GPG

GPG - , openPGP, -. , pkcs11, , pkcs11 -, scdaemon. , , GPG , , , 2.0.

.

GPG gnupg-pkcs11-scd

(, . -- red hat, -- debian)

```
sudo yum instal gnupg2 gnupg-pkcs11-scd

sudo apt-get install gpg
```

, gpg >= 2.1.19.

debian pkcs11 - gnupg-pkcs11-scd .

librtpkcs11ecp.so .

, RSA , GOST .

RSA ( ).

~/.gnupg/gpg-agent.conf :

```
scdaemon-program /usr/bin/gnupg-pkcs11-scd
```

~/.gnupg/gnupg-pkcs11-scd.conf :

```
providers rutoken

provider-rutoken-library /usr/lib64/librtpkcs11ecp.so
```

gpg-agent:

```
sudo killall gpg-agent
```

, :

```
gpg --card-status
```

:

```
[lo1ol@localhost .gnupg]$ gpg --card-status

Application ID ...: D2760001240111503131CAE8D55A1111

Version ..........: 11.50

Manufacturer .....: unknown

Serial number ....: CAE8D55A

Name of cardholder: [not set]

Language prefs ...: [not set]

Sex ..............: unspecified

URL of public key : [not set]

Login data .......: [not set]

Signature PIN ....: forced

Key attributes ...: 1R 1R 1R

Max. PIN lengths .: 0 0 0

PIN retry counter : 0 0 0

Signature counter : 0

Signature key ....: [none]

Encryption key....: [none]

Authentication key: [none]

General key info..: [none]
```

, gpg-agent. gpg-agent :

```
gpg-agent --server
SCD LEARN
```

"Bad certificate", , , GPG.

:

```
[lo1ol@localhost .gnupg]$ gpg-agent --server

OK Pleased to meet you

SCD LEARN

....

S KEYPAIRINFO 892E053AE031FC23F3E7CCC73BC60859F11F6B90 Aktiv\x20Co\x2E/Rutoken\x20ECP/3ac67ae9
/Rutoken\x20ECP\x20\x3Cno\x20label\x3E/45

OK
```

GPG

, :

```
gpg-agent --server
SCD LEARN
```

, S KEYPAIRINFO, . , :

```
S KEYPAIRINFO 892E053AE031FC23F3E7CCC73BC60859F11F6B90 Aktiv\x20Co\x2E/Rutoken\x20ECP/3ac67ae9
/Rutoken\x20ECP\x20\x3Cno\x20label\x3E/45
```

892E053AE031FC23F3E7CCC73BC60859F11F6B90. . GPG.

:

```
gpg --expert --full-generate-key
```

. RSA (13):

```
lo1ol@lo1ol-VirtualBox:~$ gpg --expert --full-generate-key

gpg (GnuPG) 2.2.4; Copyright (C) 2017 Free Software Foundation, Inc.

This is free software: you are free to change and redistribute it.

There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:

   (1) RSA and RSA (default)

   (2) DSA and Elgamal

   (3) DSA (sign only)

   (4) RSA (sign only)

   (7) DSA (set your own capabilities)

   (8) RSA (set your own capabilities)

   (9) ECC and ECC

  (10) ECC (sign only)

  (11) ECC (set your own capabilities)

  (13) Existing key

Your selection? 13
```

:

```
Enter the keygrip: 892E053AE031FC23F3E7CCC73BC60859F11F6B90
```

email . , e-mail, , :

```
Possible actions for a RSA key: Sign Certify Encrypt Authenticate

Current allowed actions: Sign Certify Encrypt

   (S) Toggle the sign capability

   (E) Toggle the encrypt capability

   (A) Toggle the authenticate capability

   (Q) Finished

Your selection?

Please specify how long the key should be valid.

         0 = key does not expire

      <n>  = key expires in n days

      <n>w = key expires in n weeks

      <n>m = key expires in n months

      <n>y = key expires in n years

Key is valid for? (0)

Key does not expire at all

Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: lo1ol

Email address: lo1ol@example.com

Comment:

You selected this USER-ID:

    "lo1ol <lo1ol@example.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O

       .

gpg: /home/lo1ol/.gnupg/trustdb.gpg: trustdb created

gpg: key 676E42AAAFBCF227 marked as ultimately trusted

gpg: directory '/home/lo1ol/.gnupg/openpgp-revocs.d' created

gpg: revocation certificate stored as '/home/lo1ol/.gnupg/openpgp-revocs.d
/0CD2B9CEE398990609D6C164676E42AAAFBCF227.rev'

public and secret key created and signed.

pub   rsa2048 2019-10-25 [SCE]

      0CD2B9CEE398990609D6C164676E42AAAFBCF227

uid                      lo1ol <lo1ol@example.com>
```

deb

dpkg-sig:

```
sudo apt-get install dpkg-sig
```

, , librtpkcs11ecp.so.

, id gpg. :

```
gpg --list-sigs
```

:

```
lo1ol@lo1ol-VirtualBox:~/Downloads$ gpg --list-sigs
/home/lo1ol/.gnupg/pubring.kbx
------------------------------
pub   rsa2048 2019-10-25 [SCE]
      0CD2B9CEE398990609D6C164676E42AAAFBCF227
uid           [ultimate] lo1ol <lo1ol@example.com>
sig 3        676E42AAAFBCF227 2019-10-25  lo1ol <lo1ol@example.com>
```

, **676E42AAAFBCF227**. . :

```
dpkg-sig -k 676E42AAAFBCF227 --sign builder librtpkcs11ecp_1.9.15.0-1_amd64.deb
```

, -k id . --sign -- , , , , . :

```
dpkg-sig --verify librtpkcs11ecp_1.9.15.0-1_amd64.deb
```

rpm

dpkg-sig:

```
sudo apt-get install rpm-sign
```

, . librtpkcs11ecp.so:

, id gpg. :

```
gpg --list-sigs
```

:

```
lo1ol@lo1ol-VirtualBox:~/Downloads$ gpg --list-sigs

/home/lo1ol/.gnupg/pubring.kbx

------------------------------

pub   rsa2048 2019-10-25 [SCE]

      0CD2B9CEE398990609D6C164676E42AAAFBCF227

uid           [ultimate] lo1ol <lo1ol@example.com>

sig 3        676E42AAAFBCF227 2019-10-25  lo1ol <lo1ol@example.com>
```

, **676E42AAAFBCF227**. . .rpmmacros :

```
%_signature gpg
%_gpg_name 676E42AAAFBCF227
```

, %_gpg_name id , .

:

```
rpm --addsign librtpkcs11ecp-1.9.15.0-1.x86_64.rpm
```

, gpg :

```
gpg -a -o ~/RPM-GPG-KEY-test --export 676E42AAAFBCF227
sudo rpm --import ~/RPM-GPG-KEY-test
```

. :

```
rpm -K librtpkcs11ecp-1.9.15.0-1.x86_64.rpm
```

:

```
librtpkcs11ecp-1.9.15.0-1.x86_64.rpm: digests signatures
```