AN13014

Moving from EdgeLock SE050 to EdgeLock SE050E or EdgeLock SE051

Rev. 1.2 — 11 April 2022 Application note

Document information

Information	Content
Keywords	EdgeLock SE050, EdgeLock SE051, Plug & Trust secure element
Abstract	This document describes the steps required to upgrade your IoT solution based on EdgeLock SE050 to the EdgeLock SE050E or EdgeLock SE051, both pre-loaded with the NXP IoT applet.

Revision history

Revision history

Revision number	Date	Description
1.0	2020-10-27	First document release
1.1	2020-12-07	Updated to lates template and fixed broken URLs
1.2	2022-04-11	Cover IoT applet 7.2 as used in EdgeLock SE050E and EdgeLock SE051. Updated comparison table: Table 1, Middleware version and defines: Section 2.3

1 About EdgeLock SE051

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.

The EdgeLock SE051 is a product family extension, further enhancing the unique value of EdgeLock SE050 solution with:

- IoT applet update capabilities.
- IoT applet personalization options.
- Extended suite of cryptographic algorithms.

With respect to the IoT applet update capabilities, 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.

With respect to the IoT applet personalization options, 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 before the device is delivered into the field.

With respect to the extended suite of cryptographic algorithms, the EdgeLock SE050 E and EdgeLock SE051 adds support for AES-GCM (including GMAC) and AES-CCM cryptographic modes of operation and support for Edwards Curve448.

2 Upgrading EdgeLock SE050

This document details the considerations for upgrading a design based on EdgeLock SE050A, B, C, F based on IoT Applet 3.x to EdgeLock SE051 A, C or SE050E solution based on IoT Applet >=7.2. It is organized in the following sections:

1. Hardware integration considerations
2. IoT applet integration considerations
3. EdgeLock SE05x Plug & Trust middleware integration considerations

2.1 Hardware integration considerations

From a hardware perspective, SE050E and EdgeLock SE051 are pin-to-pin and package compatible with EdgeLock SE050A, B, C, F. The EdgeLock SE05x product family uses an HX2QFN20 flat package (SOT1969-1) of 20 pins and dimensions of 3x3 millimeters, as shown in Figure 1.

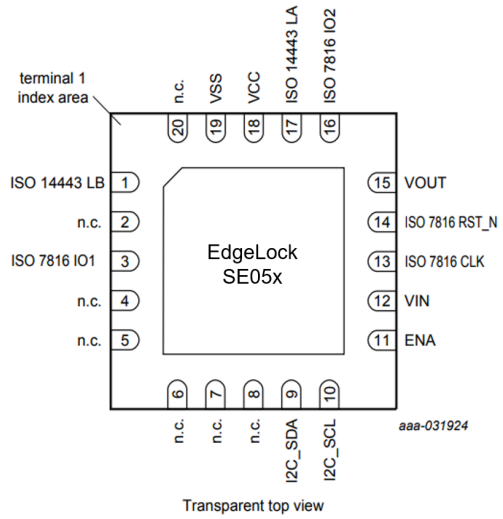

Figure 1. EdgeLock SE05x pinout description

Therefore, there is no need of any hardware adaptation when upgrading an existing design based on EdgeLock SE050A, B, C, F.

The electrical characteristics and I^2C specific timing for SDA/SCL are the same. The default configuration of I^2C clockstretching has differences:

- EdgeLock SE050 A, B, C, F : clockstretching enabled
- EdgeLock SE050E and EdgeLock SE051: clockstretching disabled

This limits the maximum available SCL clock frequency on EdgeLock SE050E and EdgeLock SE051 to 1Mhz (see datasheet section "Supported I2C frequencies". On EdgeLock SE051 this can be changed using the perso applet, see AN13015)

2.2 IoT applet integration considerations

The EdgeLock SE05x is delivered with a pre-installed JavaCard applet, which supports the increasing demand for easy-to-design and scalable IoT security. This pre-installed

IoT applet supports a generic file system allowing you to store keys, manage the credential lifecycle, and perform cryptographic operations in a secure manner, among others.

The IoT applet has been updated and extended to support additional features. Table 1 summarizes the IoT applet functionality changes that you may need to consider if you are upgrading from EdgeLock SE050 A, B, C, F. For more information on the features affected by the changes please refer to the EdgeLock SE051 APDU specification.

Table 1. EdgeLock SE05x IoT applet backward compatibility issues

Feature	SE050 Applet 3.x (SE050 A, B, C, F)	SE051 Applet 7.2 (SE050E, SE051)
ECKey session	The calculation of the master key does not use a counter value (up to applet version 3.6.0).	The calculation of the master key uses a 4-bytes counter value (0x00000001). More details are provided in EdgeLock SE051 APDU specification section "ECKey session". The EdgeLock SE05x Plug & Trust middleware automatically applies this change at runtime.
ECKeySessionGetECKAPublicKey	ECKeySessionGetECKPublicKey and ReadObject possible to read the ECKey public keys	ECKeySessionGetECKAPublicKey removed, ReadObject (with attestation) can be used instead
HKDF	Info length not limited to 80 bytes	Info length limited to 80 bytes
Feature bitmap	2-byte feature bitmap. The feature bitmap allows the user to define which features to enable / disable in the SE.	2-byte feature bitmap + 30 byte extended feature bits. More details are provided in EdgeLock SE051 APDU specification section "Supported applet features".
PCR	PCR gets initialized directly with value as given by the user.	Data gets hashed before it is used for PCR initialization.
TLSCalculatePreMasterSecret	RSA Key exchange and RSA-PSK Key exchange using OAEP padding scheme	RSA Key Exchange and RSA_PSK Key exchange using PKCS#1v1.5 padding scheme. Requires now ALLOW_TLS_PMS on the PSK input
Montgomery curves	It is not needed to use the CreateECCurve APDU before using the curve. Keys are always stored in non volatile memory.	Before using the curve, the CreateECCurve APDU must be called. This avoids writing in non-volatile memory when the external public key is stored in a transient object.
Secure object attributes	No version attribute available.	Version added (not incompatible, but this needs to be considered on attestation).
Secure object attributes	Equal for non-authentication and authentication objects.	Different for authentication and non-authentication objects. Non-authentication objects have a field for the minimum tag length (AEAD mode) and for minimum output length. The curve type will be returned as well on the commands ReadType and ReadObject
Secure Object Attributes "Object Class"	Object Class EC Keys only details if object is public, private or a key pair	Object Class for EC Keys reports curve type and length as well. Used in • ReadType • ReadIDList • ReadObject • ReadAttributes

Table 1. EdgeLock SE05x IoT applet backward compatibility issues*...continued*

Feature	SE050 Applet 3.x (SE050 A, B, C, F)	SE051 Applet 7.2 (SE050E, SE051)
Attestation	Initial Attestation format	Updated Attestation format used on commands • ReadObject • ReadAttributes • I2CMExecuteCommandSet • TriggerSelfTest
ReadAtributes/ReadSize/ReadType:	Does not require ALLOW_READ on secure object	Requires ALLOW_READ on Secure Object
UserID object	Minimum 1 byte (up to applet version 3.4.0).	Minimum 4 bytes.
UserID object	If max attempts is set, it is reported as zero in the object attributes as used for attestation.	If max attempts is set, object attributes will show the maximum number of attempts.
Policies on DESFire	ALLOW_DESFIRE_AUTHENTICATION only	Access rule ALLOW_DESFIRE_AUTHENTICATION is now split into three destinct access rules: • ALLOW_DESFIRE_AUTHENTICATION • ALLOW_DESFIRE_CHANGEKEY • ALLOW_DESFIRE_KDF
Policies on Key Derivation Functions:	ALLOW_KDF only	Access rule ALLOW_KDF split into four destinct access rules: • ALLOW_HKDF • ALLOW_PBKDF • ALLOW_TLS • ALLOW_HKDF The previous value of ALLOW_KDF is now interpreted as ALLOW_HKDF.
Default Policy	DESFire access as well as ALLOW_RFC3394_UNWRAP included in default policy	DESFire access as well as ALLOW_RFC3394_UNWRAP not included in default policy
DESKey secure objects		Cannot be used anymore as target to store the output of these commands: • ECDHGenerateSharedSecret • PBKDF2DeriveKey • DFDiversifyKey • TLSCalculatePreMasterSecret
Error Code on memory full when creating new objects	SW_CONDITIONS_NOT_SATISFIED	SW_FILE_FULL
ECDAASign	Initial API	Modified API
DFChangeKeyPart1/DFChangeKeyPart2	Requires only ALLOW_DESFIRE_AUTHENTICATION	Requires the new access rule POLICY_OBJ_ALLOW_DESFIRE_CHANGEKEY on the key which is to be changed.
DFDiversifyKey	Requires only ALLOW_DESFIRE_AUTHENTICATION	Requires the new access rule POLICY_OBJ_ALLOW_DESFIRE_KDF on the master key which is to be diversified.

In case your existing application based on EdgeLock SE050 A,B,C,F relies on the features listed in Table 1, you may need to revisit your software implementation to accommodate the updated IoT applet features.

2.3 EdgeLock SE05x Plug & Trust middleware integration considerations

The EdgeLock SE05x Plug & Trust middleware is a single software stack designed to facilitate the integration of EdgeLock SE05x product family into your host MCU or MPU software. This middleware has built-in cryptographic and device identity features, abstracts the commands and communication interface exposed by EdgeLock SE05x, and it is directly accessible from stacks like OpenSSL, mbedTLS or other cryptographic libraries. In addition, it includes code examples for implementation of major IoT security use cases.

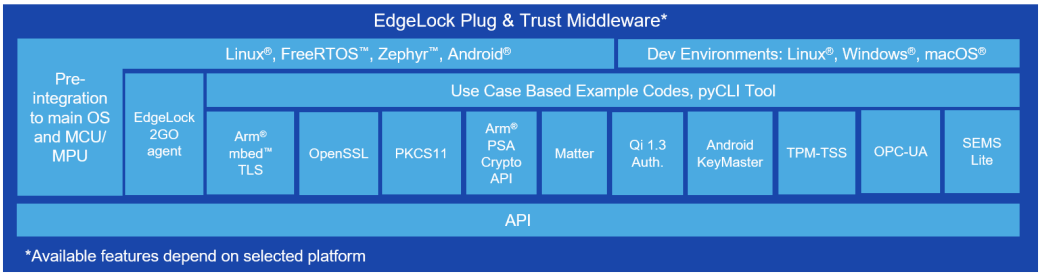

Figure 2. NXP EdgeLock SE05x Plug & Trust middleware block diagram

The EdgeLock SE05x Plug & Trust middleware is delivered with **CMake** files which allows to compile and run the Middleware on different operating systems like:

- MCU
  - Bare-Metal
  - Amazon FreeRTOS
  - Easy porting to other RTOS like Azure RTOS
- MPU
  - embedded Linux
  - Android
  - Windows/Linux PC for evaluation purpose

The EdgeLock Plug & Trust middleware inclusdes a set of project examples that demonstrate the use of Secure Authenticator and Secure Elements for different 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 following NXP MCU demo boards: MIMXRT1170-EVK, MIMXRT1060-EVK, LPC55S69-EVK and FRDM-64F

For **embedded Linux based projects** the examples can be either:

- Imported from the *CMake-based build system* included in the EdgeLock Plug & Trust middleware package.
- A pre-compiled *SD card Linux image* with the EdgeLock Plug & Trust middleware is available for the MCIMX8M-EVK demo board.

If you are upgrading your design from EdgeLock SE050 A, B, C or F, you need to use EdgeLock SE05x Plug & Trust middleware **version 04.01.xx or above** and re-compile the middleware with the compilation flags for the newer version of the IoT applet.

The quick start guides in Table 2 are describing how to compile the EdgeLock SE05x Plug & Trust middleware for different SE05x product variants.

Table 2. EdgeLock SE05x quick start guides for MCU and MPU boards

App note	Title	Product
AN13013	Get started with EdgeLock SE05x support package	SE05x
AN12450	Quick start guide with i.MX RT1060 and guide with i.MX RT1170	SE05x
AN12542	Quick start guide with LPC55S69	SE05x
AN12396	Quick start guide with Kinetis K64F	SE05x
AN12397	Quick start guide with i.MX 8M	SE05x
AN12570	Quick start guide with Raspberry Pi	SE05x
AN12398	EdgeLock SE05x Quick start guide with Visual Studio project examples	SE05x

When re-compiling the EdgeLock SE05x Plug & Trust middleware, not all the examples are built in all the versions. Depending on the configured versions only some examples are built.

Note: *If you are upgrading to a newer version of the EdgeLock SE05x Plug & Trust middleware, make sure to check* `Change log` *section of the EdgeLock SE05x Plug & Trust middleware documentation (*`simw-top/doc/changes/index.html`*) as well.*

3 Legal information

3.1 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.

3.2 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 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.

3.3 Trademarks

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

Tables

Figures

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 11 April 2022