**Génération des clés et configuration du serveur Mosquitto avec sécurité TLS/SSL et authentification par utilisateur**

**1. Création de la clé CA pour le client**

**Commande :**

openssl genrsa -des3 -out ca.key 2048

**2. Création du certificat de l'Autorité de Certification (CA) à partir de la clé CA**

**Commande :**

openssl req -new -x509 -days 1833 -key ca.key -out ca.crt

**3. Création de la clé du broker sans chiffrement**

**Commande :**

openssl genrsa -out server.key 2048

**4. Création de la demande de certificat (CSR) pour le broker**

**Commande :**

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

**5. Création du certificat du broker**

**Commande :**

openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 360

**6. Création des utilisateurs pour Mosquitto**

### **Commande :**

mosquitto\_passwd -c /mosquitto\_passwd userclient

**Commande :**

mosquitto\_passwd /mosquitto\_passwd userbroker

7. **Abonnement à un Topic MQTT avec Mosquitto (via MQTTS)**

**Commande :**

sudo mosquitto\_sub -h 10.0.20.2 -p 8883 --cafile /etc/mosquitto/certs/ca.crt -u userclient -P ciel -t sensors/temperature