ESMART®

Плагин ESMART Token CryptoPro

Содержание

1. Общая информация

Данное руководство предназначено для использования USB-ключей и карт ESMART Token с отечественными алгоритмами ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-94, ГОСТ Р 34.10-2012.

В качестве Удостоверяющего центра в примерах используется бесплатный тестовый УЦ КриптоПро с открытым русифицированным веб-интерфейсом.

Полученные сертификаты могут использоваться исключительно в ознакомительных целях и для тестирования работоспособности системы. Использовать сертификаты, полученные в тестовых удостоверяющих центрах, в рабочих проектах нельзя.

Каждая ключевая пара и сертификат на карте создается в отдельном контейнере. Если на карте должно быть несколько пар ключей с соответствующими сертификатами, для каждой пары должен быть создан отдельный контейнер с уникальным названием.

ПИН-код пользователя и администратора по умолчанию для ESMART Token: 12345678.

2. Использование в Linux

Далее описаны только основные шаги работы с ESMART Token. Более подробную информацию о работе КриптоПро в Linux можно получить на сайте http://cryptopro.ru/category/faq/linuxunix-0

2.1 Установка пакета

Установите RPM-пакет, соответствующий разрядности машины, из папки Linux\cryptopro.

Команда для установки пакета для 32-битных версий ОС Linux:

```
rpm -i isbc-cryptopro-x.x-x.i586.rpm
```

Команда для установки пакета для 64-битных версий ОС Linux:

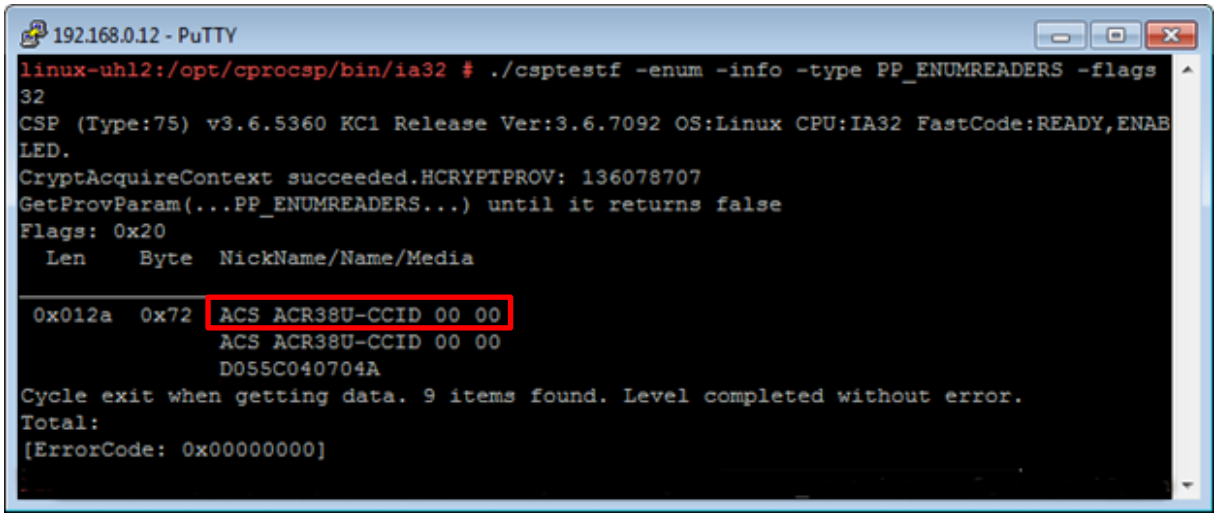
```
rpm –i isbc-cryptopro-x.x-x.x86_64.rpm --nodeps
```

Перейдите в папку, в которой установлены утилиты КриптоПро, например,

```
cd /opt/cprocsp/bin/ia32/
```

Проверьте, видит ли система карту и считыватель:

```
./csptestf -enum -info -type PP_ENUMREADERS -flags 32
```

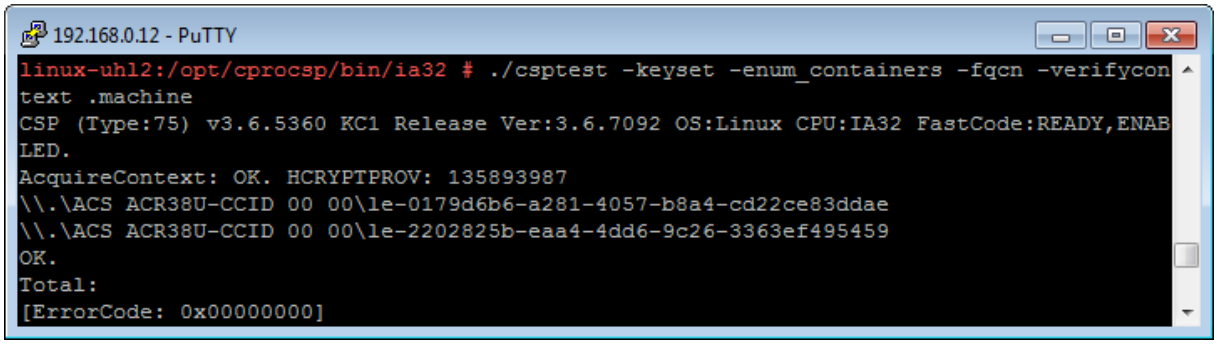


2.2 Просмотр контейнеров

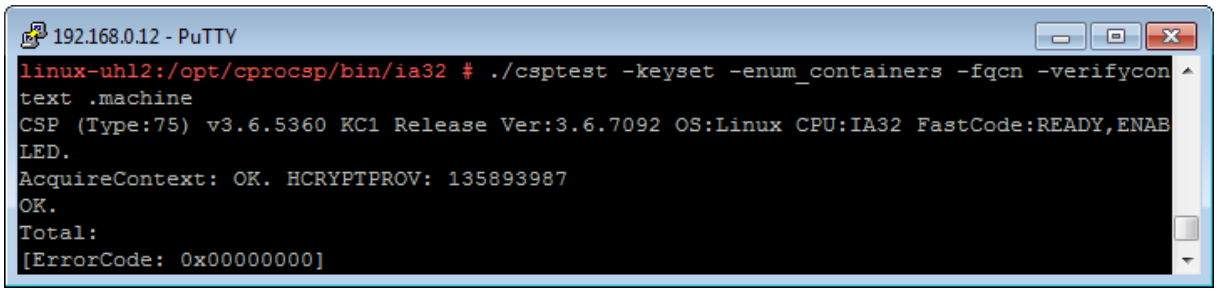
Для просмотра контейнеров на карте выполните:

```
./csptest -keyset -enum_containers -fqcn -verifycontext -machine
```

А) на карте 2 контейнера



Б) на карте нет контейнеров



2.3 Создание ключей и запроса на сертификат

Используйте следующую команду, чтобы создать контейнер, сгенерировать в контейнере ключевую пару и составить запрос на сертификат.

```
./cryptcp -creatrqst -dn CN=test -cont '\\.\ACS ACR38U-CCID 00
00\containername' cert.txt
```

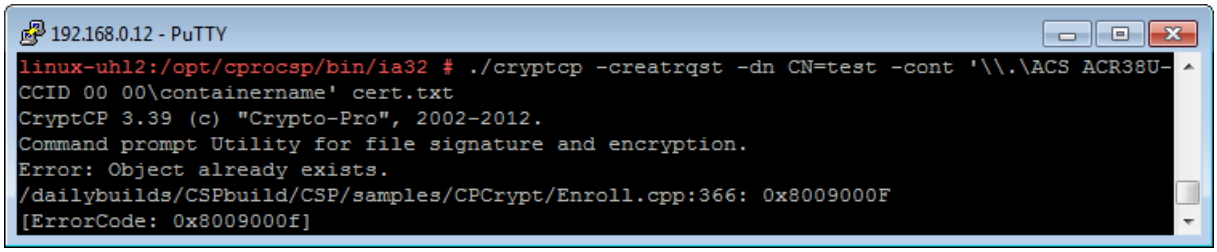
Где:

-creatrqst – команда составить запрос на сертификат

-dn – передать данные для запроса, например Common Name (CN) и др.

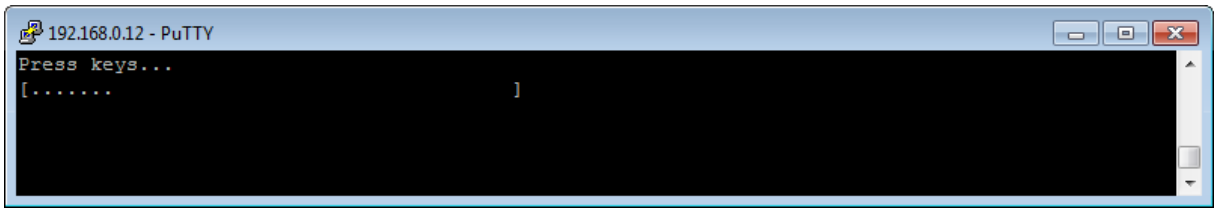
-cont – создать контейнер с уникальным именем

Каждый контейнер, создаваемый на карте, должен иметь уникальное имя, иначе появится сообщение об ошибке[1]:



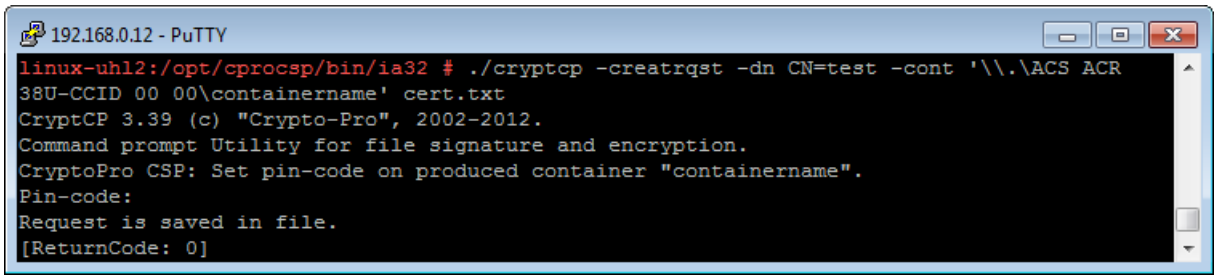
Для генерации ключевой пары требуется большое количество случайных чисел, в качестве вспомогательного средства используются значения интервалов между нажатиями клавиш. Когда появится приглашение, нажимайте произвольные клавиши. Полученные ключи не зависят от введенных символов.

[1] *Имя каждого контейнера должно быть уникальным, причем, если на карте уже был ранее создан контейнер с таким именем, но удален впоследствии, все равно может возникать ошибка*

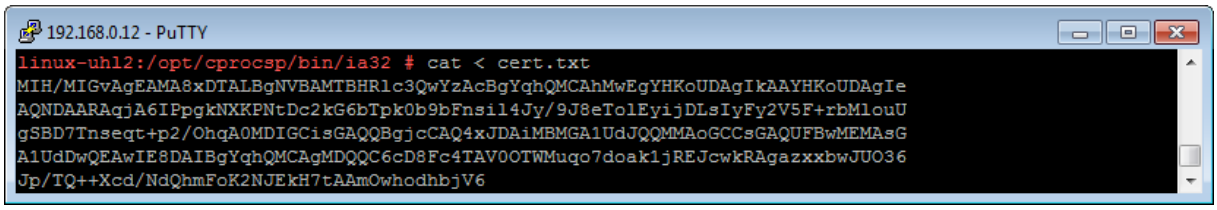


ВНИМАНИЕ! Не нажимайте кнопки слишком быстро! *После того, как закрытый и открытый ключ будут сформированы, появится приглашение ввести ПИН-код к контейнеру (к карте). Поэтому вместо правильного ПИН-кода туда могут попасть случайные символы. Произойдет ошибка и процедуру придется повторить.*

В результате выполнения команды на карте будет создана ключевая пара в контейнере и запрос на сертификат в текстовом файле.



Откройте файл в консоли (cat < cert.txt) или в блокноте и скопируйте его содержимое полностью.

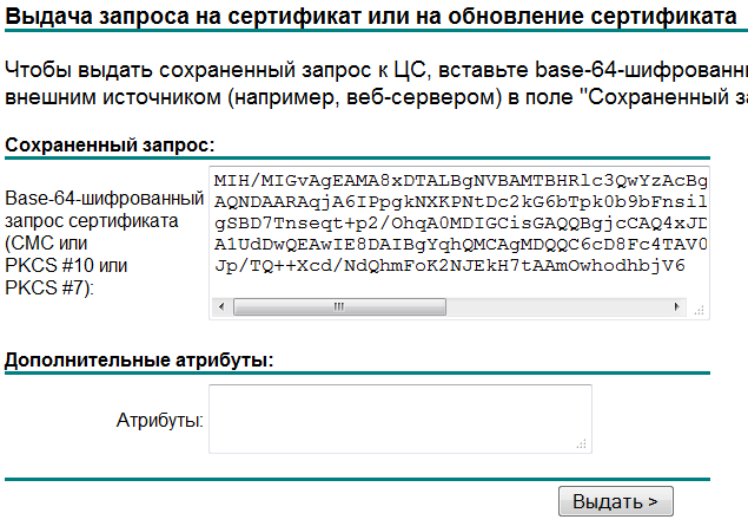


2.4 Получение сертификата в УЦ КриптоПро

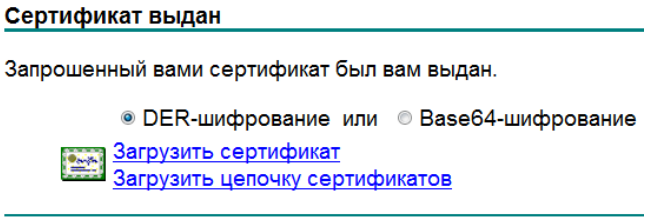
Запрос на сертификат, созданный на предыдущем этапе, содержит данные об открытом ключе пользователя, подписанные его закрытым ключом. Запрос необходимо подписать в УЦ, чтобы получить сертификат.

Перейдите на сайт http://www.cryptopro.ru/certsrv/ и выберите ***Сформировать ключи и отправить запрос на сертификат › Расширенный запрос сертификата.***

Вставьте в поле ***Сохраненный запрос*** *содержимое созданного ранее текстового файла и нажмите* ***Выдать***.



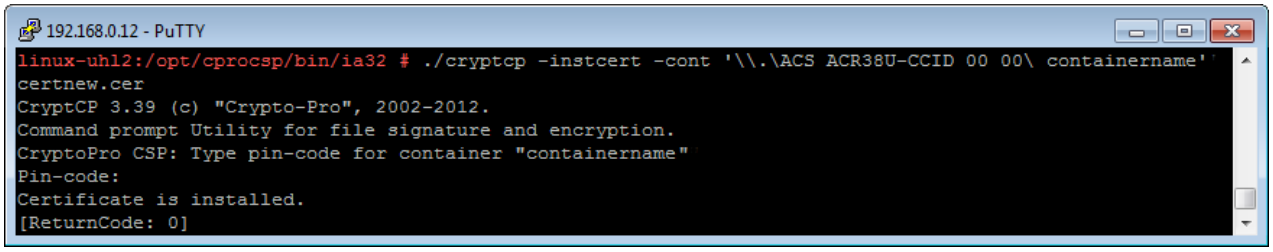
*Скачайте сертификат открытого ключа на карте в формате **DER-шифрование**.*



2.5 Запись сертификата на карту

Используйте следующую команду для записи сертификата на карту, указав название ранее созданного контейнера с соответствующим открытым ключом:

```
./cryptcp -instcert -cont '\\.\ACS ACR38U-CCID 00 00\containername'
certnew.cer
```



ESMART Token готов к работе. Он содержит открытый и закрытый ключ и сертификат, подписанный тестовым УЦ.

2.6 Удаление плагина

В OS Linux для удаления используйте RPM-пакет.

Команда для удаления пакета для 32-битных версий ОС Linux:

```
rpm -e isbc-cryptopro-x.x-x.i586.rpm
```

Команда для удаления пакета для 64-битных версий ОС Linux:

```
rpm -e isbc-cryptopro-x.x-x.x86_64.rpm
```

3. Использование в Mac OS

Далее описана установка и удаление модуля поддержки ESMART Token в качестве ключевого носителя для криптопровайдера КриптоПро CSP . Более подробную работе КриптоПро в Mac OS описана в руководстве https://www.cryptopro.ru/sites/default/files/docs/csp36r3/admin_guide_mac_os_r3.pdf

Криптопровайдер КриптоПро CSP должен быть установлен до установки модуля поддержки ESMART Token.

КриптоПро CSP 3.6 совместим с Mac OS X 10.6, КриптоПро CSP 4.0 совместим с Mac OS X 10.7 и выше.

3.1 Установка модуля поддержки

Скопируйте папку MacOS/cryptopro из дистрибутива ESMART Token на устройство. Запустите терминал и перейдите в скопированную папку на устройстве.

Запустите скрипт установки ***install.sh***

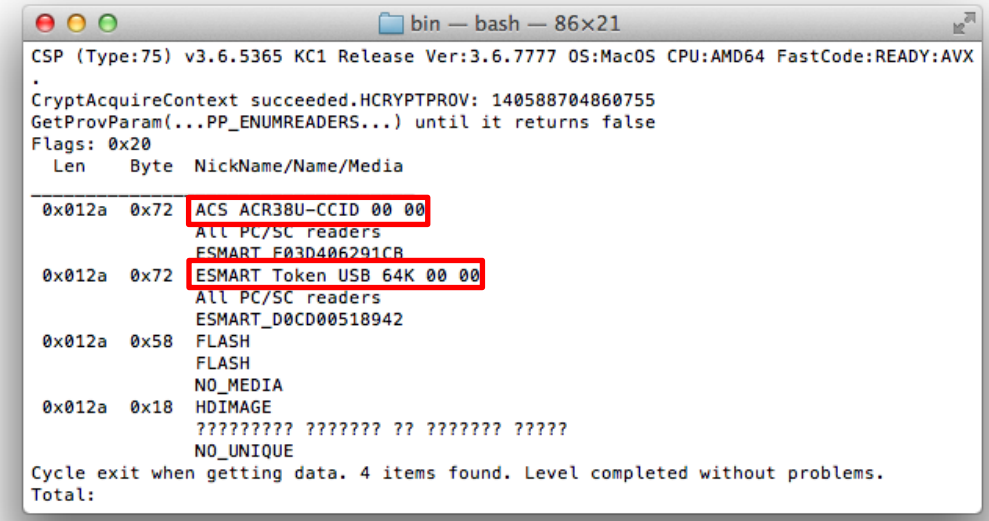
```
sudo ./install.sh
```

Проверьте, видит ли система карту и считыватель. Для этого перейдите в директорию КриптоПро CSP по умолчанию:

```
cd /opt/cprocsp/bin
```

Для получения списка подключенных считывателей, выполните команду:

```
./csptestf -enum -info -type PP_ENUMREADERS -flags 32
```



Красным отмечены имена считывателей.

3.2 Просмотр контейнеров

Для просмотра контейнеров на карте выполните:

```
./csptest -keyset -enum_containers -verifycontext -machine
```

3.3 Создание ключей и запроса на сертификат

Используйте следующую команду, чтобы создать контейнер, сгенерировать в контейнере ключевую пару и составить запрос на сертификат.

```
./cryptcp -creatrqst -dn CN=test -cont '\\.\ACS ACR38U-CCID 00
00\containername' cert.txt
```

Где:

-creatrqst – команда составить запрос на сертификат

-dn – передать данные для запроса, например Common Name (CN) и др.

-cont – создать контейнер с указанием имени считывателя и уникальным именем (\\.\<имя считывателя>\<имя контейнера>)

Каждый контейнер, создаваемый на карте, должен иметь уникальное имя, иначе появится сообщение об ошибке[2]*.*

Для генерации ключевой пары требуется большое количество случайных чисел, в качестве вспомогательного средства используются значения интервалов нажатия клавиш. Когда появится приглашение, нажимайте произвольные клавиши. Полученные ключи не зависят от введенных символов.

***ВНИМАНИЕ! Не нажимайте кнопки слишком быстро!** После того, как закрытый и открытый ключ будут сформированы, появится приглашение ввести ПИН-код к контейнеру (к карте). Поэтому вместо ПИН-кода туда могут попасть случайные символы, произойдет ошибка. Процедуру придется повторить.*

В результате работы команды на карте будет создана ключевая пара в контейнере и запрос на сертификат в текстовом файле.

Откройте файл в консоли (cat < cert.txt) или в блокноте и скопируйте его содержимое полностью.

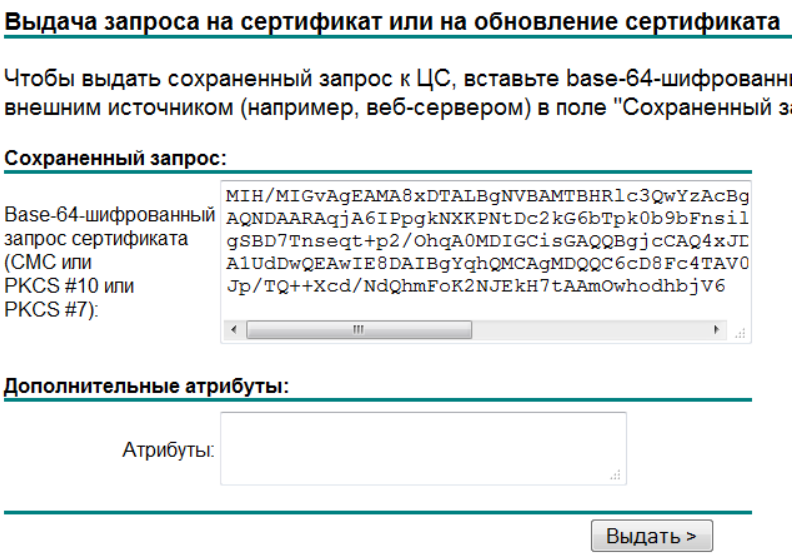
3.4 Получение сертификата в УЦ КриптоПро

Запрос на сертификат, созданный на предыдущем этапе, содержит данные об открытом ключе пользователя, подписанные закрытым ключом пользователя. Запрос необходимо подписать в УЦ, чтобы получить сертификат.

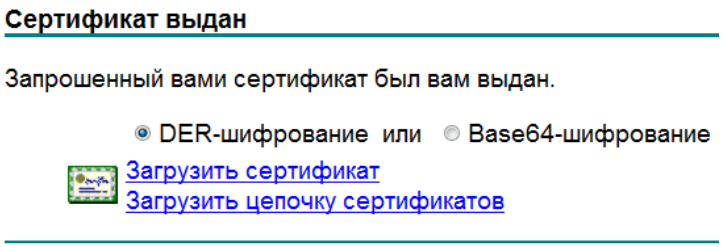
*Перейдите на сайт http://www.cryptopro.ru/certsrv/ и выберите **Сформировать ключи и отправить запрос на сертификат › Расширенный запрос сертификата.***

*Вставьте в поле **Сохраненный запрос** содержимое созданного ранее текстового файла и нажмите **Выдать**.*

[2] *Имя каждого контейнера должно быть уникальным, причем, если на карте уже был ранее создан контейнер с таким именем, но удален впоследствии, все равно может возникать ошибка*



*Скачайте сертификат открытого ключа на карте в формате **DER-шифрование**.*



3.5 Запись сертификата на карту

Используйте следующую команду для записи сертификата на карту, указав название ранее созданного контейнера с соответствующим открытым ключом:

```
./cryptcp -instcert -cont '\\.\ACS ACR38U-CCID 00 00\containername'
certnew.cer
```

ESMART Token готов к работе. Он содержит открытый и закрытый ключ и сертификат, подписанный тестовым УЦ.

3.6 Удаление модуля

Для удаления модуля запустите скрипт uninstall.sh из папки MacOS/cryptopro дистрибутива ESMART Token.

4. Использование в Windows

4.1 Криптопровайдер CryptoPro CSP

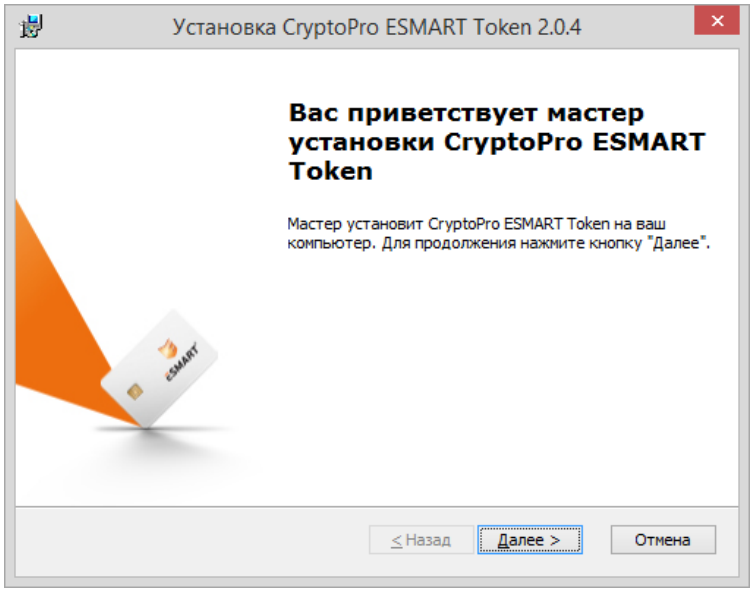
Криптопровайдер CryptoPro CSP обеспечивает взаимодействие карты или USB-ключа ESMART Token и операционной системы Windows. Для работы с отечественными алгоритмами, в системе должен был установлен CryptoPro CSP не ниже 3.6.

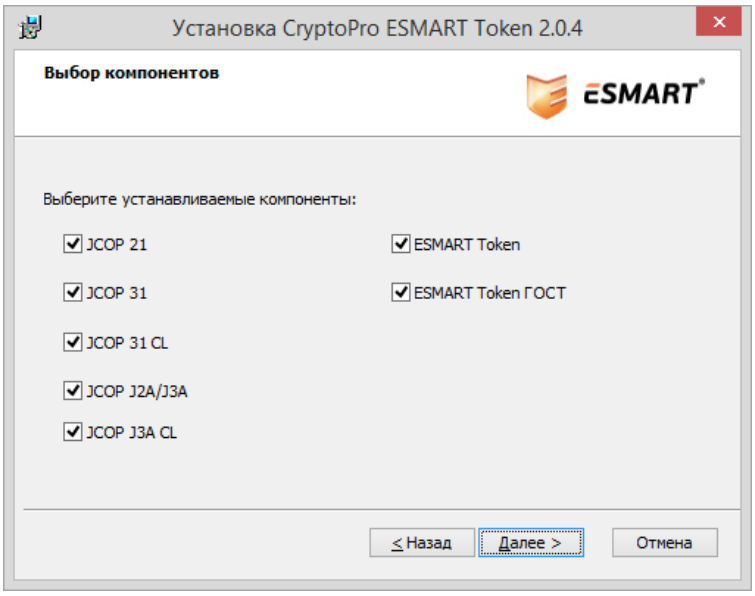
4.2 Плагин ESMART Token CryptoPro

Чтобы криптопровайдер CryptoPro CSP версии ниже 3,6 RC3 использовал в качестве носителей ключевых пар и сертификатов карты и токены ESMART Token, требуется установка плагина совместимости. Установка плагина совместимости для карт ESMART Token ГОСТ требуется для всех версий CryptoPro CSP 3.6 и выше.

Файл программы-инсталлятора находится в папке Windows/cryptopro/CryptoPro ESMART Token.exe.

Прим.: Перед установкой плагина CryptoPro ESMART Token следует установить криптопровайдер CryptoPro CSP и перезагрузить ПК.



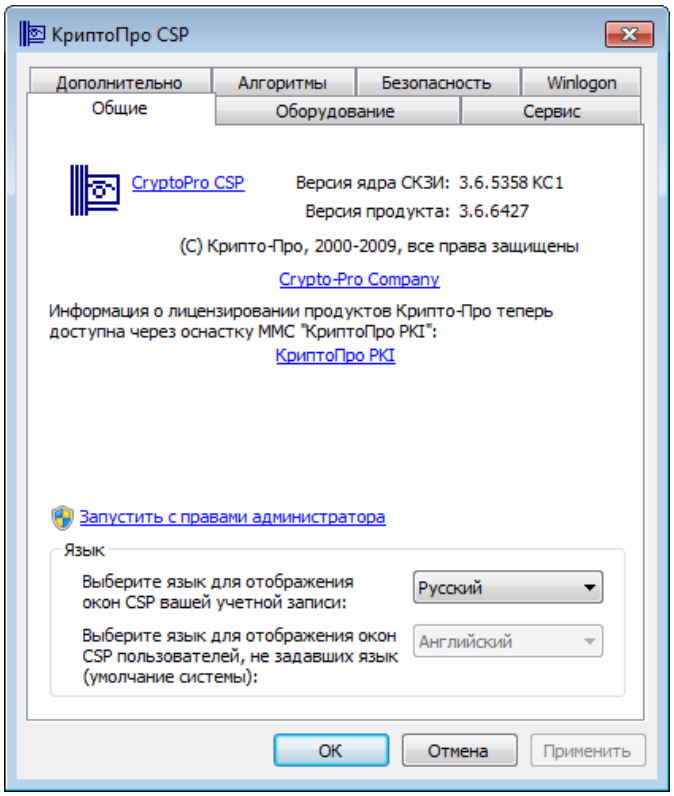


*В следующем окне установите галочку **Удалить конфликтующие записи**. Завершите установку.*

Проверить, правильно ли определяются карты, можно при помощи утилиты CryptoPro CSP, входящей в пакет CryptoPro.

Запустите утилиту по ярлыку Crypto-pro › CryptoPro CSP из меню Пуск или напрямую из папки `X:\Program Files\Crypto Pro\CSP\cpconfigadmin.exe`

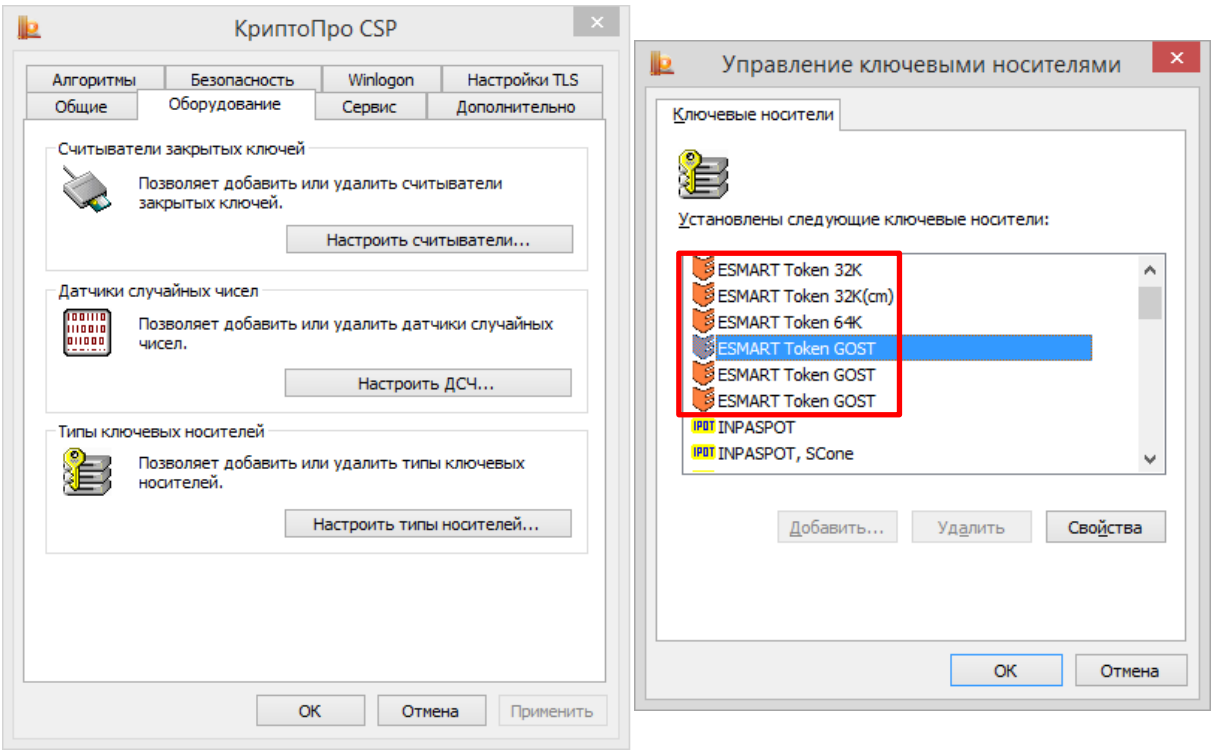
*Желательно запустить программу с правами администратора, нажав на соответствующую ссылку на вкладке **Общие**.*



*Откройте вкладку **Оборудование**. Нажмите **Настроить типы носителей**. В открывшемся окошке пролистайте список и убедитесь, что есть записи, содержащие ESMART Token.*

В списке также могут присутствовать карты JavaCard различных модификаций, если они были установлены.

Если карт ESMART Token в списке нет, установите или повторите установку плагина Esmart Token CryptoPro.

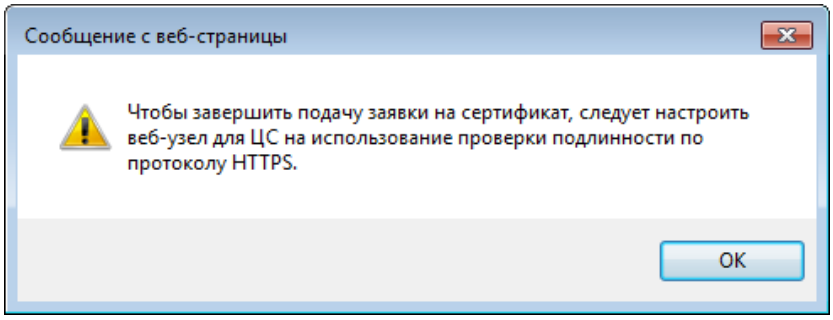

КриптоПро CSP
Алгоритмы
Безопасность
Winlogon
Настройки TLS
Общие
Оборудование
Сервис
Дополнительно
Считыватели закрытых ключей
Позволяет добавить или удалить считыватели закрытых ключей.
Настроить считыватели...
Датчики случайных чисел
Позволяет добавить или удалить датчики случайных чисел.
Настроить ДСЧ...
Типы ключевых носителей
Позволяет добавить или удалить типы ключевых носителей.
Настроить типы носителей...
OK
Отмена
Применить
Управление ключевыми носителями
Ключевые носители
Установлены следующие ключевые носители:
ESMART Token 32K
ESMART Token 32K(cm)
ESMART Token 64K
ESMART Token GOST
ESMART Token GOST
ESMART Token GOST
INPASPOT
INPASPOT, SCone
Добавить...
Удалить
Свойства
OK
Отмена

5. Генерация ключевой пары и выдача сертификата

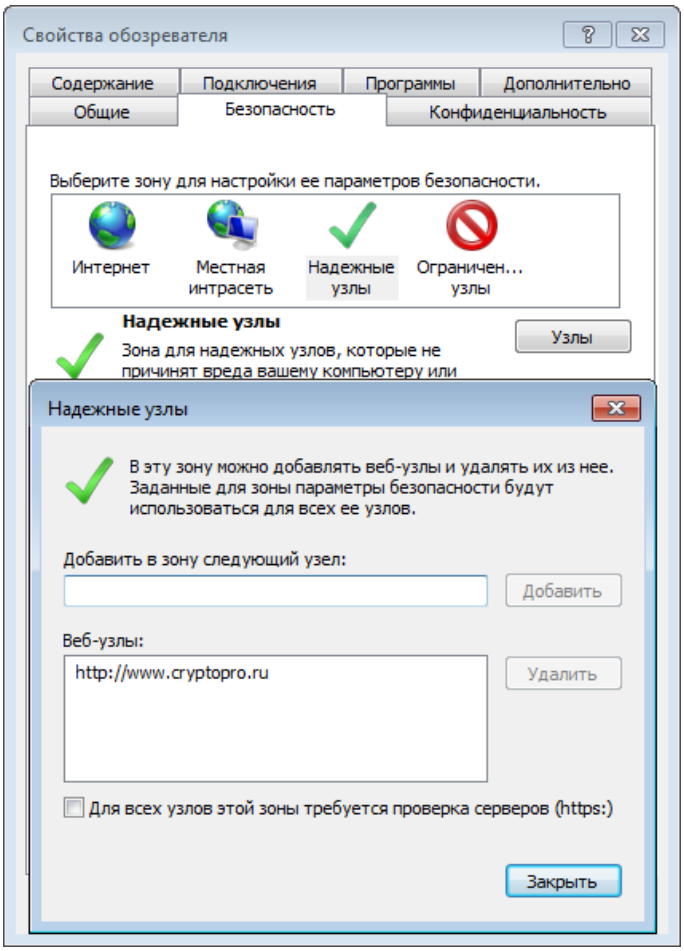
5.1 Настройка Internet Explorer

Для обеспечения работы CryptoPro CSP требуется MS Internet Explorer версии 6.0 и выше. Желательно использовать современные версии 8 или 9.

В браузере должно быть разрешено выполнение элементов управления Active X, иначе будет возникать ошибка:

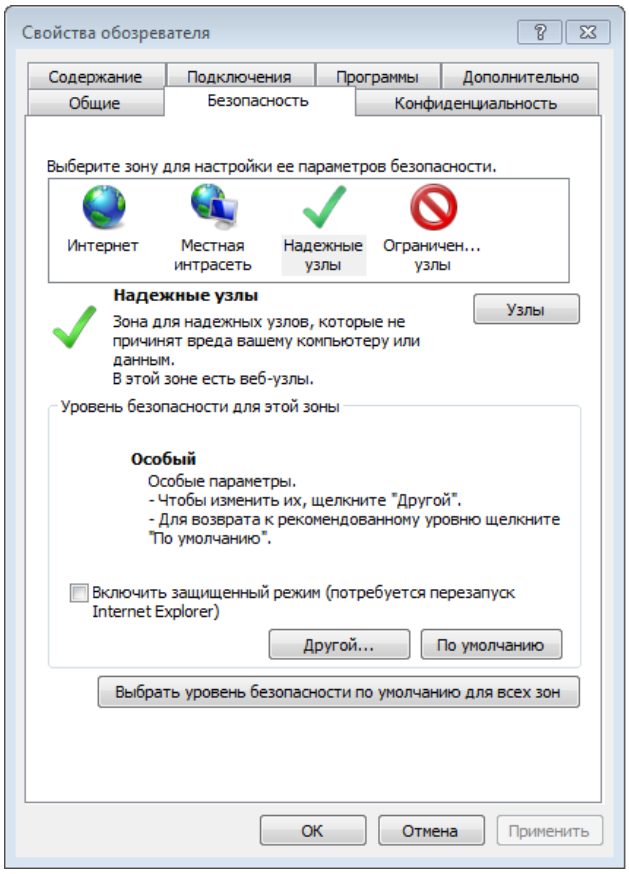


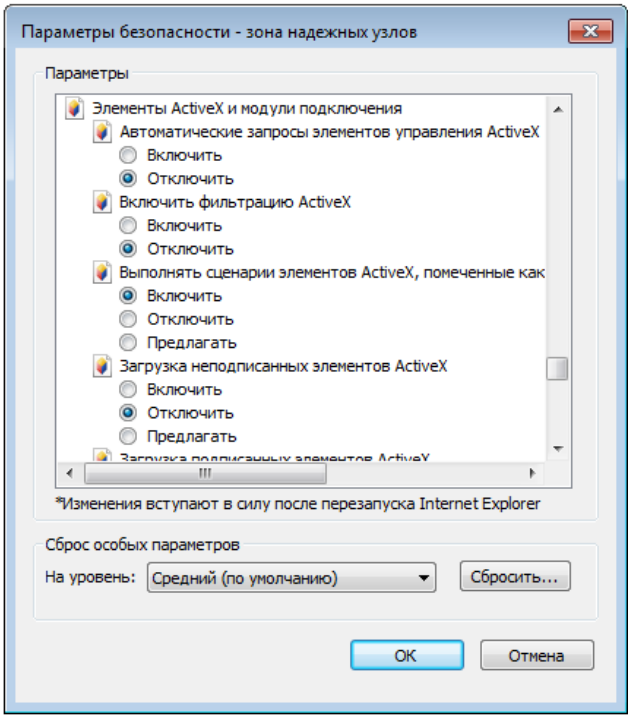
*Откройте настройки обозревателя, вкладка **Безопасность**. Выберите раздел Надежные узлы и нажмите кнопку **Узлы**. В появившемся окне добавьте http://www.cryptopro.ru в зону надежные узлы. Нажмите **Закрыть**.*



*В нижней части экрана нажмите кнопку **Другой**… В появившемся окне прокрутите список и измените следующие параметры:*

1) *Включить фильтрацию Active X – **отключить***
2) *Использование элементов Active X, не помеченных как безопасные для использования – **включить.***

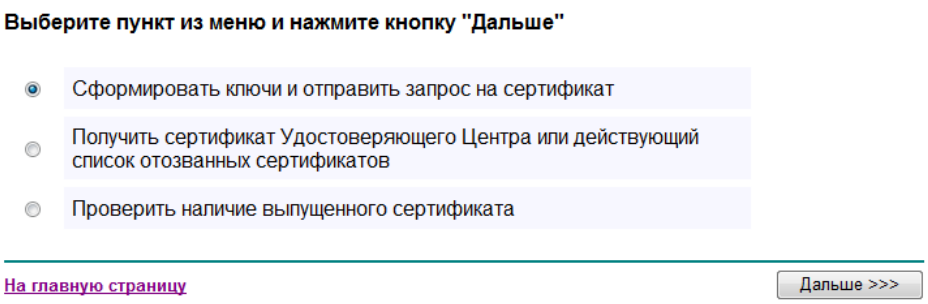




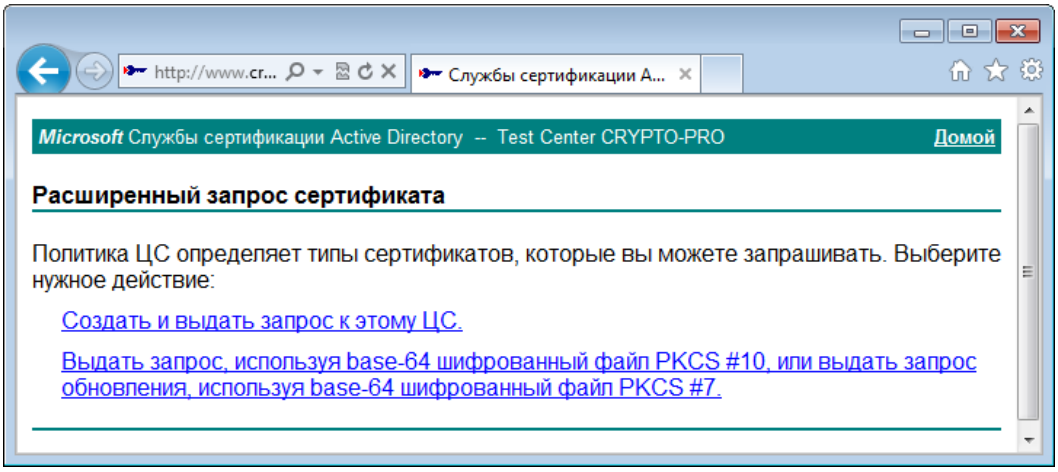
Подтвердите сохранение настроек и обязательно перезапустите Internet Explorer, чтобы изменения вступили в силу.

5.2 Использование тестового УЦ Крипто Про

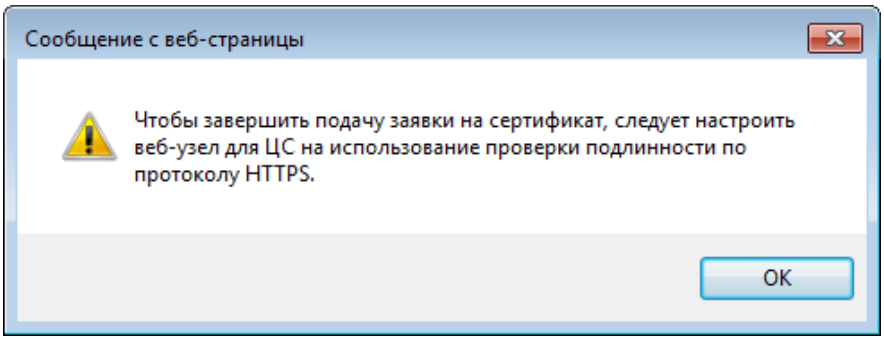
*Откройте веб-интерфейс тестового УЦ Крипто Про http://www.cryptopro.ru/certsrv/. В нижней части страницы перейдите в раздел **Сформировать ключи и отправить запрос на сертификат**.*



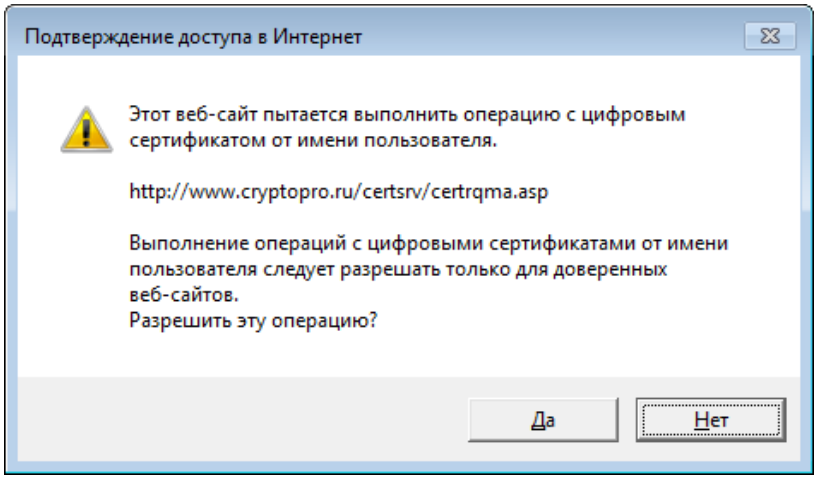
Далее выберите: ***Создать и выдать запрос этому ЦС****.*



Если появляется всплывающее окно (см. рис.), вернитесь к пункту ***Настройка Internet Explorer***



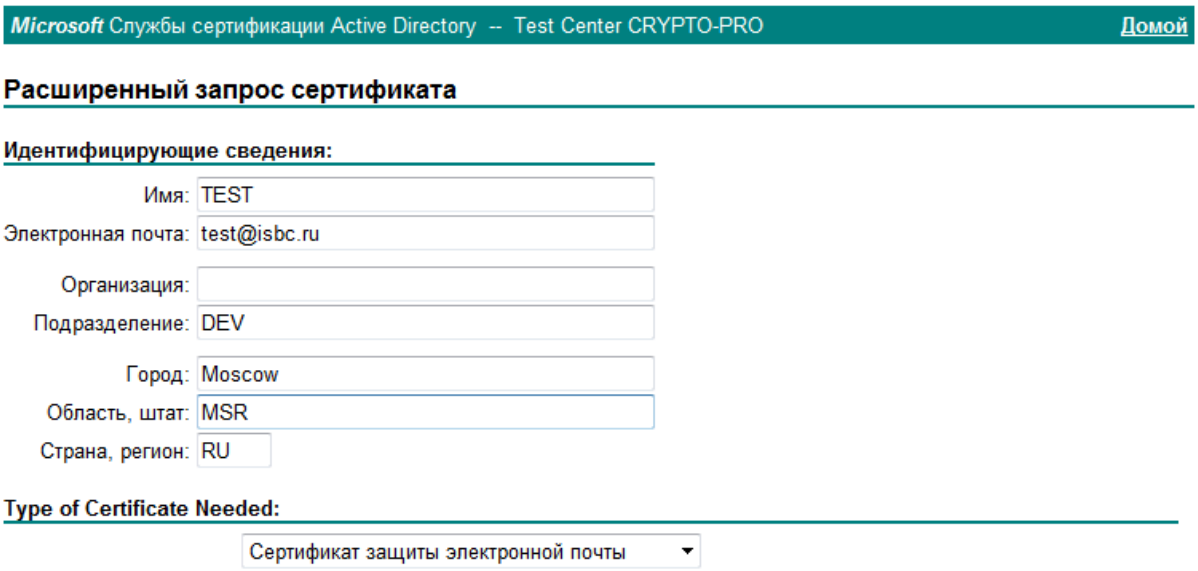
При переходе на страницу должно запрашиваться разрешение на операцию с цифровыми сертификатами:



Подтвердите выполнение операции.

5.3 Заполнение запроса на сертификат

Введите общие сведения для составления запроса на сертификат латинскими буквами и укажите тип запрашиваемого сертификата, например, сертификат защиты электронной почты.



5.4 Параметры ключевой пары

Создайте новый набор ключей. Убедитесь, что в качестве криптопровайдера установлен ***Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider*** *или* ***Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider***.

Если на карте уже был создан контейнер, содержащий открытый и закрытый ключ, выберите опцию ***Использовать существующий набор ключей*** *и укажите имя контейнера.*

Для создания нового контейнера с ключевой парой, выполните действия, описанные далее.

Задайте требуемые параметры ключевой пары и нажмите ***Выдать***.

Параметры ключа:

Создать новый набор ключей Использовать существующий набор ключей

CSP: Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider

Использование ключей: Exchange Подпись Оба

Размер ключа: 512 Минимальный:512 Максимальный:512 (стандартные размеры ключей: 512)

Автоматическое имя контейнера ключа Заданное пользователем имя контейнера ключа

Пометить ключ как экспортируемый

Включить усиленную защиту закрытого ключа

Использовать локальное хранилище компьютера для сертификата

Сохраняет сертификат в локальном хранилище вместо пользовательского хранилища сертификатов. Не устанавливает корневой сертификат ЦС. Необходимо быть администратором, чтобы создать локальное хранилище.

Дополнительные параметры:

Формат запроса: CMC PKCS10

Алгоритм хеширования: GOST R 34.11-94

Используется только для подписания запроса.

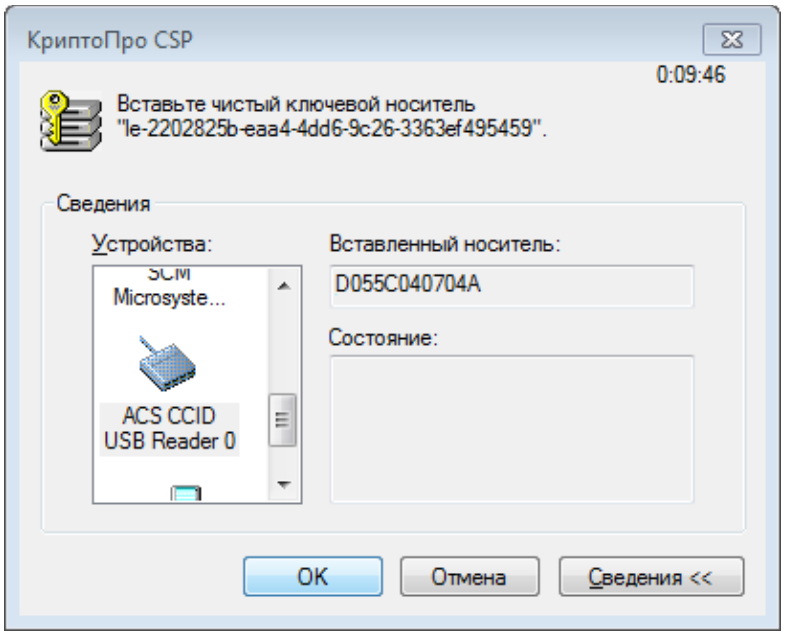
Сохранить запрос

Атрибуты:

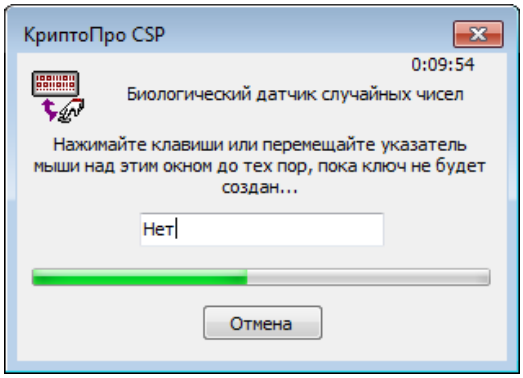
Понятное имя:

Выдать >

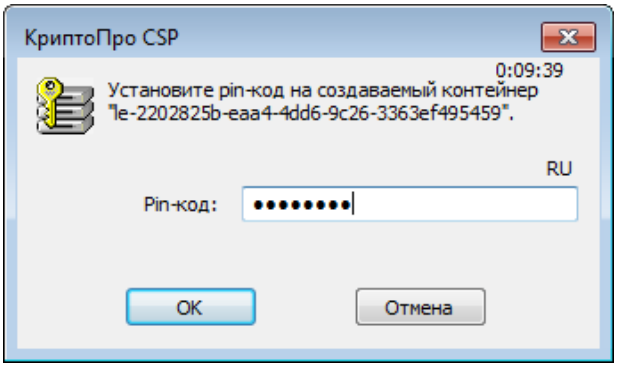
*Криптопровайдер попросит указать, на какой карте создать контейнер и ключевую пару. Выберите носитель и нажмите **OK**.*

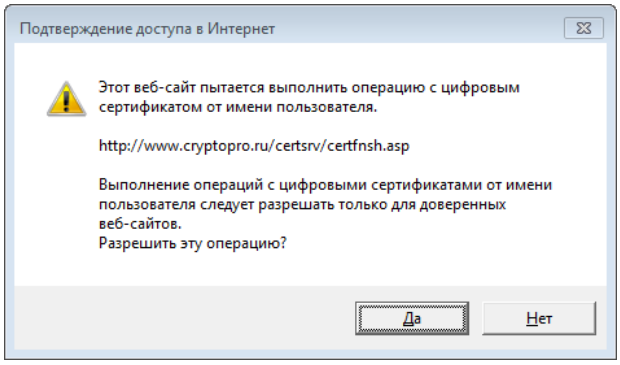


Для генерации ключей требуются случайные числа. Чтобы ускорить процесс создания ключевой пары, водите курсор над окошком в произвольном направлении или вводите с клавиатуры случайные символы[3].

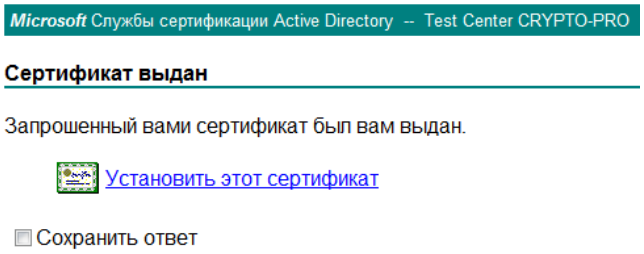


Введите ПИН-код, чтобы ключи были записаны в контейнер и подтвердите выполнение операции:



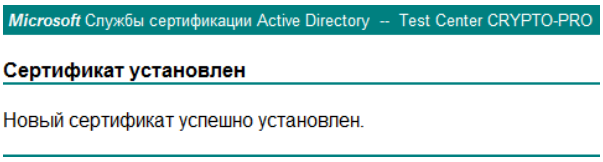


Следующим шагом создается соответствующий сертификат:



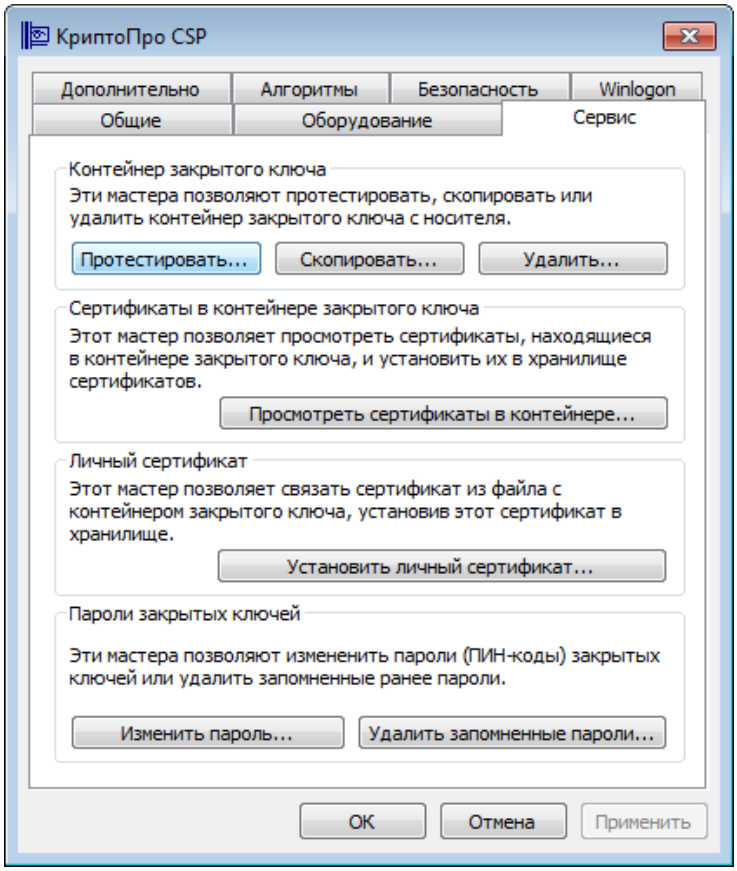
Установите сертификат, нажав на ссылку. Введите ПИН-код и подтвердите операцию. Дождитесь сообщения об успешной установке сертификата.

[3] *Прим.: В качестве случайных чисел сами символы, вводимые с клавиатуры, не используются. Замеряется только период времени между нажатиями клавиш или параметры движения мышки. Поэтому набирая определенную последовательность с клавиатуры нельзя создать или подобрать идентичные пары ключей, ключи всегда будут уникальными.*

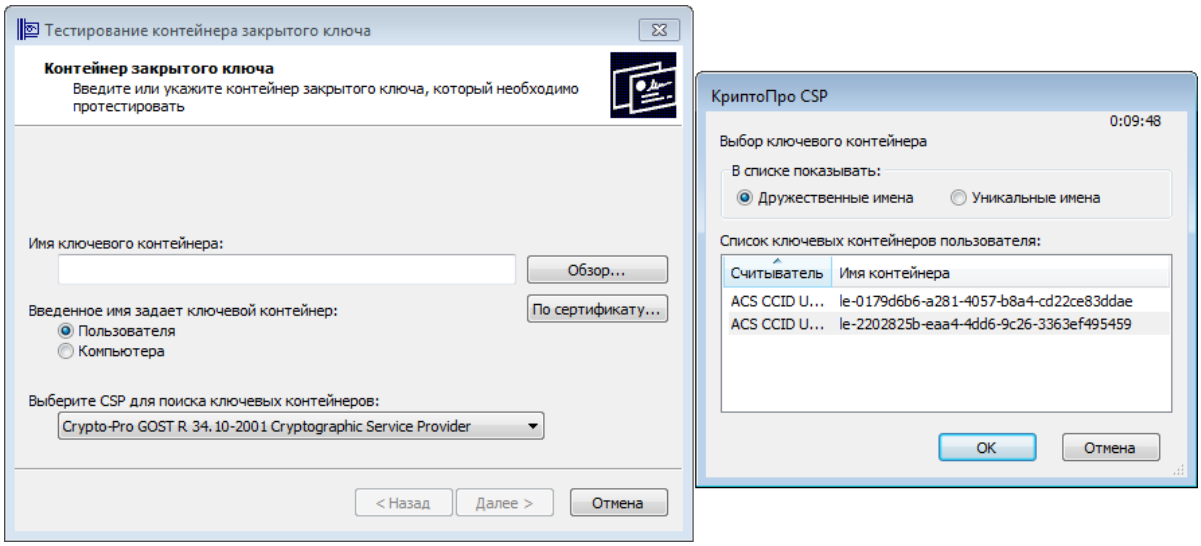


6. Проверка сертификата

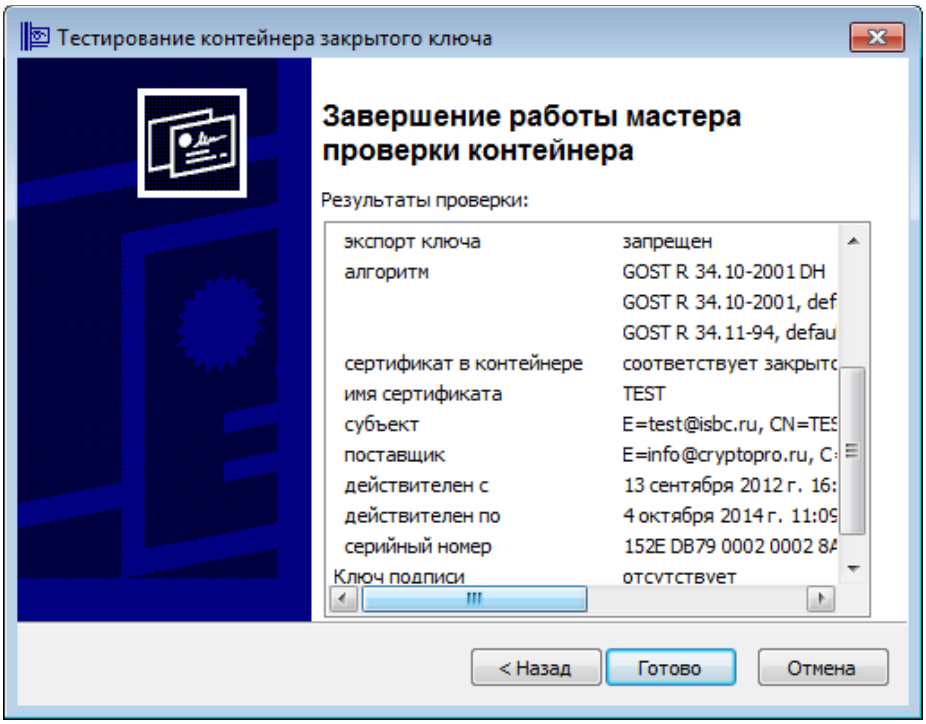
*Для проверки сертификата можно также использовать утилиту CryptoPro CSP (см. раздел **Плагин ESMART Token CryptoPro**). Откройте вкладку **Сервис**. Нажмите **Протестировать**.*



*Чтобы выбрать по названию контейнера с ключевыми парами, нажмите **Обзор** (см. рис.). Чтобы выбрать контейнер, в котором хранится определенный сертификат, нажмите **По сертификату...***



*Выберите контейнер и нажмите **Далее**. Введите ПИН-код. Информация о контейнере и его содержимом появится в отдельном окошке.*



ESMART Token готов к работе. Он содержит закрытый и открытый ключ, а также сертификат открытого ключа, подписанный тестовым УЦ КриптоПро.

6.1 Удаление из системы

Плагин Esmart Token CryptoPro удаляется из ОС Windows через панель управления, раздел «Удаление программ». После удаления плагина ESMART Token перестанет распознаваться как подходящий носитель для УЦ КриптоПро. При необходимости установите плагин заново.