Tworzenie nowego certyfikatu CA oraz generowanie certyfikatów dla klientów(modułów WiFi) i serwera MQTT

Komunikacja pomiędzy modułami WiFi zainstalowanymi w urządzeniach, a serwerem MQTT jest szyfrowana aby zapewnić bezpieczeństwo przesyłanych danych.
W tym celu serwer oraz każdy z klientów (modułów WiFi) musi posiadać własny klucz publiczny i prywatny, które będą służyły do nawiązywania bezpiecznego połączenia pomiędzy nimi. Dodatkowo unikalne zestawy kluczy prywatnych i publicznych na modułach WiFi pozwalają na autentykację modułów WiFi kiedy łączą się one do serwera MQTT.

Dzięki temu nie jest możliwe tak zwane spoofowanie modułów, czyli osoby trzecie nie są w stanie łączyć się do serwera MQTT podając się za moduły WiFi, co by im pozwoliło na tworzenie sztucznych wpisów w bazie danych, lub nawet przechwycenie danych pochodzących z prawdziwych urządzeń działających w systemie.

Pierwszym krokiem do stworzenia zestawów kluczy dla serwera i urządzeń było stworzenie kluczy prywatnych i publicznych dla tak zwanego CA(certificate authority), następnie został także stworzony dla niego certyfikat. Zostało to zrobione posługując się następującymi poleceniami:

```
#gen ca priv key
openssl genrsa -des3 -out ca.key 2048   # << with password
openssl genrsa -out ca.key 2048   # << without password
openssl req -new -x509 -days 3650 -extensions v3_ca -keyout ca.key -out ca.crt
```

Kolejnym krokiem było stworzenie kluczy prywatnych i publicznych dla serwera MQTT:

```
openssl genrsa -out server.key 2048   #generates priv key
openssl req -out server.csr -key server.key -new   #generate signing request
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days
1825
```

Na koniec wygenerowano klucze dla tworzonych dziesięciu modułów WiFi

```
openssl genrsa -out 10.key 2048
```

```
openssl req -out 10.csr -key 10.key -new
openssl x509 -req -in 10.csr -CA ../ca.crt -CAkey ../ca.key -CAcreateserial -out 10.crt -days 10950  #30 years
```

Klucze prywatne CA są przechowywane w bezpiecznym miejscu i zaszyfrowane, są one potrzebne i używane tylko w przypadku gdy trzeba stworzyć zestawy kluczy dla nowych modułów WiFi.

10 zestawów kluczy dla modułów WiFi zostało wgrane na 10 modułów WiFi które zostały stworzone.