Для создания сертификата и закрытого ключа сервера, необходимо выполнить следующие шаги:

Сгенерировать закрытый ключ сервера:

openssl genrsa -out server.key 2048

Эта команда сгенерирует закрытый ключ длиной 2048 бит и сохранит его в файле server.key.

Создать запрос на сертификат:

openssl req -new -key server.key -out server.csr

Эта команда создаст запрос на сертификат для сервера с использованием закрытого ключа server.key и сохранит его в файле server.csr. Во время выполнения команды вам будет задано несколько вопросов, включая информацию об имени хоста и организации.

Подписать сертификат:

openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

Эта команда подпишет запрос на сертификат server.csr с использованием закрытого ключа server.key и создаст самоподписанный сертификат сроком на 365 дней, сохраняя его в файле server.crt.

Для создания самоподписанного сертификата клиента и его заверения, необходимо выполнить следующие шаги:

Сгенерировать закрытый ключ клиента:

openssl genrsa -out client.key 2048

Эта команда сгенерирует закрытый ключ длиной 2048 бит и сохранит его в файле client.key.

Создать запрос на сертификат:

openssl req -new -key client.key -out client.csr

Эта команда создаст запрос на сертификат для клиента с использованием закрытого ключа client.key и сохранит его в файле client.csr. Во время выполнения команды вам будет задано несколько вопросов, включая информацию об имени хоста и организации.

Подписать сертификат клиента:

openssl x509 -req -days 365 -in client.csr -CA server.crt -CAkey server.key -set\_serial 01 -out ca-certificates.crt

Эта команда подпишет запрос на сертификат client.csr с использованием закрытого ключа сервера server.key и самоподписанный сертификат сервера server.crt, создавая заверенный сертификат клиента сроком на 365 дней, сохраняя его в файле ca-certificates.crt.

=================================

"server.crt" и "server.key" - это файлы сертификата и закрытого ключа сервера. Они используются для создания SSL/TLS соединения между сервером и клиентом.

"ca-certificates.crt" - это файл, содержащий сертификаты доверенных центров сертификации (Certificate Authority, CA), которые используются клиентом для проверки сертификата сервера. Этот файл обычно предустанавливается в операционной системе, и клиентские приложения используют его для проверки подлинности сертификата сервера. Если сертификат сервера не был подписан одним из доверенных центров сертификации, то клиент может получить предупреждение об отсутствии доверия к сертификату.