Smart Locker Protocol

Ver:1.0

Contents

[General preview 2](#_Toc196909301)

[MQTT topics 2](#_Toc196909302)

[Custom protocol 2](#_Toc196909303)

[Heartbeat 3](#_Toc196909304)

[Gateway 3](#_Toc196909305)

[Application to device commands 3](#_Toc196909306)

[Device to application events. 6](#_Toc196909307)

[Error codes 8](#_Toc196909308)

[Authentication 9](#_Toc196909309)

[Parameters 10](#_Toc196909310)

[Application settings struct. 10](#_Toc196909311)

[Application Extended1 settings struct. 10](#_Toc196909312)

[Password settings struct. 10](#_Toc196909313)

[FOTA settings struct. 10](#_Toc196909314)

# General preview

This protocol is used for communication between the locker gateway and the application. All packets are transmitted over the MQTT protocol.  
The current protocol version does not include session encryption, however this may be considered in future updates.  
Due to the complexity of the data structure, the custom protocol is encapsulated within the MQTT payload.

# MQTT topics

We have the following MQTT root topics:

|  |  |
| --- | --- |
| **Application to device** | **Device to application** |
| Locker/deviceID/commands/general | Locker /deviceID/events/general |
|  |  |
|  | Locker /deviceID/events/ heartbeat |
|  |  |
|  |  |

Note: deviceID – Unique 12 byte device identifier(24 character).

# Custom protocol

Custom protocol is wrapped in inside MQTT payload and has the following data structure:



**Timestamp**  – 4 byte timestamp value.

**Command** – 1 byte address-specific command .

**Length** – 1 byte optional payload length.

**Payload** – n byte optional payload.

# Heartbeat

Heartbeat machine helps to developer easily determine device online/offline states. Heartbeat data publish period is 180 seconds over Locker/deviceID/events/ heartbeat topic.

Heartbeat payload consists of real time data events. In our case we have Network source and Received signal strength value for cellular or WiFi networks in percentage (0 – 100%).



# Gateway

## Application to device commands













## Device to application events.













## Error codes

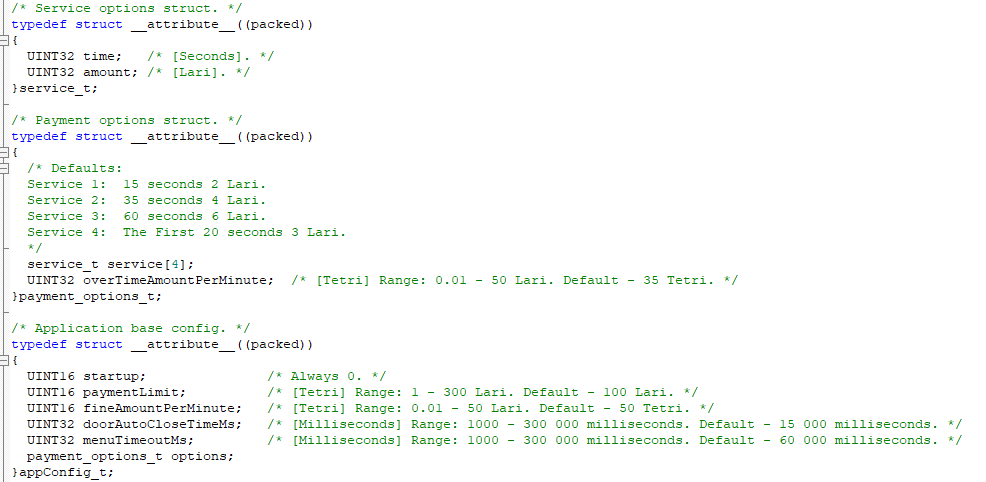


# Authentication

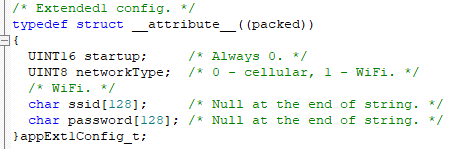
For enhancing a security level, we use MQTT based authentication. User field is empty, password filed contains hash password. Hash itself represents MD5 based hash algorithm, for hashing sensitive password. When device is new and is not registered into database it uses a default password (hash) attempting to open a connection to server. Server allows access on default password, stores all necessary data from device, generates new hash password followed publishing password hash packet back. (see command above)

# Parameters

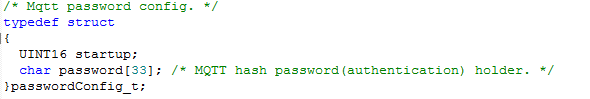
## Application settings struct.



## Application Extended1 settings struct.



## Password settings struct.



## FOTA settings struct.

