ALT Linux 6.0-8.0 2.0

, pam_pkcs11 librtpkcs11ecp.so.

- , .

-.

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 pam_pkcs11 pcsc-lite-ccid openssl-
engine_pkcs11
```

- - Synaptic :

- opensc,
- pam_pkcs11,
- pcsc-lite-ccid,
- openssl-engine_pkcs11.

2

- rtPKCS11ecp GNU/Linux RPM 32-bit (x86)
- rtPKCS11ecp GNU/Linux RPM 64-bit (x86_64)

, /usr/lib (/usr/lib64) librtpkcs11ecp.so.

3 -

- . dmesg , .

```
usb 2-2.2: new full speed USB device number 6 using uhci_hcd
usb 2-2.2: New USB device found, idVendor=0a89, idProduct=0030
usb 2-2.2: New USB device strings: Mfr=1, Product=2, SerialNumber=0
usb 2-2.2: Product: Rutoken ECP
usb 2-2.2: Manufacturer: Aktiv
usb 2-2.2: configuration #1 chosen from 1 choice
```

32- :

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

64- :

```
$ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -T
```

4

RSA , .

RSA - 2048 .

, 4-8.

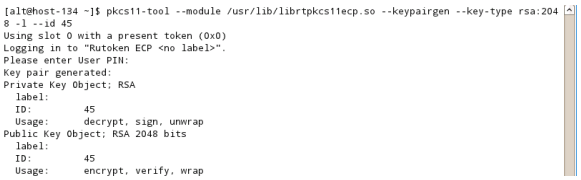
! PIN- . .

32- :

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

64- :

```
$ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so --keypairgen --key-
type rsa:2048 -l --id 45
```



pkcs11-tool opensc.

, :

--module <arg>	pkcs11 ()
--keypairgen	
-- key-type <arg>	. – rsa, - 2048 (1024)
-l	PIN- - ()
--id <arg>	id ( )

5 PEM

openssl pkcs11:

32- :

```
$ openssl
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib/openssl/engines
/libpkcs11_gost.so -pre ID:pkcs11 -pre LIST_ADD:1 -pre LOAD -pre
MODULE_PATH:/usr/lib/librtpkcs11ecp.so
```

64- :

```
$ openssl
OpenSSL>  engine dynamic -pre SO_PATH:/usr/lib64/openssl/engines
/libpkcs11_gost.so -pre ID:pkcs11 -pre LIST_ADD:1  -pre LOAD -pre
MODULE_PATH:/usr/lib64/librtpkcs11ecp.so
```

```
[alt@host-134 ~]$ openssl
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib/openssl/engines/engine_pkcs11.so -pre ID:pkcs11 -pr
e LIST_ADD:1 -pre LOAD -pre MODULE_PATH:/usr/lib/librtpkcs11ecp.so
(dynamic) Dynamic engine loading support
[Success]: SO_PATH:/usr/lib/openssl/engines/engine_pkcs11.so
[Success]: ID:pkcs11
[Success]: LIST_ADD:1
[Success]: LOAD
[Success]: MODULE_PATH:/usr/lib/librtpkcs11ecp.so
Loaded: (pkcs11) pkcs11 engine
OpenSSL>
```

PEM-. ! PIN- .

```
 OpenSSL>  req -engine pkcs11 -new -key 0:45 -keyform engine -x509 -out
cert.pem  -text
```

```
OpenSSL> req -engine pkcs11 -new -key 0:45 -keyform engine -x509 -out cert.pem -text
engine "pkcs11" set.
PKCS#11 token PIN:
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) [RU]:
State or Province Name (full name) []:Moscow
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) []:Aktiv
Organizational Unit Name (eg, section) []:Aktiv
Common Name (e.g., your name or your server's hostname) []:alt
Email Address []:alt@mail.ru
```

:

-key	(0:45 – :ID)
-x509	

6 PEM CRT

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

7

openssl (exit). C CRT .! PIN- .

32- :

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

64- :

```
$ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l -y cert -w cert.crt
--id 45
```

```
[alt@host-134 ~]$ pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y cert -w cert.crt --id 45
Using slot 0 with a present token (0x0)
Logging in to "Rutoken ECP <no label>".
Please enter User PIN:
Created certificate:
Certificate Object, type = X.509 cert
  label:
  ID:         45
```

:

-y <arg>	(cert, privkey, pubkey, data)
-w <arg>	

8 , ,

! PIN- .

32- :

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

64- :

```
$ pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -O -l
```

9 pam_pkcs11

, pam_pkcs11.

:

```
$ su
Password:
#
```

ALT Lixnux 6.0 7.0 :

```
# cp /usr/share/pam_pkcs11/pam_pkcs11.conf.example /etc/security/pam_pkcs11
/pam_pkcs11.conf
# cp /usr/share/pam_pkcs11/subject_mapping.example /etc/security/pam_pkcs11
/subject_mapping
```

ALT Lixnux 8 :

```
# cp /usr/share/doc/pam_pkcs11/pam_pkcs11.conf.example /etc/security
/pam_pkcs11/pam_pkcs11.conf
# cp /usr/share/doc/pam_pkcs11/subject_mapping.example /etc/security
/pam_pkcs11/subject_mapping
```

"y"

10

```
# rm /etc/pam.d/system-auth
# ln -s /etc/pam.d/system-auth-pkcs11 /etc/pam.d/system-auth
```

"y"

11

/etc/pam.d/system-auth.

, , .

mcedit

```
# mcedit /etc/pam.d/system-auth
```

32- :

```
auth               [success=1 default=ignore]        pam_pkcs11.so
pkcs11_module=/usr/lib/librtpkcs11ecp.so
```

64- :

```
auth               [success=1 default=ignore]        pam_pkcs11.so
pkcs11_module=/usr/lib64/librtpkcs11ecp.so
```

12 pam_pkcs11

/etc/security/pam_pkcs11/pam_pkcs11.conf

, , .

mcedit

```
# mcedit  /etc/security/pam_pkcs11/pam_pkcs11.conf
```

32- :

```
pam_pkcs11 {
  nullok = false;
  debug = false;
  use_first_pass = false;
  use_authtok = false;
  card_only = false;
  wait_for_card = false;
  use_pkcs11_module = rutokenecp;

  # Aktiv Rutoken ECP
  pkcs11_module rutokenecp {
    module = /usr/lib/librtpkcs11ecp.so
    slot_num = 0;
    support_thread = true;
    ca_dir = /etc/pam_pkcs11/cacerts;
        crl_dir = /etc/pam_pkcs11/crls;
          cert_policy = signature;
  }

  use_mappers = subject;
  mapper_search_path = /lib/pam_pkcs11;

  mapper subject {
                debug = false;
                module = internal;
                ignorecase = false;
                mapfile = file:///etc/security/pam_pkcs11/subject_mapping;
  }
}
```

64-

module = /usr/lib/librtpkcs11ecp.so module = /usr/lib64/librtpkcs11ecp.so

mapper_search_path = /lib/pam_pkcs11; mapper_search_path = /lib64/pam_pkcs11;

13 ALT Linux.

pkcs11_inspect

```
# pkcs11_inspect > /etc/security/pam_pkcs11/subject_mapping
```

mcedit

```
# mcedit  /etc/security/pam_pkcs11/subject_mapping
```

```
# Printing data for mapper subject:
/C=RU/ST=Moscow/L=Moscow/O=Aktiv/OU=Aktiv/CN=alt/emailAddress=alt@mail.ru -
> alt
```

! **alt**

whoami ( )

```
$ whoami
```

14

, , login. , , .

login , - Rutoken.

```
[alt@host-134 ~]$ sudo login
Found the Smart card.
Welcome Rutoken ECP <no label>!
Smart card PIN:
[alt@host-134 ~]$
```

. .

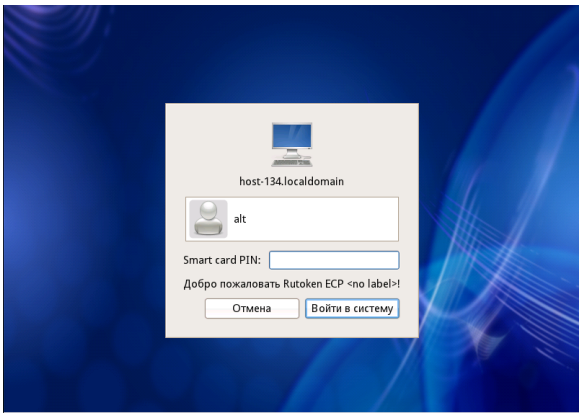
:

1. pam_pkcs11.conf "debug = false;", "debug = true;".
2. /etc/pam.d/system-auth "debug".

.

15 !

. :



16

:

1) . , " - ", .

2) . ( )

subject_mapping ( )