

## Generating Local CA and Certificates Using SSL

Since we don't have a certificate authority, we'll create a local CA and generate the necessary certificates for our setup. Follow these steps:

### 1. Create a Local CA

**Create a directory for certificates:**

```
mkdir certs  
cd certs
```

**Generate the CA private key:**

```
openssl genrsa -des3 -out ca.key 2048
```

Enter a passphrase with at least 4 characters. Remember this passphrase as it will be used in subsequent steps. I have use (1234)

### 2. Create a CA Signing Request

**Generate a Certificate Signing Request (CSR) for the CA:**

```
openssl req -new -key ca.key -out ca.csr -sha256
```

Enter the same passphrase chosen in the previous step.

Leave all other fields empty for simplicity.

### 3. Create the CA Root Certificate

**Create the CA root certificate, valid for 180 days:**

```
openssl x509 -req -in ca.csr -signkey ca.key -out ca-root.crt -days  
180 -sha256
```

Enter the passphrase when prompted.

### 4. Generate the Mosquitto Certificate Key

**Generate the private key for Mosquitto:**

```
openssl genrsa -out mosquitto.key 2048
```

## 5. Create a Certificate Signing Request for Mosquitto

Generate a CSR for Mosquitto using the private key:

```
openssl req -new -key mosquitto.key -out mosquitto.csr -sha256
```

When prompted for the “Common Name”, use `localhost` (or your DNS entry if applicable). All other fields can be left empty.

## 6. Create the Mosquitto Certificate

Generate the Mosquitto certificate, valid for 180 days, using the CSR and the CA root certificate:

```
openssl x509 -req -in mosquitto.csr -CA ca-root.crt -CAkey ca.key  
-CAcreateserial -out mosquitto.crt -days 180
```

## 7. Final Files

After completing these steps, you should have the following files in the `certs` directory:

- `ca-root.crt` – Certificate authority root certificate
- `ca.csr` – Certificate authority certificate signing request
- `ca.key` – Certificate Authority private key
- `mosquitto.crt` – Mosquitto certificate
- `mosquitto.csr` – Mosquitto certificate signing request
- `mosquitto.key` – Mosquitto private key

**Note:** Not all of these files are required for Mosquitto to run or for SSL message transmission, but they are essential for generating the necessary certificates.

**Important:** Change the folder name from `certs` to `certs_copy`