AN12907 Secure update of EdgeLock SE051 IoT applet Rev. 1.2 — 23 November 2023 641112

Application note

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.



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.

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	2 / 43

Secure update of EdgeLock SE051 applets using SEMS Lite 2

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.



 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

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	3 / 43

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 <u>Section 2</u>, 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.

Secure update of EdgeLock SE051 IoT applet



- 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 <u>Section 4</u> for detailed instructions on how to do this.
- 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 <u>Section 5.4</u> 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 <u>Section 6</u> 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.

a / EdgeLook 200 managed inquiry	
Request access to the "E	dgeLock 2GO – Managed"
service	
ou can evaluate the service for free for 6 m	onths.
tarred (*) fields are required.	
irst Name *	Last Name *
John	Smith
mail Address (must be corporate email) *	Full Company Name *
user@nxp.com	NXP
country *	
AUSTRIA	~
lease describe your project and your interest	in "EdgeLock 2GO – Managed"
My project description	
give my permission to share my information	with Authorized NXP Distribution Partners *
Yes	×
Ves I would like to receive important technical	undates and information on new products training and
more from NXP	apades and mornation of now products, training, and

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.

Secure update of EdgeLock SE051 IoT applet



4.2 Log in to EdgeLock 2GO

Follow the instructions in <u>Section 4.1</u> 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:

Welcome to Edge	eLock™ 2GO
Sign in to NXP.com to access the	e EdgeLock™ 2GO portal.
Email Address or NXP ID*	
Password*	Show
Forgot your password? Reset it.	
Keep me signed in (uncheck device).	t if using public
SIGN IN	
Not registere	d yet?
CREATE AN ACC	COUNT
Need help? My NXP Account FAQ: Figure 6. Login to EdgeLock 2GO	s or contact support.

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.

Secure update of EdgeLock SE051 IoT applet

To protect your account and confirm your identity, we will send a verification code to your mobile number ending in 0382 .
How do you want to get your code?
CANCEL SEND CODE
Don't have access to this phone? Reset ² ctor authentication via email

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:

Enter your code to sign in We sent a verification code to your mobile number ending in 0382. Enter the code below to sign in.			
Enter code			
123456			
CANCEL SIGN IN Didn't get the code? Resend tex essage or voice call			
igure 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.

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	10 / 43

Secure update of EdgeLock SE051 IoT applet

NKO EdgeLock 2GO 🚍	PRIVACY AND TERMS Terms & Conditions Privacy Policy Third-Party Attribution	ns
Privacy & Terms		
ப் Logout	GENERAL Terms a Terms and Conditions of EdgeLoc	and Conditions
	SERVICE RESOURCES	Terms and Conditions for the NXP EdgeLock 2GO (the Terms and Conditions') are between you (Customer of the Semiconductors Netherlands & X, a corporation incorporated under the laws of the Netherlands, shualed of Bendrous 0, 5656 AG, Eindhven, the Netherlands ('Supplier' or YXP'). Besides the Terms and Conditions the toters and the Netherlands ('Supplier' or YXP'). Besides the Terms and Conditions of the Netherlands ('Supplier' or YXP'). Besides the Terms and Conditions the toters devices on the or ('Supplier' or YXP'). Besides the Terms and Conditions the Y, a corporation incorporated under the laws of the Netherlands, shualed of the Customer and Supplier' or YXP'). Besides the Terms and Conditions the toters of the Ocustomer clicks and if a cacept' button or check hox presented with these devices of the Services on the Ocustomer and Services 2GO. Supplier for visions and the EdgeLock 2GO of the terms of the terms of the Agreement, the vision of the Zeres of the terms of the terms of the terms of the Agreement and Service Description may be amended by tXP at any time, terms and Conditions, the Documentation and Service Description and be attemed terms.

Figure 9. Accept EdgeLock 2GO terms and conditions

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

NKO EdgeLock 2GO 🚍	MY ACCOUNT	
Devices	Settings	
Secure Objects		
🛱 Intermediate CA	EMAIL	
Services		
5 Activity	LANGUAGES	Ŧ
C Applet Update		
Documentation	SAVE CHANGES	
My Account		
Company Settings		
Alerts		
Privacy & Terms		
Logout		
ure 10. EdgeL	ock 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.

Secure update of EdgeLock SE051 IoT applet

NKO EdgeLock 2GO 😑	MY ACCOUNT	
Devices	Settings	
🛱 Secure Objects		
\overline{E}_{H}^{h} Intermediate CA	EMAIL	
Services		
4 Activity	LANGUAGES	English
So Applet Update		
Documentation		SAVE CHANGES
음 My Account		
Ocompany Settings		
⇔ Alerts		
ໍດໍ່ບໍ່ Privacy & Terms		
U Logout	+	
Figure 11. Logou	t 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 <u>AN12973 SE051 Configurations</u>)

NKO EdgeLock 2GO			
michael salfer@rep.com NXP Customer Application Support	APPLET OPDATE		
0	Browse		
🚋 inardian	1 cosult O a01wl	SEARCH CLEAR	
II) memory	Tresure 20100		
🕀 dense	12nc	Hardware Type 🔶	Packages
(i) ***	935414457472 2	SE051C2HQ1/Z01XD	7
	20 vitems per page. Showing 1-1 of	1 results	
O Applet Update			_
$\underline{\underline{\Box}}$ Q Documentation			
्रि Admin Settings			
∠→ Events & Alerts			
ို ို Privacy & Terms			
(¹) Logout			
Figure 12 Open Applet Update page in Edgel ock 260			
rigure 12. Open Applet Optiate page in EugeLock 200			

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.

APPLET UPDATE > 935414457472 - SE051C2	HQ1/Z01XD			
Packages Details				
7 results Q. Search by PACKAGE NAME OR VERSION	SEARCH			
Package Name	Version \checkmark	Created	Description	Actions
Update NXP SE051 IoT Applet	7.3	2 years ago	Multicast Package to update the NXP SE05	⊻ ₽
Update NXP-IoT-Applet A8FA	7.3	2 years ago	Multicast Package to update the NXP SE05	2 💵 3
Update NXP SE051 IoT Applet	7.2	2 years ago	Multicast Package to update the NXP SE05	⊻ 🛛
Update NXP-IoT-Applet A8FA	7.2	2 years ago	Multicast Package to update or revert th	⊻ 🖓
Upgrade_NXP-IoTApplet	6.0	2 years ago	Multicast Package to update the NXP SE05	⊻ 🛛
Delete NXP-Perso-Applet A8FA	1.0	a yéar ago	Multicast Package to delete the NXP-Pers_	⊻ 🛛
Delete_NXP-PersoApplet A564	1.0	a year ago	Multicast Package to delete the NXP-Pers_	⊻ 🖸
20 💌 items per page. Showing 1 - 7 of 7 results				1
Figure 13. Download the	update script fro	om EdgeLock 2	GO	

Run an IoT applet update script in EdgeLock SE051 5

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.

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	13 / 43

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:

NXP Semiconductors

Secure update of EdgeLock SE051 IoT applet

AN12907



3. Download the latest DAPLink firmware version as shown in Figure 15:

Secure update of EdgeLock SE051 IoT applet



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):



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.

Secure update of EdgeLock SE051 IoT applet

	er (E:)			~ 0	Search BOOTLOADER (E:)	Q
✔ Quick access 脂 MobileKnowledge ➡ This PC	Name	Date modified 12/14/2012 2:52 PM	Type HTM File	Size 1 KB		
BOOTLOADER (E:)						
🕳 USB Drive (D:)						
	k	20dx_frdmk64f_if_crc _legacy_0x5000.bin				
item						

- 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.



5.2.2 OM-SE051ARD jumper configuration

The OM-SE051ARD boards have jumpers that allow you to configure the I²C interface of EdgeLock SE051 secure elements via the Arduino header. Configure the jumper settings as shown in <u>Figure 19</u> to enable this option.

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



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:



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



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 <u>NXP website</u>. 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 <u>Section 4.3</u>), 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 <u>Figure 22</u>:

(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 loT 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 <u>Section 5.5</u>) and a pair of C files (.c and .h) that can be used with the SEMS Lite Agent demo project (see <u>Section 5.4</u>).

Note: if you don't have Python installed, you can download it from <u>https://www.python.org/downloads/</u>. **Note**: on windows it might be necessary to call "py" instead of "python"

C:\Windows\System32\cmd.exe				
			_	- 🗆 X
Microsoft Windows [Version 10.0.18363.108 (c) 2019 Microsoft Corporation. All right	2] s reserved.			
C:\se05x_middleware\simw-top\semslite\too Requirement already satisfied: pytlv in c Requirement already satisfied: jsonschema Requirement already satisfied: attrs>=17 e 2)) (20.2.0) Requirement already satisfied: setuptools () (47.1.0) Requirement already satisfied: pyrsistent (line 2)) (0.17.3) Requirement already satisfied: six>=1.11. 2)) (1.15.0)	<pre>ls\sems-lite-generator>python -m p :\python38\lib\site-packages (from in c:\python38\lib\site-packages 4.0 in c:\python38\lib\site-packages in c:\python38\lib\site-packages >=0.14.0 in c:\python38\lib\site-packages 0 in c:\python38\lib\site-packages</pre>	pip install -r requi n -r requirements.tx (from -r requiremen ges (from jsonschema->- (from jsonschema->- packages (from jsons s (from jsonschema->	irements.txt (ine 1)) (0 hts.txt (line 2) >->-r requirements cr requirements schema->-r requi >-r requirements	.71))) (3.2.0) nts.txt (lin .txt (line 2 irements.txt s.txt (line
<pre>:/se05x middleware/simw-top/semslite/too</pre>	ls\sems-lite-generator>python sems	slite json converter	.py C:\UpdateSo	cript 🤈
:\UpdateScript\iot_applet_update_script DEF ID : A4A6			· /	
	Name	Date modified	Туре	Size
	Name	Date modified	Type BIN File	Size 2 K
	Name	Date modified 29/09/2020 15:00 29/09/2020 15:00	Type BIN File C File	Size 2 K 2 K
	Name iot_applet_update_script.bin iot_applet_update_script.c iot_applet_update_script.h	Date modified 29/09/2020 15:00 29/09/2020 15:00 29/09/2020 15:00	Type BIN File C File H File	Size 2 K 2 K 13 K
	Name iot_applet_update_script.bin iot_applet_update_script.c iot_applet_update_script.h iot_applet_update_script.h	Date modified 29/09/2020 15:00 29/09/2020 15:00 29/09/2020 15:00 29/09/2020 15:00	Type BIN File C File H File JCSH File	Size 2 K 2 K 13 K 6 K
	Name iot_applet_update_script.bin iot_applet_update_script.c iot_applet_update_script.h iot_applet_update_script.jcsh iot_applet_update_script.jcsh iot_applet_update_script.jcsh	Date modified 29/09/2020 15:00 29/09/2020 15:00 29/09/2020 15:00 29/09/2020 15:00 21/09/2020 14:13	Type BIN File C File H File JCSH File JSON file	Size 2 K 2 K 13 K 6 K 5 K
	Name iot_applet_update_script.bin iot_applet_update_script.c iot_applet_update_script.jcsh iot_applet_update_script.jcsh iot_applet_update_script.jcon iot_applet_update_script.jcon	Date modified 29/09/2020 15:00 29/09/2020 15:00 29/09/2020 15:00 21/09/2020 15:00 21/09/2020 14:13 29/09/2020 15:00	Type BIN File C File H File JCSH File JSON file PROTO File	Size 2 K 2 K 13 K 6 K 5 K 9 K
	Name iot_applet_update_script.bin iot_applet_update_script.c iot_applet_update_script.h iot_applet_update_script.jcsh iot_applet_update_script.jroto	Date modified 29/09/2020 15:00 29/09/2020 15:00 29/09/2020 15:00 29/09/2020 15:00 21/09/2020 14:13 29/09/2020 15:00	Type BIN File C File H File JCSH File JSON file PROTO File	
	Name iot_applet_update_script.bin iot_applet_update_script.c iot_applet_update_script.jcsh iot_applet_update_script.json iot_applet_update_script.proto iot_applet_update_script.tmpbin	Date modified 29/09/2020 15:00 29/09/2020 15:00 29/09/2020 15:00 29/09/2020 15:00 21/09/2020 14:13 29/09/2020 15:00 29/09/2020 15:00	Type BIN File C File H File JCSH File JSON file PROTO File TMPBIN File	Size 21 21 131 61 51 91 21

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 <u>Section 4</u>. For demonstration purposes in the present document the IoT applet will be updated from version 7.2 to version 7.3 as shown in <u>Figure 23</u>.

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.



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.

Update N	lanager SEMS Lite	e Agent
	<pre>sems_lite_agent_init_context ()</pre>	
	sems_lite_agent_session_open()	
	<pre>sems_lite_agent_load_package()</pre>	
	Status Code	
	<pre>sems_lite_agent_session_close()</pre>	
Figure 24. EdgeLock SE	051 Plug & Trust middleware SEMS Lite API calls to update	e loT 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 loT 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 <u>NXP website</u>.

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:

my_workspace - MCUXpresso IDE	TOS Window Help	– 🗆 ×
'ne Edit Ivavigate Search Project Configitools Kun Pre) S window Heip 🦻 🔗 ▾ 🗊 🗐 🔲 🐨 🖳 🔍 D 💷 🕺 ス 🗇 .c. 🗮 🏋 D 🕼 🕼 କ ス 🗞 .c. ! Ø ▾	2 8 1 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5
		Quick Access
pr. 23 Per. and Re. 40 Pa		
E 😵 🖽 🧐 🔳 🔹 🖉	MCUXpresso IDE SDK import - O X	
	Are you sure you want to import the following SDK in the common 'mcuxpresso' folder?	
	Sethumely/02.11.03/setOfs_jade-fremk644_v03.00.00_s000728_j304301.np Do net ask for confirmation on SDK Drag and Drap joint 2 OK Cancel	
Qui (*)= Glo (*)= Vari 💁 Bre 📴 Outl 🗖 🗖	🍘 Installed SDKs 🙁 🔲 Properties 📮 Console 🦹 Problems 🚦 Memory 🙀 Debugger Console 🐞 Instruction 1	Trace 📼 Power Measurement T 🖾 SWO Trace Config 📮 🗖
		④ \$2 □ E E
MCUXpresso IDE - Quickstart Panel 🏻	🕅 Installed SDKs	Í
IDE No project selected	To install an SDK, simply drag and drop an SDK (zip file/folder) into the 'Installed SDKs' view. [Common 'mcuxpresso' folder	er]
Create or import a project	Name SDK Version Manifest Version Location	SDK Details
New project		Selected SDK content.
📝 🔣 Import SDK example(s)		
Import project(s) from file system	co05x kodk	
 Build your project 	frdmk64f v03.00.00 20200728 104101.zip	
🚱 🐐 Build		
my workspace		en :

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:

🕽 Installed SDKs 🙁 🔲 Properties Prob	olems 📮 Console 🔊 Terminal 🐻	👌 lmage Info 🛛 🙀 Debugger Co	onsole 📋 Memory 🛛 Heap and Stack Usage	□ [
				🛯 🕹 🔲 🗄 🖽
Name	SDK Version	Manifest Version	Location	
SDK_2.x_FRDM-K64F	2.7.0	3.5.0	Common>\frdmk64f_ksdk.zip	
		<u>&</u>	:	<u>M0xxx12 (frdmk6pdate)</u>

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

NXP Semiconductors

AN12907

Secure update of EdgeLock SE051 IoT applet

Workspace - Welcome page - MCUXpresso IDE	Common Managerer Hale					– ø ×
	■ M 2. O. LE = X D= 0 = 2. O. LE = 1	ol 🖉 📕 💺 🕸 🕸 = O = 💁 = 🐲	- ◎ ◎ ■ ◎ + ◎ + ◎ + ◎	·		Quick Access
Project Ex 😢 🚼 Peripheral 🔠 Registers 🌞 Faults 📟 🗖	() Welcome ⊠					
🖻 😵 🖽 🖘 🔳 👻 🖉	⇔ ⇔ ■ ⊕ ▼ file:///C:/nxp/MCUXpressolDE_11.0.1_2563.	ide/plugins/com.crt.lpcxpresso.brand_11.0.1.2019	08201036/pages/registered.htm			
		MCUXpress				
		v	Velcome to MCUXpresso IDE	/11.0.1		
		MCUXpresso IDE provides an Cortex%-M cores, including LP0 compiling, and debugging featu debugging, and integrated conf	easy-to-use Eclipse-based development environ C and Kinetis microcontrollers and i.MX RT cros rres with the addition of MCU-specific debugging iguration fools.	ment for NXP MCUs based on ARM® sover processors. It offers advanced editing, views, code trace and profiling, multicore		
		Documentation				
		For information on how to get a please consult the supplied MC # Help -> MCUXpresso IDE U	tarted with MCUXpresso IDE, as well as how to UXpresso IDE User Guide. This is also availab Jser Guide	use many of the more powerful features, le from the Help menu:		
		Further product documentation = Help -> Help Contents	is provided within the MCUXpresso IDE via the	Help menu:		
		The MCUXpresso IDE document	ntation is also supplied in PDF format within the	installation directory.		
		Help us improve MCUXpresso II	DE	IDE includion the built in Config Tools and		
		with which MCUs. This informat can turn this information collect # Preferences -> MCUXprest	tion can help us to improve the functionality of the ion off at any time by unticking so IDE -> General -> Help us improve the tool	e tools as well as to resolve problems. You		
U Quickstart Panel 🕃 (I)= Variables 💁 Breakpoints 📟 🗖		Disabling this Welcome Page				
MCUXpresso IDE - Quickstart Panel		To disable the display of this pa Preferences -> MCUXpress	age when running MCUXpresso IDE in future, ur so IDE -> General -> Show Welcome Page	Bek		
Materia and Alexandrea project	街 Installed SDKs 💥 📰 Properties 🖹 Problems 💿 Consol	🕫 🎜 Terminal 🔛 Image Info 🛛 🖳 Debugger Co	insole 🚺 Memory 00= Heap and Stack Us	sge	ç	
Timport project(s) nom me system	🕅 Installed SDKs					^
Build your project	To install an SDK, simply drag and drop an SDK (zip file/folder) int	o the 'Installed SDKs' view. [Common 'mcuxpress	o' folder]			
Clean	Name	SDK Version	Manifest Version	Location		
▼ Debug your project S ▼ S × S × S × S ×	SDK_2.x_FRDM-K64F	2.7.0	3.5.0	Common>\frdmk64f_ksdk.zip		
😥 🌞 Debug 🌞 Terminate, Build and Debug						,
Done					U	
Figure 27. Import p	rojects 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:

Secure update of EdgeLock SE051 IoT applet

X SDK Import Wizard					_	
 Importing project(s) for device 	e: MK64FN1M0xxx12 using board: FRDM-K64F					
Board and/or Devi	ice selection page					
- SDK MCUs	Available boards					↓ ^a z↑ ^a z│ <i>Q</i>
MCUs from installed SDKs.	Please select an available board for your project.					
Please visit mcuxpresso.nxp.co to obtain additional SDKs	M Supported boards for device: MK64FN1M0xxx12	2				
NXP MK64FN1M0xxx12	SBK frdmk64f					
Selected Device: MK64FN1M	0xxx12 using board: FRDM-K64F	SDKs for selected MCU				
Taynat Cayas		Name	SDK Versi	Manifest	Location	
Description: K64_120: Kii (MCUs) base	netis® K64-120 MHz, 256KB SRAM Microcontrollers ed on ARM® Cortex®-M4 Core	SDK_2.x_FRDM-K64F	2.7.0	3.5.0	<pre>Common>\se0</pre>	5x_ksdk-frd
(?)		< <u>B</u> ack	Next	>	2	Cancel
Figure 28. SDK in	nport 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.

NXP Semiconductors

AN12907

Secure update of EdgeLock SE051 IoT applet

Project name suffix:
e\frdmk64f Brov
Project Ontions
SDK Debug Console O Semihost UART Example default Copy sources Import other files
Description Version
The mainA71CH demo application demonstrates the usage of Secure Module function
This demo demonstrates connection to AWS IoT Console using pre-provisioned device
This demo demonstrates connection to Azure IoTHub using pre-provisioned device cre
This demo demonstrates connection to Google Cloud Platform using pre-provisioned
This demo demonstrates connection to IBM Watson IoT platform using pre-provisione
The vcomA71CH demo application allows the board to be used as a bridge between th
This project can be used to get SE05X platform information.
This example reads Accelerometer data via the I2C master interface.
This is a bare minimum example for se050. This gets the amount of free memory.
This demo demonstrates connection to AWS IoT Console using pre-provisioned device
This demo demonstrates connection to Azure lo IHub using pre-provisioned device cre
This demo demonstrates connection to Google Cloud Platform using pre-provisioned
This generates demonstrates connection to iBivi watson io i platform using pre-provisione
This example does a elliptic curve cryptography signing and verify operation.
This example does a WMAC Key derivation operation based on the info and calt
This example does a HMAC Key derivation operation based on the info and salt. This example does a Message Digest bashing operation
This example does a HMAC Key derivation operation based on the info and salt. This example does a Message Digest hashing operation. This example does a BSA signing and verify operation.
This example does a HMAC Key derivation operation based on the info and salt. This example does a Message Digest hashing operation. This example does a RSA signing and verify operation. This example does a symmetric cryptography AES encryption and decryption operation.
This example does a HMAC Key derivation operation based on the info and salt. This example does a Message Digest hashing operation. This example does a RSA signing and verify operation. This example does a symmetric cryptography AES encryption and decryption operation. This project can be used to upgrade the Applet

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

Secure update of EdgeLock SE051 IoT applet

workspace - frdmk64f_se05x_sems_lite_ex_update/source/sen	ns_lite_ex_update.c - MCUXpresso IDE		- 0
Edit Source Refactor Navigate Search Project Co	onfigTools Run Analysis FreeRTOS Window Help		
💌 🔚 🕼 🛛 🕶 🔦 🕶 🔜 🖓 😓 🖢 🔌 🗆 💷		🌯 🕶 🍅 🤺	१ • ♪ № ■ ॥ ध • ी • ७ ० • ० •
			Quick Access
Projec 🕺 🛃 Perip 👭 Regist 株 Faults 😑 🗖	is sems_lite_ex_update.c ⋈	- 0	E Outline 🔀 🕫 Global Variables
Image: Control of the control of t	<pre>10 /* 2 * Copyright 2018-2020 100P 3 * All rights reserved. 4 5 * SPOX-License-Identifier: 850-3-Clause 6 */ 7 9 /* Includes 10 /* 11 finclude <ex_sss.ho 12="" 13="" <ex_sss.ho="" <fall="" finclude="" sss.e00x.h=""> 14 finclude <fall sss.e00x.h=""> 15 finclude <fall sss.e00x.h=""> 15 finclude <fall sss.e00x.h=""> 16 finclude <fall sss.e00x.h=""> 17 finclude <fall sss.e00x.h=""> 18 finclude <fall sss.e00x.h=""> 19 finclude <fall sss.e00x.h=""> 19 finclude <fall sss.e00x.h=""> 10 finclude <fall sss.e00x.h=""> 11 finclude <fall sss.e00x.h=""> 12 finclude <fall sss.e00x.h=""> 13 finclude <fall sss.e00x.h=""> 14 finclude <fall sss.e00x.h=""> 15 finclude <fall sss.e00x.h=""> 15 finclude <fall sss.e00x.h=""> 17 finclude <fall ssss.e00x.h=""> 17</fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></fall></ex_sss.ho></pre>	*	<pre>I'z & x' • ** ec_sss.h ec_sss.boot.h fsl_sss_se0Xc.apis.h mctog.App.h ssem_lite.api.h e' gev_sss_boot_ctv:re_sss_boot_ctv_t # EX_SSS_BOOT_PCONTEXT # EX_SSS_BOOT_DCONTEXT # EX_SSS_BOOT_CONTEXT # EX_SSS_BOOT_SKIP_SELECT_APPLET ec_sss_main_inc.h multicast_package:multicast_package_t ec_sss_entry(ec_sss_boot_ctv_t'):sss_statur_t</pre>
Quickstart P 💥 (X)= Variables 👻 Breakpoints 👘 🗋	🍘 Install 🔲 Prope 🦹 Probl 📮 Console 🛛 🖉 Termi 🗟 Imag 🗟 Debug 🖓 🗖	Memory 🛛	(x)= Heap and Stack Usage
MCUXpresso IDE - Quickstart Panel Project: frdmk64f_se05x_sems_lite_ex_update (Debi	CDT Build Console (frdmk64i,se05x,sems_lite_ex,update) Me	onitors 👍 🕽	101 (10 📑 🖬 🔯 🖏 🕶
Create or import a project			
New project Import SDK example(s) Import project(s) from file system			
Build your project			
Suild	y.		
Debug your project	< >		
framkfulf sellfsy sems lite av undate/source/sems lite av un	date.c		(I) NVD MK64EN11M0mm12 (Enderlife, and ata)

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 <u>Section 5.3</u>, then add to the example project the script to update the IoT applet as shown in <u>Figure 31</u>:

(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.

Secure update of EdgeLock SE051 IoT applet



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.



- 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.

^{et} Tera Term: New co	nnection			×			
Оторир	I.I.e. etc	muhaatavamal	0.00m	^	Port:	COM7 ~	ОК
OTCEAP	nust.	mynosuexampi	C.COM	×	Baud rate:	9600 ~	
	Service:	 ✓ History ○ Telnet 	TCP port#: 22		Data:	110 300	Cance
		⊚ SSH S	SH version: SSH2	~	Parity:	600 1200	
		○ Other	Protocol: UNSPEC	~	Stop:	2400 4800	Help
					Flow control:	14400	
Serial	Port:	COM3: Intel(R) A	Active Management 1 Active Management 1	boology - SOL (COM3)	-Transmit delay	19200 38400	
	ОК	COM7: USB Ser	ial Device (COM7)		0 msech	57600 115200	msec/line
		COMJ. WIRdar C				230400	
				~	L	460800	
						921600	

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



4. Go to the MCUXpresso Quickstart Panel and click the *Debug* button as shown in <u>Figure 35</u>. 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.

	Probes disco	vered		— 🗆 X	Quick A	cess 🛛 🖻 🔀
Project 🛿 🛃 Periphe 🔠 Registers 🎋 Faults 🖳 🗖	Welcor Connect to ta	net: MK64EN1M0yyy12				-
E 😫 🖶 🍫 🕅 🕶 🗵		get. Mikouria inioxxx 12			.0.201905281035/pages/registered.htm	× ►
frdmk64f se SE05x ex mals update <debug></debug>	1 probe found.	Select the probe to use:			interiore in the second s	
Project Settings					1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
Binaries	Available a	ttached probes			Name Name Name Name Name Affinish Amerikan Statistics Paral Name Name Name	
Includes			Louis Ison		MARY AND	
😕 CMSIS	Name	Serial number/ID	Type Man	u IDE Debug Mode	Barranov Barranov	
😂 board	LS CMSIS-DAI	0240000040214	LinkS ARM	Non-Stop	DECEMBENT OF THE CONTRACT OF THE OWNER OF THE OWNER OF THE OWNER OF THE OWNER	
😂 component						
29 device					1 - V/V/V/	
😕 drivers					The Carton of th	
					and in a frame frame from from the same is	
mbeatis						
A se hostlik						
					E v11 0 0	
b fsl sss ftr.h	Supported Pro	es (tick/untick to enable/disable)				
> c mals ex update.c	MCIIXpres	IDE LinkSenver (inc. (MSIS-DAP) n	rober		vironment for NXP MCUs based on ARM®	
> h MALS_UpgrateTo_iotDev-4.4.0-20200128-00.h	Res Micro	prober	10003		ging views, code trace and profiling, multicore	
> c semihost_hardfault.c		probes				
😂 startup	M SEGGER J-L	ink probes				
😕 utilities					w to use many of the more powerful features,	
🗁 Debug	Probe search o	ptions			ailable from the Help menu:	
ui 💥 (x)= Vari 📴 Outl 💁 Bre (x)= Glo 🖓 🗖	1 Installe Search again				ory 🗵 Heap and Stack Usage 🛛 🙀 Debugger Console	_
	Remember	v selection (for this Launch configura	tion)		🖹 🖬 🗟 🖉 🖉	- 🖻 🖻 - 1
wild your project	RedlinkSen	y second (for this counter county it	, and any			
und your project	WireInit ?	2	OK	Cancel		
🚬 🔏 Build	CoresCon	-				
🛃 🧹 Clean	PacketSize = 64					
	Reference Count = 0					
bebug your project	HasSWV = FALSE					
The Debug	HasJTAG = TRUE					
Terminate, Build and Debug	HasSWD = TRUE					
	Probe Type = CMSIS-DAP					
Aiscellaneous	Probe Reference Count	= 0				
Edit project settings						
MCUXnresso Config Tools>>	<					
					toth commences and	

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 <u>36</u>.

Secure update of EdgeLock SE051 IoT applet

workspace - frdmk64f se SE05x ex mals undate/se	e hostlih/sss/ev/inc/ex sss main inc h - MCUXnresso IDF	— П `
nonspace name not be been and be been been been been been been been	Constant, 2014 Sector Barriero, Barr	
e Edit Source Refactor Navigate Search P		
	■ 1 4 mm m = 14 m m m m m m m m m m m m m m m m m m	
		Quick Access 🕴 😭 📈 🕏
Pr. 8 - Pe. 111 Re. 4 Fa	15 Deb 23	🍇 🙀 🗸 🖵 (
	a debédé se SEOSy av male undete sef (MK64EN1M0vv12 (sector m0))	n -
🕒 🥸 🖽 🐨 🖉 🖌 👻	Thread #11(Subscience: Intersection (Internet intersection) Thread #11(Subscience: Intersection)	
se_nostlib	main() at exists main inc.h:1240x7228	
> 🗁 mal	arm-none-eabi-gdb (8.2.50.20181213)	
> > nxp_iot_agent	O Welson D. B. States of March 2010 B. States and State M.	
Y 🗁 555	weicome is startup_mkowfi2.c in ex_sss_main_inc.n 23	
∽ (<u>⇒</u> ex	124 sss_status_t status = kStatus_SSS_Fail; 125 const char *portName;	^
✓ 🧁 inc		
> h ex_a71ch_scp03.h	127 #if EX_SSS_BOOT_EXPOSE_ARGC_ARGV	
> h ex_sss_auth.h	128 gex_sss_argc = argc; 129 gex_ss_argc = argc;	
> h ex_sss_boot.n	130 #endif // EX_SSS_BOUT_EXPOSE_ARGC_ARGV	
ex sss main inc frdmk64f.h	131	
> h ex sss main inc imx rt.h	132 #1fdet HAVE_KSDK	
> h ex_sss_main_inc_ksdk.h	134 #endif // HAVE_KSDK	
> h ex_sss_main_inc_linux.h		
> h ex_sss_main_inc_lpcxpresso55:	136 #11 defined(inux) && defined(1012C) && SSS_MAVE_SE05X	
> 🔓 ex_sss_main_inc.h	138 #endif // defined(linux) && defined(T10I2C) && SSS_HAVE_SE05X	
> h ex_sss_objid.h		
> h ex_sss_ports.h	140 LOG_1(PLOGANDIRUSI_PROU_NAME_VER_FULL); 141	
> in ex_sss_scpus_keys.n	142 #ifdef EX_SSS_BOOT_PCONTEXT	
> h ex_sss.h	<pre>143 memset((EX_SSS_BOOT_PCONTEXT), 0, sizeof(*(EX_SSS_BOOT_PCONTEXT))); 144 media (/ ex_SSS_BOOT_PCONTEXT);</pre>	
	145	
	146 #if AX_EMBEDDED	
Quicks 💥 (x)= Variabl 💁 Break 🗖 🗖	147 portName = NULL;	>
Import project(s) from file system	🍘 Installed SDKs 🔲 Properties 👔 Problems 📮 Console 🕱 🖉 Terminal 🕋 Image Info 🐼 Debugger Console 🗻 Memory 🕬 Hea	p and Stack Usage
Build your project		🔳 X 🔆 🖹 🛼 🚮 🖗 🖓 🛃 🖬 🕇
💽 🐔 Build	frdmkb4f_se_SE00x_ex_mals_update LinkServer Debug [C/C++ (NXP Semiconductors) MCU Application] frdmkb4f_se_SE00x_ex_mals_update.axf	+ 53062 @ 127 @ @ 1]
🗘 🧹 Clean	[neoxh.esso semtioscrub_leruer_consore_lorLommon_se_scox_ex_mars_objare_ruksei.iet_peopE_scarced_on_por	c 55662 @ 127.0.0.1]
Debug your project 💽 👻 🔛		
参 Debug 株 Terminate, Build and Debug		
Miscellaneous		
/frdmk64f.co.SE05v.ev.male.undate/co.hantib/an	lew line lew erer main inc.h	
/munikowi_se_scusx_ex_mais_update/se_nostlib/sss/	Vevine evasion (Charles Control Contro	 NXP MK64EN1M0xxx12 (trdmk6pdate)

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).

Secure update of EdgeLock SE051 IoT applet



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 <u>NXP website</u>, 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 <u>here</u>. When compiling the tool, make sure that the following CMake compilation flags are set as shown in <u>Figure 38</u> (-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.

AN12907	
Application note	

Secure update of EdgeLock SE051 IoT applet

🛕 CMake 3.23.2 -	/simw-top_build/se_x86 —	
<u>File Tools Options</u>	<u>H</u> elp	
Where is the source code:	simw-top	Browse Source
Preset:	<custom></custom>	
Where to build the binaries:	simw-top_build/se_x86	Browse <u>B</u> uild
Search:	Grouped Advanced 🕂 Add Entry 🗱 Remove Entry	Environment
Name	Value	^
CMAKE_BUILD_TYPE CMAKE_CONFIGURATIOI CMAKE_INSTALL_PREFIX NXPInternal PTMW_A71CH_AUTH PTMW_Applet PTMW_FIPS PTMW_Host PTMW_Host PTMW_HostCrypto PTMW_Log PTMW_SEL PTMW_SBL PTMW_SBL PTMW_SEDSX_Auth PTMW_SE05X_Ver PTMW_SE05X_Ver PTMW_SMCOM PTMW_mbedTLS_ALT SSSFTR_SE05X_AES <	Release Debug;Release;MinSizeRel;RelWithDebInfo C:/Program Files (x86)/PlugAndTrustMW None SE05X_C None PCWindows MBEDTLS Default Default None SCP03_SSS None 07 02 VCOM None VCOM	×
Press C	onfigure to update and display new values in red, then press Generate to generate selected build files.	
Configure Generati	e Open Project Current Generator: Visual Studio 16 2019	
Figure 38. Set CMa	ake 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:



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:

	simw-top > binaries > MCU > se05x	ې 5 م	Search se05x		
	Name	Date modified	Туре	Size	
	se05x_ccid-T1ol2C_GP1_0-frdmk64f.bin	23.06.2022 17:58	BIN File	47 KB	
	se05x_ccid-T1ol2C-frdmk64f.bin	23.06.2022 17:58	BIN File	47 KB	
	se05x_vcom-T1ol2C_GP1_0-evkmimxrt10	23.06.2022 17:58	BIN File	47 KB	
	se05x_vcom-T1ol2C_GP1_0-frdmk64f.bin	23.06.2022 17:58	BIN File	31 KB	
	se05x_vcom-T1ol2C-evkmimxrt1060.bin	23.06.2022 17:58	BIN File	47 KB	
	se05x_vcom-T1ol2C-evkmimxrt1170.bin	23.06.2022 17:58	BIN File	50 KB	
	se05x_vcom-T1ol2C-frdmk64f.bin	23.06.2022 17:58	BIN File	31 KB	
	se05x_vcom-T1ol2C-lpcxpresso55s69.bin	23.06.2022 17:58	BIN File	33 KB	
	se050_GetInfo-T1oI2C-evkmimxrt1060.bin	23.06.2022 17:58	BIN File	55 KB	
	se050_GetInfo-T1ol2C-frdmk64f.bin	23.06.2022 17:58	BIN File	40 KB	
	se051_GetInfo-T1oI2C_GP1_0-evkmimxrt	23.06.2022 17:58	BIN File	55 KB	
	se051_GetInfo-T1ol2C_GP1_0-frdmk64f.bin	23.06.2022 17:58	BIN File	40 KB	
	se051_GetInfo-T1ol2C-evkmimxrt1060.bin	23.06.2022 17:58	BIN File	55 KB	
	se051_GetInfo-T1ol2C-frdmk64f.bin	23.06.2022 17:58	BIN File	40 KB	
🗻 🖂 🗐 📕 🖛 🔤 Manage	FRDM-K64FD (D:)				- C
File Home Share View Drive Tools					
\leftarrow \rightarrow \checkmark \uparrow \checkmark \rightarrow FRDM-K64FD (D:)	ٽ ~	,○ Search FRDM-I	K64FD (D:)		
> Desktop ^ Name	^	Date modified	Туре	Size	
> 🖹 Documents 📄 porta	LO DIT	22/02/2016 15 20	T . D		1.170
Delai	LS.IXI	22/03/2016 15:30	lext Docu	ument	I KB
> - Downloads	INFO.HTM	22/03/2016 15:30	Firefox H	TML Docu	1 KB
> 🎝 Music	٠				
> 📰 Pictures					
> 🔢 Videos					
> 🟥 OS (C:)					
> 🥪 FRDM-K64FD (D:)					
> 🧅 FRDM-K64FD (D:)					
Figure 40. Install VCOM driver i	n FRDM-K64F				

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



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



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:

 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:

AN12907		
Application	note	

(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

C:\Windows\System32\cmd.exe		_	×
C:\se05x_mw_v03.00.03_20200923_223455\simw-top\binaries\ex>SET EX_SSS_BOOT_SSS_PORT=COM9 [
C:\se05x mw v03.00.03 20200923 223455\simw-top\binaries\ex>VCOM-se051 sems lite cli app.exe			
App:INFO :VCOM-sems_lite_cli_app.exe [loadpkg] path-to-SEMS-Lite-applet-package-binary-fileApp:INFO :VCOM-sems_lite_cli_app.exe [getuid]			
App :INFO :VCOM-sems_lite_cli_app.exe [getappcontents] optional-app-aid App :INFO :VCOM-sems_lite_cli_app.exe [getpkgcontents] optional-pkg-aid App :INFO :VCOM-sems_lite_cli_app.exe [getpkgcontents] optional-pkg-aid			
App :INFO :VCOM-sems_lite_cli_app.exe [semslitegetversion] App :INFO :VCOM-sems_lite_cli_app.exe [semslitegetversion]			
App :INFO :VCOM-sems_lite_cli_app.exe [checkTear] App :INFO :VCOM-sems_lite_cli_app.exe [checkUpgradeProgress]	2		
App :INFO :VCOM-sems_lite_cli_app.exe [getENCIdentifier] App :INFO :VCOM-sems_lite_cli_app.exe [testapplet] applet-aid, apdu-command App :INFO :VCOM-sems_lite_cli_app.exe [getCAIdentifier]			
App :INFO :VCOM-sems_lite_cli_app.exe [getcAKeyIdentifier] App :INFO :VCOM-sems_lite_cli_app.exe [getpkgversion]			
App :INFO :VCOM-sems_lite_cli_app.exe [getFreePHeap] App :INFO :VCOM-sems_lite_cli_app.exe [getECParameter]			
App ::INFO :VCOM-sems_lite_cli_app.exe [getFIPSInfo]			

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 <u>Section 5.3</u>, then use the SEMS Lite CLI tool to run the script as shown in <u>Figure 44</u>. 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.



6 Appendix: Register an NXP account

Follow these steps to register an NXP account:

1. If you want to register a new account, visit <u>https://www.nxp.com/webapp-signup/register</u>, fill in the fields with your data and then click on the *Register* button as shown in <u>Figure 45</u>. 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.

Secure update of EdgeLock SE051 IoT applet

PRODUCTS APPLICATIONS DESIGN SUPPORT COMPANY	Q Search		LANGUAGE ~ 🛱
Register to access secure documents and additional site features.	Create an Account Already have an account? Sign in		
 Product Samples 	Peter		
 Software and tools 	Last Name *		
 On-demand training 	Morrison		
and live courses	Email * (Use work email for faster response)		
 Technical help 	peter.morrison@mail.com		
	Retype Email *		
	peter.morrison@mail.com		
	Password * (Minimum 8 characters, include 3 of the following character types: uppercase, lowercase, numeric, special character	ter)	
	•••••		
	Retype Password *		
	•••••		
	Full Company Name *		
	MyCompany		
	Yes	~	—
	 Yes, I would like to receive important technical updates and information on new products, training, and more from NXP I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy I have read and accept the Terms of Use and Privacy Policy 		
Figure 45. NXP account registration			

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

NP	PRODUCTS APPLICATIONS DESIGN SUPPORT COMPANY		Q Search	Ge So oping & MY NXP
Home / My Accor	int			
	Welcome, Peter Morrison			
	You logged in at 06-18-2020 23:09:01 MST			
	L Profile	III My Apps		
	Change My Password	DocStore	My LPCXpresso	activations
	2-Factor Authentication (Off)	Manage My Public SSH Key	ROM Programmi	ing
	Change User Information	MCU Programming Center	Software Licensi	ng and Support
	Orders			
	Subscription Center			
	Notifications			
	Documentation and Tools Updates			
Figure 4	6. 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:

Protect your account with 2-factor authentication Secure your account by turning on 2-factor authentication. If enabled, a single-use verification code will be sent to your phone when you login. This extra security will prevent unauthorized logins, even if someone has your password.
What mobile phone number do you want to use?
How do you want to get your code? Text me Call me Cancel Send Code
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

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	37 / 43

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.



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 <u>Section 3</u> Updated Edgelock 2GO login in <u>Section 4.2</u> Updated binaries location and MW build defines in in <u>Section 5.5</u> Update instructions to applet 7.2 in general and middleware compilation instructions in <u>Section 5.5</u>
1.1	2020-12-07	Updated to latest template and fixed broken links
1.0	2020-10-27	Initial version

Secure update of EdgeLock SE051 IoT applet

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 <u>PSIRT@nxp.com</u>) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

 $\ensuremath{\mathsf{NXP}}\xspace \mathsf{B.V.}\xspace \longrightarrow$ 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.

Secure update of EdgeLock SE051 IoT applet

EdgeLock — is a trademark of NXP B.V. Kinetis — is a trademark of NXP B.V.

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.

Secure update of EdgeLock SE051 IoT applet

Tables

 Tab. 1.
 OM-SE051ARD development kit details14

Tab. 2. FRDM-K64F details 14

Figures

Fig. 1.	High level overview of IoT applet update
	process using SEMS Lite and EdgeLock
- . 0	2GO2
Fig. 2.	Applet update using SEMS Lite
Fig. 3.	IOT applet update flow using SEMS Lite
	and EdgeLock 2GO
FIG. 4.	Request an EdgeLock 2GO account
FIG. 5.	Login to Edgel ock 200
FIG. 7	Login to EdgeLock 2GO
гig. 7.	Login to EugeLock 200 - 2-lactor
Eig 8	Login to Edgel ock 2CO 2 factor
Fly. 0.	authentication (2)
Fig 9	Accept Edgel ock 2GO terms and
i ig. 0.	conditions 11
Fig 10	EdgeLock 2GO homenage
Fig. 10.	Logout from Edgel ock 2GO
Fig. 12	Open Applet Update page in Edgel ock
	2GO
Fig. 13.	Download the update script from EdgeLock
U U	2GO
Fig. 14.	DAPLink firmware update - select board15
Fig. 15.	DAPLink firmware update - select board 16
Fig. 16.	Enter bootloader mode16
Fig. 17.	Enter bootloader mode17
Fig. 18.	Enter bootloader mode17
Fig. 19.	Jumper configuration for FRDM-K64F18
Fig. 20.	Arduino connectors of OM-SE051ARD and
	FRDM-K64F boards18
Fig. 21.	OM-SE051ARD mounted in FRDM-K64F
	board
Fig. 22.	Convert update script using semslite_json_
	converter20

Fig. 23.	NXP IoT Applet update to version 7.3 with	
	SEMS Lite project example	20
Fig. 24.	EdgeLock SE051 Plug & Trust middleware	
	SEMS Lite API calls to update IoT applet	21
Fig. 25.	Import FRDM-K64F board SDK into	
	MCUXpresso environment	22
Fig. 26.	Imported FRDM-K64F SDK	22
Fig. 27.	Import projects from SDK	23
Fig. 28.	SDK import wizard	24
Fig. 29.	Select projects to import	25
Fig. 30.	Imported projects in MCUXpresso	
U	workspace	26
Fig. 31.	Add the IoT applet update script to the	
0	example	27
Fig. 32.	Connect boards to the laptop	27
Fig. 33.	TeraTerm setup	28
Fig. 34.	Build projects in MCUXpresso workspace	28
Fig. 35.	Debug projects in MCUXpresso workspace.	29
Fig. 36.	Run projects in MCUXpresso workspace	30
Fig. 37.	TeraTerm logs - frdmk64f se05x sems	
•	lite ex update project example	31
Fig. 38.	Set CMake flags	32
Fig. 39.	Enter bootloader mode	33
Fig. 40.	Install VCOM driver in FRDM-K64F	33
Fig. 41.	Connect FRDM-K64F usign VCOM	34
Fig. 42.	Retrieve VCOM port number	34
Fig. 43.	Use the SEMS Lite CLI tool	35
Fig. 44.	Execute SEMS Lite script using SEMS Lite	
0	CLI	35
Fig. 45.	NXP account registration	36
Fig. 46.	Activate 2-factor authentication	37
Fig. 47.	Configure 2-factor authentication	37
Fig. 48.	Confirm activation of 2-factor authentication .	38

Secure update of EdgeLock SE051 IoT applet

Contents

1	Introduction	2
2	Secure update of EdgeLock SE051	
	applets using SEMS Lite	3
3	Leveraging EdgeLock 2GO and SEMS	
	Lite to update EdgeLock SE051 IoT	
	applet	4
4	Use EdgeLock 2GO to download IoT	
	applet update scripts	6
4.1	Obtain an EdgeLock 2GO account	6
4.2	Log in to EdgeLock 2GO	8
4.3	Download IoT applet update scripts	12
5	Run an IoT applet update script in	
	EdgeLock SE051	13
5.1	Hardware required	14
5.2	Boards setup	14
5.2.1	Update FRDM-K64F board with DAPLink	
	firmware	14
5.2.2	OM-SE051ARD jumper configuration	18
5.2.3	OM-SE051ARD and FRDM-K64F board	
	connection	18
5.3	Convert the IoT applet update script	19
5.4	Run an IoT applet update script using the	
	SEMS Lite Agent Demo	20
5.4.1	Software requirements	21
5.4.2	Install FRDM-K64F SDK	22
5.4.3	Import SEMS Lite update project in	
	MCUXpresso	22
5.4.4	Build, run and debug SEMS Lite project	
	example	27
5.5	Run an IoT applet update script using the	
	SEMS Lite CLI	31
5.5.1	Software requirements	31
5.5.2	Build the SEMS Lite CLI tool	31
5.5.3	Install VCOM drivers	32
5.5.4	Use the SEMS Lite CLI and execute the IoT	
	applet update script	34
6	Appendix: Register an NXP account	35
7	Note about the source code in the	
	document	38
8	Revision history	39
	Legal information	40
	-	

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© 2023 NXP B.V.

All rights reserved.

For more information, please visit: https://www.nxp.com

Date of release: 23 November 2023 Document identifier: AN12907 Document number: 641112