

Создание сертификата локального сервера

Для создания сертификата требуется программа [OpenSSL](#). Скачать сборку для *Windows* можно [здесь](#).

Создание доверенного центра сертификации

- Создание файла случайных чисел

```
openssl rand -out <Directory-Path>/<Random-Number-Filename> <Size-to-seed-the-Random-Number>
```

- Создание секретного ключа сертификата центра сертификации

```
openssl genrsa -rand <Directory-Path>/<Random-Number-Filename> -out <Directory-Path>/<CA-Key-Filename> <Key-Strength: Number-of-bits>
```

- Создание сертификата центра сертификации

```
openssl req -x509 -new -key <Directory-Path>/<CA-Key-Filename> -out <Directory-Path>/<CA-Cert-Filename> -days <Number-of-Days>
```

■ В папке с программой **GOSTunnel** поставляются файлы доверенного центра сертификации *localhost* по пути `certs/{rand.pem,localhost_ca.crt,localhost_ca.key}`.

Создание клиентского сертификата

- Создание секретного ключа сертификата клиента

```
openssl genrsa -rand <Directory-Path>/<Random-Number-Filename> -out <Directory-Path>/<Client-Certificate-Key-Filename> <Key-Strength-in-Bits>
```

- Создание запроса на получение сертификата

```
openssl req -new -out <Directory-Path>/<Client-CSR-Filename> -key <Directory-Path>/<Client-Certificate-Key-Filename>
```

- Создание и подпись сертификата клиента

```
openssl x509 -req -in <Directory-Path>/<Client-Certificate-Request-Filename> -out <Directory-Path>/<Client-Certificate-Filename> -CAkey <Directory-Path>/<CA-Key-Filename> -CA <Directory-Path>/<CA-Cert-Filename> -days <Number-of-Days> -CAcreateserial -Cserial serial
```