КриптоПро

Содержание

О КриптоПро

КриптоПро — линейка криптографических утилит (вспомогательных программ) — так называемых криптопровайдеров. Они используются во многих программах российских разработчиков для генерации ЭЦП, работы с сертификатами, организации структуры PKI и т.д.

Сайт: http://www.cryptopro.ru/

Совместимость

По информации разработчика, с ALT Linux совместимы следующие продукты КриптоПро:

- КриптоПро CSP

- КриптоПро JCP
- КриптоПро HSM
- КриптоПро TSP
- КриптоПро OCSP
- КриптоПро ЭЦП Browser plug-in
- КриптоПро SSF
- КриптоПро Stunnel
- Браузер КриптоПро Fox

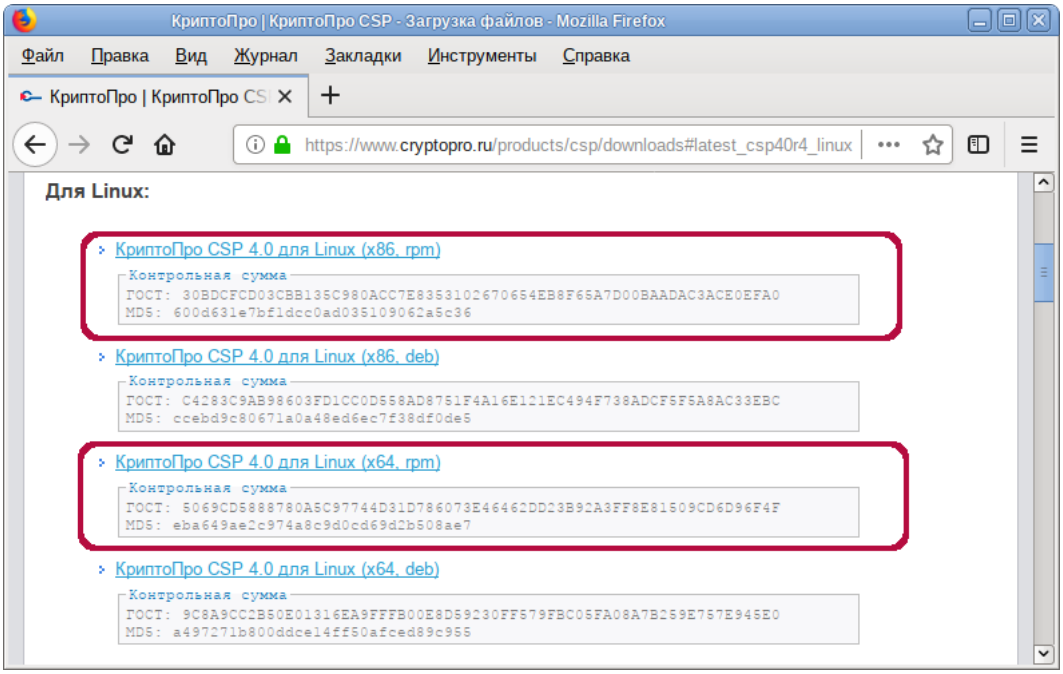
> **Примечание:** В репозитории доступен пакет `firefox-gost`, аналогичный КриптоПро Fox, с патчем от КриптоПро.

Установка КриптоПро CSP

Загрузка

Архив с программным обеспечением (КриптоПро CSP 4.0 R4 — сертифицированная версия, КриптоПро CSP 5.0 — несертифицированная) можно загрузить (http://www.cryptopro.ru/downloads) после предварительной регистрации (http://www.cryptopro.ru/products/csp/overview):

- linux-ia32.tgz (19,3 МБ, для i586) КриптоПро CSP 4.0 для Linux (x86, rpm) для 32 разрядный систем;
- linux-amd64.tgz (20,1 МБ, для x86_64) КриптоПро CSP 4.0 для Linux (x64, rpm) для 64 разрядный систем.



> **Внимание!** По умолчанию при скачивании с сайта КриптоПро выдаётся лицензия **на три месяца**

Установка пакетов

1. Установите пакет `cryptopro-preinstall`:

```
# apt-get install cryptopro-preinstall
```

Этот пакет установит все требуемое для КриптоПро (включая инфраструктуру поддержки карт Рутокен S и Рутокен ЭЦП).

> **Примечание:** Пакет `cryptopro-preinstall` вытягивает зависимости `libpangox-compat`, `opensc`, `pcsc-lite`, `pcsc-lite-rutokens`, `pcsc-lite-ccid`, `newt52`.

2. Распакуйте архив, скачанный с официального сайта КриптоПро:

```
$ tar -xf linux-amd64.tgz
```

Таблица 1. Описание необходимых пакетов КриптоПро.

Пакет	Описание
Базовые пакеты:	
`cprocsp-curl`	Библиотека libcurl с реализацией шифрования по ГОСТ
`lsb-cprocsp-base`	Основной пакет КриптоПро CSP
`lsb-cprocsp-capilite`	Интерфейс CAPILite и утилиты
`lsb-cprocsp-kc1`	Провайдер криптографической службы KC1

lsb-cprocsp-kc2	Провайдер криптографической службы KC2 (требует наличия аппаратного датчика случайных чисел или гаммы)
lsb-cprocsp-rdr	Поддержка ридеров и RNG
Дополнительные пакеты:	
cprocsp-rdr-gui-gtk	Графический интерфейс для диалоговых операций
cprocsp-rdr-rutoken	Поддержка карт Рутокен
cprocsp-rdr-jacarta	Поддержка карт JaCarta
cprocsp-rdr-pcsc	Компоненты PC/SC для ридеров КриптоПро CSP
lsb-cprocsp-pkcs11	Поддержка PKCS11
ifd-rutokens	Конфигурация Рутокеновских карт (или можно взять pcsc-lite-rutokens из репозитория)

3. Установите пакеты КриптоПро:

- под правами пользователя root перейдите в папку с распакованным архивом:

```
# cd /home/user/linux-amd64/
```

- установите базовые пакеты:

```
# apt-get install cprocsp-curl* lsb-cprocsp-base* lsb-cprocsp-capilite* lsb-cprocsp-kc1* lsb-cprocsp-rdr-64*
```

Примечание: Для 32-битной версии вместо последнего пакета — lsb-cprocsp-rdr-4*

- установите пакеты для поддержки токенов (Рутокен S и Рутокен ЭЦП):

```
# apt-get install cprocsp-rdr-gui-gtk* cprocsp-rdr-rutoken* cprocsp-rdr-pcsc* lsb-cprocsp-pkcs11* pcsc-lite-rutokens pcsc-lite-ccid
```

- установите пакет для поддержки токенов (JaCarta):

```
# apt-get install cprocsp-rdr-jacarta*
```

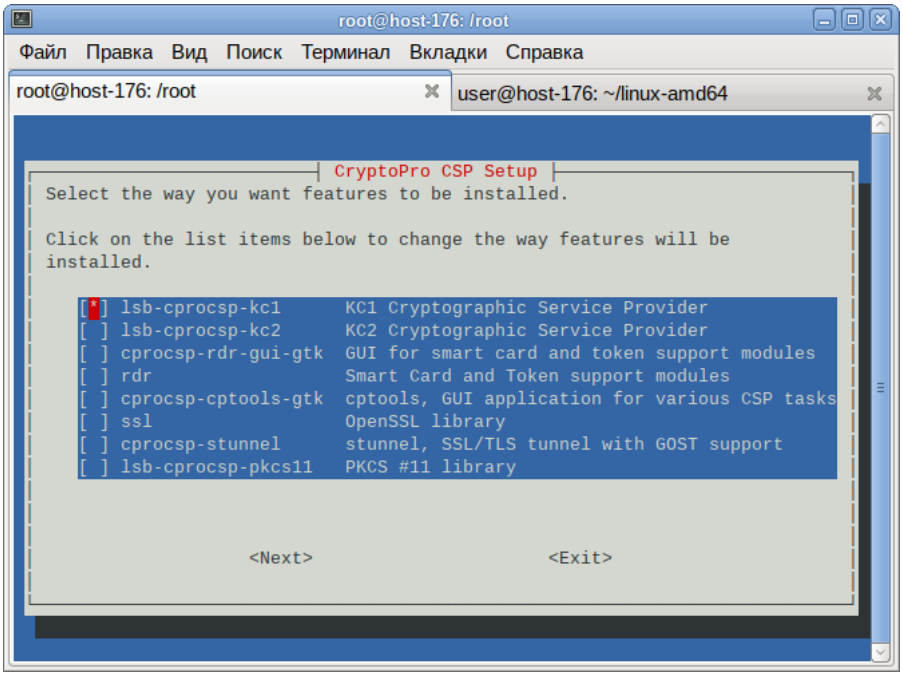
Примечание: Для установки cprocsp-rdr-jacarta может понадобиться предварительно удалить openct.

- Для установки сертификатов Главного удостоверяющего центра:

```
# apt-get install lsb-cprocsp-ca-certs*
```

Можно выполнить установку КриптоПро, запустив ./install_gui.sh в распакованном каталоге и выбрав необходимые модули:

```
# /home/user/install_gui.sh
```



Примечания:

- Для КриптоПро CSP 3.6 R2 потребуется установить пакет cprocsp-compat-altlinux-1.0.0-1.noarch.rpm
- Для установки cprocsp-rdr-gui может понадобиться libXm.so.3 (https://bugzilla.altlinux.org/show_bug.cgi?id=27115) (libopenmotif3) и для вывода кириллицы fonts-bitmap-cyr_rfx-iso8859-5.
- Для установки cprocsp-rdr-gui-gtk потребуется предварительно установить libpangox-compat.
- В версии 4.0.0-alt5 пакета cryptopro-preinstall добавлены подпакеты:
  - cryptopro-preinstall-base для установки с cprocsp-compat-altlinux, «предоставляющим» lsb (в случае нежелательности «лишних» зависимостей вроде libqt3), и
  - cryptopro-preinstall-full для автоустановки зависимостей cprocsp-rdr-gui.

Обновление КриптоПро

> **Внимание!** Пакеты КриптоПро становятся нерабочие при их обновлении. Рекомендуется удалить все пакеты и установить пакеты снова.

Для обновления КриптоПро необходимо:

1. Запомнить текущую конфигурацию:
   - набор установленных пакетов:

     ```
     $ rpm -qa | grep cprocsp
     ```

   - настройки провайдера (для простоты можно сохранить `/etc/opt/cprocsp/config[64].ini`).
2. Удалить штатными средствами ОС все пакеты КриптоПро:

   ```
   # apt-get remove lsb-cprocsp-base
   ```

3. Установить аналогичные новые пакеты КриптоПро.
4. При необходимости внести изменения в настройки (можно просмотреть diff старого и нового `/etc/opt/cprocsp/config[64].ini`).
5. Ключи и сертификаты сохраняются автоматически.

Прописывание путей к исполняемым файлам

Утилиты КриптоПро расположены в директориях `/opt/cprocsp/sbin/<название_архитектуры>` и `/opt/cprocsp/bin/<название_архитектуры>`.

Чтобы каждый раз не вводить полный путь к утилитам КриптоПро:

- после установки пакета `cryptopro-preinstall` начните новый сеанс пользователя в консоли;

> **Примечание:** Не работает для суперпользователя.

или

- выполните от имени пользователя, который будет запускать команды (будет действовать до закрытия терминала):

```
export PATH="$(/bin/ls -d /opt/cprocsp/{s,}bin/*|tr '\n' ':')$PATH"
```

> **Внимание!** Если установлен пакет `mono` или `mono4-devel`, может быть конфликт по имени утилиты certmgr

Проверка лицензии

Проверить срок истечения лицензии можно командой (обратите внимание на строки **Expires:**):

```
$ cpconfig -license -view
License validity:
4040E-G0037-EK8R3-C6K4U-HCXQG
Expires: 2 month(s) 23 day(s)
License type: Server.
```

> **Примечание:** Для версии КриптоПро CSP под Linux все лицензии считаются серверными, поэтому не смущайтесь строкой «License type: Server».

Для установки другой лицензии выполните (под root):

```
# cpconfig -license -set <серийный_номер>
```

> **Примечание:** Серийный номер следует вводить с соблюдением регистра символов.

Проверка версии

Проверить версию КриптоПро можно командой:

```
$ csptest -keyset -verifycontext | sed -n 's/.* Ver:*\([0-9.]\+\).*/\1/p'
4.0.9963
```

Удаление КриптоПро

```
# apt-get remove lsb-cprocsp-base
```

Настройка оборудования

Настройка устройств хранения (носителей) и считывания (считывателей) ключевой информации и датчиков случайных чисел.

> **Примечание:** Если не работает под обычным пользователем, то проверить правила polkit (https://access.redhat.com/blogs/766093/posts/1976313).

Считыватели (readers) — устройства, предназначенные для чтения ключей. К считывателям относится считыватели дискет (FAT12), считыватели флеш-накопителей (FLASH), считыватели смарт-карт и токенов, считыватель образа дискеты на жестком диске (HDIMAGE) и др.

Ключевые носители (media) являются местом хранения электронной подписи. В качестве носителя ключевой информации могут использоваться: защищенный флэш-накопитель (токен) (Рутокен, JaCarta, ESMART и др.), смарт-карта, флэш-накопитель, дискета.

Ключевые контейнеры — это способ хранения закрытых ключей, реализованный в КриптоПро. Их физическое представление зависит от типа ключевого носителя (на флеш-накопителе, дискете, жестком диске это каталог в котором хранится набор файлов с ключевой информацией; в случае со смарт-картами — файлы в защищенной памяти смарт-карты).

Встроенный в «КриптоПро CSP» датчик случайных чисел (далее ДСЧ) используется для генерации ключей.

Для смарт-карт: ключи дополнительно защищаются кодом доступа к защищенной памяти смарт-карты (PIN). При всех операциях с защищенной памятью (чтение, запись, удаление...) требуется вводить PIN. Для других носителей: для повышения безопасности на контейнер можно установить пароль. В этом случае всё содержимое контейнера хранится не в открытом виде, а в зашифрованном на этом пароле. Пароль задается при создании контейнера, в дальнейшем для чтения ключей из контейнера необходимо будет вводить пароль.

> **Примечание:** Подробнее про работе с разными ключевыми носителями: Рутокен, JaCarta, ESMART

Управление считывателями

Просмотр доступных (настроенных) считывателей:

```
$ cpconfig -hardware reader -view

Nick name: Aladdin R.D. JaCarta [SCR Interface] 00 00
Connect name:
Reader name:

Nick name: FLASH
Connect name:
Reader name:

Nick name: HDIMAGE
Connect name:
Reader name:
```

Либо:

```
$ csptest -enum -info -type PP_ENUMREADERS | iconv -f cp1251
CSP (Type:80) v4.0.9006 KC1 Release Ver:4.0.9708 OS:Linux CPU:AMD64 FastCode:READY:AVX.
CryptAcquireContext succeeded.HCRYPTPROV: 6679203
GetProvParam(...PP_ENUMREADERS...) until it returns false
  Len    Byte  NickName/Name
_____________________
 0x012a  0x72  ACS ACR38U-CCID 00 00
               All PC/SC readers
 0x012a  0x72  Aktiv Co. Rutoken S 00 00
               All PC/SC readers
 0x012a  0x58  FLASH
               FLASH
 0x012a  0x18  HDIMAGE
               Структура дискеты на жестком диске
Cycle exit when getting data. 4 items found. Level completed without problems.
Total: SYS: 0,000 sec USR: 0,170 sec UTC: 0,190 sec
[ErrorCode: 0x00000000]
```

Инициализация считывателя HDIMAGE, если его нет в списке доступных считывателей (под правами root):

```
# cpconfig -hardware reader -add HDIMAGE store
Adding new reader:
Nick name: HDIMAGE
Succeeded, code:0x0
```

Считыватель HDIMAGE размещается на `/var/opt/cprocsp/keys/<имя пользователя>/`.

Для работы со считывателем PC/SC требуется пакет cprocsp-rdr-pcsc. После подключения считывателя можно просмотреть список видимых считывателей (не зависимо от того, настроены ли они в КриптоПро как считыватели, зависит только от того, какие установлены драйверы для считывателей):

```
$ list_pcsc
Aladdin R.D. JaCarta [SCR Interface] 00 00
Aktiv Co. Rutoken S 00 00
```

Инициализация считывателя `Aktiv Co. Rutoken S 00 00` (требуется, если считыватель есть в списке видимых считывателей и отсутствует в списке настроенных), в параметре -add указывается имя, которое было получено при просмотре видимых считывателей, в параметре -name — удобное для обращения к считывателю имя, например, `Rutoken` (под правами root):

```
# cpconfig -hardware reader -add 'Aktiv Co. Rutoken S 00 00' -name 'Rutoken'
Adding new reader:
Nick name: Aktiv Co. Rutoken S 00 00
Name device: Rutoken
Succeeded, code:0x0
```

Современные аппаратные и программно-аппаратные хранилища ключей, такие как Рутокен ЭЦП или eSmart ГОСТ, поддерживаются через интерфейс PCSC. За реализацию этого интерфейса отвечает служба `pcscd`, которую необходимо запустить перед началом работы с соответствующими устройствами:

```
# systemctl start pcscd
```

Можно включить службу `pcscd` в автозапуск при загрузке системы:

```
# systemctl enable pcscd
```

Управление носителями

Просмотр доступных носителей:

```
$ cpconfig -hardware media -view | iconv -f cp1251
```

Управление ДСЧ

Просмотр списка настроенных ДСЧ:

```
$ cpconfig -hardware rndm -view

Nick name: CPSD
Connect name:
Rndm name:
Rndm level: 3

Nick name: BIO_GUI
Connect name:
Rndm name:
Rndm level: 4

Nick name: BIO_TUI
Connect name:
Rndm name:
Rndm level: 5
```

Настройка криптопровайдера

Просмотреть доступные типы криптопровайдеров можно командой `cpconfig -defprov -view_type`:

```
$ cpconfig -defprov -view_type
Provider type   Provider Type Name
_____________   _____________________________________
      75    GOST R 34.10-2001 Signature with Diffie-Hellman Key Exchange
      80    GOST R 34.10-2012 (256) Signature with Diffie-Hellman Key Exchange
      81    GOST R 34.10-2012 (512) Signature with Diffie-Hellman Key Exchange
      16    ECDSA Full and AES
      24    RSA Full and AES
```

Просмотр свойств криптопровайдера нужного типа:

```
$ cpconfig -defprov -view -provtype 80
Listing Available Providers:
Provider type   Provider Name
_____________   _____________________________________
       80   Crypto-Pro GOST R 34.10-2012 KC1 CSP
       80   Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider

Provider types and provider names have been listed.
```

Управление контейнерами

Создание контейнера

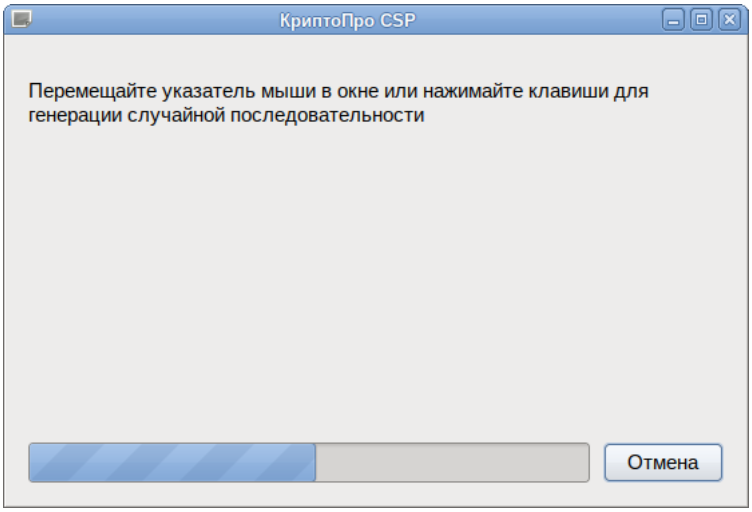
> **Примечание:** Для того, чтобы сертификат из контейнера можно было использовать через модуль pkcs11 (из пакета `lsb-cprocsp-pkcs11`) в браузере `firefox-gost`, необходимо создать его с -provtype 75 (поддержка ГОСТ-2001).

> **Внимание!** С 1 января 2019 г. по указанию ФСБ РФ и Минкомсвязи всем аккредитованным УЦ запрещен выпуск сертификатов ЭП по ГОСТ 2001. Ключи и запрос на сертификат необходимо формировать ГОСТ 2012.

Создадим контейнер с именем «*test*» в локальном считывателе *HDIMAGE*.

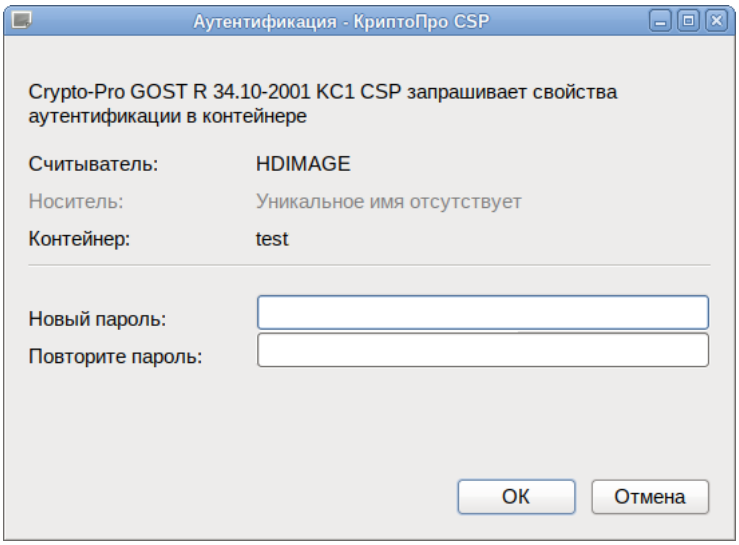
```
$ csptest -keyset -provtype 75 -newkeyset -cont '\\.\HDIMAGE\test'
```

При установленном пакете `cprocsp-rdr-gui-gtk` будет показано графическое окно, где будет предложено перемещать указатель мыши или нажимать клавиши:



Примечание: Если такой пакет не установлен, будет предложено ввести любые символы с клавиатуры.

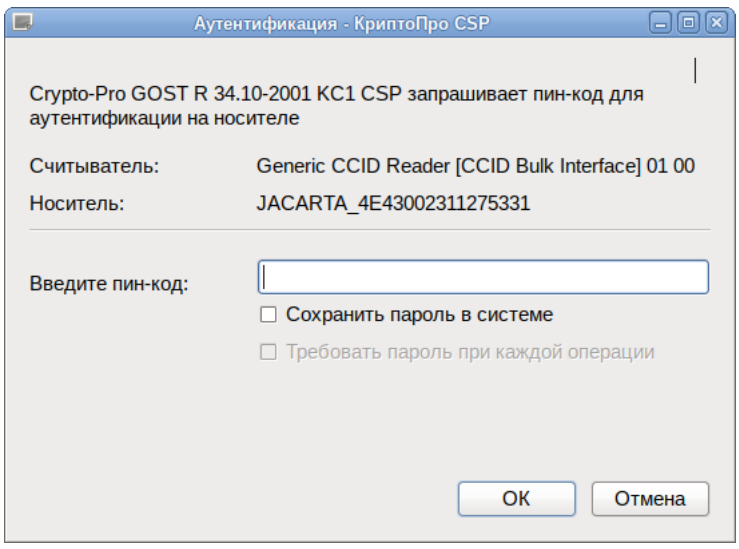
После этого будет предложено указать пароль на контейнер (можно указать пустой, тогда пароль запрашиваться не будет):



Внимание! При создании контейнера на токене:

```
$ csptest -keyset -provtype 75 -newkeyset -cont '\\.\Aladdin R.D. JaCarta [SCR Interface] 01 00\test'
```

Пароль не создается, а предъявляется (PIN-код пользователя):



После указания пароля снова будет предложено перемещать указатель мыши.

Вывод команды:

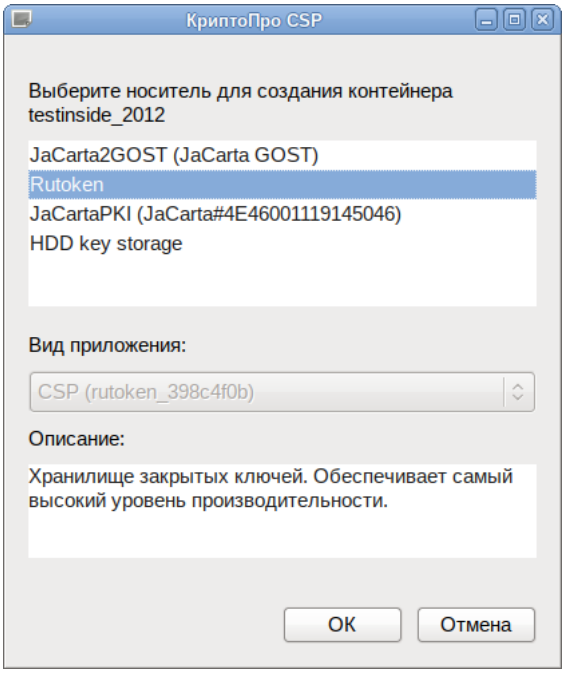
```
CSP (Type:75) v4.0.9006 KC1 Release Ver:4.0.9708 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 6679219
GetProvParam(PP_NAME): Crypto-Pro GOST R 34.10-2001 KC1 CSP
Container name: "test"
Signature key is not available.
Attempting to create a signature key...
a signature key created.
Exchange key is not available.
Attempting to create an exchange key...
an exchange key created.
Keys in container:
  signature key
  exchange key
Extensions:
  OID: 1.2.643.2.2.37.3.9

  OID: 1.2.643.2.2.37.3.10
Total: SYS: 0,030 sec USR: 0,160 sec UTC: 22,910 sec
[ErrorCode: 0x00000000]
```

Локальный контейнер создан.

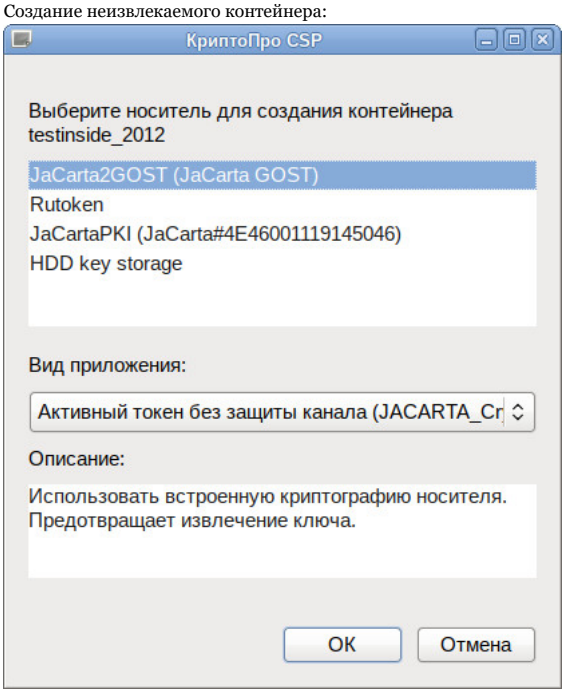
В КриптоПро 5 появилась возможность интерактивно выбирать носитель и тип создаваемого контейнера. Теперь можно создавать неизвлекаемые контейнеры.
Для этого необходимо выполнить команду, где `testinside_2012` — имя контейнера:

```
$ csptest -keyset -provtype 80 -newkeyset -cont testinside_2012
```

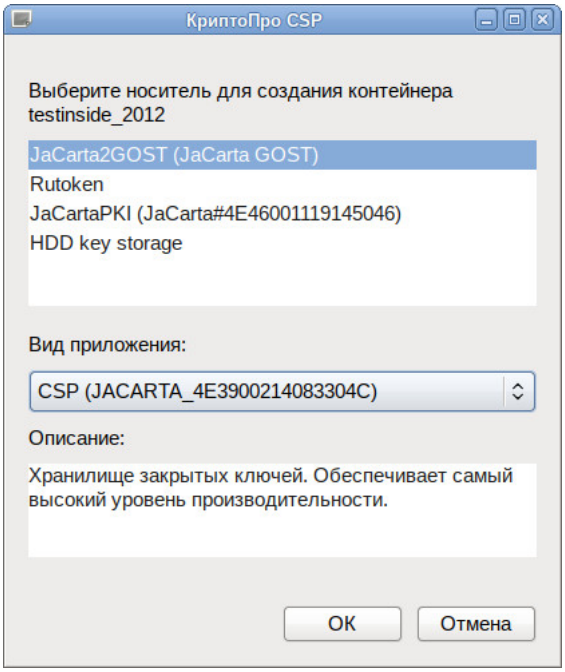
Откроется окно выбора носителя и способа создания контейнера. Для некоторых носителей нет возможности выбрать способ создания контейнера (Рутокен S, JaCarta PKI):



Для некоторых носителей можно выбрать способ создания контейнера (Рутокен ЭЦП, JaCarta-2 PKI/ГОСТ).
Создание неизвлекаемого контейнера:



Создание обычного контейнера:



Просмотр доступных контейнеров

> **Внимание!** При подключении токена в порт USB3, контейнеры видны не будут.

> **Примечание:** Вы можете загрузить все сертификаты с подключенных токенов командой:

```
csptestf -absorb -certs -autoprov
```

Проверить наличие контейнеров можно с помощью команды:

```
$ csptest -keyset -enum_cont -fqcn -verifyc | iconv -f cp1251
CSP (Type:80) v4.0.9006 KC1 Release Ver:4.0.9708 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 6679203
\\.\HDIMAGE\test
OK.
Total: SYS: 0,000 sec USR: 0,070 sec UTC: 0,130 sec
[ErrorCode: 0x00000000]
```

> **Внимание!** Имена контейнеров могут содержать названия в кодировке cp1251 (например, на токенах), что делает работу с ними по этим именам проблематичной. Можно показать список контейнеров с их уникальными именами командой:
>
> ```
> $ csptest -keyset -enum_cont -fqcn -verifyc -uniq
> CSP (Type:80) v4.0.9006 KC1 Release Ver:4.0.9708 OS:Linux CPU:AMD64 FastCode:READY:AVX.
> AcquireContext: OK. HCRYPTPROV: 6679203
> \\.\Aktiv Co. Rutoken S 00 00\card              |\\.\Aktiv Co. Rutoken S 00 00\SCARD\rutoken_2b8654f7\0A00\6AD1
> \\.\HDIMAGE\test                               |\\.\HDIMAGE\HDIMAGE\\test.000\2EF8
> OK.
> Total: SYS: 0,020 sec USR: 0,190 sec UTC: 1,510 sec
> [ErrorCode: 0x00000000]
> ```
>
> Уникальные имена указаны после символа «|».

Просмотр подробной информации о контейнере:

```
csptestf -keyset -container '\\.\HDIMAGE\test' -info
```

Удаление контейнера

Удалить контейнер можно с помощью команды:

```
$ csptest -keyset -deletekeyset -cont '\\.\HDIMAGE\test'
CSP (Type:80) v4.0.9006 KC1 Release Ver:4.0.9708 OS:Linux CPU:AMD64 FastCode:READY:AVX.
Container \\.\HDIMAGE\test deleted.
Total: SYS: 0,010 sec USR: 0,240 sec UTC: 0,260 sec
[ErrorCode: 0x00000000]
```

Управление сертификатами

cryptcp — приложение командной строки для создания запросов на сертификаты, шифрования и расшифрования файлов, создания и проверки электронной подписи файлов с использованием сертификатов открытых ключей, хэширования файлов. Результатом работы приложения в большинстве случаев является файл с CMS-сообщением (PKCS#7) в кодировке DER или BASE64.

Создание запроса на получение сертификата

Создание запроса на получение сертификата средствами КриптоПро:

```
cryptcp -creatrqst -dn "список имён полей" -cont 'путь к контейнеру' <название_файла>.csr
```

Для создания запроса на получение сертификата потребуется:

1. DN — данные, которые будут храниться в поле Subject сертификата (cn=Test User5,e=cas@altlinux.org).
2. Имя контейнера вместе со считывателем (например, в локальном хранилище hdimage: `\\.\HDIMAGE\test`).
3. Имя файла, в котором следует сохранить запрос (`test5.csr`).

> **Внимание!** Для использования проверки подлинности клиента в браузере потребуется также указать, что запрос создается по ГОСТ 2001 и добавляется тип применения подлинности клиента: `-provtype 75 -certusage "1.3.6.1.5.5.7.3.4,1.3.6.1.5.5.7.3.2"`.

С помощью опции -certusage можно указать OID назначение сертификата. Назначение сертификата представляется в сертификате объектным идентификатором, присвоенным этой политике, — OID. Если в сертификате указано несколько политик, то это означает, что сертификат соответствует всем этим политикам списка.

Таблица 2. Типы применения.

OID	Назначение
1.3.6.1.5.5.7.3.1	Аутентификация сервера
1.3.6.1.5.5.7.3.2	Аутентификация клиента
1.3.6.1.5.5.7.3.3	Подписывание кода
1.3.6.1.5.5.7.3.4	Защищенная электронная почта
1.3.6.1.5.5.7.3.8	Простановка штампов времени
1.3.6.1.4.1.311.10.5.1	Цифровые права
1.3.6.1.4.1.311.10.3.12	Подписывание документа

Таблица 3. Поле Subject сертификата

OID	Алиас	Назначение	Примечание
2.5.4.3	CN	Общее имя	Наименование ЮЛ (если ИНН начинается с "00") или ФИО владельца. Длина не более 64 символов
2.5.4.4	SN	Фамилия	
2.5.4.42	GN/G	Имя Отчество	Общая длина текста в полях SN и G должна быть не более 64 символов (с учетом одного пробела между текстом из Фамилии и текстом из Имени)
1.2.840.113549.1.9.1	emailAddress/E	Адрес электронной почты	ivanov@mail.mail
1.2.643.100.3	SNILS	СНИЛС	Должно быть записано 11 цифр (допускается 11 нулей для иностранных граждан).
1.2.643.3.131.1.1	INN	ИНН	12 цифр, для ЮЛ первые две цифры 00
2.5.4.6	C	Страна	Двухсимвольный код страны (RU)
2.5.4.8	S	Регион	Наименование субъекта РФ ЮЛ: по адресу местонахождения, ФЛ: по адресу регистрации (39 Калининградская обл.)
2.5.4.7	L	Населенный пункт	Наименование населенного пункта (Калининград)
2.5.4.9	street	Название улицы, номер дома	Пр-т Победы 14 кв.3
2.5.4.10	O	Организация	Полное или сокращенное наименование организации (только для ЮЛ)
2.5.4.11	OU	Подразделение	В случае выпуска СКПЭП на должностное лицо – соответствующее подразделение организации (только для ЮЛ)
2.5.4.12	T	Должность	В случае выпуска СКПЭП на должностное лицо – его должность (только для ЮЛ)
1.2.643.100.1	OGRN	ОГРН	ОГРН организации (только для ЮЛ)

Создать запрос на субъект "cn=Test User5,e=cas@altlinux.org", используя открытый ключ, сгенерированный в контейнере test текущего пользователя криптопровайдером «GOST R 34.10-2001» (тип — 75) и сохранить его в файл test5.req, назначение ключа — аутентификация и защита электронной почты:

```
$ cryptcp -creatrqst -dn "cn=Test User5,e=cas@altlinux.org" -provtype 75 -nokeygen -cont '\\.\HDIMAGE\test' -certusage "1.3.6.1.5.5.7.3.4,1.3.6.1.5.5.7.3.2" test5.req
CryptCP 4.0 (c) "КРИПТО-ПРО", 2002-2018.
Утилита командной строки для подписи и шифрования файлов.
Запрос успешно создан и сохранен в файле.
[ErrorCode: 0x00000000]
```

Созданный запрос будет сохранен в файле test5.req. Эти данные нужны для получения сертификата в удостоверяющем центре.

Создать запрос на физическое лицо, используя открытый ключ, сгенерированный в контейнере test_2012 (тип — 80) текущего пользователя криптопровайдером «Crypto-Pro GOST R 34.10-2012 KC1 CSP» (тип — 80) и сохранить его в файл test2012.req, назначение ключа — аутентификация и защита электронной почты:

```
$ cryptcp -creatrqst \
```

```
-dn "CN=Иванов Иван Иванович,SN=Иванов,G=Иван Иванович,E=ivanov@mail.mail,C=RU,L=Калининград,ST=39 Калининградская обл.,street=Пр-т Победы 14
кв.3,SNILS=102301111222,INN=11223344556" \
-provtype 80 -nokeygen  \
-cont '\\.\HDIMAGE\test_2012'  \
-certusage "1.3.6.1.5.5.7.3.4,1.3.6.1.5.5.7.3.2" test2012.req
```

Тот же запрос, используя OID:

```
$ cryptcp -creatrqst \
-dn "2.5.4.3=Иванов Иван Иванович,2.5.4.4=Иванов,2.5.4.42=Иван Иванович,1.2.840.113549.1.9.1=ivanov@mail.mail,2.5.4.6=RU,2.5.4.8=39 Калининградская
обл.,2.5.4.7=Калининград,2.5.4.9=Пр-т Победы 14 кв.3,1.2.643.3.131.1.1=102301111222,1.2.643.100.3=11223344556" \
-provtype 80 -nokeygen -cont '\\.\HDIMAGE\test_2012' \
-certusage "1.3.6.1.5.5.7.3.4,1.3.6.1.5.5.7.3.2" test2012.req
```

> **Примечание:** Подробную инструкцию (http://cryptopro.ru/sites/default/files/products/cryptcp/cryptcp_5.0.x.pdf) по работе с утилитой cryptcp можно скачать со страницы http://cryptopro.ru/products/other/cryptcp

Установка сертификата

Добавление сертификата, без привязки к ключам (только проверка ЭЦП):

```
$ certmgr -inst -file cert.cer
```

Ассоциировать сертификат с контейнером, сертификат попадет в пользовательское хранилище uMy:

```
$ certmgr -inst -file cert.cer -store uMy -cont '\\.\HDIMAGE\test'
```

Запись сертификата клиента в контейнер:

```
$ cryptcp -instcert -provtype 80 -cont '\\.\HDIMAGE\test' -ku -askpin cert.cer
```

Основные опции:

-provtype — указать тип криптопровайдера (по умолчанию 75);

-provname — указать имя криптопровайдера;

-cont — задать имя ключевого контейнера (по умолчанию выбор из списка);

-ku — использовать контейнер пользователя (CURRENT_USER);

-km — использовать контейнер компьютера (LOCAL_MACHINE);

-dm — установка в хранилище компьютера (LOCAL_MACHINE);

-du — установка в хранилище пользователя (CURRENT_USER);

-askpin — запросить пароль ключевого контейнера из с консоли;

<имя файла> — имя файла, содержащего сертификат.

Добавление сертификата УЦ из файла certne_ucw.cer в хранилище машины (для текущего пользователя):

```
$ certmgr -inst -file certne_ucw.cer -store uRoot
```

Добавление корневых сертификатов из файла cert.p7b (для текущего пользователя):

```
$ certmgr -inst -all -file cert.p7b -store uRoot
```

Необходимо последовательно добавить все сертификаты.

> **Примечание:** Корневые сертификаты для всех пользователей ставятся в хранилище машины — т.е. с параметром `-store mRoot`.
> Например: `# certmgr -inst -store mRoot -file /tmp/cert.cer`

Просмотр сертификатов

Для просмотра установленных сертификатов можно воспользоваться командой:

```
$ certmgr -list
Certmgr 1.1 (c) "Crypto-Pro",  2007-2018.
program for managing certificates, CRLs and stores

=============================================================================
1-------
Issuer              : E=support@cryptopro.ru, C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN=CRYPTO-PRO Test Center 2
Subject             : CN=Test User5, E=cas@altlinux.org
Serial              : 0x120012447FA7E652B76808CD7900000012447F
SHA1 Hash           : 0xcb8e7ca68bea0ffbbd84c326d565de68cd8a15f5
SubjKeyID           : 6f7507353601d6d943f1406aae60c21ab65190e0
Signature Algorithm : ГОСТ Р 34.11/34.10-2001
PublicKey Algorithm : ГОСТ Р 34.10-2001 (512 bits)
Not valid before    : 18/12/2018  13:41:38 UTC
Not valid after     : 18/03/2019  13:51:38 UTC
PrivateKey Link     : Yes
```

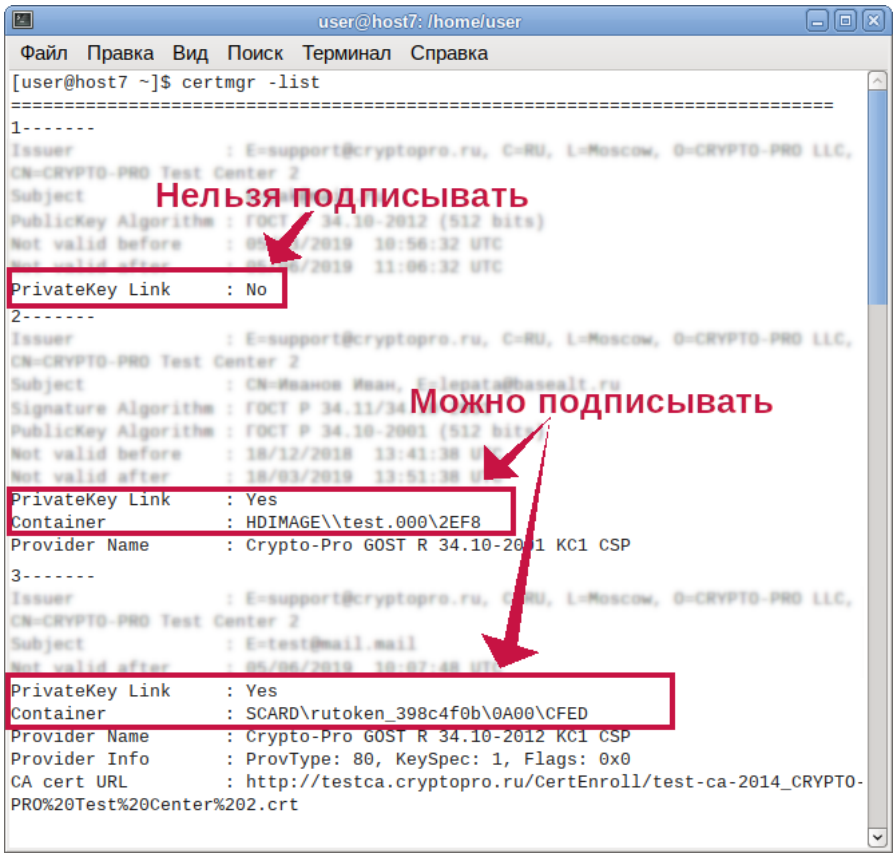
```
Container           : HDIMAGE\\test.000\2EF8
Provider Name       : Crypto-Pro GOST R 34.10-2001 KC1 CSP
Provider Info       : ProvType: 75, KeySpec: 1, Flags: 0x0
CA cert URL         : http://testca.cryptopro.ru/CertEnroll/test-ca-2014_CRYPTO-PRO%20Test%20Center%202.crt
OCSP URL            : http://testca.cryptopro.ru/ocsp/ocsp.srf
CDP                 : http://testca.cryptopro.ru/CertEnroll/CRYPTO-PRO%20Test%20Center%202.crl
Extended Key Usage  : 1.3.6.1.5.5.7.3.4
                      1.3.6.1.5.5.7.3.2
=====================================================================

[ErrorCode: 0x00000000]
```

Просмотр сертификатов в локальном хранилище uMy:

```
$ certmgr -list -store uMy
```

Примечание:

Если в списке сертификатов выводится **PrivateKey Link: Yes. Container: HDIMAGE\\test.000\2EF8**, то сертификат ассоциирован (связан) с приватным ключом, а если выводится **PrivateKey Link: No** — связи нет, и использовать такой контейнер для подписи не удастся:



Просмотр сертификатов в контейнере:

```
$ certmgr -list -container '\\.\Aktiv Rutoken ECP - CP 00 00\Rutoken'
```

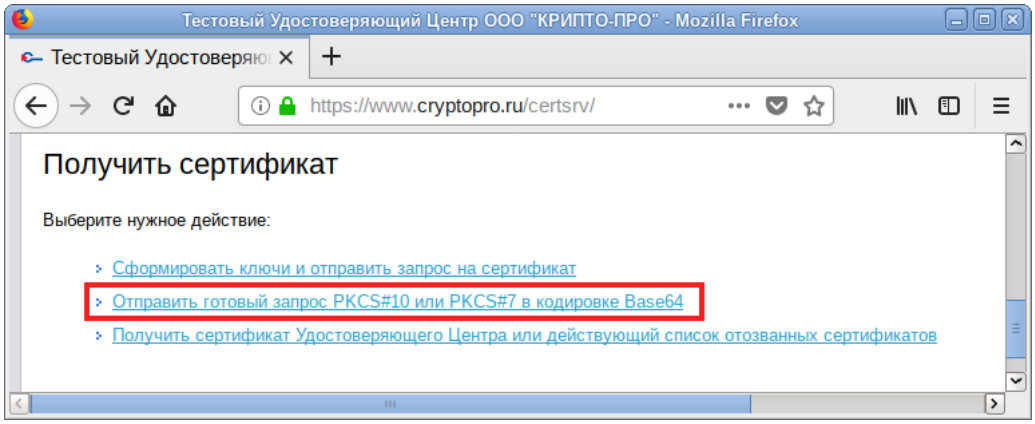
Просмотр корневых сертификатов:

```
$ certmgr -list -store uRoot
```

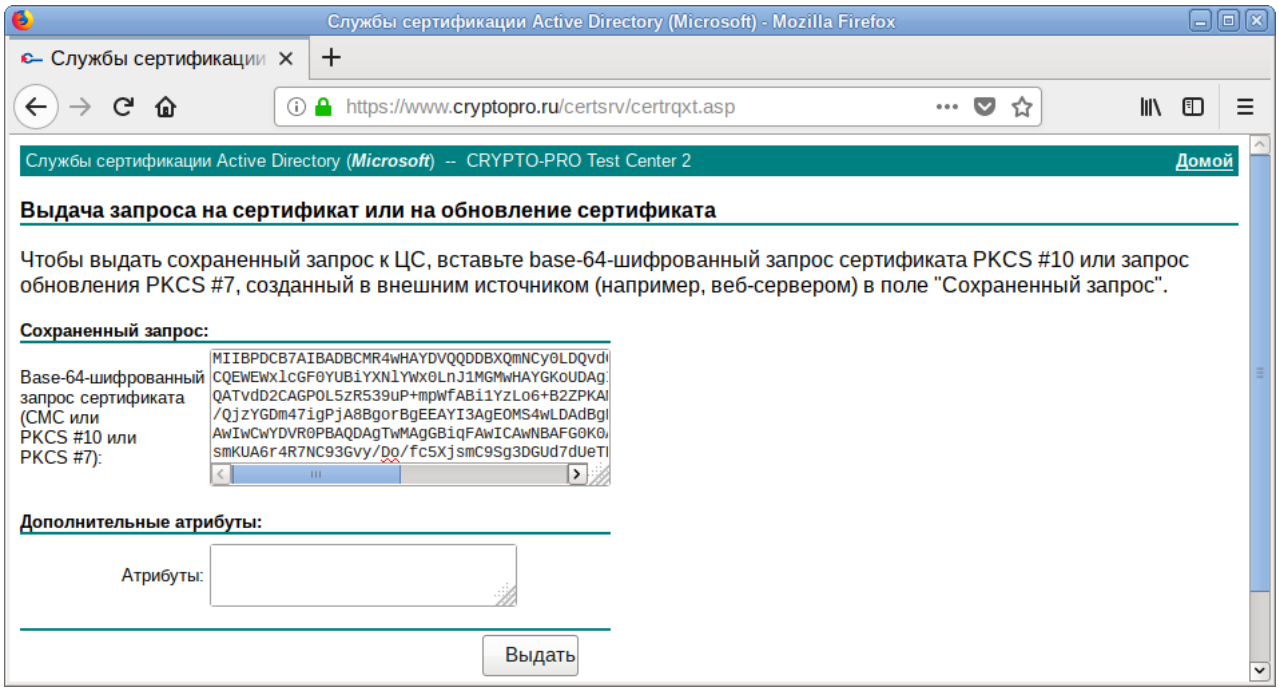
Получение сертификата в УЦ и его установка

Для получения сертификата в УЦ (на примере тестового удостоверяющего центра КриптоПро), необходимо выполнить следующие действия:

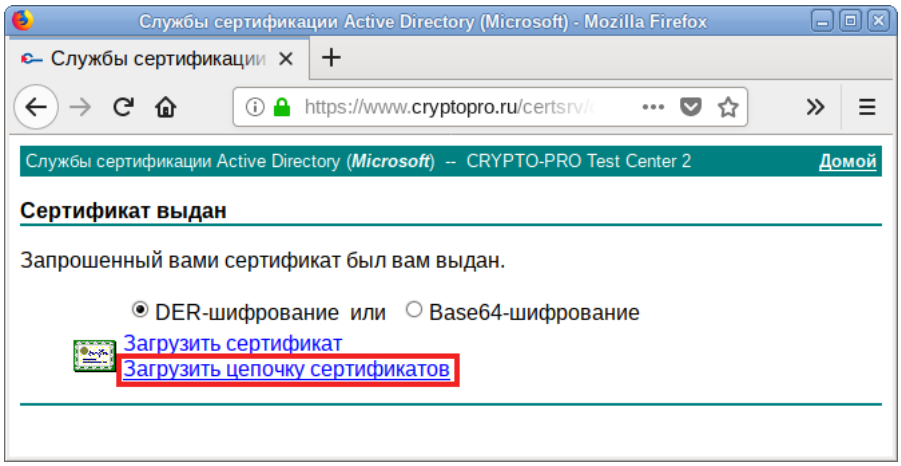
1. Откройте в браузере ссылку http://www.cryptopro.ru/certsrv (тестовый удостоверяющий центр КриптоПро).
2. Нажмите ссылку «Отправить готовый запрос PKCS#10 или PKCS#7 в кодировке Base64»:



3. Вставьте в поле «Base-64-шифрованный запрос сертификата» содержимое файла `test5.req` и нажмите кнопку «Выдать»:



4. Сохраните файл по ссылке «Загрузить цепочку сертификатов» (по умолчанию предлагается имя `certnew.p7b`):



Примечание:

Просмотреть содержимое файла `test5.req` можно, выполнив команду:

```
$ cat test5.req
MIIBMDCB4AIBADA2MRMwEQYDVQQDDApUZXN0IFVzZXI1MR8wHQYJKoZIhvcNAQkBFhBjYXNAYWx0
bGludXgub3JnMGMwHAYGKoUDAgITMBIGByqFAwICJAAGByqFAwICHgEDQwAEQDq5IAql+tHfVT7r
oz+P5dPgOUVXc7dg91nzGM7fkUBSKlapGO2A2xUDRUBHLtW/hBCiZsxdH3ydhzlZ6nhcbNKgPjA8
BgorBgEEAYI3AgEOMS4wLDAdBgNVHSUEFjAUBggrBgEFBQcDBAYIKwYBBQUHAwIwCwYDVR0PBAQD
AgTwMAgGBiqFAwICAwNBAFYnhGI6SsCwFRSl5p6EVnM7y6Hx9JGM6BFS4U3xTEGvzMK7yzk9j1kG
EKU7YZO5cFluPuDdi0WuYskhdz4SEg4=
```

Просмотреть полученный сертификат можно, выполнив команду:

```
$ certmgr -list -file certnew.p7b
```

```
Certmgr 1.1 (c) "CryptoPro",  2007-2018.
program for managing certificates, CRLs and stores

=============================================================================
1-------
Issuer              : E=support@cryptopro.ru, C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN=CRYPTO-PRO Test Center 2
Subject             : E=support@cryptopro.ru, C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN=CRYPTO-PRO Test Center 2
Serial              : 0x2B6E3351FD6EB2AD48200203CB5BA141
SHA1 Hash           : 0x046255290b0eb1cdd1797d9ab8c81f699e3687f3
SubjKeyID           : 15317cb08d1ade66d7159c4952971724b9017a83
Signature Algorithm : ГОСТ Р 34.11/34.10-2001
PublicKey Algorithm : ГОСТ Р 34.10-2001 (512 bits)
Not valid before    : 05/08/2014  13:44:24 UTC
Not valid after     : 05/08/2019  13:54:03 UTC
PrivateKey Link     : No
2-------
Issuer              : E=support@cryptopro.ru, C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN=CRYPTO-PRO Test Center 2
Subject             : CN=Test User5, E=cas@altlinux.org
Serial              : 0x120012447FA7E652B76808CD7900000012447F
SHA1 Hash           : 0xcb8e7ca68bea0ffbbd84c326d565de68cd8a15f5
SubjKeyID           : 6f7507353601d6d943f1406aae60c21ab65190e0
Signature Algorithm : ГОСТ Р 34.11/34.10-2001
PublicKey Algorithm : ГОСТ Р 34.10-2001 (512 bits)
Not valid before    : 18/12/2018  13:41:38 UTC
Not valid after     : 18/03/2019  13:51:38 UTC
PrivateKey Link     : No
CA cert URL         : http://testca.cryptopro.ru/CertEnroll/test-ca-2014_CRYPTO-PRO%20Test%20Center%202.crt
OCSP URL            : http://testca.cryptopro.ru/ocsp/ocsp.srf
CDP                 : http://testca.cryptopro.ru/CertEnroll/CRYPTO-PRO%20Test%20Center%202.crl
Extended Key Usage  : 1.3.6.1.5.5.7.3.4
                      1.3.6.1.5.5.7.3.2
=============================================================================

[ErrorCode: 0x00000000]
```

Цепочка сертификатов содержит два сертификата:

- Сертификат удостоверяющего центра.
- Сертификат клиента.

Для установки сертификата удостоверяющего центра:

- выполните команду:

```
$ certmgr -inst -file certnew.p7b -store uRoot
```

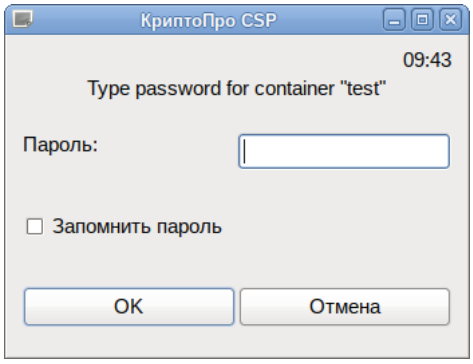
- в ответ на запрос команды нажмите 1.

Для записи сертификата клиента в контейнер:

- выполните команду:

```
$ certmgr -inst -file certnew.p7b -store uMy -cont '\\.\HDIMAGE\test'
```

- в ответ на запрос команды нажмите 2.
- введите пароль на контейнер \\.\HDIMAGE\test при запросе:



> **Примечание:**
>
> Корневые сертификаты для всех пользователей ставятся в хранилище машины — т.е. с параметром `-store mRoot`. Например: `# certmgr -inst -store mRoot -file /tmp/cert.cer`
>
> CRL ставятся точно также только с параметром -crl. CRL ставить не обязательно, но нужно убедиться что в `/etc/opt/cprocsp/config64.ini` в секции apppath указан правильный путь для libcurl.so. По умолчанию там путь до библиотеки от КриптоПро и если curl от КриптоПро не установлен — загрузка CRL работать не будет. Установка параметра на 64-битных системах:
>
> ```
> # cpconfig -ini \\config\\apppath -add string libcurl.so /opt/cprocsp/lib/amd64/libcpcurl.so
> ```

Проверка цепочки сертификатов

> **Внимание!** В кэше сертификатов для выпущенного сертификата должны присутствовать корневые сертификаты удостоверяющих центров. В противном случае он будет недоступен в плагине для браузера!

Таблица 4. Сертификаты популярных удостоверяющих центров.

Удостоверяющий Центр	Источник	Сертификаты
ПАК «Головной удостоверяющий центр»	https://e-trust.gosuslugi.ru/MainCA	https://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=8CAE88BBFD404A7A53630864F9033606E1DC45E2
ЗАО «Национальный удостоверяющий центр»	https://www.nucrf.ru/info/	https://www.nucrf.ru/download/nucrf.p7b
Удостоверяющий центр СКБ Контур	https://ca.kontur.ru/about/certificates (выбрать 2015 год)	http://cdp.skbkontur.ru/certificates/kontur-root-2015.crt

Для проверки можно скопировать персональный сертификат в файл:

```
cryptcp -copycert -dn "CN=Иванов Иван Иванович" -df  tt.cer
CryptCP 5.0 (c) "КРИПТО-ПРО", 2002-2018.
Утилита командной строки для подписи и шифрования файлов.

Будет использован следующий сертификат:
Субъект:11223344556, 102301111222, Пр-т Победы 14 кв.3, 39 Калининградская обл., Калининград, RU, ivanov@mail.mail, Иван Иванович, Иванов, Иванов Иван Иванович
Действителен с 21.02.2019 13:16:38 по 21.05.2019 13:26:38

Цепочки сертификатов проверены.
Копирование сертификатов завершено.
[ErrorCode: 0x00000000]
```

Из вывода следует, что все сертификаты есть в цепочке сертификатов.

Если же команда возвращает «Цепочка сертификатов не проверена для следующего сертификата:» или другую ошибку:

```
$ cryptcp -copycert -dn E=user@test.ru -df personal.cer

CryptCP 4.0 (c) "Crypto-Pro", 2002-2015.
Command prompt Utility for file signature and encryption.

The following certificate will be used:
RDN:******
Valid from 13.07.2016 12:03:00 to 13.07.2017 12:04:00

Certificate chain is not checked for this certificate:
RDN:******
Valid from 13.07.2016 12:03:00 to 13.07.2017 12:04:00

The certificate or certificate chain is based on an untrusted root.
Do you want to use this certificate ([Y]es, [N]o, [C]ancel)?
```

(нажмите C и Enter, чтобы выйти).

Можно запустить вышеуказанную команду с отладкой цепочки:

```
$ CP_PRINT_CHAIN_DETAIL=1 cryptcp -copycert -dn E=user@test.ru -df personal.cer
...
----------- Error chain -----------
Chain status:IS_UNTRUSTED_ROOT
Revocation reason:unspecified
1.
 Subject:'E=ca@skbkontur.ru, C=ru, L=:0B5@8=1C@3, O= ◆$ ◆!▒ ▒>=BC@◆, CN=uc skb kontur (root)'
 Issuer:'E=ca@skbkontur.ru, C=ru, L=:0B5@8=1C@3, O= ◆$ ◆!▒ ▒>=BC@◆, CN=uc skb kontur (root)'
 Cert status:IS_UNTRUSTED_ROOT
...
```

То есть нам надо установить сертификат УЦ с **CN=uc skb kontur (root)**:

```
$ certmgr -inst -store uRoot -file kontur-root-2015.crt
```

После этого:

```
$ cryptcp -copycert -dn E=user@test.ru -df personal.cer
CryptCP 4.0 (c) "Crypto-Pro", 2002-2015.
Command prompt Utility for file signature and encryption.

The following certificate will be used:
RDN:******
Valid from 13.07.2016 12:03:00 to 13.07.2017 12:04:00

Certificate chains are checked.
Certificate's been copied.
[ReturnCode: 0]
```

Всё в порядке и сертификат виден в плагине Cades.

Удаление сертификата

Удалить сертификат с "CN=Иванов Иван Иванович" из хранилища КриптоПро:

```
$ certmgr -delete -dn "CN=Иванов Иван Иванович"
```

Удалить сертификат с "CN=Иванов Иван Иванович" из контейнера:

```
$ certmgr -delete -dn "CN=Иванов Иван Иванович" -container '\\.\Aladdin R.D. JaCarta [SCR Interface] 01 00\test'
```

Удалить все сертификаты из хранилища КриптоПро:

```
$ certmgr -delete -all
$ certmgr -delete -store uRoot
```

Удалить все сертификаты установленные в хранилище машины:

```
# certmgr -delete -store mRoot
```

Экспорт контейнера и сертификата на другую машину

Если при создании контейнера он был помечен как экспортируемый (ключ -exportable), то его можно экспортировать на USB-диск:

```
$ csptest -keycopy -contsrc '\\.\HDIMAGE\test_export' -contdest '\\.\FLASH\test_new'
CryptAcquireContext succeeded.HCRYPTPROV: 36965843
CryptAcquireContext succeeded.HCRYPTPROV: 37297363
Total: SYS: 0,100 sec USR: 0,200 sec UTC: 13,420 sec
[ErrorCode: 0x00000000]
```

При этом потребуется ввести пароль от контейнера '\\.\HDIMAGE\test_export' и задать пароль на новый контейнер '\\.\FLASH\test_new'.

> **Примечание:**
> Будьте внимательны при операциях импорта/экспорта контейнера с использованием токена:
>
> ```
> $ csptest -keycopy -contsrc '\\.\HDIMAGE\test_export' -contdest '\\.\Aladdin R.D. JaCarta [SCR Interface] (000000000000) 00 00\test_export'
> ```
>
> необходимо будет предъявлять pin токена.

Просмотр списка контейнеров:

```
$ csptest -keyset -enum_cont -fqcn -verifyc | iconv -f cp1251
CSP (Type:80) v5.0.10001 KC1 Release Ver:5.0.11319 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 41622371
\\.\FLASH\test_new
\\.\HDIMAGE\test_export
\\.\HDIMAGE\test
OK.
Total: SYS: 0,030 sec USR: 0,060 sec UTC: 0,160 sec
[ErrorCode: 0x00000000]
```

Экспортировать сертификат из локального хранилища в файл:

```
$ certmgr -export -dn 'CN=Ли Александр Сергеевич' -dest test.cer
```

Скопировать сертификат на USB-диск:

```
$ cp test.cer /run/media/user/NAMEUSB/
```

Экспорт контейнера с USB-диска на жесткий диск:

```
$ csptest -keycopy -contsrc '\\.\FLASH\test_new' -contdest '\\.\HDIMAGE\test_export'
CryptAcquireContext succeeded.HCRYPTPROV: 35778003
CryptAcquireContext succeeded.HCRYPTPROV: 36125907
Total: SYS: 0,050 sec USR: 0,240 sec UTC: 19,390 sec
[ErrorCode: 0x00000000]
```

> **Примечание:** Экспорт сертификата на жесткий диск необходимо выполнять под пользователем, который будет использовать данный контейнер для подписи.

Ассоциировать сертификат с контейнером, сертификат попадет в пользовательское хранилище My:

```
$ certmgr -inst -file /run/media/user/NAMEUSB/test.cer -cont '\\.\HDIMAGE\test_export'
```

Экспорт сертификатов на другую машину

Закрытые ключи к сертификатам находятся в `/var/opt/cprocsp/keys`.

Для экспорта сертификатов необходимо:

1. Перенести ключи из `/var/opt/cprocsp/keys` на нужную машину в тот же каталог.
2. Экспортировать сертификаты (их, количество можно определить, выполнив: certmgr -list, в примере сертификатов 3):

   ```
   $ for i in `seq 1 3`; do echo $i | certmgr -export -dest $i.cer; done
   ```

3. Перенести файлы сертификатов (1.cer, 2.cer, 3.cer) на нужную машину.
4. На машине, куда переносятся сертификаты, просмотреть какие контейнеры есть (должны появится контейнеры с первой машины):

   ```
   $ csptest -keyset -enum_cont -verifycontext -fqcn
   ```

5. Связать сертификат и закрытый ключ:

   ```
   $ certmgr -inst -file 1.cer -cont '\\.\HDIMAGE\container.name'
   ```

   Если закрытый ключ и сертификат не подходят друг к другу, будет выведена ошибка:

```
Cannot install certificate
Public keys in certificate and container are not identical
```

6. Если закрытого ключа нет, то просто поставить сертификат:

```
$ certmgr -inst -file 1.cer
```

Импорт персонального сертификата

Вы можете импортировать собственный сертификат в локальный считыватель **HDIMAGE**.

Если у вас нет сертификата, самое время его создать:

- Создание через cert-sh-functions (требует установки пакета `cert-sh-functions`)
- Создание сертификатов PKCS12 (достаточно только пакета `openssl`)

Допустим, мы пошли по первому пути и создали сертификат web-server (**делать это строго под правами root**):

```
# . cert-sh-functions
# ssl_generate 'web-server'
```

Сертификат по умолчанию будет лежать в `/var/lib/ssl/certs/web-server.cert`, а ключ — в `/var/lib/ssl/private/web-server.key`

Для импорта потребуется файл сертификата и закрытый ключ в контейнере PKCS#12 (http://ru.wikipedia.org/wiki/PKCS12).

Создадим для нашего ключа и сертификата необходимый контейнер:

```
openssl pkcs12 -export -in /var/lib/ssl/certs/web-server.cert -inkey /var/lib/ssl/private/web-server.pem -out web-server.p12
```

> **Примечание:** При создании контейнера будет дважды запрошен пароль для экспорта. По соображениям безопасности вводимые символы не показываются. После ввода каждого пароля нажимайте Enter.

Проверка созданного контейнера (при запросе введите пароль, введённый в предыдущей команде):

```
# openssl pkcs12 -in web-server.p12 -nodes | grep BEGIN
Enter Import Password:
MAC verified OK
-----BEGIN CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
```

И сертификат и ключ попали в контейнер.

После генерации сертификата проверим наличие считывателя:

```
# cpconfig -hardware reader -view | grep ^Nick
Nick name: FLASH
Nick name: HDIMAGE
```

Для импорта сертификата в КриптоПро используйте программу `certmgr`. В нашем случае:

```
$ certmgr -inst -file web-server.p12 -cont HDIMAGE
```

Если Вам необходимо импортировать сертификат с токена:

```
certmgr -inst -cont '\\.\Aktiv Co. Rutoken S 00 00\le-fb25d25d-23e9-4723-ae4c-fe0c95f2fcc1'
```

Если контейнер защищен паролем используйте ключ -pin <пароль>

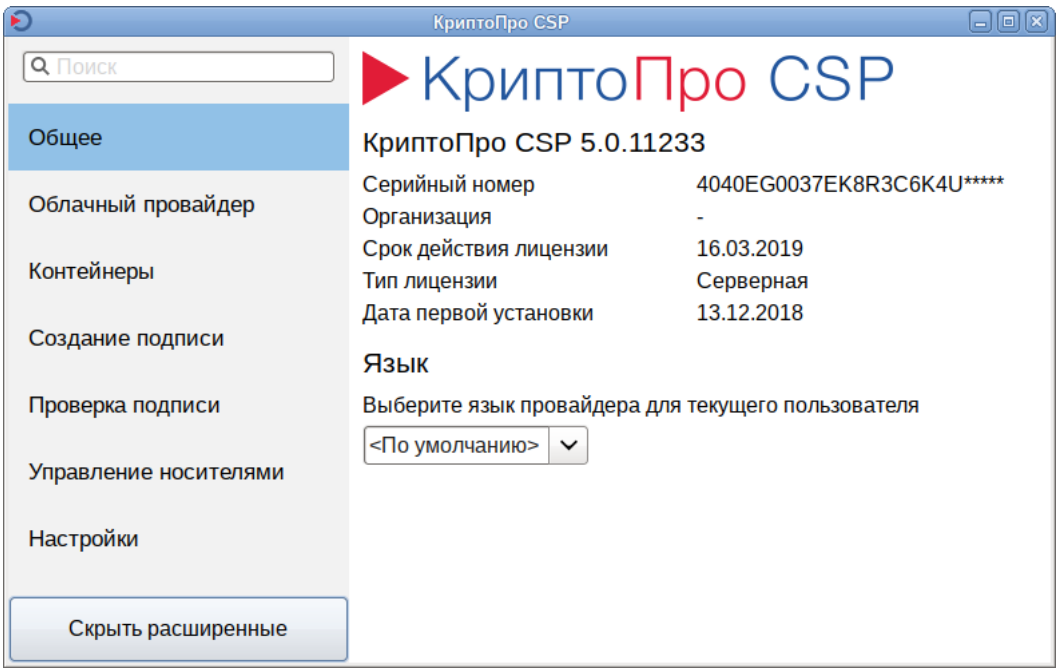
Использование cptools

В версии КриптоПРО 5 появилась графическая утилита для работы с сертификатами — cptools.
Для использования cptools необходимо установить пакет `cprocsp-cptools-gtk` из скаченного архива:

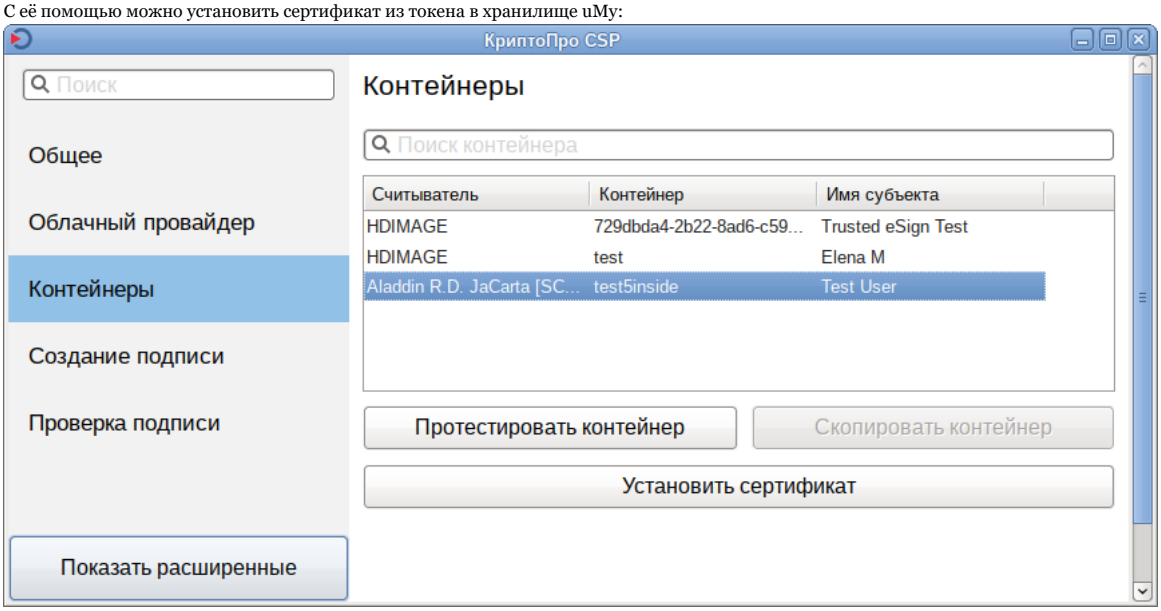
```
# apt-get install cprocsp-cptools-gtk*
```

После этого её можно запустить из консоли:

```
$ cptools
```



С её помощью можно установить сертификат из токена в хранилище uMy:



Работа с сертификатами в token-manager

token-manager предоставляет графический интерфейс управления ключевыми носителями и сертификатами. С помощью этой программы можно:

- просматривать подключенные ключевые носители (токены);
- изменять PIN-код ключевого носителя;
- устанавливать, просматривать и удалять сертификаты;
- просматривать и устанавливать лицензию КриптоПро.

Установка и запуск

Установка пакета `token-manager`:

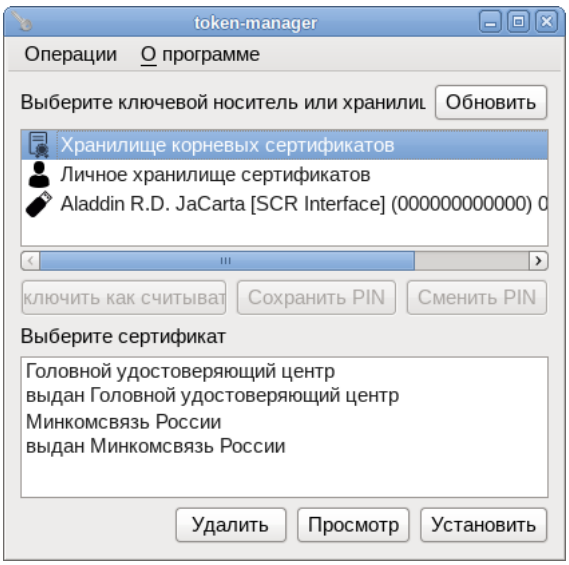
```
# apt-get install token-manager
```

Запустить token-manager можно:

- из командной строки:

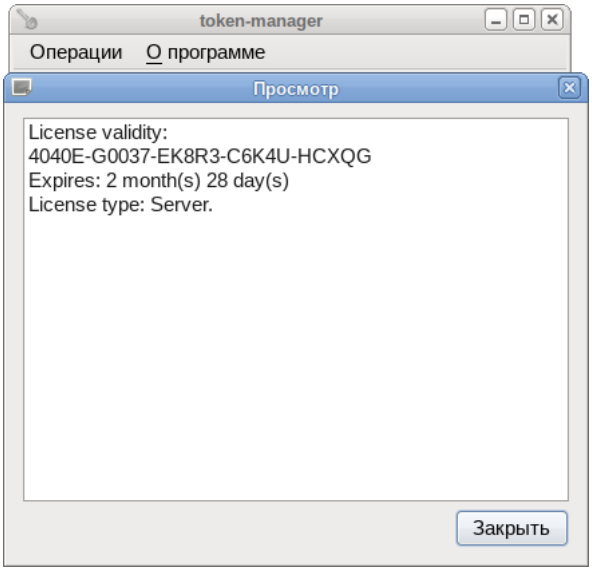
```
$ python /usr/bin/token-manager.py
```

- в рабочей среде Mate: Меню Система ▷ Администрирование ▷ Ключевые носители и сертификаты;
- в рабочей среде KDE5: Меню запуска приложений ▷ Настройки ▷ Ключевые носители и сертификаты.

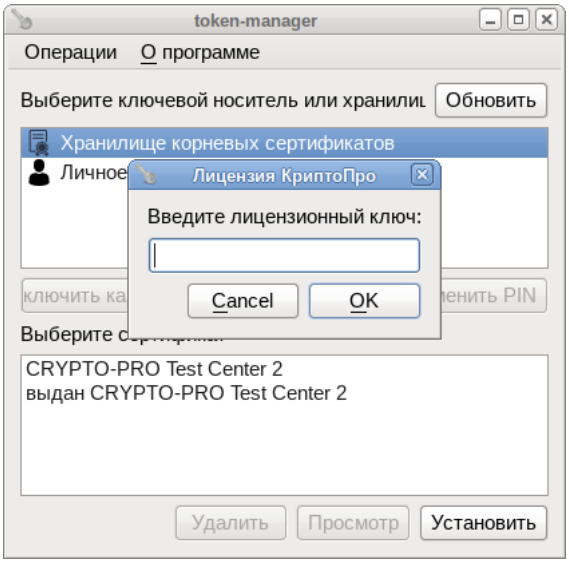


Проверка лицензии

Проверить срок истечения лицензии КриптоПРО можно выбрав в меню token-manager пункт Операции ▷ Просмотр лицензии КриптоПро CSP:

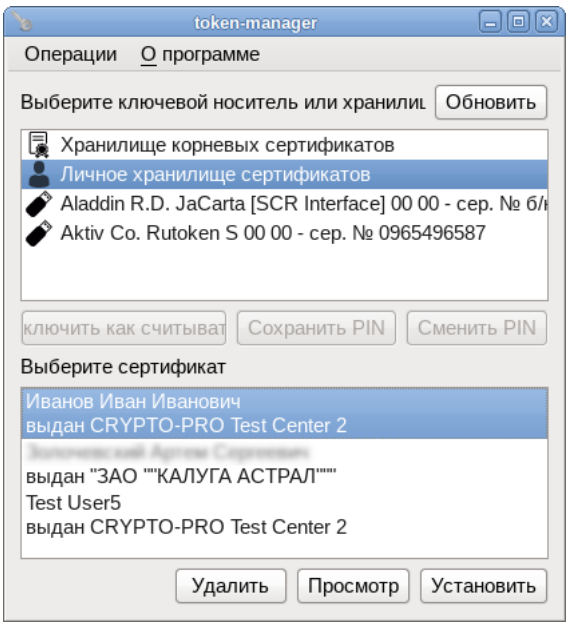


Для установки другой лицензии КриптоПРО выберите в меню token-manager пункт Операции ▷ Ввод лицензии КриптоПро CSP:

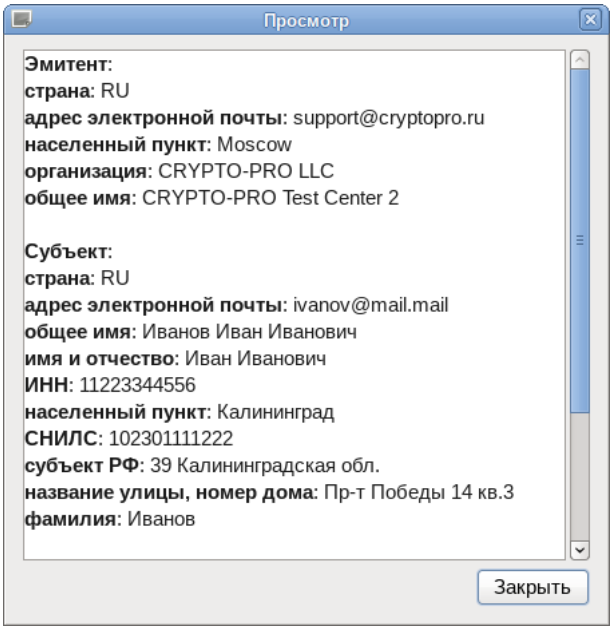


Просмотр сертификатов

Просмотреть список сертификатов в хранилище или на ключевом носителе, можно выбрав соответствующий носитель:



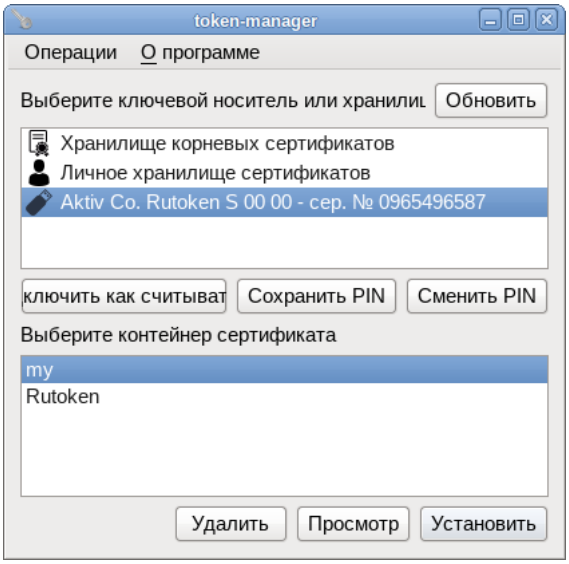
Для просмотра сертификата, необходимо выбрать сертификат и нажать кнопку «Просмотр»:



Для просмотра корневых сертификатов, необходимо выбрать в меню token-manager пункт Операции ▷ Просмотр корневых сертификатов.

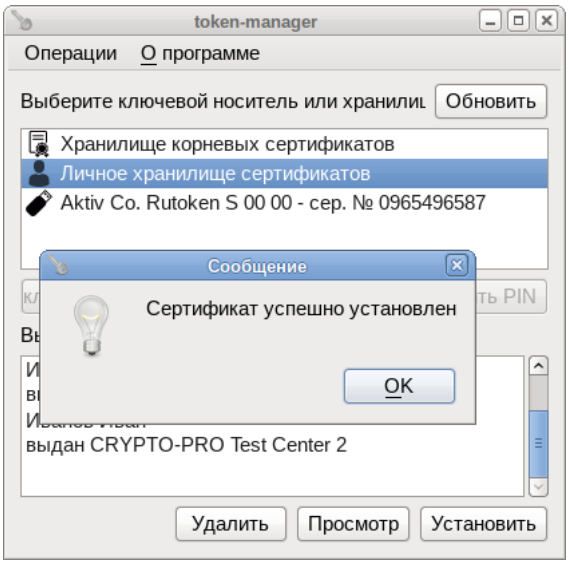
Установка сертификата

Чтобы установить сертификат с токена в локальное хранилище, необходимо выбрать контейнер на токене и нажать кнопку «Установить»:



Сертификат будет установлен в локальное хранилище сертификатов и будет связан с закрытым ключом на токене.

Чтобы установить сертификат в локальное хранилище из файла, необходимо выбрать «Личное хранилище сертификатов», нажать кнопку «Установить», выбрать файл сертификата и нажать кнопку «Открыть». Появится сообщение об успешном импорте сертификата:



Сертификат будет установлен в локальное хранилище сертификатов, но не будет связан ни с каким закрытым ключом. Этот сертификат можно использовать для проверки подписи.

Электронная подпись

Существуют два вида электронной подписи:

- прикреплённая (attached) — в результирующий файл упакованы данные исходного файла и подпись;
- откреплённая (detached) — подписываемый документ остается неизменным, подпись же сохраняется в отдельном файле. Для проверки отсоединенной подписи нужны оба файла, файл подписи и файл исходного документа.

Создание и проверка подписи в командной строке

Создание подписи

Для создания электронной подписи файла необходимо указать сертификат и имя подписываемого файла.

Для создания прикрепленной (attached) электронной подписи выполните команду:

> **Примечание:** Проще всего для указания сертификата использовать адрес e-mail.

```
$ cryptcp -sign -dn E=user@test.ru -der zayavlenie.pdf
CryptCP 4.0 (c) "КРИПТО-ПРО", 2002-2018.
Утилита командной строки для подписи и шифрования файлов.

Будет использован следующий сертификат:
Субъект:user@test.ru, Иванов Иван
Действителен с 18.12.2018 13:41:38 по 18.03.2019 13:51:38

Цепочки сертификатов проверены.
Папка './':
zayavlenie.pdf... Подпись данных...

Подписанное сообщение успешно создано.
[ErrorCode: 0x00000000]
```

где

- **-dn E=user@test.ru** — сертификат по e-mail;
- **-der** — использовать формат DER для файла подписи (по умолчанию используется формат Base64);
- **zayavlenie.pdf** — имя подписываемого файла.

На выходе появится файл `zayavlenie.pdf.sig`, содержащий как сам подписываемый файл, так и электронную подпись.

Для создания откреплённой (detached) подписи необходимо заменить ключ *-sign* на *-signf*:

```
$ cryptcp -signf -dn E=user@test.ru -der zayavlenie.pdf
```

Тогда рядом с оригинальным файлом будет лежать файл подписи — `zayavlenie.pdf.sgn`.

Проверка подписи

Для проверки прикреплённой подписи выполните команду:

```
$ cryptcp -verify zayavlenie.pdf.sig
CryptCP 4.0 (c) "КРИПТО-ПРО", 2002-2018.
Утилита командной строки для подписи и шифрования файлов.

Будет использован следующий сертификат:
Субъект:user@test.ru, Иванов Иван
```

```
Действителен с 18.12.2018 13:41:38 по 18.03.2019 13:51:38

Цепочки сертификатов проверены.
Папка './':
zayavlenie.pdf.sig... Проверка подписи...
Автор подписи: user@test.ru, Иванов Иван
 Подпись проверена.
[ErrorCode: 0x00000000]
```

Показано, кто подписывал и что подпись проверена.

Для проверки откреплённой подписи выполните команду:

```
$ cryptcp -vsignf zayavlenie.pdf
CryptCP 4.0 (c) "КРИПТО-ПРО", 2002-2018.
Утилита командной строки для подписи и шифрования файлов.

Будет использован следующий сертификат:
Субъект:user@test.ru, Иванов Иван
Действителен с 18.12.2018 13:41:38 по 18.03.2019 13:51:38

Цепочки сертификатов проверены.
Папка './':
234.pdf... Проверка подписи...

Автор подписи: user@test.ru, Иванов Иван
 Подпись проверена.
[ErrorCode: 0x00000000]
```

Также для проверки электронной подписи можно воспользоваться сервисом на сайте Госуслуг — https://www.gosuslugi.ru/pgu/eds.

Извлечение подписанного файла

Для извлечения файла с данными из файла электронной подписи необходимо указать имя файла, в который будут извлечены данные, в конце команды проверки подписи:

```
$ cryptcp -verify zayavlenie.pdf.sig zayavlenie.pdf
```

Создание и проверка ЭЦП в gost-crypto-gui

gost-crypto-gui — средство для создания электронной подписи и шифрования файлов.

Установить пакет `gost-crypto-gui` из репозитория можно, выполнив команду:

```
# apt-get install gost-crypto-gui
```

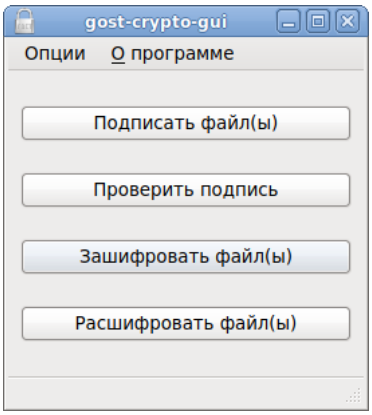
Запустить программу можно:

- из командной строки:

  ```
  $ python /usr/bin/gost-crypto-gui.py
  ```

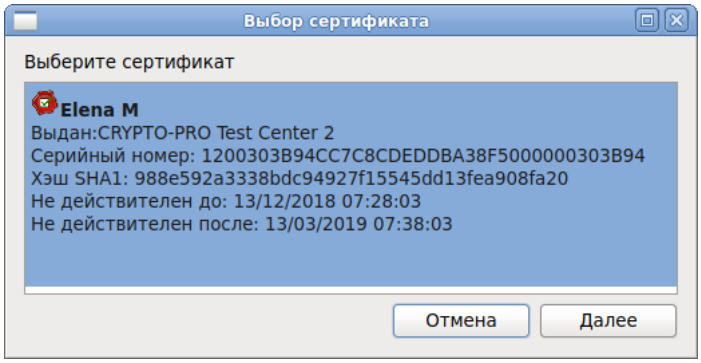
- в рабочей среде Mate: Меню Система ▷ Администрирование ▷ Подпись и шифрование файлов;
- в рабочей среде KDE: Меню запуска приложений ▷ Настройки ▷ Подпись и шифрование файлов.

С её помощью можно подписывать и проверять подписи файлов:



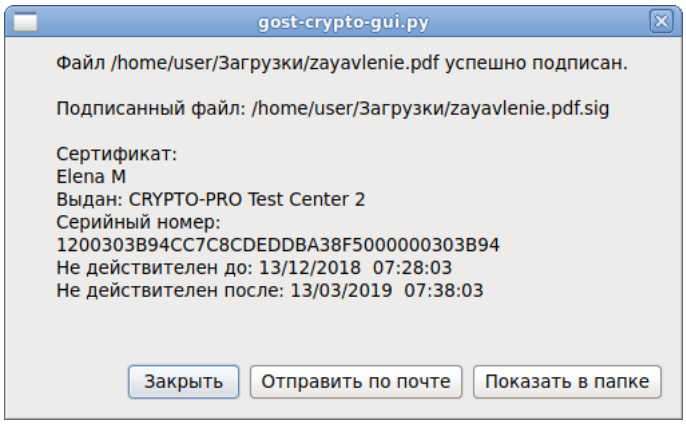
Для создания электронной подписи файла необходимо:

1. Нажать кнопку «Подписать файл(ы)».
2. Выбрать файл, который необходимо подписать.
3. Выбрать сертификат и нажать кнопку «Далее»:

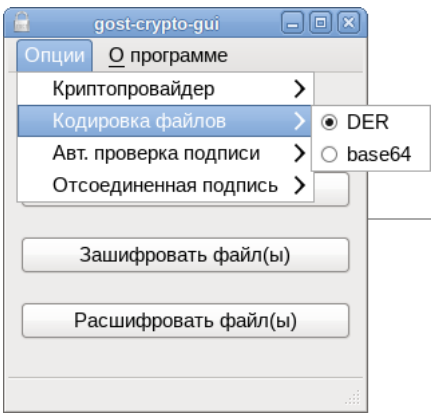


4. Ввести пароль на контейнер (если он был установлен):

5. Появится сообщение о подписанном файле:

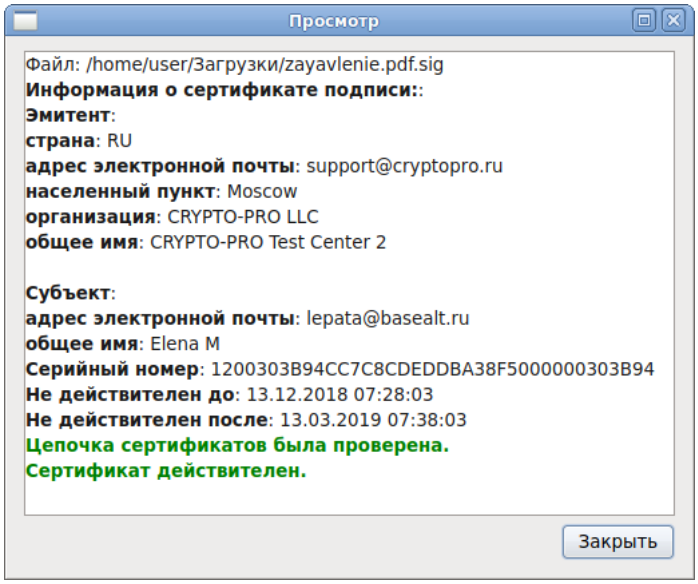


Опции ЭП настраиваются в меню «Опции» (параметр «Отсоединенная подпись» не работает???):



Для проверки электронной подписи следует:

1. Нажать кнопку «Проверить подпись».
2. Выбрать подписанный файл.
3. Появится информация о сертификате подписи:



Создание и проверка ЭЦП с использованием cptools

> **Примечание:** cptools доступна версии КриптоПро 5.

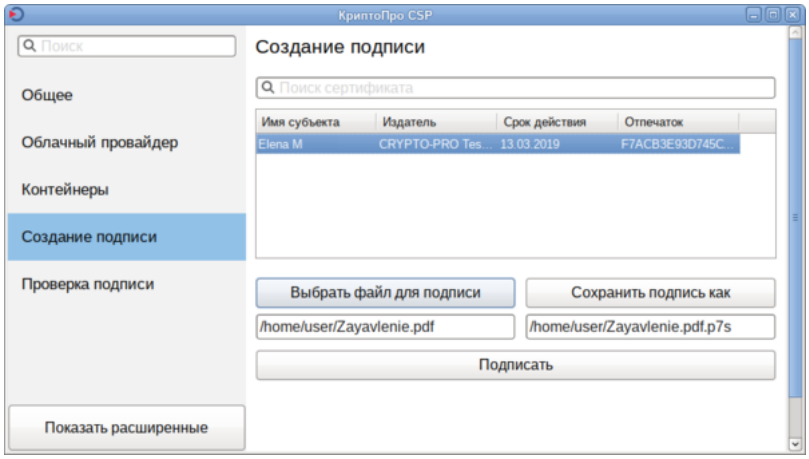
Запустить программу можно из консоли (должен быть установлен `cprocsp-cptools-gtk` из скаченного архива КриптоПро):

```
$ cptools
```

С помощью cptools можно подписывать и проверять подписи файлов.

Для создания электронной подписи файла необходимо:

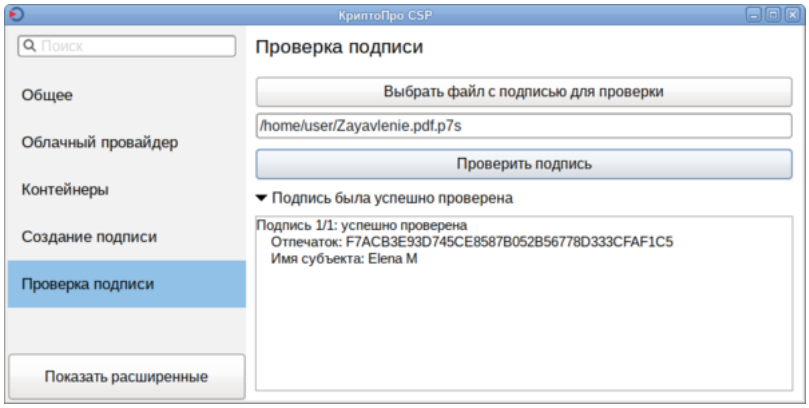
1. В левом меню выбрать пункт «Создание подписи».
2. Выбрать файл, который необходимо подписать, нажав кнопку «Выбрать файл для подписи» (или ввести адрес файла в текстовое поле под кнопкой «Выбрать файл для подписи»).
3. Изменить имя файла подписи, если оно вас не устраивает:



4. Нажать кнопку «Подписать».
5. Ввести пароль на контейнер (если он был установлен).
6. Появится сообщение о подписанном файле: «Создание подписи завершилось успехом».

Для проверки электронной подписи следует:

1. В левом меню выбрать пункт «Проверка подписи».
2. Выбрать файл с подписью, нажав кнопку «Выбрать файл с подписью для проверки» (или ввести адрес файла в текстовое поле под этой кнопкой).
3. Нажать кнопку «Проверить подпись».
4. Появится информация о результате проверки:



Web

Информацию о создании и проверки ЭЦП на веб-сайтах с помощью плагина КриптоПро можно найти в руководстве разработчика КриптоПро ЭЦП Browser plug-in:

- КриптоПро ЭЦП. Руководство разработчика (http://cpdn.cryptopro.ru/default.asp?url=content/cades/indexpage.html)

КриптоПро ЭЦП Browser plug-in

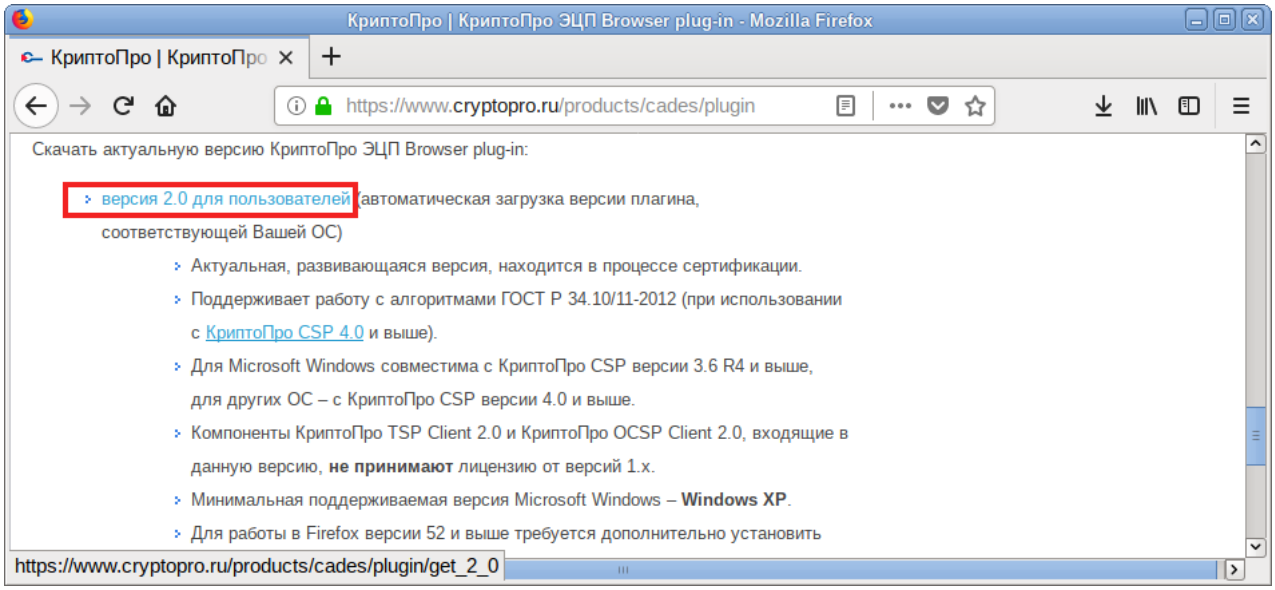
> **Внимание!** Последняя доступная версия плагина КриптоПро ЭЦП Browser plug-in 2.0 требует КриптоПро 4.0. С более ранними версиями КриптоПро плагин не работает и конфликтует.

КриптоПро ЭЦП Browser plug-in предназначен для создания и проверки электронной подписи (ЭП) на веб-страницах с использованием СКЗИ «КриптоПро CSP».

Плагин проверки ЭЦП для браузера требует установленного КриптоПро CSP, пакета `cprocsp-rdr-gui-gtk` из его комплекта и расширения для браузера CryptoPro Extension for CAdES Browser Plug-in (для работы в Firefox версии 52 и выше).

Для установки плагина:

1. Скачайте архив по ссылке http://www.cryptopro.ru/products/cades/plugin/get_2_0 (будет скачан архив под архитектуру браузера) или на странице https://www.cryptopro.ru/products/cades/plugin/ нажмите ссылку «версия 2.0 для пользователей»:



2. Распакуйте архив:

```
$ tar -xf cades_linux_amd64.tar.gz
```

3. Установите пакеты (под правами root, из папки с установочными файлами):

```
# apt-get install cprocsp-pki-*-{cades,plugin}.rpm
```

4. Разместите ссылки (под правами root):

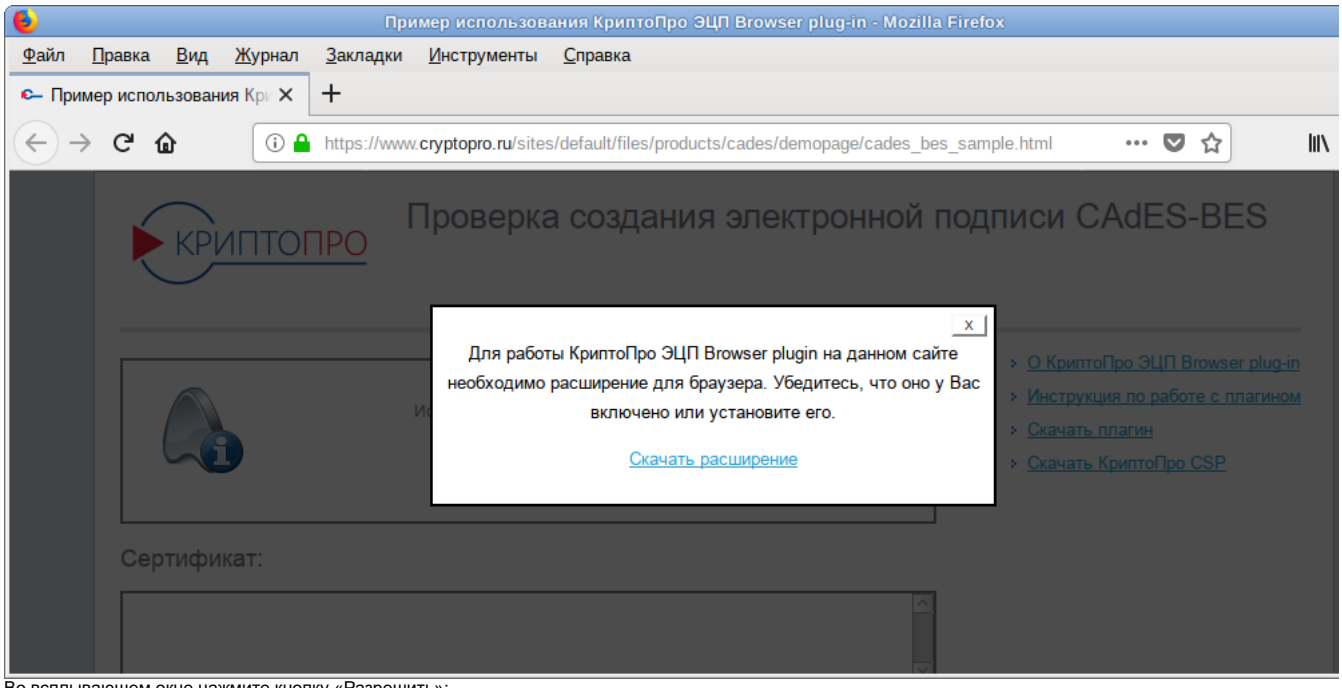
   Для Chromium:

```
# ln -s /usr/share/chromium-browser/extensions /usr/lib64/chromium/extensions
```

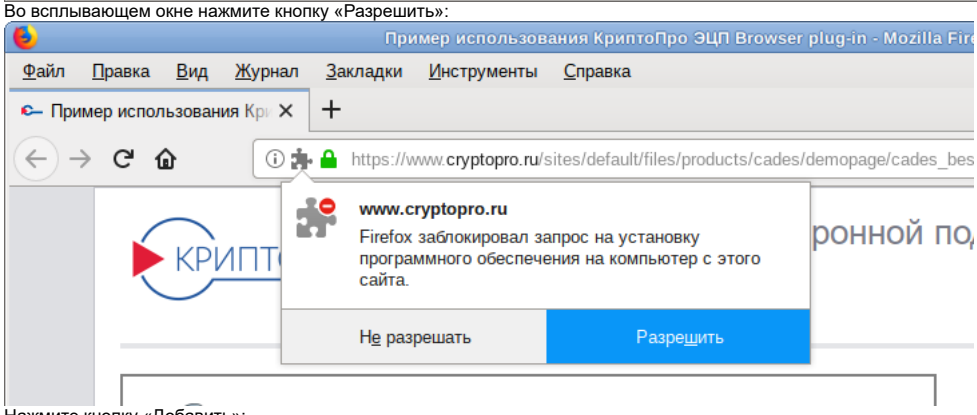
   Для Firefox (64-битная версия):

```
# cp /opt/cprocsp/lib/amd64/libnpcades.so.2.0.0 /usr/lib64/browser-plugins/libnpcades.so
```

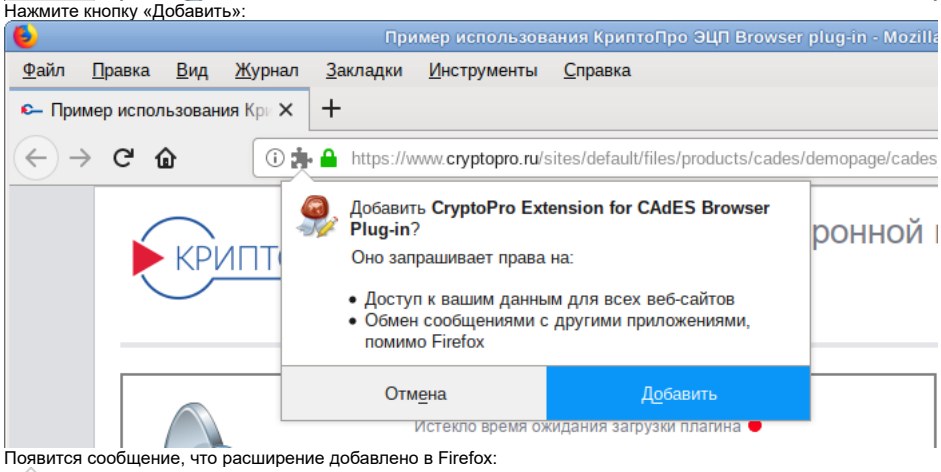
5. Для работы в Firefox версии 52 и выше установите расширение для браузера Инструкция на сайте производителя (https://www.cryptopro.ru/products/cades/plugin). Для установки расширения в Mozilla Firefox скачайте его по ссылке https://www.cryptopro.ru/sites/default/files/products/cades/extensions/firefox_cryptopro_extension_latest.xpi или нажмите на ссылку «Скачать расширение для браузера» на странице https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html



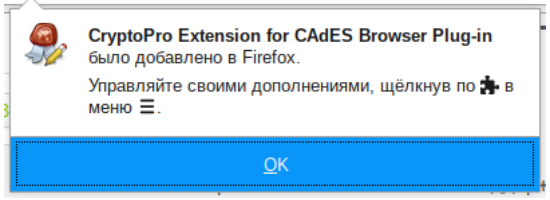
Во всплывающем окне нажмите кнопку «Разрешить»:



Нажмите кнопку «Добавить»:

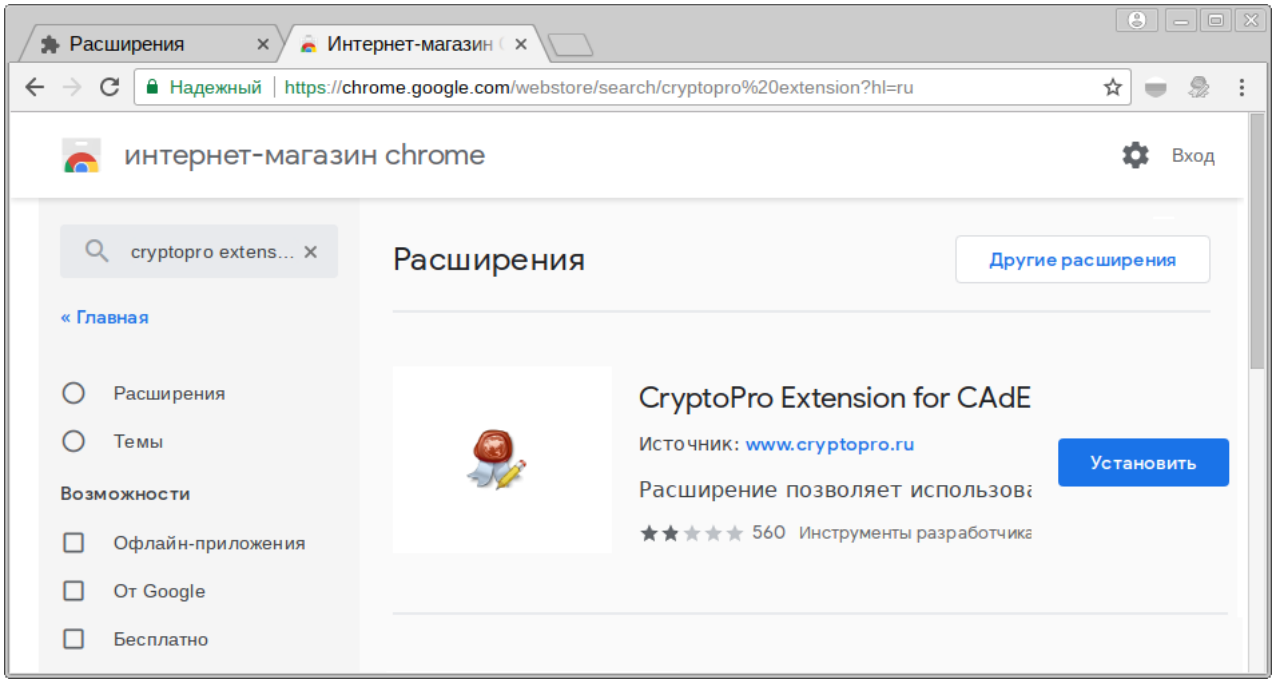


Появится сообщение, что расширение добавлено в Firefox:

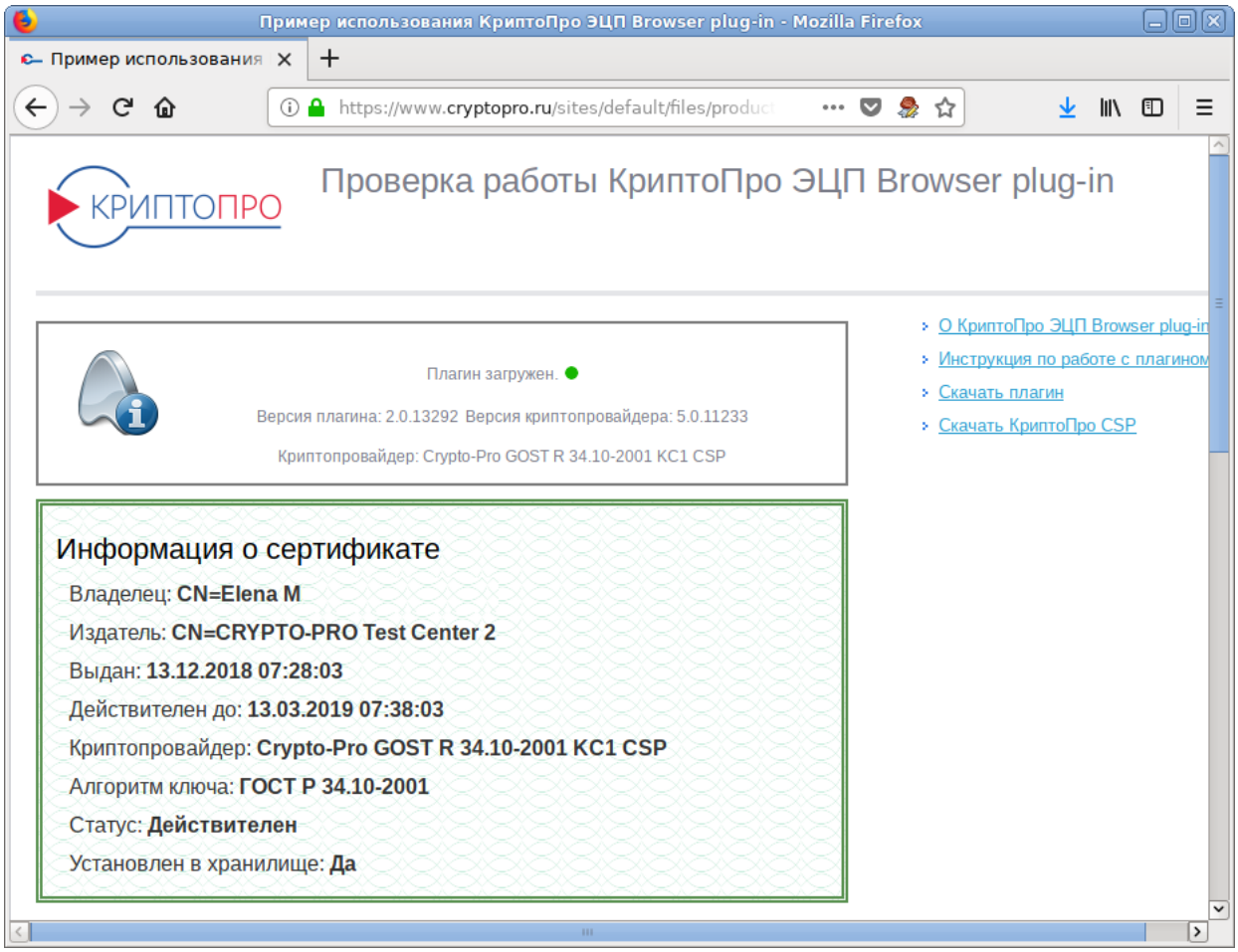


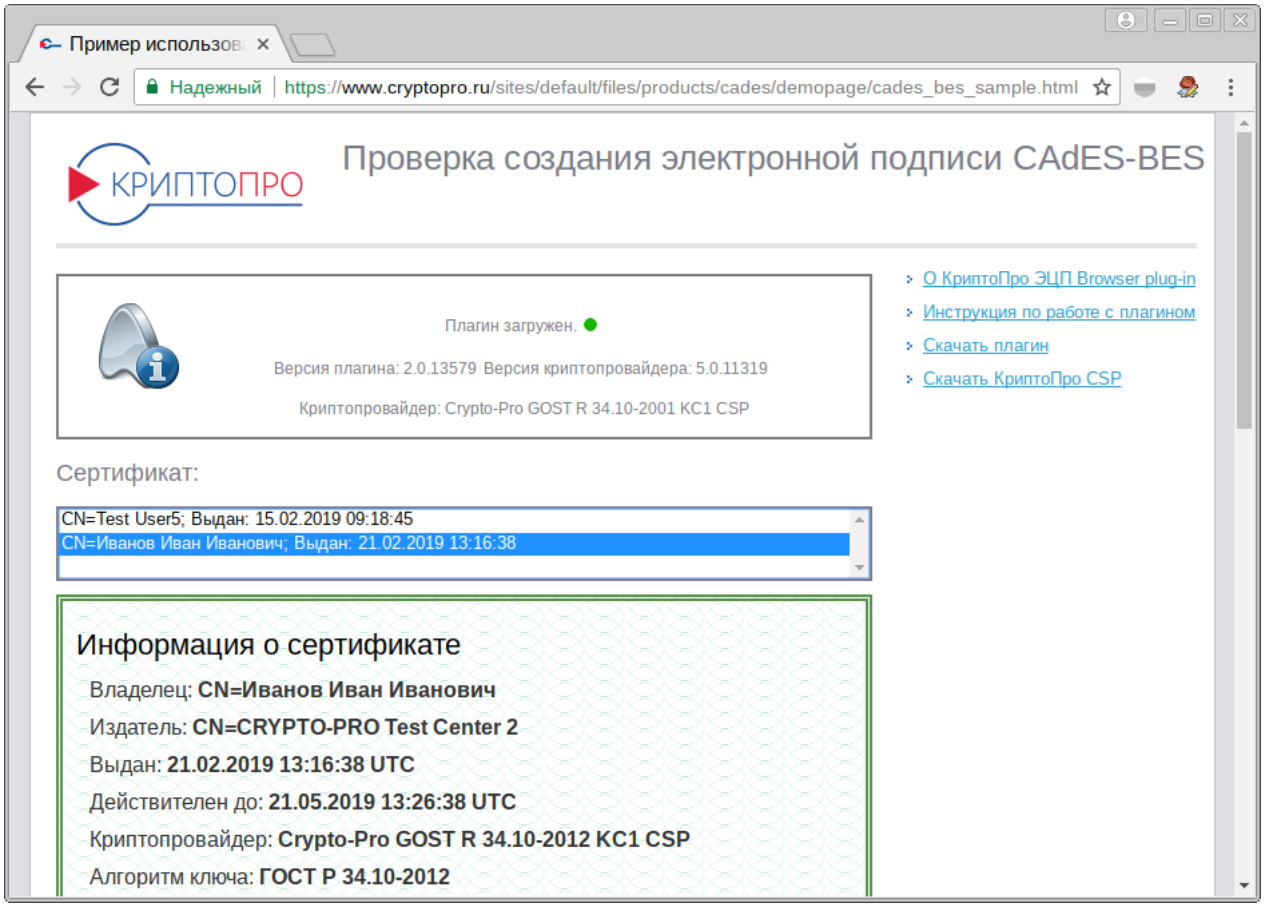
Убедиться, что плагин установлен можно на странице `about:addons` (или `about:plugins` в более ранних версиях Mozilla Firefox). Сделайте его активируемым по умолчанию.

6. Для работы в Chromium установите расширение для браузера на странице `chrome://extensions/`:



7. На странице https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html вверху должна появится надпись: «Плагин загружен» и должен показаться сертификат в списке:





Внимание! Если список пуст, необходимо проверить правильность цепочки сертификатов

1. **Внимание!** Если при переходе на страницу https://www.cryptopro.ru/sites/default/files/products/cades/demopage/simple.html получаем ошибку SEC_ERROR_NO_MODULE, необходимо на странице about:config изменить параметр security.tls.version.max;3 на 2 или 1

zakupki.gov.ru

Для входа в личный кабинет на http://zakupki.gov.ru необходимо:

1. Браузер с поддержкой ГОСТового TLS: Chromium-gost или `firefox-gost`.

2. Так как сертификат у этого сайта неправильный, потребуется новая версия КриптоПро (**4.0.9963** или новее) и выключение строгой проверки имени сервера (под правами root)[1] (https://forum.astralinux.ru/threads/419/#post-3702):

```
# /opt/cprocsp/sbin/amd64/cpconfig -ini '\config\parameters' -add long Rfc6125_NotStrict_ServerName_Check 1
```

Проверка под обычным пользователем:

```
$ /opt/cprocsp/bin/amd64/csptestf -tlsc -server zakupki.gov.ru -nosave
HDEContext expired: OK if file is completely downloaded
Reply status: HTTP/1.1 200 OK
1 connections, 589 bytes in 0.200 seconds;
Total: SYS: 0,020 sec USR: 0,150 sec UTC: 0,250 sec
[ErrorCode: 0x00000000]
```

Вход в ЕСИА

Для аутентификации через ЕСИА (https://esia.gosuslugi.ru/) потребуется установить версию не позже CSP 4.0R3 и плагин IFCPlugin

Подробнее:

- Вход в ЕСИА
- Вход с помощью электронной подписи на портал Госуслуг на Linux (от КриптоПро) (https://support.cryptopro.ru/index.php?/Knowledgebase/Article/View/275)

Примечание:

Для старых версий плагина (< 3.0.0) необходимо добавить в файл `/etc/ifc.cfg` после раздела с Jacarta (для 64-битных систем):

```
{ name  = "CryptoPro CSP";
  alias = "cryptoprocsp";
  type  = "pkcs11";
```

```
   lib_linux = "/opt/cprocsp/lib/amd64/libcppkcs11.so";
 },
```

Примечание:

Для работы с контейнерами КриптоПро (в том числе с ГОСТ-2012) для плагина 3.0.5 необходимо добавить в файл `/etc/ifc.cfg` (для 64-битных систем):

```
{ name  = "CryptoPro CSP5";
   alias = "cprocsp5";
   type  = "pkcs11";
   alg   = "gost2001";
   model = "CPPKCS 3";
   lib_linux = "/opt/cprocsp/lib/amd64/libcppkcs11.so";
 },
 { name  = "CryptoPro CSP5 2012 256";
   alias = "cprocsp5_2012_256";
   type  = "pkcs11";
   alg   = "gost2012_256";
   model = "CPPKCS 3";
   lib_linux = "/opt/cprocsp/lib/amd64/libcppkcs11.so";
 },
{ name  = "CryptoPro CSP5 2012 512";
   alias = "cprocsp5_2012_512";
   type  = "pkcs11";
   alg   = "gost2012_512";
   model = "CPPKCS 3";
   lib_linux = "/opt/cprocsp/lib/amd64/libcppkcs11.so";
 }
```

И сделать символическую ссылку на библиотеку pkcs11:

```
# ln -s /opt/cprocsp/lib/amd64/libcppkcs11.so.4.0.4 /usr/lib/mozilla/plugins/lib/libcppkcs11.so
```

Журнал работы плагина можно найти в файле `/var/log/ifc/engine_logs/engine.log`.

Особенности работы с токенами

Rutoken S

При входе в ЕСИА с помощью Rutoken S не находится приватная часть ключа. В журнале ifc появляется строка:

```
IFC:do_work_sign_cms:ERROR:get_priv_key_by_id error:ifc_sign_cms.c:110
```

Для этого надо перенести приватный ключ в локальное хранилище и задействовать его:

```
$ csptest -keycopy -contsrc 'имя_контейнера_например\\.\Aktiv Rutoken ECP 00 00\xxxxx' -contdest '\\.\HDIMAGE\private' -pindest пароль
$ certmgr -inst -cont '\\.\HDIMAGE\private'
```

КриптоПро JCP

- Для установки КриптоПро JCP нужно установить Oracle Java 1.7.0 (через собственную сборку или пакеты для Fedora)
- Распакуйте архив и перейдите в каталог
- Выполните

```
# ./install.sh /usr/java/jre1.7.0_51 XXXXX-XXXXX-XXXXX-XXXXX-XXXXX "Your Company"
```

Поддержка Рутокена

- Загрузите драйвер для JCP http://www.rutoken.ru/support/download/rutoken-for-cp/ и распакуйте его
- Выполните:

```
# java -jar rtjlib.jar -install -rutoken
```

Запуск контрольной панели

```
$ ./ControlPane.sh /usr
```

(требует графического дисплея)

Ссылки

- ЖТЯИ.00050-03 90 02-02. СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux (из электронной документации по КриптоПро; доступно для скачивания с демонстрационной версией)
- ЖТЯИ.00050-03 90 07. КриптоПро CSP. Приложение командной строки
- Инструкция по настройке **IFCPlugin** (сайт госуслуг) для работы с КриптоПро (https://www.cryptopro.ru/forum2/default.aspx?g=posts&m=83121#post83121)
- ЭЦП
- Набор скриптов для подписания и проверки ЭЦП КриптоПро на Linux (http://pushorigin.ru/cryptopro/linux-crypto-pro)