AN12907

Secure update of EdgeLock SE051 IoT applet

Rev. 1.2 — 23 November 2023   **Application note**
641112

Document information

| Information	Content
Keywords	EdgeLock SE051, Plug & Trust, secure element, IoT, applet, SEMS Lite
Abstract	This document describes the SEMS Lite feature and explains how it can be leveraged, together with the EdgeLock 2GO platform, to update the EdgeLock SE051 IoT applet. This document only applies to EdgeLock SE051 variants that come with a pre-installed IoT applet.

1 Introduction

Due to their diffusion and scale, IoT devices are progressively becoming the target of cyberattacks. These attacks might be performed to extract valuable information from the IoT device or simply to disrupt its normal operation. Offloading security-critical operations to a Secure Element (SE) such as EdgeLock SE051 is a huge step forward in obtaining top-grade security for IoT devices. In fact, the SE becomes the focus for sensitive operations and leverages hardened and tamperproof hardware and software to ensure that those operations are conducted securely.

EdgeLock SE051 is a ready-to-use SE solution that provides a secure, CC EAL 6+ certified tamper-resistant hardware to accommodate all the security needs of an IoT device. EdgeLock SE051 provides a root of trust at the IC level and gives an IoT system a state-of-the-art, edge-to-cloud security capability right out of the box. EdgeLock SE051 secure memory allows the user to protect mission critical cryptographic keys and credentials and use them to perform cryptographic operations in EdgeLock SE051 secure hardware environment.

To ease integration in the IoT solution and reduce the time to market, EdgeLock SE051 variants A and C offer a fully-featured, pre-installed **IoT applet** that can be leveraged to manage credential life cycle operations and cryptographic operations. The EdgeLock SE051 Plug & Trust middleware allows the user to easily integrate the IoT applet functionalities in the IoT device thanks to its API and broad range of supported MCUs.

In addition, EdgeLock SE051 provides advanced applet management capabilities through NXP's Secure Element Management Service Lite (SEMS Lite) feature. SEMS Lite is an exclusive feature offered by NXP for EdgeLock SE051 that allows IoT device vendors to update applets and patch applets security vulnerabilities as soon as they are discovered by using a single secure script valid for all the OEM's IoT devices.

In this context, SEMS Lite can be leveraged, in combination with NXP's EdgeLock 2GO platform, to easily apply to the pre-installed EdgeLock SE051 IoT applet the latest security patches and updates offered by NXP while preserving all the secure objects created by the IoT applet. IoT devices can therefore take advantage of the latest IoT applet features and security improvements as soon as they are available and always enjoy a high protection level for stored credentials. A high level overview of the update process of EdgeLock SE051 IoT applet using SEMS Lite and EdgeLock 2GO is shown in Figure 1.

Figure 1. High level overview of IoT applet update process using SEMS Lite and EdgeLock 2GO
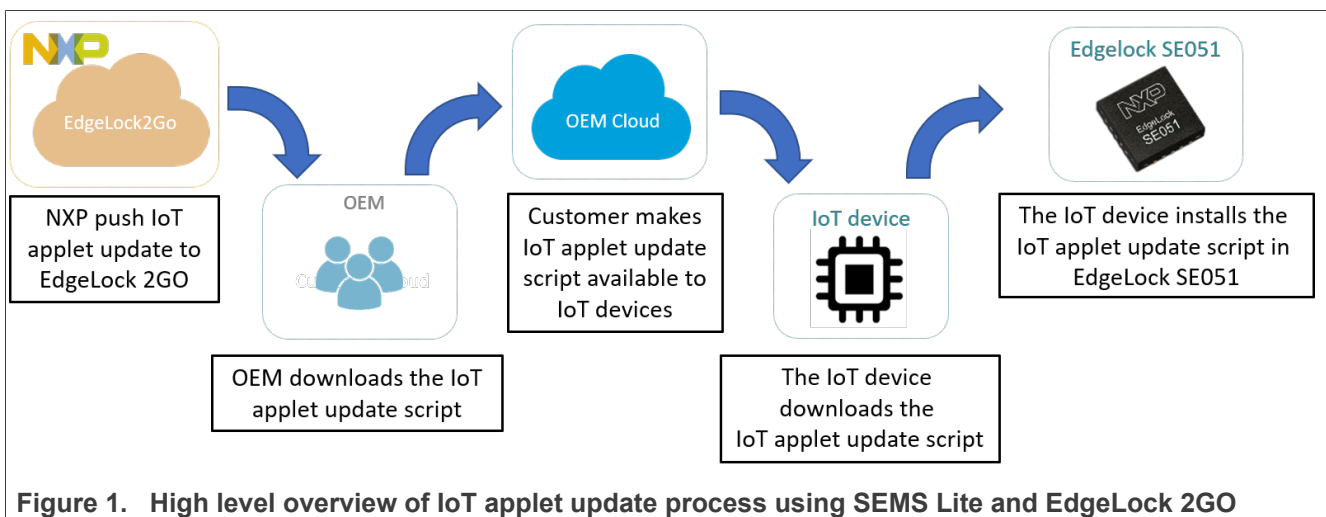
This document provides a detailed explanation of how an OEM can leverage SEMS Lite to securely update the pre-installed EdgeLock SE051 IoT applet.

Note: *Development, deployment and update of custom applets is only supported for EdgeLock SE051 variant P. If you are interested in these features, please get in touch with your NXP representative for more information.*

2 Secure update of EdgeLock SE051 applets using SEMS Lite

IoT devices that integrate a secure element such as EdgeLock SE051 depend on it to provide critical security functionalities to the rest of the system. Keeping the secure element up to date is therefore essential to guarantee that the IoT device is always using the latest security features and is protected against recently discovered threats and vulnerabilities.

To achieve this, EdgeLock SE051 supports SEMS Lite, a feature that enables OEMs to easily update applets installed in the secure element using a secure, signed and encrypted script. SEMS Lite is multicast in nature and therefore allows the OEM to remotely update all the devices with a single script without the need to manage the credentials of every single device. Moreover, since the update script is cryptographically secure, OEMs enjoy the flexibility of using their preferred communication channel to distribute the update. The SEMS Lite update script consists of a sequence of commands that trigger content management operations in the secure element. The SEMS Lite update script is typically generated by the secure element owner, which is usually the chip manufacturer, but can also be generated by the OEM with credentials provided by the secure element owner (as done with EdgeLock SE051P type).

To apply the update script to the secure element, SEMS Lite relies on three software components: the Update Manager, the SEMS Lite Agent and the SEMS Lite applet as shown in Figure 2.
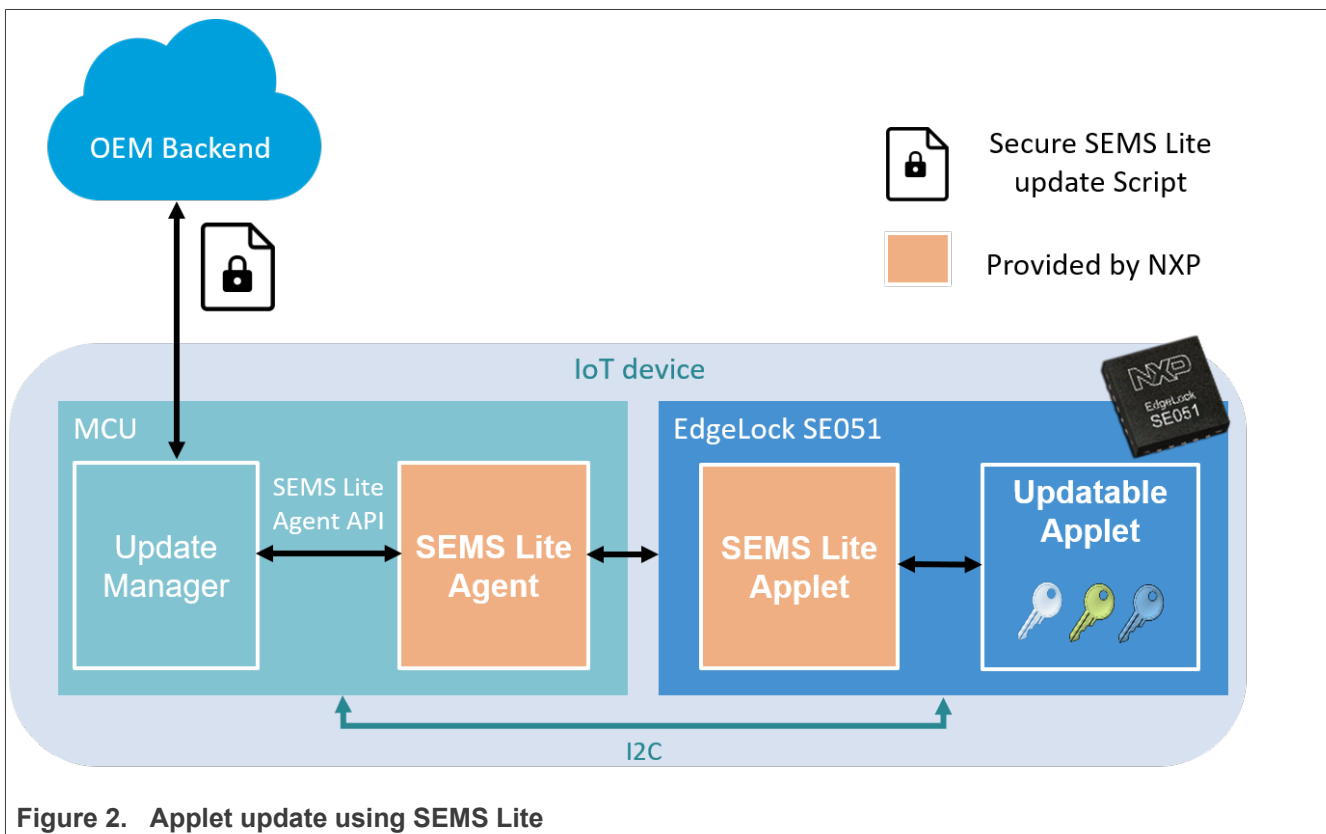

Figure 2.   Applet update using SEMS Lite

- **Update Manager:** this software component runs in the MCU and takes care of securely downloading the correct SEMS Lite update script from the OEM backend and forwarding it to the SEMS Lite Agent component for execution. After downloading the SEMS Lite script, the Update Manager is responsible for defining the best time to apply the update depending on the IoT device status, for example depending on the IoT device battery level or the usage profile of the IoT device. The Update Manager shall be implemented by the OEM according to the requirements of the IoT application and shall use the API exposed by the SEMS Lite Agent

component to manage the life cycle of the update. Optionally, the Update Manager can be used to report to the backend the result of the script execution as communicated by the SEMS Lite Agent.

- **SEMS Lite Agent:** this software module runs in the MCU and acts as a bridge between the Update Manager and EdgeLock SE051 for the management of operations related with SEMS Lite. The SEMS Lite Agent exposes a functional API that can be used by the Update Manager to query the state of the system, load a SEMS Lite script in EdgeLock SE051, track the update progress and recover the system in case of update failure. The SEMS Lite Agent is provided by NXP as part of the EdgeLock SE051 Plug & Trust middleware package. This allows OEMs to easily and quickly integrate SEMS Lite in their IoT devices. More details on how the Update Manager can leverage the EdgeLock SE051 Plug & Trust middleware SEMS Lite API are provided in Section 5.4 and in the EdgeLock SE051 Plug & Trust middleware documentation.
- **SEMS Lite Applet:** when the SEMS Lite update script is loaded by the SEMS Lite Agent in EdgeLock SE051, the request is handled by the SEMS Lite Applet that has been pre-loaded by NXP in EdgeLock SE051 ICs. The SEMS Lite Applet takes care of decrypting the SEMS Lite update script and verifying if it has the necessary permissions to execute. If all requirements are satisfied, the update script commands are executed one by one and the target applet is updated. The update status is reported to the SEMS Lite Agent and then to the Update Manager.

3   Leveraging EdgeLock 2GO and SEMS Lite to update EdgeLock SE051 IoT applet

EdgeLock SE051 is shipped with the pre-loaded NXP's IoT applet. The IoT applet allows customers to easily manage the life cycle of credentials stored in the secure element and to execute cryptographic operations.

By taking advantage of EdgeLock SE051 SEMS Lite feature described in Section 2, it is possible to keep the IoT applet up to date so that the IoT device can always have access to the latest security features and security patches for the secure element.

It is important to emphasize that when updating the IoT applet using a SEMS Lite update script, the following data is preserved:

- All secure objects, e.g. keys, that have been generated or imported by the IoT applet;
- Secure Channel Protocol (SCP) keys if the SCP authentication method is in use.

The generation of the secure SEMS Lite script to update the IoT applet is completely managed by NXP. The IoT applet SEMS Lite update script is distributed to OEMs through NXP's EdgeLock 2GO platform: a fully-managed cloud service for easy, secure deployment and management of IoT devices that use secure elements of the EdgeLock family.

The IoT applet update flow in EdgeLock SE051 using SEMS Lite and EdgeLock 2GO is depicted in Figure 3.

Figure 3.   IoT applet update flow using SEMS Lite and EdgeLock 2GO
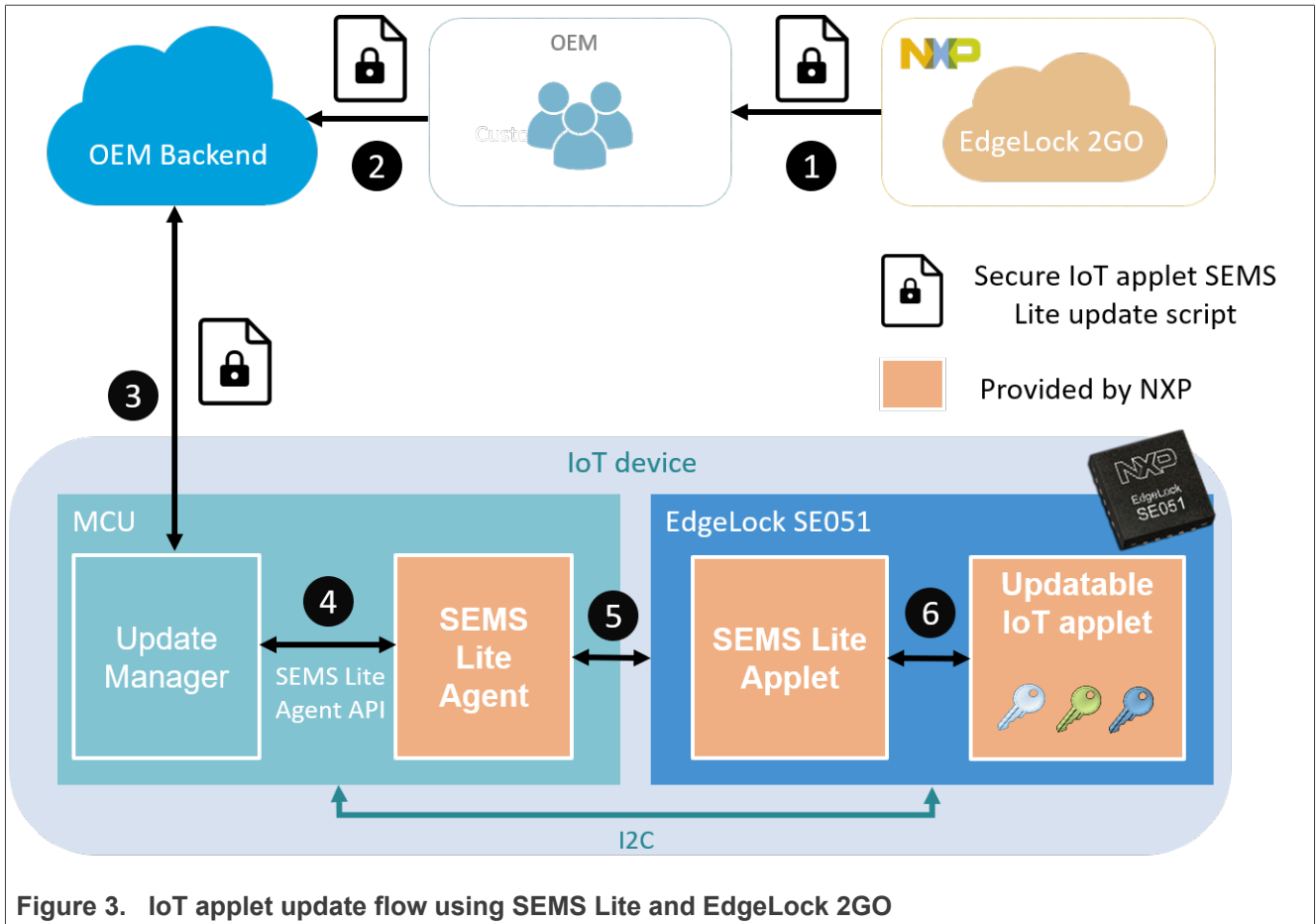
1. When a new version of the IoT applet is available, NXP pushes the corresponding SEMS Lite update script to EdgeLock 2GO. The OEM can then download the IoT applet SEMS Lite update script from EdgeLock 2GO either by using the EdgeLock 2GO web dashboard or the EdgeLock 2GO REST API. See Section 4 for detailed instructions on how to do this.

2. The OEM should store the IoT applet SEMS Lite update script retrieved from EdgeLock 2GO in a suitable location accessible to IoT devices deployed in the field, e.g. in a proprietary cloud backend server.
   Note: *currently, the IoT applet update script cannot be retrieved by IoT devices directly from EdgeLock 2GO.*

3. At the most convenient time, the Update Manager downloads the IoT applet SEMS Lite update script to the IoT device. This might require, for example, to periodically poll the OEM backend to check for new updates and, if an update is available, to establish a secure connection to the OEM backend; e.g. using TLS, to retrieve the IoT applet SEMS Lite update script.

4. When the device is ready to be updated, the Update Manager forwards the IoT applet SEMS Lite update script to the SEMS Lite Agent using the SEMS Lite Agent API. More information on the usage of the SEMS Lite Agent API can be found in Section 5.4 and in the EdgeLock SE051 Plug & Trust middleware documentation.

5. The SEMS Lite Agent connects to EdgeLock SE051 and triggers the execution of the IoT applet update script.

6. The pre-loaded SEMS Lite Applet checks the validity of the IoT applet SEMS Lite update script and executes the update commands. If the process executes correctly, the IoT applet is updated to the new version.

Note: the update of the IoT applet will fail under normal conditions if EdgeLock SE051 is running a version of the IoT applet higher than the one that is being loaded by the IoT applet update script.

7. To prevent installations of lower versions of the applet from previous valid SEMS Lite scripts under all conditions additionally a SEMS Lite key rotation script must be executed. This rotation script updates the key used within SEMS Lite to check the validity of scripts and as such invalidates all previously generated SEMS Lite scripts for this type with the old key. NXP provides rotation scripts on all types where this is appliable together with the applet update scripts. The key rotation script download and preparation is identical to the handling of update scripts.

Which script is runnable on any type can be checked via comparing the public key given in the field "PkSemsCaAut" of the downloaded SEMS Lite script with the reported public key of SEMS Lite applet which can be read using:

```
sems_lite_cli_app --getPbKeyID
```

4 Use EdgeLock 2GO to download IoT applet update scripts

This section describes how to register to the EdgeLock 2GO platform and how to use EdgeLock 2GO to download SEMS Lite update scripts for the IoT applet.

1. Obtain an EdgeLock 2GO account
2. Create an NXP account and log in to EdgeLock 2GO
3. Download IoT applet update scripts

4.1 Obtain an EdgeLock 2GO account

To obtain an EdgeLock 2GO account follow the instructions provided below. If you do not have one already, register an NXP account as described in Section 6 before proceeding:

1. Visit the NXP website at https://contact.nxp.com/edgelock2go-signup;
2. Fill in the fields shown in Figure 4 with your contact information and then click on the *Send* button to forward the account creation request to NXP. Use the same email address associated to your NXP account since it will be used to create the EdgeLock 2GO account.

Figure 4. Request an EdgeLock 2GO account

3. An NXP representative will review your application. If you are eligible for an account, you will receive an email similar to the one shown in Figure 5. Use the *Go to Login* button to perform the first login using the NXP credentials associated to the email you provided. For information on how to log in to EdgeLock 2GO follow the instructions in Section 4.2.
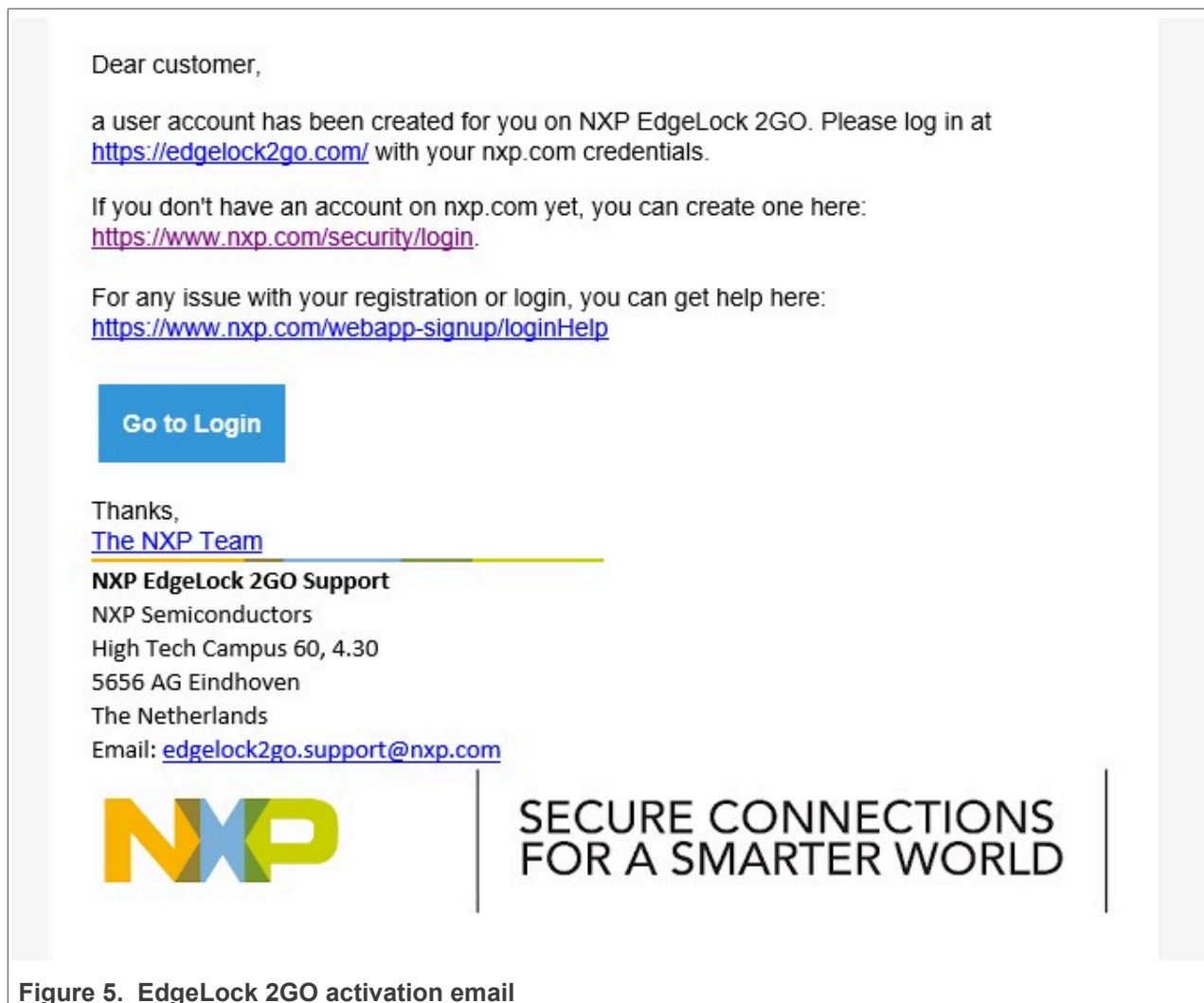
Figure 5. EdgeLock 2GO activation email

4.2 Log in to EdgeLock 2GO

Follow the instructions in Section 4.1 to request an EdgeLock 2GO account. Once an account is created in EdgeLock 2GO using the email address you provided, you can use an NXP account associated to that email to log in to EdgeLock 2GO.

To log in to EdgeLock 2GO follow the steps below:

1. You can login to EdgeLock 2GO with your NXP credentials at https://edgelock2go.com/ as shown in Figure 6:

Figure 6. Login to EdgeLock 2GO

2. If you activated 2-factor authentication, you will be asked how you prefer to receive the single use code as shown in Figure 7:
   (1) Select if you want to receive the single use code by SMS or by phone call;
   (2) Click on *Send Code*. You should soon receive the single use code in your mobile phone through the channel you selected.
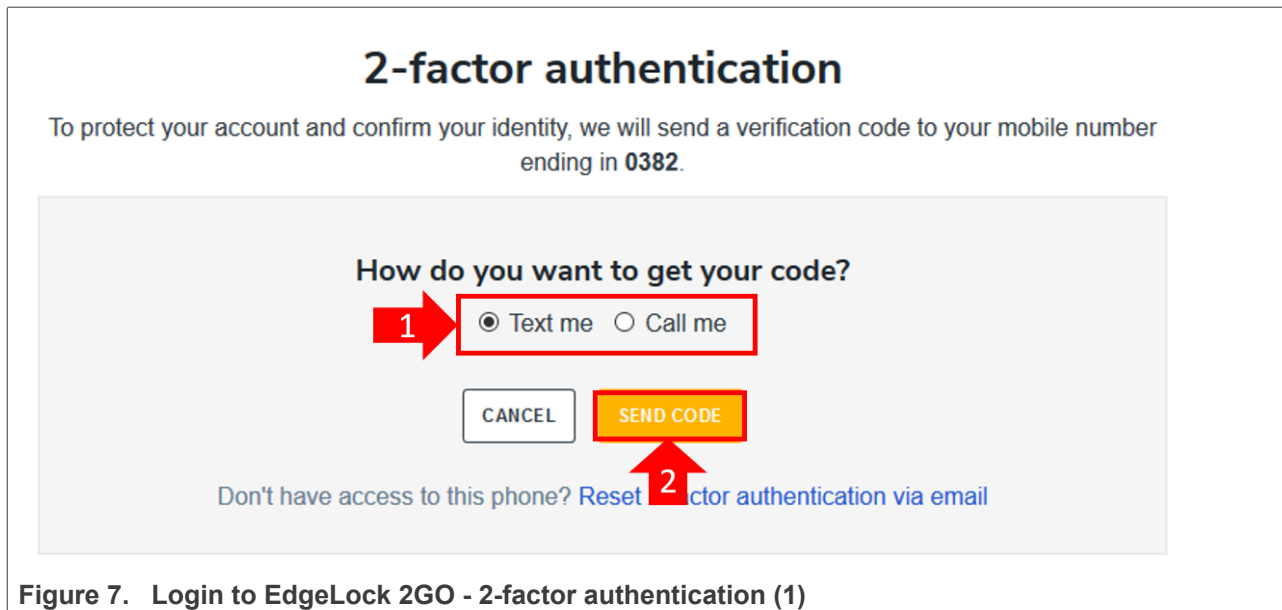
Figure 7. Login to EdgeLock 2GO - 2-factor authentication (1)

3. Insert the code you just received and then click on the *Sign In* button as shown in Figure 8 to login to EdgeLock 2GO:
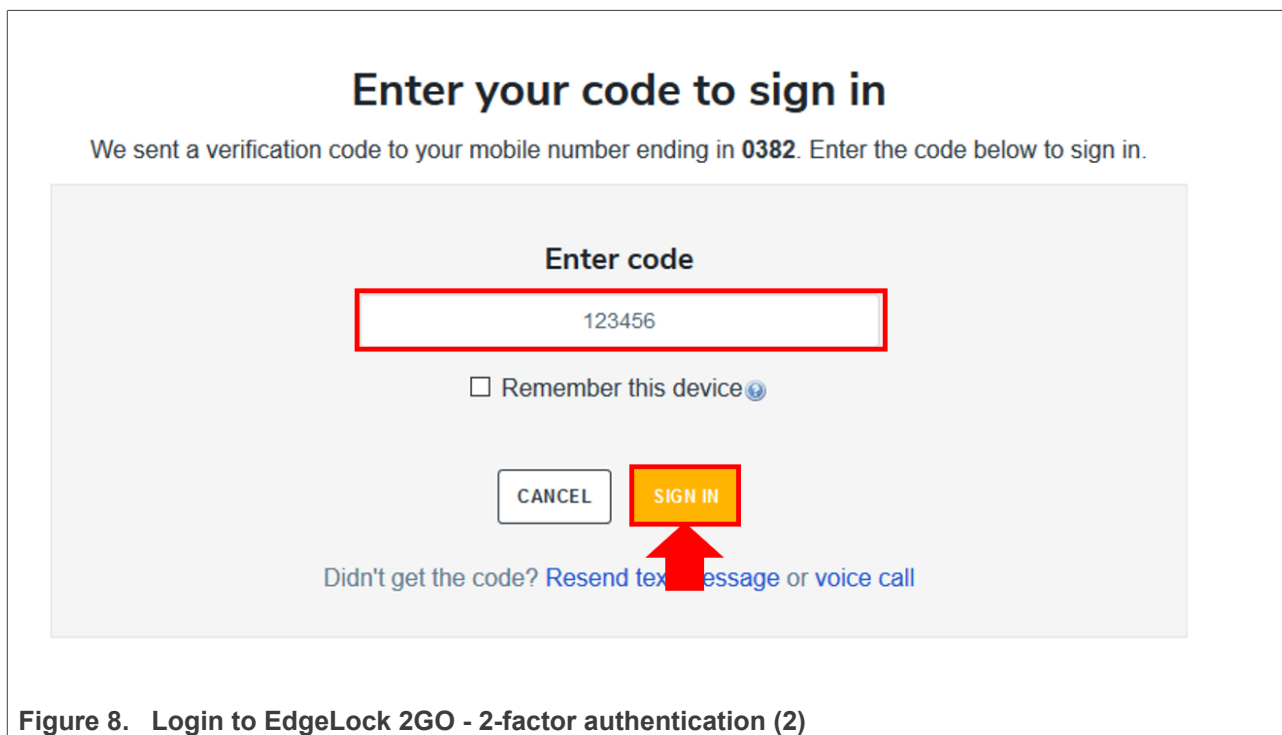
Figure 8. Login to EdgeLock 2GO - 2-factor authentication (2)

Note: if you trust the device that you are using to log in, you can tick the 'Remember this device' box to reduce the number of times you will be asked to authenticate using 2-factor authentication.

4. If this is your first login, you will be redirected to the terms & conditions screen. You will have to accept the terms & conditions by clicking on the *I Accept* button as shown in Figure 9 in order to use the service.
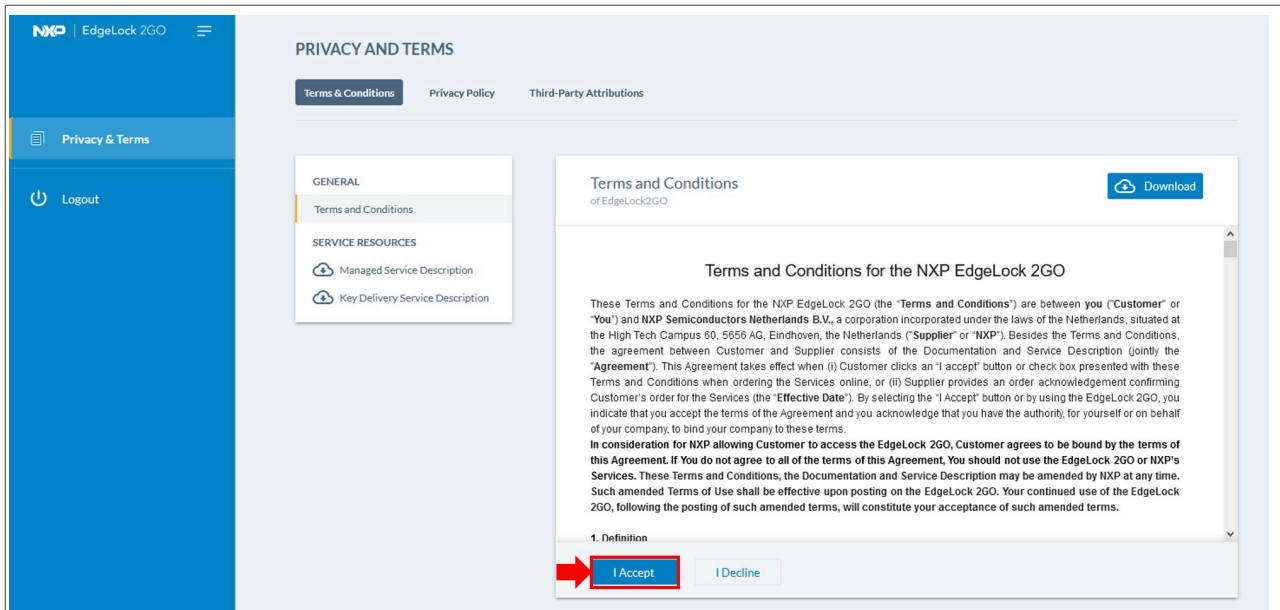
Figure 9. Accept EdgeLock 2GO terms and conditions

5. You should now see the homepage of EdgeLock 2GO as shown in Figure 10:
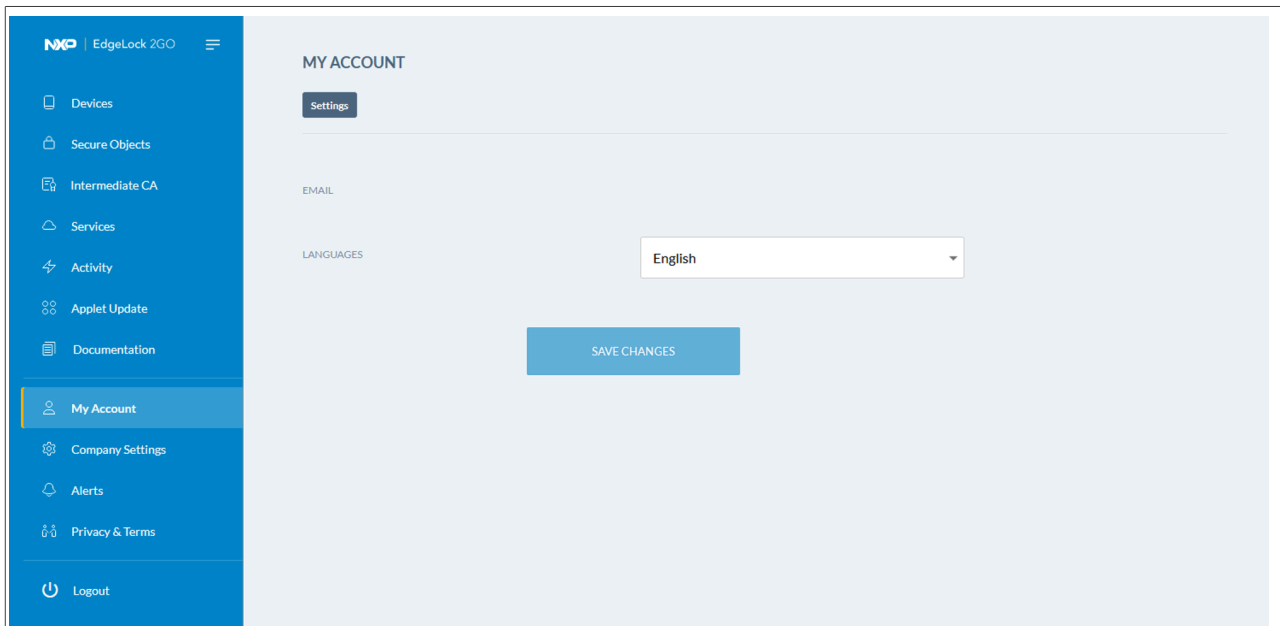
Figure 10. EdgeLock 2GO homepage

6. You can logout at any time from EdgeLock 2GO by clicking on the *Logout* button in the left pane as shown in Figure 11.
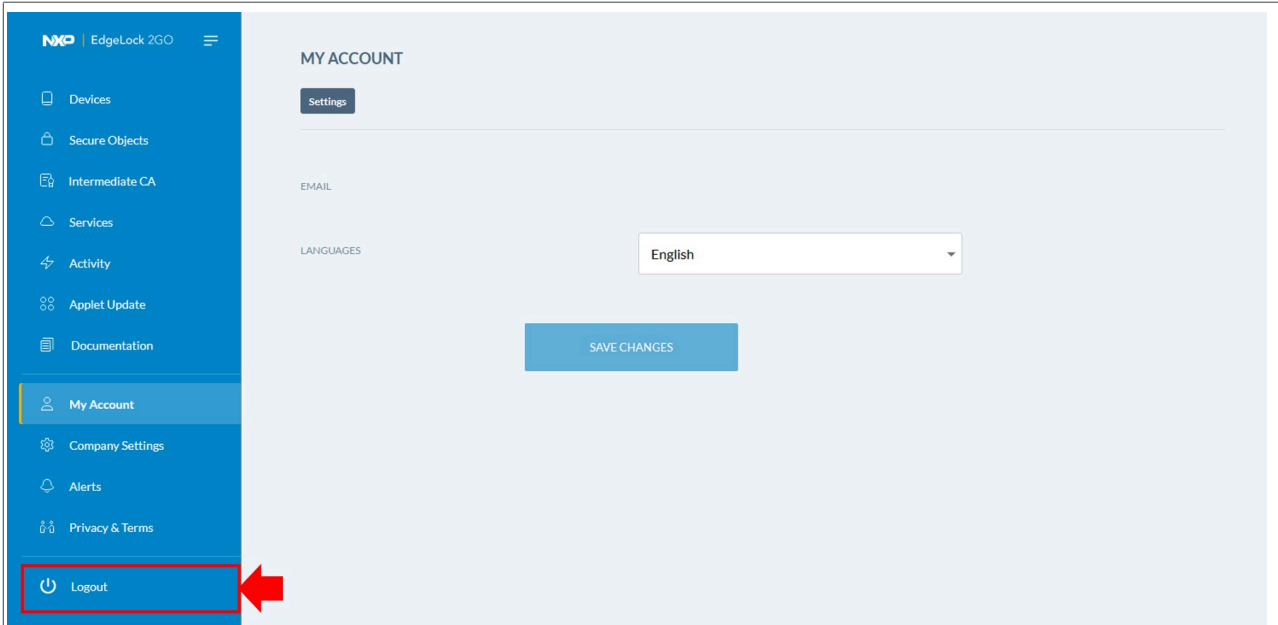
Figure 11.   Logout from EdgeLock 2GO

4.3 Download IoT applet update scripts

Follow these instructions to download an IoT applet update script from EdgeLock 2GO:

1. (1) Open the *Applet Update* page in EdgeLock 2GO and then (2) click on the 12NC code of the product you are downloading the script(s) for as shown in Figure 12.
    Note: the EdgeLock SE051 chip on OM-SE051ARD corresponds to hardware type SE051C2HQ1/Z01XD (12NC: 935414457472) based on the configuration OEF A564. New boards since begin of 2022 are already delivered with updated IoT Applet 7.2 and are based on OEF A8FA (see AN12973 SE051 Configurations)
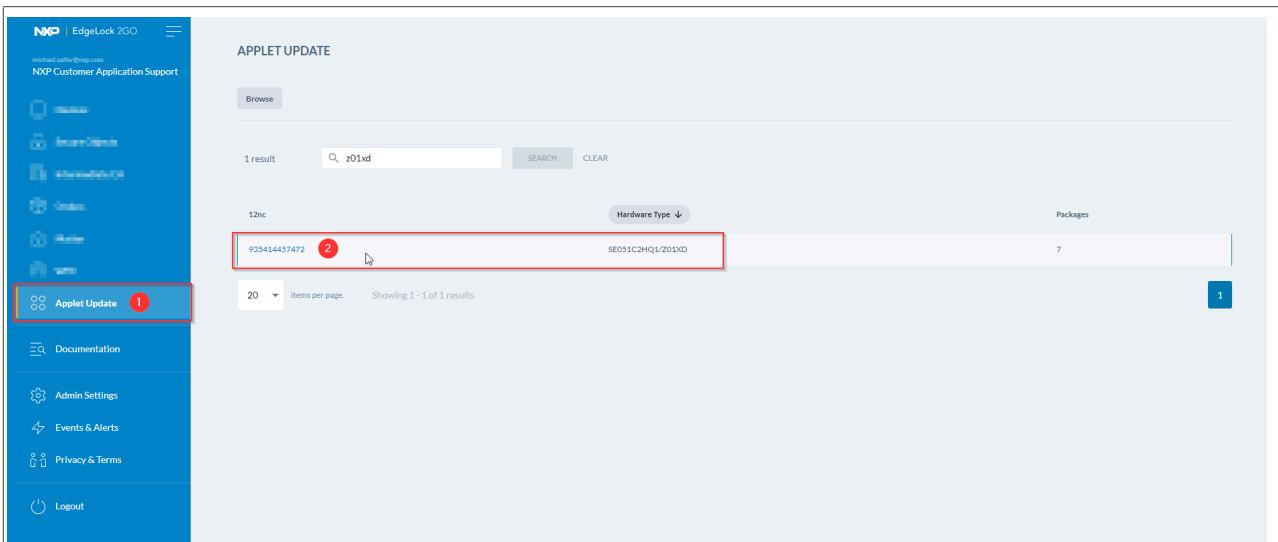
Figure 12. Open Applet Update page in EdgeLock 2GO

2. In the new page that appears you can see the list of available packages as shown in Figure 13:

(1) In the list you can find information on the package name and version. Select the IoT applet update package corresponding to the version that you want to upgrade to.

(2) Click on the *Download* icon to download the script in JSON format. Save the script in your preferred location.

Note: *EdgeLock SE051 already contains IoT applet version 6.0 or 7.2. The 6.0 and 7.2 IoT Applet update recovery are special scripts which needs only be used in case the update to version 6.1 resp. 7.3 fails due to an internal logical error.*

(3) You can copy the SHA-512 checksum of the file in your clipboard. You can use this value to check the integrity of the script when you transfer it to the IoT device.
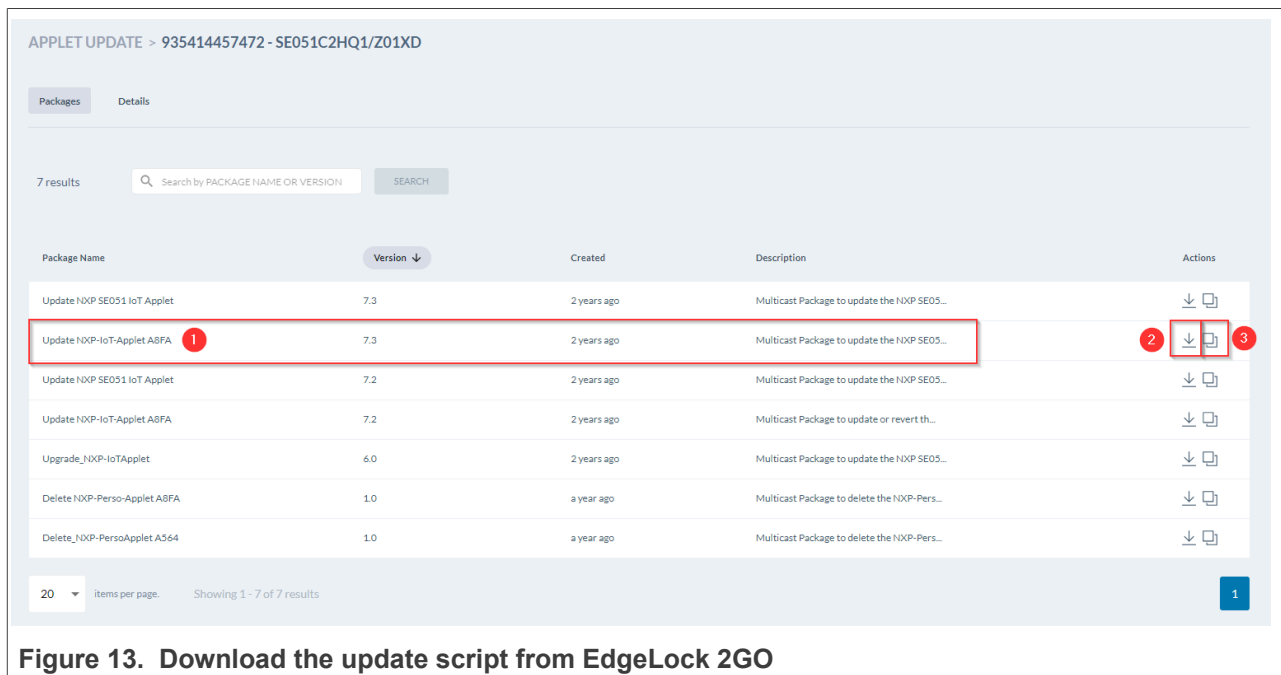
Figure 13. Download the update script from EdgeLock 2GO

5 Run an IoT applet update script in EdgeLock SE051

This section describes how to use the software examples included in the EdgeLock SE051 Plug & Trust middleware to execute an IoT applet update script using SEMS Lite.

Go to Section 5.1 for the list of hardware material that is used throughout this document for evaluation purposes. Make sure to setup the boards as described in Section 5.2 before running the examples.

Two examples are presented in the following sections:

SEMS Lite Agent Demo: this example provides a reference implementation of the SEMS Lite Agent. The example code can be adapted and recompiled to run a SEMS Lite update script. Go to Section 5.4 to learn how to compile and run the SEMS Lite Agent demo example in the IoT device. Before running the example make sure you have downloaded the IoT applet update script from EdgeLock 2GO (`.json` file) and converted it to a format suitable for the example (`.h` and `.c` files) as described in Section 5.3.

SEMS Lite CLI Tool: this CLI tool can be conveniently used to execute SEMS Lite scripts in EdgeLock SE051 using a simple command line interface. Go to Section 5.5 to learn how to execute the SEMS Lite script in EdgeLock SE051 using the SEMS Lite CLI tool. Before running the example, make sure you have downloaded the IoT applet update script from EdgeLock 2GO (`.json` file) and converted it to a supported format (`.bin` file) as described in Section 5.3.

5.1 Hardware required

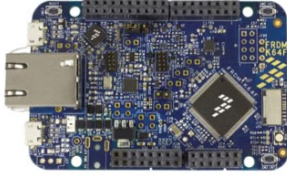The ordering details of the boards used for running the examples in this section are:

1. OM-SE051ARD development kit:

Table 1. OM-SE051ARD development kit details

Part number	12NC	Content	Picture
OM-SE051ARD	935399187598	EdgeLock SE051 development board	

2. FRDM-K64F board:

Table 2. FRDM-K64F details

Part number	12NC	Content	Picture
FRDM-K64F	935326293598	Freedom development platform for Kinetis K64, K63 and K24 MCUs	

5.2 Boards setup

This section explains how to prepare the OM-SE051ARD board and FRDM-K64F board. This consists of:

1. Update FRDM-K64F with DAPLink firmware
2. Hardware setup for FRDM-K64F
3. OM-SE051ARD and FRDM-K64F board connection.

5.2.1 Update FRDM-K64F board with DAPLink firmware

Arm Mbed DAPLink is an open-source software project that enables programming and debugging application software running on Arm Cortex CPUs. DAPLink runs an open-source bootloader and enables developers with drag-and-drop programming, a serial port and CMSIS-DAP based debugging.

Note: To debug MCUXpresso project examples, we need to flash FRDM-K64F with DAPLink firmware. If your FRDM-K64F board already includes DAPLink firmware, you can skip these steps.

To flash DAPLink firmware, follow these steps:

1. Go to NXP OpenSDA site
2. Scroll down and select FRDM-K64F board from the **Download - OpenSDA bootloader and application** drop down list as indicated in Figure 14:

Figure 14. DAPLink firmware update - select board

3. Download the latest DAPLink firmware version as shown in :

Figure 15.   DAPLink firmware update - select board

4. Start the board's bootloader mode. To do so, (1) keep reset button pressed while (2) connecting the USB cable to the SDA USB port and release it after 1s (Figure 16):
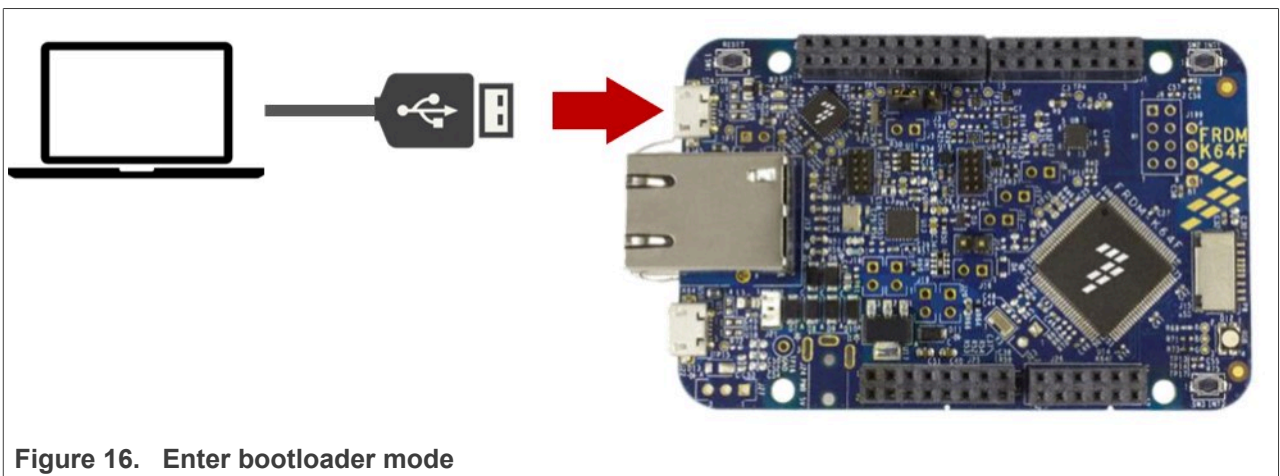

Figure 16.   Enter bootloader mode

5. Drag and drop or copy and paste the binary file into the BOOTLOADER drive from your computer file explorer as shown in Figure 17. The FRDM-K64F will automatically un-mount after the drag and drop operation.
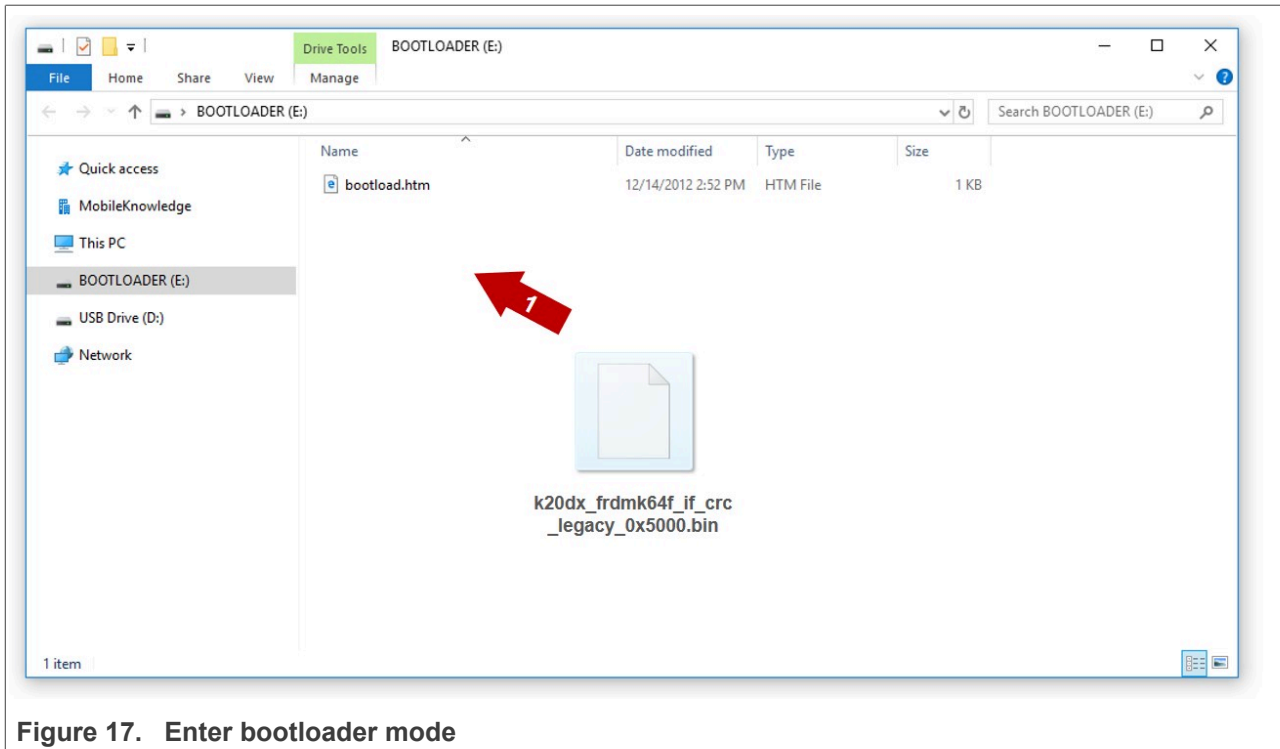
Figure 17. Enter bootloader mode

6. Un-plug and re-plug the USB cable from the SDA USB port *without* keeping reset button pressed.
7. Check the category Ports (COM & LTP) from your computer Device Manager to ensure that new devices have been properly detected and their driver was correctly installed by your computer OS.
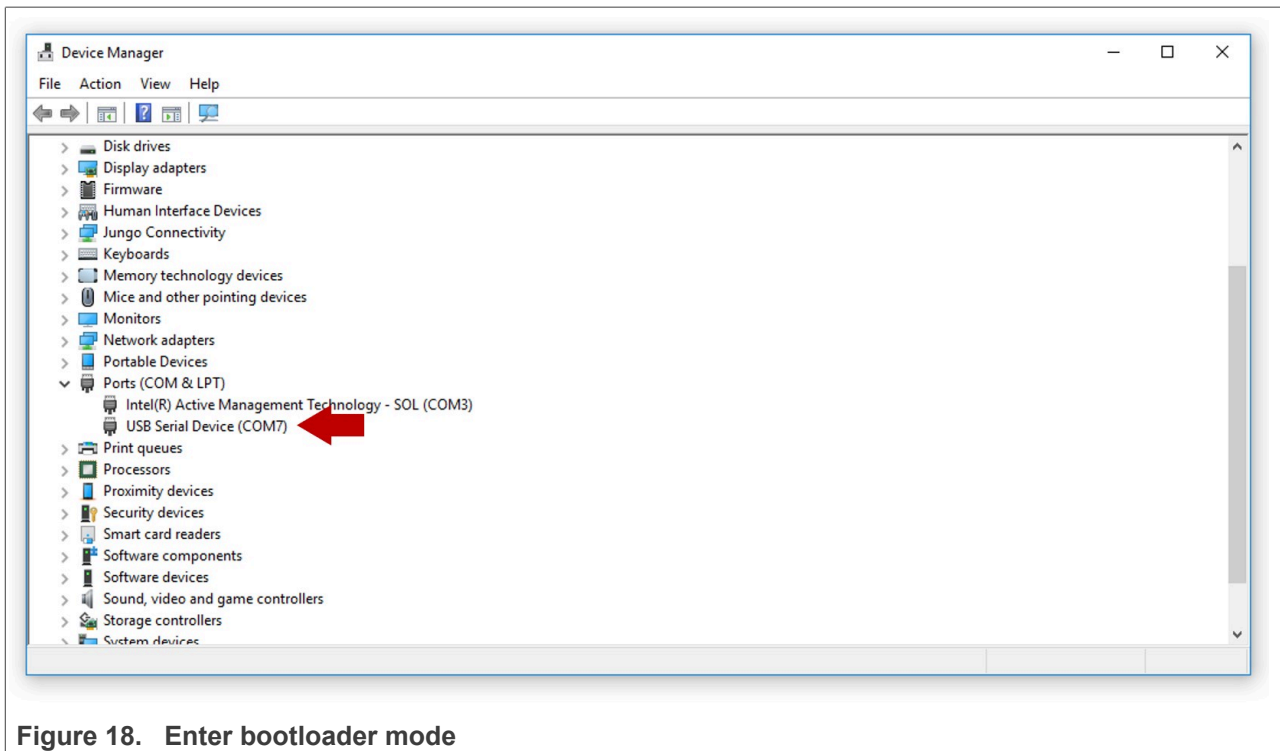

Figure 18. Enter bootloader mode

5.2.2 OM-SE051ARD jumper configuration

The OM-SE051ARD boards have jumpers that allow you to configure the I^{2}C interface of EdgeLock SE051 secure elements via the Arduino header. Configure the jumper settings as shown in Figure 19 to enable this option.

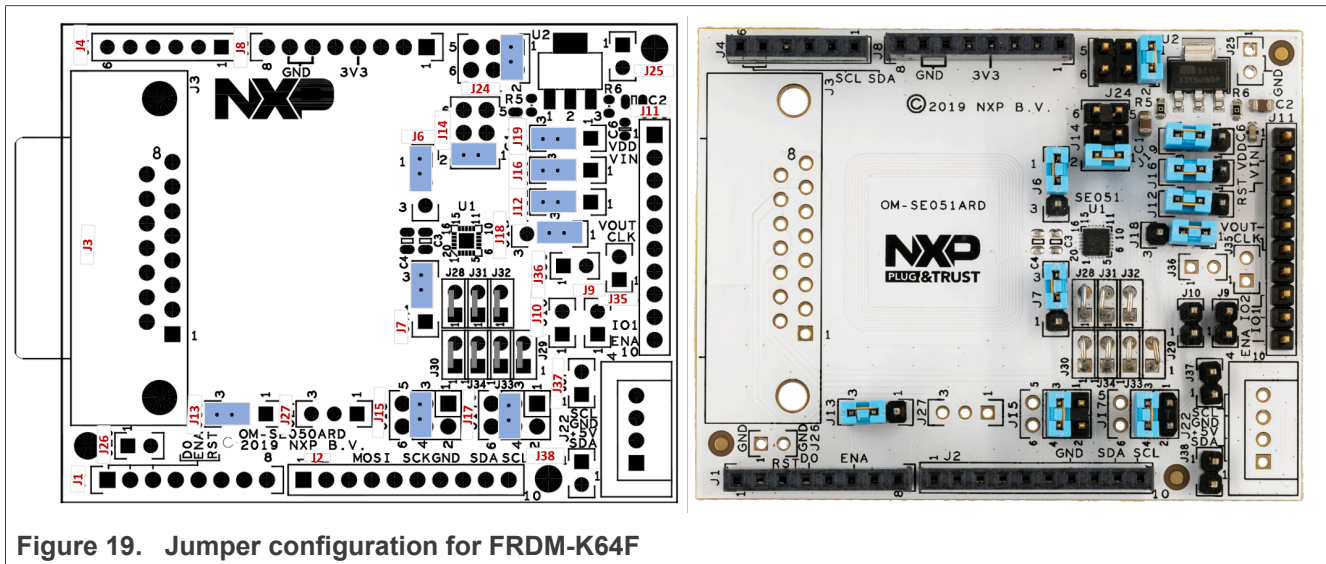*Note*: *For more information about the jumper settings, refer to AN13016.*

Figure 19. Jumper configuration for FRDM-K64F

5.2.3 OM-SE051ARD and FRDM-K64F board connection

The OM-SE051ARD boards and FRDM-K64F board can be directly connected using the Arduino connectors. The OM-SE051ARD boards come with male connectors while the FRDM-K64F board comes with female headers.

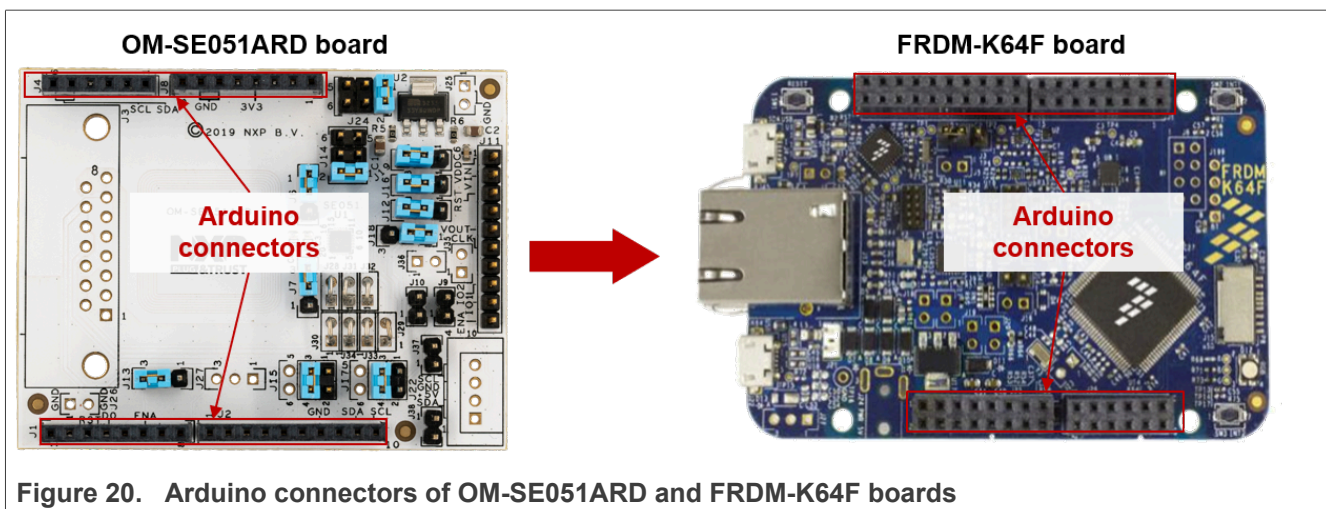Mount any OM-SE051ARD board on top of the FRDM-K64F as shown in Figure 20:

Figure 20. Arduino connectors of OM-SE051ARD and FRDM-K64F boards

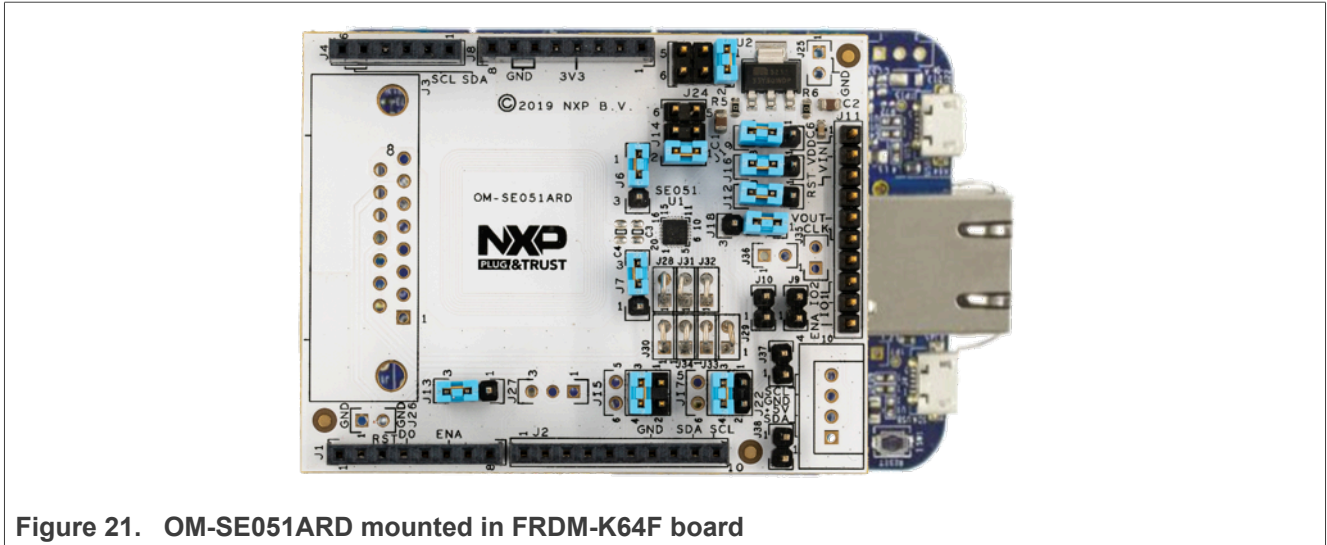Double check that the two boards are connected as shown in Figure 21:

Figure 21.   OM-SE051ARD mounted in FRDM-K64F board

Note: *Refer to [Figure 19](#) for OM-SE051ARD jumper configuration.*

5.3 Convert the IoT applet update script

IoT applet update packages can be downloaded from EdgeLock 2GO in JSON format. If you want to execute the SEMS Lite script, you must first convert it to a format that can be used either with the SEMS Lite Agent demo (`se05x_sems_lite_ex_update`) or with the SEMS Lite CLI tool (`sems_lite_cli_app`).

Follow these instructions to convert the IoT applet update script:

1. Download the EdgeLock SE051 Plug & Trust middleware package from the [NXP website](#). Unzip the file in a folder of your choice, for example `C:\se05x_middleware`;
2. Place the IoT applet update script in JSON format, as obtained from EdgeLock 2GO (see [Section 4.3](#)), in a folder of your choice, for example `C:\UpdateScript`;
3. Open a console window and navigate to the folder `<middleware_path>\simw-top\semslite\tools\sems-lite-generator`
4. Install the Python required dependencies necessary to run the *semslite_json_converter* tool and then convert the IoT applet update script as shown in [Figure 22](#):
   (1) Send > `python -m pip install -r requirements.txt`
   (2) Send > `python semslite_json_converter.py <update_script_path>`, where `<update_script_path>` is the path of the folder containing the IoT applet update script (e.g. `C:\UpdateScript`).
   (3) The converter tool will generate a set of files, including a binary file (`.bin`) that can be used with the SEMS Lite CLI tool (see [Section 5.5](#)) and a pair of C files (`.c` and `.h`) that can be used with the SEMS Lite Agent demo project (see [Section 5.4](#)).
   Note: if you don't have Python installed, you can download it from https://www.python.org/downloads/.
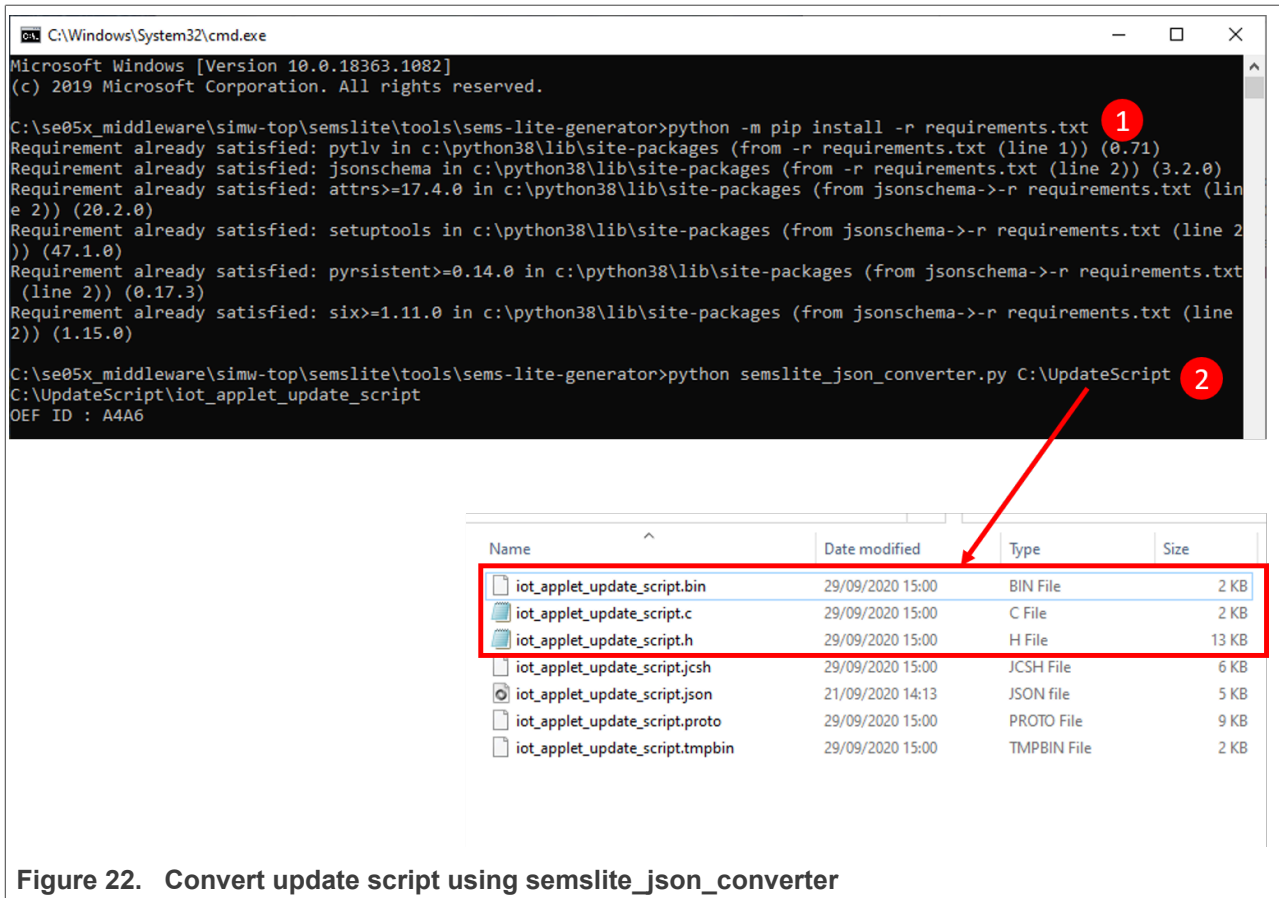   *Note: on windows it might be necessary to call "py" instead of "python"*

Figure 22.   Convert update script using semslite_json_converter

5.4 Run an IoT applet update script using the SEMS Lite Agent Demo

The SEMS Lite Agent demo project example included in the FRDM-K64F SDK demonstrates how to update the pre-loaded NXP IoT Applet in EdgeLock SE051. You can use any update script that you downloaded from EdgeLock 2GO as described in Section 4. For demonstration purposes in the present document the IoT applet will be updated from version 7.2 to version 7.3 as shown in Figure 23.

Note: *the update to version 7.3 does not add or change any functionality of the IoT applet and is used just to demonstrate the update capabilities of EdgeLock SE051.*
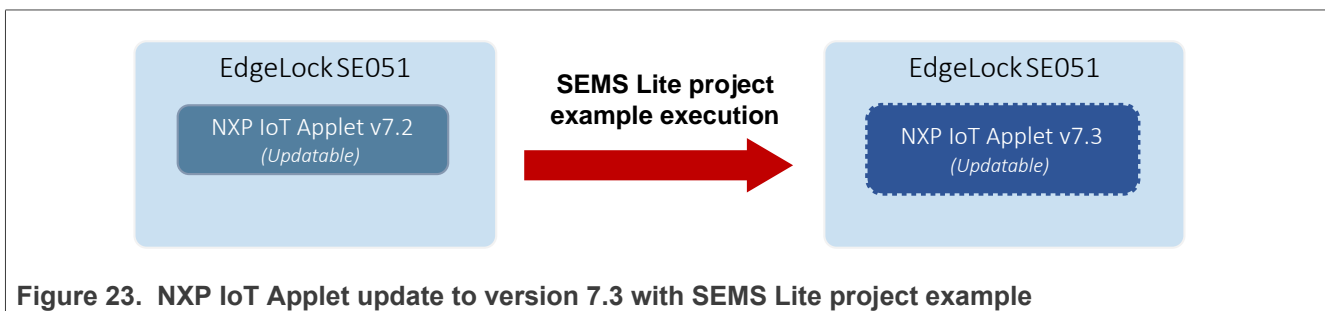

Figure 23. NXP IoT Applet update to version 7.3 with SEMS Lite project example

AN12907

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Application note

Rev. 1.2 — 23 November 2023
641112

20 / 43

The SEMS Lite Agent demo project example leverages the EdgeLock SE051 Plug & Trust middleware SEMS Lite agent API to update the IoT applet in EdgeLock SE051. The sequence of API calls required to achieve this result is shown in Figure 24.

Figure 24. EdgeLock SE051 Plug & Trust middleware SEMS Lite API calls to update IoT applet
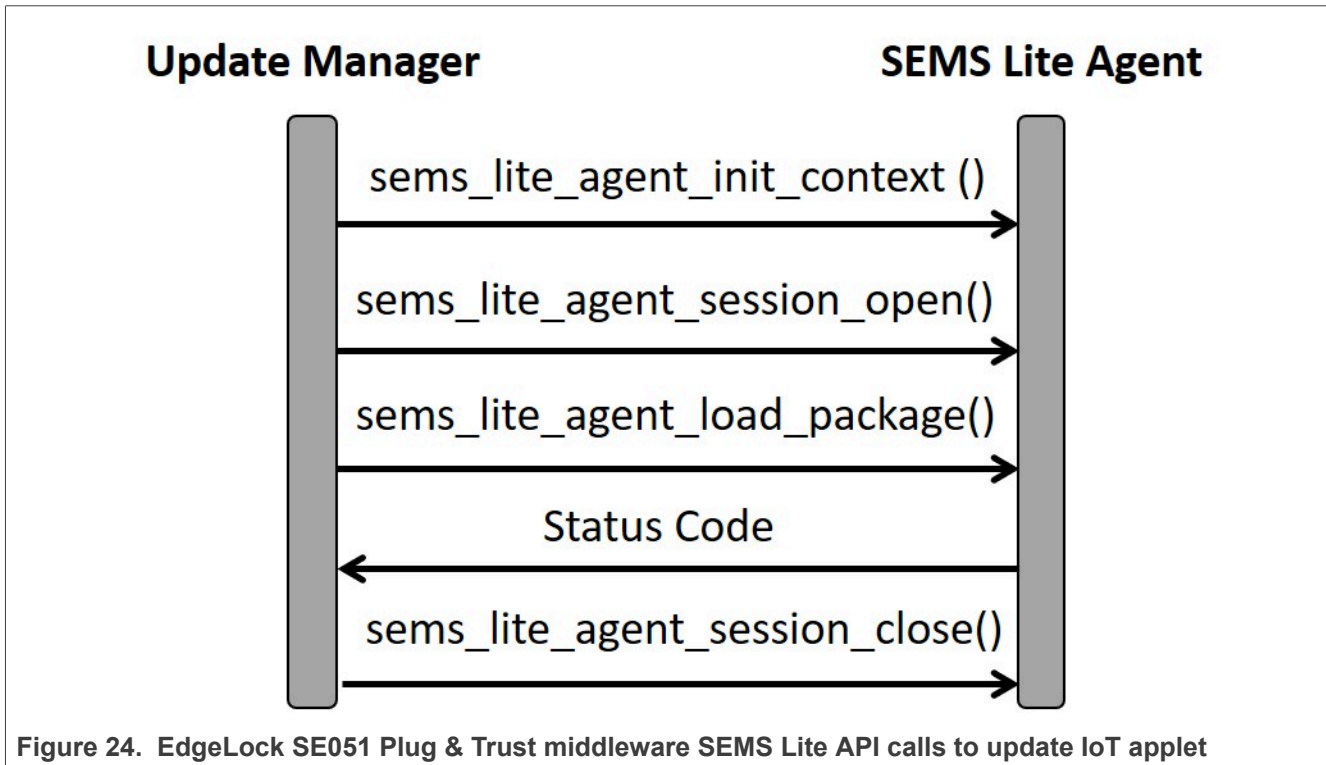
After initializing the SEMS Lite Agent context object with `sems_lite_agent_init_context()` function, a new session is opened with the SEMS Lite Agent using `sems_lite_agent_session_open()`. The `sems_lite_agent_load_package()` function receives as input the IoT applet update script and instructs the SEMS Lite Agent to execute the script. The status code returned by `sems_lite_agent_load_package()` informs about the outcome of the SEMS Lite script execution. Finally, the session is closed using the `sems_lite_agent_session_close()` function.

This section explains how to run the EdgeLock SE051 SEMS Lite project example included in the FRDM-K64F SDK.

Note: *The SEMS Lite project example can be executed more than once. However, if the NXP IoT applet is already in version 7.3, its contents will not change.*

5.4.1 Software requirements

The following software is required:

1. MCUXpresso IDE.
2. TeraTerm or an equivalent serial application.
3. FRDM-K64F SDK, publicly available from the NXP website.

5.4.2 Install FRDM-K64F SDK

After downloading the FRDM-K64F SDK, we need to install it in the MCUXpresso workspace. To install the SDK, (1) drag and drop the FRDM-K64F SDK zip file in the *Installed SDKs* section in the bottom part of the MCUXpresso IDE and (2) click *OK* as shown in Figure 25:
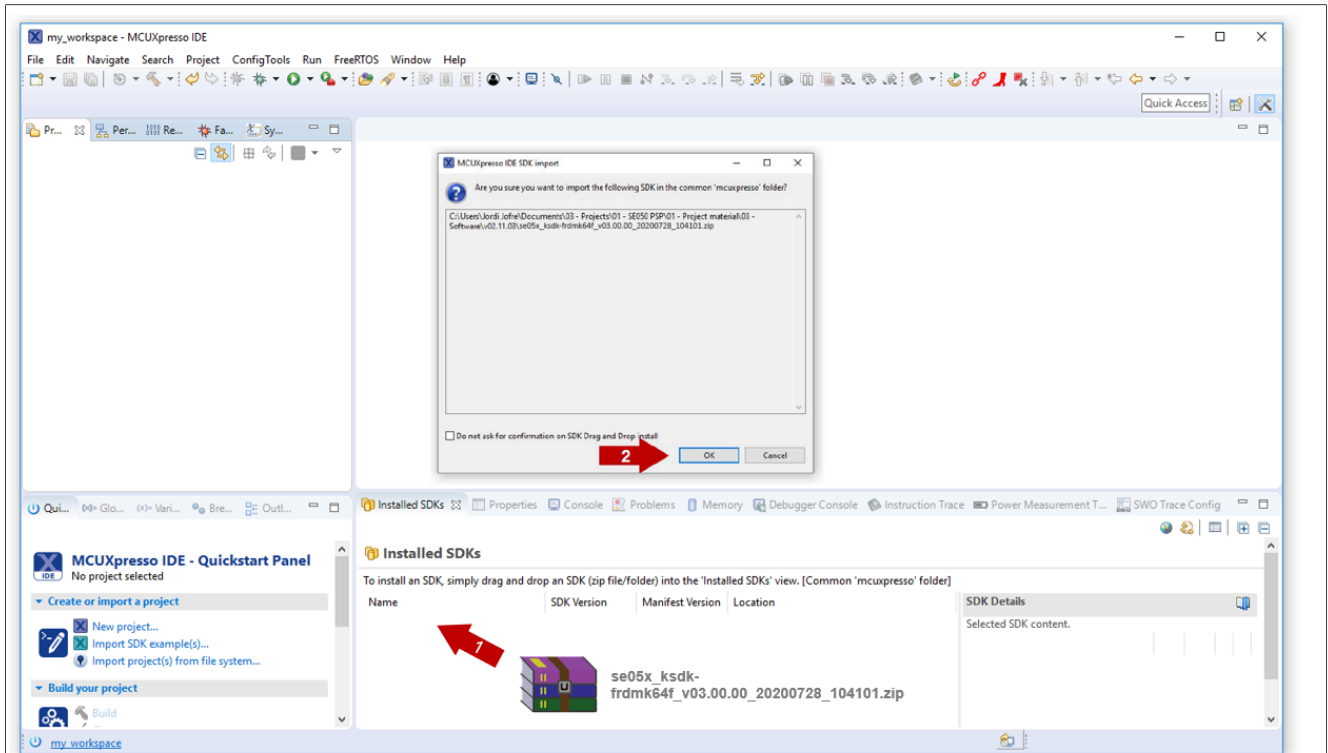

Figure 25.   Import FRDM-K64F board SDK into MCUXpresso environment

If the SDK is successfully imported, you should see it listed in the *Installed SDK* window as shown in Figure 26:
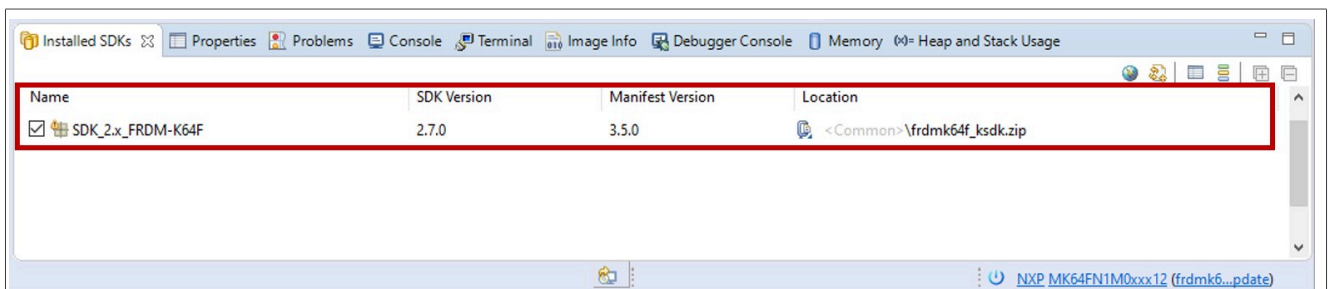

Figure 26.   Imported FRDM-K64F SDK

5.4.3 Import SEMS Lite update project in MCUXpresso

After installing the FRDM-K64F SDK in the MCUXpresso workspace, follow these instructions to import the SEMS Lite Agent demo example into the workspace:

1. Click *Import SDK examples* from file system in the MCUXpresso IDE quick start panel as shown in Figure 27
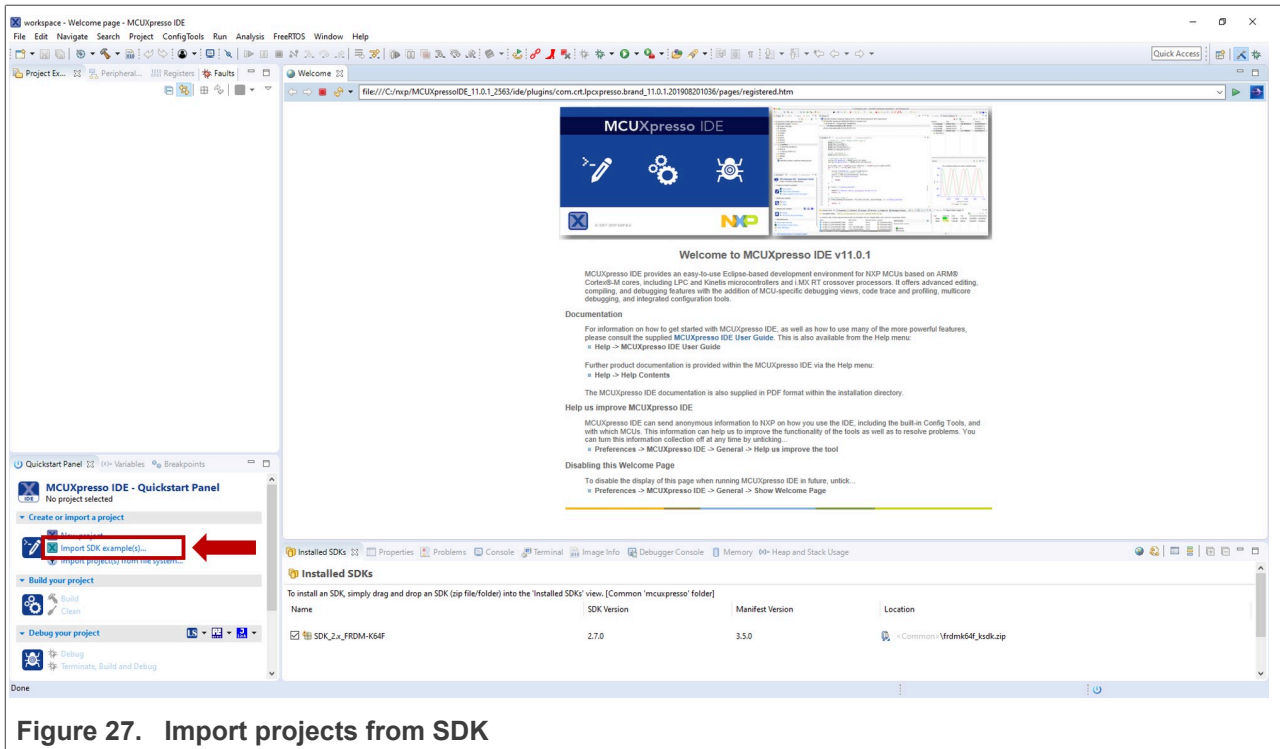
Figure 27.   Import projects from SDK

2. The SDK import wizard will be opened. You should see a figure of an FRDM-K64F board. Select the board and click the *Next* button as shown in Figure 28:
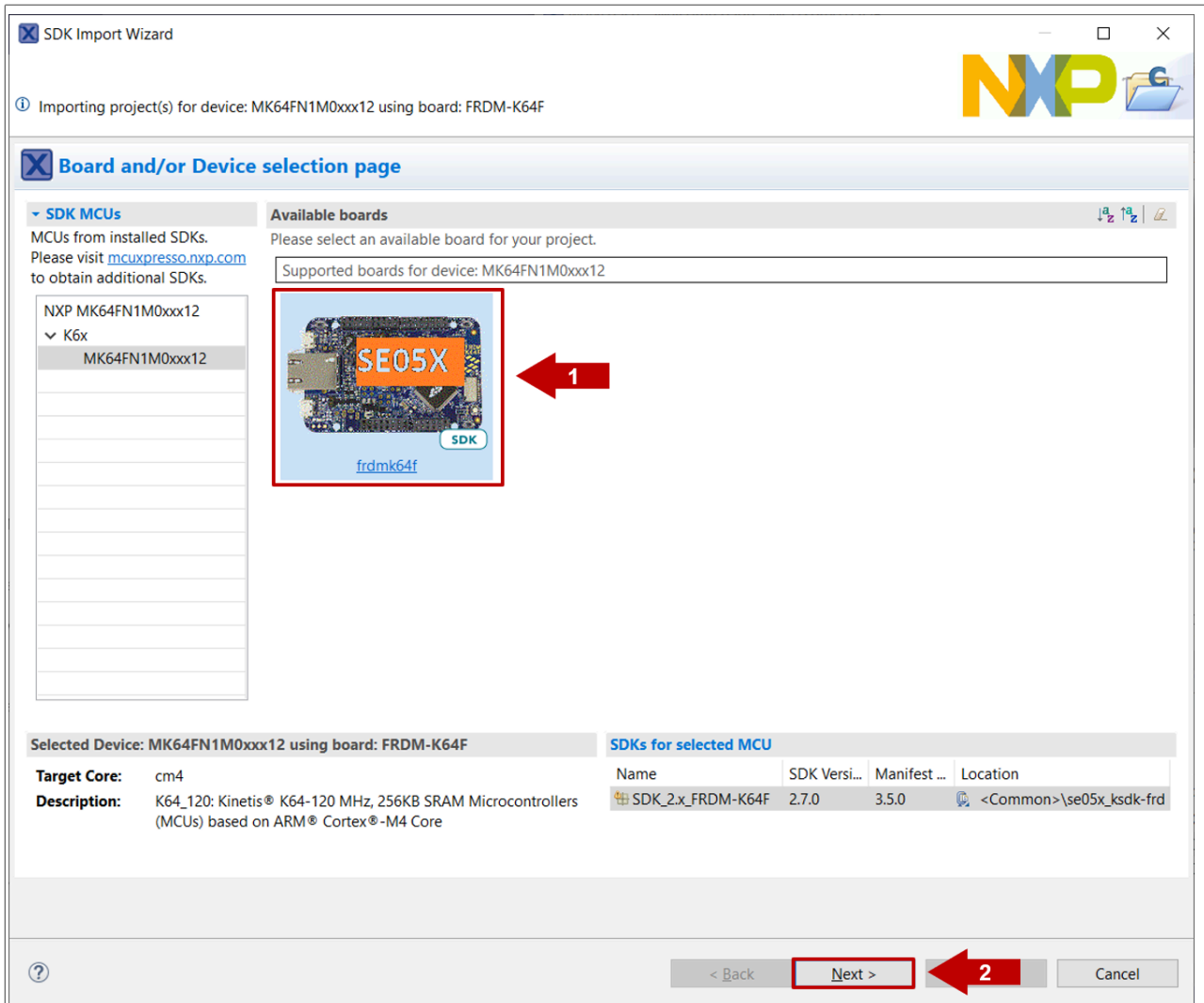
AN12907

Application note

All information provided in this document is subject to legal disclaimers.

Rev. 1.2 — 23 November 2023

641112

© 2023 NXP B.V. All rights reserved.

23 / 43

Figure 28.   SDK import wizard

3. The `se_hostlib_examples` drop down list shows the list of available project examples for the FRDM-K64F. Select the number of project examples you would like to import in your MCUXpresso workspace and click the *Finish* button. In this case, select the `se05x_sems_lite_ex_update` project as shown in Figure 29.
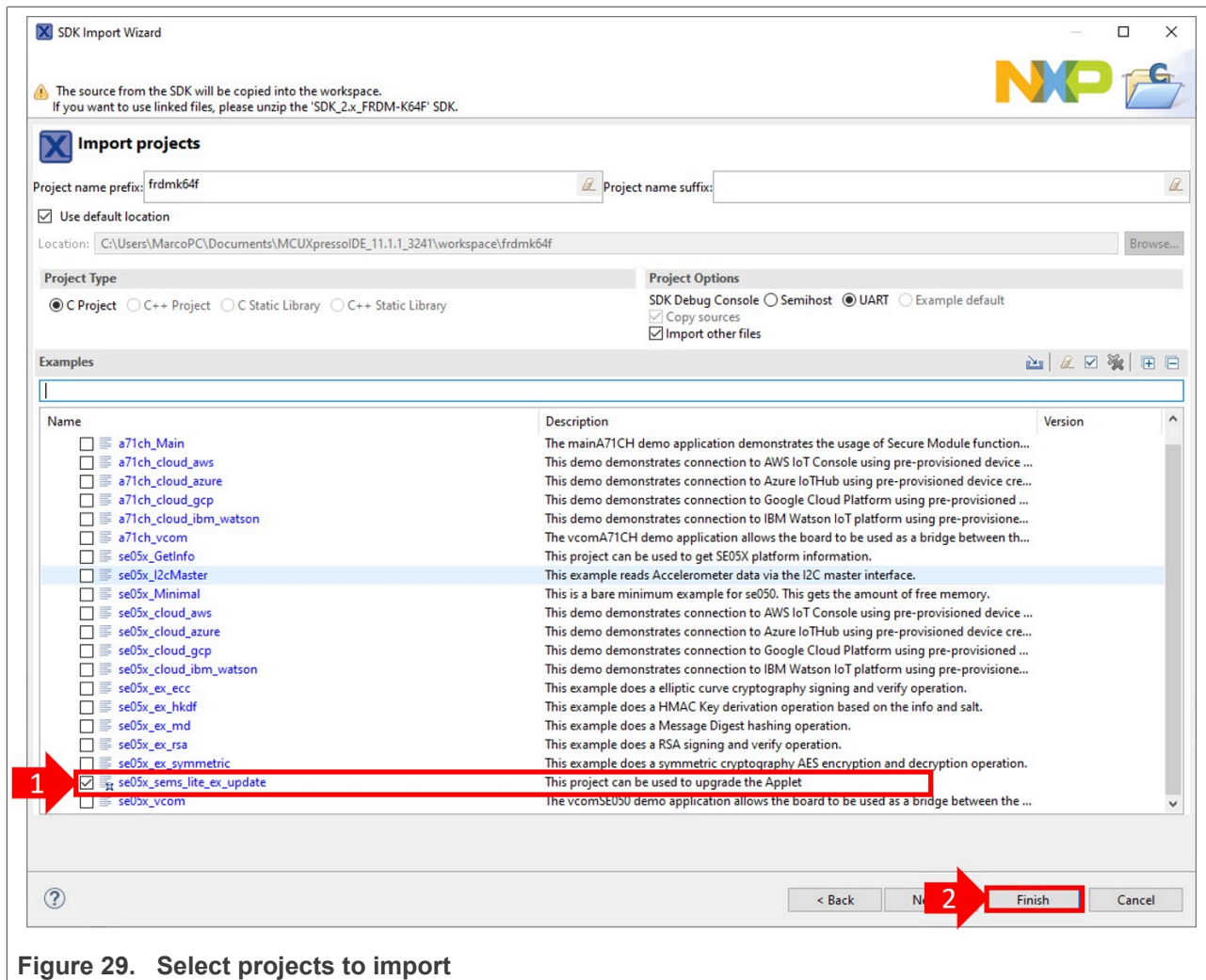
Figure 29.   Select projects to import

4. The `frdmk64f_se05x_sems_lite_ex_update` project should now be visible in the MCUXpresso workspace as shown in Figure 30:
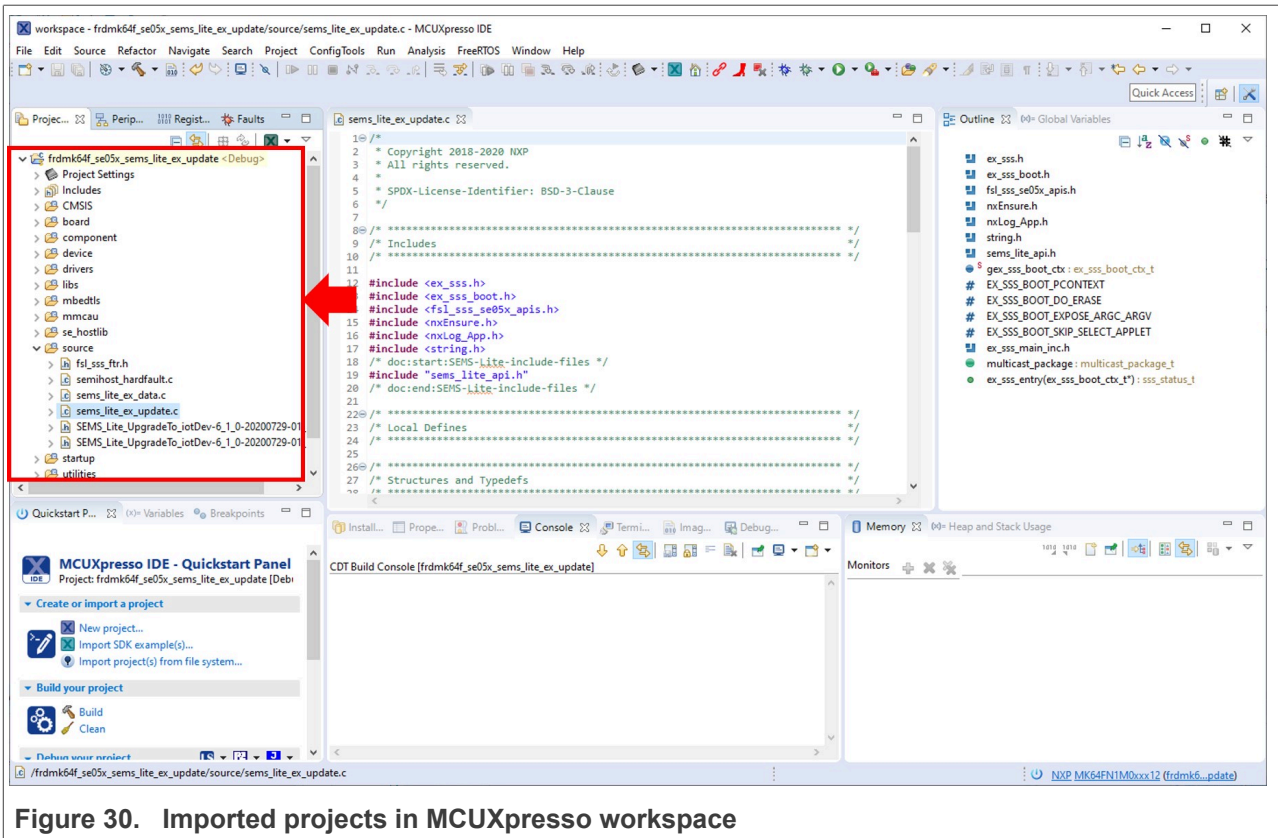
Figure 30.   Imported projects in MCUXpresso workspace

5.   Make sure you have converted the JSON script downloaded from EdgeLock 2GO to `.h` and `.c` files as described in Section 5.3, then add to the example project the script to update the IoT applet as shown in Figure 31:

(1) Copy the `.h` file obtained from the conversion (in our case `iot_applet_update_script.h`) to the `source` folder in MCUXpresso;

(2) Open the `sems_lite_ex_data.c` file in the `source` folder in MCUXpresso and substitute its entire content with the content of the `.c` file obtained from the conversion of the script (in our case `iot_applet_update_script.c`). Save the changes.

Figure 31.   Add the IoT applet update script to the example
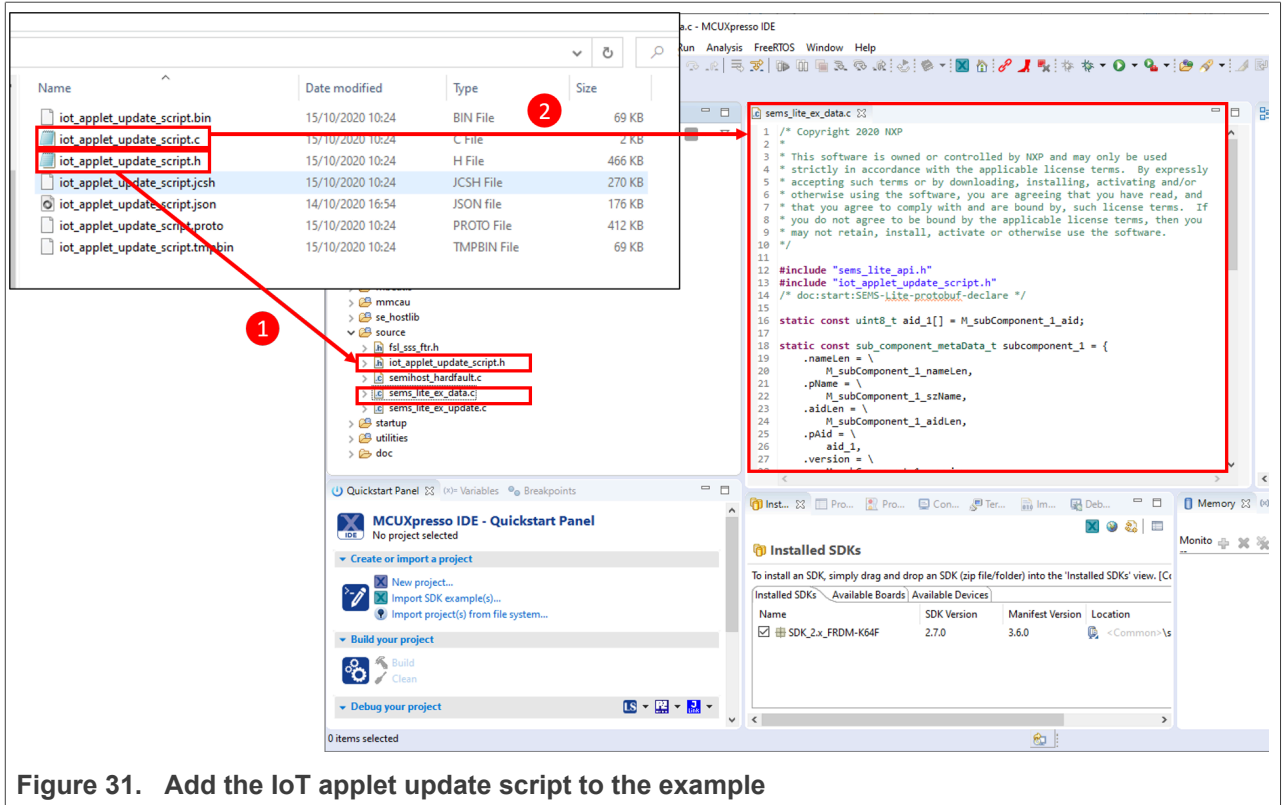
5.4.4 Build, run and debug SEMS Lite project example

After importing the SEMS Lite Agent demo example in the MCUXpresso workspace, follow these instructions to build, run and debug the project:

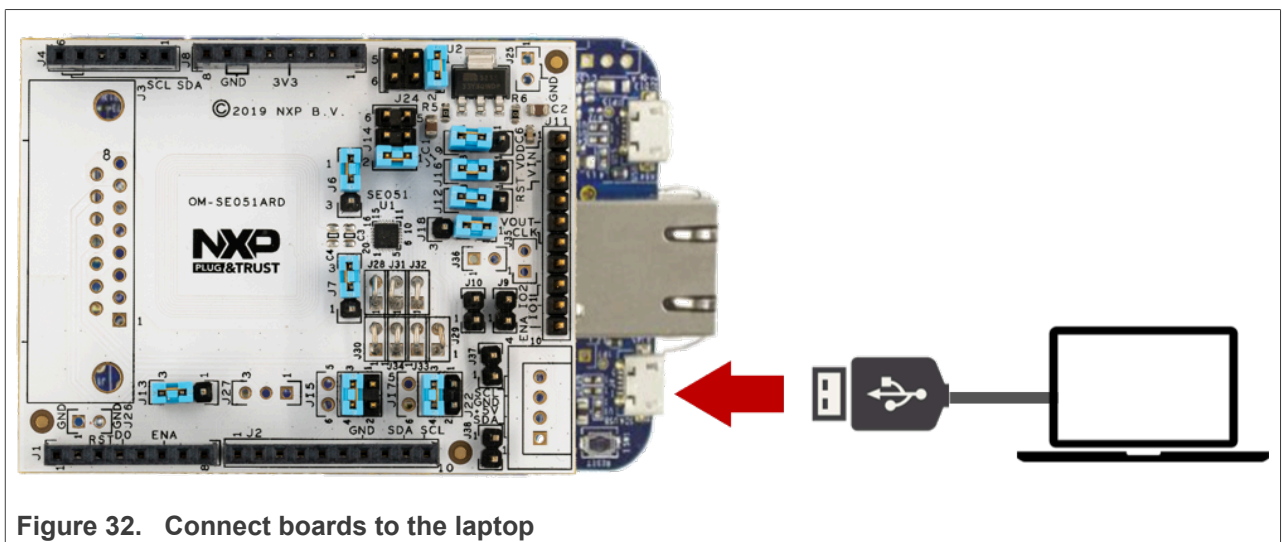1. Attach a USB cable from the computer to the K64F OpenSDA debug USB connector as shown in Figure 32.

Figure 32.   Connect boards to the laptop

2. Launch and setup TeraTerm application as shown in Figure 33:
   a. Click *Serial* option and select from the drop down list the COM port number assigned to your FRDM-K64F board
   b. Go to *Setup > Serial Port* and configure the terminal to 115200 baud rate, 8 data bits, no parity and 1 stop bit and click OK.
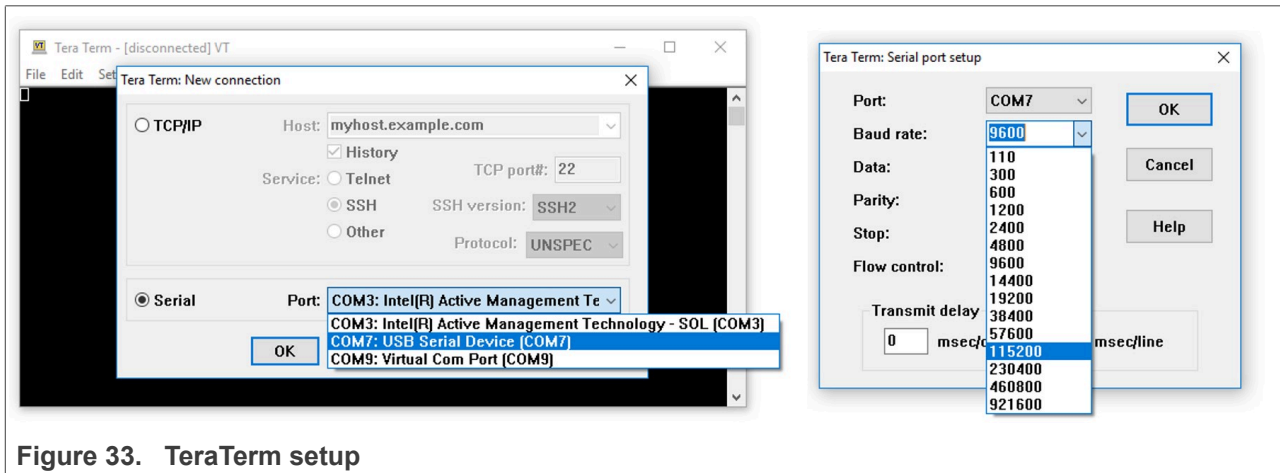

Figure 33.   TeraTerm setup

3. Go to the MCUXpresso Quickstart Panel and click *Build* button as shown in Figure 34. Wait a few seconds and check that the build process has finished successfully in the MCUXpresso console window.
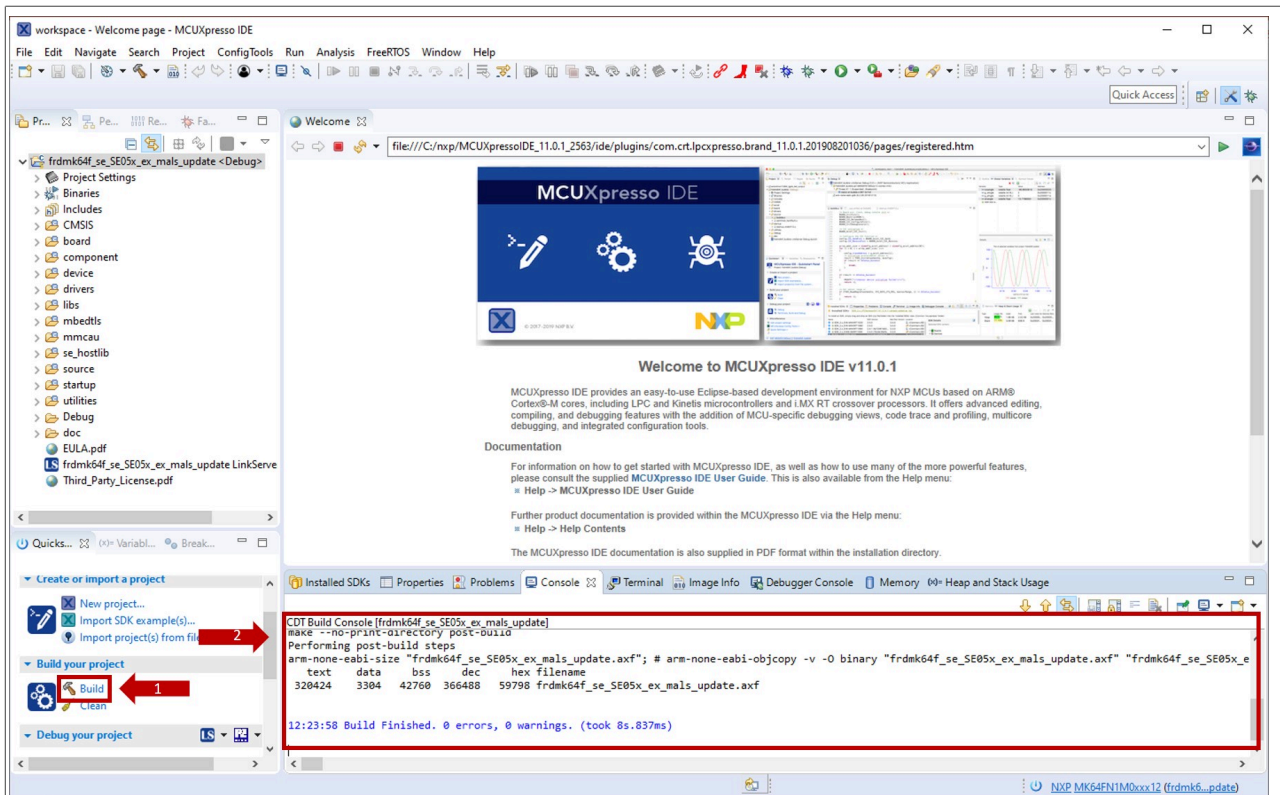

Figure 34.   Build projects in MCUXpresso workspace

AN12907

Application note

All information provided in this document is subject to legal disclaimers.

Rev. 1.2 — 23 November 2023

641112

© 2023 NXP B.V. All rights reserved.

28 / 43

4. Go to the MCUXpresso Quickstart Panel and click the *Debug* button as shown in Figure 35. If there is more than one probe attached, you have to select CMSIS-DAP debug probe from the list. Wait a few seconds until the project starts the execution.
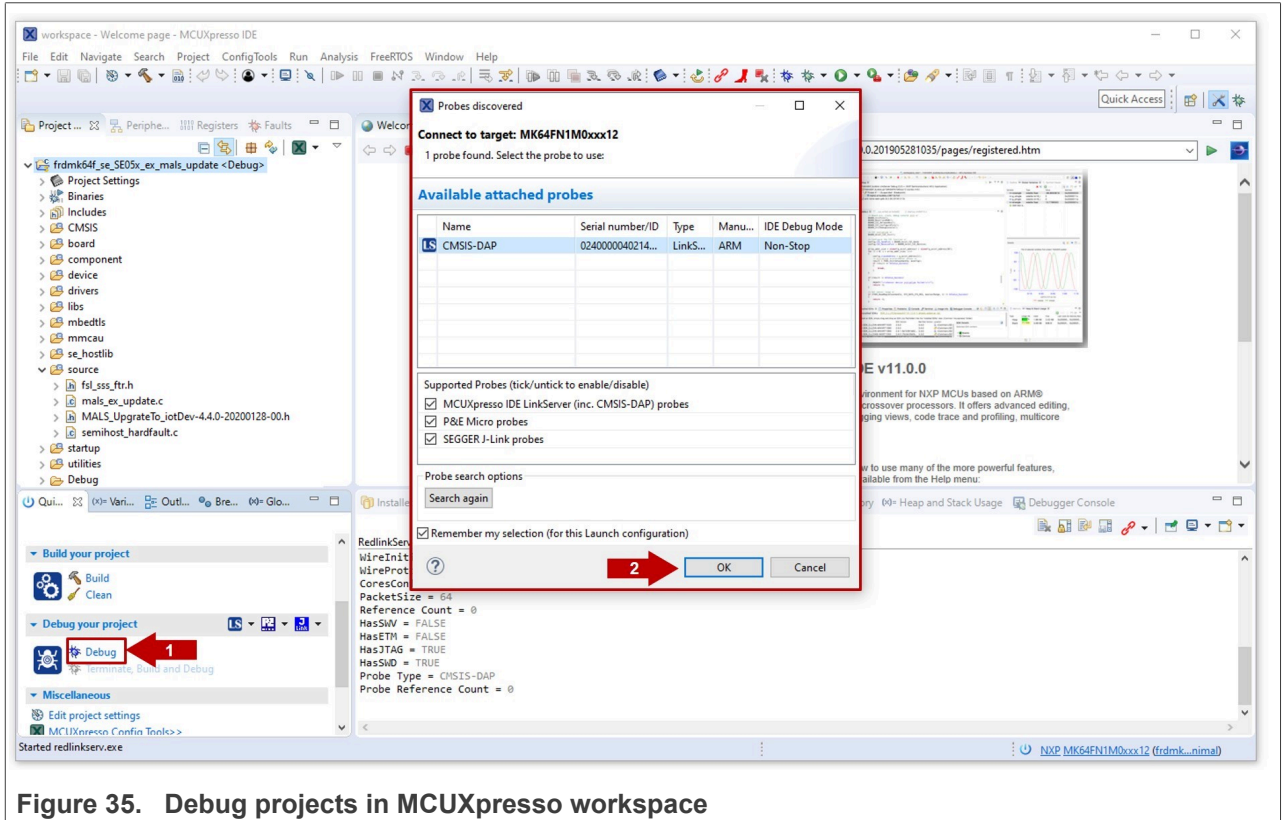

Figure 35. Debug projects in MCUXpresso workspace

5. When the execution starts, it will automatically stop in a breakpoint. Click on *Resume* to allow the software to continue its execution as shown in Figure 36.
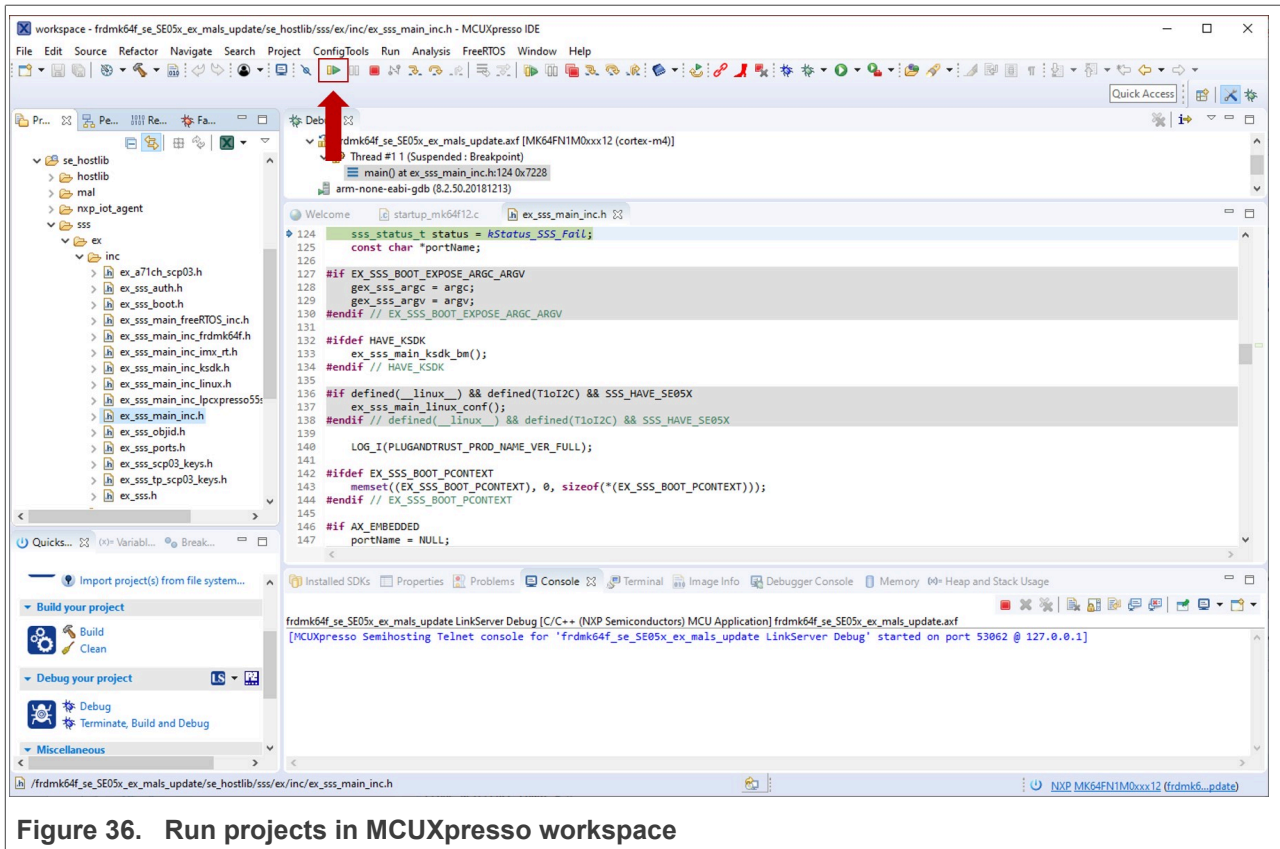
Figure 36.   Run projects in MCUXpresso workspace

6. Once the program execution continues, logs are printed in the terminal application. If the `frdmk64f_se05x_sems_lite_ex_update` project runs successfully, you should see the *"Update Applet successful"* message in the logs as show in Figure 37. The IoT applet has now been updated to a new version (in this screenshot to version 6.1).
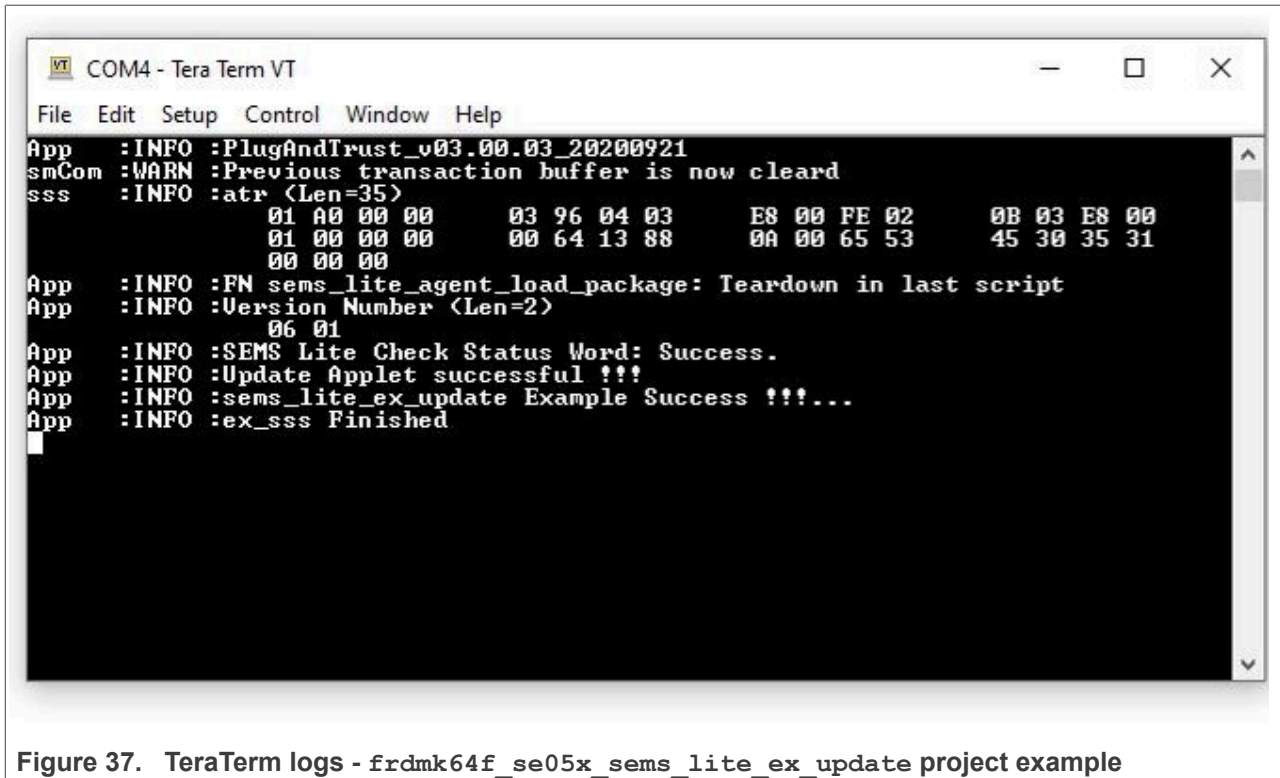
AN12907

Application note

All information provided in this document is subject to legal disclaimers.

Rev. 1.2 — 23 November 2023

641112

© 2023 NXP B.V. All rights reserved.

30 / 43

Figure 37. TeraTerm logs - `frdmk64f_se05x_sems_lite_ex_update` **project example**

5.5 Run an IoT applet update script using the SEMS Lite CLI

The SEMS Lite CLI is a tool included in the EdgeLock SE051 Plug & Trust middleware that allows users to easily execute SEMS Lite scripts in EdgeLock SE051 using only the PC and a VCOM connection to the target board (in our case the FRDM-K64F board). It is not required to compile or download any code in the target MCU.

5.5.1 Software requirements

Only the EdgeLock SE051 Plug & Trust middleware ZIP package, publicly available from the NXP website, is required. Extract the package content in a folder of your choice before proceeding.

5.5.2 Build the SEMS Lite CLI tool

- **Windows**: a pre-compiled executable of the SEMS Lite CLI tool is provided in the EdgeLock SE051 Plug & Trust middleware in the folder `<MW_installation_path>/simw-top/binaries/PCWindows`. The name of the executable is `VCOM-sems_lite_cli_app.exe`. This executable can be used without having to compile the middleware;
- **Other OSs:** the SEMS Lite CLI tool can be compiled for other OSs as well. Please refer to the Quick Start guide for your board and operating system available here. When compiling the tool, make sure that the following CMake compilation flags are set as shown in Figure 38 (`-DPTMW_SE05X_Ver=07_02 -DPTMW_SE05X_Auth=None`). The selected SE05x version needs to be at least 06.00.

In the present guide, the SEMS Lite CLI pre-compiled binary will be used as a reference, but instructions can be easily adapted to work on other platforms.
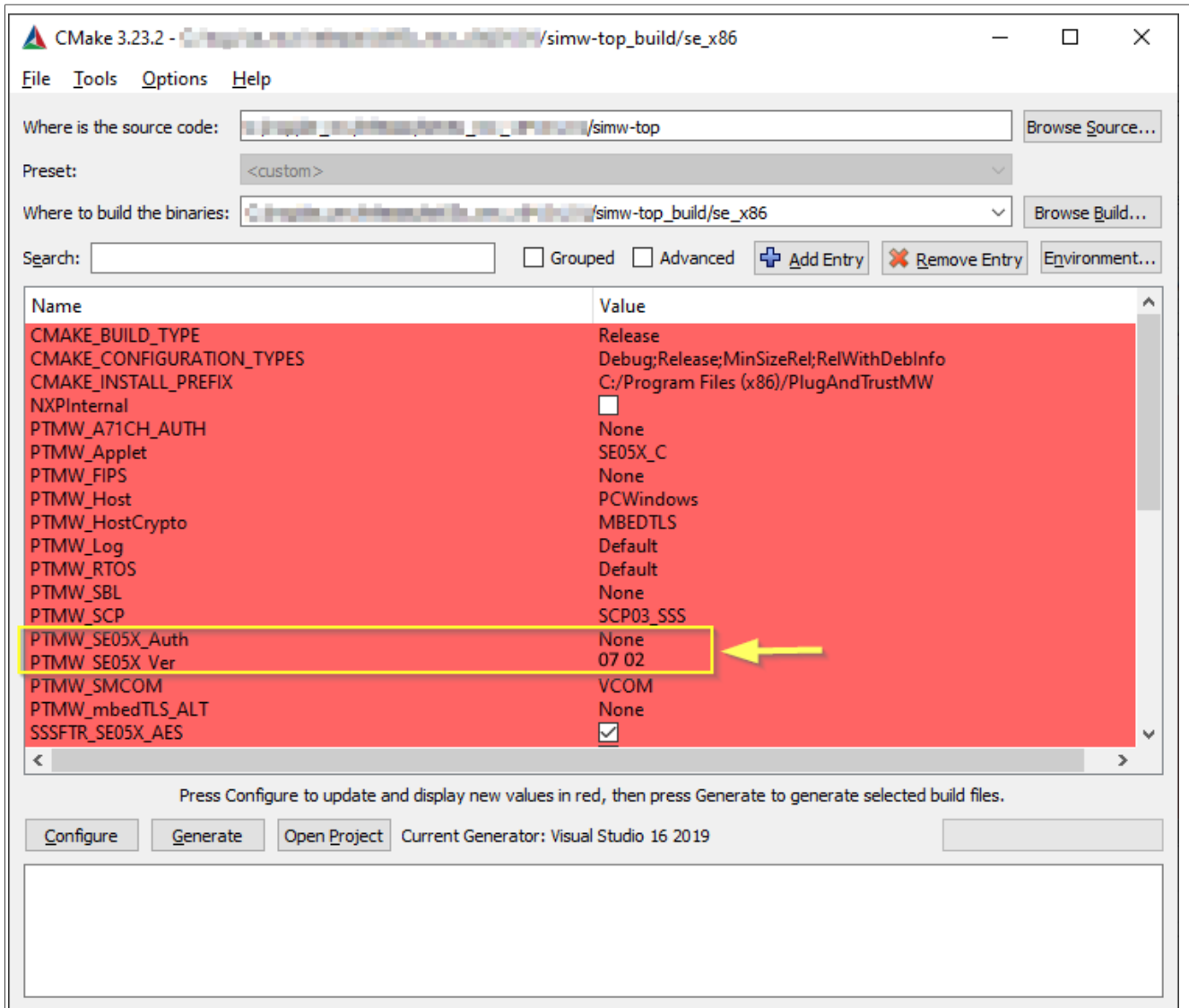
Figure 38. Set CMake flags

5.5.3 Install VCOM drivers

The SEMS Lite CLI executable uses the VCOM port to connect to the board. Follow these instructions to install the driver in the FRDM-K64F board:

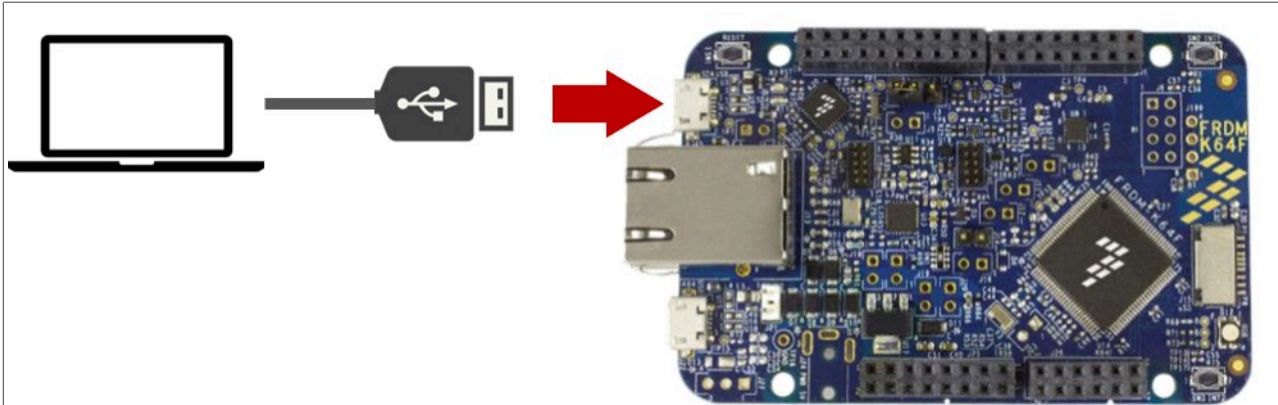1. Connect the FRDM-K64F board to the PC using the OpenSDA USB port as shown in Figure 40:

Figure 39.   Enter bootloader mode

2. Go to `<MW_installation_path>/simw-top/binaries/MCU/se05x`, locate the file `se05x_vcom-T1oI2C-frdmk64f` and then copy it in the FRDM-K64FD drive as shown in Figure 40:
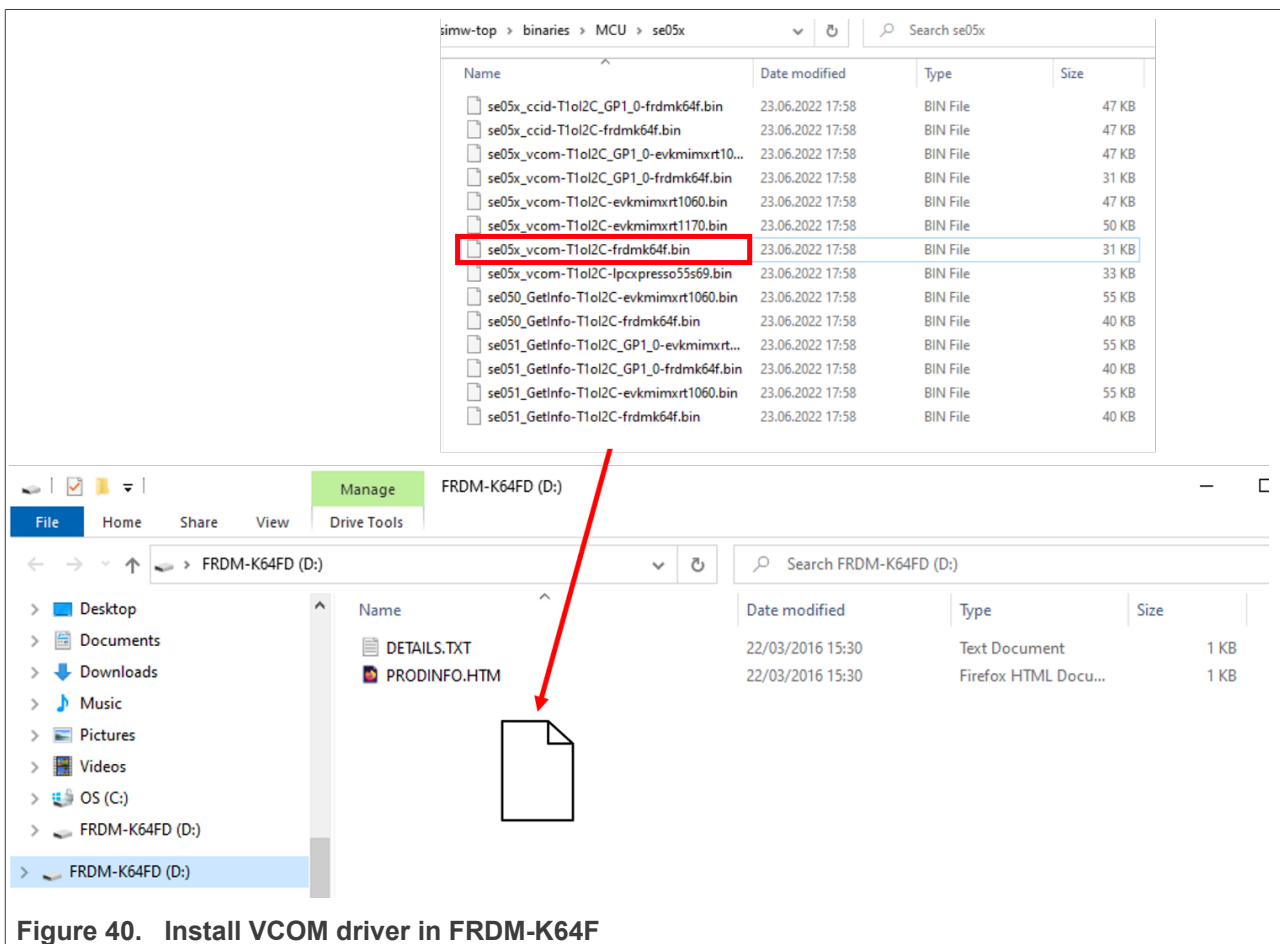

Figure 40.   Install VCOM driver in FRDM-K64F

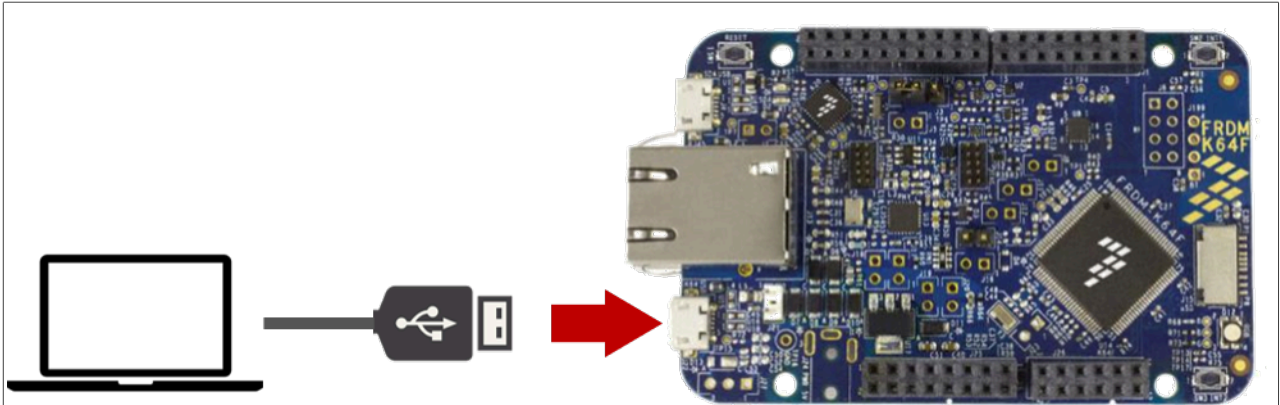3. Now connect the FRDM-K64F board to the PC using the K64 USB port as shown in Figure 41:

Figure 41. Connect FRDM-K64F usign VCOM

4. You should now see the VCOM port number in the device manager as shown in Figure 42:
   Note: the name and number of the port might be different in your system.
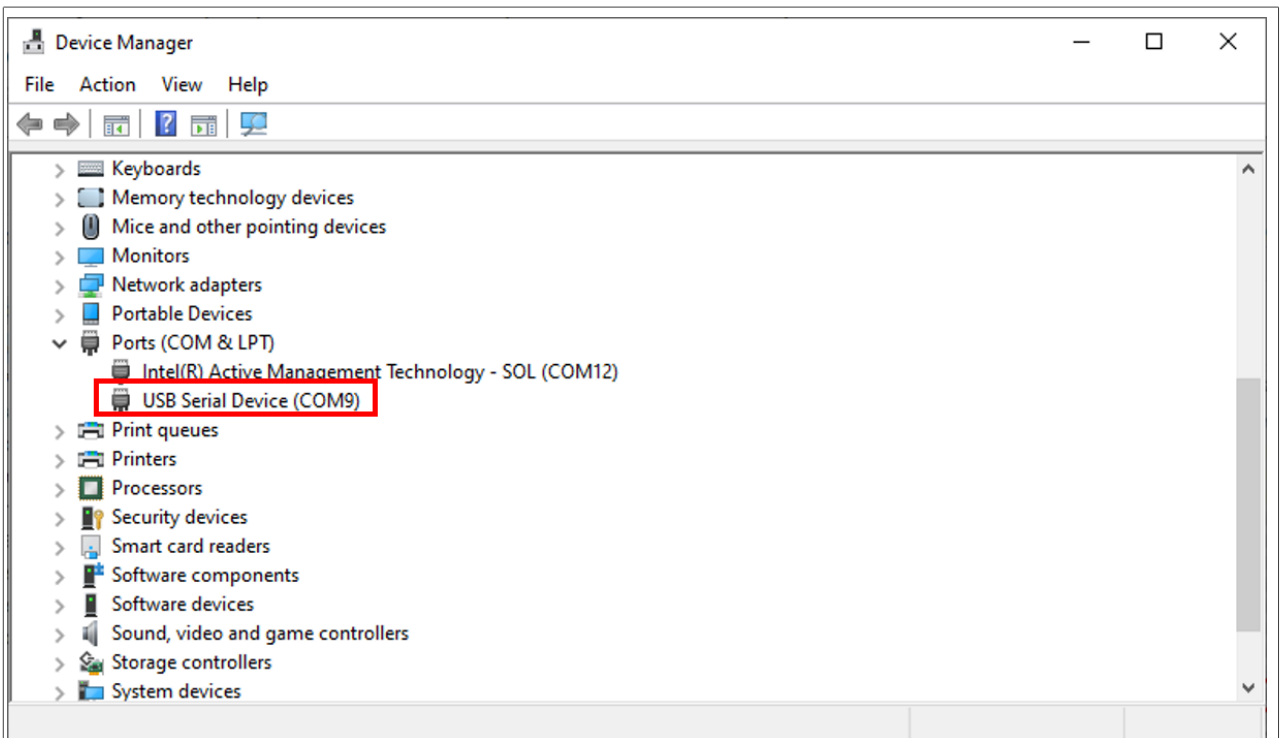

Figure 42. Retrieve VCOM port number

5.5.4 Use the SEMS Lite CLI and execute the IoT applet update script

Follow the instructions below to learn how to use the SEMS Lite CLI tool to execute an IoT applet update script in EdgeLock SE051:

1. To use the SEMS Lite CLI, open a console window, navigate to the folder where the pre-compiled executable is located (`<MW_installation_path>/simw-top/binaries/PCWindows`) and send the commands shown in Figure 43:

(1) Set the VCOM port number of the device:
Send > `SET EX_SSS_BOOT_SSS_PORT=<COM_PORT>`, where `<COM_PORT>` is the COM port used by the board (e.g. COM9).
(2) You can list all available SEMS Lite CLI tool parameters:
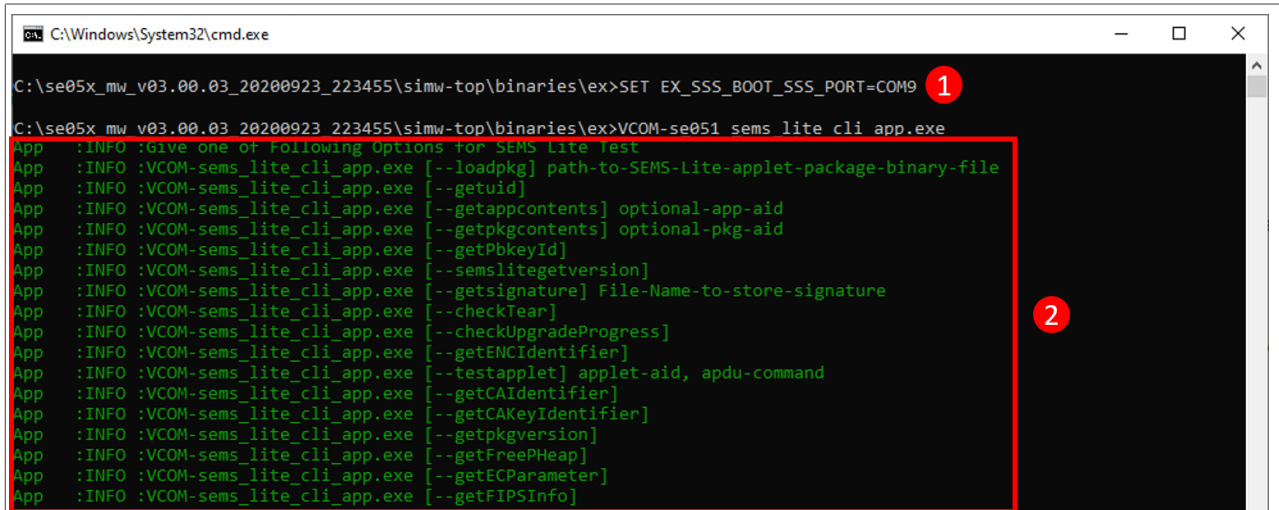Send > `VCOM-sems_lite_cli_app.exe`

Figure 43.   Use the SEMS Lite CLI tool

2. To execute the IoT applet update script that you have downloaded from EdgeLock 2GO, first convert the JSON script to `.bin` as described in Section 5.3, then use the SEMS Lite CLI tool to run the script as shown in Figure 44. Make sure that the FRDM-K64F board is connected to the PC using VCOM before proceeding. Send:
`VCOM-sems_lite_cli_app.exe --loadpkg <update_script_path>\<iot_applet_update_ script>.bin`
You will see a successful execution message.
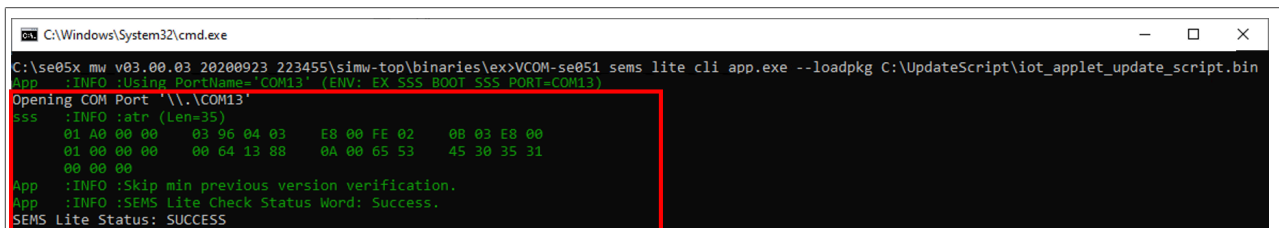

Figure 44.   Execute SEMS Lite script using SEMS Lite CLI

6   Appendix: Register an NXP account

Follow these steps to register an NXP account:

1. If you want to register a new account, visit https://www.nxp.com/webapp-signup/register, fill in the fields with your data and then click on the *Register* button as shown in Figure 45. Once this is done, an activation link will be sent to the email address you provided. Follow the instructions in the email to activate your NXP account.
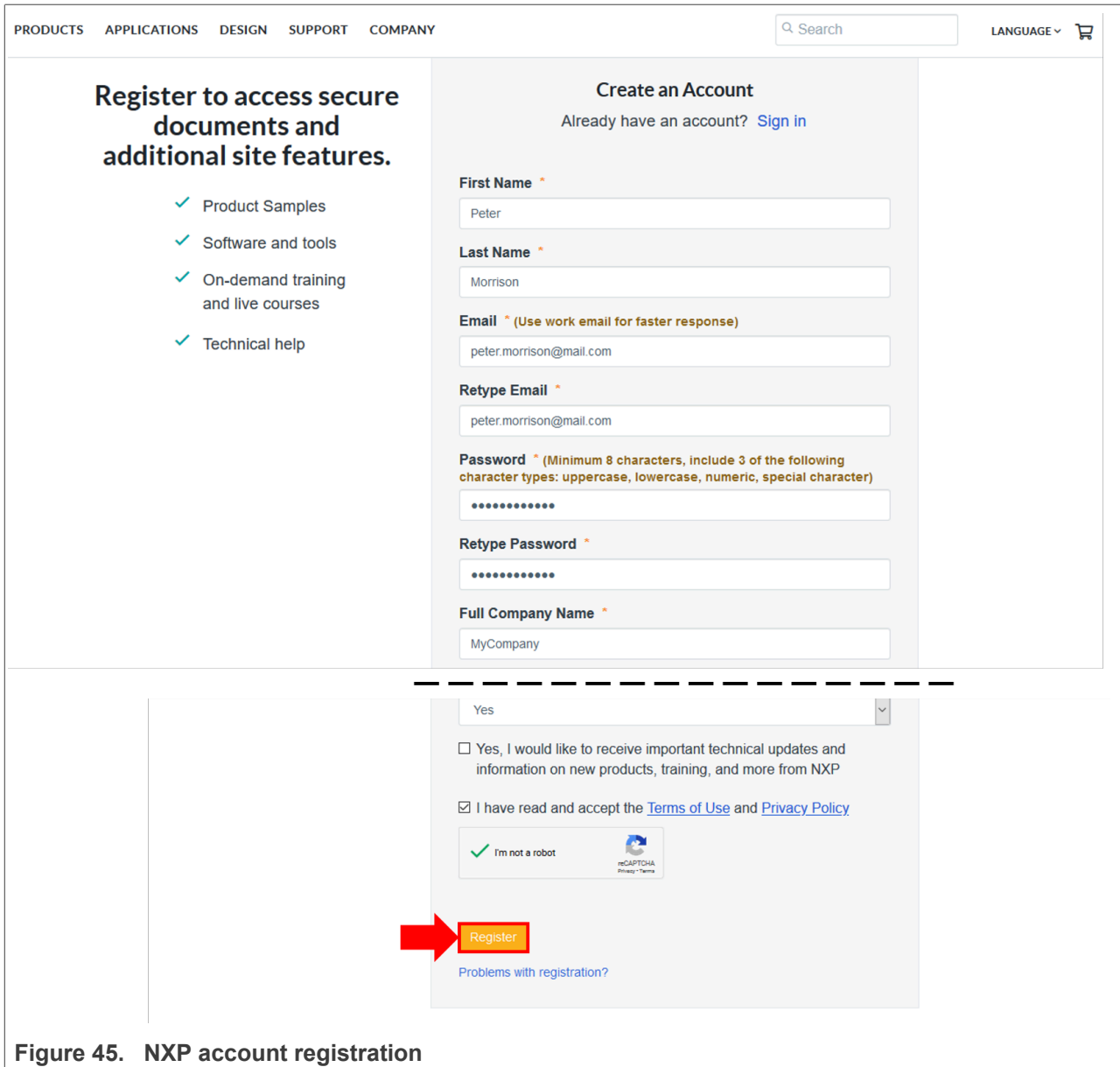
Figure 45. NXP account registration

2. When your NXP account is active, you should activate 2-Factor authentication for additional protection. Go to https://www.nxp.com/ruhp/myAccount.html, sign in with your NXP account and click on the *2-Factor Authentication (Off)* link as shown in Figure 46:

AN12907

Application note

All information provided in this document is subject to legal disclaimers.

Rev. 1.2 — 23 November 2023

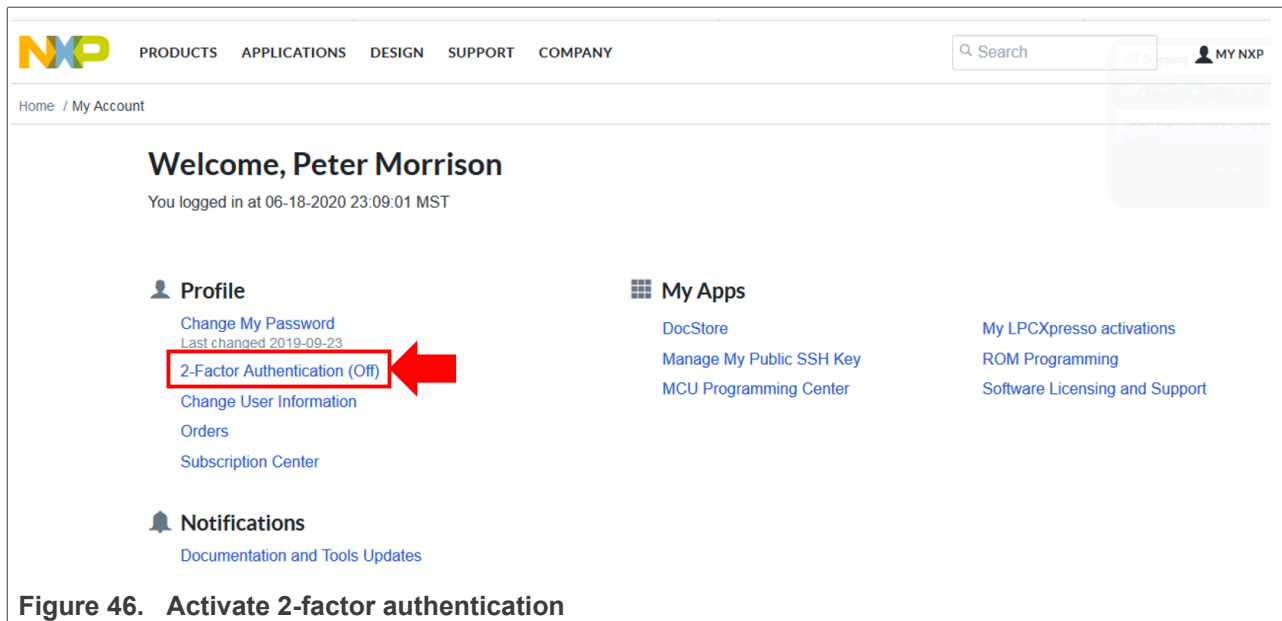641112

© 2023 NXP B.V. All rights reserved.

36 / 43

Figure 46. Activate 2-factor authentication

3. In the new page that appears, insert your mobile phone number and decide if you want to receive the 2-Factor authentication code by SMS or by phone call, then click on the *Send Code* button as shown in Figure 47:
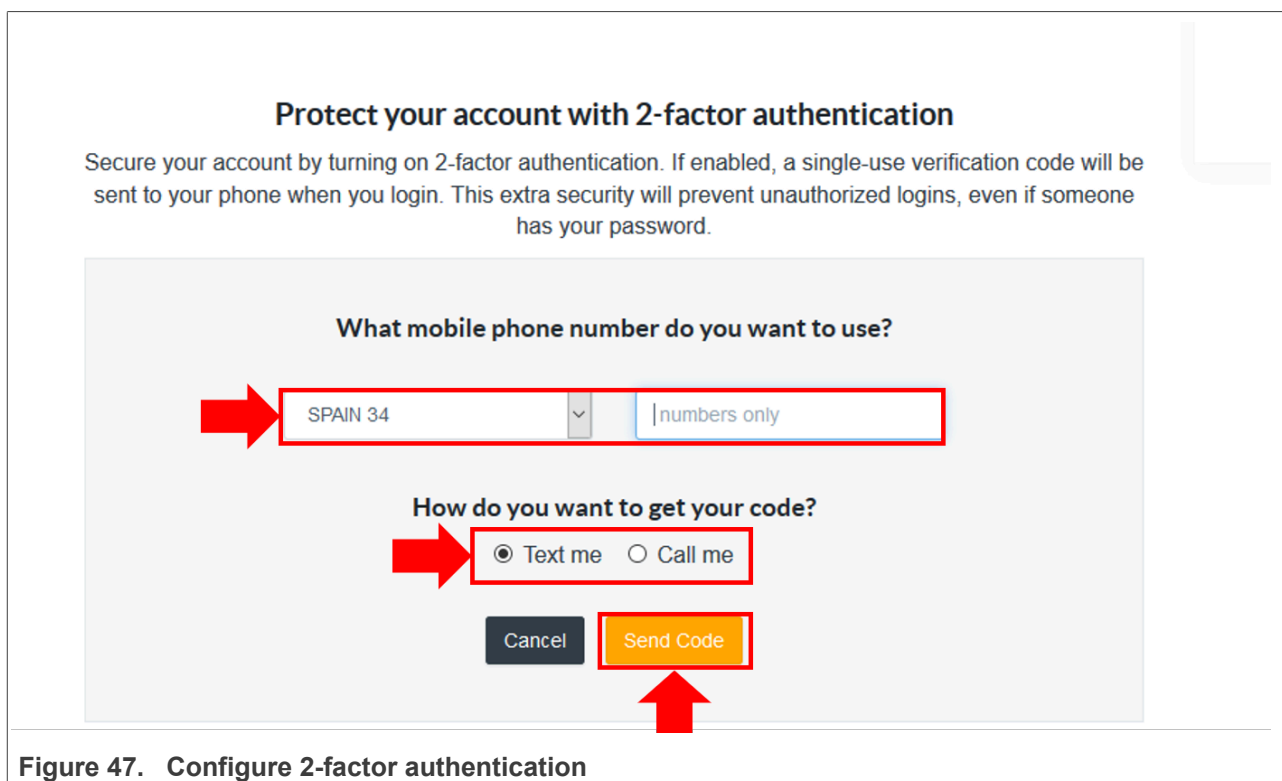

Figure 47. Configure 2-factor authentication

4. You should soon receive a confirmation code by SMS or phone call. Insert the code you just received and then click on the *Turn on 2-factor authentication* button as shown in Figure 48 to complete the activation of

2-Factor authentication for your account. From now on, every time you log in with your NXP account, you will be asked to enter a single use code that you will receive in your mobile phone.
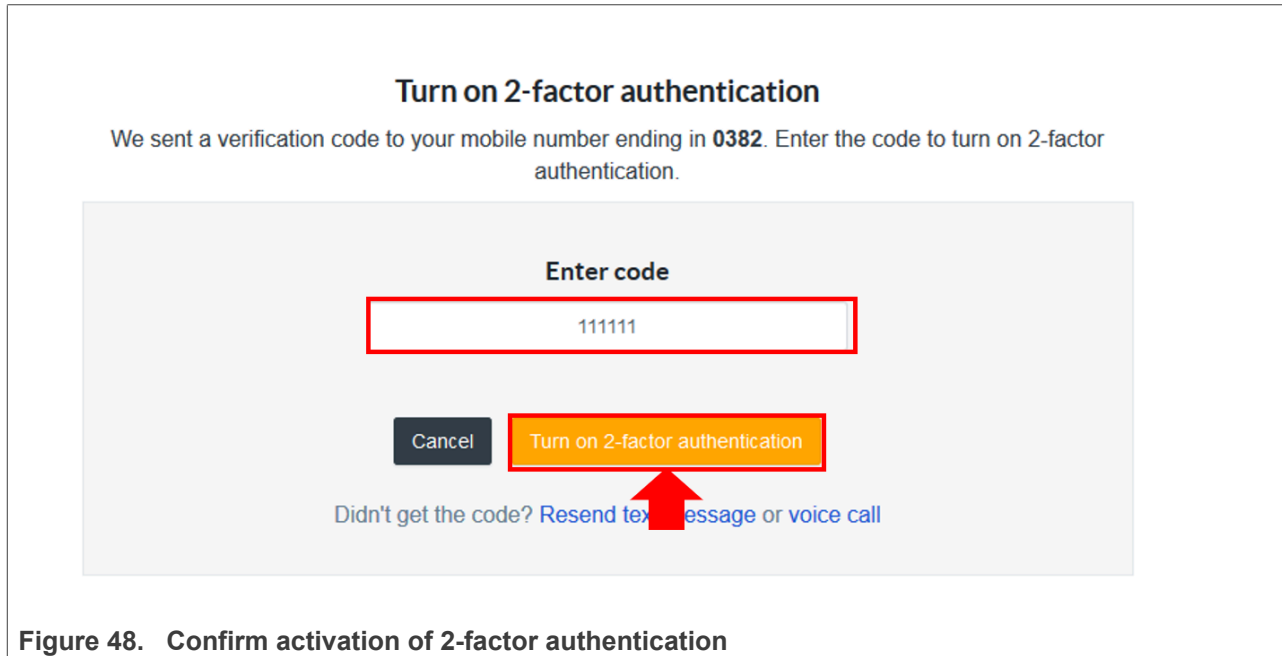

Figure 48.   Confirm activation of 2-factor authentication

7   Note about the source code in the document

Example code shown in this document has the following copyright and BSD-3-Clause license:

Copyright 2023 NXP Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials must be provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8 Revision history

Revision history

Revision number	Date	Description
1.2	2023-11-23	• Added application of key rotation scripts in Section 3 • Updated Edgelock 2GO login in Section 4.2 • Updated binaries location and MW build defines in in Section 5.5 • Update instructions to applet 7.2 in general and middleware compilation instructions in Section 5.5
1.1	2020-12-07	Updated to latest template and fixed broken links
1.0	2020-10-27	Initial version

AN12907

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Application note

Rev. 1.2 — 23 November 2023

641112

39 / 43

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

AN12907
All information provided in this document is subject to legal disclaimers.
© 2023 NXP B.V. All rights reserved.

Application note

Rev. 1.2 — 23 November 2023
641112

40 / 43

AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, µVision, Versatile — are trademarks and/or registered trademarks of Arm Limited (or its subsidiaries or affiliates) in the US and/or elsewhere. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. All rights reserved.

EdgeLock — is a trademark of NXP B.V.

Kinetis — is a trademark of NXP B.V.

AN12907

All information provided in this document is subject to legal disclaimers.

© 2023 NXP B.V. All rights reserved.

Application note

Rev. 1.2 — 23 November 2023

641112

41 / 43

Tables

Figures

Contents