TLS Certificates LV Demo

The information in this page is updated in accordance with **00.07.09.1** firmware version.

□

Contents

Summary

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

Certificate generation

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.

Teltonika Networks device

The easiest way to generate certificates and keys is by using the **Certificate Generation** page that is available in the device's WebUI:

- System → Administration → Certificates

Generation of Certificate Authority (CA) Certificate & Key

The first step is to generate a Certificate Authority (CA) certificate, which will be used to sign both

server and client certificates.

1. Choose the file type as **CA**.
2. On Teltonika routers, users can select from four **Key Size** options, ranging from **512 bits to 4096 bits.**
3. Enter the **Common Name**. This usually represents the fully qualified domain name (FQDN) of the server (e.g., example.com), but it can be any name of your choice.

2. By enabling **Subject Information**, you can provide details about the entity to which the certificate is issued (Optional):

A. **Country Code (CC)**: The two-letter country code (e.g., LT for Lithuania).
B. **State or Province Name (ST)**: The name of the state or province (e.g., California).
C. **Locality Name (L)**: The city or locality (e.g., San Francisco).
D. **Organization Name (O)**: The name of the organization or company (e.g., Teltonika).
E. **Organizational Unit Name (OU)**: The name of the department or unit within the organization (e.g., IT Department).

These fields help to clearly identify the organization or individual associated with the certificate.

2. Select the "**On**" option next to "**Sign the Certificate**." If not enabled, the Root CA will not sign or generate the new CA.
3. Enter the period of how long CA certificate will be valid
4. "**Delete Signing Request**" can be enabled, as it is not required after generation.
5. Click  button

Generation of Server Certificate & Key

A server certificate, signed by a trusted Certificate Authority (CA), is used to authenticate the server and facilitate secure, encrypted communications with clients. Generating a server certificate follows similar steps to those for creating a CA certificate.

1. Select **Server** file type.
2. Select **Key Size**
3. Enter **Common Name** of the **Server**

4. **Subject Information** of the server(Optional)
5. Select the "**On**" option next to "**Sign the Certificate**".
6. Define how long the certificate will be **valid**.
7. The system should automatically detect the CA certificate and key files from "Certificates Manager" tab.
8. "**Delete Signing Request**" (Optional)
9. Click  button

Generation of Client Certificate & Key

A client certificate, signed by a trusted Certificate Authority (CA), is used to authenticate the client and facilitate secure, encrypted communications with other clients and servers. Generating a server certificate follows similar steps to those for creating a CA certificate.

1. Select **Client** file type.
2. Select **Key Size**
3. Enter **Common Name** of the Client
4. **Subject Information** of the Client(Optional)
5. Select the "**On**" option next to "**Sign the Certificate**".
6. Define how long the certificate will be **valid**.
7. The system should automatically detect the CA certificate and key files from the "Certificates Manager" tab.
8. "**Delete Signing Request**" (Optional)
9. "**Private Key Decryption password**" (Optional)
10. Click  button

Generation of DH Parameters

The **DH parameters** refers to the parameters used in the Diffie-Hellman key exchange. This cryptographic protocol allows two parties to generate a shared secret over an untrusted communication channel securely. In practical use, such as with VPNs, TLS/SSL, or routers, DH parameters are used to securely generate session keys for encrypting data. Generating a DH Parameters follows similar steps:

1. Select **DH Parameters** file type.
2. Select **Key Size**
3. Enter **Common Name**
4. Click  button

Generation of "Let's Encrypt" Certificate & Key

Let's Encrypt provides free SSL/TLS certificates that are widely used for securing web services, VPNs, and other network communications. In practical use, such as with websites, routers, or VPNs, the Let's Encrypt certificate and key enable HTTPS connections or secure tunnels. Generating a Let's Encrypt certificate and key follows similar steps:

1. Select the "**Let's Encrypt**" file type.
2. Enter the **Domain** name of the remote server associated with the public IP.
3. Enable **Automatic renewal** if you'd like the certificates to be automatically renewed every 60 days (Optional).
4. Click  button

Computer

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

- Windows
- Linux

Certificate signing

Teltonika network products also support Certificate signing functionality, that facilitates signing and creating certificates from certificate request files. Certificate requests need to be uploaded in the Certificates Manager tab first before they can be signed.