Astra Linux

«toc»

null

. : pcscd

- **S** – -: , VipNet . . https://www.rutoken.ru/support/download/get/rtDrivers-x64-deb.html;
- **Lite** – -: , VipNet . . . PKCS #15 CCID (Astra Linux Special Edition x.7 2021-1126SE17 (1.7.1);
- **2.0** – . () , — , . 2012. . 2016 ;
- **PKI 3.0**

. : https:/dev.rutoken.ru/pages/viewpage.action?pageId=66814078

Astra Linux

, , :

Lite/S :

1. .
2. csptestf CSP. . CSP.

2.0 :

1. .
2. + .
3. OpenSSL + engine.
4. csptestf CSP. . CSP.

Lite , USB-. :

1. + .
2. CSP 5.0.
3. .
4. 1 Astra Linux cryptoarm-gost-v2.5.12.linux-aarch64.deb (: https://github.com/CryptoARM/CryptoARMGOST/releases/tag/v2.5.12).

S .

:

- Astra Linux:
  - libccid;
  - pcscd;
  - libpcsclite1;
  - pcsc-tools;
  - opensc;
  - libengine-pkcs11-openssl1.1;
- , :
  - — librtpkcs11ecp (libengine-pkcs11-openssl1.1 Astra Linux);
  - S — ifd-rutokens (,).

synaptic :

```
sudo apt install libccid pcscd libpcsclite1 pcsc-tools opensc libengine-pkcs11-openssl1.1
```

librtpkcs11ecp : https://www.rutoken.ru/support/download/pkcs/ :

```
sudo apt install ./librtpkcs11ecp_*_amd64.deb
```

librtpkcs11ecp.so . , /usr/lib/librtpkcs11ecp.so. , :

```
find /usr/*(lib|lib64) -name librtpkcs11ecp.so
```

ifd-rutokens : https://www.rutoken.ru/support/download/get/rtDrivers-x64-deb.html :

```
sudo apt install ./ifd-rutokens_*_amd64.deb
```

.

pcsc_scan

pscsc_scan pcsc-tools. pcscd. :

```
pcsc_scan
```

pscsc_scan . - . , . Ctrl+C.

:

```
Using reader plug'n play mechanism
Scanning present readers...
0: Aktiv Rutoken lite 00 00

Fri Mar 31 13:29:35 2023
 Reader 0: Aktiv Rutoken lite 00 00
  Event number: 0
  Card state: Card inserted,
  ATR: 3B 8B 01 52 75 74 6F 6B 65 6E 6C 69 74 65 C2

ATR: 3B 8B 01 52 75 74 6F 6B 65 6E 6C 69 74 65 C2
+ TS = 3B --> Direct Convention
+ T0 = 8B, Y(1): 1000, K: 11 (historical bytes)
  TD(1) = 01 --> Y(i+1) = 0000, Protocol T = 1
-----
+ Historical bytes: 52 75 74 6F 6B 65 6E 6C 69 74 65
  Category indicator byte: 52 (proprietary format)
+ TCK = C2 (correct checksum)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
3B 8B 01 52 75 74 6F 6B 65 6E 6C 69 74 65 C2
```

pkcs11-tool

:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -T
```

:

```
vailable slots:
Slot 0 (0x0): Aktiv Rutoken lite 00 00
  token label        : Rutoken
  token manufacturer : Aktiv Co.
  token model        : Rutoken lite
  token flags        : login required, rng, SO PIN to be changed, token initialized, PIN initialized, user
PIN to be changed
  hardware version   : 65.4
  firmware version   : 30.2
  serial num         : 419b79e8
  pin min/max        : 6/32
```

XCA

. XCA: .

. PAM- : libpam-csp.

.

pkcs11-tool:

```
error: PKCS11 function C_InitToken failed: rv = unknown PKCS11 error (0x200)
Aborting.
```

rtadmin, , .

```
pkcs11-tool --init-token --module /usr/lib/librtpkcs11ecp.so --so-pin
87654321 --label "Astra Linux"
```

:

- --init-token — ;
- --module — ;
- --so-pin 87654321 — — PIN- (, SO-PIN). 87654321, . ;
- --label — — ;

SO-PIN

SO-PIN- . SO-PIN- 87654321 (. PIN- ?).

SO-PIN (87654321) 987654321:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so --login --login-type so --
so-pin 87654321 --change-pin --new-pin 987654321
```

:

- --login --login-type so — ;
- --so-pin — SO-PIN- ;
- --change-pin — PIN-;
- --new-pin — SO-PIN-.

SO-PIN- , .

PIN-

PIN- .

() PIN- :

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so --so-pin 87654321 --init-
pin --pin <PIN__>
```

--pin, PIN- . , PIN- .
PIN- :

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so --login --pin <_PIN-> --
change-pin --new-pin <_PIN->
```

, PIN- :

```
 Using slot 0 with a present token (0x0)
PIN successfully changed
```

:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so --label "_" --keypairgen --
key-type rsa:2048 -l --id 45
```

:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -O -l --pin <PIN__>
```

(Certificate Object) (Public Key Object), :

```
Using slot 0 with a present token (0x0)

Public Key Object; RSA 2048 bits
  label:      Test
  ID:         45
  Usage:      encrypt, verify, wrap

Certificate Object, type = X.509 cert
  label:  Test
  ID:     45
```

(ID) .

:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -r -y cert --id {id} > __.
crt
```

{id} ID

```
Using slot 0 with a present token (0x0)
```

, . .

:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so --label "_" --keypairgen --
key-type rsa:2048 -l --id 45
```

:

```
openssl

OpenSSL> engine dynamic -pre SO_PATH:/usr/lib/x86_64-linux-gnu/engines-1.1
/pkcs11.so -pre ID:pkcs11 -pre LIST_ADD:1 -pre LOAD -pre MODULE_PATH:/usr
/lib/librtpkcs11ecp.so
```

```
(dynamic) Dynamic engine loading support
[Success]: SO_PATH:/usr/lib/x86_64-linux-gnu/engines-1.1/pkcs11.so
[Success]: ID:pkcs11
[Success]: LIST_ADD:1
[Success]: LOAD
[Success]: MODULE_PATH:/usr/lib/librtpkcs11ecp.so
Loaded: (pkcs11) pkcs11 engine
```

```
Astra Linux Special Edition 1.6  pkcs11  libengine-pkcs11-openssl  1.0.2
   librtpkcs11ecp.so.           libengine-pkcs11-openssl1.1  0.4.4-4
Astra Linux Special Edition 1001F 01 (1.6): libengine-pkcs11-openssl1.
1_0.4.4-4_amd64.deb
```

```
OpenSSL> req -engine pkcs11 -new -key 0:45 -keyform engine -x509 -out __.
crt -outform DER
```

```
engine "pkcs11" set.
Enter PKCS#11 token PIN for Rutoken ECP <no label>:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Rusbitech
Organizational Unit Name (eg, section) []: Astra
Common Name (e.g. server FQDN or YOUR name) []:Makhmadiev Shuhrat
Email Address []:shuhrat@astralinux.ru

OpenSSL> exit
```

⚠ , openssl, openssl .

, :

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y cert -w __.crt -a
"___" --id 45
```

:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -O
```

```
Using slot 0 with a present token (0x0)
Public Key Object; RSA 2048 bits
label: _
ID: 45
Usage: encrypt, verify, wrap
Certificate Object, type = X.509 cert
label: ___
ID: 45
```

Astra Linux

:

- libccid;
- pcscd;
- libpam-p11;
- libpam-pkcs11;
- libp11-2;
- libengine-pkcs11-openssl;

- opensc.

synaptic :

- Astra Linux Special Edition x.7:

```
sudo apt install opensc libengine-pkcs11-openssl libpam-pkcs11 libpam-
p11 pcscd libccid
```

- Astra Linux Special Edition Astra Linux Common Edition:

```
sudo apt install opensc libengine-pkcs11-openssl libp11-2libp11- libpam-
pkcs11 libpam-p11 pcscd libccid
```

:

1. :

```
openssl
OpenSSL> x509 -in <_>.crt -out <_>.pem -inform DER -outform PEM
```

<_>.pem - .

2. . :

```
mkdir ~/.eid
chmod 0755 ~/.eid
cat ___.pem >> ~/.eid/authorized_certificates
chmod 0644 ~/.eid/authorized_certificates
```

:

```
sudo mkdir /home/<_>/.eid
sudo chmod 0755 /home/<_>/.eid
sudo chown <_>:<_> /home/<_>/.eid
cat <_>.pem | tee -a /home/<_>/.eid/authorized_certificates
sudo chown <_>:<_> /home/<_>/.eid/authorized_certificates
sudo chmod 0644 /home/user/.eid/authorized_certificates
```

id.

1. /usr/share/pam-configs/p11 :

```
Name: Pam_p11
Default: yes
Priority: 800
Auth-Type: Primary
Auth: sufficient pam_p11_opensc.so /usr/lib/librtpkcs11ecp.so
```

2. :

```
sudo pam-auth-update
```

Pam_p11 OK

- - Fly

```
sudo login
```

. Login , Password <PIN >. , , <PIN >.

libpam-pkcs11 pkcs11_eventmgr, PKCS#11.

pkcs11_eventmgr - /etc/pam_pkcs11/pkcs11_eventmgr.conf. :

```
pkcs11_eventmgr
{
#
daemon = true;

#
debug = false;

#
polling_time = 1;

#  -
# - 0
expire_time = 0;

#  pkcs11
pkcs11_module = /usr/lib/librtpkcs11ecp.so;

#
#  :
event card_insert {
#     (  )
on_error = ignore ;

action = "/bin/false";
}

#
event card_remove {
on_error = ignore;

#
action = "fly-wmfunc FLYWM_LOCK";
}

#
event expire_time {
#     (  )
on_error = ignore;

action = "/bin/false";
}
}
```

pkcs11_eventmgr .

rtadmin

rtadmin : , PIN- , Flash-. . :

- Lite
- Lite SC
-
- 2.0
- SC
- PKI
- Flash
- 2.0 Flash/touch
- PINPad

(Debian,) : https://dev.rutoken.ru/pages/viewpage.action?pageId=7995615.

1. (-q):

```
./rtadmin -f -q
```

2. :

```
./rtadmin -f -q -p 3
```

3. , RutokenAstra, PIN- 123456789 PIN- 987654321:

```
./rtadmin -f -z /usr/lib/librtpkcs11ecp.so -L RutokenAstra -u 123456789
-a 987654321 -q
```

rtadmin :

1		-f	-
2	PIN-	-o [PIN- (32)]	87654321. -o
3	PIN-	- [PIN- (32)]	12345678. -c
4	PIN-	-a [PIN- (32)]	87654321. -a
5	PIN-	-u [PIN- (32)]	12345678. -u
6	PIN2- (PINPad.)	-t	-
7	PIN- ( )	-G < PIN- (8-32)>	-
8	PIN- ( )	-g < PIN- (8-32)>	-
9	PIN-	-b < >	-
10	PIN-	-p <>: • 1 – , • 2 – , • 3 –]	2
11	PIN-	-M < PIN->: • 6-31 Lite; • 1 S	6
12	PIN-	-m < PIN->: • 6-31 Lite; • 1 S	6
13	PIN-	-R < (3-10)>	10
14	PIN-	-r < (1-10)>	10
15	Windows-1251	-L < >	-
16	UTF-8	-D < >	-
17	UTF-8 (, PIN-)	-U	PIN- UTF-8
18		-q	-
19	PKCS#11	-z < >	librtPKCS11ecp.so
20		-n < >	-
21		-l < >	: , : rtadmin.log

Web

(https://www.rutoken.ru/products/all/rutoken-plugin/) — .

.

, , :

- Web-: https://rutoken.ru. .
- Web- : https://dev.rutoken.ru. .
- : https://kb.rutoken.ru/display/kb. , . .
- : https://forum.rutoken.ru. .
- : https://dev.rutoken.ru/pages/viewpage.action?pageId=78479384;
- : https://www.rutoken.ru/support/feedback:
  - : https://help.rutoken.ru;
  - : hotline@rutoken.ru;
  - .: +7 495 925-77-90.