Walther-Rathenau-Gewerbeschule Freiburg	**Projektarbeit** mqtt-Client (publisher) mit Temperatursensor und TLS	Fach:	Gruppe:
		25. Juni 2023	Seite **1**
		Name:	
		Klasse: FTI3T	
		Punkte:	Note:

1 Projektaufgabe(als Ersatz für eine Klassenarbeit)

1.1 Publisher, 1-Wire-Kernelmodule und libmosquitto

Es soll auf einem Raspberry-PI mit 1-Wire-Temperatursensor ein mqtt-Client als `Publisher` erzeugt werden. Der Quelltext soll in C unter Verwendung der Bibliothek *libmosquitto* geschrieben werden.
Der Temperatursensor soll über die Kernelmodule:

- `wire`
- `w1_gpio`
- `w1_therm`

ausgelesen werden.

1.2 Broker

Als Broker-Host soll der eigene Rechner (Schul-PC oder Notebook) verwendet werden. Als Broker-Software selbst soll `mosquitto` zum Einsatz kommen.

1.3 Subscriber

Um die Daten vom Broker abzuholen, soll `mosquitto_sub` auf dem gleichen Host verwendet werden, auf dem auch der Broker läuft. Die Verbindung zwischen Subscriber und Broker soll unverschlüsselt sein.

1.4 Transport Layer Security - tls

Da eine unverschlüsselte Kommunikation zwischen Publisher und Broker nicht mehr zeitgemäss ist, soll die Verbindung mit **tls** verschlüsselt werden.
Um die Sache nicht zu kompliziert zu machen, soll sich der Client *nicht* authentifizieren. D.h. die Kommunikation zwischen Client und Broker verläuft genau so, wie zwischen einem Webbrowser und einem Webserver bei Verwendung von https: auf der Clientseite ist *nur das Zertifikat der CA notwendig!*
Details hierzu siehe:

- `https://mosquitto.org/man/mosquitto-tls-7.html`
- `https://mosquitto.org/api/files/mosquitto-h.html#mosquitto_tls_set`

2 Test

Mit dem Kommando `tcpdump` kann die Kommunikation zwischen Publisher und Broker mitgeschnitten werden. Damit kann man zeigen, dass eben kein lesbarer Klartext mehr übertragen wird.

3 Dokumentation

Die Doku muss mit LaTeX erstellt werden. Wie man das macht, wird Thema einer Unterrichtsstunde sein. Es wird eine Vorlagedatei (template) zur Verfügung gestellt.

Bis das soweit ist, soll alles, was man so macht in einer Textdatei protokolliert werden.

Die Dokumentation soll eine kurze **selbstverfasste** Einleitung über die Funktion von TLS (Stichwort: hybride Verschlüsselung) enthalten.

Der Rest soll so knapp als möglich sein, aber jemanden, der die Aufgabe noch nicht bearbeitet hat in die Lage versetzen, eine TLS-Verschlüsselte Verbindung zwischen einem Publisher und einem Broker einzurichten und einen eigenen Publisher mit `libmosquitto` zu compilieren.