Cifrado por TLS - Instalando certificados y claves

Requisitos del cliente

- Un certificado de la CA (certification authority) que firmó el certificado en el servidor Mosquitto.

Requisitos del servidor

- Certificado de la CA (certification authority) que firmó el certificado en el servidor Mosquitto
- Certificado del servidor firmado por la CA.
- Clave privada del servidor.

Creación e instalación de certificados y claves del servidor

Para crear estos certificados y claves utilizamos el software openssl.

1. Genere la clave de firma de la autoridad certificadora (CA) falsa
   `$ openssl genrsa -out ca.key 2048`
2. Genere una solicitud de firma de certificado para la CA falsa `$ openssl req -new -key ca.key -out ca-cert-request.csr -sha256`
   - Asigne a la organización un nombre como "Autoridad falsa" y no ingrese un nombre común (ya que su CA falsa en realidad no reside en un servidor con un nombre)
3. Cree el certificado raíz de la CA falsa
   `$ openssl x509 -req -in ca-cert-request.csr -signkey ca.key -out ca-root-cert.crt -days 365 -sha256`
4. Cree el par de claves del servidor mosquitto
   `$ openssl genrsa -out server.key 2048`
5. Cree un pedido de firma de certificado (Certificate Signing Request - CSR) usando la clave del servidor para enviárselo a la CA falsa para verificación de indentidad

   `$ openssl req -new -key server.key -out server-cert-request.csr -sha256`

   Déle a la organización un nombre como "MQTT Broker SA" y el *common name* que debería ser el nombre de dominio exacto que use para conectarse al *broker* MQTT.
6. Ahora actuando como la CA falsa, reciba el pedido del servidor para su firma. Ha verificado que el servidor es quien dice ser (un *broker* MQTT que opera en *localhost* o su FQDN), así que cree un nuevo certificado y fírmelo con todo el poder de su autoridad falsa.

`$ openssl x509 -req -in server-cert-request.csr -CA ca-root-cert.crt -CAkey ca.key -CAcreateserial -out server.crt -days 360`

Ya tiene todo lo que necesita. Haga las siguientes configuraciones de Mosquitto en `mosquitto.conf`:

```
listener 8883
cafile certs\ca-root-cert.crt
keyfile certs\server.key
certfile certs\server.crt
```

Asegúrese que paho-mqtt esté cargando el certificado raíz de la CA falsa.

```
client1.tls_set(ca_certs="ca-root-cert.crt")
```

De esta manera el cliente sabe que el certificado de mosquitto 'server.crt' está legítimamente firmado por una "autoridad real y de confianza" y no autofirmado y por lo tanto no confiable. Mosquitto y paho deberían ahora poder conectarse y comunicarse de froma segura.