

OpenVPN

- 1
 - 2
 - 3
 - 4
- 4.1
4.2

, OpenVPN . <http://habrahabr.ru/company/aktiv-company/blog/137306/>.

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

, , . Ubuntu-12.10-desktop-i386.

1. :

```
$ sudo apt-get install pcsd libpcsclite1 libccid
```

2. XCA:

```
$ sudo apt-get install xca
```

3. XCA:

```
$ sudo xca
```

3.1 *File->New Database.*

3.2 : *Private Keys->New Key, CAkey, Keytype RSA, Keysize 2048 bit.*

: *Certificates->New Certificate .*

X Certificate and Key management

Create x509 Certificate

Source | Subject | Extensions | Key usage | Netscape | Advanced

Signing request

Sign this Certificate signing request

Copy extensions from the request

Modify subject of the request

Signing

Create a self signed certificate with the serial number

Use this Certificate for signing

Signature algorithm: SHA 1

Template for the new certificate: [default] CA

Apply extensions | Apply subject | Apply all

OK | Cancel

X Certificate and Key management

Create x509 Certificate

Source | Subject | Extensions | Key usage | Netscape | Advanced

Distinguished name

Internal name	<input type="text" value="CA"/>	organizationName	<input type="text" value="qwe"/>
countryName	<input type="text" value="RU"/>	organizationalUnitName	<input type="text" value="asd"/>
stateOrProvinceName	<input type="text" value="Moscow"/>	commonName	<input type="text" value="CA"/>
localityName	<input type="text" value="msc"/>	emailAddress	<input type="text" value="CA@mail.ru"/>

Type	Content
------	---------

Add

Delete

Private key

Used keys too

OK | Cancel

X Certificate and Key management

Create x509 Certificate

Source | Subject | Extensions | Key usage | Netscape | Advanced

Basic constraints

Type: **Certification Authority** (highlighted with a red circle)

Path length: Critical

Key identifier

Subject Key Identifier
 Authority Key Identifier

Validity

Not before: 2013-05-29 09:57 GMT
Not after: 2014-05-29 09:57 GMT

Time range

1 Years
 Midnight Local time No well-defined expiration

subject alternative name

issuer alternative name

CRL distribution point

Authority Info Access: OCSP

3.3 OpenVPN: *Private Keys*-> *New Key*, *Serverkey*, *Keytype* - RSA, *Keysize* - 2048 bit.

: *Certificates*->*New Certificate* .

X Certificate and Key management

Create x509 Certificate

Source | Subject | Extensions | Key usage | Netscape | Advanced

Signing request

- Sign this Certificate signing request
- Copy extensions from the request
- Modify subject of the request

Signing

- Create a self signed certificate with the serial
- Use this Certificate for signing

Signature algorithm: SHA 1

Template for the new certificate: [default] HTTPS server

Apply extensions | Apply subject | Apply all

OK | Cancel

X Certificate and Key management

Create x509 Certificate

Source | Subject | Extensions | Key usage | Netscape | Advanced

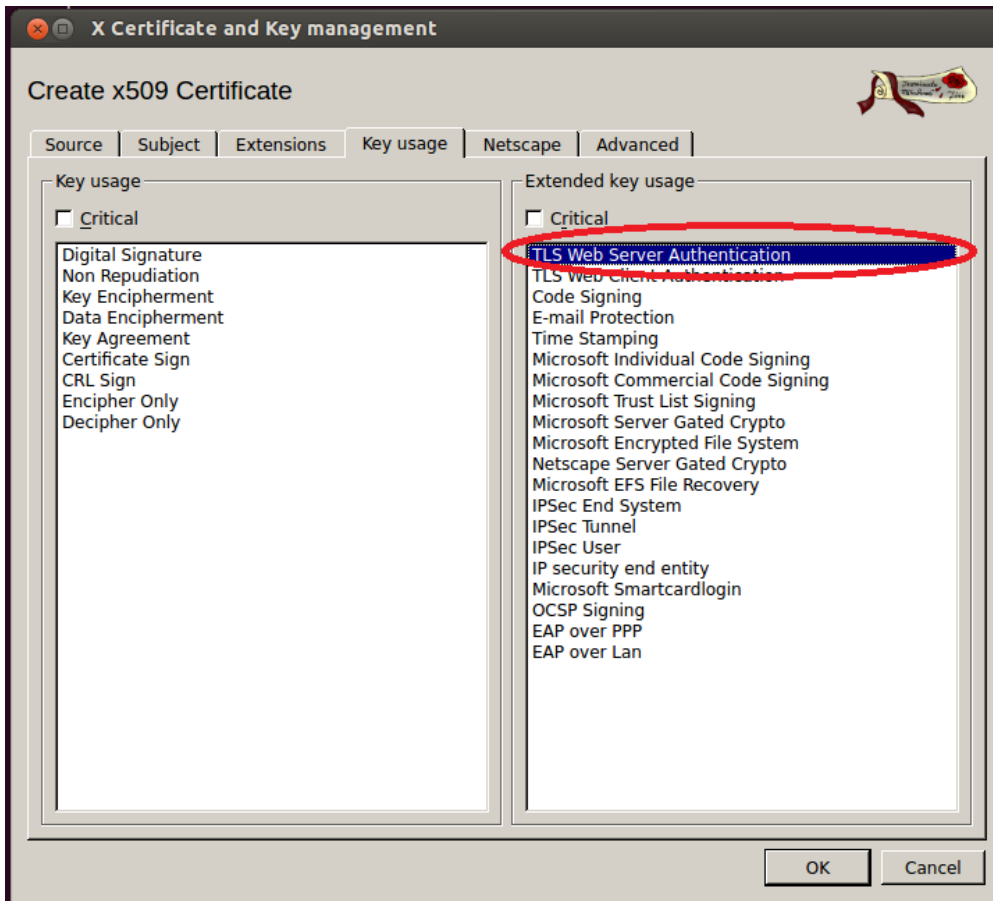
Distinguished name

Internal name	Server	organizationName	qwe
countryName	RU	organizationalUnitName	asd
stateOrProvinceName	Moscow	commonName	Server
localityName	msc	emailAddress	Server@mail.ru

Type	Content
------	---------

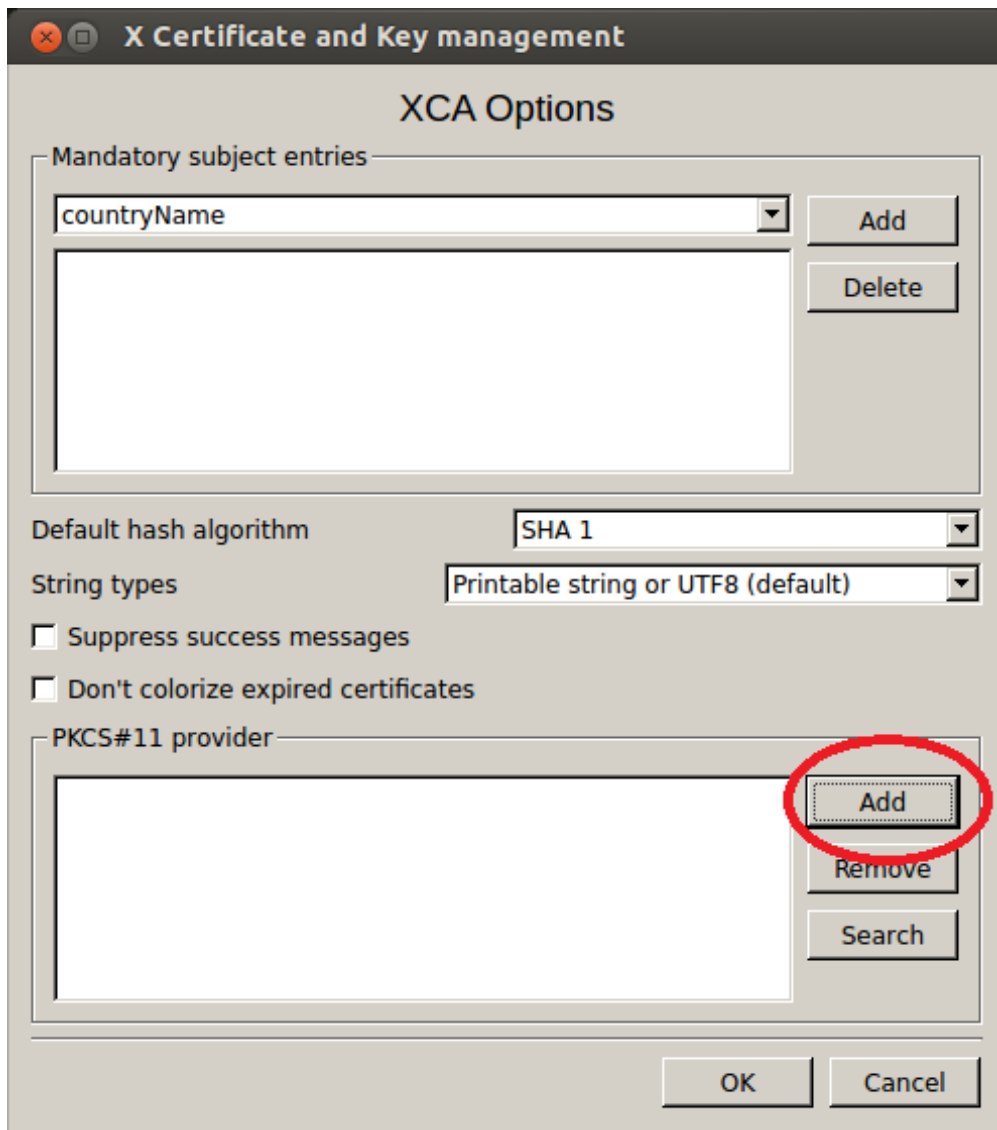
Private key: Serverkey (RSA) | Used keys too | Generate a new key

OK | Cancel

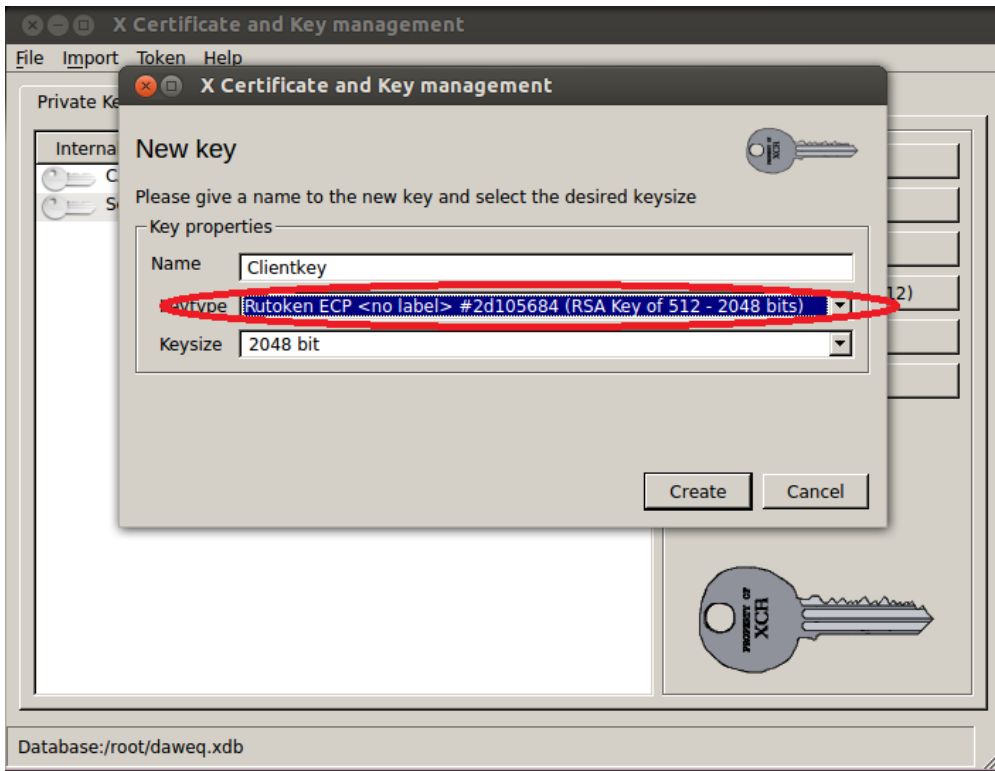


3.4 CA.crt, Serverkey.pem Server.crt (*Private Keys->Export, Certificates->Export*).

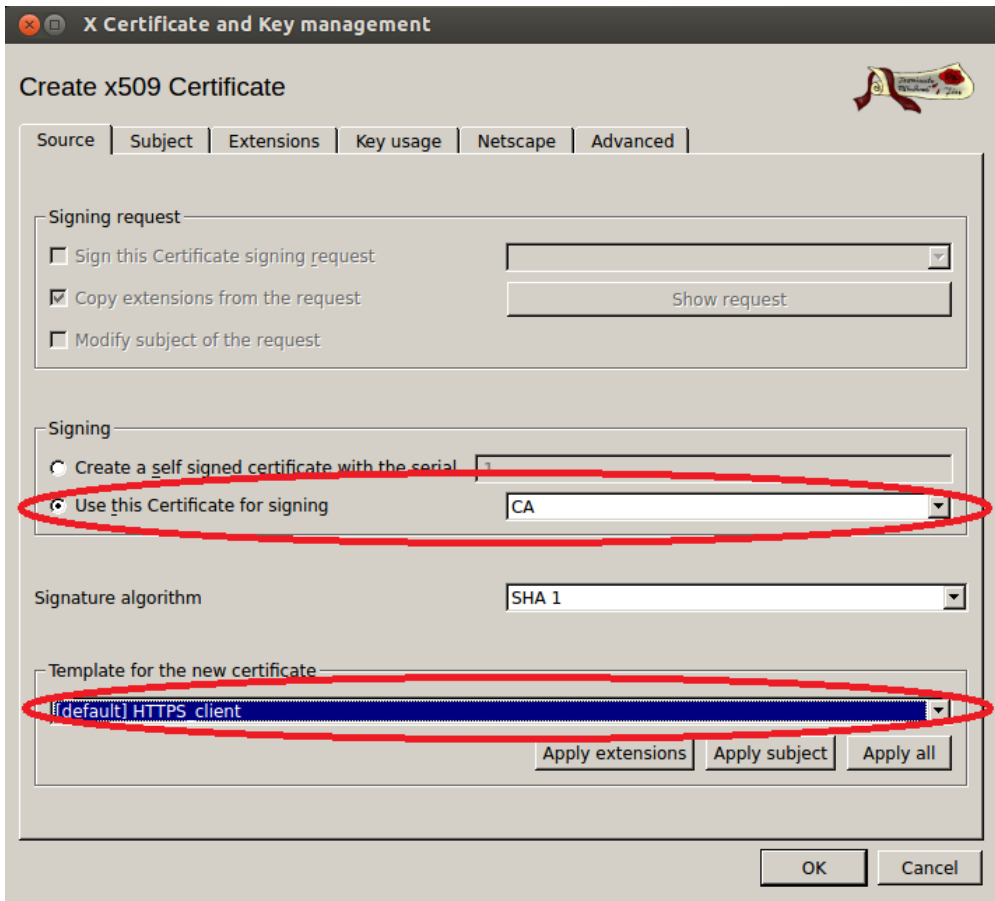
4. PKCS#11. : *File->Options*.



4.1 . « » : Private Keys -> New Key. PIN-.



4.2 :



X Certificate and Key management

Create x509 Certificate

Source | Subject | Extensions | Key usage | Netscape | Advanced

Distinguished name

Internal name	Client	organizationName	qwe
countryName	RU	organizationalUnitName	asd
stateOrProvinceName	Moscow	commonName	Client
localityName	msc	emailAddress	Client@mail.ru

Type	Content

Private key

Clientkey (Token RSA) Used keys too

X Certificate and Key management

Create x509 Certificate

Source | Subject | Extensions | Key usage | Netscape | Advanced

Key usage

Critical

- Digital Signature
- Non Repudiation
- Key Encipherment
- Data Encipherment
- Key Agreement
- Certificate Sign
- CRL Sign
- Encipher Only
- Decipher Only

Extended key usage

Critical

- TLS Web Server Authentication
- TLS Web Client Authentication**
- Code Signing
- E-mail Protection
- Time Stamping
- Microsoft Individual Code Signing
- Microsoft Commercial Code Signing
- Microsoft Trust List Signing
- Microsoft Server Gated Crypto
- Microsoft Encrypted File System
- Netscape Server Gated Crypto
- Microsoft EFS File Recovery
- IPSec End System
- IPSec Tunnel
- IPSec User
- IP security end entity
- Microsoft Smartcardlogin
- OCSP Signing
- EAP over PPP
- EAP over Lan

5. OpenVPN:

```
$ sudo apt-get install openvpn
```

6. -:

```
$ openssl dhparam -out dh1024.pem 1024
```

7. OpenVPN:

```
$ nano openvpn.conf
```

```
,, :
```

```
port 1194
proto tcp
dev tap

ca /home/asd/CA.crt
cert /home/asd/Server.crt
key /home/asd/Serverkey.pem
dh /home/asd/dh1024.pem

server 10.0.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt

keepalive 10 120

cipher BF-CBC
comp-lzo
persist-key
persist-tun
status openvpn-status.log
verb 3
```

8. OpenVPN:

```
$ sudo openvpn --config /home/asd/openvpn.conf
```

9. , :

```
$ sudo apt-get install pcsd libpcsclite1 libccid
```

10. OpenVPN:

```
$ sudo apt-get install openvpn
```

11. .

```
client
dev tap
proto tcp
remote xxx.xxx.xxx.xxx 1194
resolv-retry infinite
nobind
persist-key
persist-tun

ca /home/qwe/CA.crt
pkcs11-providers /usr/lib/librtpkcs11lecp.so
pkcs11-id 'Aktiv\x20Co\x2E/Rutoken\x20ECP/2d105684/Rutoken\x20ECP\x20\x3Cno\x20label\x3E/C67F8A314C24E080'

pkcs11-pin-cache 300

comp-lzo
verb 3
```

```
pkcs11-providers PKCS#11.
```

```
pkcs11-id ID, . ID :
```

```
$ openvpn --show-pkcs11-ids [ PKCS#11 ]
```

12. VPN:

```
$ openvpn --config [ ]
```