Self-Signed Certificate Generation

In order to obtain a valid self-signed certificate for testing purposes we should perform the following steps:

A. **Generation of CA certificate**
B. **Generation of Server certificate**

The CA certificate will sign our server certificate, ensuring that browser can ensure its validity.

CA Certificate generation:

For first thing we generate a key for CA certificate

$ openssl genrsa -aes256 -out ca.key 2048

After key generation we must generate a CSR (Certificate Signing Request)

$ openssl req -new -key ca.key > ca.csr

Once we generated both files, we could generate the certificate of CA from these

$ openssl x509 -req -days 100 -trustout -signkey ca.key < ca.csr > ca.cert

Server certificate generation:

First of all, we generate a server key

$ openssl genrsa -aes256 -out server.key 2048

Generation of CSR for server

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

Generation of server certificate from CA, valid for 100 days

$ openssl x509 -req -days 100 -CA ca.cert -CAkey ca.key -set_serial 1 < server.csr > server.cert