OpenVPN c

blocked URL

OpenVPN — .

, OpenVPN, . OpenVPN 3 :

- ;
- (. OpenVPN);
- (-).

OpenVPN . PIN- PIN-. RSA, . , .
, VPN XCA. OpenVPN . OpenVPN , OpenVPN .

http://habrahabr.ru/company/aktiv-company/blog/137306/

OpenVPN XCA Astra Linux Special Edition .10015-01 1.6 2

, XCA:

```
sudo apt install libccid libpcsclite1 pcscd xca
```

librtpkcs11ecp.so :

https://www.rutoken.ru/support/download/pkcs/

Библиотека rtPKCS11ecp для GNU/Linux DEB 32-bit (x86)

Версия: v.1.8.2.0 от 02.03.2018

Поддерживаемые ОС: 32-разрядные Debian/Ubuntu/Mint/Astra

Библиотека rtPKCS11ecp для GNU/Linux DEB 64-bit (x64)

Версия: v.1.8.2.0 от 02.03.2018

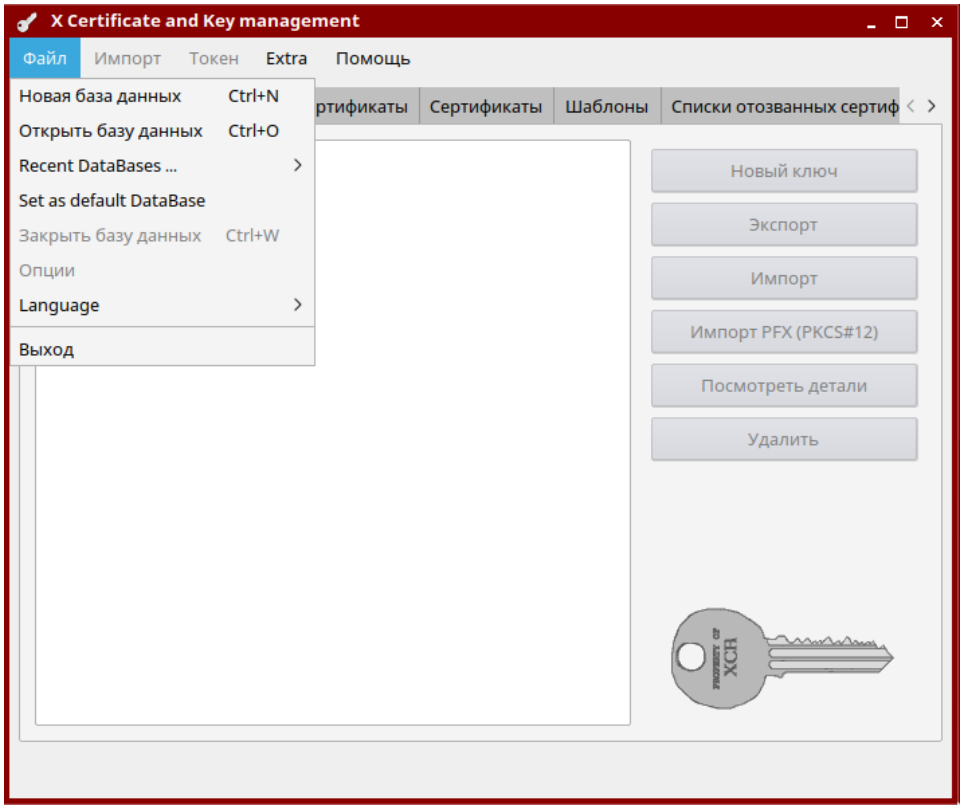
Поддерживаемые ОС: 64-разрядные Debian/Ubuntu/Mint/Astra

```
sudo dpkg -i librtpkcs11ecp_1.8.2.0-1_amd64.deb
```

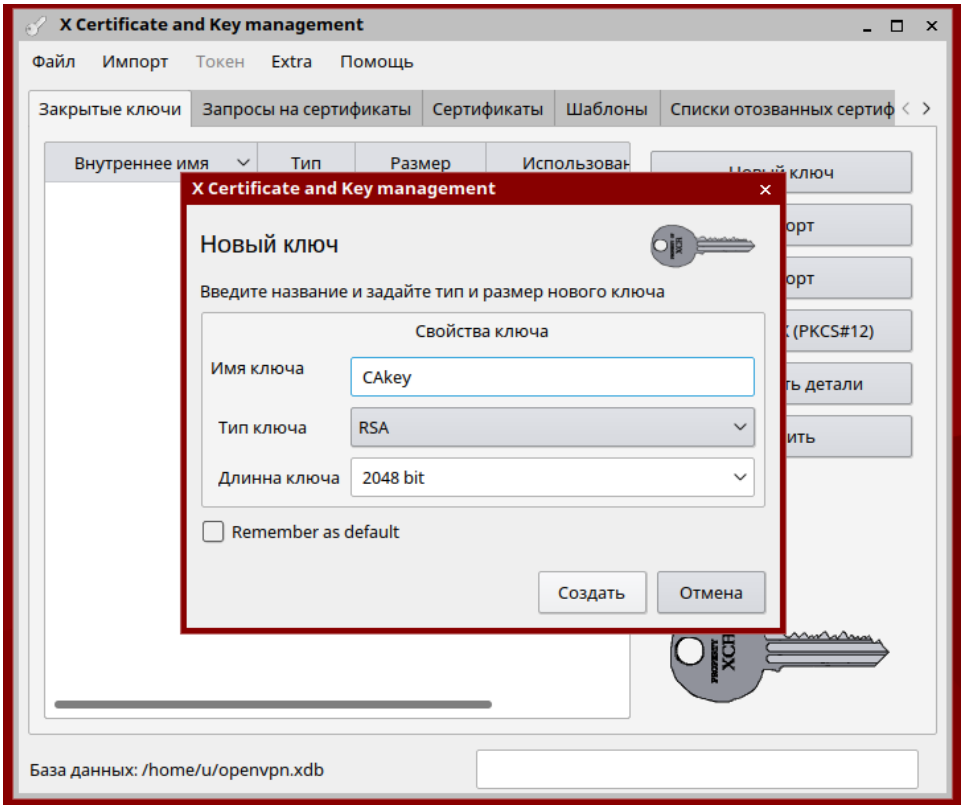
XCA:

"" XCA

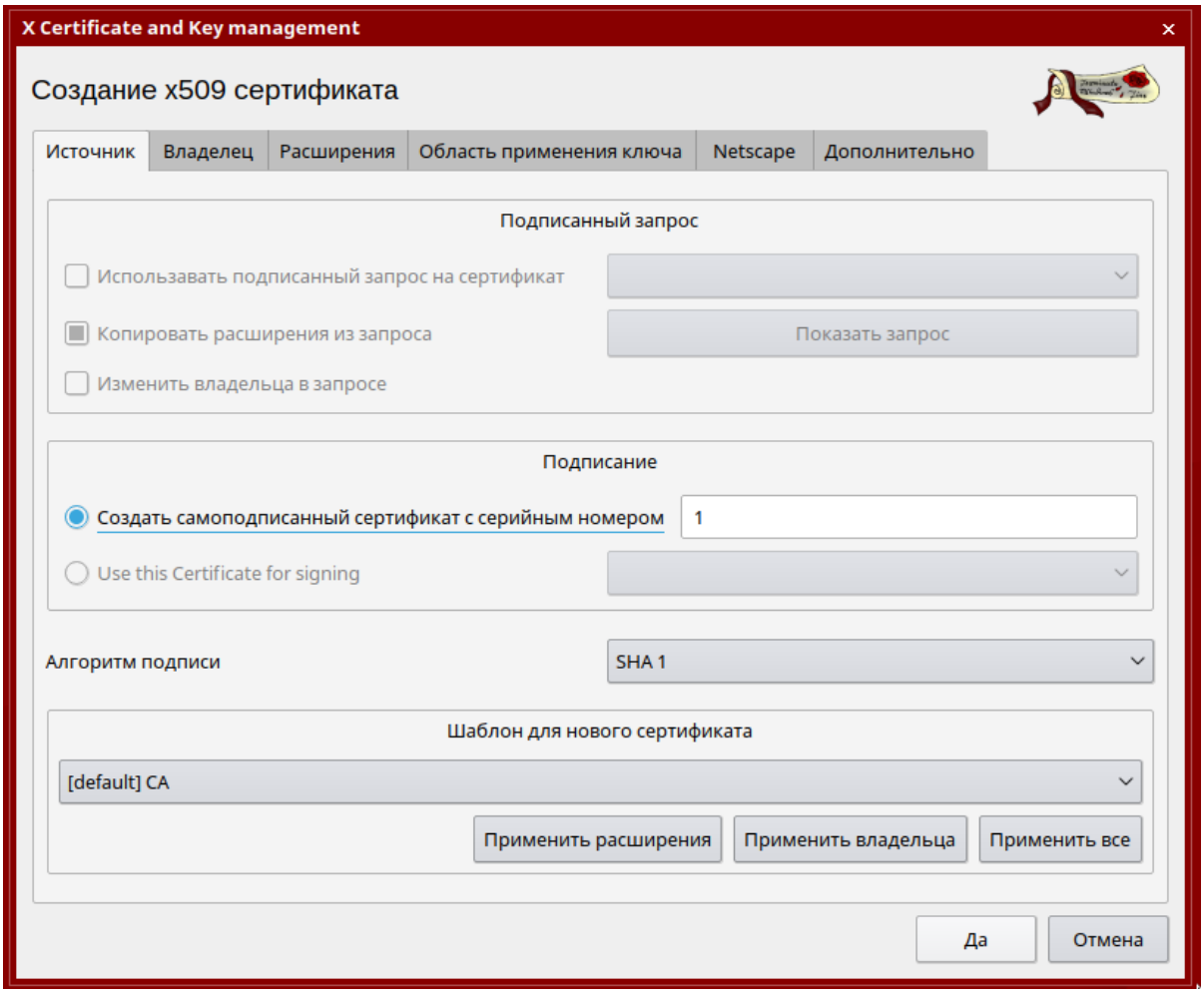
(Ctrl+N)



: " " " ", CAkey, Keytype RSA, Keysize 2048 bit.



: "" " " :


X Certificate and Key management
Создание x509 сертификата
Источник
Владелец
Расширения
Область применения ключа
Netscape
Дополнительно
Подписанный запрос
Использавать подписанный запрос на сертификат
Копировать расширения из запроса
Показать запрос
Изменить владельца в запросе
Подписание
Создать самоподписанный сертификат с серийным номером
1
Use this Certificate for signing
Алгоритм подписи
SHA 1
Шаблон для нового сертификата
[default] CA
Применить расширения
Применить владельца
Применить все
Да
Отмена

X Certificate and Key management

Создание x509 сертификата

Источник | Владелец | Расширения | Область применения ключа | Netscape | Дополнительно

Distinguished name

Внутреннее имя	CA	organizationName	Rusbitech
countryName	RU	organizationalUnitName	Astralinux
stateOrProvinceName	Moscow	commonName	CA
localityName	Moscow	emailAddress	CA@astra.rbt

Тип	Содержание

Добавить

Удалить

Закрытый ключ

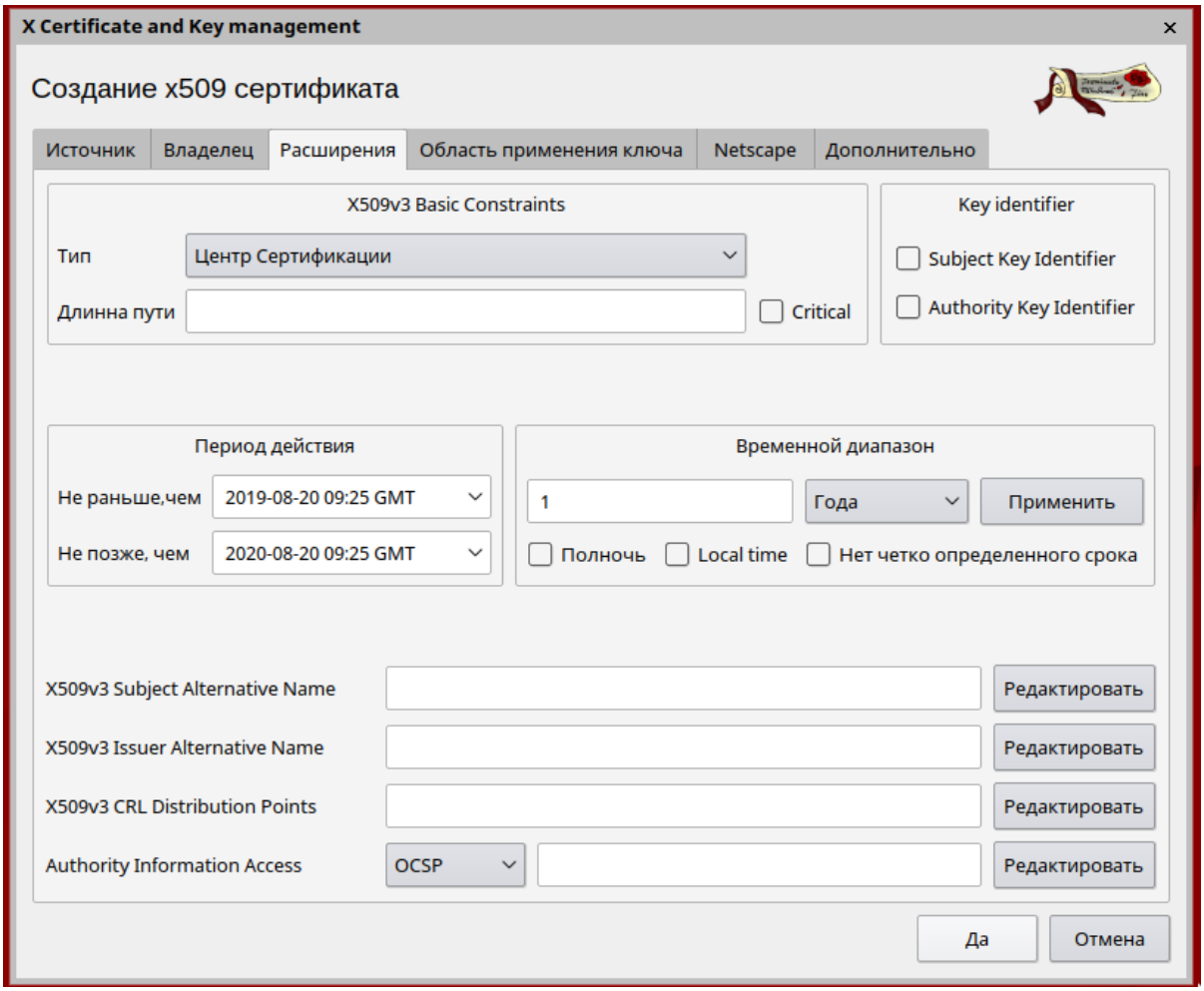
CAkey (RSA:2048 bit)

☐ Отображать уже использованные ключи

Создать новый ключ

Да

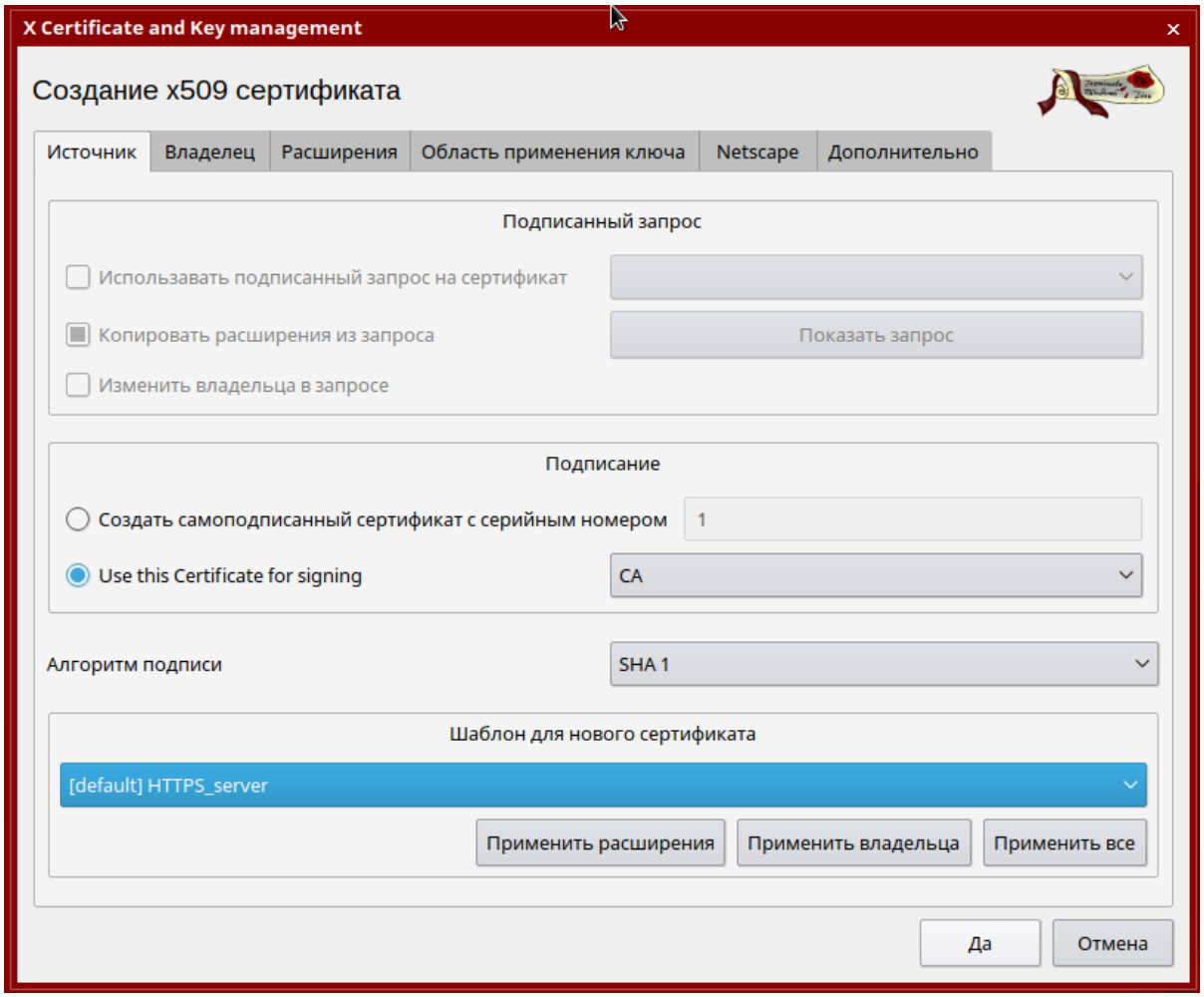
Отмена



OpenVPN

OpenVPN: " " " ", Openvpnkey, *Keytype* - RSA, *Keysize* - 2048 bit.

: "" " " :


X Certificate and Key management
Создание x509 сертификата
Источник
Владелец
Расширения
Область применения ключа
Netscape
Дополнительно
Подписанный запрос
Использавать подписанный запрос на сертификат
Копировать расширения из запроса
Показать запрос
Изменить владельца в запросе
Подписание
Создать самоподписанный сертификат с серийным номером
1
Use this Certificate for signing
CA
Алгоритм подписи
SHA 1
Шаблон для нового сертификата
[default] HTTPS_server
Применить расширения
Применить владельца
Применить все
Да
Отмена

X Certificate and Key management

Создание x509 сертификата

Источник | Владелец | Расширения | Область применения ключа | Netscape | Дополнительно

Distinguished name

Внутреннее имя	Openvpn	organizationName	Rusbitech
countryName	RU	organizationalUnitName	Astralinux
stateOrProvinceName	Moscow	commonName	Openvpn
localityName	Moscow	emailAddress	Openvpn@astra.rbt

Тип	Содержание

Добавить

Удалить

Закрытый ключ

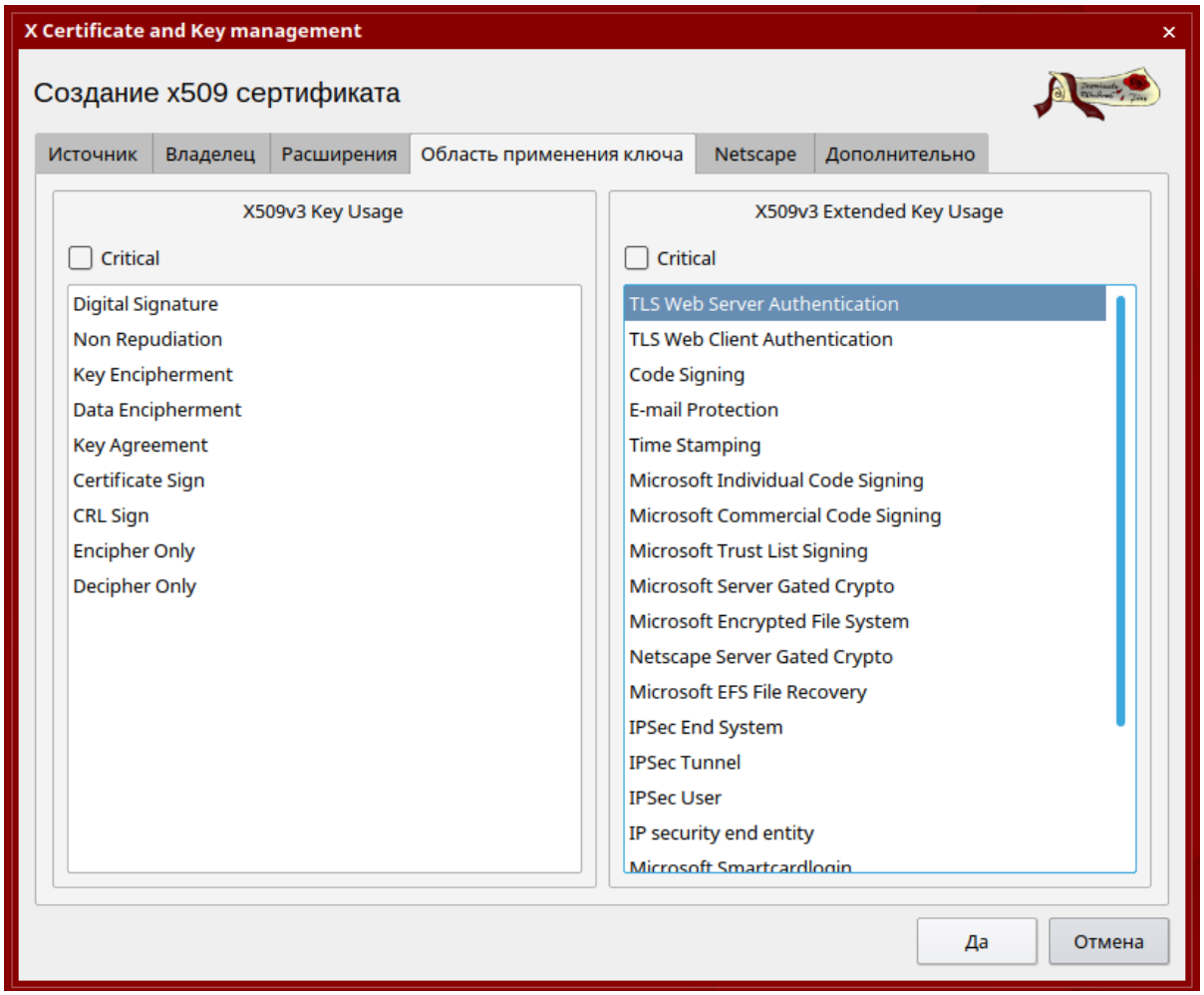
Openvpnkey (RSA:2048 bit)

Отображать уже использованные ключи

Создать новый ключ

Да

Отмена

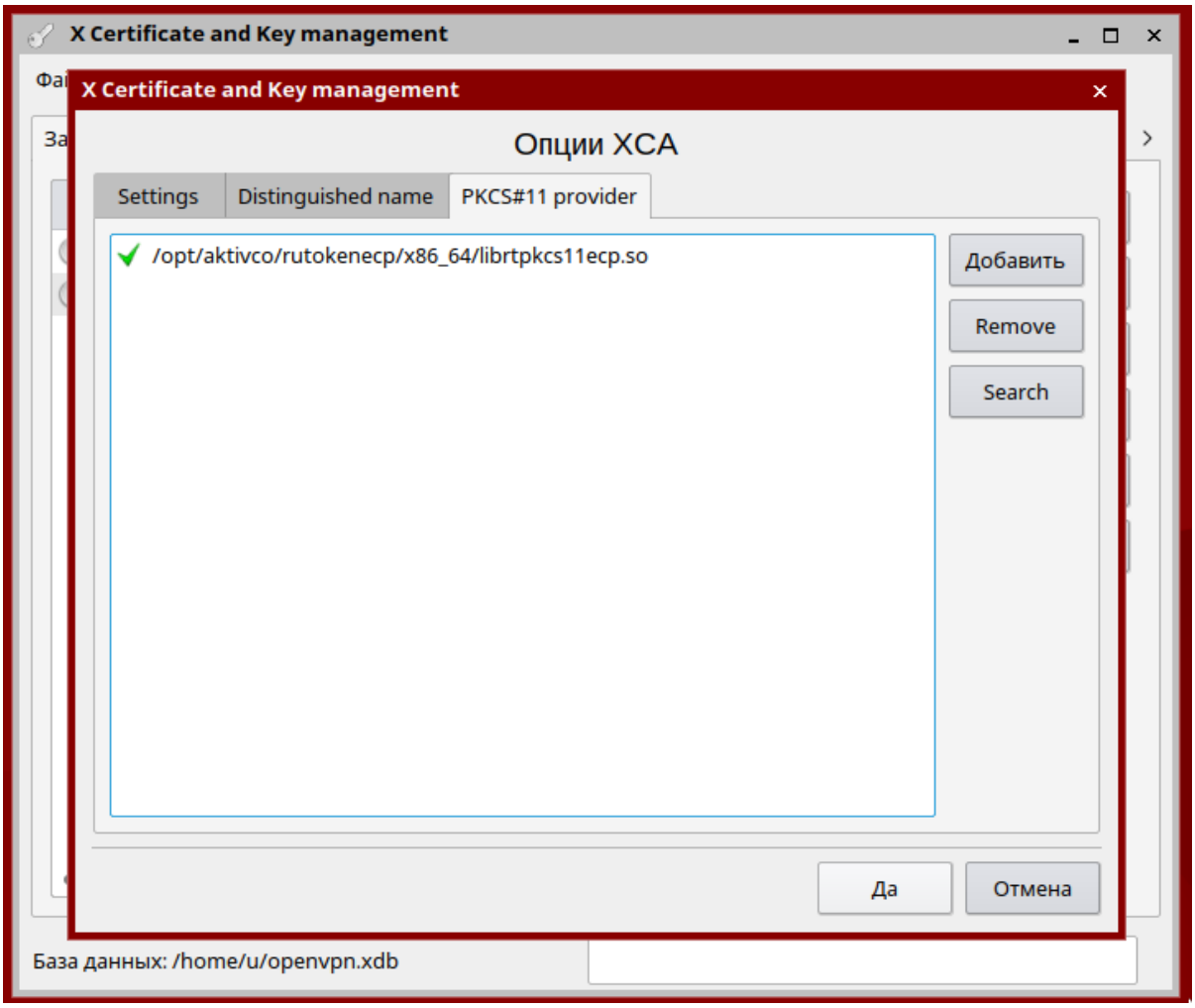


---

pkcs#11

, XCA PKCS#11 .

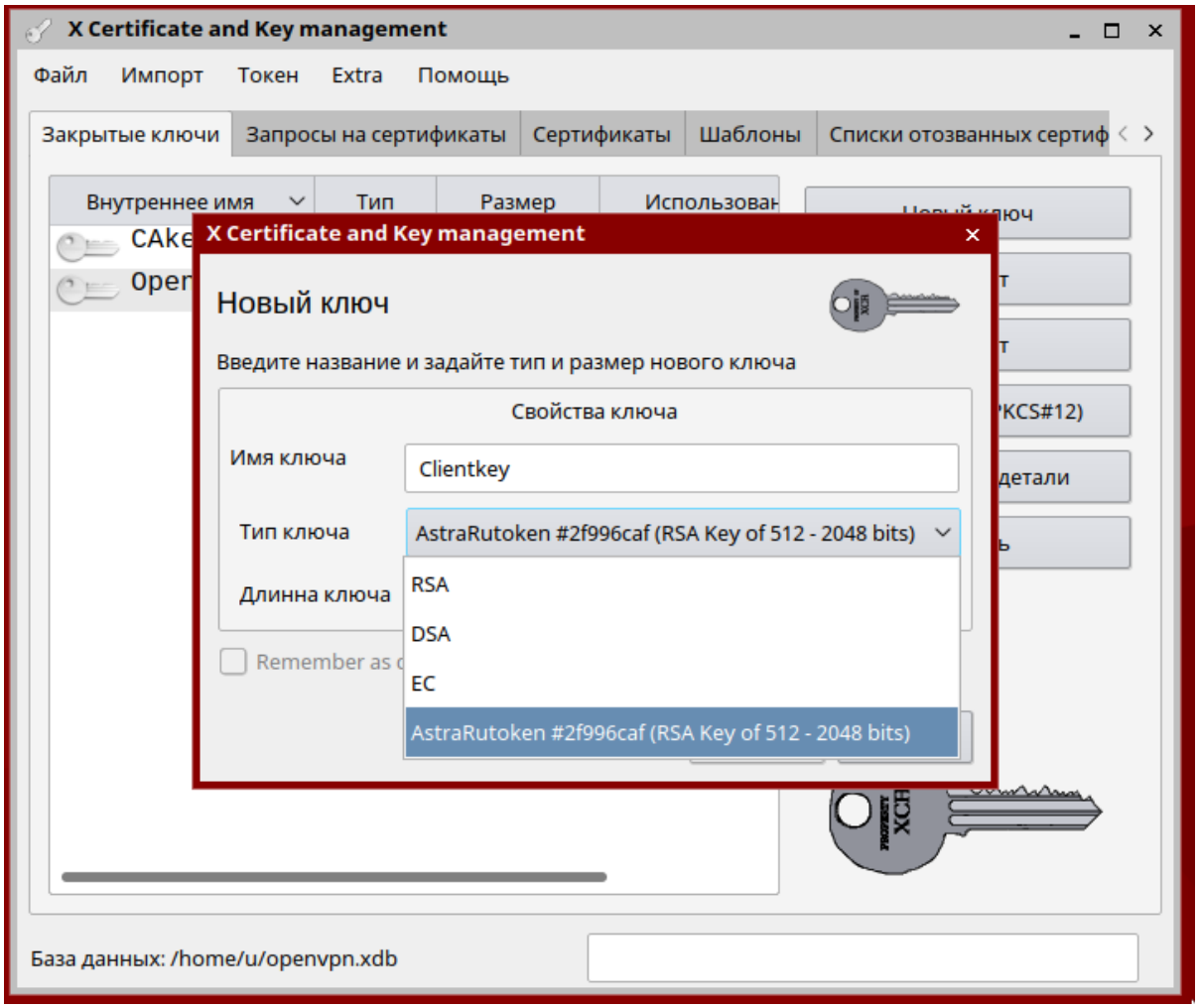
: ***PKCS#11 provider*** ***""*** *pkcs11(/opt/aktivco/rutokenecp/x86_64/librtpkcs11ecp.so)*

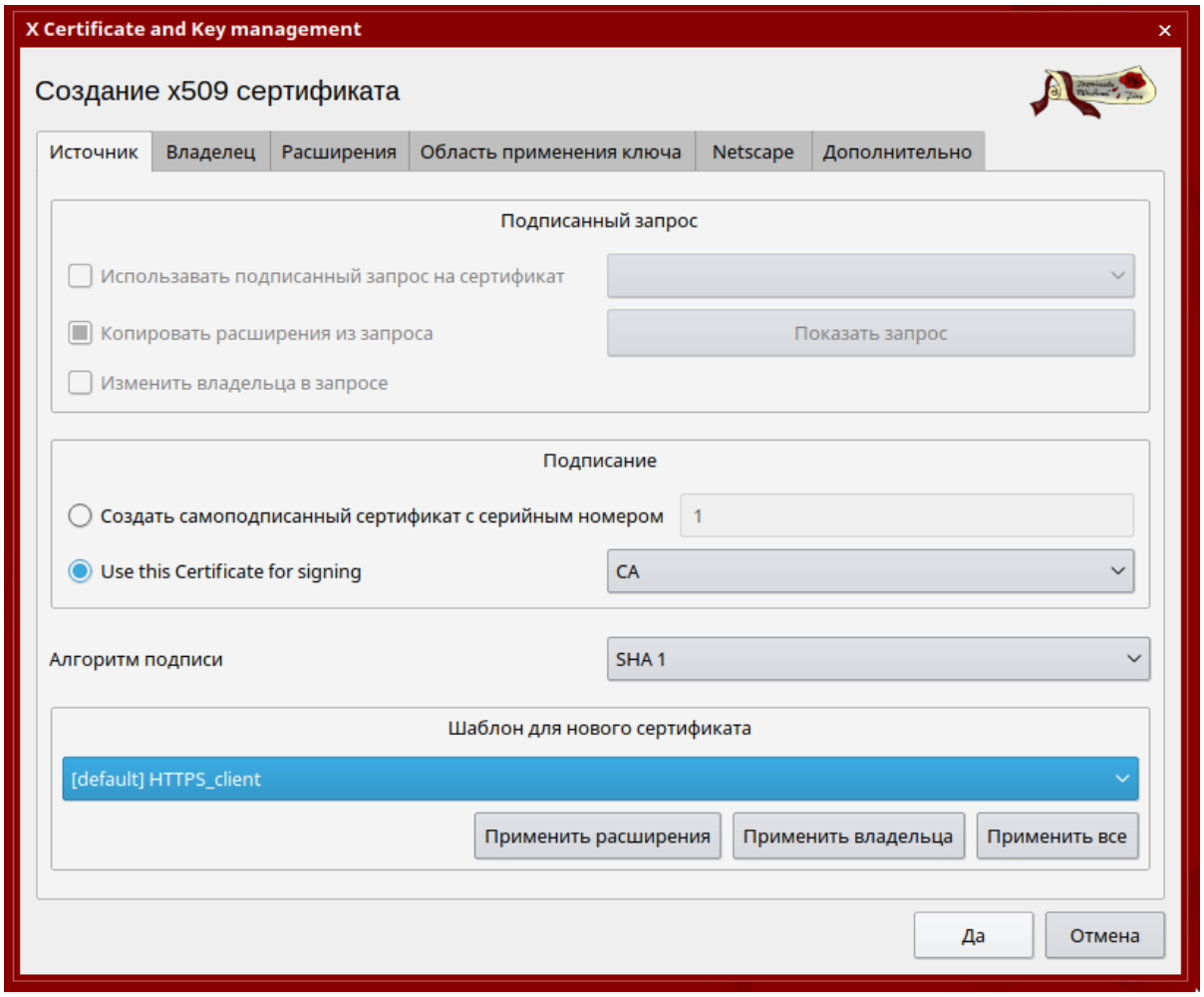


XCA:

« » : " " " " *Clientkey, Keytype - RSA(!) , Keysize - 2048 bit.*

PIN-.


X Certificate and Key management
Файл
Импорт
Токен
Extra
Помощь
Закрытые ключи
Запросы на сертификаты
Сертификаты
Шаблоны
Списки отозванных сертиф
Внутреннее имя
Тип
Размер
Использован
CAke
Open
Новый ключ
X Certificate and Key management
Новый ключ
Введите название и задайте тип и размер нового ключа
Свойства ключа
Имя ключа
Clientkey
Тип ключа
AstraRutoken #2f996caf (RSA Key of 512 - 2048 bits)
Длинна ключа
RSA
DSA
EC
AstraRutoken #2f996caf (RSA Key of 512 - 2048 bits)
Remember as
PKCS#12)
детали
База данных: /home/u/openvpn.xdb


X Certificate and Key management
Создание x509 сертификата
Источник
Владелец
Расширения
Область применения ключа
Netscape
Дополнительно
Подписанный запрос
Использавать подписанный запрос на сертификат
Копировать расширения из запроса
Показать запрос
Изменить владельца в запросе
Подписание
Создать самоподписанный сертификат с серийным номером
1
Use this Certificate for signing
CA
Алгоритм подписи
SHA 1
Шаблон для нового сертификата
[default] HTTPS_client
Применить расширения
Применить владельца
Применить все
Да
Отмена

X Certificate and Key management

Создание x509 сертификата

Источник | Владелец | Расширения | Область применения ключа | Netscape | Дополнительно

Distinguished name

Внутреннее имя	Client	organizationName	Rusbitech
countryName	RU	organizationalUnitName	Astralinux
stateOrProvinceName	Moscow	commonName	Client
localityName	Moscow	emailAddress	Client@astra.rbt

Тип	Содержание

Добавить

Удалить

Закрытый ключ

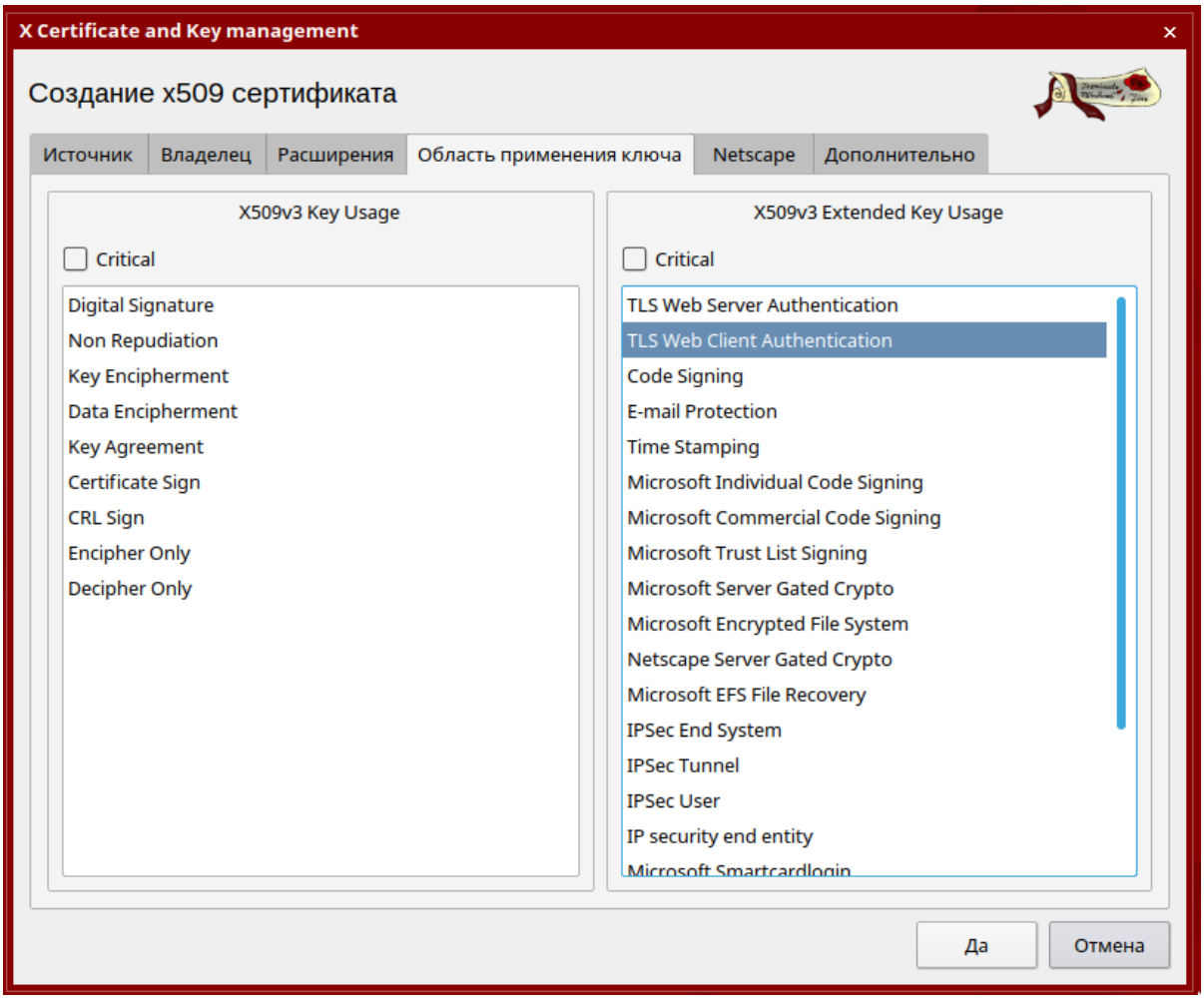
Clientkey (Токен RSA:2048 bit)

☐ Отображать уже использованные ключи

Создать новый ключ

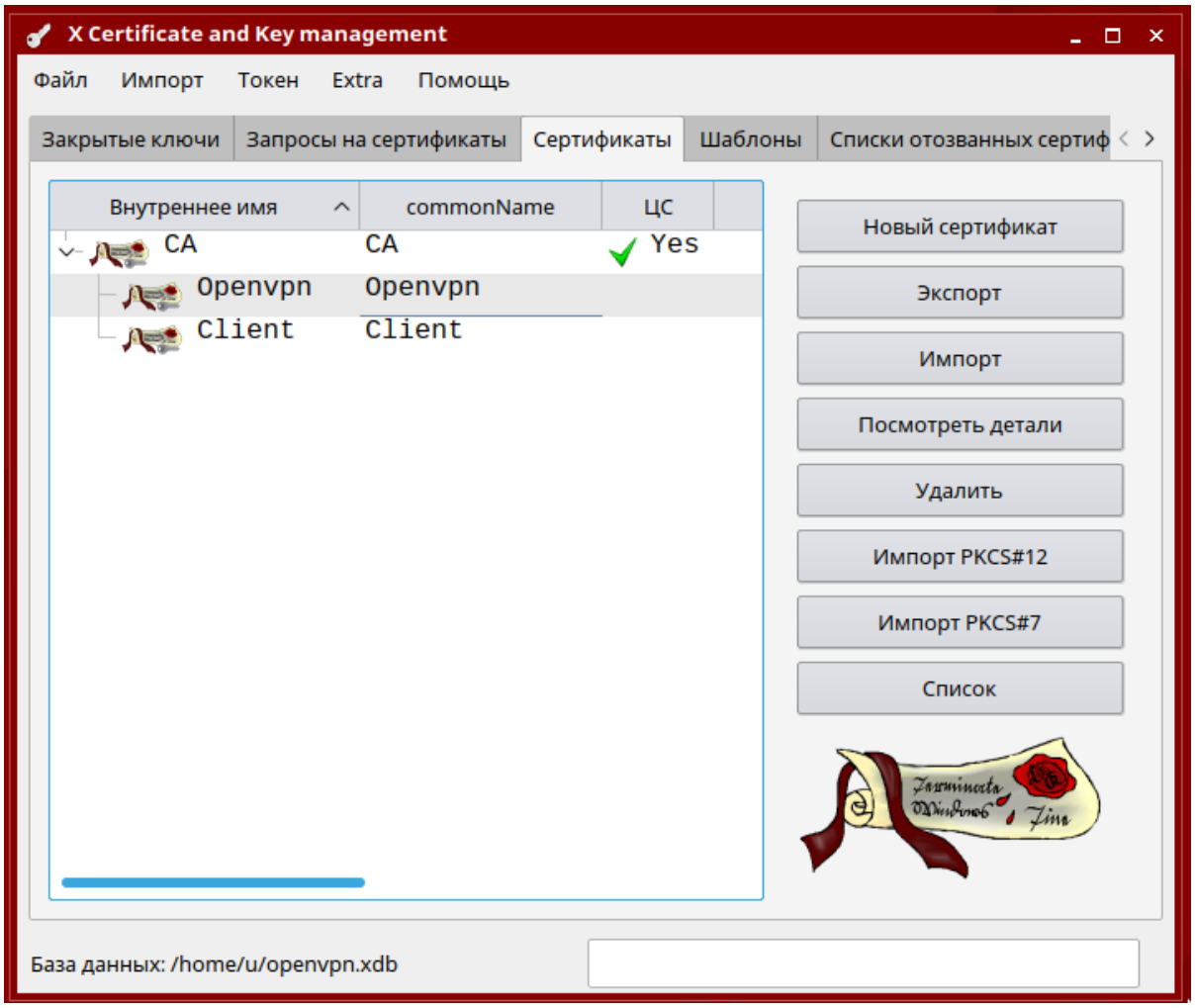
Да

Отмена



XCA , «» PIN-.

CA.crt, Openvpn.crt openvpn.pem (,) .



OpenVPN

openvpn Astra Linux, .

- , :
  - **fly-admin-openvpn-server**
  - **astra-openvpn-server**
-

fly-admin-openvpn-server astra-openvpn-server libgost-astra, .

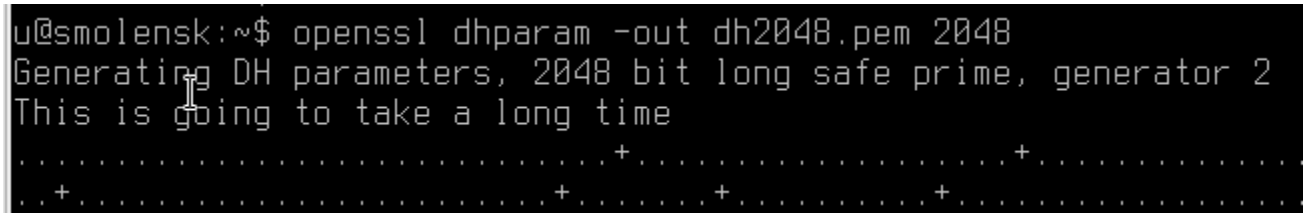
OpenVPN:

```
sudo apt-get install fly-admin-openvpn-server
```

DH (Diffie Hellman)

Diffie Hellman (-) openssl:

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



2048 , 4096.

, , .

,

OpenVPN:

```
nano openvpn.conf
```

C :

```
    port 1194
proto tcp
dev tap

ca /home/u/openvpn/CA.crt
cert /home/u/openvpn/Openvpn.crt
key /home/u/openvpn/Openvpnkey.pem
dh /home/u/openvpn/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
```

client		, (, ,).
dev	tap tun	. TUN — OSI, IP-. TAP — Ethernet OSI, Ethernet. OpenVPN , , tun. TAP , DH CP.

dev-node		Windows , . , OpenVPN.
proto	udp tcp	, . , UDP, .
remote	VPN -	, , , OpenVPN . .
remote-random		remote, , .
resolv-retry	infinite	, . , . infinite — .
nobind		.
user		(UNIX-).
group		(UNIX-).
persist-key		OpenVPN.
persist-tun		OpenVPN.
http-proxy		- .
http-proxy-retry		-, .
http-proxy-timeout		, -.
mute-replay-warnings		. .
ca		. .
cert		. .
key		. .
dh		Diffie-Hellman (-).
remote-cert-tls		mitm , .
tls-client		, TLS.
tls-auth	ta.key 1	TLS.
float		IP- , .
keepalive	1 2	1 2 , .
cipher		. : AES-256-CBC, AES-128-CBC, BF-CBC, DES-EDE3-CBC.
comp-lzo		.
verb	0 9	. 0 .
mute		- .
auth-user-pass		, . , , .
ipchange		IP.
connect-retry		, .

connect-retry-max		, .
shaper		.
tun-mtu		MTU.
status		.
log		-.

OpenVPN openvpn --help

OpenVPN

OpenVPN

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

```
root@smolensk:/home/u/openvpn# openvpn --config openvpn.conf
Mon Jun  8 12:52:27 2020 OpenVPN 2.4.5 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Mar  4 2018
Mon Jun  8 12:52:27 2020 library versions: OpenSSL 1.1.1d  10 Sep 2019, LZO 2.08
Mon Jun  8 12:52:27 2020 Diffie-Hellman initialized with 2048 bit key
Mon Jun  8 12:52:27 2020 TUN/TAP device tap0 opened
Mon Jun  8 12:52:27 2020 TUN/TAP TX queue length set to 100
Mon Jun  8 12:52:27 2020 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Mon Jun  8 12:52:27 2020 /sbin/ip link set dev tap0 up mtu 1500
Mon Jun  8 12:52:27 2020 /sbin/ip addr add dev tap0 10.0.0.1/24 broadcast 10.0.0.255
Mon Jun  8 12:52:27 2020 Could not determine IPv4/IPv6 protocol. Using AF_INET
Mon Jun  8 12:52:27 2020 Socket Buffers: R=[131072->131072] S=[16384->16384]
Mon Jun  8 12:52:27 2020 Listening for incoming TCP connection on [AF_INET][undef]:1194
Mon Jun  8 12:52:27 2020 TCPv4_SERVER link local (bound): [AF_INET][undef]:1194
Mon Jun  8 12:52:27 2020 TCPv4_SERVER link remote: [AF_UNSPEC]
Mon Jun  8 12:52:27 2020 MULTI: multi_init called, r=256 v=256
Mon Jun  8 12:52:27 2020 IFCONFIG POOL: base=10.0.0.2 size=253, ipv6=0
Mon Jun  8 12:52:27 2020 IFCONFIG POOL LIST
Mon Jun  8 12:52:27 2020 MULTI: TCP INIT maxclients=1024 maxevents=1028
Mon Jun  8 12:52:27 2020 Initialization Sequence Completed
```

⚠ "" / /home

, :

```
sudo apt install pcscd libpcsclite1 libccid
```

librtpkcs11ecp.so

```
sudo dpkg -i librtpkcs11ecp_1.8.2.0-1_amd64.deb
```

OpenVPN

OpenVPN:

```
sudo apt install openvpn
```

() /home/client/openvpn/CA.crt

```
nano openvpnclient.conf
```

C :

```
    client
dev tap
proto tcp
remote 192.168.xxx.xxx 1194
resolv-retry infinite
nobind
persist-key
persist-tun

ca /home/client/openvpn/CA.crt
pkcs11-providers /usr/lib/librtpkcs11ecp.so
pkcs11-id 'Aktiv\x20Co\x2E/Rutoken\x20ECP/2f996caf/Rutoken\x20ECP\x20\x3Cno\x20label\x3E/3C9F594E0994420E'

pkcs11-pin-cache 300

comp-lzo
verb 3
```

remote ip- VPN-

pkcs11-providers PKCS#11 .

`pkcs11-id` ID , . ID :

```
sudo openvpn --show-pkcs11-ids /usr/lib/librtpkcs11ecp.so
```

```
u@smolensk16:~/openvpn$ sudo openvpn --show-pkcs11-ids /usr/lib/librtpkcs11ecp.so

The following objects are available for use.
Each object shown below may be used as parameter to
--pkcs11-id option please remember to use single quote mark.

Certificate
       DN:             C=RU, ST=Moscow, L=Moscow, O=Rusbitech, OU=Astralinux, CN=Client, emailAddress=Client@astra.rbt
       Serial:         03
       Serialized id:  Aktiv\x20Co\x2E/Rutoken\x20ECP/2f996caf/Rutoken\x20ECP\x20\x3Cno\x20label\x3E/3C9F594E0994420E
u@smolensk16:~/openvpn$
```

VPN-

VPN-:

```
sudo openvpn --config /home/client/openvpnclient.conf
```

PIN- .

```
shuhrat@astralinux:~/readyfor/vpn$ sudo openvpn --config openvpnclient.conf
Mon Jun  8 13:36:23 2020 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [L
AEAD] built on Feb 20 2019
Mon Jun  8 13:36:23 2020 library versions: OpenSSL 1.1.1d  10 Sep 2019, LZO 2
Mon Jun  8 13:36:23 2020 PKCS#11: Adding PKCS#11 provider '/usr/lib/librtpkcs
Mon Jun  8 13:36:23 2020 WARNING: No server certificate verification method h
howto.html#mitm for more info.
NEED-OK|token-insertion-request|Please insert RutokenAstra token: ****
```