Create Root certificate

openssl req -x509 -sha256 -newkey rsa:4096 -keyout MyRoot\_prv.pem -nodes -out MyRoot.pem -days 365

generate private key and certificate of Alice

openssl genrsa -out alice\_prv.pem 2048

openssl req -new -key alice\_prv.pem -out alice.csr

get it signed by the root CA

openssl x509 -req -days 365 -in alice.csr -CA MyRoot.crt -CAkey MyRoot\_prv.pem -set\_serial 02 -out alice.crt

Extract CA root public key

openssl x509 -pubkey -noout -in MyRoot.crt > MyRoot\_pub.pem

Extract Alice’s public key

openssl x509 -pubkey -noout -in alice.crt > alice\_pub.pem

Extract Bob’s public key

openssl x509 -pubkey -noout -in bob.crt > bob\_pub.pem