

# Создание сертификатов

## Рабочие директории

```
/etc/openvpn/ccd - директория с конфигурацией пользователей  
/etc/openvpn/easy-rsa/pki/issued - директория для подписанных сертификатов пользователей  
/etc/openvpn/easy-rsa/pki/private - директория для частных ключей пользователей  
/etc/openvpn/easy-rsa/easyrsa - утилита для генерации сертификатов
```

## Генерация сертификатов

### 1. Запускаем утилиту easyrsa

```
cd /etc/openvpn/easy-rsa/  
./easyrsa gen-req fursov.m nopass
```

```
[root@petr easy-rsa]# ./easyrsa gen-req fursov-m nopass  
  
Note: using Easy-RSA configuration from: ./vars  
Generating a 2048 bit RSA private key  
.....+++  
.....+++  
writing new private key to '/etc/openvpn/easy-rsa/pki/private/fursov-m.key.OiQYuCuTom'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Common Name (eg: your user, host, or server name) [fursov-m]:
```

В процессе работы команды, будет задан вопрос о Common Name (основного имени сертификата).

Можно просто оставить пустым и **нажать Enter**.

После чего будут сгенерированы два файла **\*.req** – запрос и **\*.key** – закрытый ключ. Так же будут выведены пути, куда положила их программа.

## 2. Подписание запроса центром сертификации

Когда запрос сформирован, его необходимо подписать командой

```
./easymrsa sign-req client fursov-m
```

```
[root@petr easy-rsa]# ./easymrsa sign-req client fursov-m
Note: using Easy-RSA configuration from: ./vars

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 3650 days:

subject=
  commonName                = fursov-m

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: |
```

У вас уточнят, действительно-ли вы уверены, что вы выпускаете сертификат для данного пользователя.

Необходимо напечатать слово **yes** и нажать Enter

После подтверждения, будет запрошен пароль от СА, для подписания закрытым ключом и выпуска сертификата

```
Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from ./openssl-1.0.cnf
Enter pass phrase for /etc/openvpn/easy-rsa/pki/private/ca.key:
```

Вбиваем пароль получаем подписанный сертификат.

```
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'fursov-m'
Certificate is to be certified until Dec 25 16:01:42 2034 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openssl/easy-rsa/pki/issued/fursov-m.crt

[root@petr easy-rsa]# |
```

---

Revision #7

Created 25 March 2025 11:05:07 by admin\_vy

Updated 25 March 2025 11:54:09 by admin\_vy