FMBXX TLS/DTLS encryption scenario v0.2

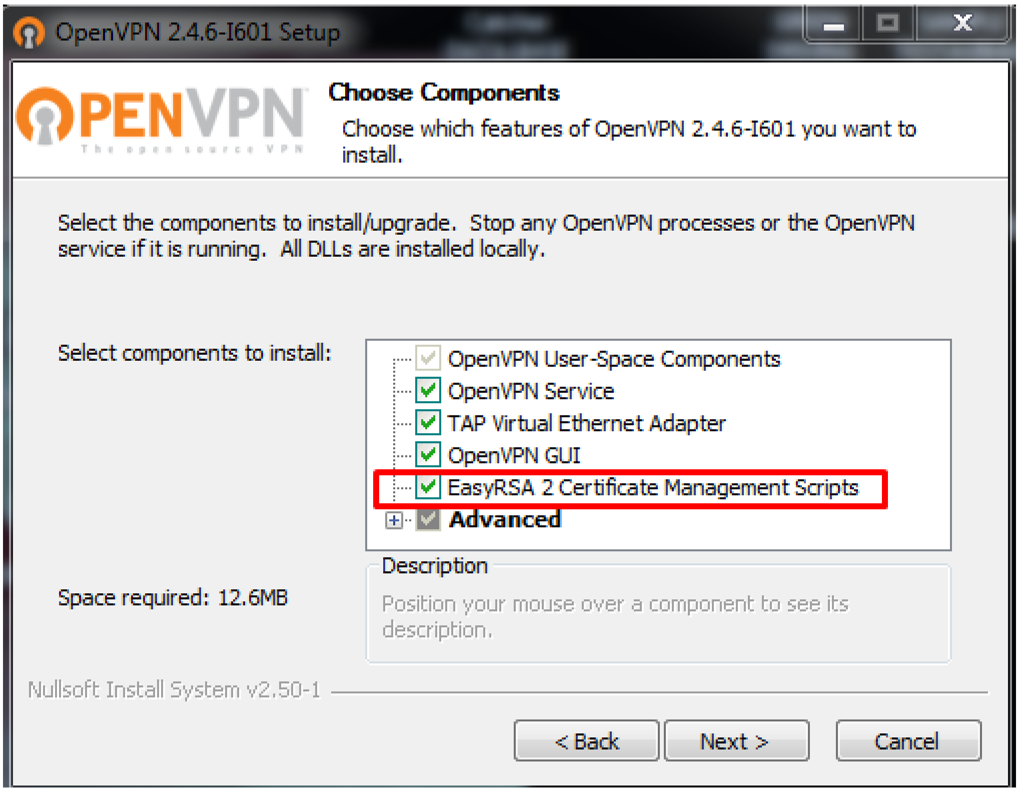
Instructions below contain information how to prepare FMBXX device configuration to send encrypted records by using TLS/DTLS encryption parameter.

Requirements:

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

1. Download and install *OPEN VPN* software:

Link: https://www.techspot.com/downloads/5182-openvpn.html
During installation process enable "EasyRSA 2 Certificate Management Scripts"



OpenVPN 2.4.6-I601 Setup

Choose Components

Choose which features of OpenVPN 2.4.6-I601 you want to install.

Select the components to install/upgrade. Stop any OpenVPN processes or the OpenVPN service if it is running. All DLLs are installed locally.

Select components to install:

- ☑ OpenVPN User-Space Components
- ☑ OpenVPN Service
- ☑ TAP Virtual Ethernet Adapter
- ☑ OpenVPN GUI
- ☑ EasyRSA 2 Certificate Management Scripts
- ☑ **Advanced**

Space required: 12.6MB

Description

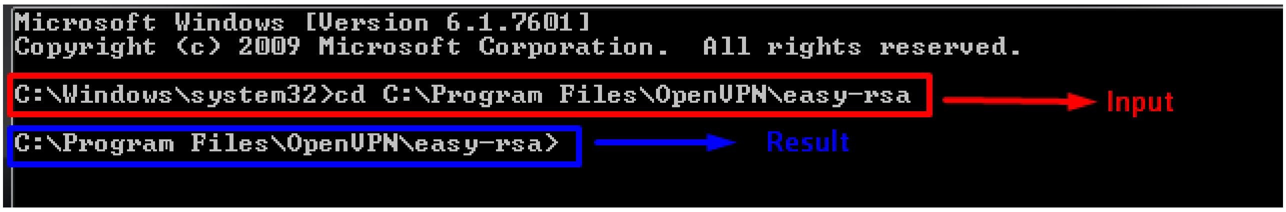
Position your mouse over a component to see its description.

Figure 1 OPEN VPN installing process.

2. Open command window (cmd.exe) as administrator:

   - After command window is running (as administrator), open easy-rsa directory over CMD:

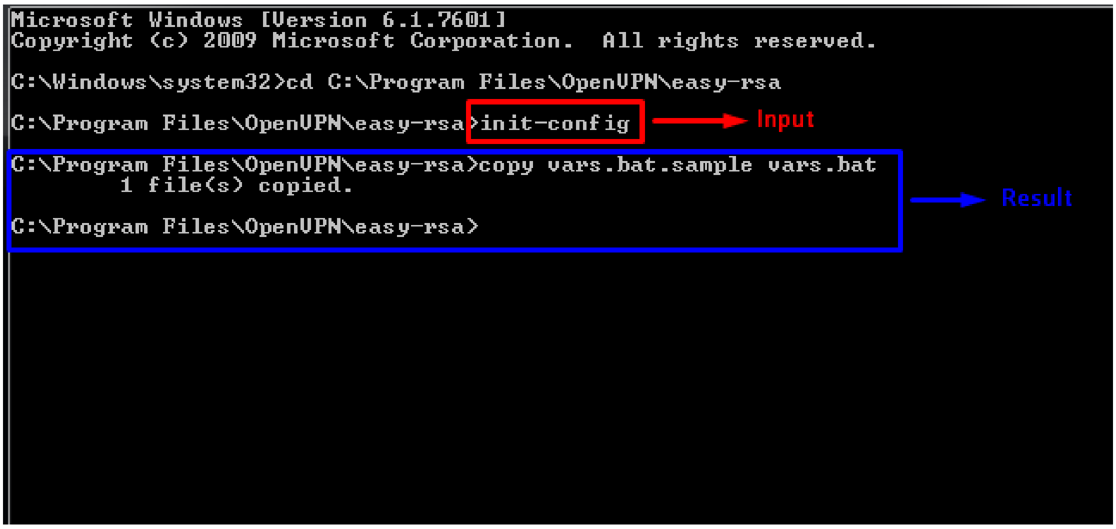
Example: "cd C:\Program Files\OpenVPN\easy-rsa"



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd C:\Program Files\OpenVPN\easy-rsa

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 2 easy-rsa command input and response.

- In opened directory enter command init-config and run the following batch file to copy configuration files into place (this will overwrite any preexisting vars.bat and openssl.cnffiles)



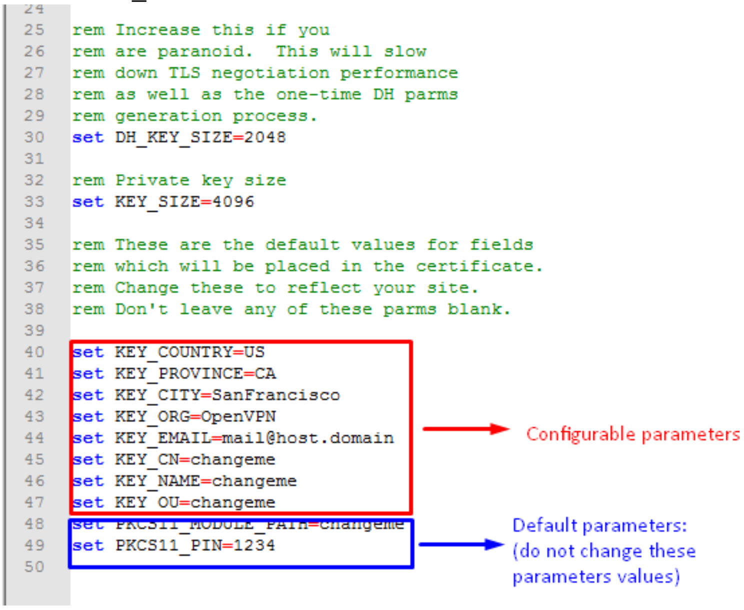
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd C:\Program Files\OpenVPN\easy-rsa

C:\Program Files\OpenVPN\easy-rsa>init-config

C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
        1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 3 init-config command input and response.

3. VAR.BAT file configuration:

   Open vars.bat file with text editor (notepad++) and set parameters of your server described below (enter information that would match to your server and company information). While editing the vars file (called vars.bat on Windows) and set the following parameters:
   KEY_COUNTRY
   KEY_PROVINCE
   KEY_CITY
   KEY_ORG
   KEY_EMAIL parameters (don’t leave any of these parameters blank)

Example:
set KEY_COUNTRY=LT
set KEY_PROVINCE=LTUS
set KEY_CITY=Vilnius
set KEY_ORG=100.10.11.222
set KEY_EMAIL=info@teltonika.lt
set KEY_CN=100.10.11.222
set KEY_NAME=TeltonikaSUPPORT
set KEY_OU=FMB



```
rem Increase this if you
rem are paranoid.  This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set DH_KEY_SIZE=2048

rem Private key size
set KEY_SIZE=4096

rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.

set KEY_COUNTRY=US
set KEY_PROVINCE=CA
set KEY_CITY=SanFrancisco
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@host.domain
set KEY_CN=changeme
set KEY_NAME=changeme
set KEY_OU=changeme
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

Configurable parameters

Default parameters:
(do not change these
parameters values)

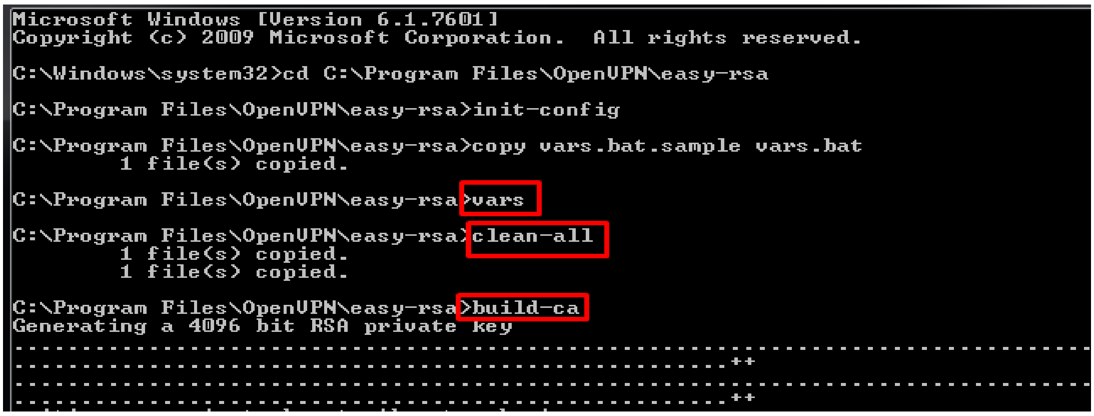
Figure 4 Notepad++ view (configurable and default parameters).

After parameters changed, save and close text editor.

4. Enter commands into CMD:

Enter 3 commands listed below one after another:

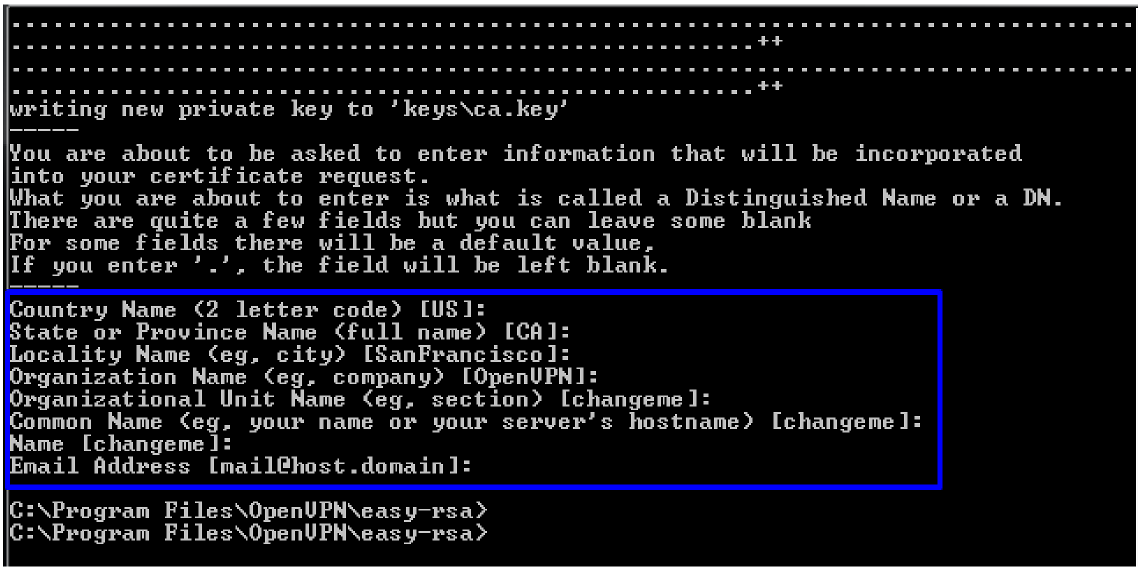
vars
clean-all
build-ca



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd C:\Program Files\OpenVPN\easy-rsa

C:\Program Files\OpenVPN\easy-rsa>init-config

C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
        1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>clean-all
        1 file(s) copied.
        1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>build-ca
Generating a 4096 bit RSA private key
................................................................................
.....................................................................++
................................................................................
.....................................................................++
```

Figure 5 vars, clean-all, build-ca commands inputs and responses.

After commands entered click enter to check all inserted parameters, when directory command appears check generated key in --> C:\Program Files\OpenVPN\easy-rsa\keys



```
...............................................................................
.....................................................++
...............................................................................
.....................................................++
writing new private key to 'keys\ca.key'
-----
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) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:
Name [changeme]:
Email Address [mail@host.domain]:

C:\Program Files\OpenVPN\easy-rsa>
C:\Program Files\OpenVPN\easy-rsa>
```

Figure 6 printed parameters which will be used in encryption certificate.

5. Generated key change:

Copy all generated files from C:\Program Files\OpenVPN\easy-rsa\keys into new folder and change ca.crt file name and extension into root.pem

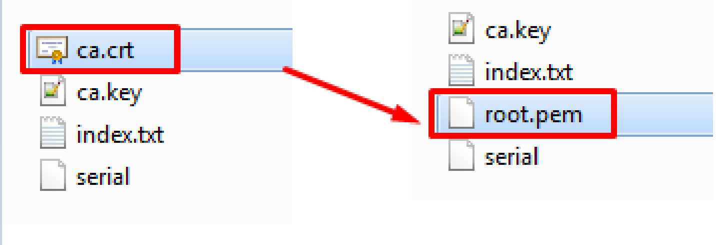
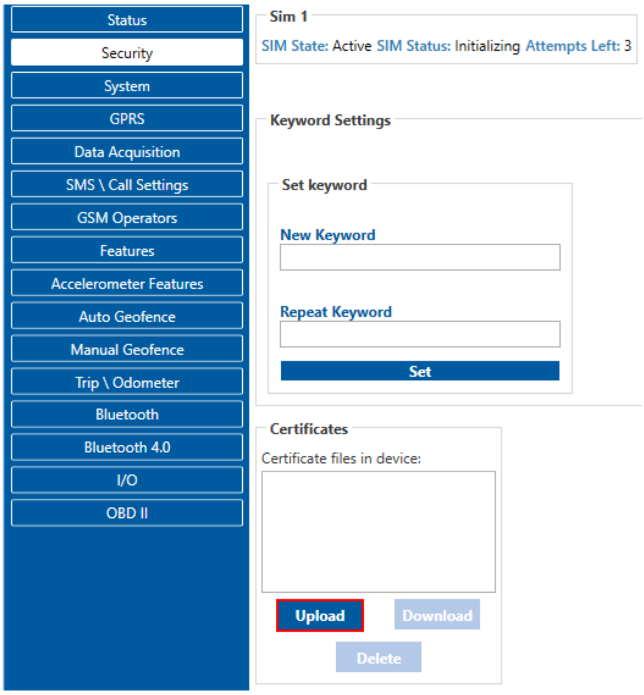


Figure 7 File name and extension change.

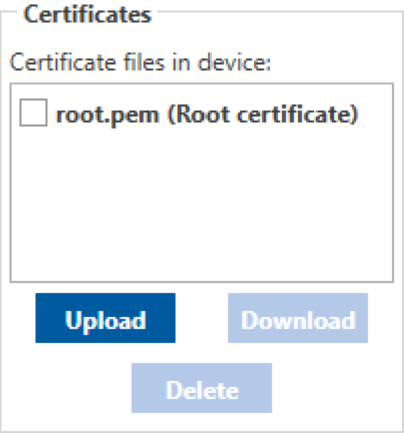
6. Upload root certificate to device:

NOTE! Certificate extension must be named "root.pem"



SIM State: Active SIM Status: Initializing Attempts Left: 3

Figure 8 File root.pem upload.

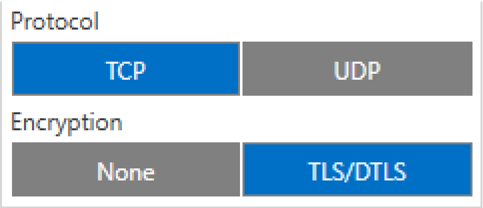


□ root.pem (Root certificate)

Figure 9 Uploaded root file.

Note: to upload new root.pem file current file must be deleted from configuration before.

7. Configure server and enable encryption mode:



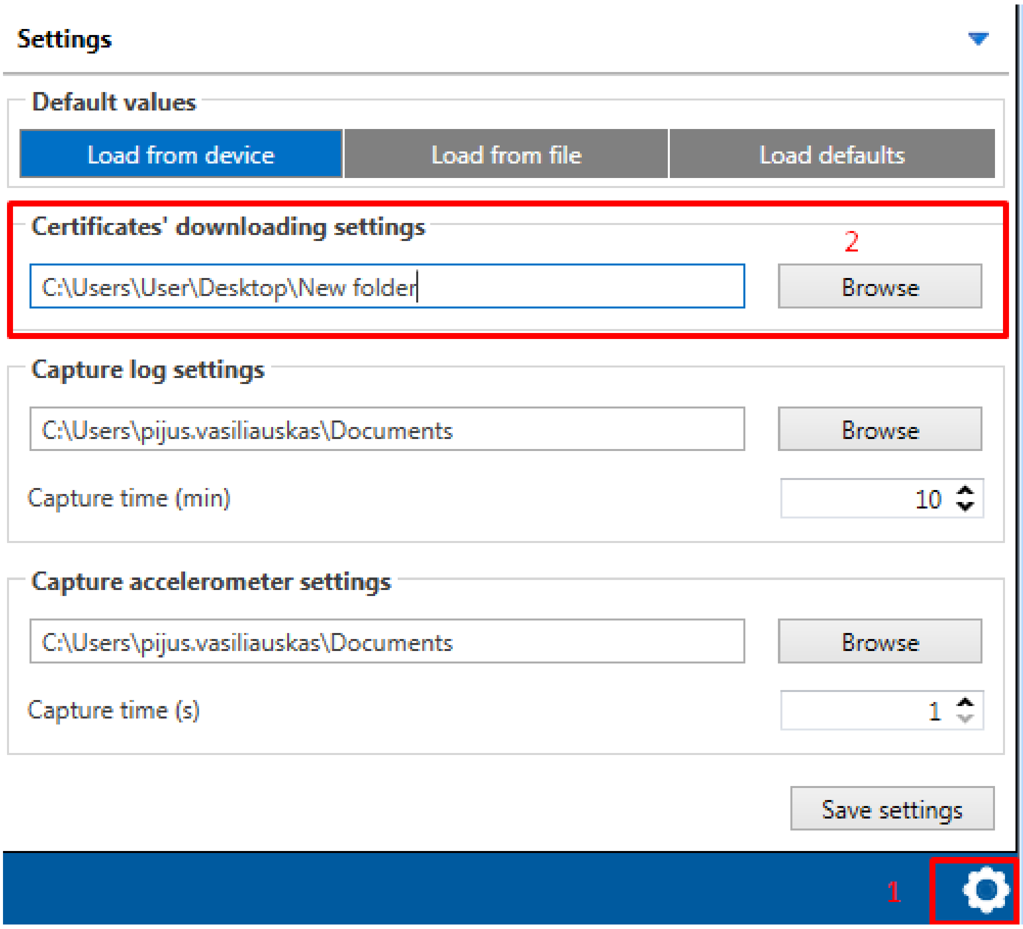
Protocol

Encryption

Figure 10 Configuration example.

8. Download certificate function:

To Download certificate from FMB device it is necessary to set a path in configurator settings.



Settings

Default values

Certificates' downloading settings

C:\Users\User\Desktop\New folder

Capture log settings

C:\Users\pijus.vasiliauskas\Documents

Capture time (min) 10

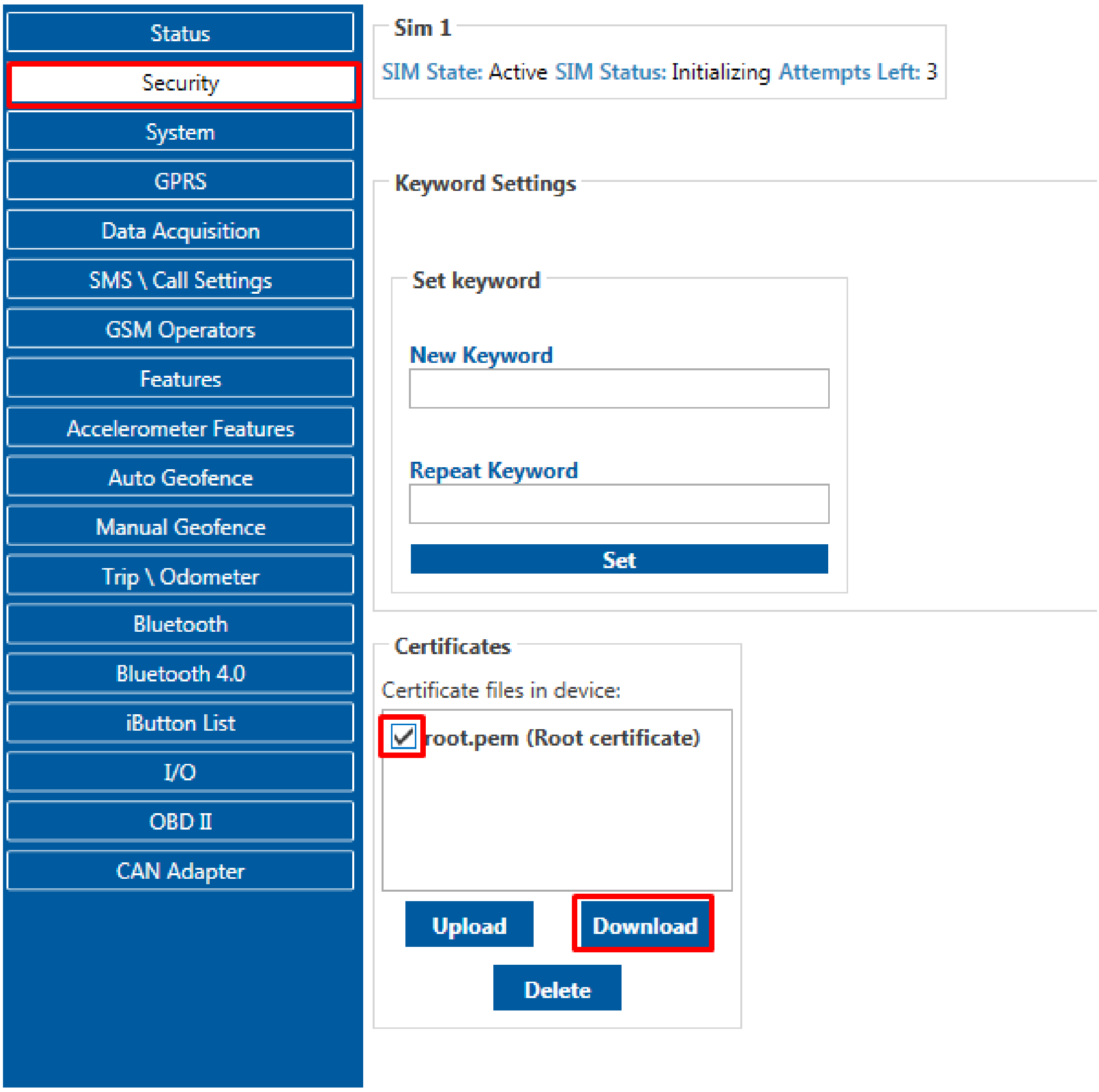
Capture accelerometer settings

C:\Users\pijus.vasiliauskas\Documents

Capture time (s) 1

Figure 11 Download certificate parameters.

- Then enter security window, mark certificate and click download.



Sim 1

SIM State: Active SIM Status: Initializing Attempts Left: 3

Keyword Settings

Set keyword

New Keyword

Repeat Keyword

Certificates

Certificate files in device:

☑ root.pem (Root certificate)

Figure 12 Download root.pem certificate window.

Change log:

Nr.	Date	Version	Comments
1	2018-11-16	0.1	Initial release
2	2020-09-11	0.2	Minor Changed