Astra Linux (pam-p11-gost)

, pam-p11, librtpkcs11ecp.so pam-p11-gost.

1. USB- .
2. USB- :

```
$ lsusb
```

USB-:

```
[dmitrieva@localhost ~]$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 004: ID 0a89:0030 Aktiv Rutoken ECP
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
```

, : **Aktiv Rutoken ECP**

1

:

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

- - Synaptic

:

- opensc
- libccid
- libpam-p11
- libp11-2
- libengine-pkcs11-openssl

2 librtpkcs11ecp.so

.

64- :

https://download.rutoken.ru/Rutoken/PKCS11Lib/Current/Linux/x86_64/librtpkcs11ecp.so

32- :

https://download.rutoken.ru/Rutoken/PKCS11Lib/Current/Linux/x86/librtpkcs11ecp.so

- - Fly

64- :

```
 $ wget --no-check-certificate https://download.rutoken.ru/Rutoken/PKCS11Lib/Current/Linux/x86_64
/librtpkcs11ecp.so
```

32- :

```
$ wget --no-check-certificate https://download.rutoken.ru/Rutoken/PKCS11Lib/Current/Linux/x64/librtpkcs11ecp.so
```

.

32- 64- :

```
$ sudo cp librtpkcs11ecp.so /usr/lib
$ sudo chmod 644 /usr/lib/librtpkcs11ecp.so
```

3

. - - Fly.

:

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

, , - .

```
Rutoken ECP <no label>
```

4 OpenSSL

4.1 OpenSSL

.

32- - https://download.rutoken.ru/Rutoken/Support_OpenSSL/201808_10.04.2016/linux-x86/libpkcs11gost-engine.so

64- - https://download.rutoken.ru/Rutoken/Support_OpenSSL/201808_10.04.2016/linux-x86_64/libpkcs11gost-engine.so

4.2

32- 64- :

```
$ sudo cp libpkcs11gost-engine.so /usr/lib/ssl/engines
$ sudo chmod 644 /usr/lib/ssl/engines/libpkcs11gost-engine.so
```

5 OpenSSL

OpenSSL, /usr/lib/ssl/openssl.cn

:

```
openssl_conf            = openssl_def
```

, :

```
[openssl_def]
engines = engine_section

[engine_section]
gost = gost_section
pkcs11 = pkcs11_section

[gost_section]
engine_id = gost
dynamic_path = /usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libgost.so
default_algorithms = ALL
init = 0

[pkcs11_section]
engine_id = pkcs11_gost
dynamic_path = /usr/lib/i386-linux-gnu/openssl-1.0.0/engines/libpkcs11gost-engine.so
MODULE_PATH = /usr/lib/librtpkcs11ecp.so
init = 0
```

6

.

- - Fly

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

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

, . 4.1

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

, , :

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

{id} ID

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

, cert.crt 5

6.1

- - Fly

```
$ openssl genpkey -engine pkcs11_gost -algorithm GOST2001 -pkeyopt key_id:50 -pkeyopt paramset:A -pkeyopt pin:
12345678
```

- **key_id** - ID
- **paramset** - :
  - A - OID 1.2.643.2.2.35.1;
  - B - OID 1.2.643.2.2.35.2;
  - C - OID 1.2.643.2.2.35.3;
  - XA - OID 1.2.643.2.2.36.0;
  - XB - OID 1.2.643.2.2.36.1;

- **pin** - PIN-

```
$ openssl req -engine pkcs11_gost -new -key 50 -keyform engine -x509 -out cert.crt -outform DER
```

```
$ pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y cert -w cert.crt --id 50
```

7

- - Fly

```
OpenSSL> x509 -in cert.crt -out cert.pem -inform DER -outform PEM
```

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

8 pam-p11-gost

8.1 GitHub

GitHub - https://github.com/AktivCo/pam-p11-gost/archive/pkcs11-gost.zip

8.2

pam-p11-gost , (gcc, make).

:

- autoconf
- libtool
- pkg-config
- libssl-dev
- libpam0g-dev

SDK, - http://www.rutoken.ru/developers/sdk/

SDK ~/SDK

```
$ sudo cp ~/SDK/Samples/rtPKCS11/Include /usr/include/pkcs11
```

8.3

pkcs11-gost.zip .

.

```
$ cd ~/pam-p11-gost-pkcs11-gost
$ mkdir m4
$ ./bootstrap
$ ./configure CFLAGS=-O2 --with-pamdir="/lib/x86_64-linux-gnu/security/" --enable-strict
$ make
$ sudo make install
```

9

- - Fly

```
$ sudo nano /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
```

, Alt + X, Y

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

Pam_p11 OK

10

- - Fly

```
$ sudo login
```

PIN-