

# AN13256

## Get started with EdgeLock A5000 support package

Rev. 1.1 — 14 September 2022

Application note

### Document information

| Information | Content  |
|-------------|--|
| Keywords    | EdgeLock A5000 Secure Authenticator, Plug & Trust Secure Authenticator   |
| Abstract    | This document is the entry point for getting familiar with EdgeLock A5000 support package contents and how to get started with them. |



## Revision history

---

### Revision history

| Revision number | Date       | Description   |
|-----------------|------------|---|
| 1.0             | 2022-03-22 | Initial version   |
| 1.1             | 2022-09-14 | Add Plug & Trust Mini Package and Plug & Trust Nano Package description in <a href="#">Section 4</a> EdgeLock Plug & Trust middleware.<br>Add note in <a href="#">Section 4.1.4.1</a> EdgeLock A5000 ssscli tool example. |

# 1 About EdgeLock A5000 Secure Authenticator Plug & Trust family

The A5000 Plug & Trust device offers enhanced Common Criteria EAL 6+ based security, for unprecedented protection against the latest attack scenarios. This ready-to-use family of authenticator 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 A5000 includes a complete product support package that simplifies design-in and reduces time to market. The EdgeLock A5000 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.
- The development kit is compatible with i.MX, I.MX RT and Kinetis® MCU boards.

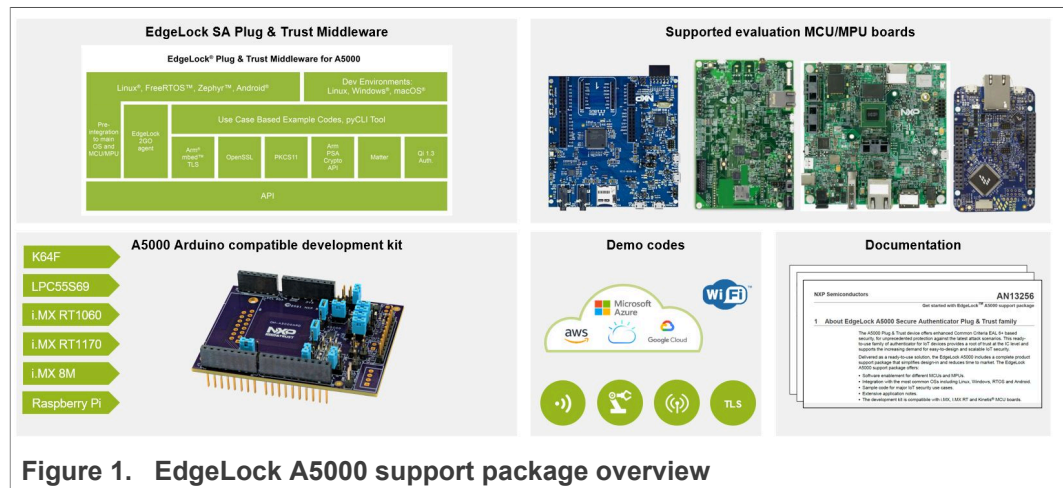


Figure 1. EdgeLock A5000 support package overview

As such, the EdgeLock A5000 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 A5000 support package, organized in the following sections:

- [EdgeLock A5000 development kits.](#)
- [Supported MCU / MPU boards.](#)
- [EdgeLock Plug and Trust middleware.](#)
- [Support documentation.](#)

To implement inclusive language, the terms "master/slave" has been replaced by "controller/target", following the recommendation MIPI.

## 2 EdgeLock A5000 development boards

The EdgeLock A5000 secure authenticator is supported by a development board that can be connected with any MCU board using the compatible Arduino headers or via direct I<sup>2</sup>C connection. [Table 1](#) summarizes the ordering details of the EdgeLock development boards:

Table 1. EdgeLock A5000 development boards.

| Part number                 | 12NC         | Description                               | Picture  |
|-----------------------------|--------------|---|--|
| <a href="#">OM-A5000ARD</a> | 935424319598 | Arduino® compatible development kit       |   |
| <a href="#">OM-SE050RPI</a> | 935379833598 | Raspberry Pi to OMSE050ARD adapter board. |  |

**Note:** You have two options to connect the Raspberry Pi to the OM-A5000ARD 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](#).

### 3 Supported MCU/MPU boards

The EdgeLock A5000 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 (MCU or MPU board). The host controller communicates with EdgeLock A5000 through an I<sup>2</sup>C interface with the host controller being the controller and the EdgeLock A5000 being the target.

[Table 2](#) summarizes the ordering details of the MCU / MPU boards supported by the EdgeLock Plug & Trust middleware:

**Table 2. Evaluation MCU/MPU boards details**

| Part number                    | 12NC         | Description  | Picture   |
|--------------------------------|--------------|--|---|
| <a href="#">FRDM-64F</a>       | 935326293598 | Freedom development platform for Kinetis K64, K63 and K24 MCUs |    |
| <a href="#">MIMXRT1060-EVK</a> | 935368284598 | MIMXRT1060-EVK low cost evaluation kit for Cortex-M7           |   |
| <a href="#">MIMXRT1170-EVK</a> | 935378982598 | MIMXRT1170-EVK low cost evaluation kit for Cortex-M7           |  |
| <a href="#">MCIMX8M-EVK</a>    | 935378743598 | Evaluation Kit for the i.MX 8M Applications Processor          |  |
| <a href="#">LPC55S69-EVK</a>   | 935377412598 | LPCXpresso55S69 Development Board                              |  |

### 3.1 MCUExpresso EdgeLock A5000 examples

The EdgeLock Plug & Trust middleware includes a set of project examples that demonstrate the use of EdgeLock A5000 in the latest Authenticator security use cases.

For MCU based projects the example can be either:

- Imported from the CMake-based build system included in the EdgeLock Plug & Trust middleware package.
- Imported from the MCUXpresso SDKs made available for the [MIMXRT1170-EVK](#), the [MIMXRT1060-EVK](#), the [FRDM-64F](#) and the [LPC55S69-EVK](#) MCU boards.

The CMake-based build system is briefly explained in [Section 4.1.2](#).

For the MIMXRT1170-EVK, the MIMXRT1060-EVK, the FRDM-64F and the 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 A5000 features, and its source code can be re-used for your own implementations. The latest SDK packages can be found in EdgeLock A5000 product website, under the *Tools & Software* tab, as shown in [Figure 2](#).

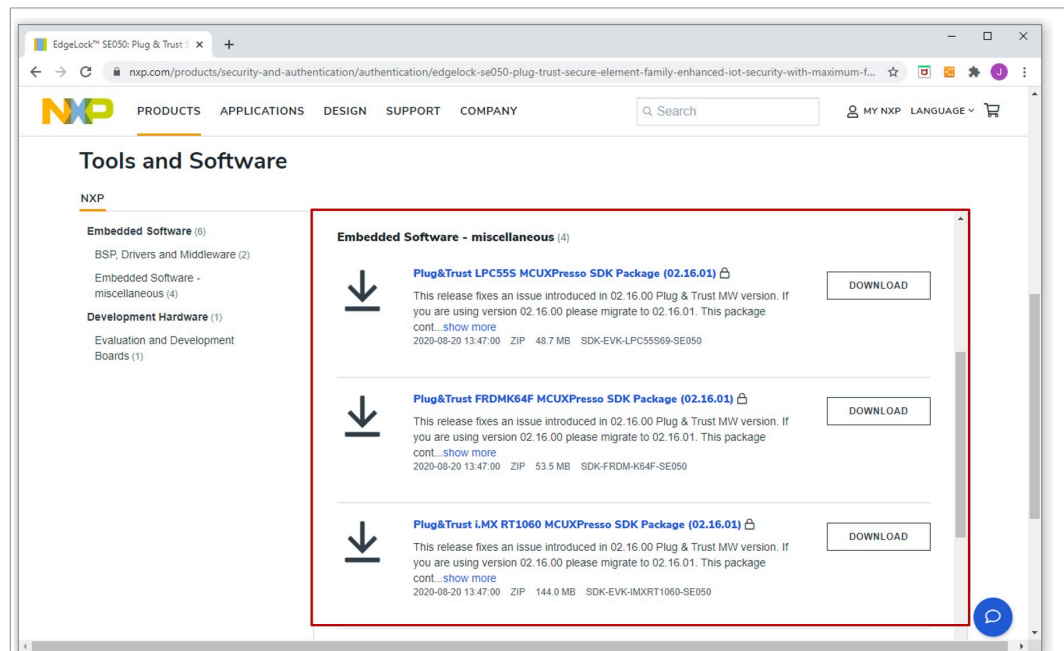


Figure 2. MCU board SDKs with EdgeLock A5000 examples

**Note:** The MCU SDKs can be downloaded also from the MCUXpresso SDK Builder website, but may not include all the EdgeLock A5000 project examples or the latest version of them.

The NXP Plug & Trust middleware supports the A5000 Secure Authenticator and the SE05x Secure Element product family through the SSS and se05x API. [Table 3](#) lists all examples supported by the A5000 Secure Authenticator when using the FRDM-64F MCUXpresso SDK.

Table 3. EdgeLock A5000 FRDM-64F MCUXpresso SDK examples

| Example Name           | Description   |
|------------------------|---|
| se05x_GetInfo          | This project can be used to get A5000/SE05x platform information.   |
| se05x_Minimal          | This is a bare minimum example for A5000/SE05x. This gets the amount of free available memory in byte.  |
| se05x_cloud_aws        | This demo demonstrates connection to AWS IoT Console using pre-provisioned device credentials and publish/subscribe procedure using MQTT.   |
| se05x_cloud_azure      | This demo demonstrates connection to Azure IoT Hub using pre-provisioned device credentials and demonstrates publish/subscribe procedure using MQTT.                                      |
| se05x_cloud_gcp        | This demo demonstrates connection to Google Cloud Platform using pre-provisioned device credentials and demonstrates publish/subscribe procedure using MQTT.                              |
| se05x_cloud_ibm_watson | This demo demonstrates connection to IBM Watson IoT platform using pre-provisioned device credentials and publish/subscribe procedure using MQTT.   |
| se05x_ex_ecc           | This example does an elliptic curve cryptography signing and verify operation.  |
| se05x_ex_hkdf          | This example does an HMAC Key derivation operation based on the info and salt.  |
| se05x_ex_md            | This example does a Message Digest hashing operation.   |
| se05x_symmetric        | This example does a symmetric cryptography AES encryption and decryption operation.   |
| se05x_iot_agent_demo   | This is an example for the EdgeLock 2GO agent.  |
| se05x_vcom             | The vcomSE050 demo application allows the board to be used as a bridge between the PC and the secure module and enables the execution of the config tool and other utilities from the PC. |

The Plug & Trust Middleware uses the feature file `fsl_sss_ftr.h` to select a dedicated EdgeLock product IC and the corresponding Authenticator application or IoT applet. The `fsl_sss_ftr.h` is located in the project `source` folder. To take advantage of EdgeLock A5000 features, it is required to change the following options in the `fsl_sss_ftr.h` header file:

1. Set the `#define SSS_HAVE_APPLET_AUTH` flag to 1 and disable all other applet variants by setting the flags to 0 (see [Figure 3](#)).
2. The authentication application version flag `#define SSS_HAVE_SE05X_VER_07_02` must be set to 1 and all other application version flags must be set to 0 as shown in [Figure 4](#).
3. Re-build the MCU Expresso project so that the settings are applied.

In [Table 5](#) you can find the corresponding application note reference which explains how to get started with EdgeLock Plug & Trust middleware using the [OM-A5000ARD](#) and the [MIMXRT1170-EVK](#), [MIMXRT1060-EVK](#), [FRDM-64F](#) or [LPC55S69-EVK](#) boards. It provides detailed instructions to run projects imported either from the MCU Expresso SDK or the CMake-based build system included in the EdgeLock Plug & Trust middleware.

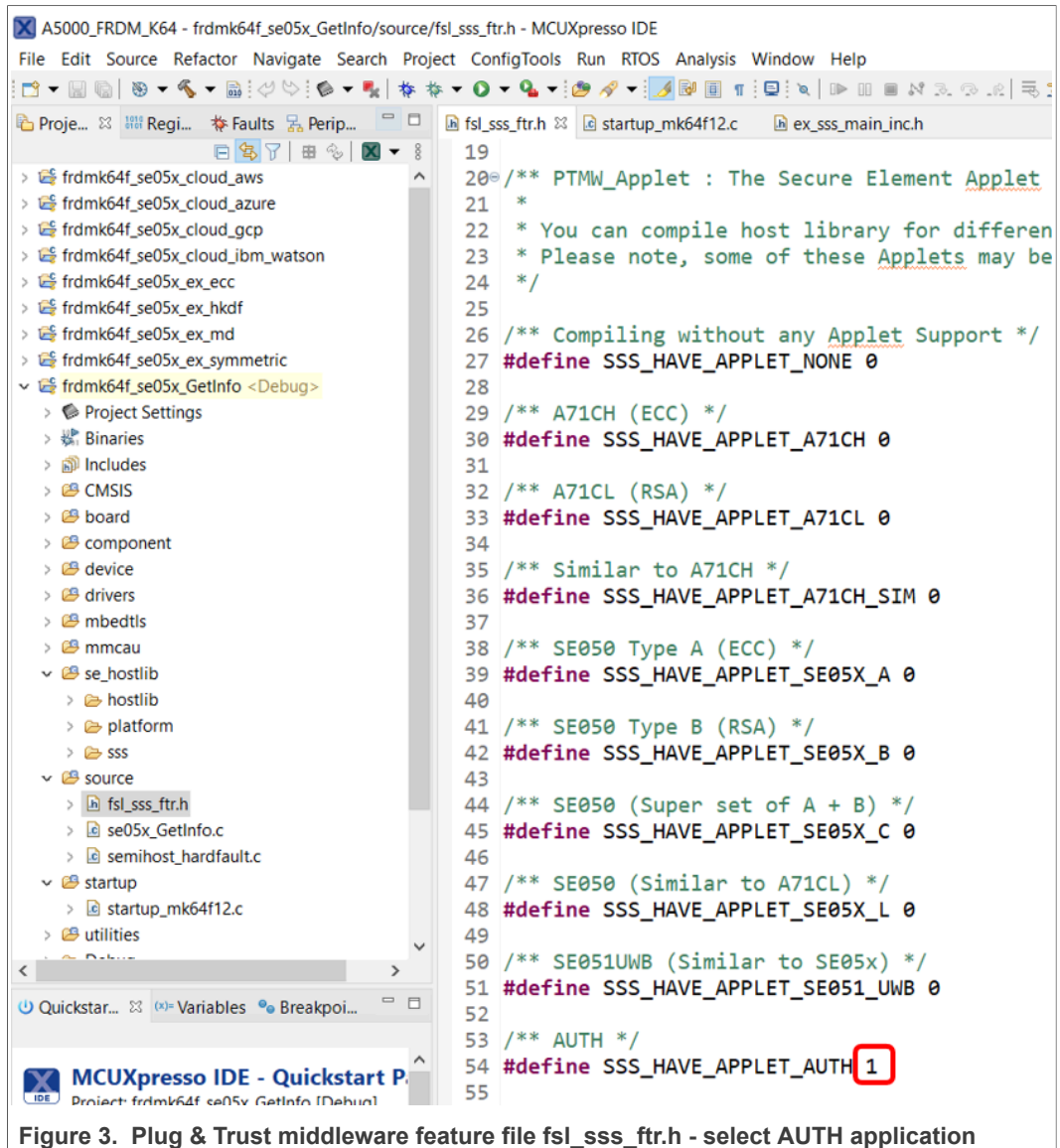
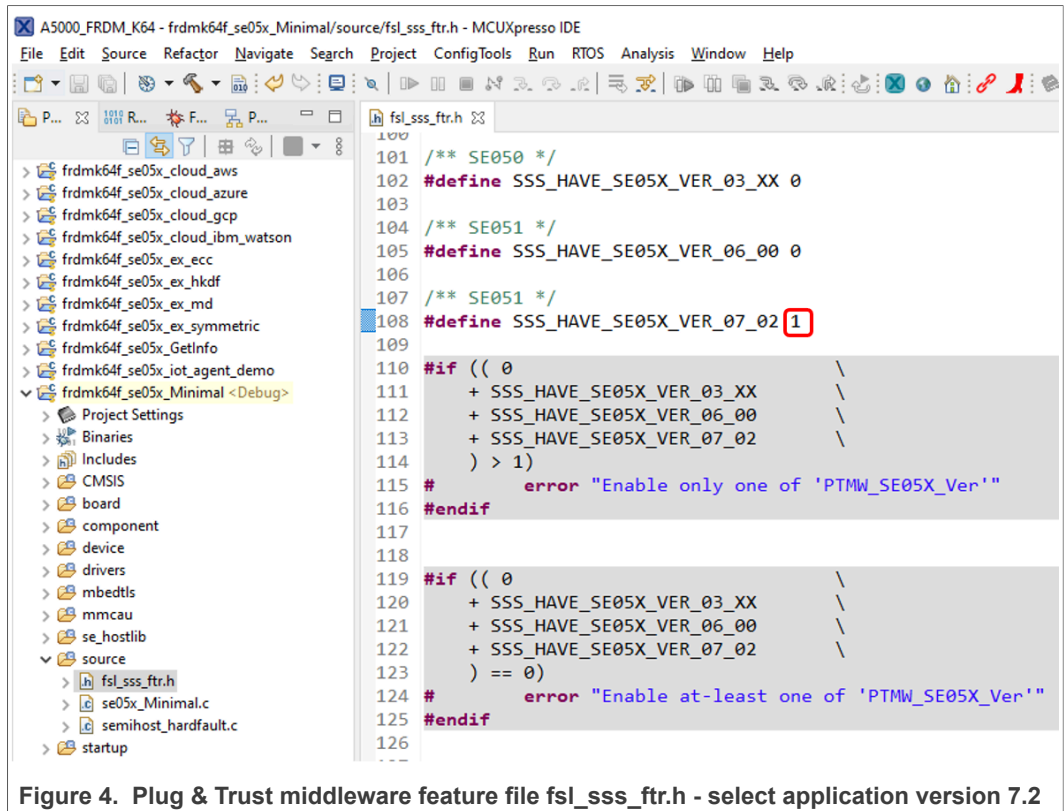


Figure 3. Plug & Trust middleware feature file fsl\_sss\_ftr.h - select AUTH application





### 3.2 MPU EdgeLock A5000 examples

A pre-compiled Linux image with the EdgeLock 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 A5000 features.

**Note:** To take advantage of EdgeLock A5000 features, please select the corresponding CMake options as described in [Section 4.1.2](#) and rebuild the middleware.

The [AN13027](#) explains How to get started with the OM-A5000ARD board and i.MX 8M board.

The latest EdgeLock Plug & Trust middleware software package pre-installed on a bootable SD Card image version can be found in product website, under the [Tools & Software](#) tab, as shown in [Figure 5](#).

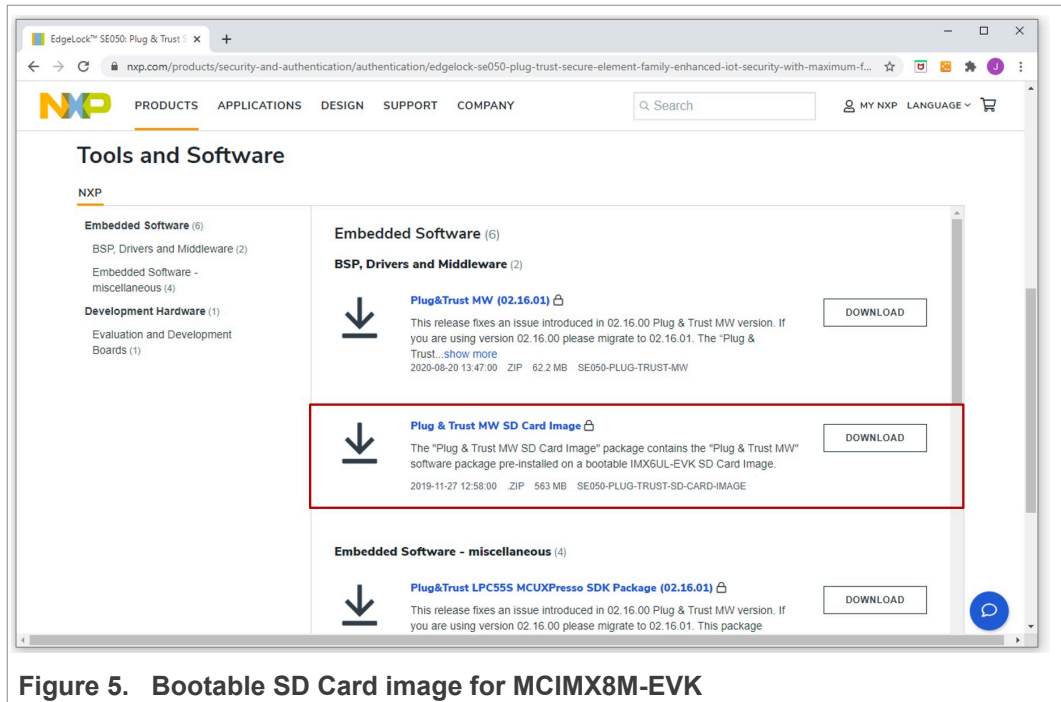


Figure 5. Bootable SD Card image for MCIMX8M-EVK

The [AN12570](#) explains how to get started with the OM-A5000ARD board and the Raspberry Pi board, as a reference for any other device running a Linux distribution.

## 4 EdgeLock 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 EdgeLock Plug & Trust middleware

The Full EdgeLock 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 use 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.

- [Section 3.1](#) describes how to use the MCUExpresso EdgeLock A5000 examples.
- [Section 3.2](#) explain how use pre-compiled Linux image for the [MCIMX8M-EVK](#).

The EdgeLock 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 6](#) is a simplified representation of the layers and components of EdgeLock Plug & Trust middleware:

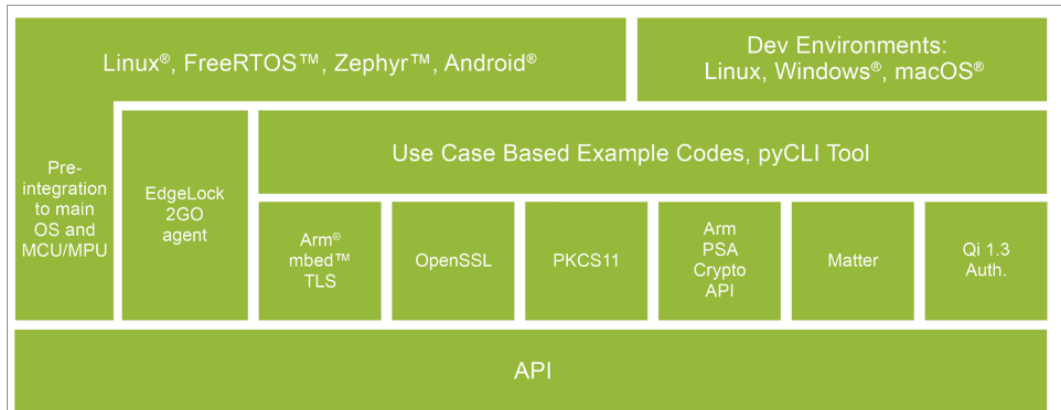


Figure 6. NXP Plug & Trust middleware block diagram

### 4.1.1 Download EdgeLock Plug & Trust middleware

The latest EdgeLock Plug & Trust middleware version can be found in EdgeLock A5000 product website, under the *Tools & Software* tab, as shown in [Figure 7](#)

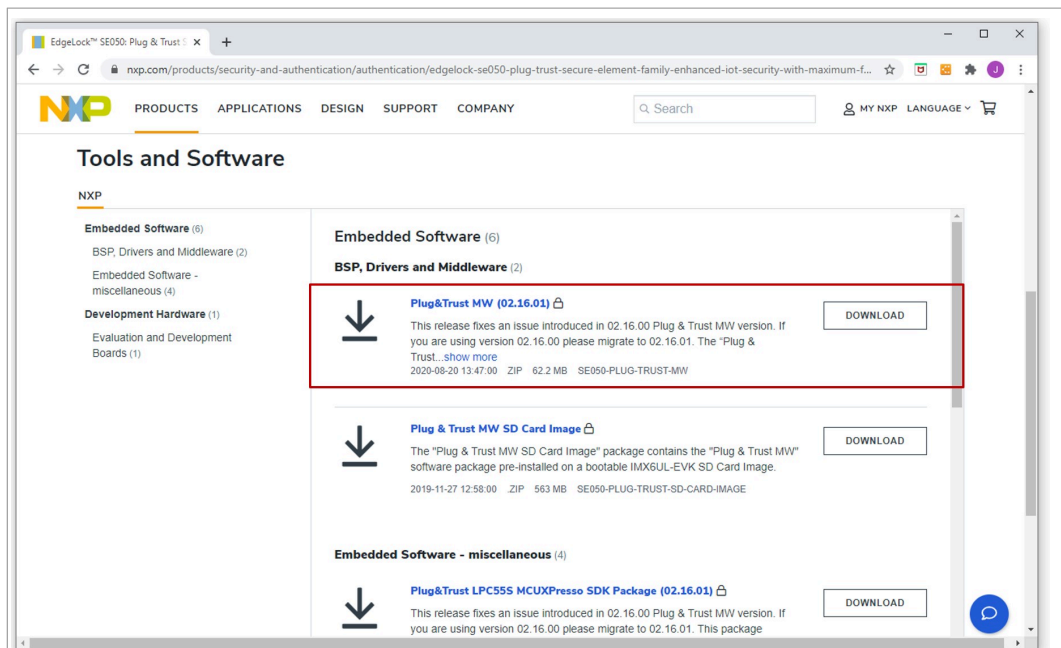


Figure 7. Download EdgeLock Plug & Trust middleware

### 4.1.2 Building and compiling EdgeLock Plug & Trust middleware

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 targets. The CMake files allow developers to build EdgeLock A5000 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 8](#) shows a CMake GUI screenshot with EdgeLock A5000 project settings.

To build the middleware to support the A5000 Secure Authenticator application the following CMake setting needs to be modified before building the middleware:

- Select **AUTH** for the CMake option **PTWM\_Applet**.
- Select **07\_02** for the CMake option **PTWM\_SE05X\_Ver**.
- **Disable** the CMake option **SSSFTR\_SE05X\_RSA**.

The project settings can be specified dynamically using the CMake GUI. The Figure below shows a CMake GUI screenshot with EdgeLock A5000 project settings.

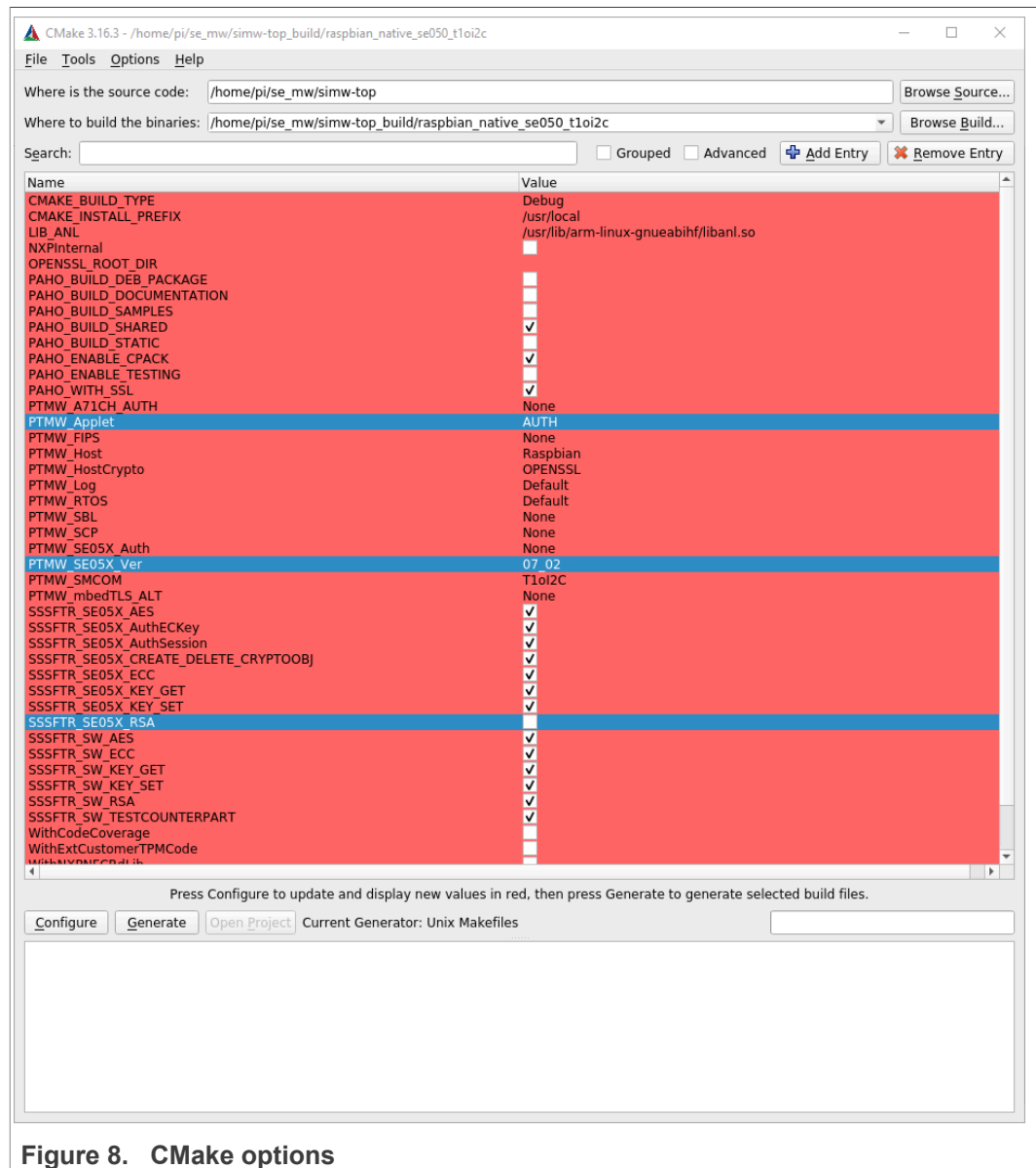


Figure 8. CMake options

4.1.3 Code documentation

The code documentation provided as part of EdgeLock 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 Plug & Trust middleware.
- Instructions to run the `ssscli` tool. See [Section 4.1.4](#) for more details.
- Developer guides to execute the demo and examples.

To open the HTML documentation:

1. Download EdgeLock Plug & Trust middleware as explained in [Section 4](#).
2. Unzip the EdgeLock 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 9](#):

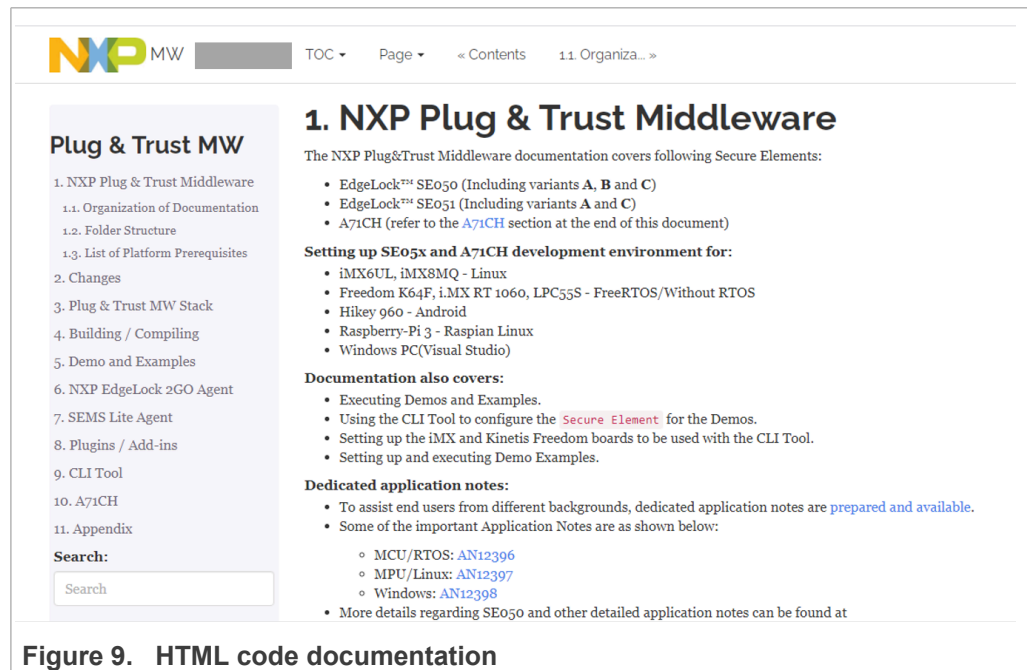


Figure 9. HTML code documentation

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 Plug & Trust middleware description,

click on Section 3. Plug & Trust MW Stack on the left hand side menu as shown in Figure 10:

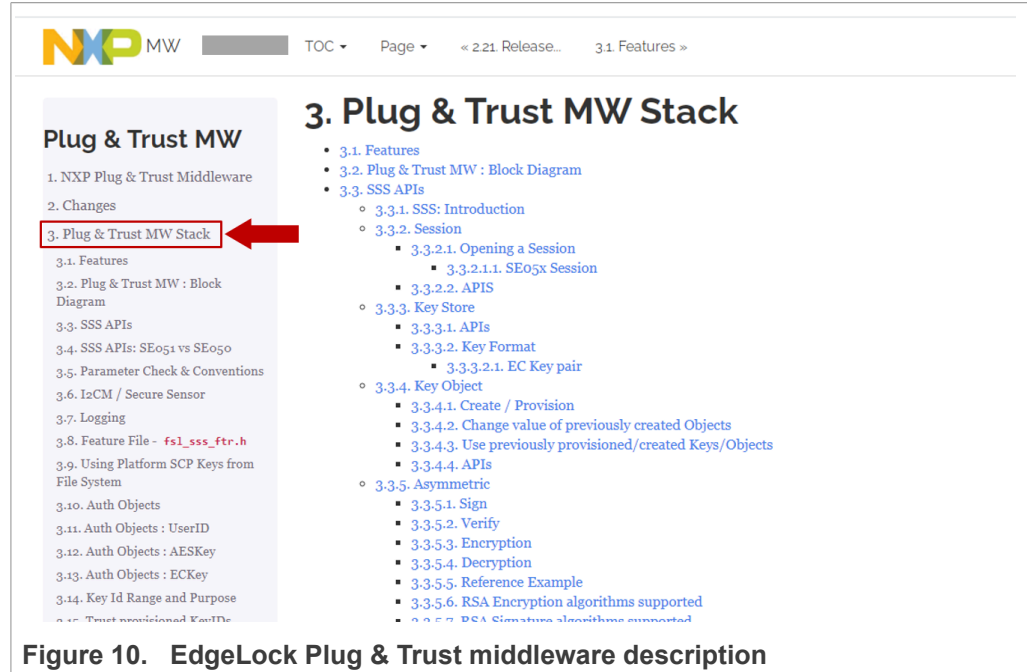


Figure 10. EdgeLock Plug & Trust middleware description

#### 4.1.4 EdgeLock A5000 ssscli tool

The `ssscli` is a command line tool that can be used to send commands to EdgeLock A5000 interactively through the command line. For example, you can use the `ssscli` to create keys and credentials in the EdgeLock A5000 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 A5000
- Attach policies to objects
- List all secure objects
- Retrieve the A5000 device unique ID
- Run some basic operations like sign/verify and encrypt/decrypt operations

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

1. Download EdgeLock Plug & Trust middleware as explained in [Section 4](#).
2. Unzip the EdgeLock 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 11](#)

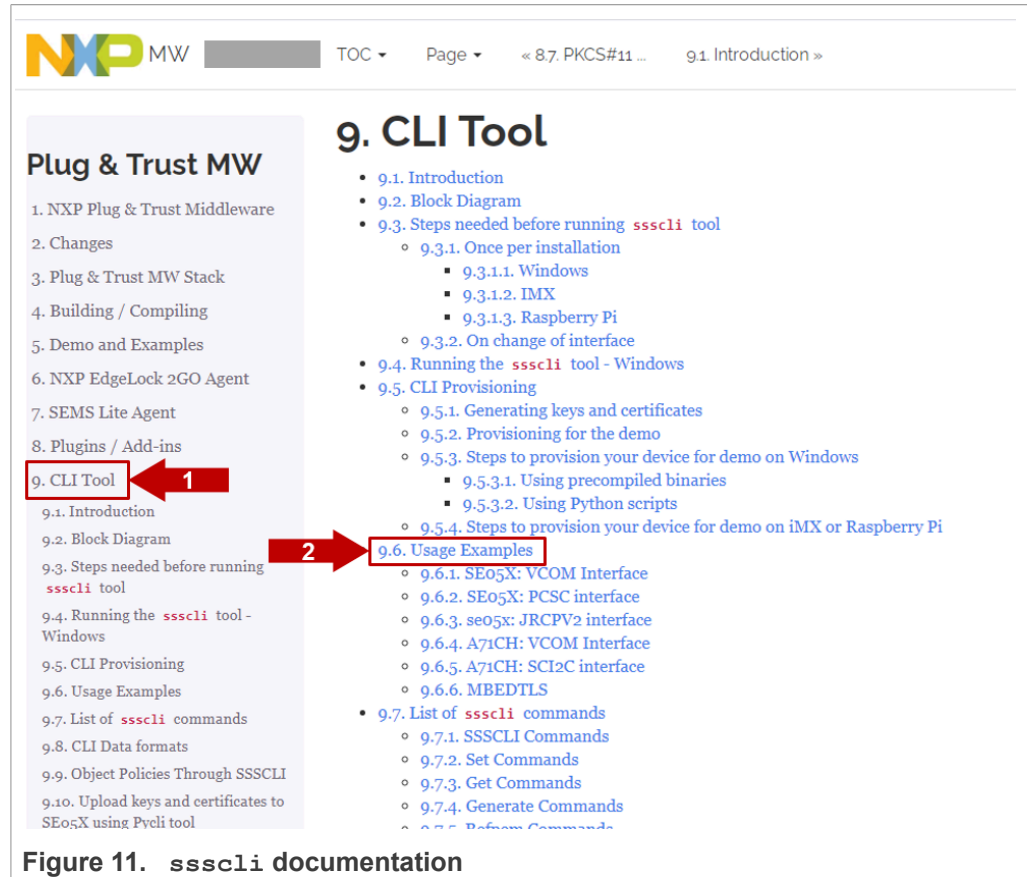


Figure 11. ssscli documentation



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

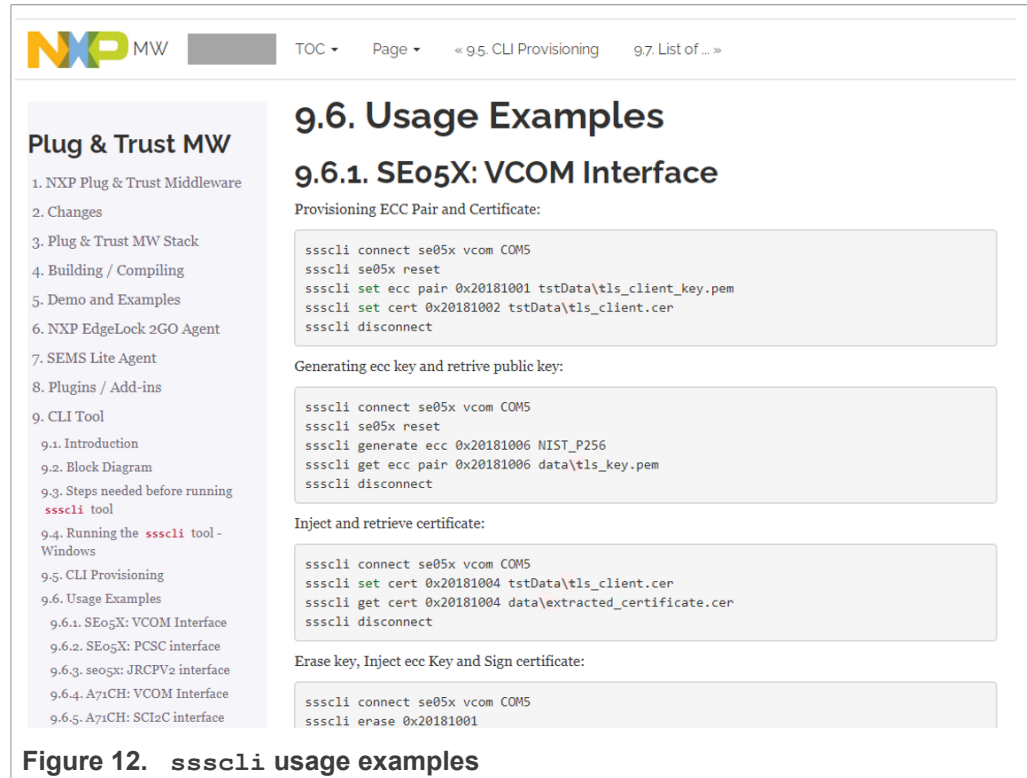


Figure 12. ssscli usage examples

**Note:** The subsystem option *auth* shall be used to open a session using *connect* command. All SE05X specific commands *certuid*, *readidlist*, *reset* and *uid* are supported by EdgeLock A5000.

#### 4.1.4.1 EdgeLock A5000 ssscli tool example

The EdgeLock Plug & Trust middleware includes all components required to verify the EdgeLock A5000 under Windows using the ssscli tool without the need to build the middleware. To be able to connect the A5000-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-64F](#)
- [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 A5000 Secure Authenticator.

This setup also allows to run the A5000 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 5](#) you can find the corresponding application note reference which explains the correct OM-A5000ARD and MCU board connecting. The quick start guides for the MCU boards are also including the correct OM-A5000ARD jumper configuration.

The precompiled VCOM binaries for the MIMXRT1170-EVK, the MIMXRT1060-EVK, the FRDM-64F and the LPC55S69-EVK MCU boards are located in `.\simw-top\binaries\MCU\se05x`. Because the EdgeLock A5000 Secure Authenticator and the SE05x Secure Element family are using the same API one of the following VCOM binaries can be used for the A5000 Secure Authenticator:

- `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 A5000 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`.*

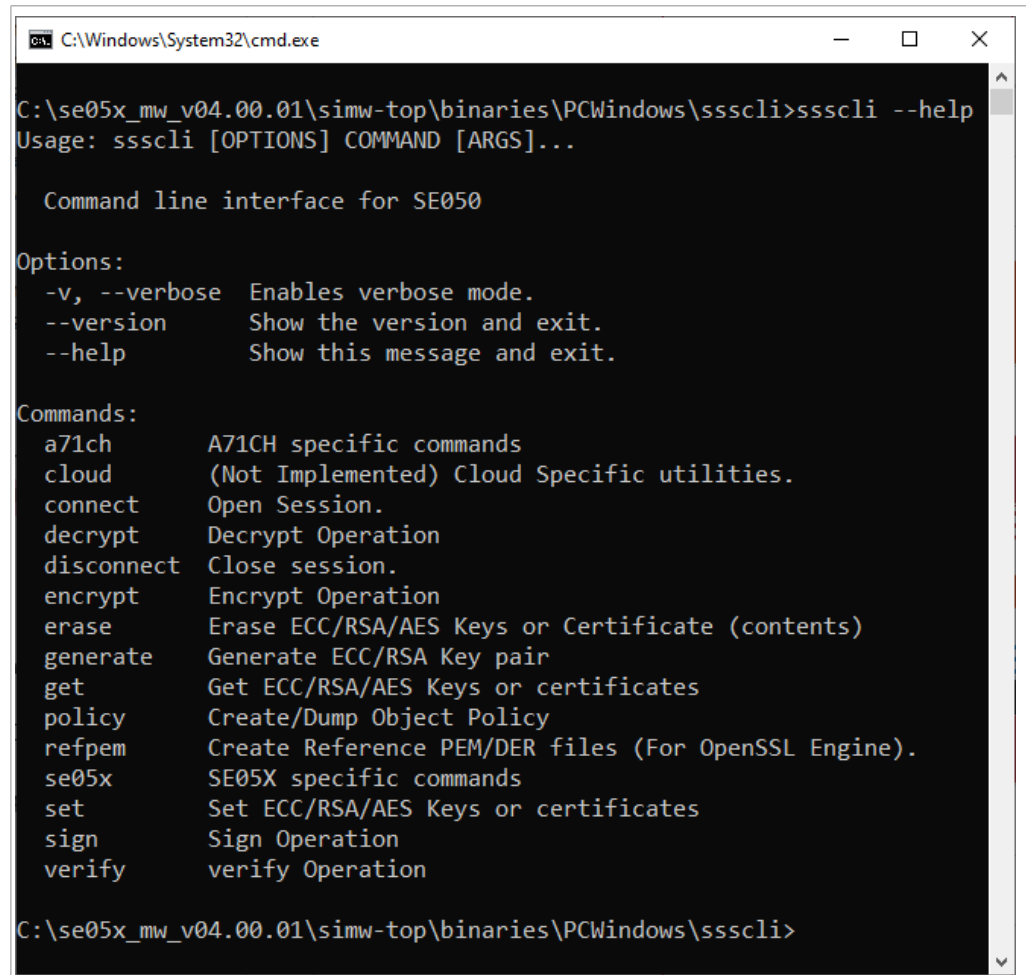
*Alternative you could re-compile the middleware in Windows using the CMake settings as described in [AN12398](#) EdgeLock SE05x Quick start guide with Visual Studio project examples. In the final step you need to copy the new generated `sssapisw.dll` from `.\simw-top\tools` into `.\simw-top\binaries\PCWindows\ssscli`.*

#### 4.1.4.1.1 List all A5000 secure objects

To list all secure objects from EdgeLock A5000 dynamic file system, follow these steps:

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

- 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 13. ssscli help

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

```

C:\Windows\System32\cmd.exe
C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\ssscli>ssscli connect --help
Usage: ssscli 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, jrppv1, jrppv2, 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|ECKey|AESKey|UserID_PlatformSCP|ECKey_PlatformSCP|AESKey_PlatformSCP]
Authentication type. Default is "None". Can
be one of "None, UserID, ECKey, AESKey,
PlatformSCP, UserID_PlatformSCP,
ECKey_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\ssscli>
    
```

Figure 14. ssscli connect help

The EdgeLock A5000 Secure Authenticator supports the same specific commands as the EdgeLock SE05x product variants.

`ssscli se05x --help`

```

C:\Windows\System32\cmd.exe
C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\ssscli>ssscli se05x --help
Usage: ssscli 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)

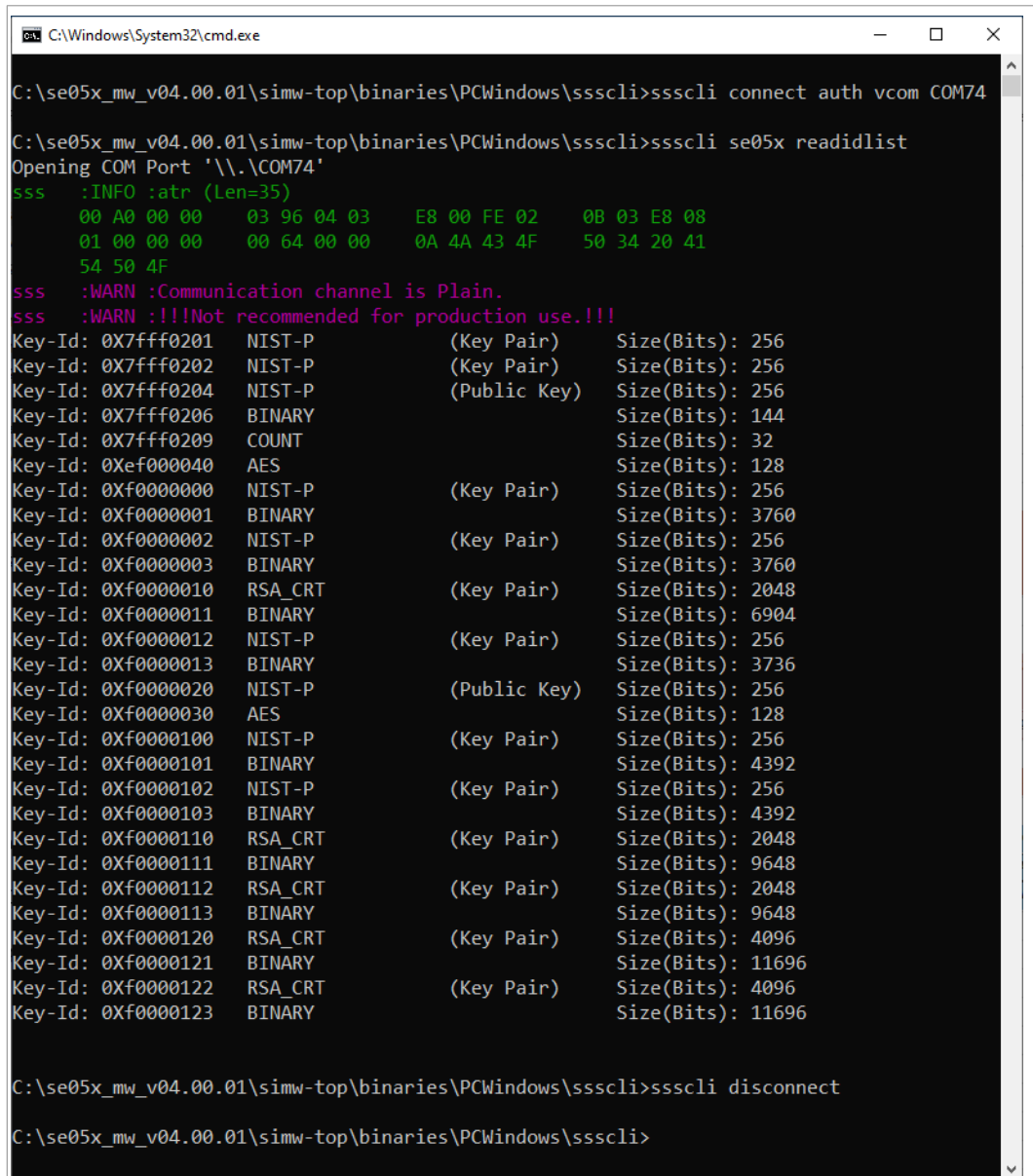
C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\ssscli>
    
```

Figure 15. ssscli se05x help

- Connect to the EdgeLock SE05x using the executable `ssscli.exe`. You need to indicate the VCOM port number corresponding to your MCU VCOM port. The subsystem option `auth` shall be to open a session with the A5000

Secure Authenticator. The following commands will connect to the A5000 Secure Authenticator, list all A5000 secure objects and close the connection.

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



```
C:\Windows\System32\cmd.exe
C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\ssscli>ssscli connect auth vcom COM74
C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\ssscli>ssscli se05x readidlist
Opening COM Port '\\.\COM74'
sss :INFO :atr (Len=35)
      00 A0 00 00   03 96 04 03   E8 00 FE 02   0B 03 E8 08
      01 00 00 00   00 64 00 00   0A 4A 43 4F   50 34 20 41
      54 50 4F
sss :WARN :Communication channel is Plain.
sss :WARN :!!!Not recommended for production use.!!!
Key-Id: 0X7fff0201  NIST-P           (Key Pair)      Size(Bits): 256
Key-Id: 0X7fff0202  NIST-P           (Key Pair)      Size(Bits): 256
Key-Id: 0X7fff0204  NIST-P           (Public Key)    Size(Bits): 256
Key-Id: 0X7fff0206  BINARY          Size(Bits): 144
Key-Id: 0X7fff0209  COUNT           Size(Bits): 32
Key-Id: 0Xef000040  AES             Size(Bits): 128
Key-Id: 0Xf0000000  NIST-P           (Key Pair)      Size(Bits): 256
Key-Id: 0Xf0000001  BINARY          Size(Bits): 3760
Key-Id: 0Xf0000002  NIST-P           (Key Pair)      Size(Bits): 256
Key-Id: 0Xf0000003  BINARY          Size(Bits): 3760
Key-Id: 0Xf0000010  RSA_CRT         (Key Pair)      Size(Bits): 2048
Key-Id: 0Xf0000011  BINARY          Size(Bits): 6904
Key-Id: 0Xf0000012  NIST-P           (Key Pair)      Size(Bits): 256
Key-Id: 0Xf0000013  BINARY          Size(Bits): 3736
Key-Id: 0Xf0000020  NIST-P           (Public Key)    Size(Bits): 256
Key-Id: 0Xf0000030  AES             Size(Bits): 128
Key-Id: 0Xf0000100  NIST-P           (Key Pair)      Size(Bits): 256
Key-Id: 0Xf0000101  BINARY          Size(Bits): 4392
Key-Id: 0Xf0000102  NIST-P           (Key Pair)      Size(Bits): 256
Key-Id: 0Xf0000103  BINARY          Size(Bits): 4392
Key-Id: 0Xf0000110  RSA_CRT         (Key Pair)      Size(Bits): 2048
Key-Id: 0Xf0000111  BINARY          Size(Bits): 9648
Key-Id: 0Xf0000112  RSA_CRT         (Key Pair)      Size(Bits): 2048
Key-Id: 0Xf0000113  BINARY          Size(Bits): 9648
Key-Id: 0Xf0000120  RSA_CRT         (Key Pair)      Size(Bits): 4096
Key-Id: 0Xf0000121  BINARY          Size(Bits): 11696
Key-Id: 0Xf0000122  RSA_CRT         (Key Pair)      Size(Bits): 4096
Key-Id: 0Xf0000123  BINARY          Size(Bits): 11696
C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\ssscli>ssscli disconnect
C:\se05x_mw_v04.00.01\simw-top\binaries\PCWindows\ssscli>
```

Figure 16. ssscli readidlist example

## 5 Support documentation

The EdgeLock A5000 support package includes product documentation and extensive application notes that explain EdgeLock A5000 features, use cases, and how to try out the sample code and demo examples provided in the EdgeLock Plug & Trust middleware.

### 5.1 Dedicated A5000 Documentation

[Table 4](#) summarizes the EdgeLock A5000 dedicated documents.

**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 4. Dedicated EdgeLock A5000 documentation

| Documention              | Title  |
|--------------------------|--|
| <a href="#">DS6676xx</a> | <a href="#">Product Data Sheet</a>   |
| <a href="#">AN13187</a>  | <a href="#">EdgeLock A5000 APDU specification</a>  |
| <a href="#">AN13266</a>  | <a href="#">EdgeLock A5000 user guidelines</a>   |
| <a href="#">AN13501</a>  | <a href="#">EdgeLock A5000 Secure Authenticator for Secure connection to OEM cloud</a>   |
| <a href="#">AN13500</a>  | <a href="#">EdgeLock A5000 Secure Authenticator for electronic anti-counterfeit protection using device-to-device authentication</a> |
| <a href="#">AN13283</a>  | <a href="#">Auth Plug &amp; Trust MW Documentation</a>   |
| <a href="#">AN13541</a>  | <a href="#">OM-A5000 hardware overview</a>   |

#### 5.1.1 DS667610 Product data sheet

The product data sheet describes the features, pre-provisioned ease of use configuration, commercial offering and electrical and pyhysical characteristics.

#### 5.1.2 AN13187 - EdgeLock A5000 APDU specification

The AN12413 provides the EdgeLock A5000 authenticator application APDU interface for customer not using the NXP Plug&Trust middleware. The Plug&Trust middleware abstracts the low level APDU interface and offers high level software APIs.

#### 5.1.3 AN12514 - EdgeLock A5000 user guidelines

The AN12514 provides the guidelines for the usability of EdgeLock A5000 and the security recommendations for using the security IC. This document also includes functional recommendation for wear-out prevention. It also describes the A5000 power saving modes including the corresponding wiring diagrams.

#### 5.1.4 AN13501 - EdgeLock A5000 Secure Authenticator for Secure connection to OEM cloud

The EdgeLock A5000 is designed to provide a tamper-resistant platform to safely store credentials needed for device authentication and registration to public or private clouds.

EdgeLock A5000 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 A5000 to establish a secure connection with the private cloud of an Original Equipment Manufacturer.

**5.1.5 AN13500 - EdgeLock A5000 Secure Authenticator for electronic anti-counterfeit protection using device-to-device authentication**

The EdgeLock A5000 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.

**5.1.6 Auth Plug & Trust MW Documentation**

The Plug&Trust Middleware provides support for the A5000 secure authenticator through the SSS and se05x API. This document gives an overview of the supported SSS and se05x APIs and examples. The document also describes the A5000 dedicated CMake settings.

**5.1.7 OM-A5000 hardware overview**

The AN13541 describes the OM-A5000ARD development kit and details how to use its jumpers to configure the different communication options with the EdgeLock A5000 security IC.

**5.2 Applicable documentation from SE05x Family**

The NXP Plug & Trust middleware supports the EdgeLock A5000 Secure Authenticator and the SE05x Secure Element product family. For many use cases the Plug & Trust middleware abstracts the hardware as well application API and allows to use existing SE05x examples and documentation for the EdgeLock A5000 Secure Authenticator. To take advantage of EdgeLock A5000 features, please select the corresponding CMake options as described in [Section 4.1.2](#).

**5.2.1 Quick start guides for MCU boards**

Table 5. Quick start guides for MCU boards

| App note                | Title   |
|-------------------------|---|
| <a href="#">AN12396</a> | <a href="#">EdgeLock SE05x Quick start guide with Kinetis K64F</a>                |
| <a href="#">AN12450</a> | <a href="#">EdgeLock SE05x Quick start guide with i.MX RT1060 and I.MX RT1170</a> |
| <a href="#">AN12452</a> | <a href="#">EdgeLock SE05x Quick start guide with LPC55S69</a>                    |
| <a href="#">AN12448</a> | <a href="#">EdgeLock SE05x Middleware porting guidelines</a>                      |

**Note:** [Section 3.1](#) describes how to configure the feature file “fsl\_sss\_ftr.h” to select the EdgeLock A5000 device.

**5.2.1.1 AN12396 - EdgeLock SE05x Quick start guide with Kinetis K64F**

The AN12396 explains how to get started with EdgeLock Plug & Trust middleware using the OM-A5000ARD 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 Plug & Trust middleware.

**5.2.1.2 AN12450 - EdgeLock SE05x Quick start guide with i.MX RT1060 and i.MX RT1170**

The AN12450 explains how to get started with EdgeLock Plug & Trust middleware using the OM-A5000ARD and i.MX RT1060 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 Plug & Trust middleware.

**5.2.1.3 AN12452 - EdgeLock SE05x Quick start guide with LPC55S69**

The AN12452 explains how to get started with EdgeLock Plug & Trust middleware using the OM-A5000ARD 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 Plug & Trust middleware.

**5.2.1.4 AN12448 - EdgeLock SE05x Plug & Trust Middleware porting guidelines**

The EdgeLock Plug & Trust middleware comes with pre-build support for various NXP MCU / MPU platforms. The AN12448 provides guidelines to port the EdgeLock 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.

**5.2.2 Quick start guides for Linux platforms**

Table 6. Quick start guides for Linux platforms

| App note                | Title  |
|-------------------------|--|
| <a href="#">AN13027</a> | <a href="#">EdgeLock SE05x Quick start guide with i.MX 8M</a>      |
| <a href="#">AN12570</a> | <a href="#">EdgeLock SE05x Quick start guide with Raspberry Pi</a> |

**Note:** [Section 4.1.2](#) describes the CMake options for the EdgeLock A5000 device.

**5.2.2.1 AN13027 - EdgeLock SE05x Quick start guide with i.MX 8M**

The AN12397 explains how to get started with the OM-A5000ARD board and i.MX 8M board. This guide provides detailed instructions for connecting the boards, installing the software, running the EdgeLock Plug & Trust middleware test examples and executing the ssscli tool.

**5.2.2.2 AN12570 - EdgeLock SE05x Quick start guide with Raspberry Pi**

The AN12570 explains how to get started with the OM-A5000ARD 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 Plug & Trust middleware.

**5.2.3 Quick start for Windows platform**

Table 7. Quick start for Windows platform

| App note                | Title  |
|-------------------------|--|
| <a href="#">AN12398</a> | <a href="#">EdgeLock SE05x Quick start guide with Visual Studio project examples</a> |



**Note:** [Section 4.1.2](#) describes the CMake options for the EdgeLock A5000 device.

**5.2.3.1 AN12398 - EdgeLock SE05x Quick start guide with Visual Studio project examples**

The AN12398 explains how to get started with EdgeLock Plug & Trust middleware using the Visual Studio project examples using FRDM-K64F and OM-A5000ARD boards. It provides detailed instructions to run the Microsoft Visual Studio projects using the CMake-based build system included in the EdgeLock Plug & Trust middleware.

**5.2.4 Quick start guides for cloud connections**

Table 8. Quick start guides for cloud connections

| App note                | Title   |
|-------------------------|---|
| <a href="#">AN12404</a> | <a href="#">EdgeLock SE05x for Secure connection to AWS IoT Core</a>          |
| <a href="#">AN12401</a> | <a href="#">EdgeLock SE05x for Secure connection to Google Cloud Platform</a> |
| <a href="#">AN12402</a> | <a href="#">EdgeLock SE05x for Secure connection to Azure IoT Hub</a>         |
| <a href="#">AN12403</a> | <a href="#">EdgeLock SE05x for Secure connection to IBM Watson IoT</a>        |

**Note:** [Section 4.1.2](#) describes the CMake options for the EdgeLock A5000 device.

**Note:** [Section 3.1](#) describes how to configure the feature file “fsl\_sss\_ftr.h” to select the EdgeLock A5000 device.

**5.2.4.1 AN12404 - EdgeLock SE05x for Secure connection to AWS IoT Core**

The EdgeLock A5000 is designed to provide a tamper-resistant platform to safely store credentials needed for device authentication and registration to public or private clouds. EdgeLock A5000 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 A5000 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-A5000ARD and an FRDM-K64F board.

**5.2.4.2 AN12401 - EdgeLock SE05x for Secure connection to Google Cloud Platform**

The EdgeLock A5000 is designed to provide a tamper-resistant platform to safely store credentials needed for device authentication and registration to public or private clouds. EdgeLock A5000 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 A5000 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-A5000ARD and an FRDM-K64F board.

**5.2.4.3 AN12402 - EdgeLock SE05x for Secure connection to Azure IoT Hub**

The EdgeLock A5000 is designed to provide a tamper-resistant platform to safely store credentials needed for device authentication and registration to public or private clouds. EdgeLock A5000 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 A5000 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-A5000ARD and an i.MX 8M board with a Linux OS.

**5.2.4.4 AN12403 - EdgeLock SE05x for Secure connection to IBM Watson IoT**

The EdgeLock A5000 is designed to provide a tamper-resistant platform to safely store credentials needed for device authentication and registration to public or private clouds. EdgeLock A5000 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 A5000 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.

**5.2.5 Use case examples**

Table 9. Use case examples

| App note                | Title  |
|-------------------------|--|
| <a href="#">AN12661</a> | <a href="#">EdgeLock SE05x for Wi-Fi credential protection</a> |
| <a href="#">AN12662</a> | <a href="#">Binding a host device to EdgeLock SE05x</a>        |

**5.2.5.1 AN12661 - EdgeLock SE05x for Wi-Fi credential protection**

The EdgeLock A5000 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 A5000 supports WPA-PSK and WPA-EAP-TLS security protocols.

In this case, the Wi-Fi module leverages EdgeLock A5000 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 A5000 is also leveraged to derive the session keys required for data exchange.

The AN12661 describes how to leverage EdgeLock A5000 for Wi-Fi credential protection. It explains how to run a demo setup that showcases the use of EdgeLock A5000 ease-of-use configuration to authenticate devices to a Wi-Fi network based on WPA-EAP-TLS protocol.

**5.2.5.2 AN12662 - Binding a host device to EdgeLock SE05x**

The EdgeLock A5000 provides manufacturers the option to bind the MCU of the IoT device to the secure element, so that security services offered by EdgeLock A5000 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

## 5.2.6 Protocol specification

Table 10. EdgeLock A5000 support documentation

| App note                | Title   | Product     |
|-------------------------|---|-------------|
| <a href="#">UM11225</a> | <a href="#">NXP EdgeLock SE05x T=1 Over I2C specification</a> | A5000/SE05x |

### 5.2.6.1 UM11225 - NXP 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 A5000 product family.

## 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.

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

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

## Tables

|         |  |    |          |  |    |
|---------|--|----|----------|--|----|
| Tab. 1. | EdgeLock A5000 development boards. ....                  | 4  | Tab. 6.  | Quick start guides for Linux platforms .....   | 24 |
| Tab. 2. | Evaluation MCU/MPU boards details .....                  | 5  | Tab. 7.  | Quick start for Windows platform .....         | 24 |
| Tab. 3. | EdgeLock A5000 FRDM-64F MCUXpresso<br>SDK examples ..... | 7  | Tab. 8.  | Quick start guides for cloud connections ..... | 25 |
| Tab. 4. | Dedicated EdgeLock A5000 documentation ....              | 22 | Tab. 9.  | Use case examples .....                        | 26 |
| Tab. 5. | Quick start guides for MCU boards .....                  | 23 | Tab. 10. | EdgeLock A5000 support documentation .....     | 27 |

Figures

|         |  |    |          |  |    |
|---------|--|----|----------|--|----|
| Fig. 1. | EdgeLock A5000 support package overview .....  | 3  | Fig. 7.  | Download EdgeLock Plug & Trust middleware .....    | 12 |
| Fig. 2. | MCU board SDKs with EdgeLock A5000 examples .....  | 6  | Fig. 8.  | CMake options .....                                | 13 |
| Fig. 3. | Plug & Trust middleware feature file fsl_ sss_ftr.h - select AUTH application .....        | 8  | Fig. 9.  | HTML code documentation .....                      | 14 |
| Fig. 4. | Plug & Trust middleware feature file fsl_ sss_ftr.h - select application version 7.2 ..... | 9  | Fig. 10. | EdgeLock Plug & Trust middleware description ..... | 15 |
| Fig. 5. | Bootable SD Card image for MCIMX8M-EVK .....   | 10 | Fig. 11. | ssscli documentation .....                         | 16 |
| Fig. 6. | NXP Plug & Trust middleware block diagram .....  | 12 | Fig. 12. | ssscli usage examples .....                        | 17 |
|         |  |    | Fig. 13. | ssscli help .....                                  | 19 |
|         |  |    | Fig. 14. | ssscli connect help .....                          | 20 |
|         |  |    | Fig. 15. | ssscli se05x help .....                            | 20 |
|         |  |    | Fig. 16. | ssscli readidlist example .....                    | 21 |

## Contents

|          |  |           |  |  |
|----------|--|-----------|--|--|
| <b>1</b> | <b>About EdgeLock A5000 Secure Authenticator Plug &amp; Trust family</b>   | <b>3</b>  |  |  |
| <b>2</b> | <b>EdgeLock A5000 development boards</b>   | <b>4</b>  |  |  |
| <b>3</b> | <b>Supported MCU/MPU boards</b>  | <b>5</b>  |  |  |
| 3.1      | MCUExpresso EdgeLock A5000 examples  | 6         |  |  |
| 3.2      | MPU EdgeLock A5000 examples  | 9         |  |  |
| <b>4</b> | <b>EdgeLock Plug &amp; Trust middleware</b>  | <b>11</b> |  |  |
| 4.1      | Full EdgeLock Plug & Trust middleware  | 11        |  |  |
| 4.1.1    | Download EdgeLock Plug & Trust middleware  | 12        |  |  |
| 4.1.2    | Building and compiling EdgeLock Plug & Trust middleware  | 12        |  |  |
| 4.1.3    | Code documentation   | 14        |  |  |
| 4.1.4    | EdgeLock A5000 ssscli tool   | 15        |  |  |
| 4.1.4.1  | EdgeLock A5000 ssscli tool example   | 17        |  |  |
| <b>5</b> | <b>Support documentation</b>   | <b>22</b> |  |  |
| 5.1      | Dedicated A5000 Documentation  | 22        |  |  |
| 5.1.1    | DS667610 Product data sheet  | 22        |  |  |
| 5.1.2    | AN13187 - EdgeLock A5000 APDU specification  | 22        |  |  |
| 5.1.3    | AN12514 - EdgeLock A5000 user guidelines   | 22        |  |  |
| 5.1.4    | AN13501 - EdgeLock A5000 Secure Authenticator for Secure connection to OEM cloud   | 22        |  |  |
| 5.1.5    | AN13500 - EdgeLock A5000 Secure Authenticator for electronic anti-counterfeit protection using device-to-device authentication | 23        |  |  |
| 5.1.6    | Auth Plug & Trust MW Documentation   | 23        |  |  |
| 5.1.7    | OM-A5000 hardware overview   | 23        |  |  |
| 5.2      | Applicable documentation from SE05x Family   | 23        |  |  |
| 5.2.1    | Quick start guides for MCU boards  | 23        |  |  |
| 5.2.1.1  | AN12396 - EdgeLock SE05x Quick start guide with Kinetis K64F   | 23        |  |  |
| 5.2.1.2  | AN12450 - EdgeLock SE05x Quick start guide with i.MX RT1060 and i.MX RT1170  | 24        |  |  |
| 5.2.1.3  | AN12452 - EdgeLock SE05x Quick start guide with LPC55S69   | 24        |  |  |
| 5.2.1.4  | AN12448 - EdgeLock SE05x Plug & Trust Middleware porting guidelines  | 24        |  |  |
| 5.2.2    | Quick start guides for Linux platforms   | 24        |  |  |
| 5.2.2.1  | AN13027 - EdgeLock SE05x Quick start guide with i.MX 8M  | 24        |  |  |
| 5.2.2.2  | AN12570 - EdgeLock SE05x Quick start guide with Raspberry Pi   | 24        |  |  |
| 5.2.3    | Quick start for Windows platform   | 24        |  |  |
| 5.2.3.1  | AN12398 - EdgeLock SE05x Quick start guide with Visual Studio project examples   | 25        |  |  |
| 5.2.4    | Quick start guides for cloud connections   | 25        |  |  |
| 5.2.4.1  | AN12404 - EdgeLock SE05x for Secure connection to AWS IoT Core   | 25        |  |  |
| 5.2.4.2  | AN12401 - EdgeLock SE05x for Secure connection to Google Cloud Platform  | 25        |  |  |
| 5.2.4.3  | AN12402 - EdgeLock SE05x for Secure connection to Azure IoT Hub  | 25        |  |  |
| 5.2.4.4  | AN12403 - EdgeLock SE05x for Secure connection to IBM Watson IoT   | 26        |  |  |
| 5.2.5    | Use case examples  | 26        |  |  |
| 5.2.5.1  | AN12661 - EdgeLock SE05x for Wi-Fi credential protection   | 26        |  |  |
| 5.2.5.2  | AN12662 - Binding a host device to EdgeLock SE05x  | 26        |  |  |
| 5.2.6    | Protocol specification   | 27        |  |  |
| 5.2.6.1  | UM11225 - NXP NXP EdgeLock SE05x T=1 Over I2C specification  | 27        |  |  |
| <b>6</b> | <b>Legal information</b>   | <b>28</b> |  |  |

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