

Плагин ESMART Token CryptoPro



Содержание

1.	Общая информация	3
2.	Использование в Linux	3
2.1	Установка пакета	3
2.2	Просмотр контейнеров	3
2.3	Создание ключей и запроса на сертификат	4
2.4	Получение сертификата в УЦ КриптоПро	5
2.5	Запись сертификата на карту	6
2.6	Удаление плагина	6
3.	Использование в Mac OS	7
3.1	Установка модуля поддержки	7
3.2	Просмотр контейнеров	7
3.3	Создание ключей и запроса на сертификат	8
3.4	Получение сертификата в УЦ КриптоПро	8
3.5	Запись сертификата на карту	9
3.6	Удаление модуля	9
4.	Использование в Windows	10
4.1	Криптопровайдер CryptoPro CSP	10
4.2	Плагин ESMART Token CryptoPro	10
5.	Генерация ключевой пары и выдача сертификата	13
5.1	Настройка Internet Explorer	13
5.2	Использование тестового УЦ Крипто Про	14
5.3	Заполнение запроса на сертификат	16
5.4	Параметры ключевой пары	16
6.	Проверка сертификата	19
6.1	Удаление из системы	20



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 <u>отдельный контейнер с уникальным названием</u>.

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 <u>http://cryptopro.ru/category/faq/linuxunix-0</u>

2.1 Установка пакета

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

Команда для установки пакета для 32-битных версий OC 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

```
- 0 X
🗬 192.168.0.12 - PuTTY
linux-uhl2:/opt/cprocsp/bin/ia32 # ./csptestf -enum -info -type PP_ENUMREADERS -flags
32
CSP (Type:75) v3.6.5360 KC1 Release Ver:3.6.7092 OS:Linux CPU:IA32 FastCode:READY,ENAB
LED.
CryptAcquireContext succeeded.HCRYPTPROV: 136078707
GetProvParam(...PP_ENUMREADERS...) until it returns false
Flags: 0x20
        Byte NickName/Name/Media
 Len
 0x012a 0x72 ACS ACR38U-CCID 00 00
              ACS ACR38U-CCID 00 00
              D055C040704A
Cycle exit when getting data. 9 items found. Level completed without error.
Total:
[ErrorCode: 0x0000000]
```

2.2 Просмотр контейнеров

Для просмотра контейнеров на карте выполните:

ESMART[®] Плагин ESMART Token CryptoPro версия 3.1 от 23.01.2015

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

А) на карте 2 контейнера

📴 192.168.0.12 - PuTTY 💼 📼 💌	
<pre>linux-uhl2:/opt/cprocsp/bin/ia32 # ./csptest -keyset -enum_containers -fqcn -verifycon /</pre>	
text .machine	
CSP (Type:75) v3.6.5360 KC1 Release Ver:3.6.7092 OS:Linux CPU:IA32 FastCode:READY,ENAB	
LED.	
AcquireContext: OK. HCRYPTPROV: 135893987	
\\.\ACS ACR38U-CCID 00 00\le-0179d6b6-a281-4057-b8a4-cd22ce83ddae	
<pre>\\.\ACS ACR38U-CCID 00 00\le-2202825b-eaa4-4dd6-9c26-3363ef495459</pre>	
OK.	
Total:	
[ErrorCode: 0x0000000]	7

Б) на карте нет контейнеров

🛃 192.168.0.12 - PuTTY	x
<pre>linux-uhl2:/opt/cprocsp/bin/ia32 # ./csptest -keyset -enum_containers -fqcn -verifycd</pre>	m 🔺
text .machine	
CSP (Type:75) v3.6.5360 KC1 Release Ver:3.6.7092 OS:Linux CPU:IA32 FastCode:READY,ENA	AB
LED.	
AcquireContext: OK. HCRYPTPROV: 135893987	
ok.	
Total:	
[ErrorCode: 0x00000000]	Ŧ

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 ошибке¹:



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

🛃 192.168.0.12 - PuTTY		
Press keys		A
[]	

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 <u>http://www.cryptopro.ru/certsrv/</u> и выберите **Сформировать ключи и отправить за**прос на сертификат > Расширенный запрос сертификата.

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



Выдача запроса на сертификат или на обновление сертификата

Чтобы выдать сохраненный запрос к ЦС, вставьте base-64-шифрованни внешним источником (например, веб-сервером) в поле "Сохраненный з

Сохраненный запрос	:	
Base-64-шифрованный запрос сертификата (СМС или PKCS #10 или PKCS #7):	MIH/MIGvAgEAMA8xDTALBgNVBAMTBHR1c3QwY2AcH AQNDAARAqjA6IPpgkNXKPNtDc2kG6bTpk0b9bFnsi gSBD7Tnseqt+p2/OhqA0MDIGCisGAQQBgjcCAQ4x A1UdDwQEAwIE8DAIBgYqhQMCAgMDQQC6cD8Fc4TAT Jp/TQ++Xcd/NdQhmFoK2NJEkH7tAAmOwhodhbjV6	3g .1 7C 70
Дополнительные атр	ибуты:	
Атрибуты:	ii.	
	Выдать >	

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

Сертификат выдан	
Запрошенный вами сертификат был ва	ам выдан.
 DER-шифрование или <u>Загрузить сертификат</u> <u>Загрузить цепочку сертифик</u> 	© Base64-шифрование катов

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 OC Linux: rpm -e isbc-cryptopro-x.x-x.i586.rpm Команда для удаления пакета для 64-битных версий OC Linux: rpm -e isbc-cryptopro-x.x-x.x86_64.rpm

ESMART[®] Плагин ESMART Token CryptoPro версия 3.1 от 23.01.2015

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 <u>https://www.cryptopro.ru/sites/default/files/docs/csp36r3/admin_guide_mac_os_r3.pdf</u>

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 Соттоп 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 ошибке².

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 <u>http://www.cryptopro.ru/certsrv/</u> и выберите **Сформировать ключи и отправить за**прос на сертификат > Расширенный запрос сертификата.

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

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



Выдача запроса на сертификат или на обновление сертификата

Чтобы выдать сохраненный запрос к ЦС, вставьте base-64-шифрованні внешним источником (например, веб-сервером) в поле "Сохраненный з

Сохраненный запрос	:
Base-64-шифрованный запрос сертификата (СМС или PKCS #10 или PKCS #7):	MIH/MIGVAGEAMA8xDTALBGNVBAMTBHR1c3QwYzAcBg AQNDAARAqjA6IPpgkNXKPNtDc2kG6bTpk0b9bFnsil gSBD7Tnseqt+p2/OhqA0MDIGCisGAQQBgjcCAQ4xJE A1UdDwQEAwIE8DAIBgYqhQMCAgMDQQC6cD8Fc4TAV0 Jp/TQ++Xcd/NdQhmFoK2NJEkH7tAAmOwhodhbjV6
Дополнительные атр	ибуты:
Атрибуты:	i.
	Выдать >

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

Сертификат выдан

Запрошенный вами сертификат был вам выдан.

 ● DER-шифрование или
 ● Base64-шифрование

 <u>Загрузить сертификат</u>
 <u>Загрузить цепочку сертификатов</u>

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 СтуртоРго СЅР

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 nanke 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**.

🖻 КриптоПро CSP				×
Дополнительно	Алгоритмы	Безопасн	ость	Winlogon
Общие	Оборудов	ание		Сервис
СтурtоРго (С) К Информация о лицен доступна через осна	С <u>SP</u> Версия Версия Крипто-Про, 2000- <u>Сгурто-Рг</u> изировании продул эстку ММС "Крипт КриптоПр	ядра СКЗИ: а продукта: -2009, все пр <u>о Company</u> ктов Крипто оПро РКІ [*] : <u>о РКІ</u>	3.6.535 3.6.642 ава заш	8 КС1 7 иищены терь
Запустить с прак Язык Выберите язык, окон CSP вашей Выберите язык, CSP пользовате, (умолчание сист	вами администрат для отображения учетной записи: для отображения пей, не задавших емы):	ора Русси окон язык	сий ийский	•
	ОК	Отм	іена	Применить

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.



P	Крипто	Про CSP	>	<			
Алгоритмы Общие	Безопасность Оборудование	Winlogon Сервис	Настройки TLS Дополнительно		Управление ключ	евыми нос	ителями 🗙
Считывател	и закрытых ключей озволяет добавить и акрытых ключей.	пи удалить счит Настроить счи	ыватели		Сстановлены следующие кли	очевые носител	и:
Датчики слу	чайных чисел озволяет добавить и исел.	пи удалить дат Настроити	чики случайных » ДСЧ		ESMART Token 32K ESMART Token 32K(cm) ESMART Token 64K ESMART Token GOST ESMART Token GOST ESMART Token GOST		
Типы ключе Пара	вых носителей озволяет добавить и осителей.	ли удалить типь Настроить типь	ы ключевых I носителей		ини посто области област	Уд <u>а</u> лить	✓ Свойства
	Oł	(Отм	ена Применить			ОК	Отмена



5. Генерация ключевой пары и выдача сертификата

5.1 Hacmpoйка 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 <u>http://www.cryptopro.ru</u> в зону надежные узлы. Нажмите **Закрыть**.

оиства обозрев	зателя			
Содержание	Подключени	ия Пр	ограммы	Дополнительно
Общие	Безопасно	ость	Конфи	иденциальность
Выберите зону	для настройки	ее парамет	гров безопа	асности.
Интернет	Местная	Надежны	е Ограни	чен
,	интрасеть	узлы	узл	ы
Наде	жные узлы			Varia
Зона д	ля надежных уз	злов, кото	рые не	УЗЛЫ
причин	ят вреда ваше	му компью	теру или	
Надежные узл				
В эту Задан	ы зону можно доб ные для зоны г	авлять ве параметры	б-узлы и уд безопаснос	алять их из нее. ти будут
В эту Задан испол Добавить в зо	ы зону можно доб иные для зоны г ьзоваться для в ну следующий	авлять ве параметры всех ее узл узел:	б-узлы и уд безопаснос юв.	алять их из нее. ти будут Добавить
В эту Задан испол Добавить в зс Веб-узлы:	ы зону можно доб иные для зоны г ьзоваться для в эну следующий	авлять ве параметры всех ее узл узел:	б-узлы и уд безопаснос юв.	алять их из нее. ти будут Добавить
В эту Задан испол Добавить в зо Веб-узлы: http://www.o	ы зону можно доб иные для зоны п ъзоваться для в эну следующий атурtopro.ru	авлять ве параметры всех ее узл узел:	б-узлы и уд безопаснос юв.	Далять их из нее. ти будут Добавить Удалить
В эту Задан испол Добавить в зо Веб-узлы: http://www.o	ы зону можно доб ные для зоны г ьзоваться для t эну следующий сгурtopro.ru злов этой зоны	авлять ве араметры узел: узел: требуется	б-узлы и уд безопаснос юв.	алять их из нее. ти будут Добавить Удалить серверов (https:)

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.

Свойства обозревателя	Параметры безопасности - зона надежных уздов
Содержание Подключения Программы Дополнительно	Параметры
Выберите зону для настройки ее параметров безопасности.	 Элементы ActiveX и модули подключения Автоматические запросы элементов управления ActiveX Включить Отключить Включить фильтов имо ActiveX
Интернет Местная Надежные Ограничен интрасеть узлы узлы	 Включить Отключить
Надежные узлы Зона для надежных узлов, которые не причинят вреда вашему компьютеру или данным. В этой зоне есть веб-узлы. Уровень безопасности для этой зоны	 выполнять сценарии элементов ActiveX, помеченные как Включить Отключить Предлагать Загрузка неподписанных элементов ActiveX Включить Отключить Отключить
Особый Особые параметры. - Чтобы изменить их, щелкните "Другой". - Для возврата к рекомендованному уровню щелкните "По умолчанию".	Предлагать Заглизиз поллисзии и элементов Астімах Тії Заглизиз поллисзии и элементов Астімах *Изменения вступают в силу после перезапуска Internet Explorer Сброс особых параметров
Включить защищенный режим (потребуется перезапуск Internet Explorer)	На уровень: Средний (по умолчанию) 🔻 Сбросить
Выбрать уровень безопасности по умолчанию для всех зон	ОК Отмена
ОК Отмена Применить	

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 <u>http://www.cryptopro.ru/certsrv/</u>. В нижней части страницы перейдите в раздел **Сформировать ключи и отправить запрос на сертификат**.

	Сформировать ключи и отправить запрос на сертификат	
)	Получить сертификат Удостоверяющего Центра или действующий список отозванных сертификатов	
)	Проверить наличие выпущенного сертификата	



Далее выберите: Создать и выдать запрос этому ЦС.



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



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

Подтверж	дение доступа в Интернет	8
<u>^</u>	Этот веб-сайт пытается выполнить операцию с цифровым сертификатом от имени пользователя. http://www.cryptopro.ru/certsrv/certrqma.asp Выполнение операций с цифровыми сертификатами от имени пользователя следует разрешать только для доверенных веб-сайтов. Разрешить эту операцию?	
	<u>Д</u> а <u>Н</u> ет	

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.

Microsoft Службы сертификации Active Directory -- Test Center CRYPTO-PRO

Домой

Расширенный запрос сертификата Идентифицирующие сведения: Имя: TEST Электронная почта: test@isbc.ru Организация: Подразделение: DEV Город: Moscow Область, штат: MSR Страна, регион: RU Туре of Certificate Needed: 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 пара	аметры:			
Формат запроса:	© CMC ● PKCS10			
Алгоритм хеширования:	GOST R 34.11-94 ▼ Используется только для подписания запроса.			
	Сохранить запрос			
Атрибуты:	→ → 4 →			
Понятное имя:				
	Выдать >			

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



Для генерации ключей требуются случайные числа. Чтобы ускорить процесс создания ключевой пары, водите курсор над окошком в произвольном направлении или вводите с клавиатуры случайные символы³.



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

КриптоПро CSP	Подтверждение доступа в Интернет	
0:09:39 Установите pin-код на создаваемый контейнер Те-2202825b-еаа4-4dd6-9c26-3363ef495459".	Этот веб-сайт пытается выполнить операцию с цифровым сертификатом от имени пользователя.	
RU Ріп-код: ••••••	http://www.cryptopro.ru/certsrv/certfnsh.asp Выполнение операций с цифровыми сертификатами от имени пользователя следует разрешать только для доверенных веб-сайтов. Разрешить эту операцию?	
ОК Отмена	Да Нет	

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.

		Безопасность	Winlogon	
06000	Оборулов		Сервис	
Контейнер закрытого ключа Эти мастера позволяют протестировать, скопировать или удалить контейнер закрытого ключа с носителя. Протестировать Удалить Сертификаты в контейнере закрытого ключа Этот мастер позволяет просмотреть сертификаты, находящиеся в контейнере закрытого ключа, и установить их в хранилище				
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 измененить пароли (ПИН-коды) закрытых ключей или удалить запомненные ранее пароли. Изменить пароль Удалить запомненные пароли				

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



📴 Тестирование контейнера закрытого ключа 🖾	
Контейнер закрытого ключа Введите или укажите контейнер закрытого ключа, который необходимо протестировать	КриптоПро CSP
	0:09:48 Выбор ключевого контейнера В списке показывать:
Имя ключевого контейнера: Обзор	Список ключевых контейнеров пользователя: Считыватель Имя контейнера
Введенное имя задает ключевой контейнер: По сертификату © Пользователя © Компьютера	ACS CCID U le-0179d6b6-a281-4057-b8a4-cd22ce83ddae ACS CCID U le-2202825b-eaa4-4dd6-9c26-3363ef495459
Выберите CSP для поиска ключевых контейнеров: Crypto-Pro GOST R 34, 10-2001 Cryptographic Service Provider	ОК Отмена
< Назад Далее > Отмена	

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

🖭 Тестирование контейнера закрытого ключа 🛛 🖂						
Завершение работы мастера проверки контейнера Результаты проверки:						
	экспорт ключа	запрещен 🔺				
	алгоритм	GOST R 34.10-2001 DH				
		GOST R 34.10-2001, def				
		GOST R 34.11-94, defau				
a start and a start and a start	сертификат в контейнере	соответствует закрытс				
	имя сертификата	TEST				
	субъект	E=test@isbc.ru, CN=TES				
	поставщик	E=info@cryptopro.ru, C: ≡				
	действителен с	13 сентября 2012 г. 16:				
	действителен по	4 октября 2014г. 11:09				
	серийный номер	152E DB79 0002 0002 84				
	Ключ подписи	отсутствует				
< Назад Готово Отмена						

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.