

RD JaCarta AstraLinux

- 1
- 2
 - 2.1 [pcs_scan](#)
 - 2.2 [pkcs11-tool](#)
 - 2.3 [XCA](#)
- 3
 - 3.1 [pkcs11-tool:](#)
- 4
- 5
 - 5.1
 - 5.2
 - 5.3
- 6 [Astra Linux](#) [JaCarta](#) [libpam-p11](#)
 - 6.1
 - 6.2
 - 6.3
 - 6.3.1
 - 6.4
- 7



∴ [pcscd](#)

USB- - JaCarta, Astra Linux

- [JaCarta PKI](#) - USB- - , (PKI);
- [JaCarta-2](#) - USB- - (—) 0, 0 . , ;
- [JaCarta SF/](#) – (,) :
 - , - USB- (-);
 - , .

:

- Astra Linux:
 - libccid;
 - libengine-pkcs11-openssl1.1 (libengine-pkcs11-openssl);
 - libpcsc-lite1;
 - pcscd;
 - opensc;
 - pcsc-tools (, [20190912SE16 \(1.6.3\)](#));
- , :
 - libjcpkcs11-2 (jcpkcs11-2);

Astra Linux :

```
sudo apt install libccid pcscd libpcsc-lite1 pcsc-tools opensc libengine-pkcs11-openssl1.1
```



Astra Linux Special Edition .10015-01 1.6 libengine-pkcs11-openssl, libjcpkcs11-2.so, libengine-pkcs11-openssl1.1 . :

- libengine-pkcs11-openssl1.1 0.4.4-4 Astra Linux Special Edition .10015-01 (1.6): [libengine-pkcs11-openssl1.1_0.4.4-4_amd64.deb](#);
- [Astra Linux Special Edition .10015-01 \(1.6\)](#) libengine-pkcs11-openssl1.1 ;

libjcpkcs11-2:

1. web- : <https://www.aladdin-rd.ru/support/downloads/jacarta>).
2. :

```
unzip jacartauc_*_al_x64.zip
```

3. :

```
sudo apt install ./jcpkcs11-*_amd64.deb
```

libjcpkcs11-2.so . :

```
find /usr/*{lib,lib64} -name libjcPKCS11-2.so
```



pcs_scan

:

```
pcsc_scan
```

:

pkcs11-tool

:

```
pkcs11-tool --module /usr/lib/libjcPKCS11-2.so -T
```

:

Available slots:

Slot 0 (0x1ffff): Aladdin R.D. JaCarta [SCR Interface] (000000000000) 00 00

token label : JaCarta-2 GOST

token manufacturer : Aladdin R.D.

token model : JaCarta GOST 2.0

token flags : login required, rng, token initialized, PIN initialized, other flags=0x800

hardware version : 1.0

firmware version : 2.55

serial num : 4E46001310573957

pin min/max : 6/32

XCA

.XCA: .



... () , JaCarta , . () .
 . PIN- () JaCarta .
 PIN- 00000000 ().
 JaCarta -2 PIN- , PUK- . , . JaCarta -2.

pkcs11-tool:

```
pkcs11-tool --module /usr/lib/libjcpkcs11-2.so --init-token --so-pin
00000000 --label 'JaCarta PKI'
```

PIN- :

```
pkcs11-tool --module /usr/lib/libjcpkcs11-2.so --init-pin --so-pin 00000000
--pin 11111111
```

:

- --init-token – ;
- --pin - PIN- JaCarta;
- --so-pin 00000000 – PIN- ;
- --label 'JaCarta PKI' - () ;
- --module - libjcpkcs11-2.so.

PIN-

PIN- :

```
pkcs11-tool --module /usr/lib/libjcpkcs11-2.so --login --pin <_PIN-> --
change-pin --new-pin <_PIN->
```

, PIN- :

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

--pin, PIN- . , PIN- .

:

```
pkcs11-tool --module /usr/lib/libjcpkcs11-2.so --pin <PIN-> -0 -1
```

, :

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

Using slot 0 with a present token (0x0)

, (.), , . .

:

```
pkcs11-tool --module /usr/lib/libjcpkcs11-2.so -r -y cert --id <id> > <_>.
cert
```

<id> (ID), .

<_>.cert , .

:

```
pkcs11-tool --module /usr/lib/libjcpkcs11-2.so --label "Astra Linux" --
keypairgen --key-type rsa:2048 -l --id 45
```

:

1. :

openssl

openssl;

2. openssl:

a. jcpkcs11-2:

```
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/libjcpkcs11-2.so
```

:

```
$ 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/libjcpkcs11-2.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/libjcpkcs11-2.so
Loaded: (pkcs11) pkcs11 engine
```

b. :

```
req -engine pkcs11 -new -key 131071:45 -keyform engine -x509 -out _.crt -outform DER
```

:



Common Name (Astra-user).

:

```
OpenSSL> req -engine pkcs11 -new -key 131071:45 -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) []:Astra-user
Email Address []:Astra-user@astralinux.ru
```

c. openssl :

```
exit
```

JaCarta:

```
pkcs11-tool --module /usr/lib/libjcpkcs11-2.so -l -y cert -w <_>.crt -a
"____" --id 45
```

JaCarta:

```
pkcs11-tool --module /usr/lib/libjcpkcs11-2.so -0 -l
```

```
-----
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 JaCarta libpam-p11

1. synaptic;
2. :
 - a. libccid;
 - b. pcscd;
 - c. libpam-p11;
 - d. libpam-pkcs11;
 - e. libp11-3 Astra Linux Special Edition x.7 libp11-2 Astra Linux Special Edition 1.6;
 - f. libengine-pkcs11-openssl;
 - g. opensc;
3. ;

:

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

1. :

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

__.pem - ;

2. (ID);
 3. , :
- a. .eid. Astra-user:

```
sudo mkdir ~Astra-user/.eid
```

- b. :

```
sudo chmod 0755 ~Astra-user/.eid
```

- c. .eid/authorized_certificates (,):

```
cat __.pem | sudo tee -a ~Astra-user/.eid/authorized_certificates
```

- d. :

```
sudo chmod 0644 ~/.eid/authorized_certificates
```

- e. , :

```
sudo chown -R Astra-user:Astra-user ~/.eid
```



1. 2.

:

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

```
Name: Pam_p11
Default: yes
Priority: 800
Auth-Type: Primary
Auth: sufficient pam_p11.so /usr/lib/libjckPKCS11-2.so
```

2. :

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

3. Pam_p11();
4. OK.

:

1. ;
2. :

```
sudo login Astra-user
```

3. <PIN >;
4. 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    JaCarta
    pkcs11_module = /usr/lib/libjcpkcs11-2.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 .

<https://www.aladdin-rd.ru> - JaCarta.

<https://kbp.aladdin-rd.ru/> , . .

<https://www.aladdin-rd.ru/support/downloads>