MQTT SSL client will need three certificates.(ca.crt / client.crt / client.key)
http://mosquitto.org/man/mosquitto-tls-7.html

The problem is that the `commonName` in your certificate does not match the hostname (in this case the IP address) you are connecting to. 1.1.3 did not verify this, and so was vulnerable to your server being impersonated.

Certificate Authority

Use ./generateCA.sh to create ca key and server certificate key

Generate a certificate authority certificate and key.

- openssl req -new -x509 -days <duration> -extensions v3_ca -keyout ca.key -out ca.crt

Server

Generate a server key.

- openssl genrsa -des3 -out server.key 2048

Generate a server key without encryption.

- openssl genrsa -out server.key 2048

Generate a certificate signing request to send to the CA.

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

Send the CSR to the CA, or sign it with your CA key:

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

Client

Generate a client key.

- openssl genrsa -des3 -out client.key 2048

Generate a certificate signing request to send to the CA.

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

Send the CSR to the CA, or sign it with your CA key:

- openssl x509 -req -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out client.crt -days <duration>

1. Start mosquitto server with SSL configuration
./mosquitto -c mosquitto.conf (IP cannot set to localhost or 127.0.0.1, must set to real IP)

2. Subscribe to listen certain topic, keyin client passwd

```
./mosquitto_sub -h 10.70.1.39 -p 8883 --cafile
/usr/local/Cellar/mosquitto/1.1.3/sbin/ca.crt --cert
/usr/local/Cellar/mosquitto/1.1.3/sbin/client.crt --key
/usr/local/Cellar/mosquitto/1.1.3/sbin/client.key -t "abc" -d
```

3. Publish to certain topic, keyin client passwd

```
./mosquitto_pub -h 10.70.1.39 -p 8883 --cafile
/usr/local/Cellar/mosquitto/1.1.3/sbin/ca.crt --cert
/usr/local/Cellar/mosquitto/1.1.3/sbin/client.crt --key
/usr/local/Cellar/mosquitto/1.1.3/sbin/client.key -t "abc" -m "hello hello" -d
```

------ mosquitto.conf ------

```
# Default listener
bind_address 10.70.1.81
port 8883
max_connections -1

# SSL/TLS support
require_certificate true
cafile /Users/sam_wang/mosquitto_key/ca.crt
capath /Users/sam_wang/mosquitto_key/
certfile /Users/sam_wang/mosquitto_key/Sams-MacBook-Air.local.crt
keyfile /Users/sam_wang/mosquitto_key/Sams-MacBook-Air.local.key
```