

AN13013

Get started with EdgeLock SE05x support package

Rev. 1.3 — 14 September 2022

Application note

Document information

Information	Content
Keywords	EdgeLock SE05x, Plug & Trust secure element
Abstract	This document is the entry point for getting familiar with EdgeLock SE05x support package contents and how to get started with them.



Revision history

Revision history

Revision number	Date	Description
1.0	2020-10-19	First document release
1.1	2020-12-07	Updated to latest template and fixed broken links
1.2	2022-03-28	Add EdgeLock SE050E product variant Update Figure 1 , Table 1 , Table 3 , Figure 2 , Figure 3 , Figure 5 , Figure 6 Add Section 4.1.2.1 Product specific CMake build settings Add Section 4.1.3 Example: SE050E CMake build settings Add Section 4.2 Binding EdgeLock SE05x to a host using Platform SCP Update chapter Section 4.4 EdgeLock SE05x ssscli tool
1.3	2022-09-14	Update to EdgeLock SE Plug & Trust Middleware version 04.02.xx. Update Figure 2 , Figure 3 , Figure 5 , Figure 6 Update Section 3 Supported MCU/MPU boards Update Section 4 EdgeLock SE05x Plug & Trust middleware Update Section 4.1.2.1 Product specific CMake build settings Update Section 4.2 Binding EdgeLock SE05x to a host using Platform SCP Update Section 4.4.1 EdgeLock SE05x ssscli tool

1 About EdgeLock SE05x Plug & Trust secure element family

The EdgeLock SE05x product family of Plug & Trust devices offers enhanced Common Criteria EAL 6+ based security, for unprecedented protection against the latest attack scenarios. This ready-to-use family of secure elements for IoT devices provides a root of trust at the IC level and supports the increasing demand for easy-to-design and scalable IoT security.

Delivered as a ready-to-use solution, the EdgeLock SE05x includes a complete product support package that simplifies design-in and reduces time to market. The EdgeLock SE05x support package offers:

- Software enablement for different MCUs and MPUs.
- Integration with the most common OSs including Linux, Windows, RTOS and Android.
- Sample code for major IoT security use cases.
- Extensive application notes.
- Development kits compatible with i.MX, I.MX RT and Kinetis® MCU boards.

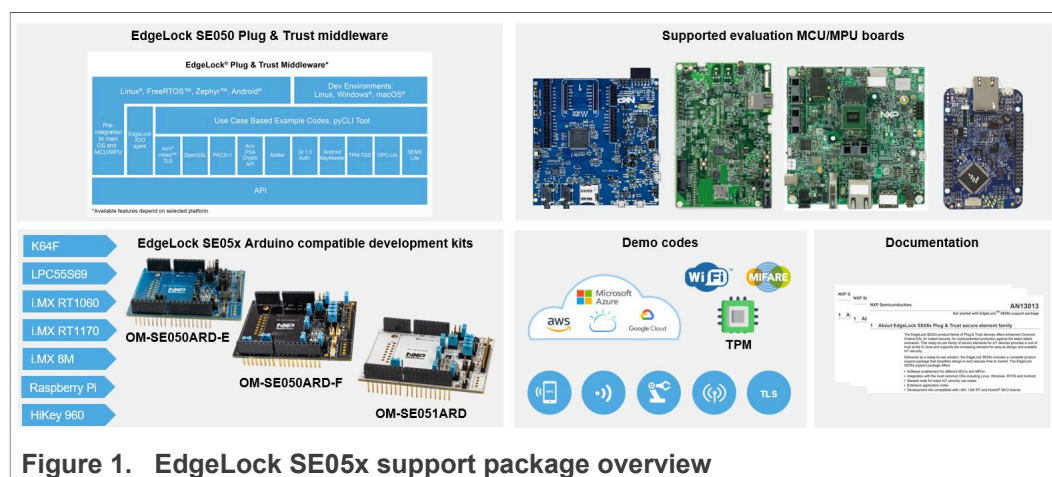


Figure 1. EdgeLock SE05x support package overview

As such, the EdgeLock SE05x support package supplies you with all you need to evaluate, prototype and implement your next secure IoT application. This document lists the existing material within EdgeLock SE05x support package, organized in the following sections:

- [EdgeLock SE05x development kits.](#)
- [Supported MCU / MPU boards.](#)
- [EdgeLock SE05x Plug & Trust middleware.](#)
- [Support documentation.](#)

To implement inclusive language, the terms "master/slave" has been replaced by "controller/target", following the recommendation MIPI.

2 EdgeLock SE05x development boards

The EdgeLock SE05x product family is supported with development boards that can be connected with any MCU or MPU board using the compatible Arduino headers or via direct I²C connection. The table below summarizes the ordering details of the EdgeLock SE05x development boards:


Table 1. EdgeLock SE05x development boards.

Part number	12NC	Description	Picture
OM-SE050ARD-E	9354 332 66598	SE050E Arduino® compatible development kit	
OM-SE050ARD-F	9354 357 63598	SE050F Arduino® compatible development kit	
OM-SE050ARD	9353 832 82598	SE050 Arduino® compatible development kit	
OM-SE051ARD	9353 991 87598	SE051 Arduino® compatible development kit	

You have two options to connect the Raspberry Pi to the OM-SE05xARD board:

1. Using the OM-SE05xRPI adapter board. This board does not include any active component.
2. Using the OM-SE05xARD connected with wires, as described in [AN12570](#).

Table 2. OM-SE050RPI adapter board details

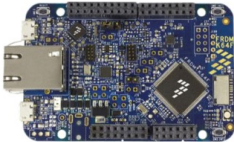


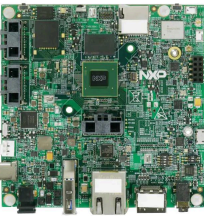
Part number	12NC	Content	Picture
OM-SE050RPI	935398642598	Raspberry Pi to OM-SE050ARD adapter	

3 Supported MCU/MPU boards

The EdgeLock SE05x security IC is designed to be used as a part of an IoT system. It works as an auxiliary security device attached to a host controller. The host controller communicates with EdgeLock SE05x through an I²C interface with the host controller being the I²C controller and the EdgeLock SE05x being the I²C target.

[Table 3](#) summarizes the ordering details of the MCU / MPU boards supported by the EdgeLock SE05x Plug & Trust middleware:

Table 3. Evaluation MCU/MPU boards details

Part number	12NC	Description	Picture
FRDM-K64F	935326293598	Freedom development platform for Kinetis K64, K63 and K24 MCUs	
MIMXRT1060-EVK	935419011598	MIMXRT1060-EVK low cost evaluation kit for Cortex-M7	
MIMXRT1170-EVK	935378982598	MIMXRT1170-EVK low cost evaluation kit for Cortex-M7	
MCIMX8M-EVK	935378743598	Evaluation Kit for the i.MX 8M Applications Processor	
LPC55S69-EVK	935377412598	LPCXpresso55S69 Development Board	

Note: Besides the mandatory connection to the host controller, some EdgeLock SE05x product variants can optionally be connected to a sensor node or similar element through a separate I²C interface. In this case, the EdgeLock SE05x device is the I²C controller and the sensor node is the I²C target. Lastly, some EdgeLock SE05x product variants has a connection for a native contactless antenna, providing a wireless interface to an external device like a smartphone.

3.1 MIMXRT1070-EVK, MIMXRT1060-EVK, FRDM-K64F and LPC55S69-EVK MCU board examples

For the [MIMXRT1070-EVK](#), the [MIMXRT1060-EVK](#), the [FRDM-K64F](#) and [LPC55S69-EVK](#), a set of project examples can be directly imported from the board SDK package to your MCUXpresso workspace.

These project examples offer a quick way to evaluate EdgeLock SE05x features, and its source code can be re-used for your own implementations. The latest SDK packages can be found in [EdgeLock SE05x product website](#), under the *Tools & Software* tab, as shown in [Figure 2](#).

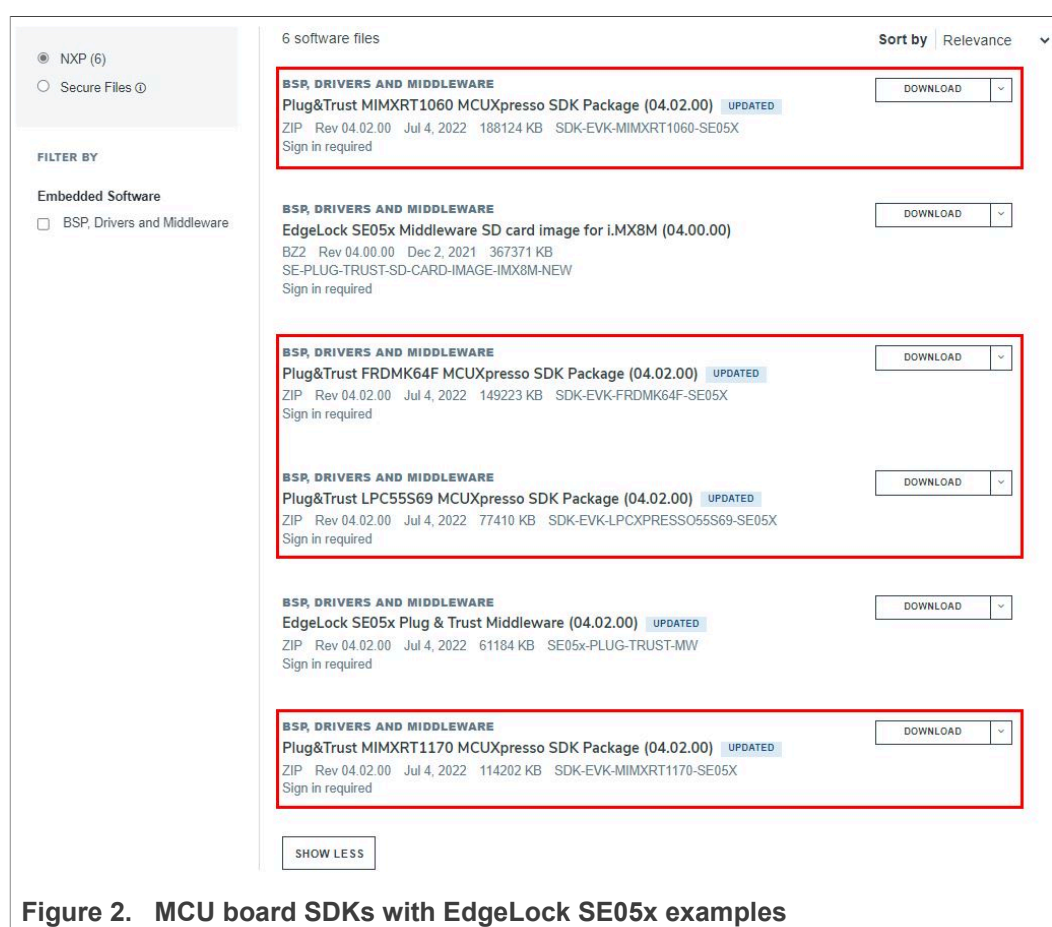


Figure 2. MCU board SDKs with EdgeLock SE05x examples

Note: The MCUXpresso SDK builder for the [MIMXRT1070-EVK](#), the [MIMXRT1060-EVK](#), the [FRDM-K64F](#) and [LPC55S69-EVK](#) also includes a subset of the Plug & Trust MCUXpresso SDKs. The release cycle of the MCUXpresso SDKs and the Plug&Trust middleware is different. Therefore, the MCUXpresso SDK may include an older Plug&Trust middleware version compared to the SDK package provided via the [EdgeLock SE05x product website](#).

Note: The default build configuration of the EdgeLock SE05x Plug & Trust middleware $\geq v04.02.0x$ generates code for the OM-SE050ARD-E development board. You need to adapt settings in the feature header file `fsl_sss_ftr.h` in case you are using a different EdgeLock secure element development board or a different secure

element product IC. The `fsl_sss_ftr.h` settings are described in following MCU board application notes:

- [AN12396](#) EdgeLock SE05x Quick start guide with Kinetis K64F
- [AN12450](#) EdgeLock SE05x Quick start guide with i.MX RT1060 and i.MX RT1170
- [AN12452](#) EdgeLock SE05x Quick start guide with LPC55S69

Note: In addition, the Full Multiplatform EdgeLock SE05x Plug & Trust middleware is delivered with CMake files which allows to compile the [MIMXRT1070-EVK](#), the [MIMXRT1060-EVK](#), the [FRDM-K64F](#) and [LPC55S69-EVK](#) with the help of the CMake-based build system. The CMake-based option is provided for developers familiar with this build system or willing to run exactly the same project example on PC/Windows/Linux and embedded targets. The MCU board application notes are also describing the CMake-build system.

3.2 MCIMX8M-EVK board examples

Similarly, a pre-compiled Linux image with the EdgeLock SE05x Plug & Trust middleware is available for the [MCIMX8M-EVK](#). This pre-compiled Linux image can be directly flashed into a micro-SD card, and booted from [MCIMX8M-EVK](#) for evaluation of EdgeLock SE05x features. The latest EdgeLock SE05x Plug & Trust middleware software package version to create a bootable SD Card image version can be found in [EdgeLock SE05x](#) and [EdgeLock SE051](#) product website, under the *Tools & Software* tab, as shown in [Figure 2](#).

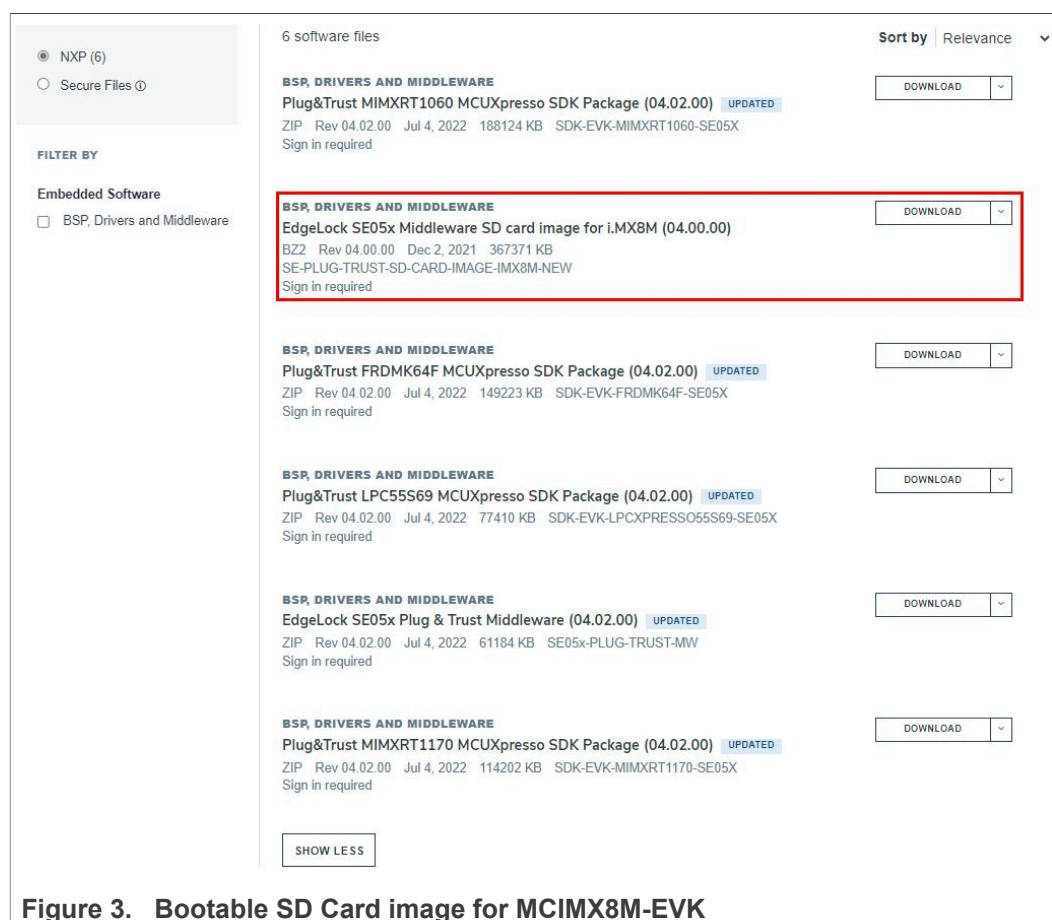


Figure 3. Bootable SD Card image for MCIMX8M-EVK

Note: The default build configuration of the EdgeLock SE05x Plug & Trust middleware $\geq v04.02.0x$ generates code for the OM-SE050ARD-E development board. You need to adapt the CMake settings in case you are using a different EdgeLock secure element development board or a different secure element product IC. The settings are described in chapter [Section 4.1.2](#) and in the application note [AN13027](#) EdgeLock SE05x Quick start guide with i.MX 8M.

3.3 Raspberry Pi board examples

As a reference for device running a Linux distribution, the Full Multiplatform EdgeLock SE05x Plug & Trust middleware includes examples for the Raspberry Pi board.

Note: The default build configuration of the EdgeLock SE05x Plug & Trust middleware $\geq v04.02.0x$ generates code for the OM-SE050ARD-E development board. You need to adapt the CMake settings in case you are using a different EdgeLock secure element development board or a different secure element product IC. The settings are described in chapter [Section 4.1.2](#) and in the application note [AN12570](#) EdgeLock SE05x Quick start guide with Raspberry Pi.

4 EdgeLock SE05x Plug & Trust middleware

To support different application requirements the Plug & Trust Middleware is provided in different packages:

- Full Multiplatform Plug & Trust middleware package
- Plug & Trust Mini Package
- Plug & Trust Nano Package

The **Full Multiplatform Plug & Trust middleware package** is described in [Section 4.1](#).

The **Plug & Trust Mini package** on [GitHub](#) is a subset of the Full Multiplatform Plug & Trust middleware package. It contains the minimal content needed for the Linux target platform and is provided under an Apache 2 license. The source files included are identical to the Full Multiplatform Plug & Trust package. The build system is also simplified and builds only the library with one included example (ex_ecc).

The **Plug & Trust Nano package** on [GitHub](#) is an optimized middleware for communicating between a host processor or microcontroller and the EdgeLock SE05x secure elements and the A5000 authenticator. The Plug & Trust Nano Package has been designed for memory constrained devices and consumes only 1KB of RAM for SCP03 encrypted communication over I2C.

Note: *The examples and libraries contained in the Plug & Trust Nano package have been specifically designed to fit into constrained devices and are not compatible with examples and libraries available in the Full Multiplatform Plug & Trust package.*

4.1 Full Multiplatform EdgeLock SE05x Plug & Trust middleware

The EdgeLock SE05x Plug & Trust middleware is a single software stack designed to facilitate the integration of NXP security ICs into your microcontroller or microprocessor software. This middleware has built-in cryptographic and device identity features,

abstracts the commands and communication interface exposed by NXP security ICs, and it is directly accessible from stacks like OpenSSL, mbedTLS or other cryptographic libraries. In addition, it includes code examples for quick integration of features and uses cases such as TLS and cloud service onboarding. It also comes with support for various NXP MCU / MPU platforms and can be ported to multiple host platforms and host operating systems.

The EdgeLock SE05x Plug & Trust middleware exposes an API called *Secure Sub System (SSS)*, which supports the access to the cryptography and identity features of:

- A71CH
- EdgeLock SE050
- EdgeLock SE051
- Auth-EdgeLock A5000

[Figure 4](#) is a simplified representation of the layers and components of EdgeLock SE05x Plug & Trust middleware:

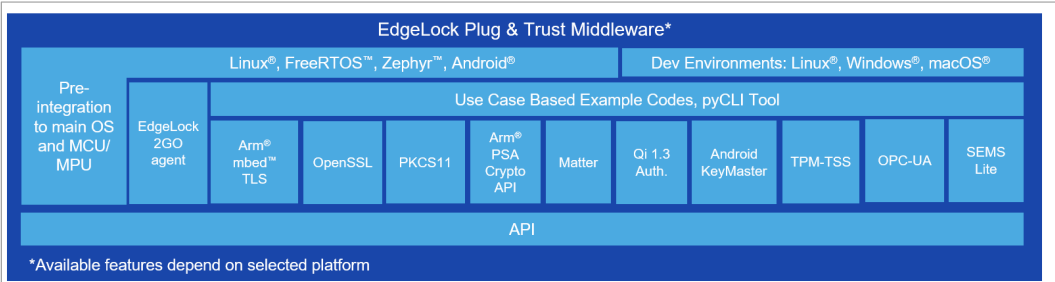


Figure 4. NXP Plug & Trust middleware block diagram

4.1.1 Download the EdgeLock SE05x Plug & Trust middleware

The latest EdgeLock SE05x Plug & Trust middleware version can be found in [EdgeLock SE050](#) and [EdgeLock SE051](#) product websites, under the *Tools & Software* tab, as shown in [Figure 5](#)

Get started with EdgeLock SE05x support package

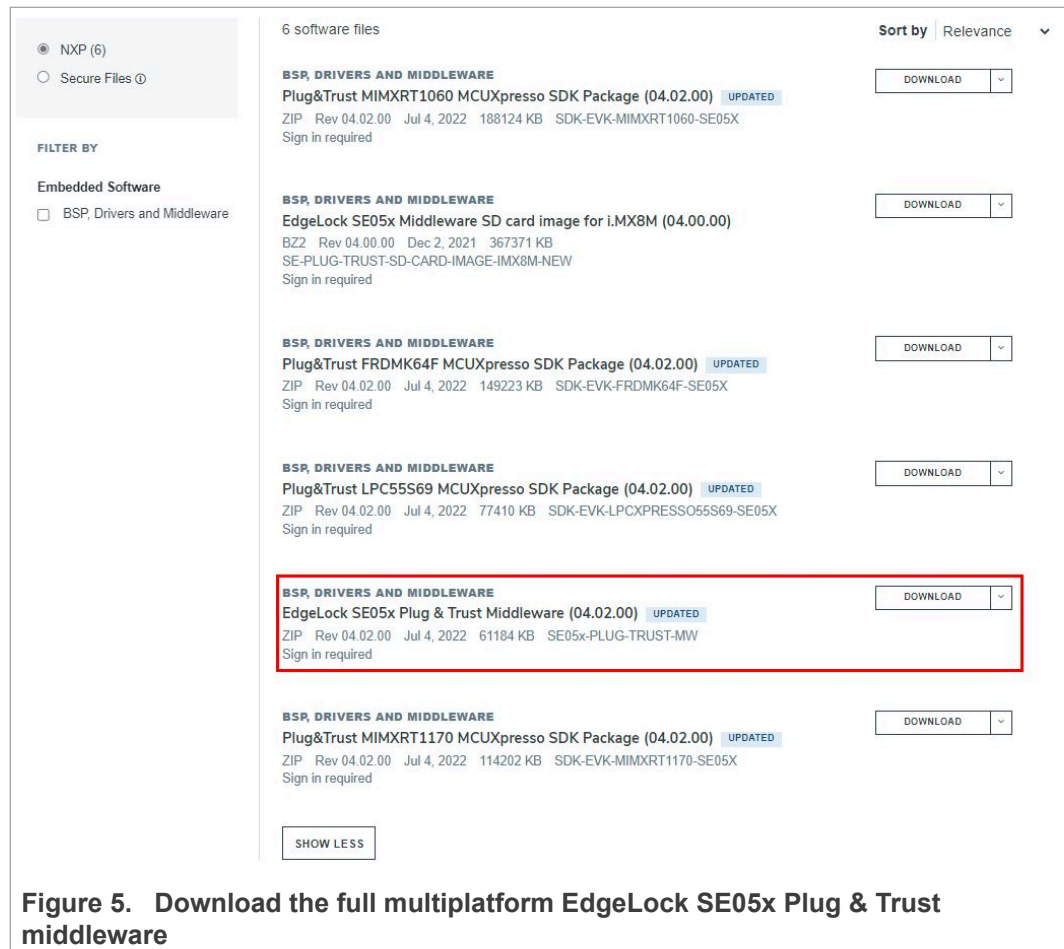


Figure 5. Download the full multiplatform EdgeLock SE05x Plug & Trust middleware

4.1.2 Building and compiling the EdgeLock SE05x Plug & Trust middleware

The EdgeLock SE05x Plug & Trust middleware is delivered with CMake files that include the set of directives and instructions describing the project's source files and targets. The CMake files allow developers to build EdgeLock SE05x middleware in their target platform, enable or disable features or change setting flags, among others. The CMake-based compilation option is provided as a convenient way for developers to run a project example on different target platforms; e.g. Windows and Linux PCs and embedded platforms.

The project settings can be specified dynamically using the CMake GUI. [Figure 6](#) shows a CMake GUI screenshot with EdgeLock SE05x project settings.

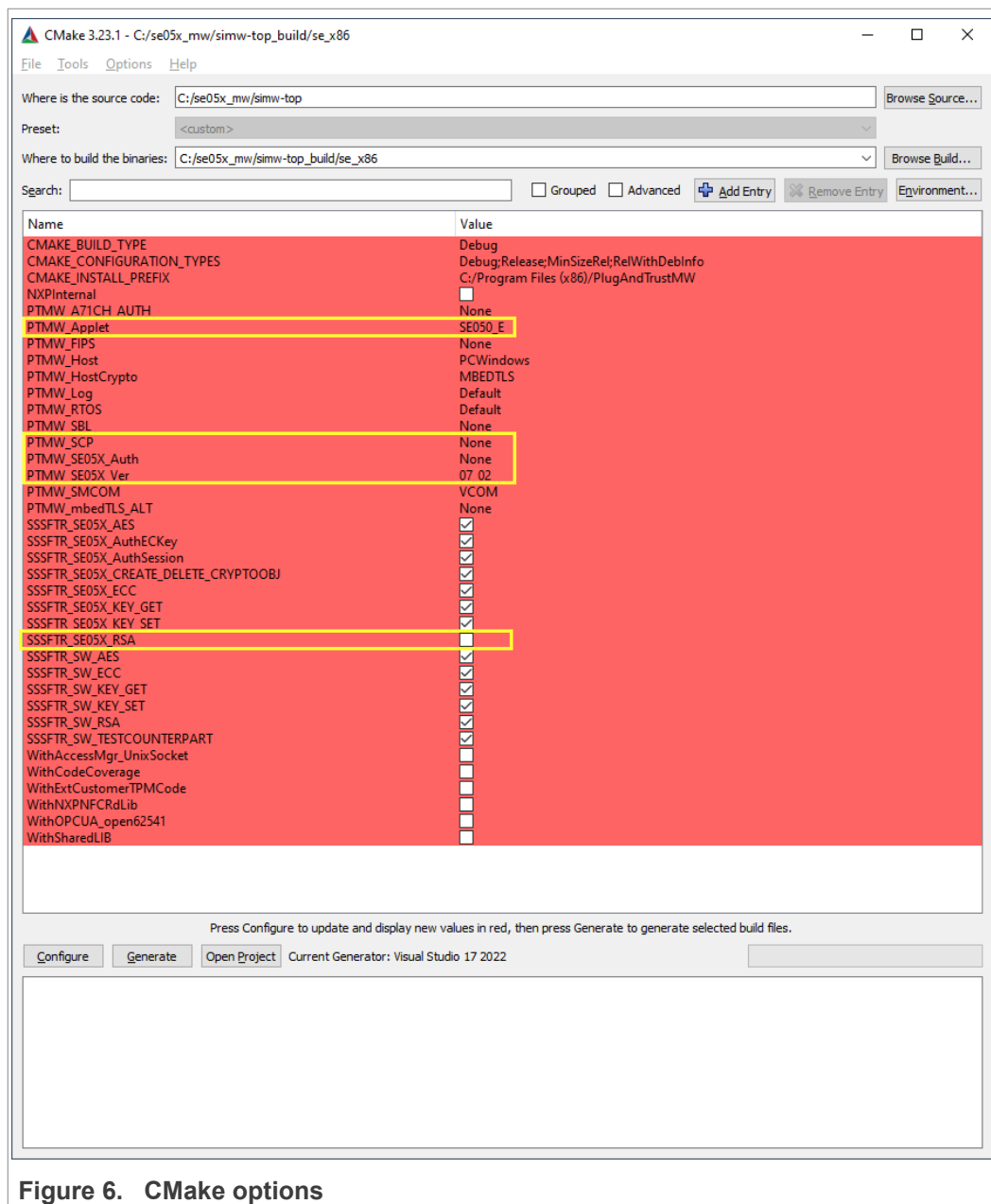


Figure 6. CMake options

Note: The default build configuration of the EdgeLock SE05x Plug & Trust middleware $\geq V04.02.0x$ generates code for the OM-SE05xARD-E development board. You need to adapt the CMake settings in case you are using a different EdgeLock secure element development board or a different secure element product IC. The settings are described in [Section 4.1.2.1](#).

4.1.2.1 Product specific CMake build settings

The EdgeLock Plug & Trust middleware is delivered with CMake files that include the set of directives and instructions describing the project's source files and the build targets. The CMake files are used to select a dedicated EdgeLock product IC and the corresponding IoT applet or Authenticator application.

The SE050 product identification can be obtained as described in [AN12436](#) chapter 1 *Product Information*. [AN12973](#) describes the same procedure for the SE051 product family.

The following tables show the required PTMW CMake options to build the MCUXpresso SDK for a dedicated product variant. The SSSFTR_SE05X_RSA CMake option is used to optimize the memory footprint for product variants that do not support RSA.

Table 4. CMake Settings for SE050E product variants

Variant	OEF ID	PTMW_Applet	PTMW_FIPS	PTMW_SE05X_Ver	PTMW_SE05X_Auth	PTMW_SCP	SSSFTR_SE05X_RSA
SE050E Dev. Board OM-SE050ARD-E	A921	SE05X_E	None	07_02	any option	None	disabled
SE050E2	A921					or SCP03_SSS	

Table 5. CMake Settings for SE050F product variants

Variant	OEF ID	PTMW_Applet	PTMW_FIPS	PTMW_SE05X_Ver	PTMW_SE05X_Auth	PTMW_SCP	SSSFTR_SE05X_RSA
SE050F Dev.Board OM-SE050ARD-F	A92A	SE05X_C	SE050	03_XX	PlatfSCP03	SCP03_SSS	enabled
SE050F2	A92A				or UserID_PlatfSCP03 or AESKey_PlatfSCP03 or ECKey_PlatfSCP03		

Table 6. CMake Settings for SE050 Previous Generation product variants

Variant	OEF ID	PTMW_Applet	PTMW_FIPS	PTMW_SE05X_Ver	PTMW_SE05X_Auth	PTMW_SCP	SSSFTR_SE05X_RSA
SE050A1	A204	SE05X_A	None	03_XX	any option	None	disabled
SE050A2	A205					or SCP03_SSS	
SE050B1	A202	SE05X_B	None	03_XX	any option	None	enabled
SE050B2	A203					or SCP03_SSS	
SE050C1	A200	SE05X_C	None	03_XX	any option	None	enabled
SE050C2	A201					or	
SE050 Dev Board OM-SE050ARD	A1F4					SCP03_SSS	

Table 6. CMake Settings for SE050 Previous Generation product variants...continued

Variant	OEF ID	PTMW_ Applet	PTMW_ FIPS	PTMW_ SE05X_ Ver	PTMW_SE05X_Auth	PTMW_ SCP	SSSFTR_ SE05X_ RSA
SE050F2	A77E ^[1]	SE05X_C	SE050	03_XX	PlatfSCP03 or UserID_PlatfSCP03 or AESKey_PlatfSCP03 or ECKey_PlatfSCP03	SCP03_ SSS	enabled

[1] All SE050F2 with variant A77E have date code in year 2021. All the SE050F2 with date code in the year 2022 have the variant identifier A92A.

Table 7. CMake Settings for SE051 product variants

Variant	OEF ID	PTMW_ Applet	PTMW_ FIPS	PTMW_ SE05X_ Ver	PTMW_SE05X_Auth	PTMW_ SCP	SSSFTR_ SE05X_ RSA
SE051A2	A920	SE05X_A	None	07_02	any option	None or SCP03_ SSS	disabled
SE051C2	A8FA	SE05X_C	None	07_02	any option	None or SCP03_ SSS	enabled
SE051W2	A739	SE05X_C	None	07_02	any option	None or SCP03_ SSS or SCP03_ SSS	enabled
SE051A2	A565	SE05X_A	None	06_00	any option	None or SCP03_ SSS	disabled
SE051C2	A564	SE05X_C	None	06_00	any option	None or SCP03_ SSS	enabled

4.1.3 Example: SE050E CMake build settings

The following images show the configuration for the SE050E development board OM-SE05ARD-E.

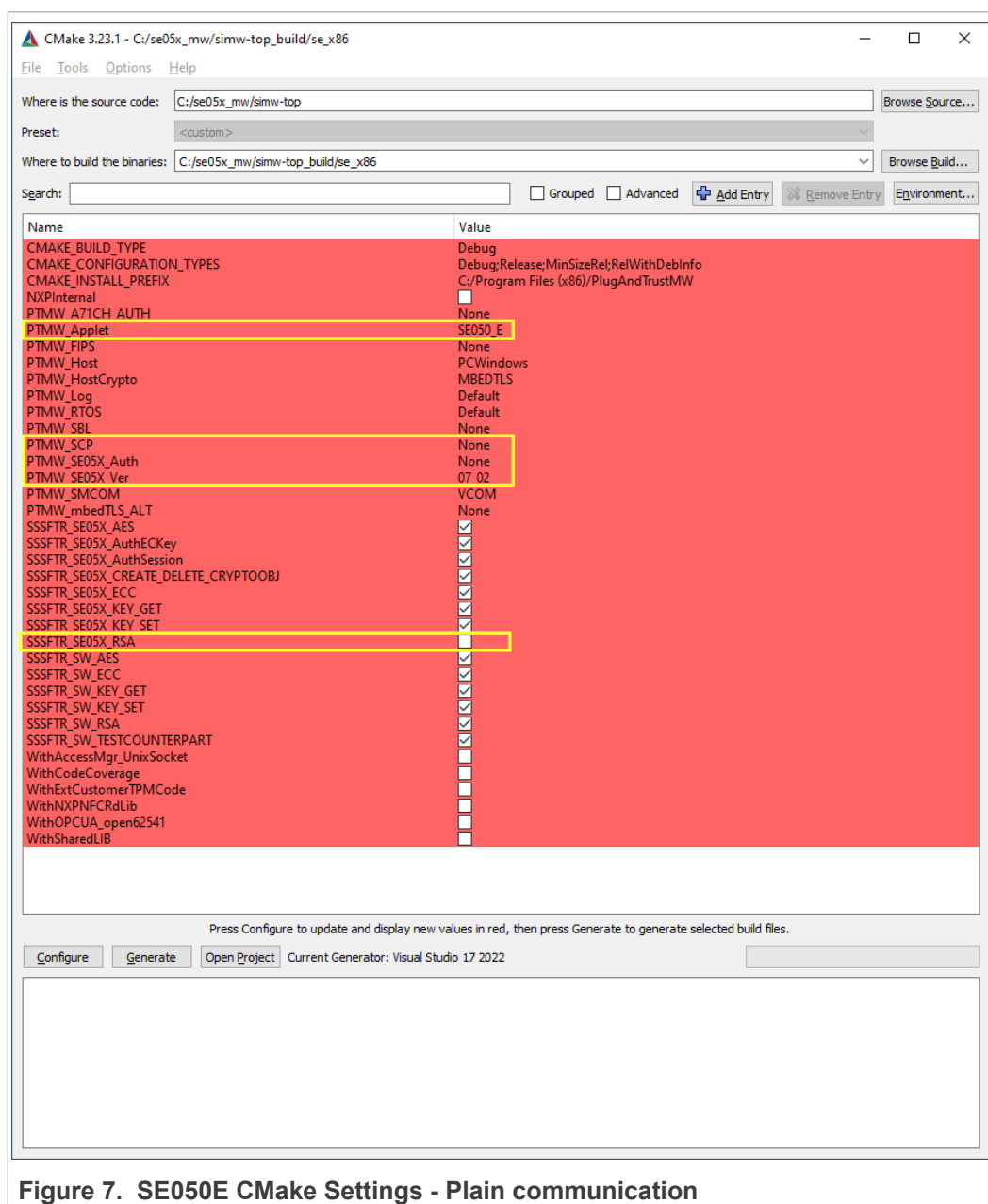
- Select SE05X_E for the CMake option PTMW_Applet.
- Select None for the CMake option PTMW_FIPS.

- Select 07_02 for the CMake option PTMW_SE05X_Ver.
- Disable the CMake option SSSFTR_SE05X_RSA.

In this example we use plain communication. Plain communication for the example execution is enabled by selecting the following options:

- Select None for the CMake option PTMW_SE05X_Auth.
- Select None for the CMake option PTMW_SCP.

How to enable Platform SCP is described in [Section 4.2.3](#).



4.2 Binding EdgeLock SE05x to a host using Platform SCP

Binding is a process to establish a pairing between the IoT device host MPU/MCU and EdgeLock SE05x, so that only the paired MPU/MCU is able to use the services offered by the corresponding EdgeLock SE05x and vice versa.

A mutually authenticated, encrypted channel will ensure that both parties are indeed communicating with the intended recipients and that local communication is protected against local attacks, including man-in-the-middle attacks aimed at intercepting the communication between the MPU/MCU and the EdgeLock SE05x and physical tampering attacks aimed at replacing the host MPU/MCU or EdgeLock SE05x.

EdgeLock SE05x natively supports Global Platform Secure Channel Protocol 03 (SCP03) for this purpose. PlatformSCP uses SCP03 and can be enabled to be mandatory.

This chapter describes the required steps to enable Platform SCP in the middleware for EdgeLock SE05x.

The following topics are discussed:

- [Section 4.2.1](#) Introduction to the Global Platform Secure Channel Protocol 03 (SCP03)
- [Section 4.2.2](#) How to configure the Platform SCP keys
- [How to enable Platform SCP](#) How to enable Platform SCP

4.2.1 Introduction to the Global Platform Secure Channel Protocol 03 (SCP03)

The Secure Channel Protocol SCP03 authenticates and protects locally the bidirectional communication between host and EdgeLock SE05x against eavesdropping on the physical I2C interface.

EdgeLock SE05x can be bound to the host by injecting in both the host and EdgeLock SE05x the same unique SCP03 AES key-set and by enabling the Platform SCP feature in the EdgeLock SE05x Plug & Trust middleware. The [AN12662 Binding a host device to EdgeLock SE05x](#) describes in detail the concept of secure binding.

SCP03 is defined in [Global Platform Secure Channel Protocol '03' - Amendment D v1.2](#) specification.

SCP03 can provide the following three security goals:

- **Mutual authentication (MA)**
 - Mutual authentication is achieved through the process of initiating a Secure Channel and provides assurance to both the host and the EdgeLock SE05x entity that they are communicating with an authenticated entity.
- **Message Integrity**
 - The Command- and Response-MAC are generated by applying the CMAC according NIST SP 800-38B.
- **Confidentiality**
 - The message data field is encrypted across the entire data field of the command message to be transmitted to the EdgeLock SE05x, and across the response transmitted from the EdgeLock SE05x.

The SCP03 secure channel is set up via the EdgeLock SE05x Java Card OS Manager using the standard ISO7816-4 secure channel APDUs.

The establishment of an SCP03 channel requires three static 128-bit AES keys shared between the two communicating parties: *Key-ENC*, *Key-MAC* and *Key-DEK*. These keys

are stored in the Java Card Secondary Security Domain (SSD) and not in the secure authenticator applet.

Key-ENC and Key-MAC keys are used during the SCP03 channel establishment to generate the session keys. Session Keys are generated to ensure that a different set of keys are used for each Secure Channel Session to prevent replay attacks.

Key-ENC is used to derive the session key S-ENC. The S-ENC key is used for encryption/decryption of the exchanged data. The session keys S-MAC and R-MAC are derived from Key-MAC and used to generate/verify the integrity of the exchanged data (C-APDU and R-APDU).

Key-DEK key is used to encrypt new SCP03 keys in case they get updated.

Table 8. Static SCP03 keys

Key	Description	Usage	Key Type
Key-ENC	Static Secure Channel Encryption Key	Generate session key for Decryption/Encryption (AES)	AES 128
Key-MAC	Static Secure Channel Message Authentication Code Key	Generate session key for Secure Channel authentication and Secure Channel MAC Verification/Generation (AES)	AES 128
Key-DEK	Data Encryption Key	Sensitive Data Decryption (AES)	AES 128

The session key generation is performed by the EdgeLock SE05x Plug & Trust middleware host crypto.

Table 9. SCP03 session keys

Key	Description	Usage	Key Type
S-ENC	Session Secure Channel Encryption Key	Used for data confidentiality	AES 128
S-MAC	Secure Channel Message Authentication Code Key for Command	Used for data and protocol integrity	AES 128
S-RMAC	Secure Channel Message Authentication Code Key for Response	User for data and protocol integrity	AES 128

Note: For further details please refer to [Global Platform Secure Channel Protocol '03' - Amendment D v1.2.](#)

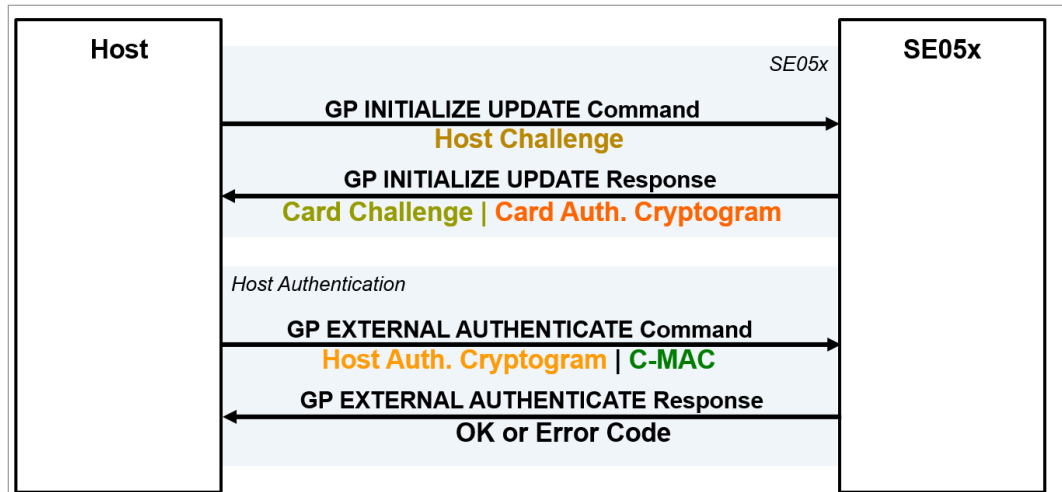


Figure 8. SPC03 mutual authentication – principle

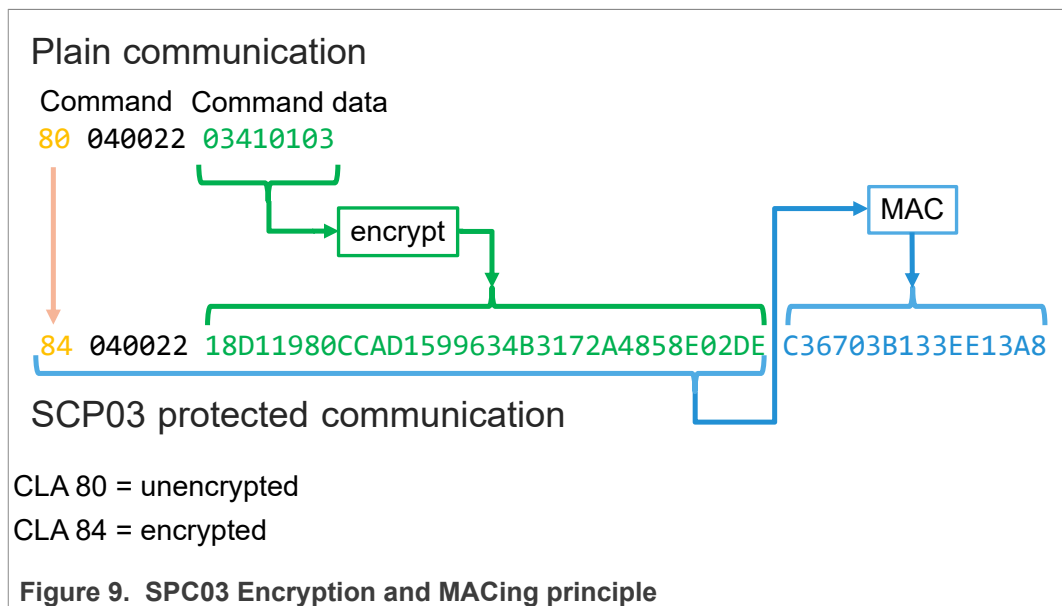


Figure 9. SPC03 Encryption and MACing principle

4.2.2 How to configure the product specific default Platform SCP keys

The default Platform SCP key values are described for the EdgeLock SE05x product variants in [AN12436](#) and for the EdgeLock SE05x variants in [AN12973](#).

The Platform SCP keys can be defined in the EdgeLock SE05x Plug & Trust middleware source code.

The EdgeLock SE05x Plug & Trust middleware header file `ex_sss_tp_scp03_keys.h` contains the default values of all EdgeLock SE05x, EdgeLock SE05x, A5000 and A71CH product variants.

The `ex_sss_tp_scp03_keys.h` header file can be found in the following location: `C:\se05x_mw\simw-top\sss\ex\inc`

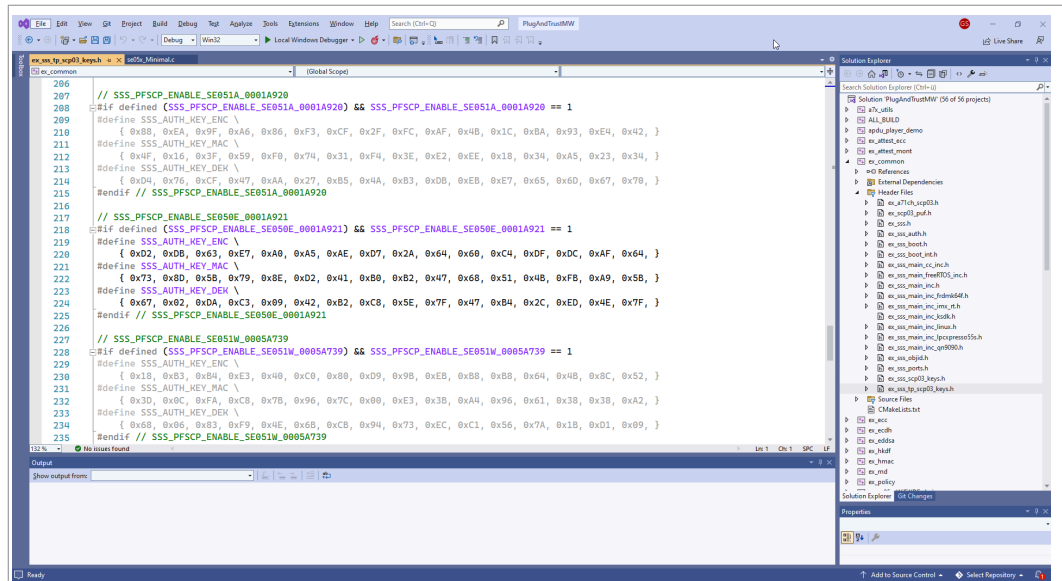


Figure 10. Default Platform SCP keys are defined in ex_sss_tp_scp03_keys.h

The fsl_sss_ftr.h.in file includes options to select one of the predefined default Platform SCP keys. This file is located in: C:\se05x_mw\simw-top\sss\inc

Select the desired value of the compilation option by setting exclusively the corresponding C-preprocessor define SSS_PFSCP_ENABLE_XX to 1 (enable). All other values for the same option (represented by C-preprocessor defines SSS_PFSCP_ENABLE_XX) must be set to 0.

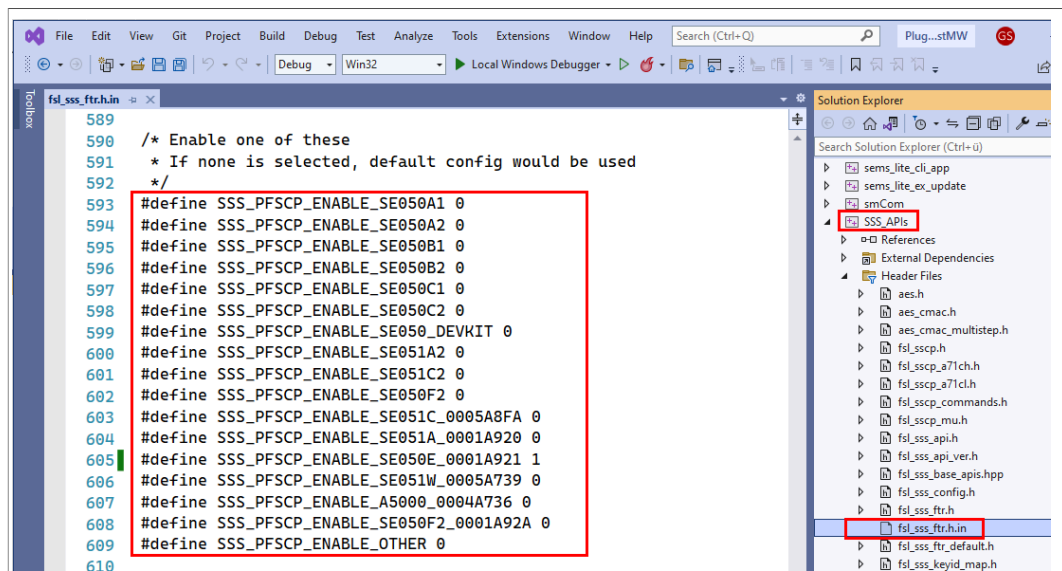


Figure 11. Select the default Platform SCP keys in fsl_sss_ftr.h.

The Plug & Trust Middleware uses a feature file to select/detect used/enabled features within the middleware stack. The file fsl_sss_ftr.h is automatically generated into the used build directory. CMake is overwriting the fsl_sss_ftr.h file every time CMake is invoked. CMake is using the SCP key settings of the fsl_sss_ftr.h.in file as input to generate the the fsl_sss_ftr.h file. You do not have to manually edit

the `fsl_sss_ftr.h` feature file. Selections from CMake edit cache would automatically make relevant updates into the generated feature file.

Note: The Platform SCP key selection in the `fsl_sss_ftr.h` in CMake input file is persistent.

The location of the generated `fsl_sss_ftr.h` feature header file is: `C:\se05x_mw\simw-top_build\se_x86`

The following tables contains the the Platform SCP key header file define to be set to 1 (enable) for the different secure element and secure authenticator product variants.

Table 10. Platform SCP key define prefix for SE050E product variants

Variant	OEF ID	Platform SCP key define to be set to '1'
SE050E Dev. Board OM-SE050ARD-E	A921	SSS_PFSCP_ENABLE_SE050E_0001A921
SE050E2	A921	SSS_PFSCP_ENABLE_SE050E_0001A921

Table 11. Platform SCP key define prefix for SE050F product variants

Variant	OEF ID	Platform SCP key define to be set to '1'
SE050F Dev.Board OM-SE050ARD-F	A92A	SSS_PFSCP_ENABLE_SE050F2_0001A92A
SE050F2	A92A	SSS_PFSCP_ENABLE_SE050F2_0001A92A

Table 12. Platform SCP key define prefix for SE050 Previous Generation product variants

Variant	OEF ID	Platform SCP key define to be set to '1'
SE050A1	A204	SSS_PFSCP_ENABLE_SE050A1
SE050A2	A205	SSS_PFSCP_ENABLE_SE050A2
SE050B1	A202	SSS_PFSCP_ENABLE_SE050B1
SE050B2	A203	SSS_PFSCP_ENABLE_SE050B2
SE050C1	A200	SSS_PFSCP_ENABLE_SE050C1
SE050C2	A201	SSS_PFSCP_ENABLE_SE050C2
SE050 Dev Board OM-SE050ARD	A1F4	SSS_PFSCP_ENABLE_SE050_DEVKIT
SE050F2	A77E ^[1]	SSS_PFSCP_ENABLE_SE050F2

[1] All SE050F2 with variant A77E have date code in year 2021. All the SE050F2 with date code in the year 2022 have the variant identifier A92A.

Table 13. Platform SCP key define prefix for SE051 product variants

Variant	OEF ID	Platform SCP key define to be set to '1'
SE051A2	A920	SSS_PFSCP_ENABLE_SE051A_0001A920
SE051C2	A8FA	SSS_PFSCP_ENABLE_SE051C_0005A8FA
SE051W2	A739	SSS_PFSCP_ENABLE_SE051W_0005A739
SE051A2	A565	SSS_PFSCP_ENABLE_SE051A2
SE051C2	A564	SSS_PFSCP_ENABLE_SE051C2

Table 14. Platform SCP key define prefix for A5000 product variants

Variant	OEF ID	Platform SCP key define to be set to '1'
A5000 Dev. Board OM-A5000ARD	A736	SSS_PFSKP_ENABLE_A5000_0004A736
A5000	A736	SSS_PFSKP_ENABLE_A5000_0004A736

4.2.3 How to enable Platform SCP

To enable Platform SCP is required to rebuild the SDK with the following CMake options:

- Select `SCP03_SSS` for the CMake option `PTMW_SCP`.
- Select `PlatfSCP03` for the CMake option `PTMW_SE05X_Auth`.

The following images show the configuration for the SE050E development board OM-SE05ARD-E.

1. Open a command prompt and go to the directory where the EdgeLock SE05x Plug & Trust middleware is built.
Send: `cd C:\se05x_mw\simw-top_build\se_x86`
2. Open the cmake configuration interface.
Send: `cmake-gui .`

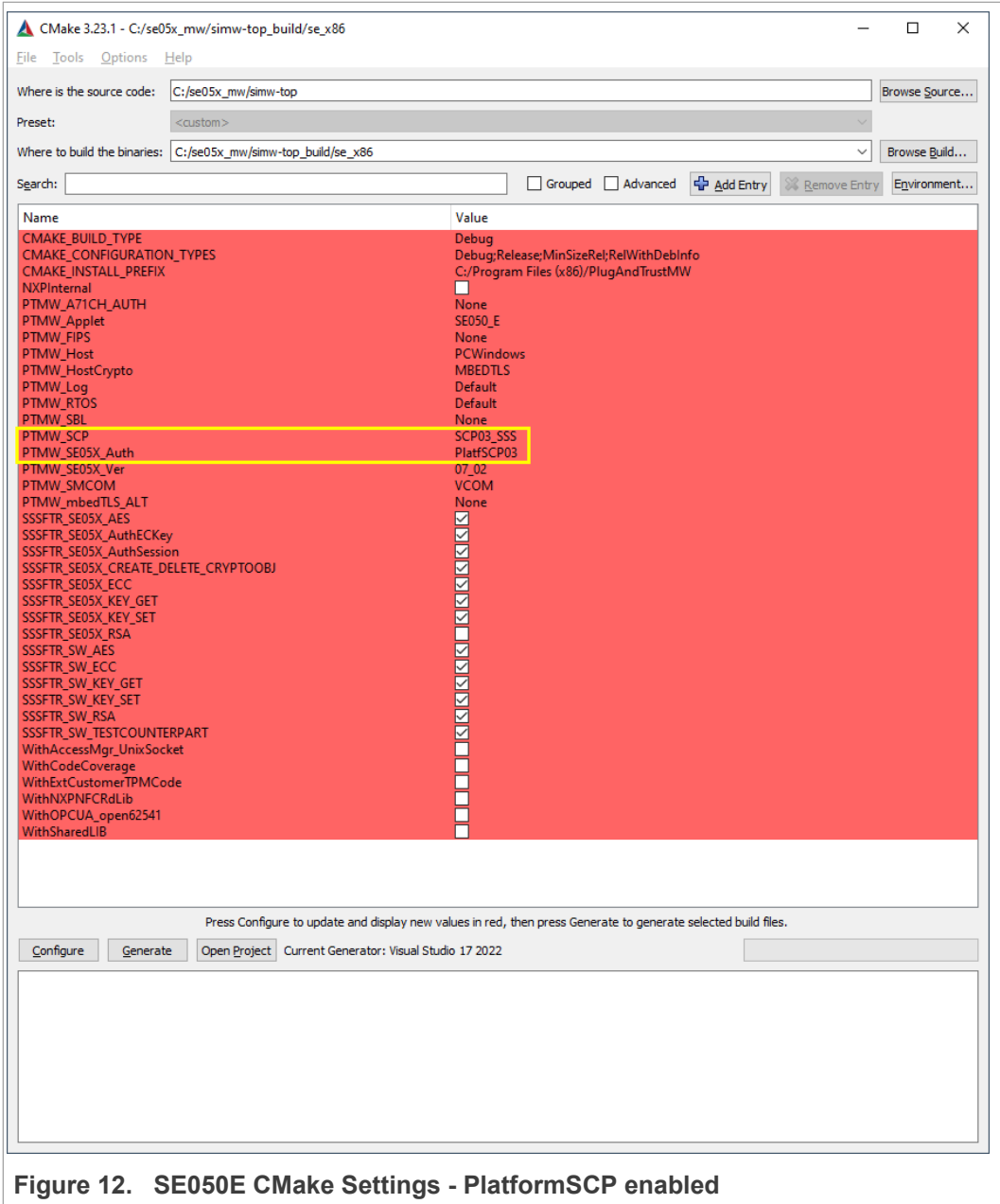


Figure 12. SE050E CMake Settings - PlatformSCP enabled

If you have edited any of the parameters in the menu, before exiting press the buttons **Configure** and **Generate** to apply the changes. In the next step we need to rebuild the Visual Studio solution. Finally, we can verify if we successfully enabled Platform SCP. For this purpose we run again the se05x_minimal example as described in [AN12398](#).

```

Microsoft Visual Studio Debug Console
App :INFO :PlugAndTrust_v04.02.00_20220524
App :INFO :Running C:\se05x_mw\simw-top_build\se_x86\bin\Debug\se05x_Minimal.exe
App :INFO :Using PortName='\\.\COM9' (gszCOMPortDefault)
App :INFO :If you want to over-ride the selection, use ENV=EX_SSS_BOOT_SSS_PORT or pass in command line arguments.
App :INFO :Using default PlatfSCP03 keys. You can use keys from File using ENV=EX_SSS_BOOT SCP03 PATH
Opening COM Port '\\.\COM9'
sss :INFO :atr (Len=35)
01 A0 00 00 03 96 04 03 E8 00 FE 02 0B 03 E8 00
01 00 00 00 00 64 13 88 0A 00 65 53 45 30 35 31
00 00 00
App :INFO :mem=32767
App :WARN :If 32768 bytes or more bytes are available, 32767 bytes free is reported.
App :INFO :se05x_Minimal Example Success !!!...
App :INFO :ex_sss Finished

C:\se05x_mw\simw-top_build\se_x86\bin\Debug\se05x_Minimal.exe (process 2868) exited with code 0.
Press any key to close this window . . .

```

Figure 13. Verify that se05x_minimal project is running with Platform SCP enabled

The Plug & Trust Middleware provides the following additional examples to rotate the PlatformSCP Keys and to mandate Platform SCP.

- **SE05x Rotate PlatformSCP Keys example:** Showcases authentication with default Platform SCP03 keys and the rotation (update) of those keys with user defined keys. The example documentation is available in the EdgeLock SE05x Plug & Trust Middleware documentation (C:\se05x_mw\simw-top\doc\demos\se05x\se05x_RotatePlatformSCP03Keys\Readme.html). The example source code is available at C:\se05x_mw\simw-top\demos\se05x\se05x_RotatePlatformSCP03Keys.
- **SE05X Mandate SCP example:** Showcases how to make Platform SCP03 authentication mandatory in EdgeLock SE05x. The example documentation is available in the EdgeLock SE05x Plug & Trust Middleware documentation (C:\se05x_mw\simw-top\doc\demos\se05x\se05x_MandatePlatformSCP\Readme.html). The example source code is available at C:\se05x_mw\simw-top\demos\se05x\se05x_MandatePlatformSCP.
- **SE05x AllowWithout PlatformSCP example:** This project demonstrates how to configure SE05X to allow without platform SCP. The example documentation is available in the EdgeLock SE05x Plug & Trust Middleware documentation (~\se_mw\simwtop\doc\demos\se05x\se05x_AllowWithoutPlatformSCP\Readme.html). The example source code is available at ~\se_mw\simw-top\demos\se05x\se05x_AllowWithoutPlatformSCP.

4.3 Code documentation

The code documentation provided as part of EdgeLock SE05x Plug & Trust middleware package is supplied in HTML and PDF form. The primary audience of this HTML documentation are programmers, developers, system architects and system designers. It includes:

- Technical API reference guide.
- Instructions to compile and build EdgeLock SE05x Plug & Trust middleware.
- Instructions to run the `sssccli` tool. See [Section 4.4](#) for more details.
- Developer guides to execute the demo and examples.

To open the HTML documentation:

1. Download EdgeLock SE05x Plug & Trust middleware as explained in [Section 4](#).
2. Unzip the EdgeLock SE05x Plug & Trust middleware package.
3. In the unzipped package, go to `simw-top\doc\` folder.
4. Double click in the `index.html` file.
5. A browser with the documentation landing page will open as shown in [Figure 14](#):

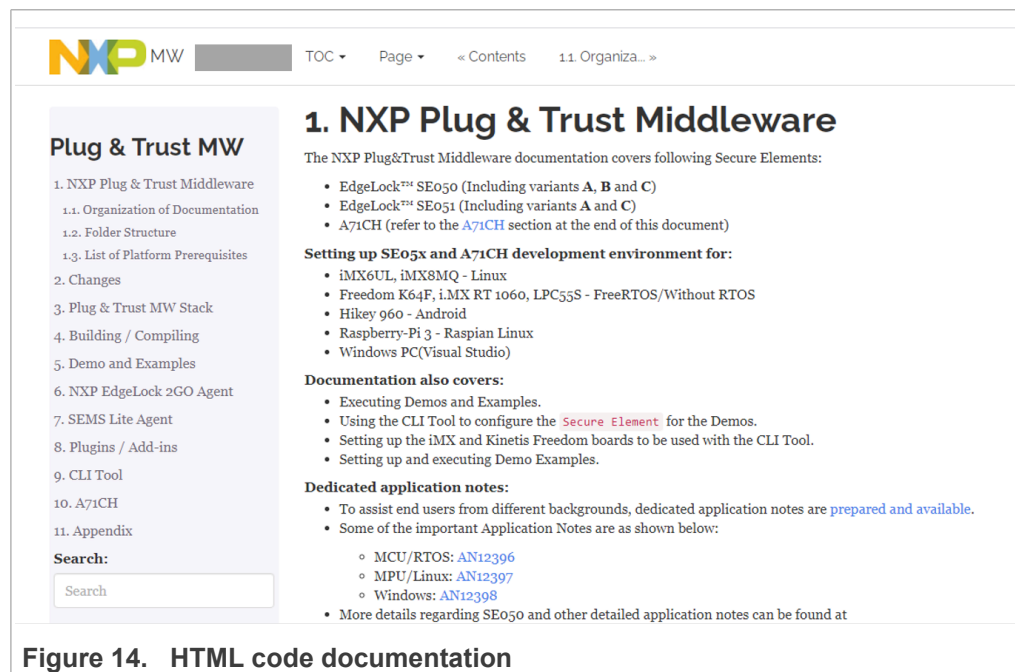


Figure 14. HTML code documentation

6. From the same browser, you can navigate through the different document sections using the left-hand side menu or the hyper-linked table of contents shown in the center. For instance, to check the EdgeLock SE05x Plug & Trust middleware

description, click on Section 3. Plug & Trust MW Stack on the left hand side menu as shown in [Figure 15](#):

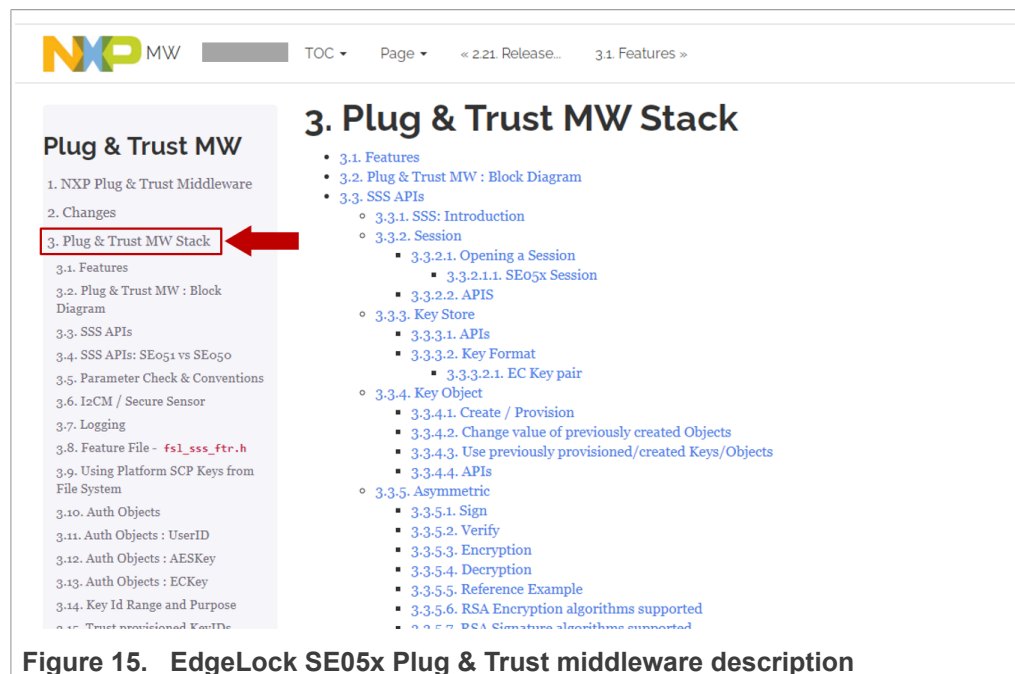


Figure 15. EdgeLock SE05x Plug & Trust middleware description

4.4 EdgeLock SE05x ssscli tool

The `ssscli` is a command line tool that can be used to send commands to EdgeLock SE05x interactively through the command line. For example, you can use the `ssscli` to create keys and credentials in the EdgeLock SE05x security IC during evaluation, development and testing phases. The `ssscli` tool is written in Python and supports complex provisioning scripts that can be run in Windows, Linux, OS X and other embedded devices. It can be used to:

- Insert keys and certificates
- Read reference-keys and certificates
- Delete (erase) keys and certificates
- Generate keys inside the EdgeLock SE05x
- Attach policies to objects
- List all secure objects
- Retrieve the EdgeLock SE05x device unique ID
- Run some basic operations like sign/verify and encrypt/decrypt operations

The EdgeLock SE05x Plug & Trust middleware code documentation provides detailed usage examples of the `ssscli` tool. To find these usage examples:

1. Download EdgeLock SE05x Plug & Trust middleware as explained in [Section 4.1.1](#).
2. Unzip the EdgeLock SE05x Plug & Trust middleware package.
3. Go to `simw-top\doc\` folder.
4. Double click in the `index.html` file.

5. Click on Section 9 CLI tool and then click on the Section 9.6 Usage examples as shown in [Figure 16](#)

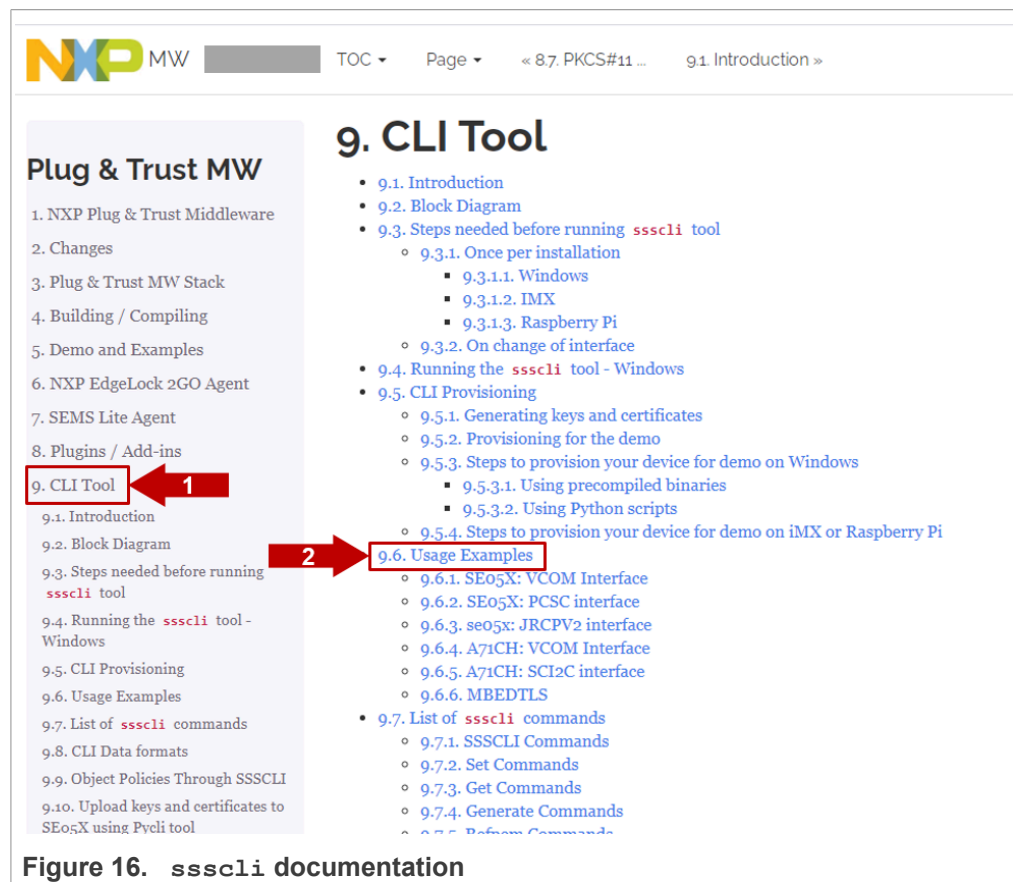
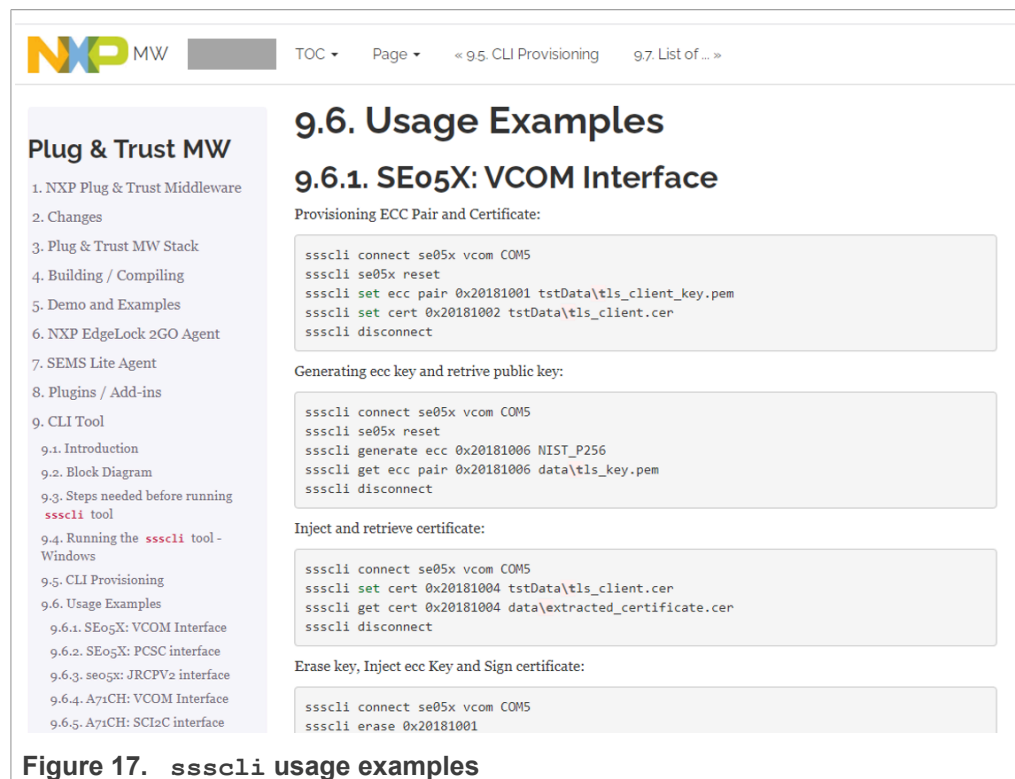


Figure 16. `sscli` documentation

6. You will see a new page with examples describing how to use ssscli tool for the most common operations:



4.4.1 EdgeLock SE05x ssscli tool example

The EdgeLock SE05x Plug & Trust middleware includes all components required to verify the EdgeLock SE05x under Windows using the ssscli tool without the need to build the middleware. To be able to connect the SE05x-ARD board to a Windows PC, one of the following MCU boards running a VCOM to T1 Over I2C firmware is required:

- [MIMXRT1170-EVK](#)
- [MIMXRT1060-EVK](#)
- [FRDM-K64F](#)
- [LPC55S69-EVK](#)

The MCU boards are connected via USB to the Windows PC and the MCU board VCOM to T1 Over I2C firmware is acting as a bridge between the PC VCOM interface and the EdgeLock SE05x Secure Element.

This setup also allows to run the EdgeLock SE05x middleware Visual Studio project examples on a Windows platform. Further details can be found in [AN12398](#) EdgeLock SE05x Quick start guide with Visual Studio project examples explains.

In [Table 15](#) you can find the corresponding application note reference which explains the correct OM-SE05xARD and MCU board connecting. The quick start guides for the MCU boards are also including the correct OM-SE05xARD jumper configuration.

The precompiled VCOM binaries for the MIMXRT1170-EVK, the MIMXRT1060-EVK, the FRDM-K64F and the LPC55S69-EVK MCU boards are located in `.\simw-top\binaries\MCU\se05x:`

- se05x_vcom-T1oI2C-evkmimxrt1170.bin
- se05x_vcom-T1oI2C-evkmimxrt1060.bin
- se05x_vcom-T1oI2C-frdmk64f.bin
- se05x_vcom-T1oI2C-lpcxpresso55s69.bin

The pre-compiled Windows ssscli tool is located in `.\simw-top\binaries\PCWindows\ssscli`.

Note: The Windows ssscli tool `ssscli.exe` (folder `.\simw-top\binaries\PCWindows\ssscli`) is using a pre-compiled `sssapisw.dll`. This DLL is compiled for applet version 3.xx to support the previous SE050 product versions. To take advantage of all SE050E features it is recommended to use the pre-compiled `sssapisw.dll` for applet version 7.02 (folder: `.\simw-top\binaries\PCWindows\ssscli\07_02`). You need to rename the `sssapisw_07_02.dll` to `sssapisw.dll` first. In the next step you need to copy the `sssapisw.dll` from `.\simw-top\binaries\PCWindows\ssscli\07_02` into `.\simw-top\binaries\PCWindows\ssscli`.

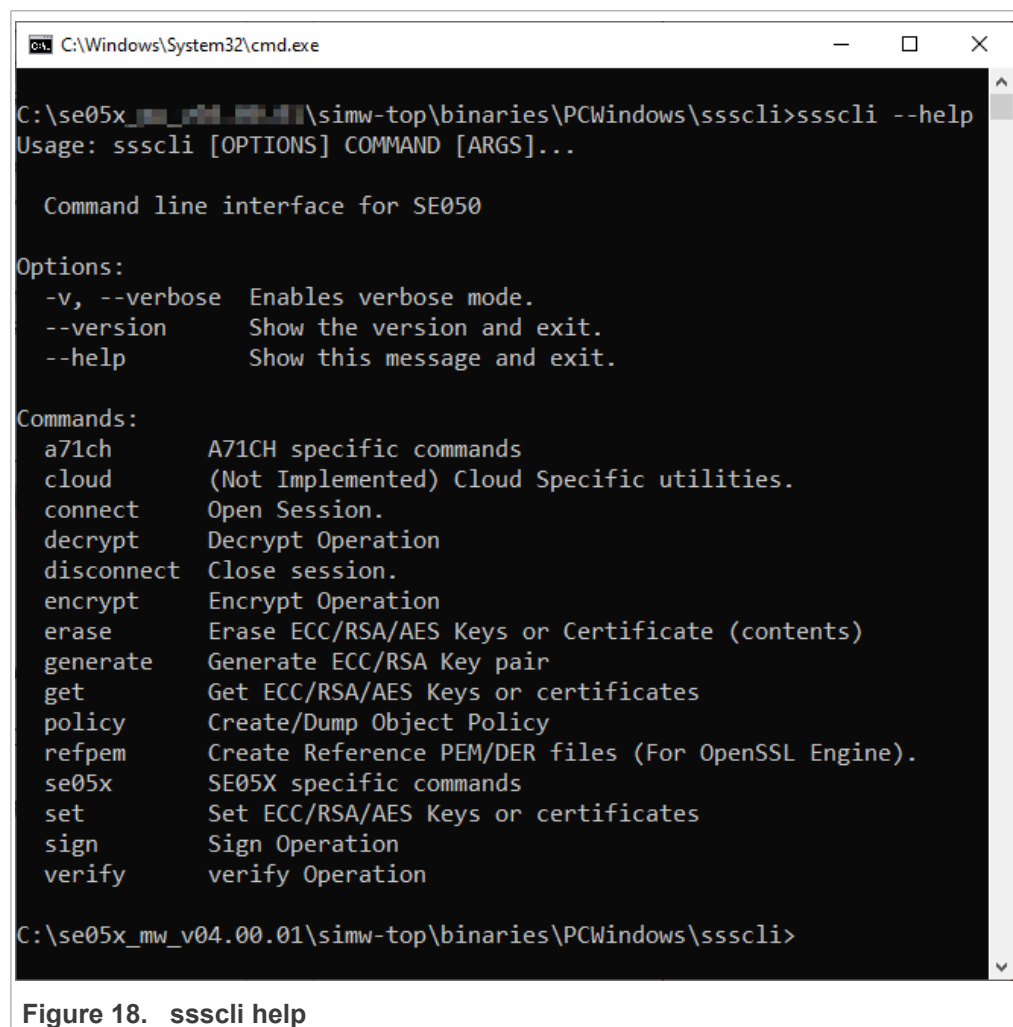
Alternative you could re-compile the middleware in Windows using the CMake settings as described in [AN12398](#) EdgeLock SE05x Quick start guide with Visual Studio project examples. In the final step you need to copy the new generated `sssapisw.dll` from `.\simw-top\tools` into `.\simw-top\binaries\PCWindows\ssscli`.

4.4.1.1 List all SE05x secure objects

To list all secure objects from EdgeLock EdgeLock SE05x dynamic file system, follow these steps:

1. First, open a command prompt and navigate to `.\simw-top\binaries\PCWindows\ssscli`.

2. You can use the following command to display the ssscli build in help:
`ssscli --help`.



```
C:\Windows\System32\cmd.exe

C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\ssscli>ssscli --help
Usage: ssscli [OPTIONS] COMMAND [ARGS]...

Command line interface for SE050

Options:
  -v, --verbose  Enables verbose mode.
  --version      Show the version and exit.
  --help        Show this message and exit.

Commands:
  a71ch      A71CH specific commands
  cloud      (Not Implemented) Cloud Specific utilities.
  connect    Open Session.
  decrypt    Decrypt Operation
  disconnect  Close session.
  encrypt    Encrypt Operation
  erase       Erase ECC/RSA/AES Keys or Certificate (contents)
  generate    Generate ECC/RSA Key pair
  get        Get ECC/RSA/AES Keys or certificates
  policy     Create/Dump Object Policy
  refpem     Create Reference PEM/DER files (For OpenSSL Engine).
  se05x      SE05X specific commands
  set        Set ECC/RSA/AES Keys or certificates
  sign       Sign Operation
  verify     verify Operation

C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\ssscli>
```

Figure 18. ssscli help

3. To get all option for the connect command use: `sscli connect --help`.

```

C:\Windows\System32\cmd.exe
C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\sscli>sscli connect --help
Usage: sscli connect [OPTIONS] subsystem method port_name

Open Session.

subsystem = Security subsystem is selected to be used. Can be one of "se05x,
auth, a71ch, mbedtls, openssl"

method = Connection method to the system. Can be one of "none, sci2c, vcom,
t1oi2c, jrcpv1, jrcpv2, pcsc"

port_name = Subsystem specific connection parameters. Example: COM6,
127.0.0.1:8050. Use "None" where not applicable. e.g. SCI2C/T1oI2C. Default
i2c port (i2c-1) will be used for port name = "None".

Options:
--auth_type [None|PlatformSCP|UserID|EKey|AESKey|UserID_PlatformSCP|EKey_PlatformSCP|AESKey_PlatformSCP]
Authentication type. Default is "None". Can
be one of "None, UserID, EKey, AESKey,
PlatformSCP, UserID_PlatformSCP,
EKey_PlatformSCP, AESKey_PlatformSCP"
--scpkey TEXT
File path of the platformscp keys for
platformscp session
--help
Show this message and exit.

C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\sscli>

```

Figure 19. `sscli connect help`

The EdgeLock SE05x supports same specific commands.

`sscli se05x --help`

```

C:\Windows\System32\cmd.exe
C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\sscli>sscli se05x --help
Usage: sscli se05x [OPTIONS] COMMAND [ARGS]...

SE05X specific commands

Options:
--help Show this message and exit.

Commands:
certuid      Get SE05X Cert Unique ID (10 bytes)
readidlist  Read contents of SE050
reset       Reset SE05X
uid         Get SE05X Unique ID (18 bytes)

C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\sscli>

```

Figure 20. `sscli se05x help`

4. Connect to the EdgeLock SE05x using the executable `sscli.exe`. You need to indicate the VCOM port number corresponding to your MCU VCOM port. The subsystem option `se05x` shall be to define a session with the EdgeLock SE05x. The

following commands will connect to the EdgeLock SE05x, list all EdgeLock SE05x secure objects and close the connection.

- ssscli connect se05x vcom COMxx
- ssscli se05x readidlist
- ssscli disconnect

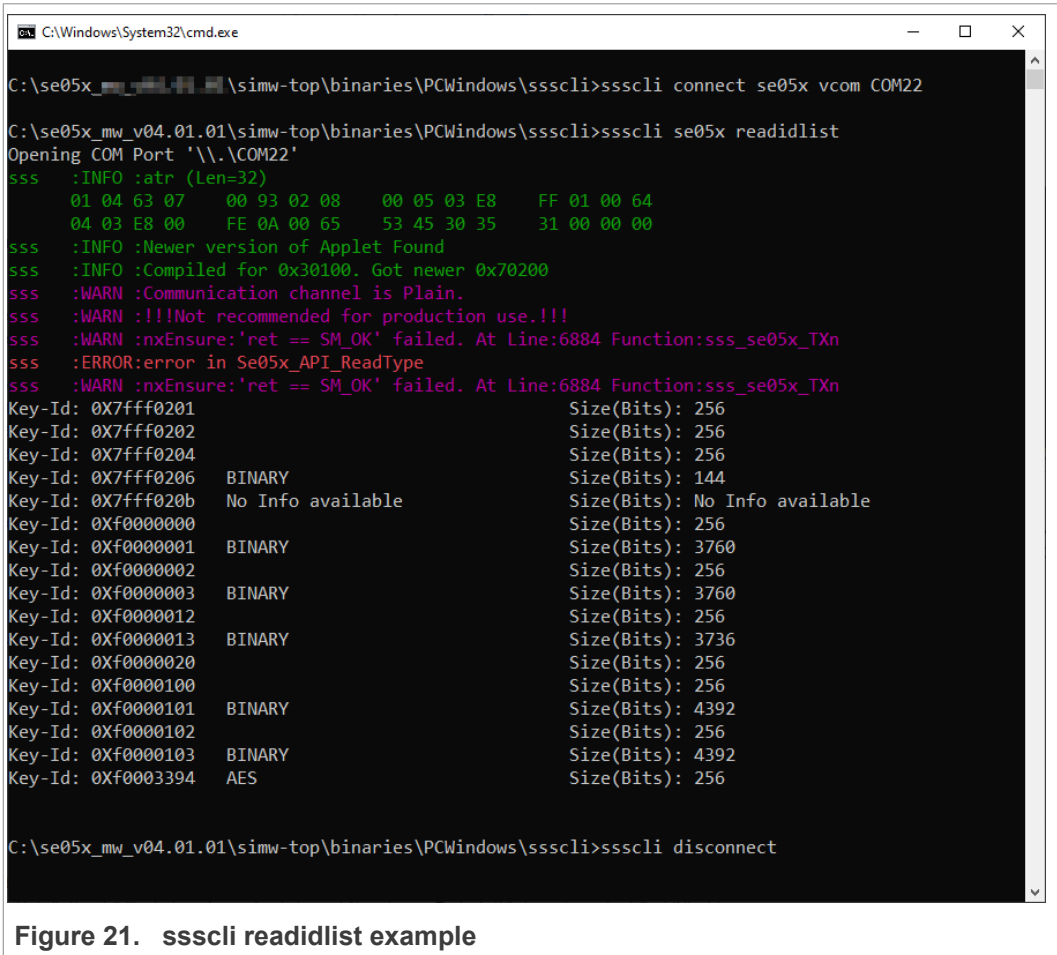


Figure 21. ssscli readidlist example

5 Support documentation

The EdgeLock SE05x support package includes extensive application notes that explain EdgeLock SE05x features, use cases, and how to try out the sample code and demo examples provided in the EdgeLock SE05x Plug & Trust middleware.

[Table 15](#) summarizes the EdgeLock SE05x application notes available and indicates for which product family each one is applicable.

Note: Click on the hyperlink in the app note numbers to download the document, or click on the hyperlink in the app note title to navigate through the specific app note section.

Table 15. EdgeLock SE05x support documentation

App note	Title	Product
AN12396	Quick start guide with Kinetis K64F	SE05x

Table 15. EdgeLock SE05x support documentation...continued

App note	Title	Product
AN13027	Quick start guide with i.MX 8M	SE05x
AN12450	Quick start guide with i.MX RT1060 and i.MX1170	SE05x
AN12452	Quick start guide with LPC55S69	SE05x
AN12570	Quick start guide with Raspberry Pi	SE05x
AN12398	Quick start guide with Visual Studio project examples	SE05x
AN12404	Secure connection to AWS IoT Core	SE05x
AN12401	Secure connection to Google Cloud Platform	SE05x
AN12402	Secure connection to Azure IoT Hub	SE05x
AN12403	Secure connection to IBM Watson IoT	SE05x
AN12400	Secure connection to OEM cloud	SE05x
AN12449	Sensor data protection	SE05x
AN12399	Device-to-device authentication	SE05x
AN12569	Secure access control in Industrial IoT	SE05x
AN12661	Wi-Fi credential protection	SE05x
AN12664	NFC late-stage configuration	SE05x
AN12662	Binding a host device to EdgeLock SE05x	SE05x
AN12660	Ease ISA/IEC 62443 compliance with EdgeLock SE05x	SE05x
AN12448	Middleware porting guidelines	SE05x
AN12663	TPM functionality	SE05x
UM11225	NXP EdgeLock SE05x T=1 Over I2C specification	SE05x
AN13539	OM-SE05xARD board hardware overview	SE05x
AN12543	SE05x APDU specification APDU specification	SE050E/ SE051
AN12413	EdgeLock SE050 APDU specification	SE050A/B/C/F
AN13483	SE050E - User Guidelines	SE050E
AN13482	SE050F - User Guidelines	SE050F available in Secure Files
AN12514	EdgeLock SE050 user guidelines	SE050A/B/C/F
AN12436	EdgeLock SE050 product configurations	SE050
AN12543	EdgeLock SE051 APDU specification	SE050E/ SE051
AN12973	EdgeLock SE051 product configurations	SE051
AN12730	EdgeLock SE051 user guidelines	SE051
AN12907	Secure update of EdgeLock SE051 IoT applet	SE051
AN13015	How to use EdgeLock SE051 personalization applet	SE051

5.1 AN12396 - Quick start guide with Kinetis K64F

The AN12396 explains how to get started with EdgeLock SE05x Plug & Trust middleware using the OM-SE05xARD and FRDM-K64F MCU boards. It provides detailed instructions

to run projects imported either from the FRDMK64F SDK or the CMake-based build system included in the EdgeLock SE05x Plug & Trust middleware.

5.2 AN13027 - Quick start guide with i.MX 8M

The AN13027 explains how to get started with the OM-SE05xARD board and i.MX 8M board. This guide provides detailed instructions for connecting the boards, installing the software, running the EdgeLock SE05x Plug & Trust middleware test examples and executing the ssscli tool.

5.3 AN12450 - Quick start guide with i.MX RT1060 and i.MX RT1170

The AN12450 explains how to get started with EdgeLock SE05x Plug & Trust middleware using the OM-SE05xARD and i.MX RT1060/1170 MCU boards. It provides detailed instructions to run projects imported either from the i.MX RT1060 SDK or the CMake-based build system included in the EdgeLock SE05x Plug & Trust middleware.

5.4 AN12452 - Quick start guide with LPC55S69

The AN12452 explains how to get started with EdgeLock SE05x Plug & Trust middleware using the OM-SE05xARD and LPC55S69 MCU boards. It provides detailed instructions to run projects imported either from the LPC55S69 SDK or the CMake-based build system included in the EdgeLock SE05x Plug & Trust middleware.

5.5 AN12570 - Quick start guide with Raspberry Pi

The AN12570 explains how to get started with the OM-SE050ARD board and the Raspberry Pi board, as a reference for any other device running a Linux distribution. This guide provides detailed instructions for connecting the boards and running the project examples included in EdgeLock SE05x Plug & Trust middleware.

5.6 AN12398 - Quick start guide with Visual Studio project examples

The AN12398 explains how to get started with EdgeLock SE05x Plug & Trust middleware using the Visual Studio project examples. It provides detailed instructions to run the Microsoft Visual Studio projects using the CMake-based build system included in the EdgeLock SE05x Plug & Trust middleware.

5.7 AN12404 - Secure connection to AWS IoT Core

The EdgeLock SE05x is designed to provide a tamper-resistant platform to safely store credentials needed for device authentication and registration to public or private clouds. EdgeLock SE05x helps to set up a trusted TLS connection to onboard devices to the cloud without writing security code or exposing credentials or keys

The AN12404 describes how to leverage the EdgeLock SE05x for secure cloud onboarding to the AWS IoT Core IoT Hub cloud platform. It provides detailed instructions to run the software example provided as part of the support package using an OM-SE05xARD and an FRDM-K64F board.

5.8 AN12401 - Secure connection to Google Cloud Platform

The EdgeLock SE05x is designed to provide a tamper-resistant platform to safely store credentials needed for device authentication and registration to public or private clouds. EdgeLock SE05x helps to set up a trusted TLS connection to onboard devices to the cloud without writing security code or exposing credentials or keys

The AN12401 describes how to leverage the EdgeLock SE05x ease-of-use configuration for secure cloud onboarding to the Google Cloud IoT Core cloud platform. It provides detailed instructions to run the software example provided as part of the support package using an OM-SE05xARD and an FRDM-K64F board.

5.9 AN12402 - Secure connection to Azure IoT Hub

The EdgeLock SE05x is designed to provide a tamper-resistant platform to safely store credentials needed for device authentication and registration to public or private clouds. EdgeLock SE05x helps to set up a trusted TLS connection to onboard devices to the cloud without writing security code or exposing credentials or keys

The AN12402 describes how to leverage the EdgeLock SE05x ease-of-use configuration for secure cloud onboarding to the Azure IoT Hub cloud platform. It provides detailed instructions to run the software example provided as part of the support package using an OM-SE05xARD and an iMX6UltraLite or i.MX 8M board with a Linux OS.

5.10 AN12403 - Secure connection to IBM Watson IoT

The EdgeLock SE05x is designed to provide a tamper-resistant platform to safely store credentials needed for device authentication and registration to public or private clouds. EdgeLock SE05x helps to set up a trusted TLS connection to onboard devices to the cloud without writing security code or exposing credentials or keys

The AN12403 note describes how to leverage the EdgeLock SE05x ease-of-use configuration for secure cloud onboarding to the Watson IoT cloud platform. It provides detailed instructions to run the software example provided as part of the support package using an OM-SE050ARD and an FRDM-K64F board.

5.11 AN12400 - Secure connection to OEM cloud

The EdgeLock SE05x is designed to provide a tamper-resistant platform to safely store credentials needed for device authentication and registration to public or private clouds. EdgeLock SE05x helps to set up a trusted TLS connection to onboard devices to the cloud without writing security code or exposing credentials or keys.

The AN12400 describes how to leverage EdgeLock SE050 to establish a secure connection with the private cloud of an Original Equipment Manufacturer.

5.12 AN12449 - Sensor data protection

The EdgeLock SE05x is designed to be used as a companion chip to any type of MCU or MPU. Sensors can be directly connected to EdgeLock SE05x using an I²C controller interface. EdgeLock SE05x allows you to set up a secure, end-to-end connection from the sensor or actuator to your local IoT gateway or cloud-based service, protecting the interface between the sensor and the security IC. As such, EdgeLock SE05x helps you to provide a higher level of security in your IoT system by:

- **Preventing data manipulation:** The data extracted by the sensor is collected privately and cannot be manipulated.
- **Authenticating the sensor:** The system authenticates the sensor as a proof of origin.
- **Providing end-to-end security:** The data collected over the private sensor can be encrypted and securely transferred to your gateway or cloud for further treatment and analysis.

The AN12449 note describes how to leverage EdgeLock SE05x for guaranteeing sensor data protection. It gives insights into the integration of EdgeLock SE05x from a hardware and software perspective for this use case. It also provides detailed instructions to run a code example that demonstrates how to leverage EdgeLock SE05x to protect data from a security-sensitive sensor

5.13 AN12399 - Device-to-device authentication

The EdgeLock SE05x provides a tamper-resistant hardware that is capable of securely storing keys and credentials needed to verify the authenticity of an IoT device and a server. The AN12399 describes how to implement a strong mutual authentication mechanisms using digital certificates.

5.14 AN12569 - Secure access control in Industrial IoT

The EdgeLock SE05x can be used as a Secure Access Module (SAM) to increase the security of your IoT-enabled card reader for physical or logical access. In this context, the EdgeLock SE05x can be used by a card reader to setup a secure transaction with MIFARE DESFire EV2 contactless cards. As such, EdgeLock SE05x helps you to provide a higher level of security in your access control system by:

- **Protecting the master keys:** The master keys used for card authentication are protected inside the EdgeLock SE05x and can not be read or manipulated.
- **Authenticating the card:** EdgeLock SE05x supports the authentication protocol and the session key generation algorithm of MIFARE DESFire EV2 card.
- **Performing securely related commands:** EdgeLock SE05x supports secure key change or key diversification of MIFARE DESFire EV2 cards

The AN12569 describes how EdgeLock SE05x, in combination with a microcontroller, supports secure access control in any industrial operation or environment. It gives insights into the integration of EdgeLock SE05x from a hardware and software perspective for this use case. It also provides detailed instructions to run a set of code examples that demonstrate how to leverage EdgeLock SE05x and LPC55S to support secure operation with a MIFARE DESFire EV2 card. In this case, the LPC55SS is used as an example and the same concept is applicable using another host MCU.

5.15 AN12661 - Wi-Fi credential protection

The EdgeLock SE05x allows you to authenticate devices attempting to connect to a Wi-Fi router or wireless LAN network and, in this way, it helps secure access to restricted networks. EdgeLock SE05x supports WPA-PSK and WPA-EAP-TLS security protocols.

In this case, the Wi-Fi module leverages EdgeLock SE05x to safely store the password (in case of WPA-PSK protocol) or the private key and certificate (in case of WPA-EAP-TLS authentication) that are used to establish the secure WiFi connection. During the Wi-Fi connection setup, EdgeLock SE05x is also leveraged to derive the session keys required for data exchange.

The AN12661 describes how to leverage EdgeLock SE05x for Wi-Fi credential protection. It explains how to run a demo setup that showcases the use of EdgeLock SE05x ease-of-use configuration to authenticate devices to a Wi-Fi network based on WPA-EAP-TLS protocol.

5.16 AN12664 - NFC late-stage configuration

The EdgeLock SE05x comes with an integrated, fully ISO/IEC14443 A compliant interface that allows you to perform a secure and convenient late stage parameter configuration of industrial IoT devices already deployed in the field using an NFC reader. As such, EdgeLock SE05x acts like a bridge between the IoT device and the contactless reader.

The AN12664 describe how to leverage EdgeLock SE05x to enable a secure and convenient late-stage parameter configuration of IoT devices in the factory, before shipment, or in the field.

5.17 AN12662 - Binding a host device to EdgeLock SE05x

The EdgeLock SE05x provides manufacturers the option to bind the MCU of the IoT device to the secure element, so that security services offered by EdgeLock SE05x can only be used by that particular MCU.

The AN12662 describes the different stages during the product manufacturing where the binding process can be implemented, depending on the IoT device security requirements and the available MCU

5.18 AN12660 Ease ISA/IEC 62443 compliance with EdgeLock SE05x

The EdgeLock SE05x can support the ISA/IEC 62443, a series of standards which addresses the security of Industrial Automation and Control Systems (IACS) throughout their lifecycle. The AN12660 elaborates on the use of EdgeLock SE05x to reduce the implementation complexity to satisfy the security requirements mandated by the ISA/IEC 62443-4-2 standard.

5.19 AN12448 - Middleware porting guidelines

The EdgeLock SE05x Plug & Trust middleware comes with pre-build support for various NXP MCU / MPU platforms. The AN12448 provides guidelines to port the EdgeLock SE05x Plug & Trust middleware to other platforms. It details the layers and software components that must be adapted to use the EdgeLock SE050 Plug & Trust middleware in your host platform and host operating system.

5.20 AN12663 - TPM functionality

Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys. TPM chips can be used with any major laptop operating system and work best in conjunction with other security technologies such as firewalls, antivirus software, smart cards and biometric verification.

The AN12663 application note describes how to use the EdgeLock SE05x as a Trusted Platform Module (TPM). This document first introduces both the TPM standard and the TPM Software Stack (TSS), how they work and their most important use cases. It

then describes in detail how to take advantage of the EdgeLock SE05x Plug & Trust middleware TSS integration to simplify the usage of EdgeLock SE05x as a TPM.

5.21 UM11225 - NXP EdgeLock SE05x T=1 Over I2C specification

The UM11225 is the specification for the data link layer protocol T=1 over I2C on the EdgeLock SE05x product family.

5.22 AN13539 - OM-SE05xARD board hardware overview

The AN13539 describes the OM-SE05xARD development kits and details how to use its jumpers to configure the different communication options with the EdgeLock SE05x security IC.

5.23 AN12543 - SE05x APDU specification

The AN12543 provides the API description for the IoT applet version 7.xx. The IoT applet version 7.xx is available for the SE050E and SE051 product variants.

5.24 AN12413 - EdgeLock SE050 APDU specification

The AN12413 provides the API description for IoT applet version 3.xx. The IoT applet version 3.xx is available for the SE050A/B/C/D/F product variants.

5.25 AN12514 - SE050A/B/C/D user guidelines

The AN12514 provides the guidelines for the usability of EdgeLock SE050 and the security recommendations for using the security IC.

5.26 AN13483 SE050E - User Guidelines

The AN13483 provides the guidelines for the usability of SE050E and the security recommendations for using the security IC.

5.27 AN13482 SE050F - User Guidelines

The AN13482 provides the guidelines for the usability of SE050F and the security recommendations for using the security IC. This document is available in [Secure Files](#).

5.28 AN12436 - EdgeLock SE050 product configurations

The AN12436 describe the product differences between the EdgeLock SE050 variants and details the credentials injected in each one as part of the EdgeLock SE050 pre-configuration for ease of use.

5.29 AN12730 - EdgeLock SE050 user guidelines

The AN12730 provides the guidelines for the usability of EdgeLock SE051 and the security recommendations for using the security IC.

5.30 AN12973 - EdgeLock SE051 product configurations

The AN12973 describe the product differences between the EdgeLock SE051 variants and details the credentials injected in each one as part of the EdgeLock SE051 pre-configuration for ease of use.

5.31 AN12907 - Secure update of EdgeLock SE051 IoT applet

The EdgeLock SE051 provides advanced applet management capabilities through NXP's Secure Element Management Service Lite (SEMS Lite) feature. SEMS Lite feature allows customers to update the pre-installed IoT applet with the latest security patches and updates offered by NXP.

The AN12907 describes the SEMS Lite service and explains how it can be leveraged, together with the EdgeLock 2GO platform, to update the preloaded EdgeLock SE051 IoT applet.

5.32 AN13015 - How to use EdgeLock SE051 personalization applet

The EdgeLock SE051 is shipped with a pre-installed personalization applet. This personalization applet enables the configuration of EdgeLock SE051 so that OEMs can personalize the configuration of EdgeLock SE051 after the security IC has been manufactured and before it is delivered into the field.

The AN13015 introduces the personalization applet pre-installed in EdgeLock SE051 and describes how it can be used to configure EdgeLock SE051 before the device is delivered into the field and it shows how it can be deleted afterwards with a SEMS Lite script.

6 Legal information

6.1 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.

6.2 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.

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.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out of the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US\$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a 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 or documented vulnerabilities. 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.

6.3 Trademarks

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

Tables

Tab. 1.	EdgeLock SE05x development boards.	4	Tab. 10.	Platform SCP key define prefix for SE050E product variants	19
Tab. 2.	OM-SE050RPI adapter board details	4	Tab. 11.	Platform SCP key define prefix for SE050F product variants	19
Tab. 3.	Evaluation MCU/MPU boards details	5	Tab. 12.	Platform SCP key define prefix for SE050 Previous Generation product variants	19
Tab. 4.	CMake Settings for SE050E product variants	12	Tab. 13.	Platform SCP key define prefix for SE051 product variants	19
Tab. 5.	CMake Settings for SE050F product variants	12	Tab. 14.	Platform SCP key define prefix for A5000 product variants	20
Tab. 6.	CMake Settings for SE050 Previous Generation product variants	12	Tab. 15.	EdgeLock SE05x support documentation	30
Tab. 7.	CMake Settings for SE051 product variants	13			
Tab. 8.	Static SCP03 keys	16			
Tab. 9.	SCP03 session keys	16			

Figures

Fig. 1.	EdgeLock SE05x support package overview	3	Fig. 11.	Select the default Platform SCP keys in <code>sssl_ftr.h</code>	18
Fig. 2.	MCU board SDKs with EdgeLock SE05x examples	6	Fig. 12.	SE050E CMake Settings - PlatformSCP enabled	21
Fig. 3.	Bootable SD Card image for MCIMX8M-EVK	7	Fig. 13.	Verify that <code>se05x_minimal</code> project is running with Platform SCP enabled	22
Fig. 4.	NXP Plug & Trust middleware block diagram	9	Fig. 14.	HTML code documentation	23
Fig. 5.	Download the full multiplatform EdgeLock SE05x Plug & Trust middleware	10	Fig. 15.	EdgeLock SE05x Plug & Trust middleware description	24
Fig. 6.	CMake options	11	Fig. 16.	sssscli documentation	25
Fig. 7.	SE050E CMake Settings - Plain communication	14	Fig. 17.	sssscli usage examples	26
Fig. 8.	SPC03 mutual authentication – principle	17	Fig. 18.	sssscli help	28
Fig. 9.	SPC03 Encryption and MACing principle	17	Fig. 19.	sssscli connect help	29
Fig. 10.	Default Platform SCP keys are defined in <code>ex_sssl_tp_scp03_keys.h</code>	18	Fig. 20.	sssscli se05x help	29
			Fig. 21.	sssscli readidlist example	30

Contents

1	About EdgeLock SE05x Plug & Trust secure element family	3			
2	EdgeLock SE05x development boards	3			
3	Supported MCU/MPU boards	4			
3.1	MIMXRT1070-EVK, MIMXRT1060-EVK, FRDM-K64F and LPC55S69-EVK MCU board examples	6			
3.2	MCIMX8M-EVK board examples	7			
3.3	Raspberry Pi board examples	8			
4	EdgeLock SE05x Plug & Trust middleware	8			
4.1	Full Multiplatform EdgeLock SE05x Plug & Trust middleware	8			
4.1.1	Download the EdgeLock SE05x Plug & Trust middleware	9			
4.1.2	Building and compiling the EdgeLock SE05x Plug & Trust middleware	10			
4.1.2.1	Product specific CMake build settings	11			
4.1.3	Example: SE050E CMake build settings	13			
4.2	Binding EdgeLock SE05x to a host using Platform SCP	15			
4.2.1	Introduction to the Global Platform Secure Channel Protocol 03 (SCP03)	15			
4.2.2	How to configure the product specific default Platform SCP keys	17			
4.2.3	How to enable Platform SCP	20			
4.3	Code documentation	22			
4.4	EdgeLock SE05x ssscli tool	24			
4.4.1	EdgeLock SE05x ssscli tool example	26			
4.4.1.1	List all SE05x secure objects	27			
5	Support documentation	30			
5.1	AN12396 - Quick start guide with Kinetis K64F	31			
5.2	AN13027 - Quick start guide with i.MX 8M	32			
5.3	AN12450 - Quick start guide with i.MX RT1060 and i.MX RT1170	32			
5.4	AN12452 - Quick start guide with LPC55S69	32			
5.5	AN12570 - Quick start guide with Raspberry Pi	32			
5.6	AN12398 - Quick start guide with Visual Studio project examples	32			
5.7	AN12404 - Secure connection to AWS IoT Core	32			
5.8	AN12401 - Secure connection to Google Cloud Platform	33			
5.9	AN12402 - Secure connection to Azure IoT Hub	33			
5.10	AN12403 - Secure connection to IBM Watson IoT	33			
5.11	AN12400 - Secure connection to OEM cloud	33			
5.12	AN12449 - Sensor data protection	33			
5.13	AN12399 - Device-to-device authentication	34			
5.14	AN12569 - Secure access control in Industrial IoT	34			
5.15	AN12661 - Wi-Fi credential protection	34			
5.16	AN12664 - NFC late-stage configuration	35			
5.17	AN12662 - Binding a host device to EdgeLock SE05x	35			
5.18	AN12660 Ease ISA/IEC 62443 compliance with EdgeLock SE05x	35			
5.19	AN12448 - Middleware porting guidelines	35			
5.20	AN12663 - TPM functionality	35			
5.21	UM11225 - NXP EdgeLock SE05x T=1 Over I2C specification	36			
5.22	AN13539 - OM-SE05xARD board hardware overview	36			
5.23	AN12543 - SE05x APDU specification	36			
5.24	AN12413 - EdgeLock SE050 APDU specification	36			
5.25	AN12514 - SE050A/B/C/D user guidelines	36			
5.26	AN13483 SE050E - User Guidelines	36			
5.27	AN13482 SE050F - User Guidelines	36			
5.28	AN12436 - EdgeLock SE050 product configurations	36			
5.29	AN12730 - EdgeLock SE050 user guidelines	36			
5.30	AN12973 - EdgeLock SE051 product configurations	37			
5.31	AN12907 - Secure update of EdgeLock SE051 IoT applet	37			
5.32	AN13015 - How to use EdgeLock SE051 personalization applet	37			
6	Legal information	38			

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