

Astra Linux (RSA)

0

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

--

:

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

Astra Linux SE 1.6 pkcs11 libengine-pkcs11-openssl 1.0.2 librtpkcs11ecp.so. , libengine-pkcs11-openssl1.1 0.4.4-4 1.6:

 [libengine-pkcs11-openssl1.1_0.4.4-4_amd64.deb](#)

2 librtpkcs11ecp.so

.

64- :

<https://download.rutoken.ru/Rutoken/PKCS11Lib/Current/Linux/x64/librtpkcs11ecp.so>

32- :

<https://download.rutoken.ru/Rutoken/PKCS11Lib/Current/Linux/x32/librtpkcs11ecp.so>

- - Fly

64- :

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

32- :

```
$ wget --no-check-certificate https://download.rutoken.ru/Rutoken/PKCS11Lib/Current/Linux/x32/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

- - Fly

```
$ pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -0
```

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 -0
```

```
, cert.crt 5
```

4.1

- - Fly

```
$ pkcs11-tool --module /usr/lib/librtpkcs11ecp.so --keypairgen --key-type rsa:2048 -1 --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
OpenSSL> req -engine pkcs11 -new -key 0:45 -keyform engine -x509 -out cert.crt -outform DER
```

```
$ pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y cert -w cert.crt --id 45
```

5

- - 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
```

6

- - 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

7

- - Fly

```
$ sudo login
```

PIN-

8

```
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/librtpkcs11lecp.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 .