

Установка CryptoPro 4.0.0 x64

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: www.cryptopro.ru

Примечание.

Для корректной работоспособности электронной подписи в информационных системах необходимо выполнить установку в последовательности:

- Установить программное обеспечение для работы с корневыми и личными сертификатами по инструкции.
- Установить браузер Chromium или Спутник.
- Установить плагин Госуслуг и КриптоПро, в зависимости от системных требований к информационной системе.

Обзор установки

1. Скачайте архив с сайта КриптоПро по [ссылке](#).
2. Распакуйте архив в папку (в примере /home/test/).

```
cd /home/test  
tar -xvf linux-amd64.tgz
```

3. Перейдите в папку с КриптоПро:

```
cd /home/test/linux-amd64
```

4. Установите права на запуск:

```
chmod +x install_gui.sh
```

Выполните следующую команду (для того чтобы далее выполнять команды от пользователя root):

```
su root
```

5. Установите КриптоПро, выполнив команду:

```
./install_gui.sh
```

Появится окно установки КриптоПро:


 image.png and or type unknown

Нажмите кнопку «**Next**» для продолжения установки.

В следующем окне выберите пакеты, указанные на скриншоте:

 image.png and or type unknown

Нажмите кнопку «**Next**» для продолжения установки:

 image.png and or type unknown

Нажмите «**Install**» для установки пакетов.

6. Установите дополнительные пакеты и драйверы.

6.1 Установка драйверов для токенов **Rutoken S**:

для РЕД ОС 7.1 или 7.2:

```
yum install -y ifd-rutokens
```

для РЕД ОС 7.3 и старше:

```
dnf install -y ifd-rutokens
```

6.2 Установка драйверов для токенов Jacarta:

Перейдите в папку:

```
cd /home/test/linux-amd64
```

для РЕД ОС 7.1 или 7.2 выполните команду установки:

```
yum localinstall cprocsp-rdr-jacarta*.rpm
```

для РЕД ОС 7.3 и старше перейдите в папку:

```
dnf install cprocsp-rdr-jakarta*.rpm
```

Проверка лицензии

Вывод серийного номера лицензии:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -view
```

Ввод номера лицензии:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -set <серийный_номер>
```

Установка программного обеспечения для работы с сертификатами

1. Установка средства управления сертификатами token-manager:

для РЕД ОС 7.1 или 7.2:

```
yum install token-manager
```

для РЕД ОС 7.3 и старше:

```
dnf install token-manager
```

2. Установка программного обеспечения для подписи файлов **gostcrypto**.

2.1 Для рабочего стола **Mate**:

для РЕД ОС 7.1 или 7.2:

```
yum install gostcryptogui caja-gostcryptogui
```

для РЕД ОС 7.3 и старше:

```
dnf install gostcryptogui caja-gostcryptogui
```

2.2 Для рабочего стола **Cinnamon**:

для РЕД ОС 7.1 или 7.2:

```
yum install nemo-gostcryptogui.noarch
```

для РЕД ОС 7.3 и старше:

```
dnf install nemo-gostcryptogui.noarch
```

Работа с ключевыми носителями и сертификатами.

Ключевые носители и сертификаты

Для работы с ключевыми носителями и сертификатами используется утилита «Ключевые носители и сертификаты», которую мы установили ранее. Найти его можно в «Главном меню» - «Администрирование» - «Ключевые носители и сертификаты».

Окно программы выглядит следующим образом:

image.png
image not found or type unknown

В меню «**Операции**» можно выполнить:

- Ввод лицензии КриптоПро CSP;
- Просмотр лицензии;
- Установка корневых сертификатов;
- Установка списка отозванных сертификатов;
- Просмотр корневых сертификатов;
- Просмотр списков отозванных сертификатов;
- Скопировать контейнер с токена;
- Скопировать контейнер с **usb-flash** накопителя;
- Скопировать токен из HDIMAGE на токен.

Рассмотрим более подробно копирование контейнера с **usb-flash** накопителя.

1. Необходимо с **RuToken** скопировать закрытую часть электронной подписи (ЭП) на usb-flash накопитель, выполнить это необходимо на КристоПро в ОС Windows.
2. Вставьте **usb-flash** накопитель в компьютер и запустите утилиту Ключевые носители и сертификаты.
3. Перейдите в меню «**Операции**» и выберите «**Скопировать контейнер с usb-flash накопителя**».
4. Появится окно с выбором контейнера. Выберите необходимый контейнер, отметив чекбокс в поле «**Выбранный**».

image.png
image not found or type unknown

5. Задайте имя контейнеру.

image.png
image not found or type unknown

6. Выберите контейнер, в который требуется скопировать.

image.png
image not found or type unknown

7. Далее потребуется ввести PIN-код контейнеров.

8. Появится окно с успешной привязкой контейнера с сертификата. Сертификат отобразится в «**Личном хранилище сертификатов**».

image.png
image not found or type unknown

Работа по копированию контейнеров с токена или из HDIMAGE имеет схожую логику.

1. Для выбора необходимого контейнера требуется выбрать галочкой необходимый.

image.png
image not found or type unknown

2. Следующим этапом необходимо выбрать пункт назначения копирования.

Пользователю предоставляется возможность задать новое имя копируемого контейнера (настоятельно рекомендуем использовать латиницу).

image.png
image not found or type unknown

3. Далее выбирается токен или **HDIMAGE**.

image.png
image not found or type unknown

4. После ввода PIN-кодов, в случае успеха, вы увидите сообщение:

В последних версиях token-manager была добавлена возможность консольного запуска утилиты с использованием ряда ключей:

```
token-manager.py --help
```

Подсказки по использованию ключей в token-manager:

В данной реализации token-manager поддерживает явное указание архитектуры КриптоПро, вместо автоматического.

--amd64 вызов 64-битной версии КриптоПро;

--ia32 вызов 32-битной версии КриптоПро;

--aarch64 вызов aarch64 версии КриптоПро;

--e2k64 вызов e2k64 версии КриптоПро;

--version вывод номера версии token-manager;

--debug-output пробный вызов основных функций утилиты;

--debug-output --amd64 пробный вызов основных функций утилиты для архитектуры amd64;

--debug-output --ia32 пробный вызов основных функций утилиты для архитектуры ia32;

--debug-output --aarch64 пробный вызов основных функций утилиты для архитектуры aarch64;

--debug-output --e2k64 пробный вызов основных функций утилиты для архитектуры e2k64;

Пример вывода версии утилиты:

```
token-manager.py --version
```

```
token-manager версия 2.0
```

GOST-CRYPTO-GUI

Формат подписи может настраиваться в графической утилите **gostcryptogui**, которую мы рассмотрим далее.

Запуск утилиты производится из «**Главного меню**» - «**Администрирование**» - «**Подпись и шифрование файлов**».

Окно программы выглядит следующим образом:

image.png
image not found or type unknown

Доступны следующие опции:

- Криптопровайдер;
- Кодировка файлов;

- Авт. проверка подписи;
- Отсоединённая подпись.

Для примера зашифруйте файл, но с использованием другого сертификата, размещённого на ключевом носителе **Rutoken**.

Выберите необходимый файл:

image.png

Затем укажите ваш сертификат:

image.png

Зашифрованный файл формируется с тем же именем и расширением .enc.

image.png

После этого попробуйте его расшифровать.

Нажмите «**Расшифровать файл(ы)**», выберите зашифрованный файл, затем сертификат, которым был зашифрован наш файл.

image.png

Подпись документов в LibreOffice

Для активации подписания документов потребуется установить плагин:

```
dnf install LibreOffice-plugin-altcsp
```

Для активации подписи требуется нажать кнопку «Файл». Если меню «Файл» недоступно, нажмите предварительно кнопку, выделенную на скриншоте:

image.png

Нажмите кнопку «**Электронная подпись**»:

image.png

Для подписи вам будет предложен выбор сертификата:

image.png

Также не забудьте проверить, что для выбранного сертификата у вас установлены все необходимые корневые и отозванные сертификаты. Пример необходимых сертификатов можно проверить командой:

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

```
***
```

```
CA cert URL : http://testgost2012.cryptopro.ru/CertEnroll/root2018.crt
```

```
CDP : http://testgost2012.cryptopro.ru/CertEnroll/!0422!0435!0441!0442!043e!0432!044b!0439%20!0423!0426%
```

```
CDP : http://testgost2012.cryptopro.ru/CertEnroll/testgost2012(1).crl
```

```
***
```

Как показано в примере, необходимо доставить **3 сертификата**. Выполнить это можно через **token-manager** и установку сертификатов из утилиты.

В случае успешной подписи вы увидите следующее уведомление:

image.png
image not found or type unknown

Проверить подпись можно из «**gostcryptogui**» - «**Проверить подпись**».

После выбора документа вы увидите следующую информацию:

image.png
image not found or type unknown

Revision #3

Created 16 October 2023 12:20:37 by Admin

Updated 13 November 2023 05:27:53 by Admin