

Работа с КриптоПро CSP



- 1 КриптоПро CSP
 - 1.1 Назначение
- 2 Установка КриптоПро CSP
 - 2.1 Описание необходимых пакетов КриптоПро
 - 2.2 Для просмотра всех установленных пакетов КриптоПро CSP, следует ввести команду:
 - 2.3 Прописывание путей к исполняемым файлам
 - 2.4 Установка дополнительных пакетов с модулем поддержки для токена
 - 2.5 Установка лицензии
- 3 Носители и контейнеры
 - 3.1 Идентификация токена
 - 3.1.1 Информация о контейнерах
 - 3.1.2 Проверка работы контейнера
 - 3.1.3 Удаление контейнера
 - 3.1.4 Копирование контейнера
- 4 Менеджер сертификатов КриптоПРО в Linux
 - 4.1 4 категории сертификатов
 - 4.2 Установка
 - 4.3 Просмотр
 - 4.4 Удаление
 - 4.5 Экспорт сертификатов на другую машину
 - 4.6 Проверка цепочки сертификатов
- 5 Подписание документа ЭЦП
 - 5.1.1 Подпись файлов (присоединённая)
 - 5.1.2 Подпись файлов(отсоединённая)
 - 5.2 Проверка подписи в файле
 - 5.2.1 Для прикрепленной подписи
 - 5.2.2 естественный
 - 5.2.3 обучающий
 - 5.3 Извлечение подписанного файла
- 6 Графический интерфейс КриптоПро CSP v. 5.0 (cptools)
- 7 Удаление КриптоПро CSP
- 8 Отключение окон о необходимости перехода на ГОСТ Р 34.10-2012
- 9 Полезные ссылки
 - 9.1 КриптоПро: IFCP plugin для входа ЕСИА (Госуслуги)
 - 9.2 КриптоПро CADES ЭЦП Browser plug-in
 - 9.3 Таблица поддерживаемых устройств Крипто-Про CSP
 - 9.4 База знаний КриптоПро
 - 9.5 Обсуждение КриптоПро CSP на форуме astralinux
 - 9.6 Chromium+КриптоПРО
 - 9.7 Список ГИС и ЭТП использующих cades-bes plugin
 - 9.8 Перечень аккредитованных удостоверяющих центров
- 10 Диагностический архив для обращения в тех. поддержку

КриптоПро CSP

Назначение

Криптопровайдер КриптоПро CSP предназначен для:

- авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной подписи (ЭП) в соответствии с отечественными стандартами ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012 (с использованием ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012);
- обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;
- обеспечения аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS;
- контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;
- управления ключевыми элементами системы в соответствии с регламентом средств защиты.

<https://www.cryptopro.ru/products/csp>

Установка КриптоПро CSP

Архив с программным обеспечением (КриптоПро CSP) можно [загрузить](#) с официального сайта www.cryptopro.ru, предварительно зарегистрировавшись на сайте.

Для ОС Astra Linux следует загрузить пакет:

[КриптоПро CSP 4.0 для Linux \(x64, deb\)](#) - пакет для 64 разрядной системы.



Пробный период использования КриптоПро CSP составляет 3 месяца, по истечении которых необходимо приобрести полноценную лицензию.

К моменту написания статьи, была использована сертифицированная версия ПО «КриптоПро» «4.0 R4».

Для примера был проделан следующий алгоритм действий:

1) Загрузка архива с сертифицированной версией ПО «КриптоПро»:

Название полученного файла: [linux-amd64_deb.tgz](#).

2) Открыть "Терминал Fly" (alt+T)

3) Разархивируем скаченный архив в терминале командой:

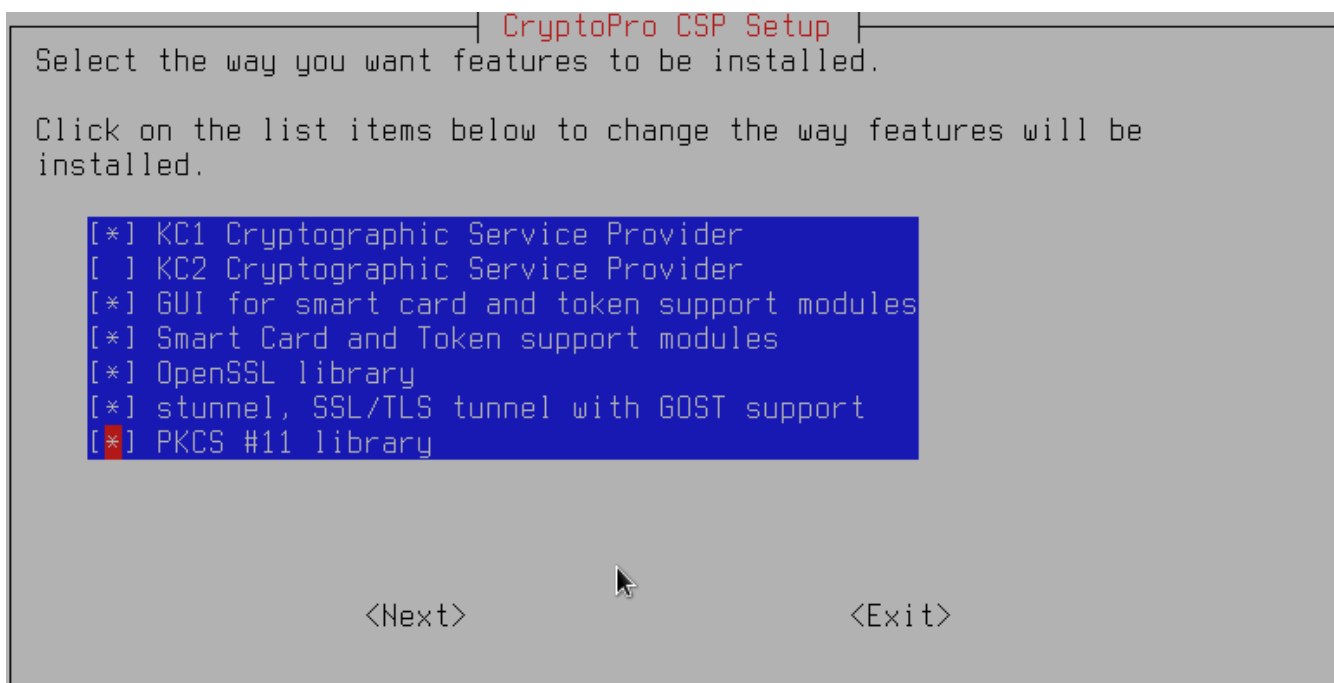
```
tar -zxf linux-amd64_deb.tgz
```

5) Перейдем в директорию с ПО

```
cd linux-amd64_deb
```

6) выполним установку ПО с помощью запуска скрипта "install.sh" или "instal_gui.sh" командой:

```
sudo ./install_gui.sh
```



* Выбрать необходимые модули, библиотеки.

Описание необходимых пакетов КриптоПро

Пакет	Описание
Базовые пакеты:	
сprocsp-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-rdr	Поддержка ридеров и RNG
Дополнительные пакеты:	
сprocsp-rdr-gui-gtk	Графический интерфейс для диалоговых операций
сprocsp-rdr-rutoken	Поддержка карт Рутокен
сprocsp-rdr-jacarta	Поддержка карт JaCarta
сprocsp-rdr-pcsc	Компоненты PC/SC для ридеров КриптоПро CSP
lsb-cprocsp-pkcs11	Поддержка PKCS11

Для просмотра всех установленных пакетов Криптопро CSP, следует ввести команду:

```
dpkg -l | grep сprocsp
```

```

root@smakhmadiev:~# dpkg -l | grep cprosp
ii cprosp-compat-debian      1.0.0-1          all          CryptoPro CSP compatibility extension for non-LSB Debian/Ubuntu
ii cprosp-cpopenssl-64      4.0.9944-5      amd64       OpenSSL. Build 9944.
ii cprosp-cpopenssl-base    4.0.9944-5      all         Openssl common Build 9944.
ii cprosp-cpopenssl-gost-64 4.0.9944-5      amd64       OpenSSL capi_gost engine. Build 9944.
ii cprosp-curl-64           4.0.9944-5      amd64       CryptoPro Curl shared library and binaris. Build 9944.
ii cprosp-pki-cades         2.0.0-2          amd64       CryptoPro PKI
ii cprosp-pki-plugin        2.0.0-2          amd64       CryptoPro PKI
ii cprosp-rdr-emv-64        4.0.9944-5      amd64       EMV/Genalto support module
ii cprosp-rdr-gui-gtk-64    4.0.9944-5      amd64       GUI components for CryptoPro CSP readers. Build 9944.
ii cprosp-rdr-inpasport-64 4.0.9944-5      amd64       Inpasport support module
ii cprosp-rdr-jakarta-64   5.0.0            amd64       JaCarta components for CryptoPro CSP for use JaCarta devices. Build 1114.
ii cprosp-rdr-mskey-64      4.0.9944-5      amd64       Mskey support module
ii cprosp-rdr-novacard-64   4.0.9944-5      amd64       Novacard support module
ii cprosp-rdr-pcsc-64       4.0.9944-5      amd64       PC/SC components for CryptoPro CSP readers. Build 9944.
ii cprosp-rdr-rutoken-64    4.0.9944-5      amd64       Rutoken support module
ii cprosp-stunnel-64        4.0.9944-5      amd64       Universal SSL/TLS tunnel.
ii lsb-cprosp-base          4.0.9944-5      all         CryptoPro CSP directories and scripts. Build 9944.
ii lsb-cprosp-ca-certs      4.0.9944-5      all         CA certificates. Build 9944.
ii lsb-cprosp-capilite-64   4.0.9944-5      amd64       CryptoPI lite. Build 9944.
ii lsb-cprosp-kc1-64        4.0.9944-5      amd64       CryptoPro CSP KC1. Build 9944.
ii lsb-cprosp-pkcs11-64     4.0.9944-5      amd64       CryptoPro PKCS11. Build 9944.
ii lsb-cprosp-rdr-64        4.0.9944-5      amd64       CryptoPro CSP readers. Build 9944.
root@smakhmadiev:~#

```

Прописывание путей к исполняемым файлам

Для того, чтобы не вводить каждый раз полный путь к утилитам КриптоПро CSP, в терминале FLY следует ввести команду:

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

Установка дополнительных пакетов с модулем поддержки для токена

Для корректной работы с токеном/смарт-картой обязательно требуется установить:

библиотека **libccid**, **libgost-astra**, пакеты **pcscd**

```
sudo apt install libccid pcscd libgost-astra
```

Пакеты с модулем поддержки для:

Рутокен: <https://www.rutoken.ru/support/download/nix/>

Алладин: <https://www.aladdin-rd.ru/support/downloads/jakarta>

После установки пакетов с модулем поддержки токена следует перезагрузить службу pcscd:

```
sudo service pcscd restart
```



Начиная с версии КриптоПро 4.0 R4 и выше, модули поддержки смарткарт входят в состав пакета.

Проверка лицензии

Проверить срок истечения лицензии можно командой:

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

```
root@smakhmadiev:/# /opt/cproccsp/sbin/amd64/cpconfig -license -view
License validity:
4040E-60037-EK0R3-C6K4U-HCXQG
Expires: 2 month(s) 17 day(s)
License type: Server.
```

Установка лицензии

Для установки другой лицензии следует выполнить команду :

```
sudo /opt/cproccsp/sbin/amd64/cpconfig -license -set <__>
```

Носители и контейнеры

Идентификация токена

Чтобы узнать модель подключенного токена, следует ввести команду:

```
/opt/cproccsp/bin/amd64/csptest -card -enum -v -v
```

После чего система выдаст информацию о подключенном устройстве:

```
root@smakhmadiev:/home/shuhrat/ecp# csptest -card -enum -v -v
Aktiv Rutoken ECP 00 00
  Card present, ATR=3B 8B 01 52 75 74 6F 6B 65 6E 20 44 53 20 C1
  Unknown applet
Total: SYS: 0,000 sec USR: 0,000 sec UTC: 0,000 sec
[ErrorCode: 0x00000000]
```

Проверить наличие носителей с контейнерами можно с помощью команды:

```
/opt/cproccsp/bin/amd64/csptest -keyset -verifycontext -enum -unique
```

```
root@smakhmadiev:/home/shuhrat/ecp# csptest -keyset -verifycontext -enum -unique
CSP (Type:80) v5.0.10001 KC1 Release Ver:5.0.11233 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 8495427
TestCont          ISCARD\rutoken_ecp_390a75ab\0A00\8AC7
Shuhrat           ISCARD\rutoken_ecp_390a75ab\0B00\5228
Shuhrat           IHDIMAGE\\Shuhrat.000\5228
TestCont123      IHDIMAGE\\TestCont.000\7760
OK.
Total: SYS: 0,010 sec USR: 0,080 sec UTC: 0,240 sec
[ErrorCode: 0x00000000]
```

в формате FQCN, отображается имя носителя:

```
/opt/cproccsp/bin/amd64/csptest -keyset -enum_cont -fqcn -verifyc
```

В этом случае будет выведен список носителей с контейнерами в следующем формате:

```

root@smakhmadiev:/home/shuhrat/ecp# /opt/cproscsp/bin/amd64/csptest -keyset -enum_cont -fqcn -verifyc
CSP (Type:80) v5.0.10001 KC1 Release Ver:5.0.11233 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 37105987
\\.\Aktiv Rutoken ECP 00 00\TestCont
\\.\Aktiv Rutoken ECP 00 00\Shuhrat
\\.\HDIMAGE\Shuhrat
\\.\HDIMAGE\TestCont123
OK.
Total: SYS: 0,010 sec USR: 0,080 sec UTC: 0,230 sec
[ErrorCode: 0x00000000]

```

Где \\.\HDIMAGE - локальный носитель, \\.\HDIMAGE\TestCont123 - название контейнера, \\.\Aktiv Rutoken ECP 00 00 - название носителя (токена).

Подробная информация про ["Имена контейнеров"](#)

Информация о контейнерах

Для просмотра подробной информации о контейнерах воспользуйтесь командой:

```
/opt/cproscsp/bin/amd64/csptestf -keyset -container 'ИМЯ' -info
```

```

/opt/cproscsp/bin/amd64/csptestf -keyset -container 'Shuhrat' -info
CSP (Type:80) v5.0.10001 KC1 Release Ver:5.0.11233 OS:Linux CPU:AMD64 FastCode:READY:AVX.

```

```

AcquireContext: OK. HCRYPTPROV: 8981043
GetProvParam(PP_NAME): Crypto-Pro GOST R 34.10-2012 KC1 CSP
Container name: "Shuhrat"
Signature key is available. HCRYPTKEY: 0x8f3b03
Exchange key is available. HCRYPTKEY: 0x8f9883
Symmetric key is not available.
UEC key is not available.

```

CSP algorithms info:

```
Type:Encrypt Name:'GOST 28147-89'(14) Long:'GOST 28147-89'(14)
DefaultLen:256 MinLen:256 MaxLen:256 Prot:0 Algid:00026142
```

```
Type:Hash Name:'GR 34.11-2012 256'(18) Long:'GOST R 34.11-2012 256'(22)
DefaultLen:256 MinLen:256 MaxLen:256 Prot:0 Algid:00032801
```

```
Type:Signature Name:'GR 34.10-2012 256'(18) Long:'GOST R 34.10-2012 256'(22)
DefaultLen:512 MinLen:512 MaxLen:512 Prot:0 Algid:00011849
```

```
Type:Exchange Name:'DH 34.10-2012 256'(18) Long:'GOST R 34.10-2012 256 DH'(25)
DefaultLen:512 MinLen:512 MaxLen:512 Prot:0 Algid:00043590
```

```
Type:Exchange Name:'DH 34.10-2012 256'(18) Long:'GOST R 34.10-2012 256 DH'(25)
DefaultLen:512 MinLen:512 MaxLen:512 Prot:0 Algid:00043591
```

```
Type:Hash Name:'GOST 28147-89 MAC'(18) Long:'GOST 28147-89 MAC'(18)
DefaultLen:32 MinLen:8 MaxLen:32 Prot:0 Algid:00032799
```

```
Type:Encrypt Name:'GR 34.12 64 M'(14) Long:'GOST R 34.12-2015 64 Magma'(27)
DefaultLen:256 MinLen:256 MaxLen:256 Prot:0 Algid:00026160
```

```
Type:Encrypt Name:'GR 34.12 128 K'(15) Long:'GOST R 34.12-2015 128 Kuznyechik'(33)
DefaultLen:256 MinLen:256 MaxLen:256 Prot:0 Algid:00026161
```

```
Type:Hash Name:'GR 34.13 64 M MAC'(18) Long:'GOST R 34.13-2015 64 Magma MAC'(31)
DefaultLen:64 MinLen:8 MaxLen:64 Prot:0 Algid:00032828
```

```
Type:Hash Name:'GR 34.13 128 K MAC'(19) Long:'GOST R 34.13-2015 128 Kuznyechik MAC'(37)
DefaultLen:128 MinLen:8 MaxLen:128 Prot:0 Algid:00032829
```

```
Type:Hash Name:'GR34.11-12 256 HMAC'(20) Long:'GOST R 34.11-2012 256 HMAC'(27)
DefaultLen:256 MinLen:256 MaxLen:256 Prot:0 Algid:00032820
```

Status:

```

Provider handles used: 6
Provider handles max: 1048576
CPU Usage: 6 %

```

CPU Usage by CSP: 0 %
Measurement interval: 119 ms

Virtual memory used: 15281652 KB
Virtual memory used by CSP: 116572 KB
Free virtual memory: 26053680 KB
Total virtual memory: 41335332 KB

Physical memory used: 14602360 KB
Physical memory used by CSP: 12576 KB
Free physical memory: 5857712 KB
Total physical memory: 20460072 KB

Key pair info:

HCRYPTKEY: 0x8f3b03
AlgID: CALG_GR3410_12_256 = 0x00002e49 (00011849):
AlgClass: ALG_CLASS_SIGNATURE
AlgType: ALG_TYPE_GR3410
AlgSID: 73
KP_HASHOID:
1.2.643.7.1.1.2.2 (ГОСТ Р 34.11-2012 256 бит)
KP_DHOID:
1.2.643.2.2.35.1 (ГОСТ Р 34.10 256 бит, параметры по умолчанию)
KP_SIGNATUREOID:
1.2.643.2.2.35.1 (ГОСТ Р 34.10 256 бит, параметры по умолчанию)
Permissions:
CRYPT_READ
CRYPT_WRITE
CRYPT_IMPORT_KEY
0x800
0x2000
0x20000
0x100000
KP_CERTIFICATE:
Not set.

Key pair info:

HCRYPTKEY: 0x8f9883
AlgID: CALG_DH_GR3410_12_256_SF = 0x0000aa46 (00043590):
AlgClass: ALG_CLASS_KEY_EXCHANGE
AlgType: ALG_TYPE_DH
AlgSID: 70
KP_HASHOID:
1.2.643.7.1.1.2.2 (ГОСТ Р 34.11-2012 256 бит)
KP_DHOID:
1.2.643.2.2.36.0 (ГОСТ Р 34.10 256 бит, параметры обмена по умолчанию)
KP_SIGNATUREOID:
1.2.643.2.2.36.0 (ГОСТ Р 34.10 256 бит, параметры обмена по умолчанию)
Permissions:
CRYPT_READ
CRYPT_WRITE
CRYPT_IMPORT_KEY
0x800
0x10000
0x20000
0x100000
KP_CERTIFICATE:
Subject: INN=007814508921, E=user@astralinux.ru, C=RU, CN=Махмадиев Шухрат, SN=Махмадиев
Valid : 18.10.2018 12:07:24 - 18.01.2019 12:17:24 (UTC)
Issuer : E=support@cryptopro.ru, C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN=CRYPTO-PRO Test Center 2

Container version: 2

Carrier flags:

This reader is removable.
This reader supports unique carrier names.
This carrier does not have embedded cryptography.

Keys in container:

signature key
exchange key

Extensions (maxLength: 1435):

ParamLen: 46
OID: 1.2.643.2.2.37.3.9
Critical: FALSE
Size: 19
Decoded size: 24
PrivKey: Not specified - 18.01.2020 07:31:07 (UTC)

ParamLen: 47
OID: 1.2.643.2.2.37.3.10
Critical: FALSE
Size: 19
Decoded size: 24
PrivKey: Not specified - 18.01.2020 07:31:12 (UTC)
Total: SYS: 0,020 sec USR: 0,180 sec UTC: 2,180 sec
[ErrorCode: 0x00000000]



Следует учесть про PIN-коды в контейнерах:

* если само устройство осуществляет аутентификацию (как к примеру токен), то PIN при создании не создаётся, а предъявляется, так как он - свойство устройства. Как следствие: у всех контейнеров на токене одинаковый PIN.

* если устройство не аутентифицирует (как HDIMAGE), то при создании контейнера, создаётся PIN-код. Следствие: у всех контейнеров, PIN-код на HDIMAGE может быть разным.

Проверка работы контейнера

Для того чтобы проверить работу контейнера (в том числе возможность выполнения разных операций при текущей лицензии), следует выполнить команду:

```
/opt/cproscsp/bin/amd64/csptestf -keyset -container ИМЯ -check
```

```
/opt/cproscsp/bin/amd64/csptestf -keyset -container Shuhrat -check
```

```
CSP (Type:80) v5.0.10001 KC1 Release Ver:5.0.11233 OS:Linux CPU:AMD64 FastCode:READY:AVX.
```

```
AcquireContext: OK. HCRYPTPROV: 28224051
```

```
GetProvParam(PP_NAME): Crypto-Pro GOST R 34.10-2012 KC1 CSP
```

```
Container name: "Shuhrat"
```

```
Check header passed.
```

```
Signature key is available. HCRYPTKEY: 0x1b53883
```

```
Exchange key is available. HCRYPTKEY: 0x1b57e23
```

```
Symmetric key is not available.
```

```
UEC key is not available.
```

```
License: Cert without license
```

```
Check container passed.
```

```
Check sign passed.
```

```
Check verify signature on private key passed.
```

```
Check verify signature on public key passed.
```

```
Check import passed (import restricted).
```

```
Check sign passed.
```

```
Check verify signature on private key passed.
```

```
Check verify signature on public key passed.
```

```
Check import passed.
```

```
Certificate in container matches AT_KEYEXCHANGE key.
```

```
Keys in container:
```


signature key

exchange key

Extensions:

OID: 1.2.643.2.2.37.3.9

PrivKey: Not specified - 18.01.2020 07:31:07 (UTC)

OID: 1.2.643.2.2.37.3.10

PrivKey: Not specified - 18.01.2020 07:31:12 (UTC)

Total: SYS: 0,030 sec USR: 0,140 sec UTC: 2,430 sec

[ErrorCode: 0x00000000]

Удаление контейнера

Для удаления контейнера следует воспользоваться командой:

```
/opt/cprosp/bin/amd64/csptestf -passwd -cont '\\\Aktiv Rutoken ECP 00 00\TestCont' -deletек
```

Копирование контейнера

Для примера скопируем контейнер из локального хранилища в хранилище Рутокена ЕЦП:

```
csptestf -keycopy -contsrc '\\\HDIMAGE\Контейнер_оригинал' -contdest '\\\Aktiv Rutoken ECP 00 00\Контейнер_копия'
```

Менеджер сертификатов КриптоПРО в Linux

4 категории сертификатов

Они делятся на четыре категории:

* личные сертификаты (ставятся в хранилище `иму`, где `u` = User, `my` - имя хранилища) - как правило для них есть закрытый ключ (и они требуют особой установки, чтобы в хранилище появилась ссылка на этот закрытый ключ). В результате с их использованием можно, например, подписать файл.

* корневые сертификаты - краеугольный камень безопасности, так как цепочки доверия строятся от них, то их надо добавлять в хранилища осознанно и внимательно (ставятся в `игоот`, также администратор может поставить их в `мгоот`, где `m` = Machine, такие сертификаты будут видны в `read only` в `root`-хранилищах всех пользователей)

* промежуточные сертификаты - появляются, когда есть промежуточные УЦ (головной -> промежуточный -> пользовательский). Прямое доверие к ним не требуется (ставятся в `иса`, также администратор может поставить их в `мсса`). В это же хранилище ставятся CRL-и. Обычно точки получения промежуточных сертификатов и CRL-ей правильно указаны в пользовательских сертификатах, поэтому они автоматом выкачиваются и попадают в хранилище `иса`. В общем про них можно ничего особо не знать и ничего не делать.

* сертификаты партнёров по общению, чтобы проверять их подписи и зашифровывать для них сообщения. Ставятся либо в `иму` (это беспорядок, но популярный), либо в `uAddressBook`

Установка

Пример установки личного сертификата, выданного УЦ Министерства обороны Российской Федерации

```
uMy :
$ /opt/cproscsp/bin/amd64/csptestf -absorb -cert -pattern 'rutoken'

uMy:
$ /opt/cproscsp/bin/amd64/certmgr -inst -cont '\\.\Aktiv Rutoken ECP 00 00\Ivanov'

mRoot:
$ sudo curl https://structure.mil.ru/files/morf/military/files/guc18.cer|sudo /opt/cproscsp/bin/amd64/certmgr -
inst -store mRoot -stdin

mca:
$ sudo curl http://structure.mil.ru/download/doc/morf/military/files/CA2018.cer|sudo /opt/cproscsp/bin/amd64
/certmgr -inst -store mca -stdin

(CRL), mca:
$ sudo curl http://structure.mil.ru/download/doc/morf/military/files/crl_18.crl|sudo /opt/cproscsp/bin/amd64
/certmgr -inst -store mca -stdin -crl
```



Примечание

В опции -pattern >>> 'rutoken' может быть другим в зависимости от подключенного токена.

```
, stdin -file /tmp/ca.cer -file /tmp/ca.crl
```



Примечание

- 1) Имена хранилищ указаны в формате certmgr, у gryptsp похожий формат: -mroot и -uAddressBook
- 2) Из под учетной записи пользователя ставится в uca, из под учетной записи администратора ставить в mca:
- 3) В опции -pattern можно указать пустые <' '> чтобы установить все сертификаты в uMy. Пример:

```
/opt/cproscsp/bin/amd64/csptestf -absorb -cert -pattern ''
```
- 4) В случае, если личный сертификат извлечен, следует использовать опцию -file :

```
certmgr -inst -file cert.cer -store uMy
```
- 5) Хранилища пользователей хранятся в /var/opt/cproscsp/users

Просмотр

Для просмотра выше установленных сертификатов можно воспользоваться :

```
/opt/cproscsp/bin/amd64/certmgr -list
```

```
shuhrat@smakhmadiev:/opt/cprosp/bin/amd64$ certmgr -list -store uroot
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       : 0x2B6E3351F06EB2AD40200203CB5BA141
SHA1 Hash    : 046255290b0eb1cdd1797d9ab0c81f699e3687f3
SubjKeyID    : 15317cb08d1ade66d7159c4952971724b9017a83
Signature Algorithm : GOCT P 34.11/34.10-2001
PublicKey Algorithm : GOCT P 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=dit@minsvyaz.ru, C=RU, S=77 г. Москва, L=Москва, STREET="125375 г. Москва, ул. Тверская,
ноу удостоверяющий центр
Subject      : E=uc@mail.ru, OGRN=1037700255284, INN=007704252261, C=RU, S=77 г. Москва, L=Москва, STREET=у
терство обороны Российской Федерации, CN=Министерство обороны Российской Федерации
Serial       : 0x000100F4F5000000000309
SHA1 Hash    : 3bfd61fad08931dbbc53f79bbd051aa4c4d3f03
SubjKeyID    : a21c01faf8e344ceb999ba0cd192f4ea1a8fd5c9
Signature Algorithm : GOCT P 34.11/34.10-2001
PublicKey Algorithm : GOCT P 34.10-2001 (512 bits)
Not valid before : 20/09/2018 09:11:48 UTC
Not valid after  : 20/09/2026 09:11:48 UTC
PrivateKey Link  : No
CDP          : http://rostelecom.ru/cdp/guc.crl
CDP          : http://reestr-pki.ru/cdp/guc.crl
3-----
Issuer       : E=dit@minsvyaz.ru, C=RU, S=77 Москва, L=г. Москва, STREET="улица Тверская, дом 7", O=Минком
Subject      : E=uc@mail.ru, OGRN=1037700255284, INN=007704252261, C=RU, S=77 г. Москва, L=Москва, STREET=у
терство обороны Российской Федерации, CN=Министерство обороны Российской Федерации
Serial       : 0x7CA5D4F7000000000000
SHA1 Hash    : c7588c3365f0ed78be0dcff22aa33074f11d8b95
SubjKeyID    : 4ab7c589e2d91dff0ec01225b7e6841dbee8bc33e
```

Удаление

Удаление сертификата из хранилища КриптоПро:

```
certmgr -delete 1 (номер сертификата)
```

```
certmgr -del -all (удаление всех сертификатов)
```

Экспорт сертификатов на другую машину

Закрытые ключи к сертификатам находятся тут: /var/opt/cprosp/keys.

Поэтому эти ключи переносятся просто: создаем архив и переносим на нужную машину в тот же каталог.

Экспорт сертификата:

```
/opt/cprosp/bin/amd64/certmgr -export -dest cert.cer
```

Переносим эти файлы на машину и смотрим, какие контейнеры есть:

```
csptest -keyset -enum_cont -verifycontext -fgcn
```

И как обычно, связываем 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:

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

Проверка цепочки сертификатов

Для примера: чтобы проверить цепочку сертификатов, можно скопировать персональный сертификат в файл:

```
/opt/cproscsp/bin/amd64/cryptcp -copycert -dn CN=Имя_вашего_сертификата -df /temp/сертификат.cer
```



Можно указать другое поле сертификата: CN, E, SN, OGRN, SNILS и тд.

```
CryptCP 5.0 (c) "-", 2002-2018.
.
:
: " "-
  "", , 77 .
, RU, . 26, mail@rusbitech.ru
  02.10.2018 14:31:02 02.10.2019 14:41:02
:
: " "-
  "", , , "
  "-
  "", , , 77 .
, RU, . 26, 5087746137023, 007726604816,
13407634844, mail@rusbitech.ru

  02.10.2018 14:31:02 02.10.2019 14:41:02

: ( 10000):
/dailybuilds/CSPbuild/CSP/samples/CPCrypt/Certs.cpp:396: 0x20000133
([Y], [N], [C])?
```

Из вывода следует, что у нас отсутствует некий сертификат в цепочке сертификатов. Можно запустить вышеуказанную команду в режиме debug(отладки):

```
$ CP_PRINT_CHAIN_DETAIL=1 /opt/cproscsp/bin/amd64/cryptcp -copycert -dn CN=__ -df /temp/.cer
...
----- Error chain -----
Chain status:IS_UNTRUSTED_ROOT
Revocation reason:unspecified
1.
Subject:'E=uc@mil.ru, OGRN=1037700255284, INN=007704252261, C=RU, S=77 . , L=, STREET=. .19, OU=4 () 31659,
O= , CN= '
Issuer:'E=dit@minsvyaz.ru, C=RU, S=77 , L=. , STREET=" , 7", O= , OGRN=1047702026701, INN=007710474375, CN= '
Cert status:IS_UNTRUSTED_ROOT
...
```



CP_PRINT_CHAIN_DETAIL=1 -->

В нашем примере, из логов можно сделать вывод, что нам надо установить сертификат УЦ МО с CN=Министерство обороны Российской Федерации:

```
/opt/cproscsp/bin/amd64/certmgr -inst -store uRoot -file minoboron-root-2018.crt
```

Для того, чтобы убедиться в устранении ошибки, можно повторно в режиме отладки запустить команду. При правильно установленной цепочке сертификатов, статус у сертификата будет = CERT_TRUST_NO_ERROR

```
....
Subject:'E=uc@mil.ru, OGRN=1037700255284, INN=007704252261, C=RU, S=77 . , L=, STREET=. .19, OU=4 ( ) 31659,
O= , CN= '
Issuer:'E=dit@minsvyaz.ru, C=RU, S=77 , L=. , STREET=" , 7", O= , OGRN=1047702026701, INN=007710474375, CN= '
Cert status:CERT_TRUST_NO_ERROR
...
.
.
[ErrorCode: 0x00000000]
```

Подписание документа ЭЦП

Подпись можно делать двумя способами:

* attached (присоединённая), тогда результирующий файл - это CMS-сообщение, внутри которого упакованы данные и атрибуты (типа подписи). Формат сообщения соответствует международному стандарту, поэтому извлекать данные оттуда можно любыми утилитами, типа `cryptcp / csptest / openssl / certutil` (на windows).

* detached (отсоединённая), тогда результирующий файл - это CMS-сообщение БЕЗ исходных данных, но с атрибутами (типа подписи). В этом случае для проверки надо "принести" исходный файл. Разумеется он остаётся неизменным и его можно смотреть `cat-ом`



Про CMS-сообщения, есть хорошая статья на [Хабре](#)

Подпись файлов (присоединённая)

```
/opt/cproesp/bin/amd64/cryptcp -sign -dn'CN=_' -der zayavlenie.pdf
CryptCP 5.0 (c) "-", 2002-2018.
.
:
:" ""-
""", , 77 .
, RU, . 26, mail@rusbitech.ru

02.10.2018 14:31:02 02.10.2019 14:41:02

./':
raport.pdf... ...

[ErrorCode: 0x00000000]
```

Подпись файлов(отсоединённая)

```
/opt/cproccsp/bin/amd64/cryptcp -sign -detach -dn 'CN=___' -pin 12345678 raport.pdf raport.pdf.sig

CryptCP 5.0 (c) "-", 2002-2018.

.

: " ""-
""", , 77 .
, RU, . 26, mail@rusbitech.ru

02.10.2018 14:31:02 02.10.2019 14:41:02

.
'./':
raport.pdf... ...

[ErrorCode: 0x00000000]
```

Проверка подписи в файле

Для прикрепленной подписи

Для проверки прикрепленной подписи выполните:

```
/opt/cproccsp/bin/amd64/cryptcp -verify raport.pdf.sig
CryptCP 5.0 (c) "-", 2002-2018.

.

: 4
.
'./':
raport.pdf.sig ... ...

: " ""-
""", , 77 .
, RU, . 26, mail@rusbitech.ru
02.10.2018 14:31:02 02.10.2019 14:41:02
02.10.2018 14:31:02 02.10.2019 14:41:02

.

[ErrorCode: 0x00000000]
```

естественный

использовать ключ -verall - он понимает, что надо найти всех подписавших и ищет в том числе в сообщении:

```
/opt/cprosp/bin/amd64/cryptcp -verify -verall -detached /home/shuhrat/smolensk/raport.pdf raport.pdf.sig
CryptCP 5.0 (c) "-", 2002-2018.

.
' /home/shuhrat/smolensk/':
/home/shuhrat/smolensk/raport.pdf... ...

: " ""-
""", , 77 .
, RU, . 26, mail@rusbitech.ru
02.10.2018 14:31:02 02.10.2019 14:41:02
02.10.2018 14:31:02 02.10.2019 14:41:02

.
'./':
raport.pdf... ...

[ErrorCode: 0x00000000]
```

обучающий

указать в качестве хранилища сертификатов само сообщение (ключ -f):

```
/opt/cprosp/bin/amd64/cryptcp -verify -f raport.pdf.sig -detached raport.pdf raport.pdf.sig
CryptCP 5.0 (c) "-", 2002-2018.

.

:
: " ""-
""", , 77 .
, RU, . 26, mail@rusbitech.ru
02.10.2018 14:31:02 02.10.2019 14:41:02

.
'./':
raport.pdf... ...

: " ""-
""", , 77 .
, RU, . 26, mail@rusbitech.ru
02.10.2018 14:31:02 02.10.2019 14:41:02

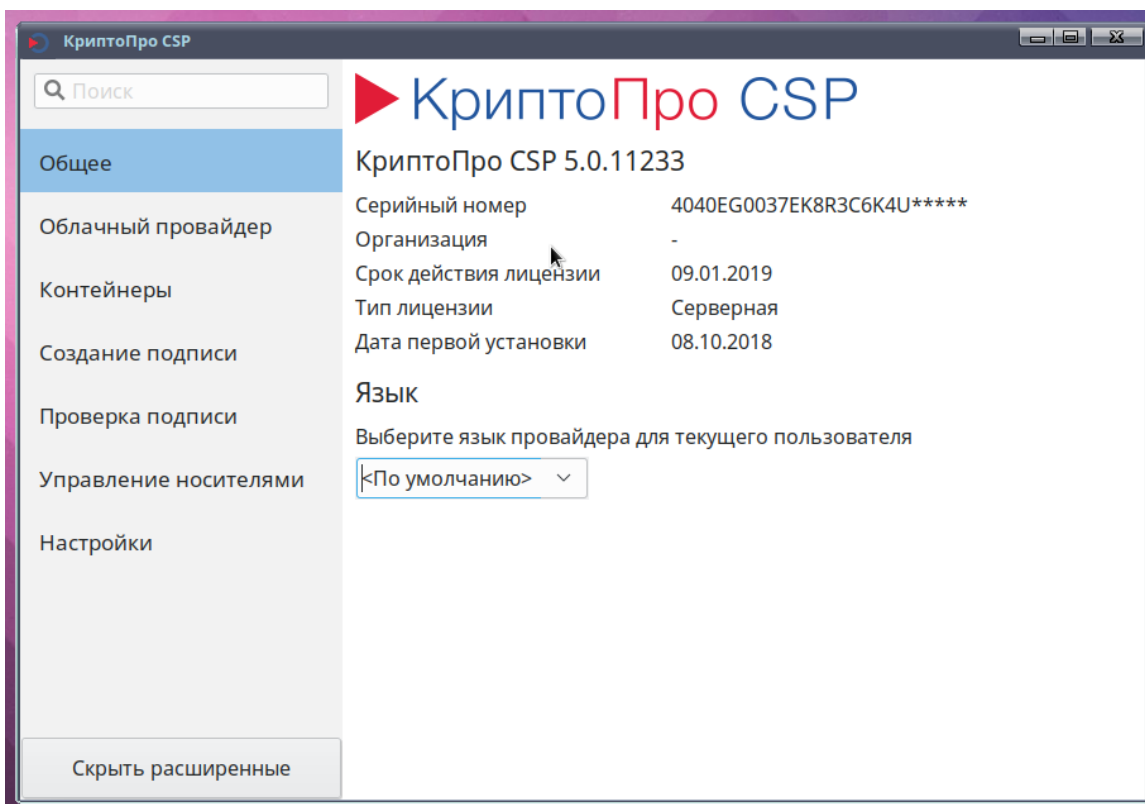
.
[ErrorCode: 0x00000000]
```

Извлечение подписанного файла

Чтобы извлечь файл, необходимо указать его имя в конце команды проверки подписи:

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

Графический интерфейс КриптоПро CSP v. 5.0 (cptools)



В версии КриптоПРО 5 появилась графическая утилита для работы с сертификатами - cptools.

её можно запустить из консоли:

```
$ cptools
```

либо

```
$ /opt/cproscsp/bin/amd64/cptools
```

Удаление КриптоПро CSP

Для того, чтобы удалить ПО КриптоПро CSP, в терминале FLY следует ввести команду:

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

Отключение окон о необходимости перехода на ГОСТ Р 34.10-2012

В соответствии с принятым в 2014 году [порядком перехода на ГОСТ Р 34.10-2012](#) до 1 января 2019 года попытка использования ГОСТ Р 34.10-2001 (кроме проверки подписи) на всех выпущенных к настоящему моменту сертифицированных версиях КриптоПро CSP 3.9, 4.0 и КриптоПро JCP 2.0 с 1 января 2019 года вызовет ошибку/предупреждение (в зависимости от продукта и режима работы), которые могут привести к неработоспособности автоматических /автоматизированных систем при использовании ими ключей ГОСТ Р 34.10-2001. В случае если ваша система использует ключи ГОСТ Р 34.10-2001, просим принять во внимание инструкцию.

Для отключения данных предупреждений в КриптоПро CSP, нужно добавить два ключа в конфигурационный файл `/etc/opt/cproscsp/config64.ini` в существующую секцию **Parameters**:

[Parameters]

#Параметрыпровайдера

warning_time_gen_2001=ll:9223372036854775807

warning_time_sign_2001=ll:9223372036854775807



На данный момент завершается сертификация обновленной версии КриптоПро CSP 4.0 R4. Для наиболее безболезненного продолжения работы с ГОСТ Р 34.10-2001 в 2019 году мы рекомендуем обновиться до этой версии. В более ранних версиях КриптоПро CSP, а также Клиент HSM 2.0 присутствуют технические ограничения формирования подписи по ГОСТ Р 34.10-2001 после 1 января 2019 года в виде соответствующих предупреждающих окон.

Полезные ссылки

КриптоПро: IFCP plugin для входа ЕСИА (Госуслуги)

[КриптоПро: IFCP plugin для входа ЕСИА \(Госуслуги\)](#)

КриптоПро CADES ЭЦП Browser plug-in

[КриптоПро CADES ЭЦП Browser plug-in](#)

Таблица поддерживаемых устройств Крипто-Про CSP

На официальном сайте СКЗИ КриптоПро в таблице указаны носители, продемонстрировавшие работоспособность с соответствующими версиями КриптоПро CSP:

<https://www.cryptopro.ru/products/csp/compare>

База знаний КриптоПро

<https://support.cryptopro.ru/index.php?/Knowledgebase/List>

Обсуждение КриптоПро CSP на форуме astralinux

<https://forum.astralinux.ru/threads/419/>

Chromium+КриптоПРО

<https://www.cryptopro.ru/news/2018/12/zashchishchennyi-brauzer-dlya-gosudarstvennykh-elektronnykh-ploshchadok-teper-i-na-linu>

<https://astralinux.ru/news/category-news/2018/brauzeryi-%C2%ABastra-linux-special-edition%C2%BB-adaptirovani-dlya-raboty/>

Список ГИС и ЭТП использующих cades-bes plugin

ЭЦП в государственных информационных системах и электронно торговых площадках

Перечень аккредитованных удостоверяющих центров

<https://e-trust.gosuslugi.ru/CA/>

Диагностический архив для обращения в тех. поддержку

По всем вопросам установки СКЗИ в операционную систему, их настройки и обеспечения доступа к электронным ресурсам в сети Интернет можно обращаться в техническую поддержку [Astra Linux](#) и [КриптоПро](#).

Для создания диагностического архива, можно воспользоваться следующей командой:

```
sudo curl http://cryptopro.ru/sites/default/files/products/csp/cprodiag 2>/dev/null|sudo perl
```

В результате должен получиться cprodiag_день_месяц_год.tar.gz архив, который следует прислать в техническую поддержку [Astra Linux](#) и [КриптоПро](#).