**Self‐Signed Certificate Generation**

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

# Generation of CA certificate

1. **Generation of Server certificate**

# CA Certificate generation:

1. Generate a key for CA certificate

openssl genrsa -aes256 -out ca.key 2048

1. Generate a CSR (Certificate Signing Request)

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

1. Generate the certificate, valid for 100 days

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

**Server certificate generation:**

1. Generate a server key

openssl genrsa -aes256 -out server.key 2048

1. Generate a CSR for the server

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

1. Generate a 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