OpenSSL (RSA)

1. USB- .
2. USB- :

```
$ lsusb
```

USB-:

, : **Aktiv Rutoken ECP**

USB- - OpenSSL opensc libengine-pkcs11-openssl:

```
Sudo apt-get install opensc libengine-pkcs11-openssl
```

librtpkcs11ecp, .

RSA2048:

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

/usr/lib/librtpkcs11ecp.so – , id 45 – .

:

```
$ openssl
```

engine PKCS#11:

```
engine -t dynamic -pre SO_PATH:/usr/lib/engines/engine_pkcs11.so -pre ID:pkcs11 -pre LIST_ADD:1 -pre LOAD -pre
MODULE_PATH:/usr/lib/librtpkcs11ecp.so
```

/usr/lib/librtpkcs11ecp.so – . openssl.

:

```
req -engine pkcs11 -new -key slot_0-id_45 -keyform engine -out /home/user/test.csr
```

slot_0-id_45- id , /home/user/test.csr – .

OpenSSL .

Certification Authority (CA):

```
openssl genpkey -algorithm RSA -out /home/user/key.pem
```

CA:

```
openssl req -x509 -new -key /home/user/key.pem -out /home/user/ca.crt
```

openssl (/etc/ssl) demoCA, – newcerts. demoCA index.txt serial. - 01.

:

```
openssl ca -keyfile /home/user/key.pem -cert /home/user/ca.crt -in /home/user/test.csr -out /home/user/user-cert.pem
```

/home/user/key.pem – CA, /home/user/ca.crt – , /home/user/test.csr – , /home/user/user-cert.pem –

DER :

```
openssl x509 -in /home/user/user-cert.pem -out /home/user/user-cert.crt -outform DER
```

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y cert -w /home/user/user-cert.crt --id 45 --label TEST
```

/home/user/user-cert.crt – .