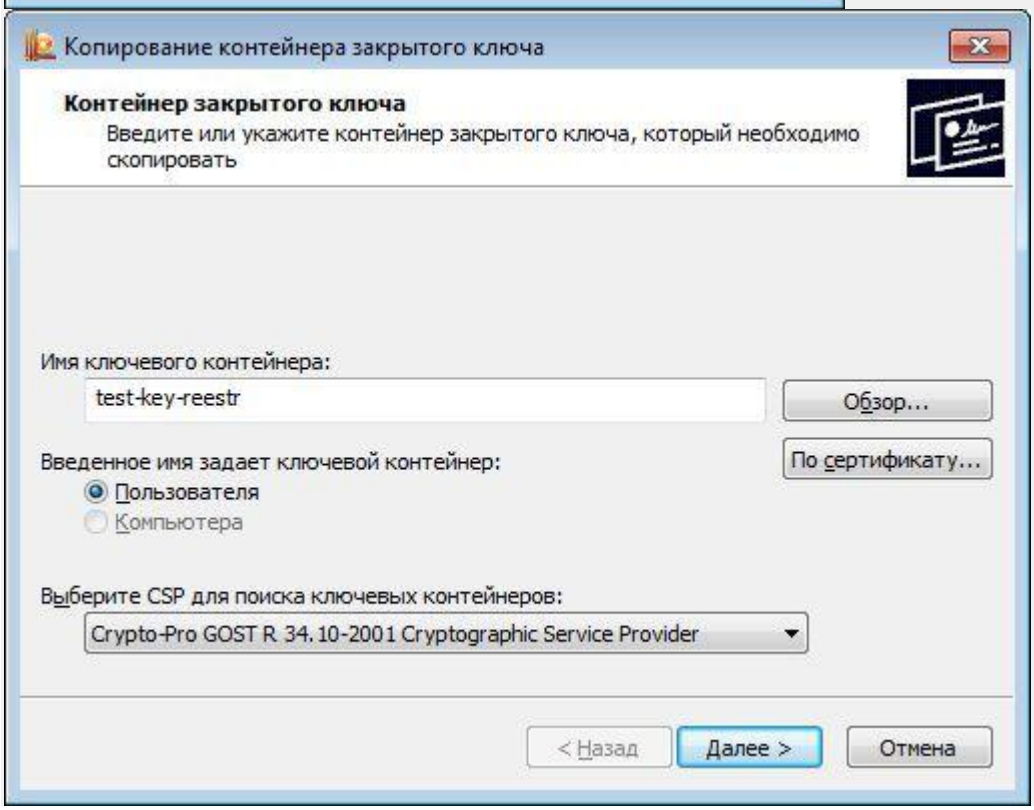


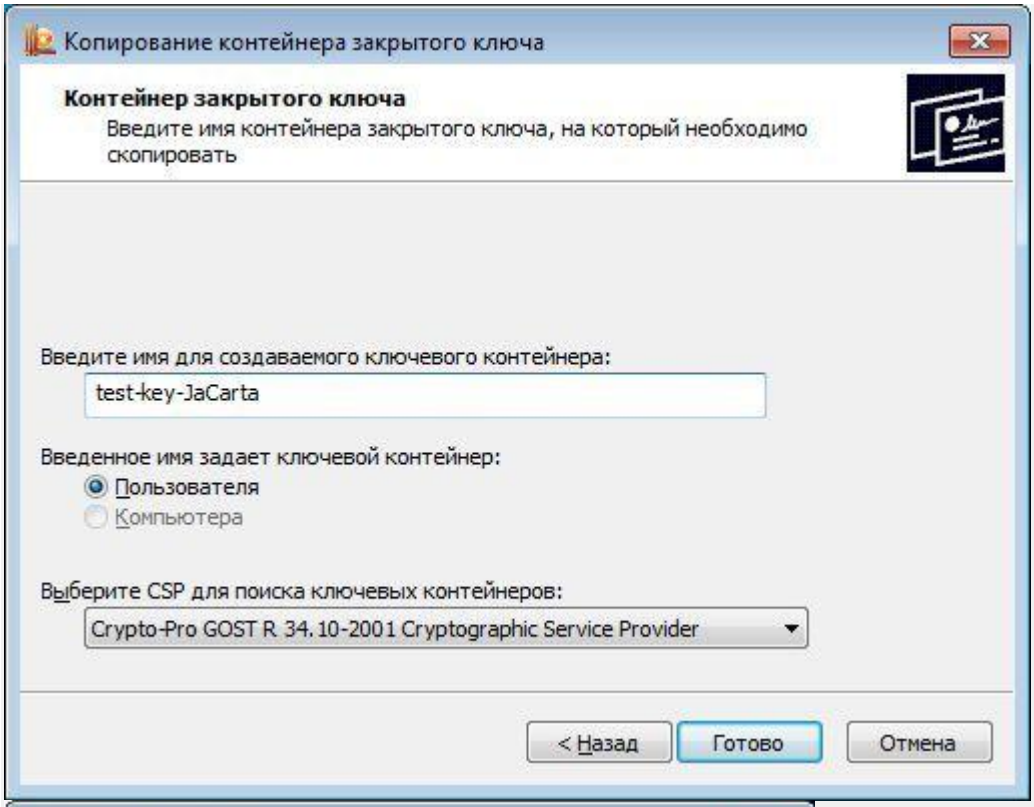


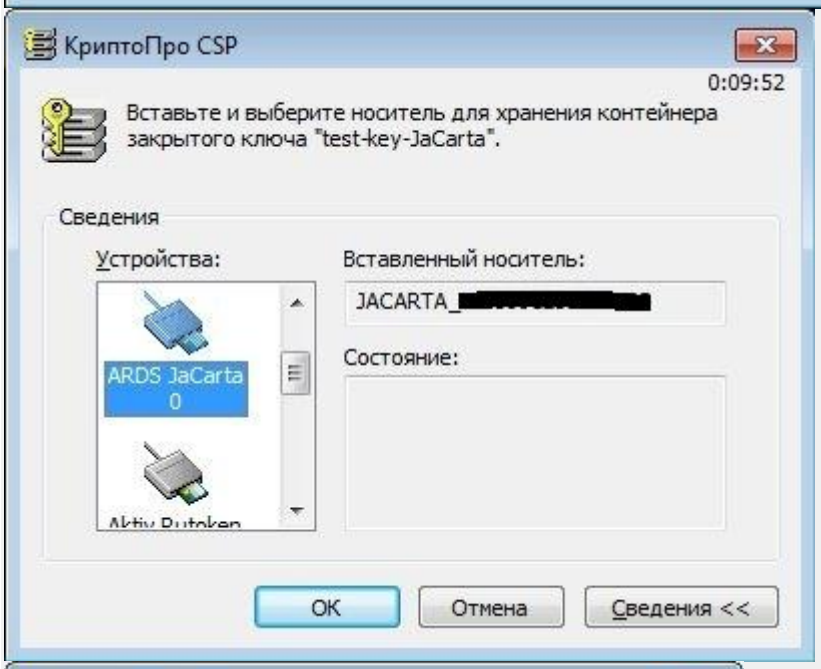
2.Сформируем *рабочие ключевые документы*.

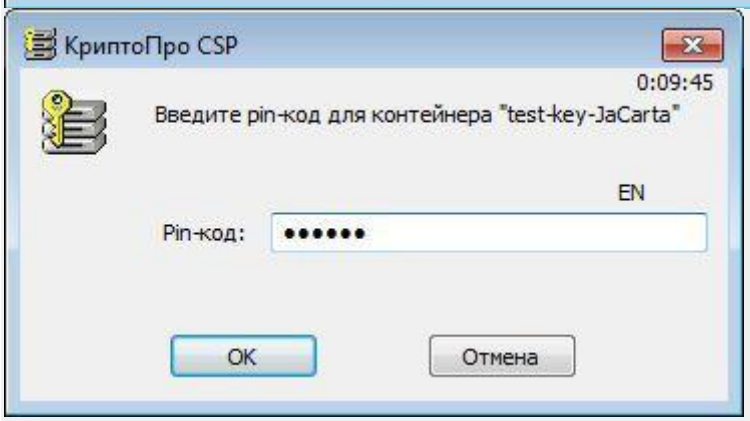
С помощью штатных средств СКЗИ КриптоПРО CSP (Пуск→Панель управления→КриптоПро CSP) скопируем ключевой контейнер test-key-reestr на ключевые носители Рутокен ЭЦП и JaCarta ГОСТ. Ключевым контейнерам на ключевых носителях присвоим имена test-key-rutoken и test-key-jacarta соответственно. Описание приведено применительно к JaCarta ГОСТ (для Рутокен ЭЦП действия аналогичны):


КриптоПро CSP
Алгоритмы
Безопасность
Winlogon
Настройки TLS
Общие
Оборудование
Сервис
Дополнительно
Контейнер закрытого ключа
Эти мастера позволяют протестировать, скопировать или удалить контейнер закрытого ключа с носителя.
Протестировать...
Скопировать...
Удалить...
Сертификаты в контейнере закрытого ключа
Этот мастер позволяет просмотреть сертификаты, находящиеся в контейнере закрытого ключа, и установить их в хранилище сертификатов.
Просмотреть сертификаты в контейнере...
Личный сертификат
Этот мастер позволяет связать сертификат из файла с контейнером закрытого ключа, установив этот сертификат в хранилище.
Установить личный сертификат...
Пароли закрытых ключей
Эти мастера позволяют изменить пароли (ПИН-коды) закрытых ключей или удалить запомненные ранее пароли.
Изменить пароль...
Удалить запомненные пароли...
OK
Отмена
Применить


Копирование контейнера закрытого ключа
Контейнер закрытого ключа
Введите или укажите контейнер закрытого ключа, который необходимо скопировать
Имя ключевого контейнера:
test-key-reestr
Обзор...
Введенное имя задает ключевой контейнер:
По сертификату...
Пользователя
Компьютера
Выберите CSP для поиска ключевых контейнеров:
Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
< Назад
Далее >
Отмена







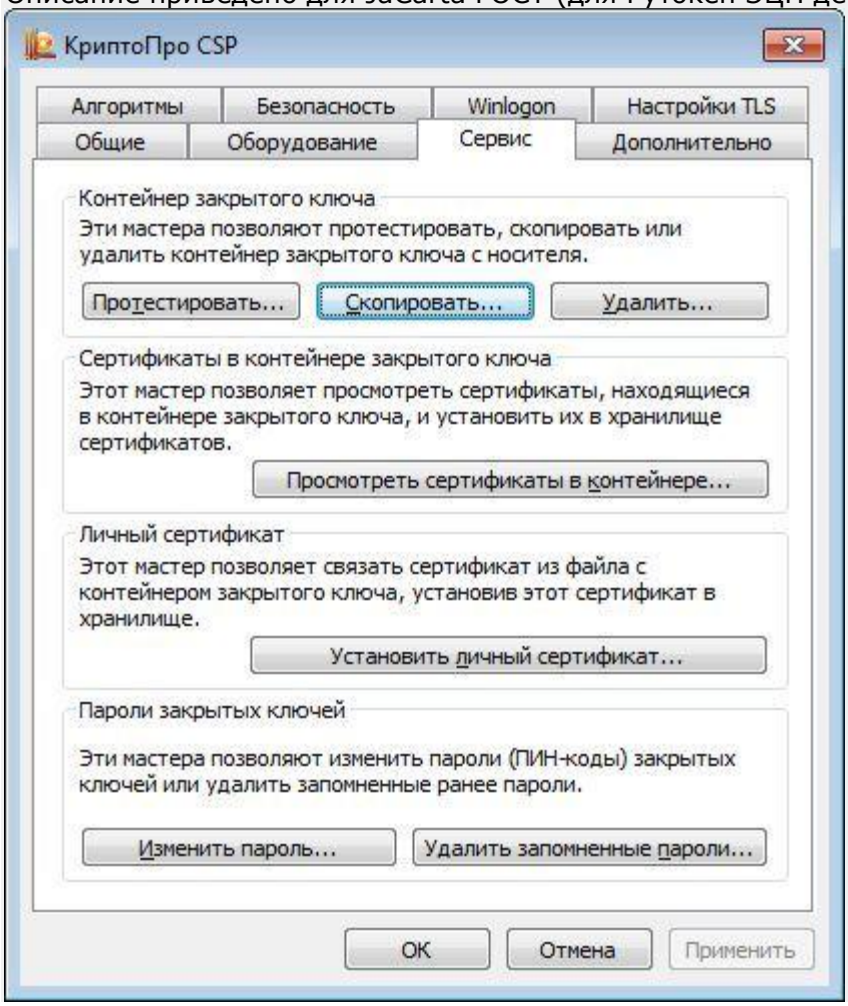
Таким образом получили *рабочие ключевые документы* на JaCarta ГОСТ (контейнер test-key-jacarta) и Рутокен ЭЦП (контейнер test-key-rutoken).

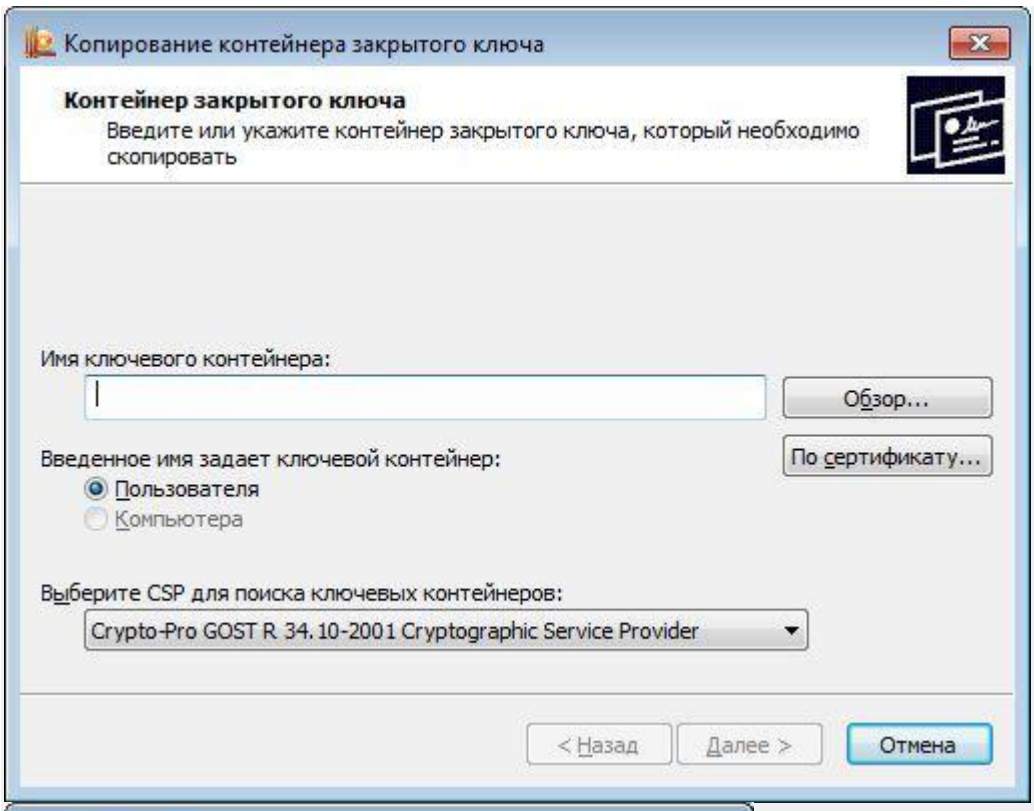
3.Уничтожим исходный ключевой документ

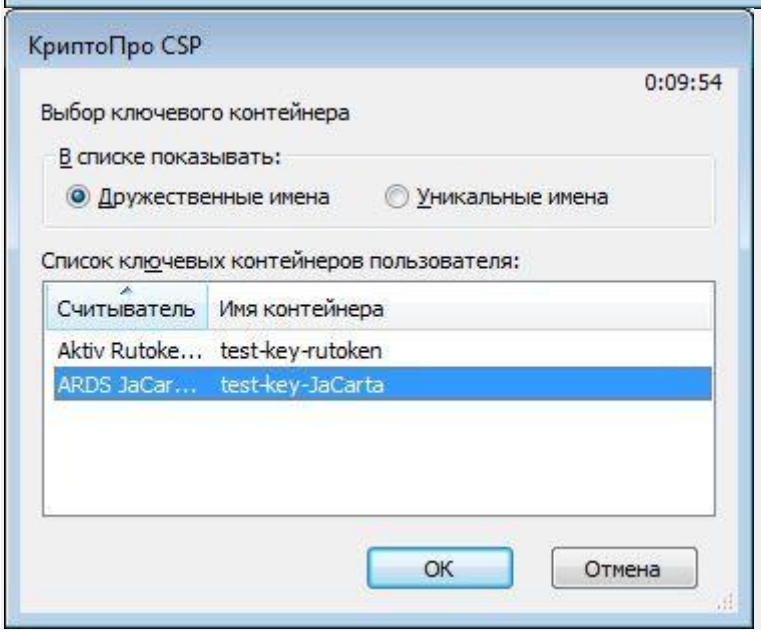
Штатными средствами СКЗИ КриптоПРО CSP удалим из реестра ключевой контейнер test-key-reestr.

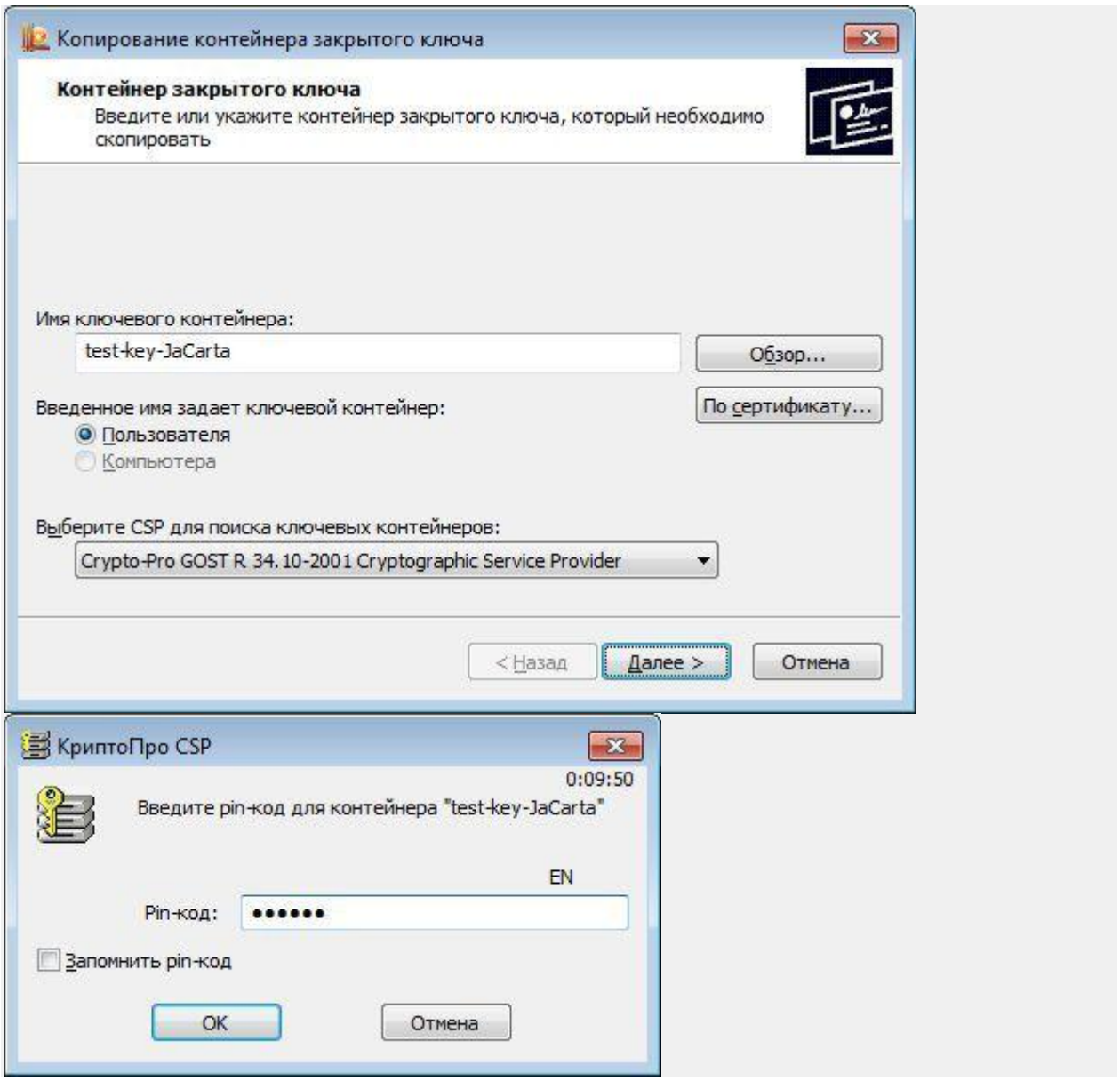
4. Скопируем ключевую информацию из *рабочих ключевых документов*

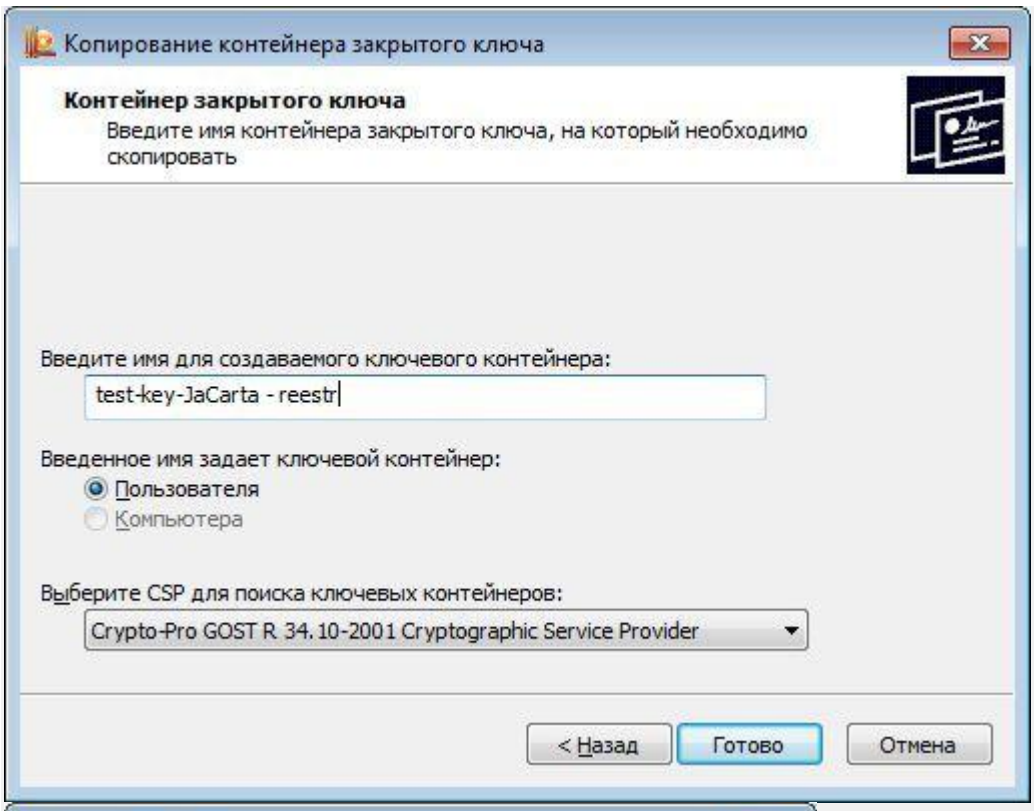
Попробуем скопировать ключевые контейнеры test-key-rutoken и test-key-jacarta обратно в реестр.
Описание приведено для JaCarta ГОСТ (для Рутокен ЭЦП действия аналогичны).

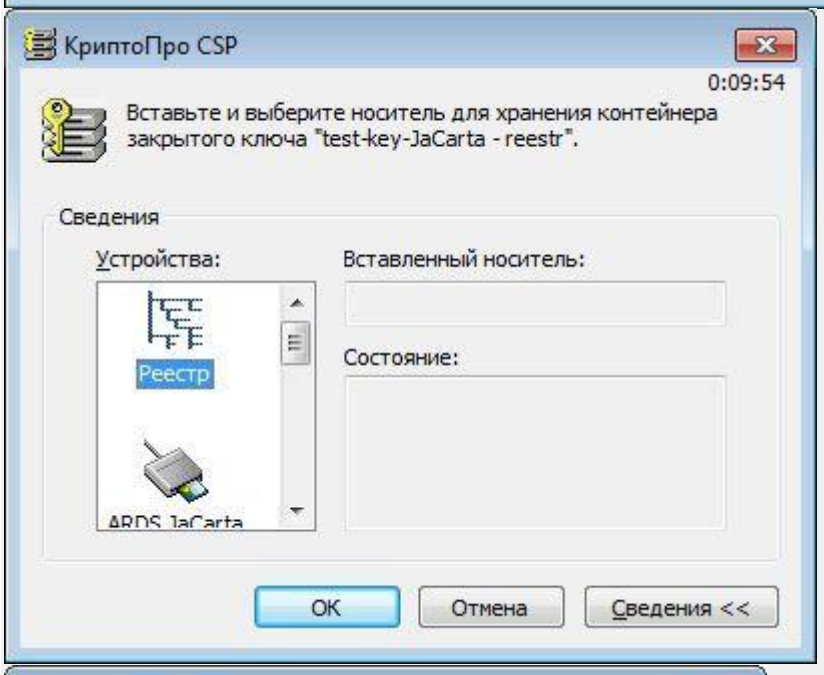


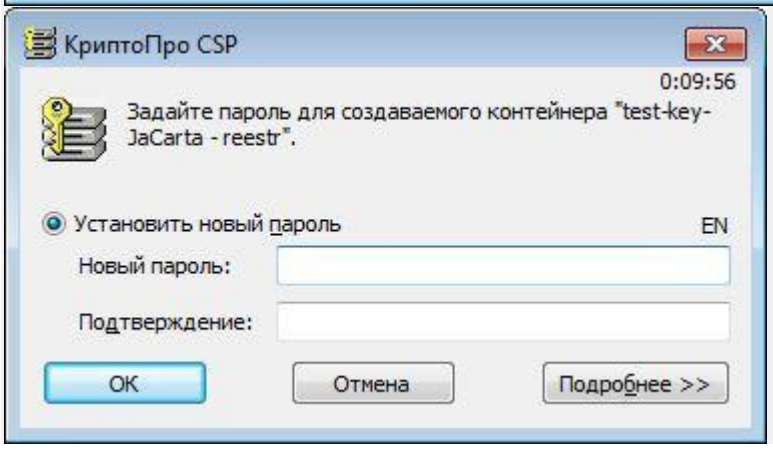

Копирование контейнера закрытого ключа
Контейнер закрытого ключа
Введите или укажите контейнер закрытого ключа, который необходимо скопировать
Имя ключевого контейнера:
Обзор...
Введенное имя задает ключевой контейнер:
По сертификату...
Пользователя
Компьютера
Выберите CSP для поиска ключевых контейнеров:
Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
< Назад
Далее >
Отмена


КриптоПро CSP
0:09:54
Выбор ключевого контейнера
В списке показывать:
Дружественные имена
Уникальные имена
Список ключевых контейнеров пользователя:
Считыватель
Имя контейнера
Aktiv Rutoke...
test-key-rutoken
ARDS JaCar...
test-key-JaCarta
OK
Отмена


Копирование контейнера закрытого ключа
Контейнер закрытого ключа
Введите или укажите контейнер закрытого ключа, который необходимо скопировать
Имя ключевого контейнера:
test-key-JaCarta
Обзор...
Введенное имя задает ключевой контейнер:
По сертификату...
Пользователя
Компьютера
Выберите CSP для поиска ключевых контейнеров:
Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
< Назад
Далее >
Отмена
КриптоПро CSP
0:09:50
Введите pin-код для контейнера "test-key-JaCarta"
EN
Pin-код:
Запомнить pin-код
OK
Отмена


Копирование контейнера закрытого ключа
Контейнер закрытого ключа
Введите имя контейнера закрытого ключа, на который необходимо скопировать
Введите имя для создаваемого ключевого контейнера:
test-key-JaCarta - reestr
Введенное имя задает ключевой контейнер:
Пользователя
Компьютера
Выберите CSP для поиска ключевых контейнеров:
Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
< Назад
Готово
Отмена


КриптоПро CSP
0:09:54
Вставьте и выберите носитель для хранения контейнера закрытого ключа "test-key-JaCarta - reestr".
Сведения
Устройства:
Вставленный носитель:
Состояние:
Реестр
ARDS JaCarta
OK
Отмена
Сведения <<


КриптоПро CSP
0:09:56
Задайте пароль для создаваемого контейнера "test-key-JaCarta - reestr".
Установить новый пароль
EN
Новый пароль:
Подтверждение:
OK
Отмена
Подробнее >>

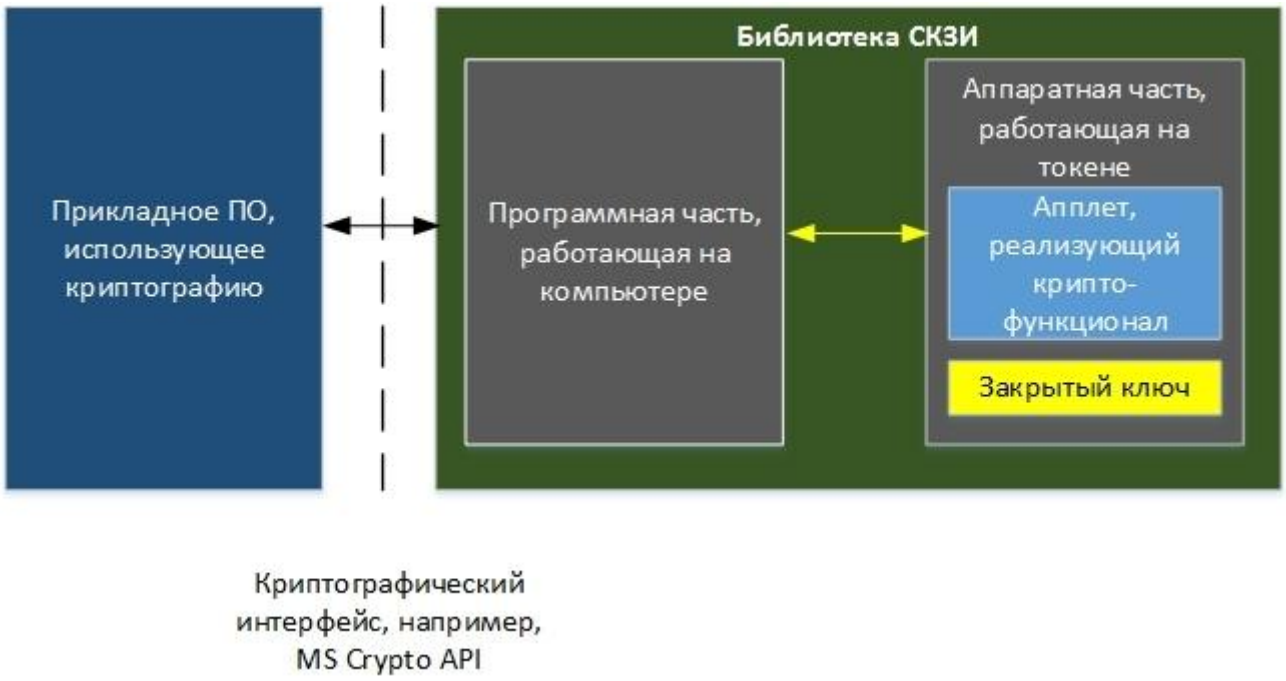
Как мы видим, ключевая информация успешно скопирована или, другим языком, извлечена из токенов с неизвлекаемым ключом. Получается, что производители токенов и СКЗИ врут? На самом деле нет, и ситуация сложнее, чем кажется на первый взгляд. Исследуем матчасть по токенам.

Матчасть

То, что на рынке принято называть токеном с неизвлекаемым ключом, правильно называется функциональным ключевым носителем (ФКН) (доп. инфо).

Главным отличием ФКН от обычных токенов (Рутокен S, JaCarta PKI, …) в том, что при выполнении криптографических преобразований (например, формирование электронной подписи) закрытый ключ не покидает устройство. В то время как при использовании обычных токенов закрытый ключ копируется с токена в память комптьютера.

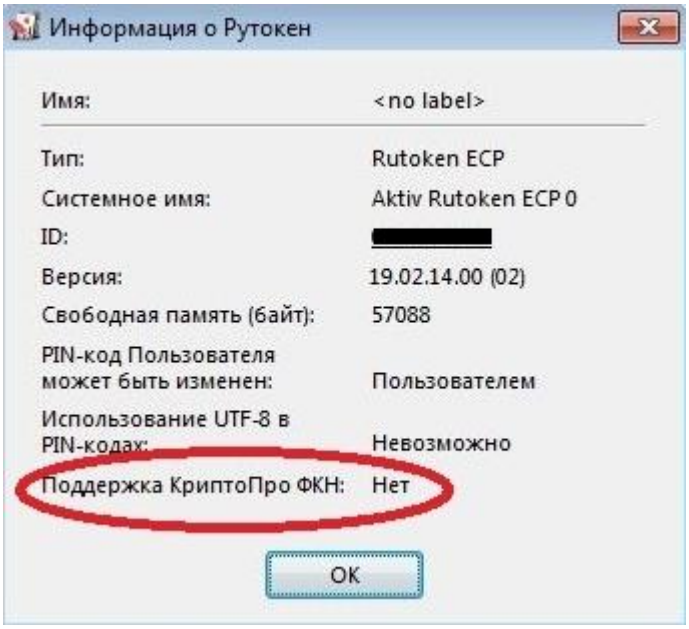
Использование ФКН требует особой организации взаимодействия между прикладным криптографическим ПО и библиотекой СКЗИ (криптопровайдером или, по-другому, CSP).



Здесь важно увидеть, что программная часть библиотеки СКЗИ должна знать о существовании на токене апплета, реализующего криптографический функционал (например, генерация ключа, подпись данных и т.д.) и уметь с ним работать.

По-новому взглянем на наш тестовый стенд

В качестве одного из ключевых носителей использовался Рутокен ЭЦП. Через «Панель управления Рутокен» о нем можно получить следующую информацию:



В последней строке указана фраза «Поддержка КриптоПРО ФКН: Нет», а это значит, что на токене нет апплета, с которым умеет работать СКЗИ КриптоПРО CSP. Таким образом, реализация технологии ФКН с использованием СКЗИ и токенов, описанных в конфигурации тестового стенда, невозможна.

Аналогичная ситуация и с JaCarta ГОСТ. Более того, СКЗИ КриптоПРО CSP, по крайней мере та версия, которая использовалась в тестовом стенде, использует данные ключевые носители как «обычные токены», которые, в свою очередь, являются просто носителями ключа.

Это утверждение очень просто подтвердить. Для этого надо поставить СКЗИ КриптоПРО CSP на чистую машину без драйверов от токенов и подключить токен JaCarta ГОСТ. ОС Windows 7 обнаружит токен JaCarta ГОСТ как «Устройство чтения смарт-карт Microsoft Usbccid (WUDF)». теперь можно попробовать создать ключ на токене и скопировать его в реестр компьютера. Весь функционал СКЗИ успешно отработает.

Как сделать, чтобы все было хорошо?

Чтобы с помощью продуктов ООО “КРИПТО-ПРО” реализовать технологию ФКН, необходимо:

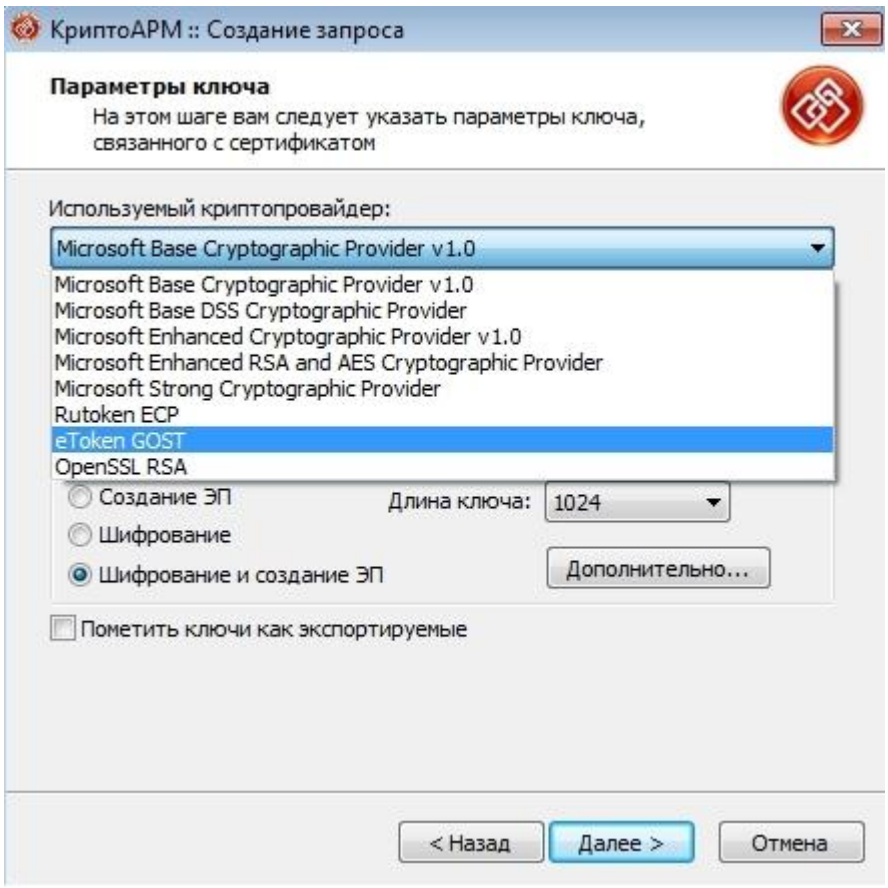
1. Купить специальную версию библиотеки СКЗИ:

- для Рутокен ЭЦП — СКЗИ КриптоПРО Рутокен CSP.
- для JaCarta ГОСТ – СКЗИ КриптоПро ФКН CSP.

2. Одновременно с библиотекой СКЗИ необходимо приобрести специально подготовленные токены, содержащие в себе программные части (апплеты), с которыми умеет работать КриптоПРО Рутокен CSP или КриптоПро ФКН CSP соответственно.

Получается, что Рутокен ЭЦП и JaCarta ГОСТ не являются токенами с неизвлекаемым ключом?

Опять нет. Данные устройства могут реализовывать функционал ФКН (но, возможно, в меньшем объеме, чем при использовании их совместно с СКЗИ КриптоПРО), но для этого нужен софт, который умеет работать с апплетами размещенными на токенах. Таким софтом может быть КриптоАРМ Стандарт 5 Плюс. Он это умеет. При генерации ключевой пары в мастере КриптоАРМ можно выбрать криптопровайдер, который будет использоваться, например, Rutoken ECP или eToken GOST. Это и позволит использовать токен как ФКН.



Выводы

- Не верьте продавцам, чушь вам городящим. Использование обычных версий криптопровайдера КриптоПРО CSP и обычных Рутокен ЭЦП или JaCarta ГОСт не позволяют реализовать технологию ФКН.
- Для использования технологии ФКН совместно с продуктами ООО «КРИПТО-ПРО» необходимы как специально подготовленные токены, содержащие апплет, с которым умеет работать СКЗИ, так и специальные версии криптопровайдера КриптоПРО CSP, которые умеют работать с апплетом на токенах.
- Рутокен ЭЦП и JaCarta ГОСТ умеет самостоятельно реализовывать технологию ФКН, но для этого необходим специальный софт.