TLS/DTLS implementation for Flespi using OpenSSL

[Main Page](#) > [Frequently Asked Questions - FAQ](#) > **TLS/DTLS implementation for Flespi using OpenSSL**

☐
Contents

Flespi is a server platform that supports Teltonika devices, with this platform, you can easily perform POCs such as sensor integration, firmware testing, capturing RAW data, and more. Because of this utility, we will use the Flespi platform as a test server. OpenSSL is open-source software with an Apache-style license, which can be used personally or commercially. These tools will be combined to implement TLS/DTLS encryption functionality in our Telematics devices.

Note: TLS/DTLS encryption is one of the security features of Teltonika Telematics, It protects private and sensitive information from eavesdroppers and hackers by encrypting data sent over the network.

General Information

Firmware version

It is always recommended to use the latest firmware, to check for the latest update, please **here**.

Requirements

- Windows OS (XP, 7, 10, 11)
- OpenSSL software.
- Teltonika Telematics device which supports TLS/DTLS (Supported versions: 1.1/1.2)
- Flespi channel with TLS/DTLS support. (Or any server that supports TLS/DTLS)
- Notepad or Notepad ++ (Optional)

Implementation Guide

The following instructions will guide you through the process of installing, creating, and configuring a TLS certificate and keys for our Telematics device. To complete this, we have 3 steps to follow. For more information, click on the links below.

1. **OpenSSL Installation**
2. **Creating Keys and Certificates**

3. **Device and Flespi Configuration**

Downloads

- **: OpenSSL download page**

- **: Notepad ++ download page**

Related links

- https://wiki.teltonika-gps.com/view/FMC130_GPRS_settings#TLS.2FDTLS
- https://teltonika-gps.com/use-cases/telematics/trackers-security/

External links

- **Flespi**

Disclaimer: