TAT240 Security info

Contents

In security section user can see SIM card security information, "Teltonika" Configurator Keyword security information and SSL/TLS Certificate information.

SIM Card

The state and status of currently connected SIM card can be observed here. If a SIM card with PIN code is used, user can enter it in this section. The remaining attempts to enter PIN code are shown as well. When SIM PIN code is entered correctly user can change PIN code or disable it from the SIM card. When SIM PIN is disabled and user would like to enable it again, user must enter the previously used PIN code.

Keyword Settings

Configuration security keyword can be set to configurator. Keyword can be saved in configuration file (.cfg), so there is no need to connect the device to the configurator to configure the keyword. Minimum keyword length is 4 symbols and maximum length is 10 symbols. Only uppercase and lowercase letters and numbers are supported. Keyword can be configured to .cfg configuration file when the device is not connected.

Certificates

TAT240 can use digital certificates for authenticated access to secured network services. Supported certificates file types: *.pem, *.pem.crt, *.key

NOTE!	These features will only show up in configurator when device is connected to a computer.

Some services (such as OpenVPN, MQTT, etc.) on Teltonika Mobility devices can be secured using **TLS** for encryption and authentication. This page discusses where one can obtain TLS certificates and key for this purpose.

What is TLS/DTLS ?

Transport Layer Security (TLS) aims primarily to provide privacy and data integrity between user (device) and server, where it negotiates the message cryptography, it authenticates code keys to ensure a safe data transfer.

Datagram Transport Layer Security (DTLS) is a communications protocol designed to protect data privacy and preventing eavesdropping and tampering. It is based on the Transport Layer Security (TLS) protocol, which is a protocol that provides security to computer-based communications networks.

The main difference between DTLS and TLS:

- **Datagram Transport Layer Security (DTLS)** uses **User Datagram Protocol (UDP)**
- **Transport Layer Security (TLS)** uses **Transmission Control Protocol (TCP)**.

Why does traffic encryption matter?

1) **It prevents a man-in-the-middle attack.** TLS encryption turns structured data into randomized noise which makes it impossible to pull anything usable out of it.
2) **It prevents data injection.** TLS connection implies an initial handshake so the connection will be closed if certificates mismatch.
3) **Traffic encryption is better than no traffic encryption.** TLS allows and guarantees data exchange in a safe and private environment between two entities, user and server.

Certificate generation

Certificates secure client and server identities. After root certificates are installed, certificates get added to the root trust stores to secure connections between users and hosts, including devices and application users.

If you are using a third party service that requires TLS, all necessary files should be provided by the provider of that service. However, if you are setting up your own solution you may find use in of the **TLS certificate generation methods** described below.

Computer

You can also use third party software to generate the certificates on your computer. Guides are available for:

- Windows