**Создать Root CA (сделано один раз)**

**Создать корневой ключ**

**Внимание:** это ключ, используемый для подписи запросов на сертификат, любой, кто владеет этим, может подписывать сертификаты от вашего имени. Так что держите его в надежном месте!

openssl genrsa -des3 -out rootCA.key 4096

Если вы хотите, чтобы ключ не был защищен паролем, просто удалите -des3опцию

**Создать и самостоятельно подписать корневой сертификат**

openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.crt

Здесь мы использовали наш корневой ключ для создания корневого сертификата, который должен распространяться на всех компьютерах, которые должны нам доверять.

**Создать сертификат (сделано для каждого сервера)**

Эту процедуру необходимо выполнить для каждого сервера / устройства, которым требуется доверенный сертификат от нашего ЦС.

**Создать ключ сертификата**

openssl genrsa -out mydomain.com.key 2048

**Создать подпись (csr)**

В запросе на подпись сертификата вы указываете детали для сертификата, который хотите сгенерировать. Этот запрос будет обработан владельцем корневого ключа (в данном случае вы его создаете ранее) для генерации сертификата.

**Важно:** обратите внимание, что при создании запроса на подпись важно указать Common Nameпредоставление IP-адреса или доменного имени для службы, в противном случае сертификат не может быть проверен.

Я опишу здесь два способа

**Метод А (Интерактивный)**

Если вы сгенерируете csr таким способом, openssl задаст вам вопросы о сертификате, который необходимо сгенерировать, например, сведения об организации и Common Name(CN), который является веб-адресом, для которого вы создаете сертификат, например mydomain.com.

openssl req -new -key mydomain.com.key -out mydomain.com.csr

**Метод Б (один вкладыш)**

Этот метод генерирует тот же вывод, что и метод A, но он подходит для использования в вашей автоматизации :).

openssl req -new -sha256 -key mydomain.com.key -subj "/C=US/ST=CA/O=MyOrg, Inc./CN=mydomain.com" -out mydomain.com.csr

Если вам нужно передать дополнительную конфигурацию, вы можете использовать этот -configпараметр, например, здесь я хочу добавить альтернативные имена в мой сертификат.

openssl req -new -sha256 \

-key mydomain.com.key \

-subj "/C=US/ST=CA/O=MyOrg, Inc./CN=mydomain.com" \

-reqexts SAN \

-config <(cat /etc/ssl/openssl.cnf \

<(printf "\n[SAN]\nsubjectAltName=DNS:mydomain.com,DNS:www.mydomain.com")) \

-out mydomain.com.csr

**Проверьте содержание CSR**

openssl req -in mydomain.com.csr -noout -text

**Создайте сертификат, используя mydomaincsr и ключ вместе с корневым ключом CA**

openssl x509 -req -in mydomain.com.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out mydomain.com.crt -days 500 -sha256

**Проверьте содержание сертификата**

openssl x509 -in mydomain.com.crt -text -noout