UAB TELTONIKA TELEMATICS
Saltoniškių st. 9B-1, LT-08105, Vilnius, Lithuania
Tel. +370 5 212 7472
info@teltonika.lt

FMBXX TLS/DTLS encryption scenario v0.3

Instructions below contain information how to prepare FMBXX device configuration to send encrypted records by using TLS/DTLS encryption parameter. This process generates a self-signed certificate for TLS use.

Requirements:

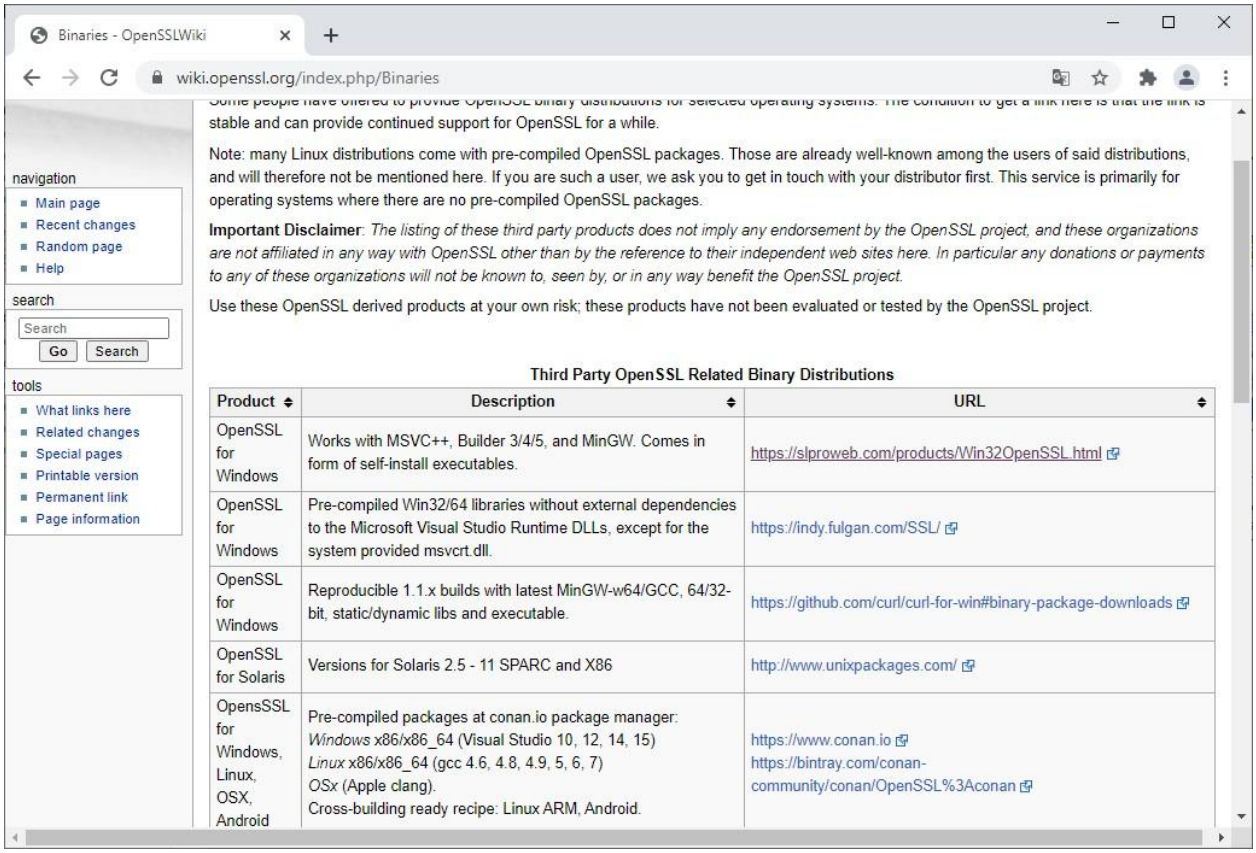
- Server with implemented TLS/DTLS functionality
- OPENSSL (or any other) software to generate certificate key
- Firmware FMB.Ver.03.27.xx or newer

1 Windows™[1] 10

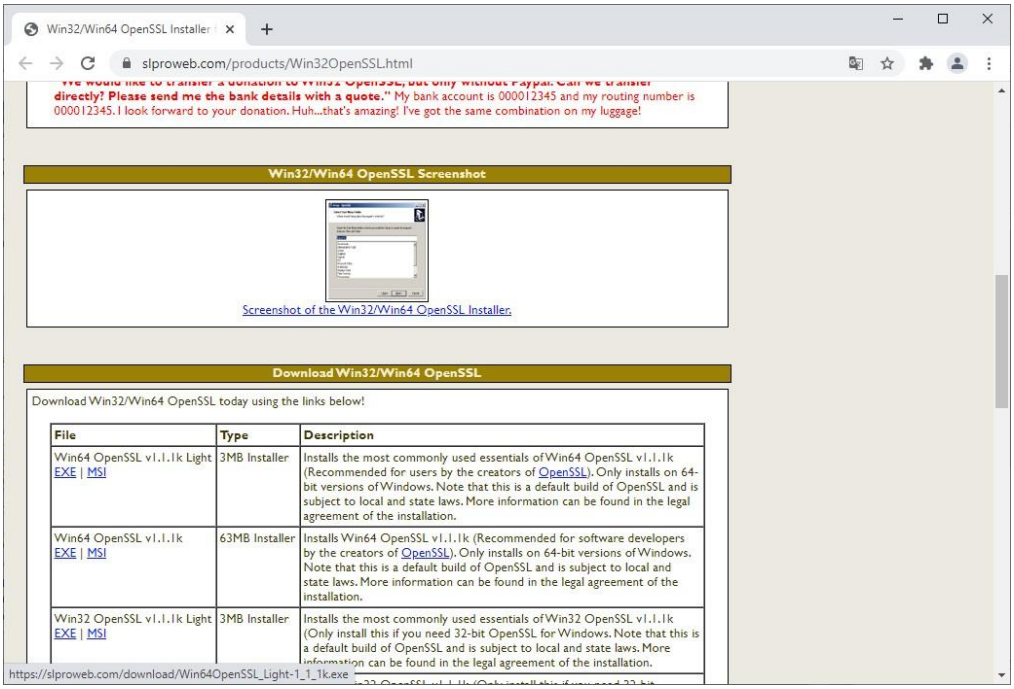
Download OpenSSL from https://wiki.openssl.org/index.php/Binaries

[1] Windows is a trademark of Microsoft Corporation; One Microsoft Way; Redmond, WA 98052-6399, USA

UAB TELTONIKA TELEMATICS
Saltoniškių st. 9B-1, LT-08105, Vilnius, Lithuania
Tel. +370 5 212 7472
info@teltonika.lt

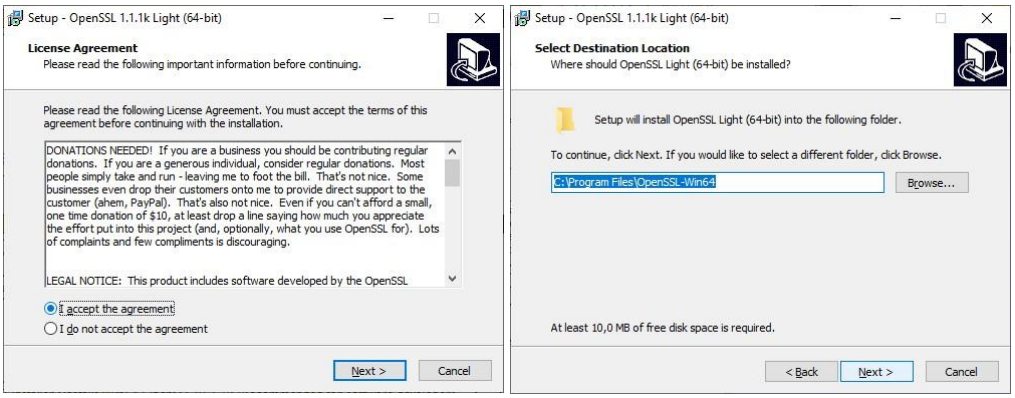


Locate the link for „slproweb“ or click here: https://slproweb.com/products/Win32OpenSSL.html

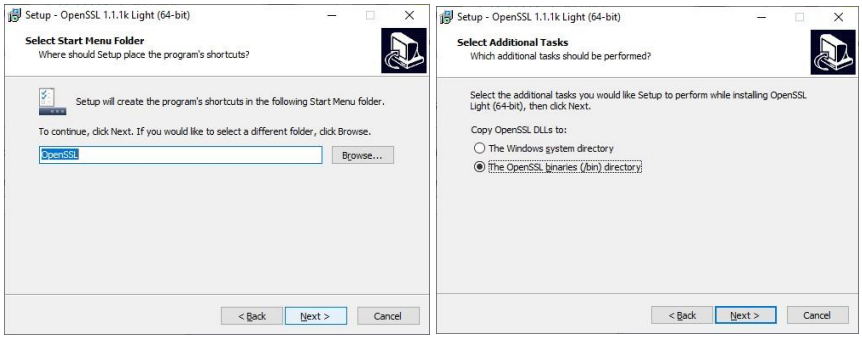


Locate the EXE or MSI link for Win64 OpenSSL v1.1.1k Light and download.

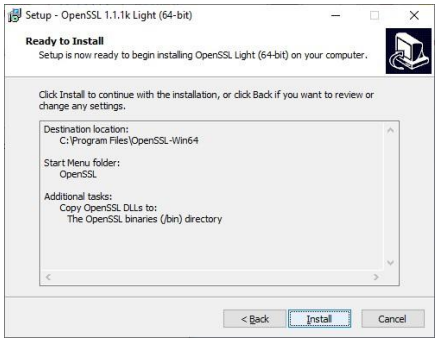
After download, install the tool.



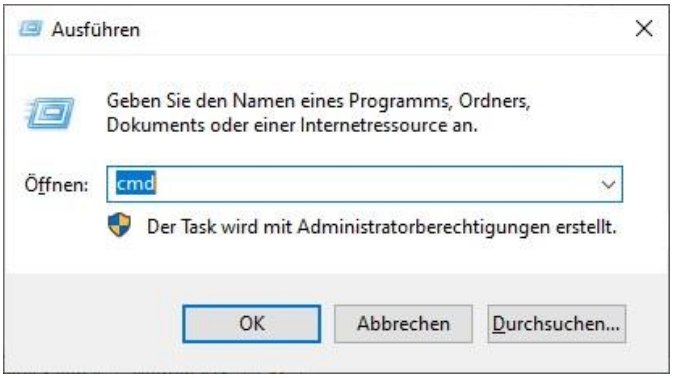
Use the default installation path (e.g. C:\Program Files), but you can choose any location you want. But be sure to remember this path on a later step.



We have use the /bin directory for installation, because „Windows system directory“ can be a little bit tricky and overloaded.



Hit Windows+R and type „cmd“



Or open the command window with the search panel on the bottom of the task bar.

A command prompt opens .

Switch to the installation directory (if you use the default) by typing (follow by Enter).

```
cd C:\Program Files\OpenSSL-Win64
```

Use your installation path in the other case.

Go forward to step 3.

2 Linux

In most distributions openssl is already preinstalled.

For the installation of packages, please refer to the instructions relevant to your operating system.

In our example an Ubuntu 20.04LTS Server installation is used.

```
banzai@banzaix:~$ sudo apt-get install openssl
[sudo] password for banzai:
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssl is already the newest version (1.1.1f-1ubuntu2.3).
openssl set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 59 not upgraded.
```

As you can see, openssl is already preinstalled in this case.

3 Generate certificate

The generation of a certificate is 99% identical with the use of openssl for all operating systems.

If you have any problems, please read the instructions for your installation.

Create a special directory to store generated files:

```
$> mkdir ssl
$> cd ssl
$ssl>
```

3.1 Generate private key

Type in console or command prompt:

```
$ssl> openssl genrsa -out private-key.pem 4096
```

```
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................................
.....++++
.....................................................................++++
e is 65537 (0x010001)
```

3.2 Generate public key

```
$ssl> openssl rsa -in private-key.pem -pubout -out public-key.pem
```

3.3 Generate certificate

```
$ssl> openssl req -new -x509 -key private-key.pem -out cert.pem
```

Fill in the options according to your own needs and follow the instructions below

- **Country Name:** Use the two-letter code without punctuation for country, for example: US or CA.
- **State or Province:** Spell out the state completely; do not abbreviate the state or province name, for example: California
- **Locality or City:** The Locality field is the city or town name, for example: San Francisco. Do not abbreviate. For example: Saint Louis, not St. Louis
- **Company:** If the company or department has an &, @, or any other symbol using the shift key in its name, the symbol must be spelled out or omitted, in order to enroll.
- **Organizational Unit:** The Organizational Unit (OU) field is the name of the department or organization unit making the request. To skip the OU field, press Enter on the keyboard.
- **Common Name:** The Common Name is the Host + Domain Name. It looks like "www.example.com" or " example.com".

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BZ
State or Province Name (full name) [Some-State]:Belize
Locality Name (eg, city) []:Belmopan
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My successful company Ltd
Organizational Unit Name (eg, section) []:Development
Common Name (e.g. server FQDN or YOUR name) []:fran fun
Email Address []:ffun@mscltd.com
```

3.4 Finalize

Copy the cert.pem and name it root.pem

```
$ssl> cp cert.pem root.pem
```

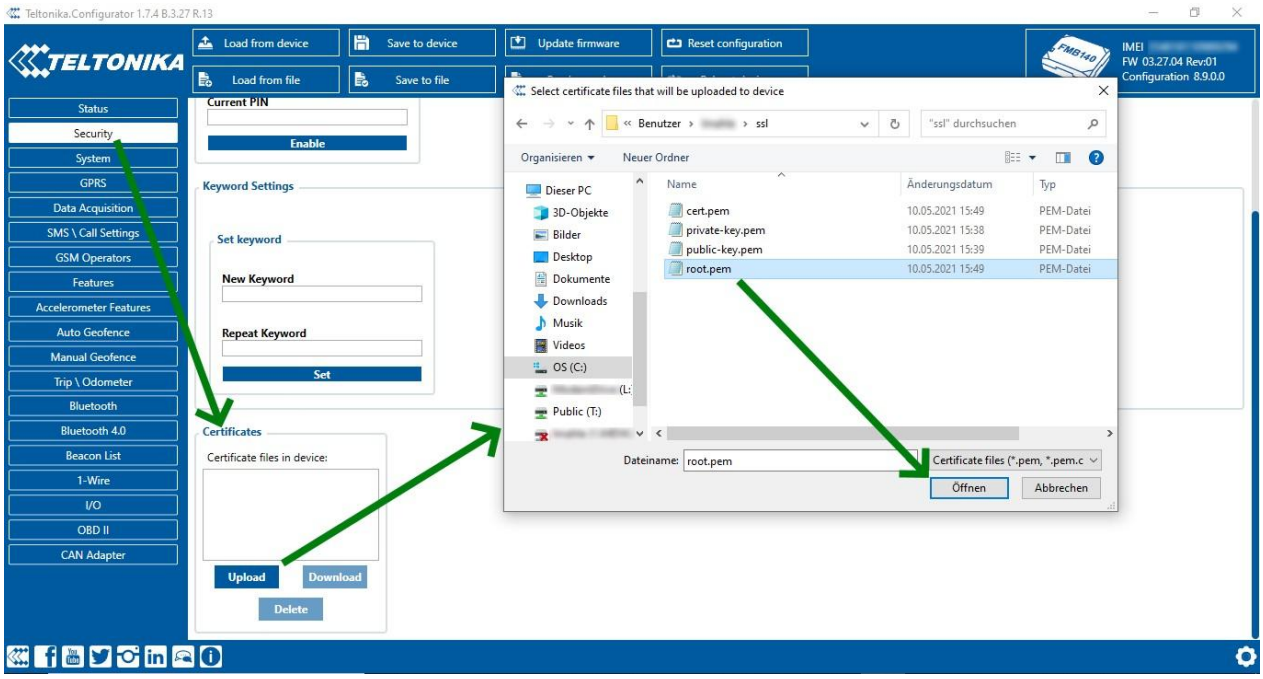
resp.

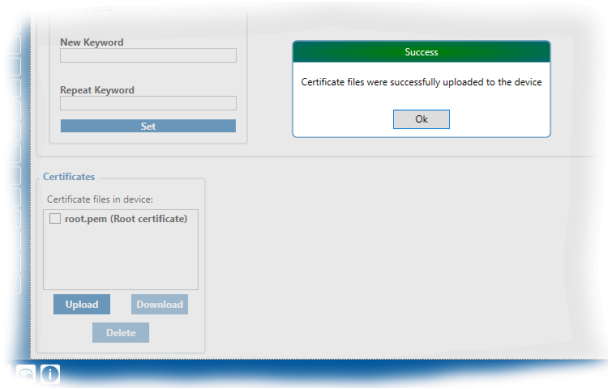
```
C:\Users\      \ssl>copy cert.pem root.pem
        1 Datei(en) kopiert.
```

You now have four files in your ssl directory.

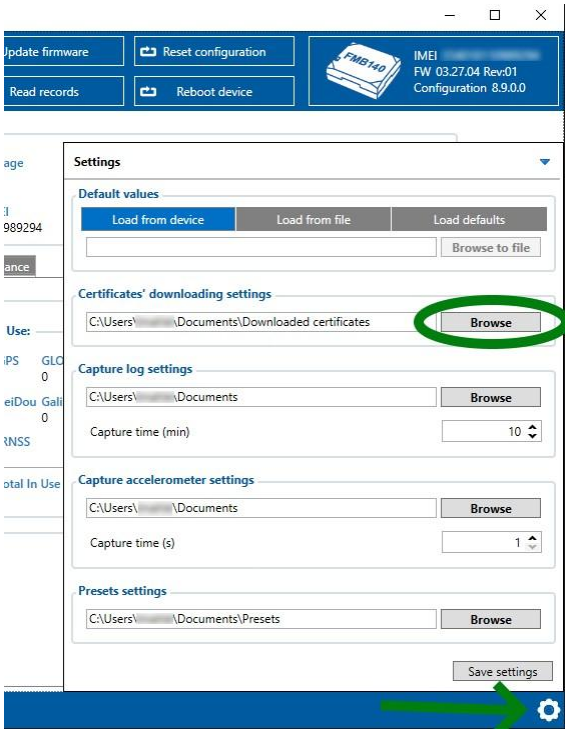
4 Installation on device

Open the Teltonika™ configuration software and goto panel „Security“.





If you want to download the certificate from the device, you must first set the destination directory in the configuration program and save the settings



Activate the feature via the panel GPRS -> Server Settings