

# Настройка аутентификации по Рутокен ЭЦП в OpenVPN на Linux

- 1 Введение
- 2 Проверка модели устройства
- 3 Стенд
- 4 Общий порядок действий
  - 4.1 Сервер
  - 4.2 Клиент

## Введение

В данной инструкции описывается, как настроить авторизацию в OpenVPN с помощью Рутокен ЭЦП 2.0.

За основу взята статья <http://habrahabr.ru/company/aktiv-company/blog/137306/>.

## Проверка модели устройства

1. Подключите USB-токен к компьютеру.
2. Для определения названия модели USB-токена откройте **Терминал** и введите команду:

```
$ lsusb
```

В результате в окне Терминала отобразится название модели USB-токена или только ID.

```
[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
```

```
:~$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 005: ID 0a89:0030
Bus 002 Device 004: ID 0e0f:0008 VMware, Inc.
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
```

Убедитесь, что используете: **Aktiv Rutoken ECP**

В некоторых случаях название устройства может не отображаться, тогда ориентируйтесь на значение **0a89** в ID - такой вендор id имеют все устройства Рутокен.

## Стенд

Для примера возьмем Рутокен ЭЦП 2.0 2100, отформатированный через Панель управления Рутокен, сервер и клиент. В качестве дистрибутива использовалась Ubuntu 1804.

## Общий порядок действий

### Сервер

1. Устанавливаем необходимые для работы Рутокен ЭЦП 2.0 пакеты:

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

2. Устанавливаем XCA:

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

3. Запускаем XCA:

```
$ sudo xca
```

3.1 Создаем новую базу *File->New Database*.

3.2 Создаем ключ УЦ: *Private Keys->New Key*, назовем его CAkey, *Keytype* выбираем RSA, *Keysize* 2048 bit.

Создаем сертификат УЦ: *Certificates->New Certificate* согласно представленным скриншотам:

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 1

Use this Certificate for signing

Signature algorithm: SHA 1

Template for the new certificate: [default] CA

Apply extensions Apply subject Apply all

OK Cancel

### Create x509 Certificate



Source Subject Extensions Key usage Netscape Advanced

#### Distinguished name

Internal name	CA	organizationName	qwe
countryName	RU	organizationalUnitName	asd
stateOrProvinceName	Moscow	commonName	CA
localityName	msc	emailAddress	CA@demo.local

Type	Content	
		Add
		Delete

#### Private key

CAkey (RSA:2048 bit)  Used keys too

OK Cancel

**X Certificate and Key management**

### Create x509 Certificate

Source Subject **Extensions** Key usage Netscape Advanced

**X509v3 Basic Constraints**

Type: Certification Authority  
Path length:   Critical

**Key identifier**

Subject Key Identifier  
 Authority Key Identifier

**Validity**

Not before: 2020-04-22 12:25 GMT  
Not after: 2021-04-22 12:25 GMT

**Time range**

1 Years   
 Midnight  Local time  No well-defined expiration

X509v3 Subject Alternative Name:

X509v3 Issuer Alternative Name:

X509v3 CRL Distribution Points:

Authority Information Access: OCSP

3.3 Создаем ключ сервера OpenVPN: *Private Keys*-> *New Key*, назовем его *Serverkey*, *Keytype* - RSA, *Keysize* - 2048 bit.

Создаем сертификат сервера: *Certificates*->*New Certificate* согласно представленным скриншотам.

### 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 1

Use this Certificate for signing CA

Signature algorithm SHA 1

#### Template for the new certificate

[default] HTTPS\_server

Apply extensions Apply subject Apply all

OK Cancel

### Create x509 Certificate



Source Subject Extensions Key usage Netscape Advanced

#### Distinguished name

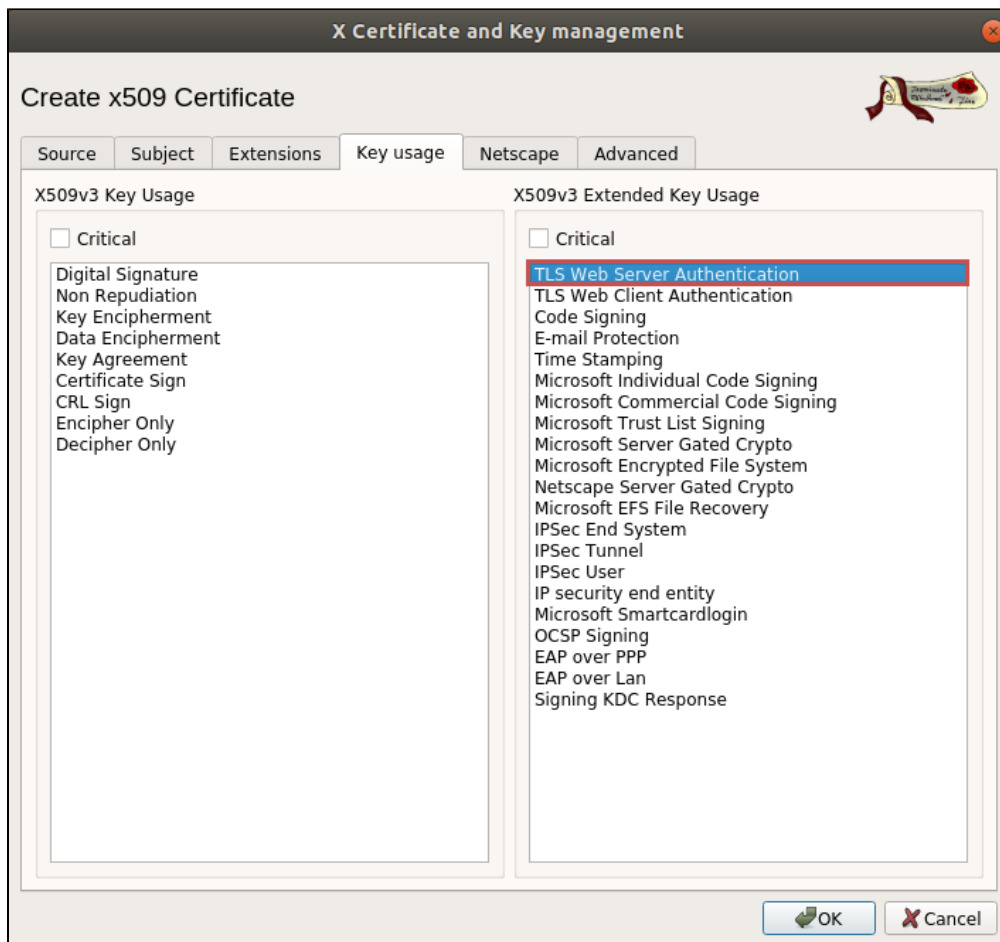
Internal name	Server	organizationName	qwe
countryName	RU	organizationalUnitName	asd
stateOrProvinceName	Moscow	commonName	Server
localityName	msc	emailAddress	Server@demo.local

Type	Content	Add
		Delete

#### Private key

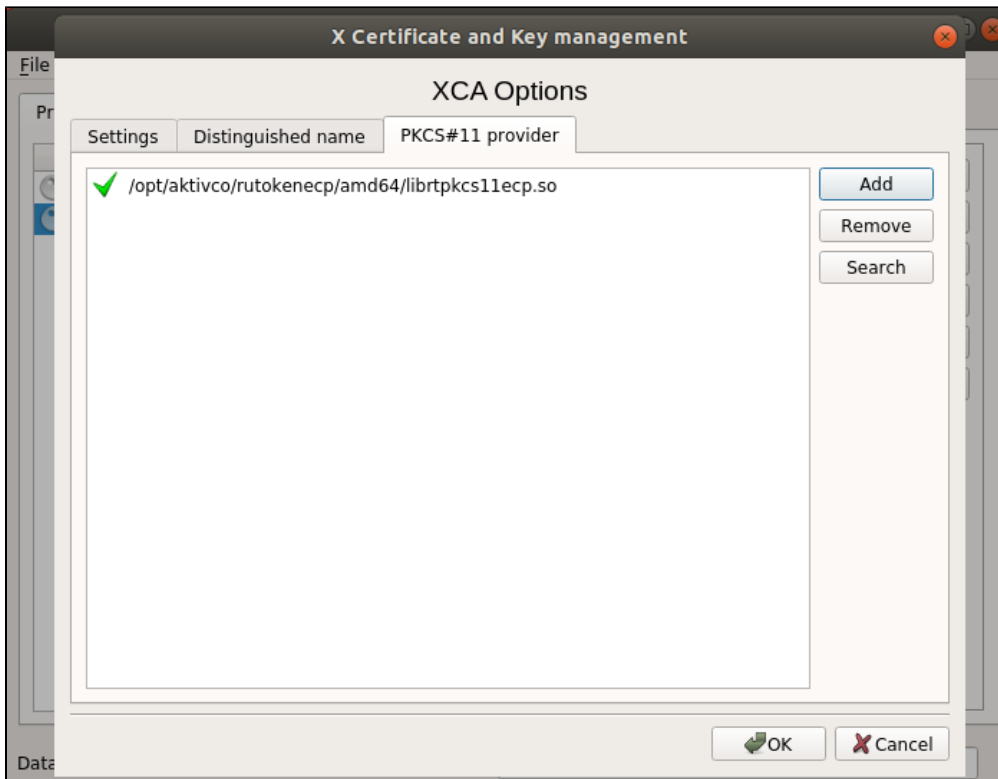
Serverkey (RSA:2048 bit)  Used keys too

OK Cancel

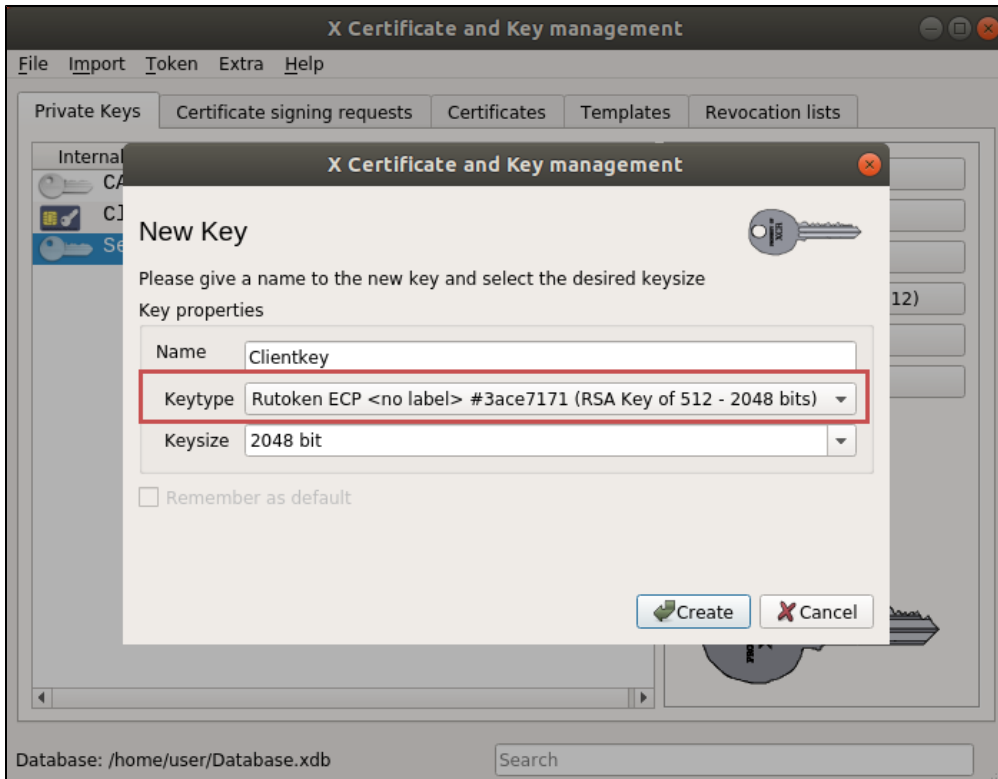


3.4 Экспортируем сертификат УЦ в файл CA.crt, ключ сервера в файл Serverkey.pem и сертификат сервера в файл Server.crt (*Private Keys->Export, Certificates->Export*).

4. Для работы с Рутокен ЭЦП нужна библиотека PKCS#11. Загрузить ее можно по [ссылке](#). После загрузки устанавливаем библиотеку и указываем путь к ней: *File->Options*.



4.1 Подключаем Рутокен. Создаем ключ «на борту» Рутокен ЭЦП: *Private Keys* -> *New Key*. По запросу вводим PIN-код.



4.2 Создаем сертификат клиента:



### 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

Show request

#### Signing

Create a self signed certificate with the serial 1

Use this Certificate for signing CA

Signature algorithm SHA 1

#### Template for the new certificate

[default] HTTPS\_client

Apply extensions Apply subject Apply all

OK Cancel

### Create x509 Certificate



Source Subject Extensions Key usage Netscape Advanced

#### Distinguished name

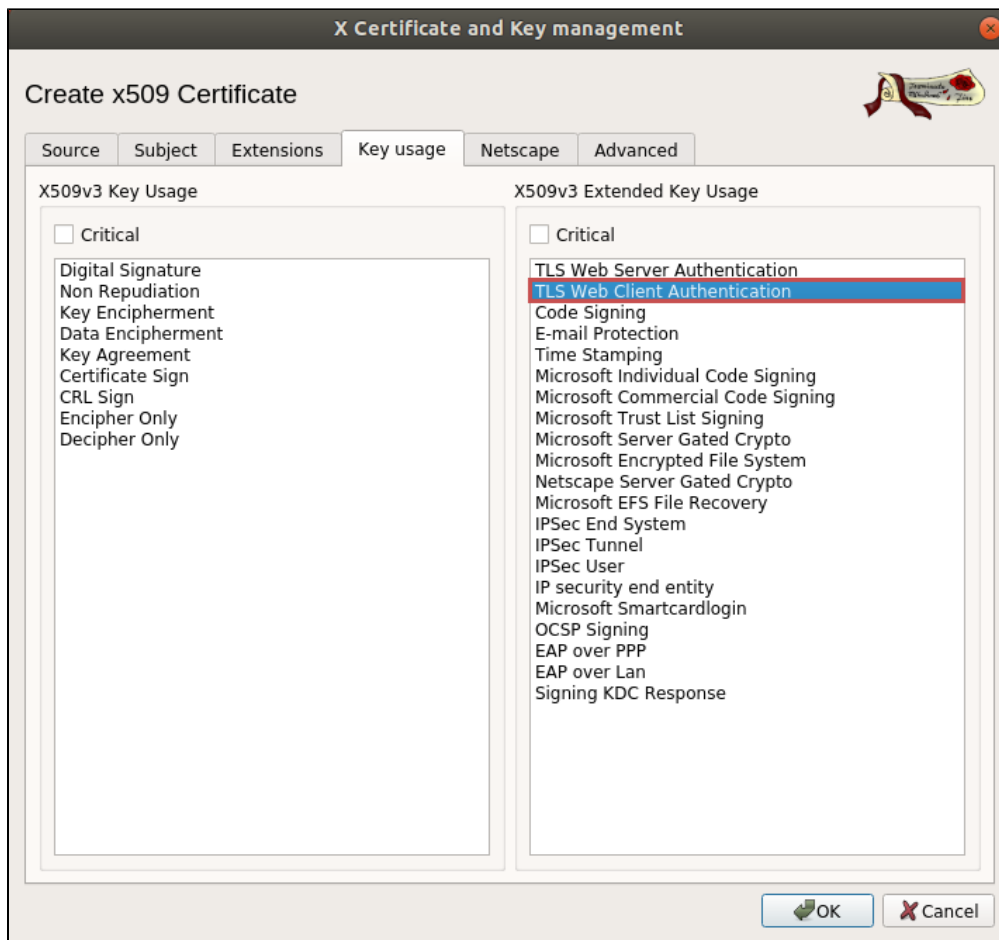
Internal name	Client	organizationName	qwe
countryName	RU	organizationalUnitName	asd
stateOrProvinceName	Moscow	commonName	Client
localityName	msc	emailAddress	Client@demo.local

Type	Content	Add
		Delete

#### Private key

Clientkey (Token RSA:2048 bit)  Used keys too

OK Cancel



4.3 Когда XCA предложит сохранить сертификат на токен, нажимаем «Yes» и вводим PIN-код. Закрываем XCA.

5. Устанавливаем OpenVPN:

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

6. Создаем файл с параметрами алгоритма Диффи-Хелмана:

```
$ openssl dhparam -out dh2048.pem 2048
```

7. Создаем конфигурационный файл сервера OpenVPN:

```
$ nano openvpn.conf
```

У нас, например, он выглядит так:

```
port 1194
proto tcp
dev tap

ca /home/user/CA.crt
cert /home/user/Server.crt
key /home/user/Serverkey.pem
dh /home/user/dh2048.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. Запускаем сервер OpenVPN:

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

## Клиент

#### 9. Устанавливаем пакеты, необходимые для работы Рутокена:

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

#### 10. Устанавливаем OpenVPN:

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

#### 11. Узнаем ID контейнера, в котором на Рутокене хранятся ключ и сертификат. Узнать этот ID можно с помощью команды:

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

#### 12. Создаем конфигурационный файл клиента.

```
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/librtpkcs11ecp.so
pkcs11-id 'Aktiv\x20Co\x2E/Rutoken\x20ECP/2d105684/Rutoken\x20ECP\x20\x3Cno\x20label\x3E/C67F8A314C24E080'

pkcs11-pin-cache 300

comp-lzo
verb 3
```

- В параметре `pkcs11-providers` указываем путь к библиотеке PKCS#11.
- В параметре `pkcs11-id` указываем ID контейнера, полученный на 11 шаге.

13. Подключаемся к VPN-серверу:

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

Если запроса PIN-кода Рутокена не происходит, выполните действия по [инструкции](#).