(OpenSSH)

OpenSSH . **librtpkcs11ecp.so**, **opensc-pkcs11.so**.

- Ubuntu x86,
- Ubuntu x86,
- Windows 7;
- , .

librtpkcs11ecp.so

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.

*nix :

1.1 :

```
$ sudo apt-get install opensc
```

1.2 `librtpkcs11ecp.so` (http://www.rutoken.ru/support/download/pkcs/) `/usr/lib/`

1.3 :

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

1.4 ssh :

```
$ ssh-keygen -D /usr/lib/librtpkcs11ecp.so -I 0:45 >> key.pub
```

0:45 - <>:<id>.

1.5 SSH- PuttySC Windows

1.5.1 :

```
$ sudo apt-get install libengine-pkcs11-openssl
$ openssl
OpenSSL> engine dynamic -pre SO_PATH:/usr/lib/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.cert -text -days 365 -text
OpenSSL> exit
```

1.5.2 DER-:

```
$ openssl x509 -in cert.cert -out cert.der -outform der
```

1.5.3 **:**

```
$ pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y cert -w cert.der --id 45 --label Rutoken1
```

*nix :

1.1 opensc. , , cb54ebf, 0.13.0rc1.

1.2 librtpkcs11ecp.so /usr/lib/

1.3 openssh-client openssl:

```
$ sudo apt-get install openssh-client openssl
```

1.4 :

```
$ openssl genrsa -out keys.pem 2048
```

1.5 :

```
$ openssl req -new -key keys.pem -out cert.csr
$ openssl x509 -req -days 700 -in cert.csr -signkey keys.pem -out cert.cert
```

1.6 DER-:

```
$ openssl rsa -inform PEM -in keys.pem -out keys.der -outform DER
$ openssl x509 -in cert.cert -out cert.der -outform der
```

1.7 DER- :

```
$ pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y privkey -w keys.der --id 10 --label Rutoken1
$ pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y cert -w cert.der --id 10 --label Rutoken1
```

1.8 ssh:

```
 $ ssh-keygen -D /usr/lib/librtpkcs11ecp.so -I 0:10 >> key.pub
```

0:10 - <>:<id>.

2.

2.1 `openssh-server`:

```
$ sudo apt-get install opensc openssh-server
```

2.2 1.4 (1.8) `key.pub ~/.ssh/authorized_keys` (,).

3. *nix-

3.1 `opensc openssh-client`:

```
$ sudo apt-get install openssh-client
```

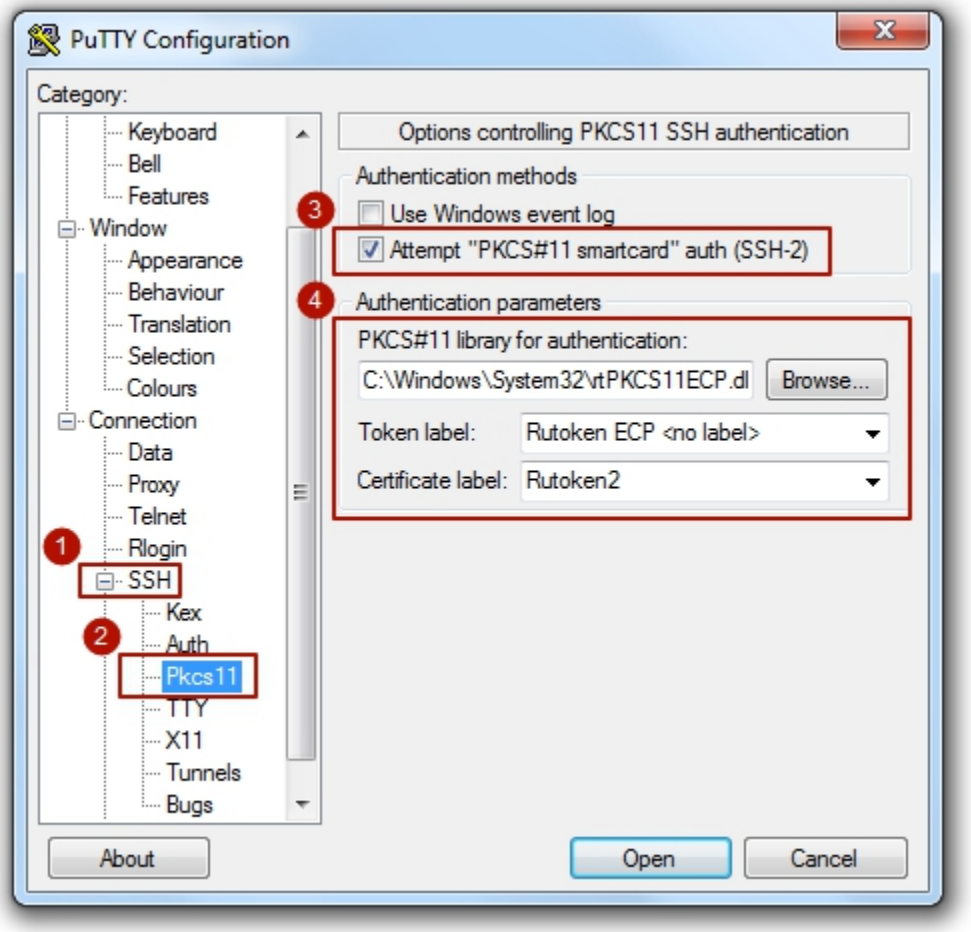
3.2 `librtpkcs11ecp.so` (http://www.rutoken.ru/support/download/pkcs/) `/usr/lib/`
3.3 :

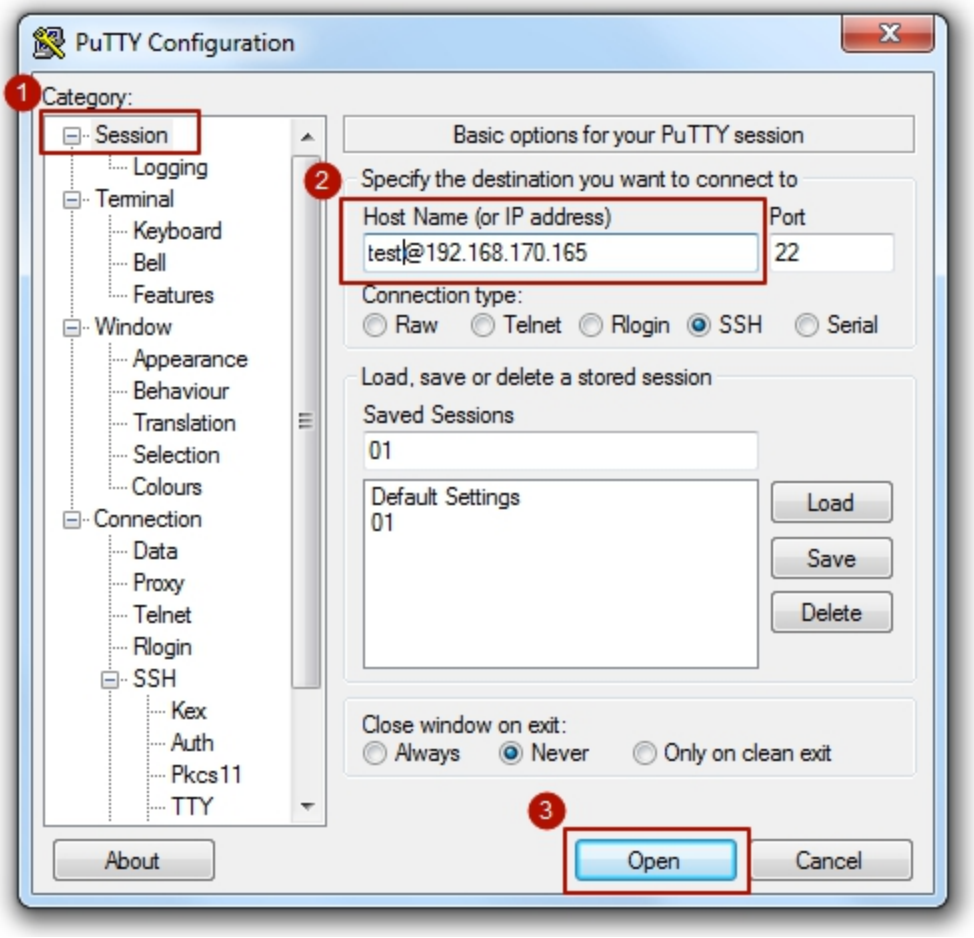
```
ssh -I /usr/lib/librtpkcs11ecp.so <username>@<server>
```

4. Windows-

4.1 http://www.rutoken.ru/support/download/drivers-for-windows/.

4.2 SSH- Windows PuttySC. SSH -> PKCS11 Attempt "PKCS#11 smartcard" auth, rtPKCS11ECP.dll, . Session () .





`opensc-pkcs11.so`

1.

1.1 `openssh-server`:

```
$ sudo apt-get install openssh-server
```

1.2 :

```
$ pkcs15-init --erase-card -p rutoken_ecp
$ pkcs15-init --create-pkcs15 --so-pin "87654321" --so-puk ""
$ pkcs15-init --store-pin --label "User PIN" --auth-id 02 --pin "12345678" --puk "" --so-pin "87654321" --
finalize
```

1.3 :

```
$ pkcs15-init -G rsa/2048 --auth-id 02 --id 42
```

1.4 ssh:

```
$ pkcs15-tool --read-ssh-key 42
```

42 – id .

1.5 `~/.ssh/authorized_keys` .

2.

2.1 `opensc openssh-client`:

```
$ sudo apt-get install opensc openssh-client
```

2.2 :

```
$ ssh -I /usr/lib/opensc-pkcs11.so <username>@<server>
```

`IdentityFile SmartcardDevice /usr/lib/librtpkcs11ecp.so`.

1. Using OpenSSH with smartcards