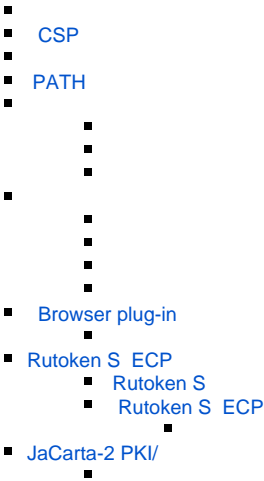


# CSP Astra Linux Common Edition



:

- Astra Linux Common Edition 2.12.42

CSP :

1. (, ):

```
sudo apt update
sudo apt dist-upgrade
```

2. libmicrohttpd12:

```
sudo apt install libmicrohttpd12
```

## CSP

CSP . CSP, «».

:

1. :

```
pushd `mktemp -d`
```

2. : <https://www.eos.ru/upload/karma/karma560219.zip> :

```
sudo apt install ca-certificates
wget https://www.eos.ru/upload/karma/karma560219.zip
```



3. :

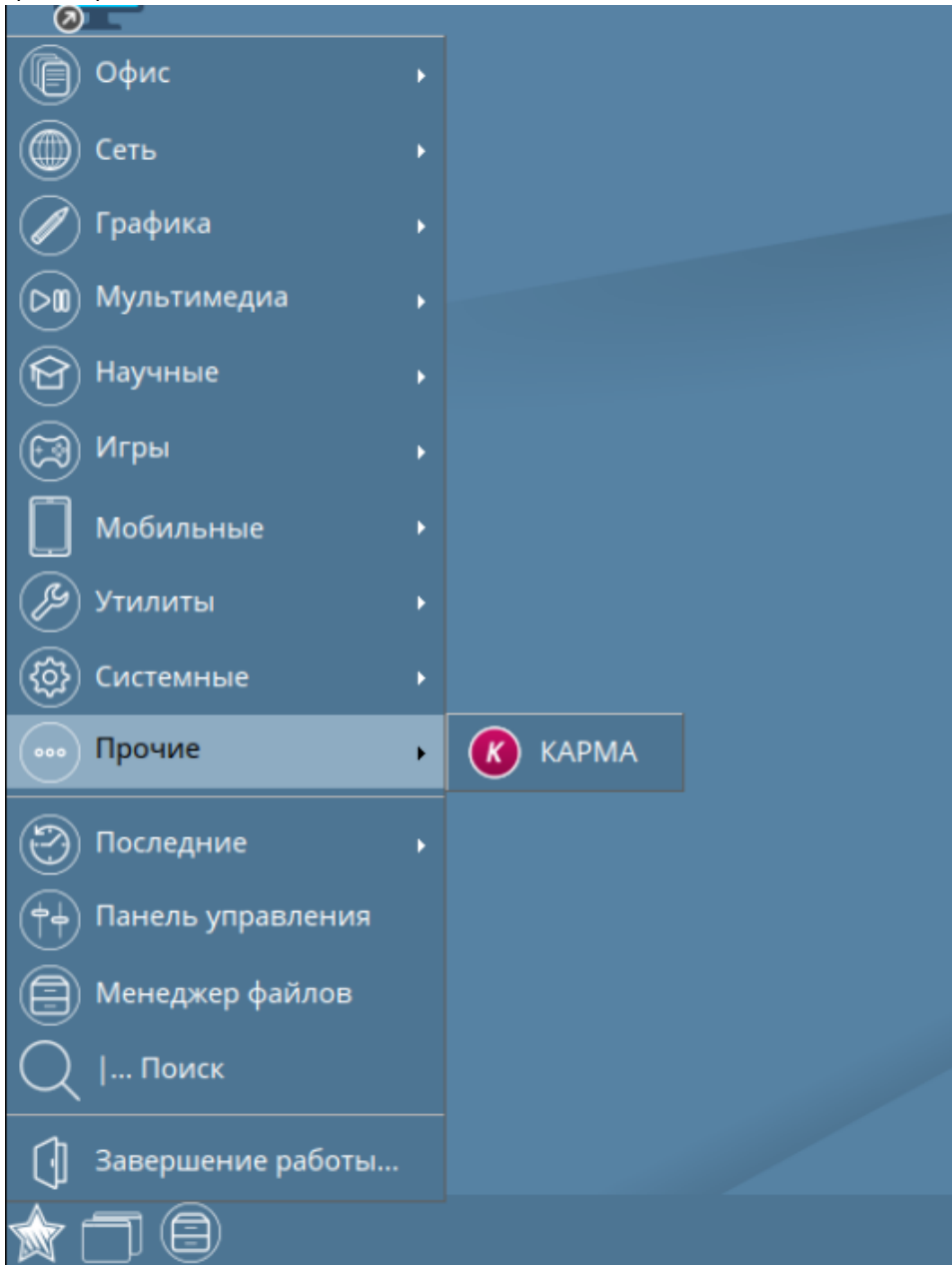
```
unzip karma*.zip
```

4. :

```
sudo dpkg -i Linux/carma-common_*-astra_amd64.deb Linux/carma-dev_*-astra_amd64.deb Linux/carma-capilite_*-astra_amd64.deb
```

5. , .

6. : — .



## PATH

:

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



, PATH .

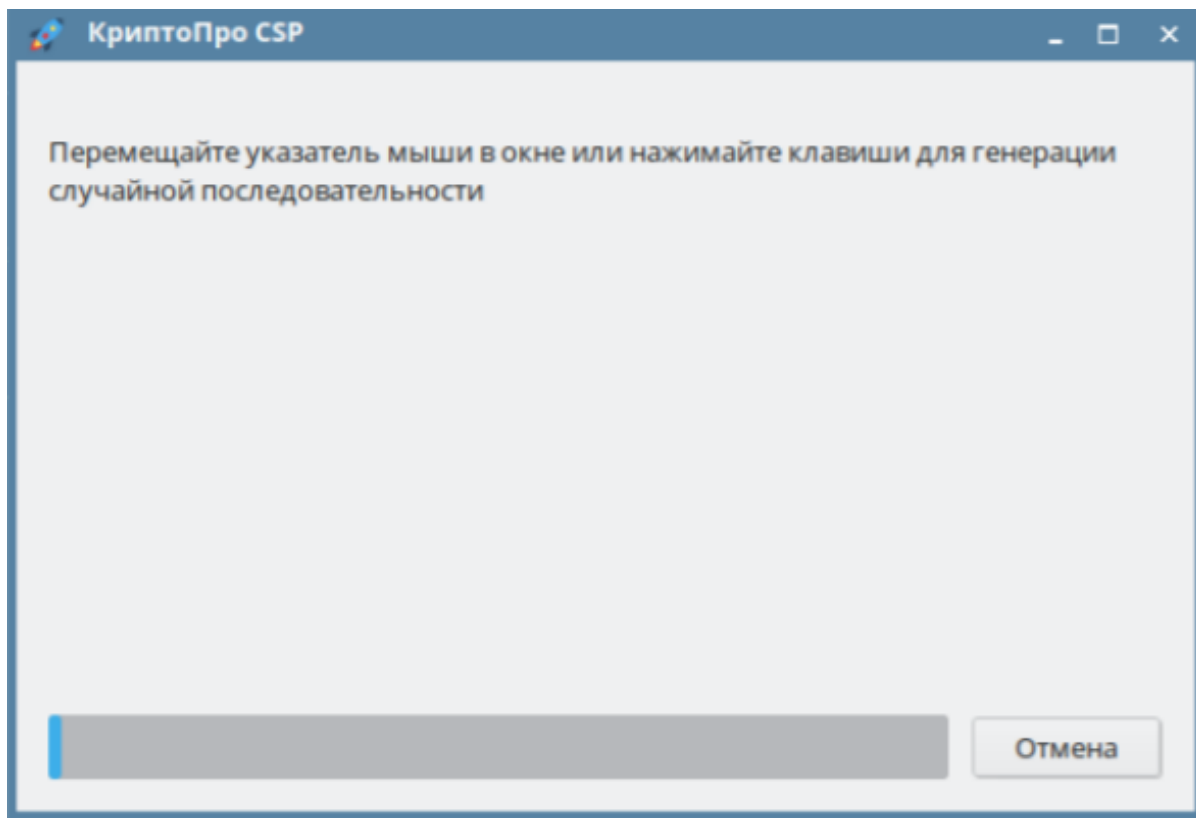
C . HDIMAGE:

```
sudo -E cpconfig -hardware reader -add HDIMAGE store
```

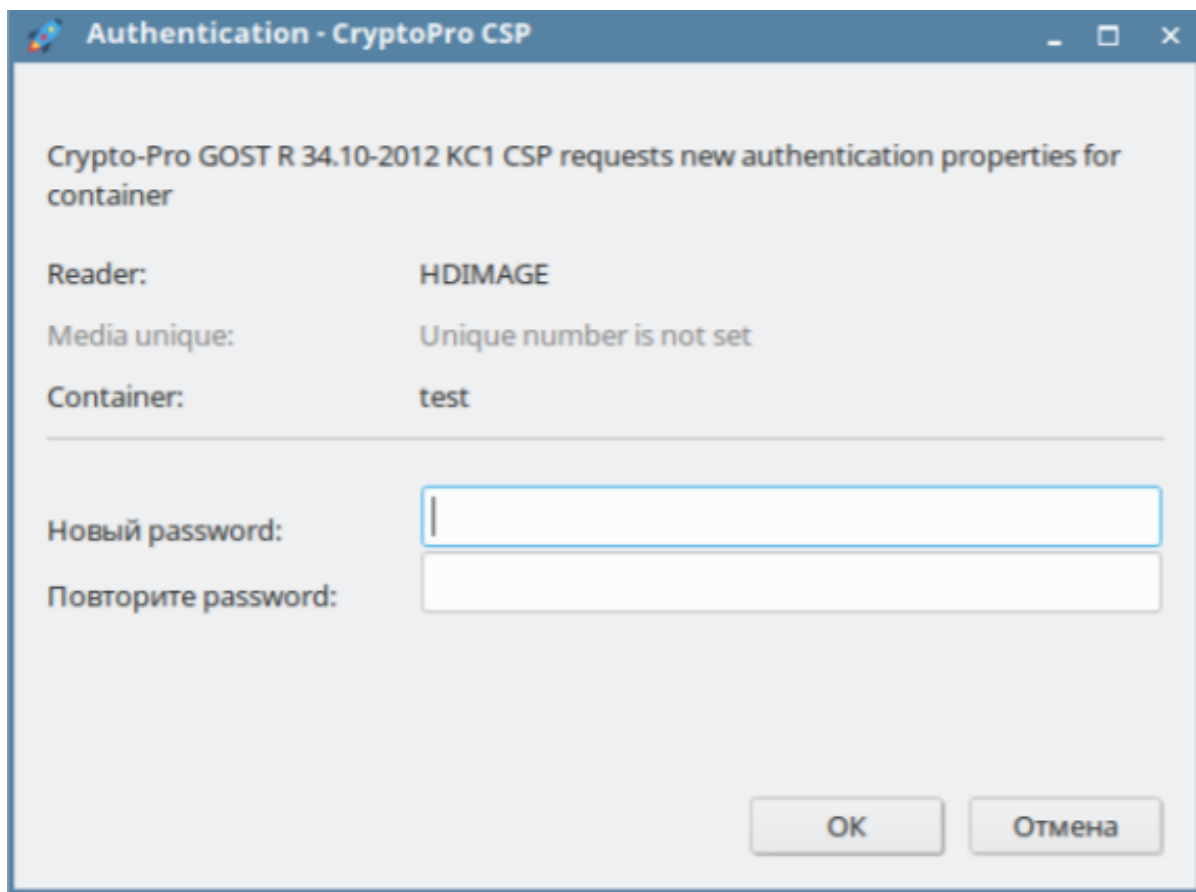
test HDIMAGE:

```
csptest -keyset -provtype 80 -newkeyset -cont '\\.\HDIMAGE\test'
```

:



:



, OK .

:

```
csptest -keyset -enum_containers -fqcn -verifycontext -unique
```

```
u@astra:~$
u@astra:~$
u@astra:~$
u@astra:~$ csptest -keyset -enum_containers -fqcn -verifycontext -unique
CSP (Type:00) v5.0.10000 KC1 Release Ver:5.0.12000 OS:Linux CPU:AMD64 FastCode:READY:AVX. DISABLED:RSA;
AcquireContext: OK. HCRYPTPROV: 15266531
\\.\HDIMAGE\test |\\.\HDIMAGE\HDIMAGE\test.000\2EF8
OK.
Total: SYS: 0,000 sec USR: 0,060 sec UTC: 0,080 sec
[ErrorCode: 0x00000000]
u@astra:~$
```

test:



!

```
csptest -keyset -deletekeyset -cont '\\.\HDIMAGE\test'
```

```
cryptcp -creatrgst -dn "cn=test,e=test@eos.ru" -provtype 80 -nokeygen -cont '\\.\HDIMAGE\test' -certusage "1.3.6.1.5.5.7.3.4,1.3.6.1.4.1.311.10.3.12" eos.req
```

```

• cn= test ,e= test@ eos.ru —, Subject :
• CN— (), —;
• E(email)— ();
• \\.\HDIMAGE\test — ;
• eos.req —, ( eos —*.req);
• -certusage —, , , ,—OID. , , , :
    ◦ 1.3.6.1.5.5.7.3.1—;
    ◦ 1.3.6.1.5.5.7.3.2—;
    ◦ 1.3.6.1.5.5.7.3.3—;
    ◦ 1.3.6.1.5.5.7.3.4—;
    ◦ 1.3.6.1.5.5.7.3.8—;
    ◦ 1.3.6.1.4.1.311.10.5.1—;
    ◦ 1.3.6.1.4.1.311.10.3.12— .

```

: <https://www.cryptopro.ru/certsrv/certrqxt.asp>.

$$, \quad *.req, \quad - eos.req.$$


-----BEGIN NEW CERTIFICATE REQUEST-----

-----END NEW CERTIFICATE REQUEST-----

## Выдача запроса на сертификат или на обновление сертификата

Чтобы выдать сохраненный запрос к ЦС, вставьте base-64-шифрованный запрос сертификата PKCS #10 или запрос обновления PKCS #7, созданный в внешнем источнике (например, веб-сервером) в поле "Сохраненный запрос".

Сохраненный запрос:

Base-64-шифрованный  
запрос сертификата  
(CMC или  
PKCS #10 или  
PKCS #7):

MIIBLzCB3QIBADAeQwCwYDQoQDAR0ZGN0MR0wGAYJKoZIhvcNAQkBFggT0XN0Q  
 OGVCy5ydTBMbM8CGCqFAwBAQEABMBMGZ0ZG9iAAEJAAGCCqFwBAQIAEABEABE  
 AQAQIBwHwrcwrmBq9r8DB0S5aZqdtIIL0sKFfboA1Iwz1VnaV6QkYJC59mm1t  
 8trA16VtZ2vxtc24ebk0EmWqQYKKYwBBYBAGN0IBDjZEMdeWHvYDVR01BBGwGyI  
 KuYBBQUXAwGCCISGAQqBgqjCAwMMYDVR0PAAQhBAQDAgTMAwGCCCFwBAQIAEABE  
 A0EAjawnEXZfY/Lk1LMN1MwAXCFODfsvIEatprtnt0u0C10fchgsFBBJcd5Pr7by  
 ocNuxbH0rQyBAewku+/Surteg=

**Дополнительные атрибуты:**

Атрибуты:

[illegible]

Выдать >

, ( certnew.p7b).

Browser plugin, , (. [Browser plug-in](#)).

<https://www.cryptopro.ru/certsrv/certcarc.asp> (certcrl.crl):

## CRL.

certnew.p7b- . \\.\\HDIMAGE\\test .



, certnew.p7b , . , .

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

1 2, 2.

:

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

1 2, 1, .

(crl)



, certcrl.crl , :

```
certmgr -inst -crl -file certcrl.crl -store CA
```

:

```
certmgr -list
```

## Browser plug-in

Browser plug-in : <https://www.cryptopro.ru/products/cades/plugin> .

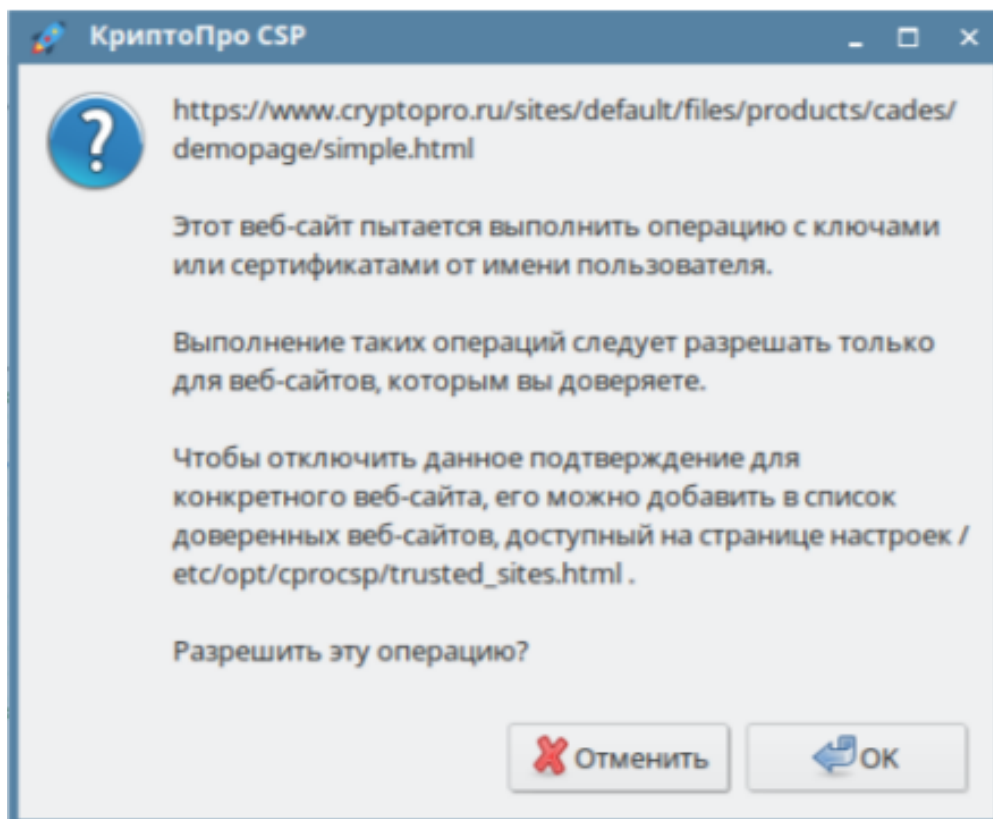
cares\_linux\_amd64.tar.gz cares\_linux\_amd64:

```
tar -xvf cares_linux_amd64.tar.gz  
cd /home/<_>/cares_linux_amd64
```

deb- cares\_linux\_amd64:

```
sudo dpkg -i *.deb
```

[https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades\\_bes\\_sample.html](https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html).



## Rutoken S ECP

Rutoken S ECP :

```
sudo apt install opensc pcscd
```

<http://www.rutoken.ru/support/download/drivers-for-nix/> Rutoken S — S GNU/Linux DEB 64-bit (x64).

## Rutoken S

Rutoken S :

```
sudo dpkg -i ifd-rutokens_1.0.4_amd64.deb
```

## Rutoken S ECP

 S ECP , S.

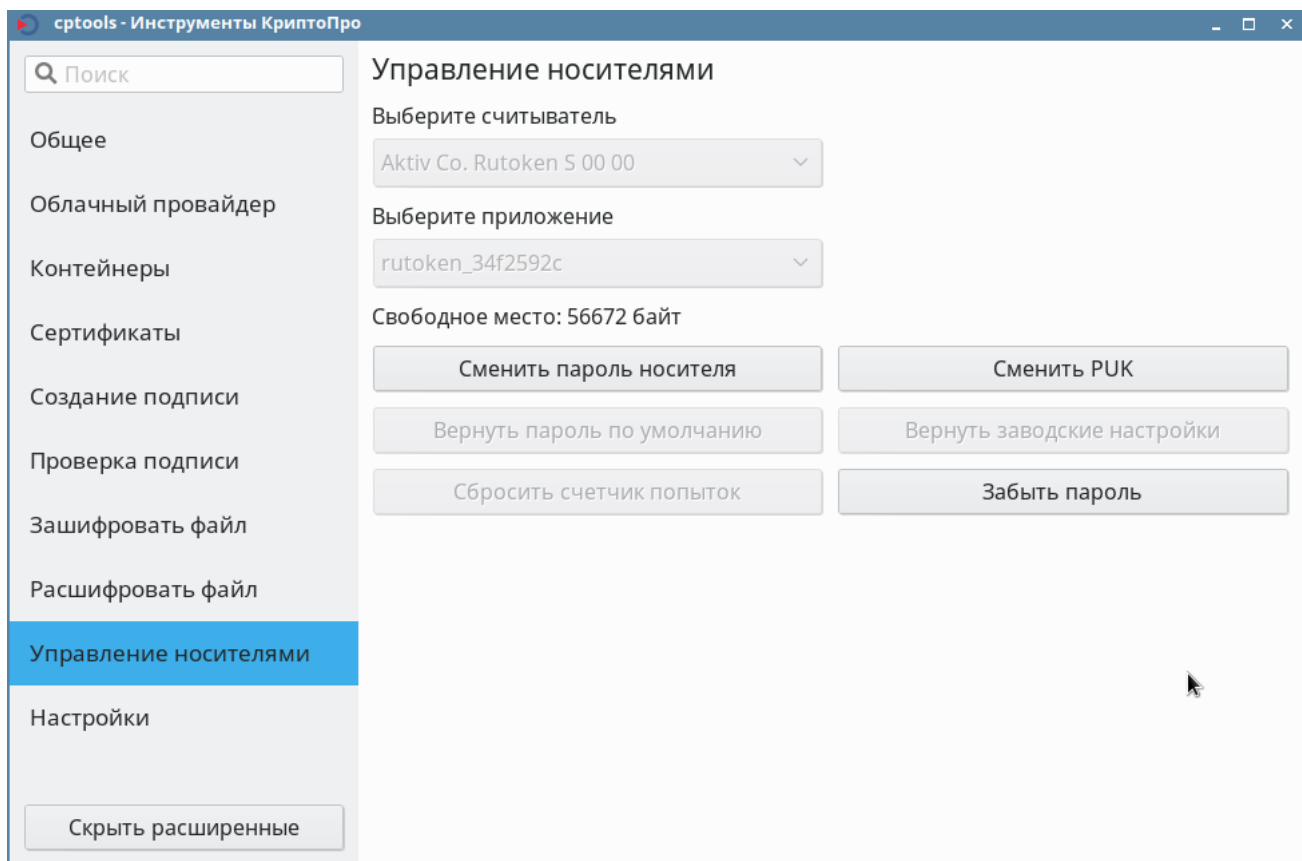
Rutoken S USB , , :

```
list_pcsc
```

```
ERROR: ScardListReaders(NULL) pcscd:
```

```
sudo service pcscd restart
```

— — — — .



eos Rutoken S:

```
csptest -keyset -provtype 80 -newkeyset -cont '\\.\Aktiv Co. Rutoken S 00 00\eos'
```

Aktiv Co. Rutoken S 00 00 — USB.

pin- ( —12345678), **OK**.

:

```
cryptcp -creatrgst -dn "cn=test ,e=test@eos.ru" -provtype 80 -nokeygen -  
cont '\\.\Aktiv Co. Rutoken S 00 00\eos' -certusage  
"1.3.6.1.5.5.7.3.4,1.3.6.1.4.1.311.10.3.12" test.req
```




test.req.

Browser plugin, .

certnew.p7b Rutoken S:




```
certmgr -inst -file certnew.p7b -store uMy -cont '\\.\Aktiv Co. Rutoken S  
00 00\eos' -inst_to_cont
```

 , certnew.p7b , .

2.

Rutoken S «Crypto Pro» , CryptoPro :

```
csptestf -absorb -cert -pattern 'rutoken'
```

 , ( . ) .

## JaCarta-2 PKI/

linux-amd64\_deb:

```
cd /home/<_>/linux-amd64_deb
```

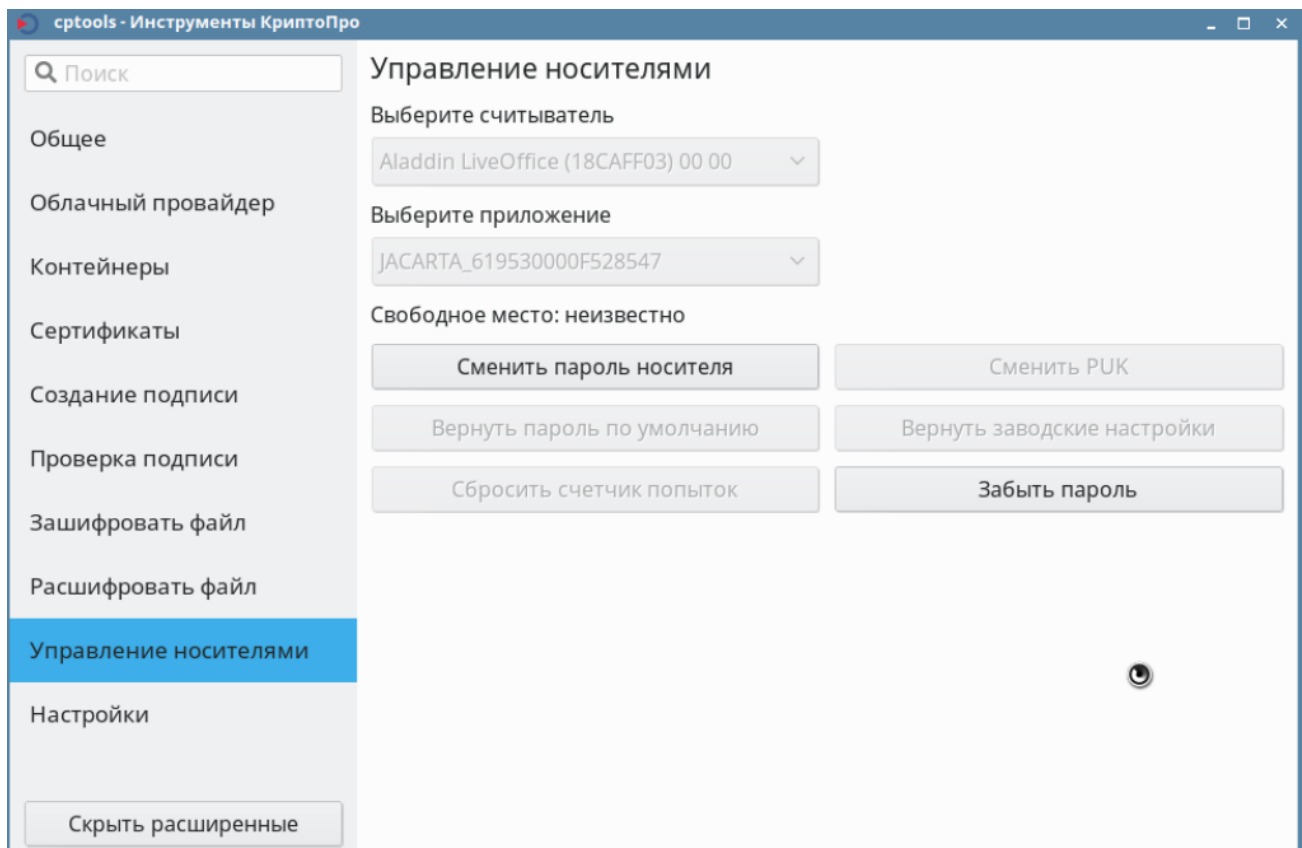
jaCarta:

```
sudo dpkg -i cprocsp-rdr-jacarta-64_5.0.0.1237-4_amd64.deb
```

JaCarta-2 PKI/ USB , , :

```
list_pcsc
```

: - - - - . .




tok JaCarta-2 PKI/ :

```
csptest -keyset -provtype 80 -newkeyset -cont '\\.\Aladdin R.D. JaCarta  
[SCR Interface] 00 00\tok'
```

Aladdin R.D. JaCarta [SCR Interface] 00 00 — USB JaCarta.

, , .

 КриптоПро CSP

Select carrier to create container tok

Aladdin R.D. JaCarta (JaCarta#4E3900131938304D)

Вид приложения:

CSP (JACARTA\_4E3900131938304D)

Описание:

Smart card as key storage. Provides the most advanced performance.

OK

Отмена

pin- ( — 11111111), .

**Authentication - CryptoPro CSP**

Crypto-Pro GOST R 34.10-2012 KC1 CSP requests pin-code

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

Media unique: JACARTA\_4E3900131938304D

---

Введите pin-code:

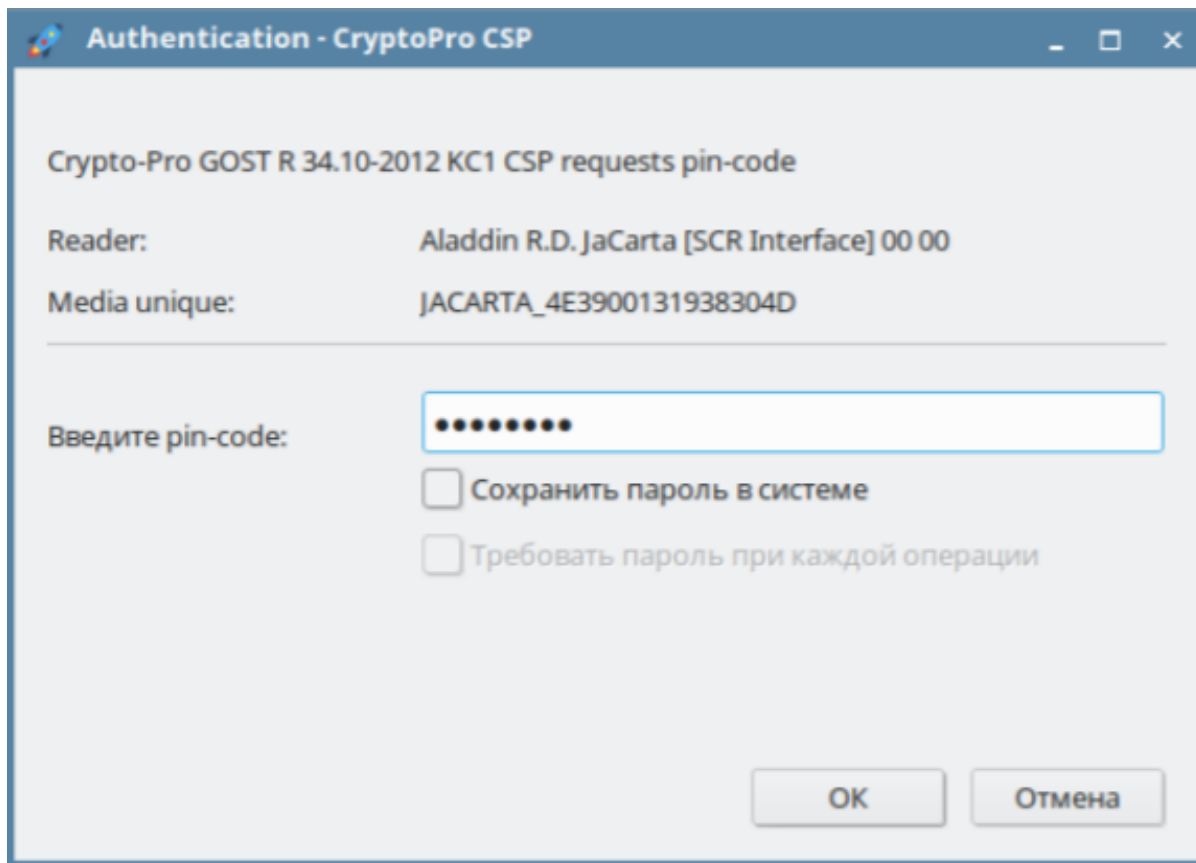
☐ Сохранить пароль в системе

☐ Требовать пароль при каждой операции

OK Отмена

```
cryptcp -creatrqst -dn "cn=test ,e=test@eos.ru" -provtype 80 -nokeygen -  
cont '\\.\Aladdin R.D. JaCarta [SCR Interface] 00 00\tok' -certusage  
"1.3.6.1.5.5.7.3.4,1.3.6.1.4.1.311.10.3.12" tok.req
```

pin- ( — 11111111), .



tok.req.

Browser plugin, .

certnew.p7b JaCarta-2 PKI/:

```
certmgr -inst -file certnew.p7b -store uMy -cont '\\.\Aladdin R.D. JaCarta  
[SCR Interface] 00 00\tok' -inst_to_cont
```

2.

pin- ( — 11111111 ), .



, ( . ) .