CSP

CSP

CSP :

- , () 34.10-2001 / 34.10-2012 (34.11-94 / 34.11-2012);
- , 28147-89;
- , TLS;
- ;
- .

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

CSP :

- CSP 4.0 R4;
- CSP 5.0;

1-Base 2-Base.

CSP 2-Base - ().

, , - . , BIOS , , BIOS.

CSP.

CSP

(CSP) c www.cryptopro.ru, .

Astra Linux CSP 4 - 64 .

CSP 3 , .

«» «4.0 R4». :

1) «». : «linux-amd64_deb.tgz»;

2) " Fly" (alt+T);

3) :

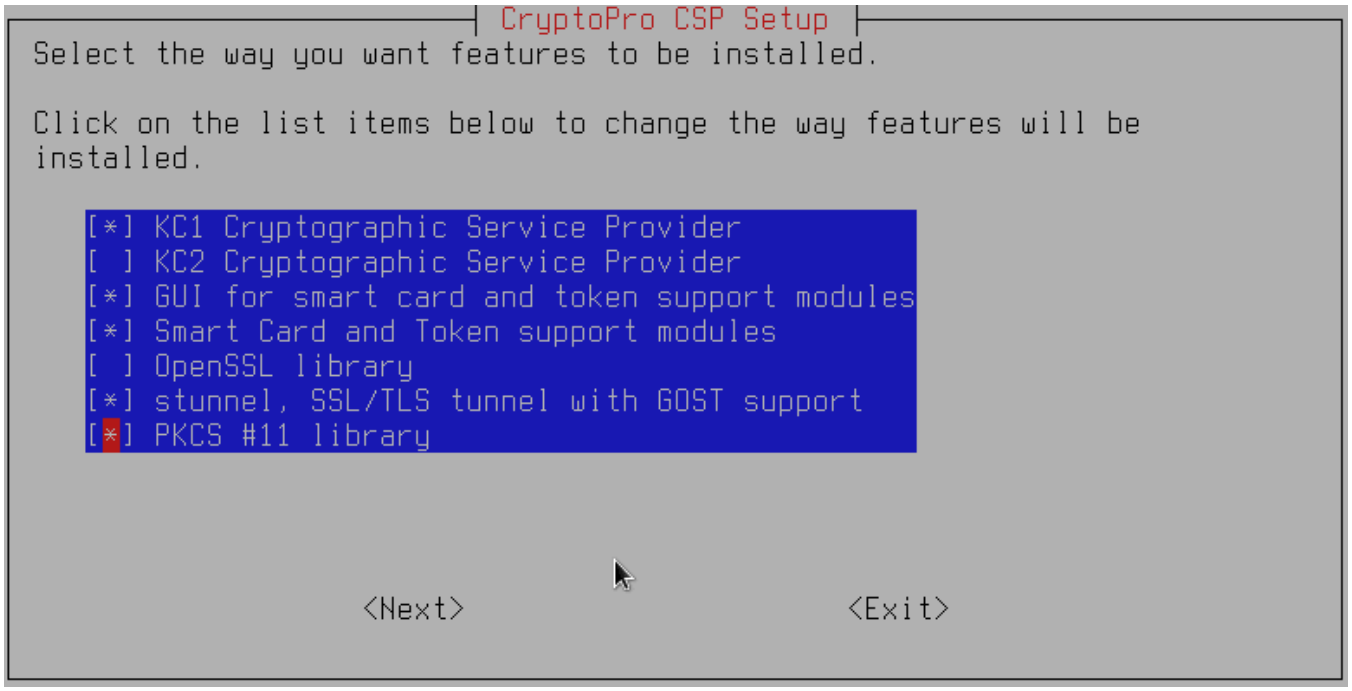
```
tar -zxf linux-amd64_deb.tgz
```

5) :

```
cd linux-amd64_deb
```

6) "install.sh" "instal_gui.sh" :

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



* , .

:	
cprocsp-curl	libcurl
lsb-cprocsp-base	CSP
lsb-cprocsp-capilite	CAPILite
lsb-cprocsp-kc1	KC1
lsb-cprocsp-rdr	RNG
:	
cprocsp-rdr-gui-gtk	
cprocsp-rdr-rutoken	
cprocsp-rdr-jacarta	JaCarta
cprocsp-rdr-pcsc	PC/SC CSP
lsb-cprocsp-pkcs11	PKCS11

CSP :

```
dpkg -l | grep cprocsp
```

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

, CSP, FLY :

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

/- :

libccid, libgost-astra , pcscd

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

:

- : https://www.rutoken.ru/support/download/nix/
- : https://www.aladdin-rd.ru/support/downloads/jacarta

pcscd:

```
sudo service pcscd restart
```

4.0 R4 , - .

Astra Linux SE.

, :

- **astra-digsig-oldkeys;**
- Astra Linux SE /etc/digsig/keys/legacy/cryptopro;
- :

  ```
  sudo update-initramfs -uk all
  ```

- .

. Astra Linux Special Edition:

:

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

```
root@smakhmadiev:/# /opt/cprocsp/sbin/amd64/cpconfig -license -view
License validity:
4040E-G0037-EK8R3-C6K4U-HCXQG
Expires: 2 month(s) 17 day(s)
License type: Server.
```

:

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

:

```
/opt/cprocsp/sbin/amd64/cpconfig -hardware reader -view
```

```
shuhrat@astralinux:~$ cpconfig -hardware reader -view

Nick name: CLOUD
Connect name:
Reader name: Cloud Token

Nick name: Aktiv Rutoken lite 00 00
Connect name:
Reader name: Aktiv Rutoken lite 00 00

Nick name: AKS ifdh [Main Interface] 00 00
Connect name:
Reader name: AKS ifdh [Main Interface] 00 00
```

, :

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

:

```
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]
```

:

```
/opt/cprocsp/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                        |SCARD\rutoken_ecp_390a75ab\0A00\8AC7
Shuhrat                         |SCARD\rutoken_ecp_390a75ab\0B00\5228
Shuhrat                         |HDIMAGE\\Shuhrat.000\5228
TestCont123                     |HDIMAGE\\TestCont.000\7760
OK.
Total: SYS: 0,010 sec USR: 0,080 sec UTC: 0,240 sec
[ErrorCode: 0x00000000]
```

FQCN, :

```
/opt/cprocsp/bin/amd64/csptest -keyset -enum_cont -fqcn -verifyc | iconv -f
cp1251
```

:

```
root@smakhmadiev:/home/shuhrat/ecp# /opt/cprocsp/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]
```

\\.\HDIMAGE - , \\.\HDIMAGE\TestCont123 - , \\.\Aktiv Rutoken ECP 00 00 - ().

" "

:

```
/opt/cprocsp/bin/amd64/csptestf -keyset -container '' -info
```

:

```
/opt/cprocsp/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 (  34.11-2012 256 )
  KP_DHOID:
    1.2.643.2.2.35.1 (  34.10 256 ,   )
  KP_SIGNATUREOID:
    1.2.643.2.2.35.1 (  34.10 256 ,   )
  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 (  34.11-2012 256 )
  KP_DHOID:
    1.2.643.2.2.36.0 (  34.10 256 ,    )
  KP_SIGNATUREOID:
    1.2.643.2.2.36.0 (  34.10 256 ,    )
  Permissions:
    CRYPT_READ
    CRYPT_WRITE
    CRYPT_IMPORT_KEY
    0x800
    0x10000
    0x20000
    0x100000
KP_CERTIFICATE:
Subject: INN=007814508921, E=user@astralinux.ru, C=RU, CN= , SN=
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]
```

. :

```
/opt/cprocsp/bin/amd64/csptest -keys -enum -verifyc -fqcn -un
```


PIN- :

- (, ,), PIN , , - . : PIN.
- (HDIMAGE), PIN-. : , PIN- HDIAMGE .

( ), :

```
/opt/cprocsp/bin/amd64/csptestf -keyset -container  -check
```

:

```
/opt/cprocsp/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]

:

```
/opt/cprocsp/bin/amd64/csptestf -passwd -cont '\\.\Aktiv Rutoken ECP 00
00\TestCont' -deletek
```

:

```
csptestf -keycopy -contsrc '\\.\HDIMAGE\_' -contdest '\\.\Aktiv Rutoken ECP 00
00\_'
```

( )

```
/opt/cprocsp/bin/amd64/csptestf -passwd -cont '\\.\Aktiv Rutoken ECP 00
00\TestContainer' -change '_' -passwd '_
```

⚠ , PIN, :

```
/opt/cprocsp/bin/amd64/csptestf -passwd -cont '\\.\Aktiv Rutoken ECP 00
00\TestContainer' -change '__'
```

Linux

:

- (umy, u = User, my -). , , (,). , , ;
- - , . (uroot, mroot, m = Machine, read only root-);
- - , (" " -> " " -> " "). (uca, mca). (CRL). (CRL) , ucache. .
- , . umy (,), uAddressBook;

, :

uMy :

```
/opt/cprocsp/bin/amd64/csptestf -absorb -certs -autoprov
```

uMy:

```
/opt/cprocsp/bin/amd64/certmgr -inst -cont '\\.\Aktiv Rutoken ECP 00 00\Ivanov'
```

mRoot:

```
wget https://structure.mil.ru/download/doc/morf/military/files/ca2020.cer -O -
| sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mRoot -stdin
```

(CRL), mca:

```
wget https://structure.mil.ru/download/doc/morf/military/files/crl_20.crl -O -
| sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mca -stdin -crl
```

-pattern >>> 'rutoken' .

, CRL , , , . -stdin -file . :

1. :

```
wget https://structure.mil.ru/download/doc/morf/military/files
/ca2020.cer
wget https://structure.mil.ru/download/doc/morf/military/files
/crl_20.crl
```

2. ;
3. :

```
sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mRoot -file ca2020.
cer
sudo /opt/cprocsp/bin/amd64/certmgr -inst -store mca -file crl_20.
crl -crl
```

1) certmgr, cryptcp : -mroot -uAddressBook

2) uca, mca:

3) -pattern < '' > uMy. :

```
/opt/cprocsp/bin/amd64/csptestf -absorb -cert -pattern ''
```

4) , , **-file :**

```
certmgr -inst -file cert.cer -store uMy
```

5) /var/opt/cprocsp/users

:

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

```
shuhrat@smakhmadiev:/opt/cprocsp/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              : 0x2B6E3351FD6EB2AD48200203CB5BA141
SHA1 Hash           : 046255290b0eb1cdd1797d9ab8c81f699e3687f3
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=dit@minsvyaz.ru, C=RU, S=77 г. Москва, L=Москва, STREET="125375 г. Москва, ул. Тверская,
ной удостоверяющий центр
Subject             : E=uc@mil.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              : 0x00D100F4F5000000000309
SHA1 Hash           : 3bfd61fadc08931dbbc53f79bbd051aa4c4d3f03
SubjKeyID           : a21c01faf8e344ceb999ba8cd192f4ea1a8fd5c9
Signature Algorithm : ГОСТ Р 34.11/34.10-2001
PublicKey Algorithm : ГОСТ Р 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@mil.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              : 0x7CA5D4F7000000000D0
SHA1 Hash           : c7588c3365f0ed78be0dcff22aa33074f11d8b95
SubjKeyID           : 4ab7c589e2d91df0ec01225b7e6841dbee8bc33e
```

:

```
/opt/cprocsp/bin/amd64/certmgr -delete
```

.

:

```
/opt/cprocsp/bin/amd64/certmgr -del -all
```

/var/opt/cprocsp/keys.

: .

:

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

, :

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

, :

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

, :

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

: , :

```
/opt/cprocsp/bin/amd64/cryptcp -copycert -dn 'CN=__' -df  /temp/.cer
```

: CN, E, SN, OGRN, SNILS .

```
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])?
```

, . debug():

```
$ CP_PRINT_CHAIN_DETAIL=1 /opt/cprocsp/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 -->

, , CN= :

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

, , . , = 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]
```

:

* attached (), - CMS-, ( ). , , cryptcp / csptest / openssl / certutil (windows).

* detached (), - CMS- , ( ). "" . cat-

> ⚠ CMS-,

()

```
/opt/cprocsp/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]
```

()

```
/opt/cprocsp/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]
```

:

```
/opt/cprocsp/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]
```

-verall, , , :

```
/opt/cprocsp/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]
```

(-f):

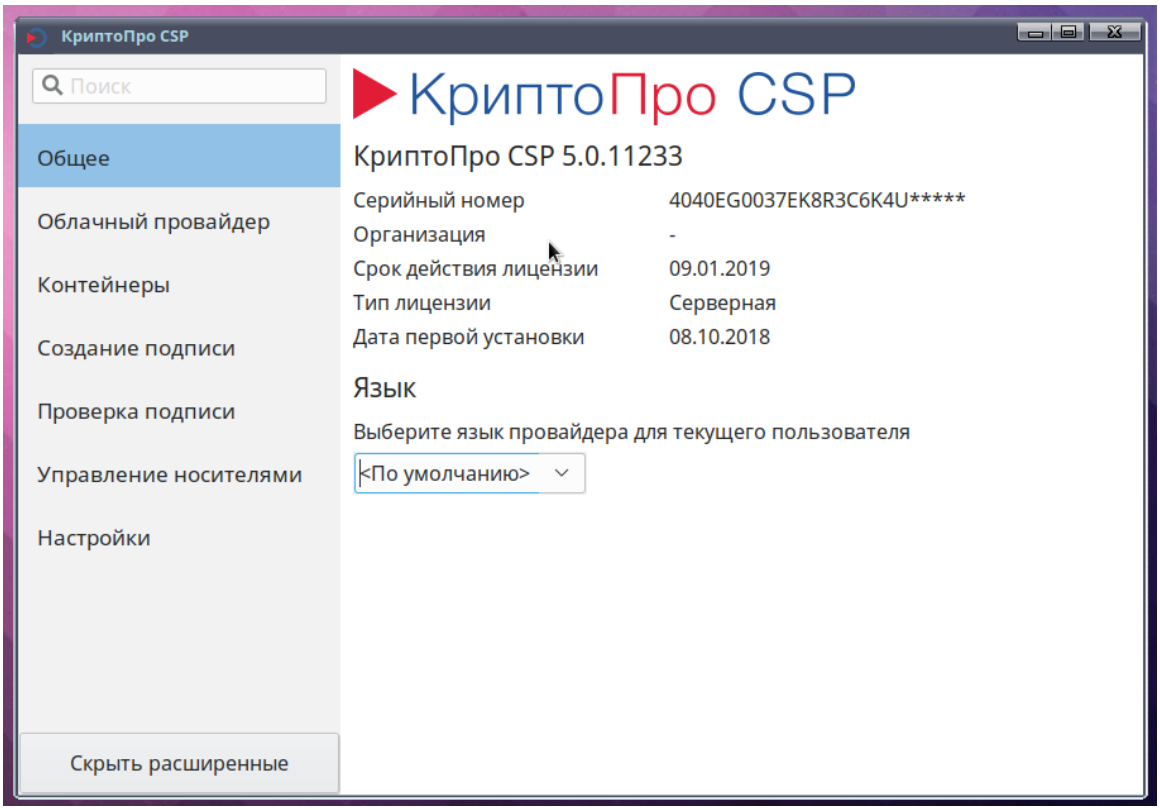
```
/opt/cprocsp/bin/amd64/cryptcp -verify -f raport.pdf.sig -detached raport.pdf
raport.pdf.sig
```

```
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]
```

, :

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

CSP v. 5.0 (cptools)



5 - cptools.

:

```
cptools
```

```
/opt/cprocsp/bin/amd64/cptools
```

CSP

, CSP, FLY 3 :

```
sudo rm -rf /opt/cprocsp
sudo rm -rf /var/opt/cprocsp/
sudo rm -rf /etc/opt/cprocsp/
```

34.10-2012

2014 34.10-2012 1 2019 34.10-2001 ( ) CSP 3.9, 4.0 JCP 2.0 1 2019 / ( ), / 34.10-2001. 34.10-2001, .

CSP, **/etc/opt/cprocsp/config64.ini** **Parameters**:

```
[Parameters]
#
warning_time_gen_2001=ll:9223372036854775807
warning_time_sign_2001=ll:9223372036854775807
```

⚠ CSP 4.0 R4. 34.10-2001 2019 . CSP, HSM 2.0 34.10-2001 1 2019 .

: IFCP plugin ()

: IFCP plugin ()

CADES Browser plug-in

CADES Browser plug-in

- CSP

, CSP:

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

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

CSP astralinux

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

Chromium+

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-adaptirovanyi-dlya-rabotyi/

cades-bes plugin

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

.

, Astra Linux .

, :

sudo /opt/cprocsp/bin/amd64/curl http://cryptopro.ru/sites/default/files/products/csp/cprodiag 2>/dev/null|sudo perl

cprodiag___.tar.gz , Astra Linux .