**Emaan Bano (251-705783)**

**COMMANDS**

**Generate the Private Key (2048-bit RSA)**:

openssl genrsa -out private\_key.pem 2048

**Generate the Public Key**:

openssl rsa -in private\_key.pem -pubout -out public\_key.pem

**Generate the CSR** using the Private Key:

openssl req -new -key private\_key.pem -out certificate\_request.csr

**Create the Self-Signed Certificate** (valid for 365 days):

openssl x509 -req -days 365 -in certificate\_request.csr -signkey private\_key.pem -out self\_signed\_certificate.crt

**Create a Directory Structure for the CA**:

mkdir -p ~/myCA/newcerts

mkdir ~/myCA/private

mkdir ~/myCA/certs

touch ~/myCA/index.txt

echo 1000 > ~/myCA/serial

**Generate the CA's Private Key**:

openssl genrsa -out ~/myCA/private/ca\_key.pem 2048

**Generate the CA's Self-Signed Certificate** (valid for 3650 days):

openssl req -new -x509 -days 3650 -key ~/myCA/private/ca\_key.pem -out ~/myCA/certs/ca\_cert.pem

**Sign the CSR** to issue a certificate signed by your CA:

openssl x509 -req -in certificate\_request.csr -CA ~/myCA/certs/ca\_cert.pem -CAkey ~/myCA/private/ca\_key.pem -CAcreateserial -out signed\_cert.pem -days 365

**Verify the Signed Certificate** to ensure it is valid:

openssl verify -CAfile ~/myCA/certs/ca\_cert.pem signed\_cert.pem





