# Mosquitto SSL Configuration -MQTT TLS Security

Install openssl using : **sudo apt-get install openssl**

#### Step 1:

First create a key pair for the **CA**

Command is: **openssl genrsa -dsa3 -out ca.key 2048**

**Step 2:**

Now Create a certificate for the CA using the **CA key** that we created in step 1

Command is: **openssl req -new -x509 -days 1826 -key ca.key -out ca.crt**

#### Step 3:

Now we create a server key pair that will be used by the broker

Command is: **openssl genrsa -out server.key 2048**

#### Step 4:

Command is: **openssl req -new -out server.csr -key server.key**

#### Step 5:

Now we use the **CA key** to verify and sign the server certificate. This creates the **server.crt** file

Command is:  **openssl**

**Now you should have a few files inside the current folder. The important files to take notes are, ca.crt, server.cet, server.key**

#### Step 6:

Copy the files **ca.crt, serever.crt** and**server.key** to a folder under the mosquitto folder.

on Linux you should already have a **ca\_certificates** folder under **/etc/mosquitto/** and also a **certs** folder.

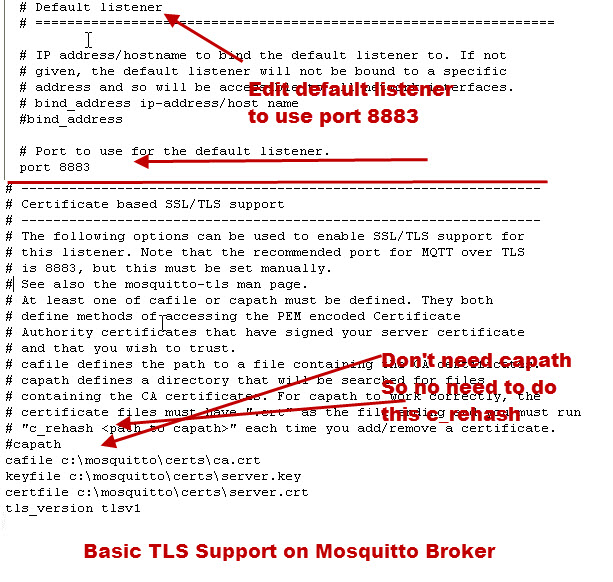
Use the **ca\_certificates** folder for the **CA certificate** and the **certs** folder for the s**erver certificate and key**.

#### Step 7:

Copy the **CA certificate file** **ca.crt** to the client.

**Step 8:**

Edit the mosquitto.conf file as shown:



#### Step 9 -Client Configuration:

Edit the client to tell it to use**TLS** and give it the path of the **CA certificate** file that you copied over.

Source : <http://www.steves-internet-guide.com/mosquitto-tls/>