AN14028

Moving from EdgeLock SE050F to EdgeLock SE052F

Rev. 1.0 — 2 April 2024 Application note

Document information

Information	Content
Keywords	EdgeLock SE050, EdgeLock SE052, Plug & Trust secure element
Abstract	This document describes the steps required to upgrade your IoT solution based on EdgeLock SE050F to EdgeLock SE052F

1 About EdgeLock SE052F

The EdgeLock SE052F product 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 SE052F is a product family extension, enhancing the SE050F solution with:

- IoT applet update capabilities
- Extended suite of cryptographic algorithms
- More available memory
- Updated FIPS certification now with FIPS 140-3

Regarding the IoT applet update capabilities, the SE051 and SE052 provides advanced applet management capabilities through Secure Element Management Service Lite (SEMS Lite) feature of NXP. SEMS Lite feature allows customers to update the preinstalled IoT applet with the latest security patches and updates offered by NXP.

2 Upgrading EdgeLock SE050F

This document details the considerations for upgrading a design based on SE050F solution to EdgeLock SE052F. 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, the pad layout of SE052 must be slightly adapted in layout and pin usage. The EdgeLock SE052F uses an HVQFN20 flat package (SOT917-6) of 20 pins and dimensions of 4 mm x 4 mm with a thickness of 0.85 mm. The EdgeLock SE050 product family uses an HX2QFN20 flat package (SOT1969-1) of 20 pins and dimensions of 3 mm x 3 mm, as shown in Figure 1.

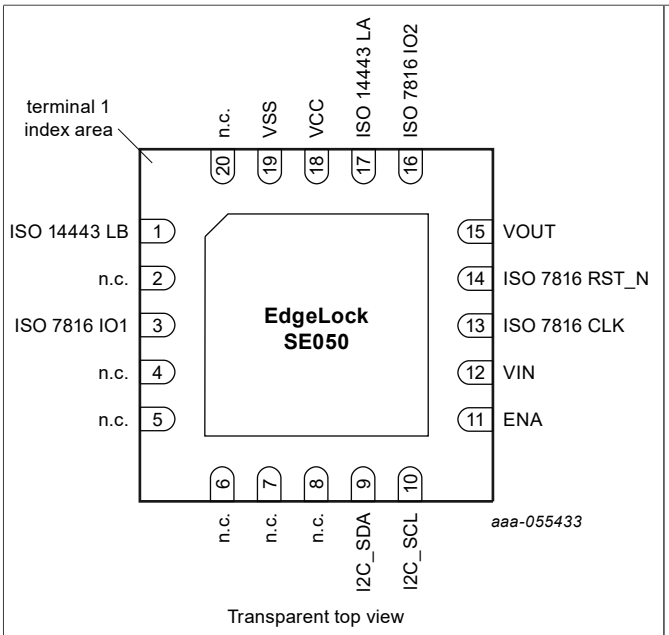

Figure 1. SE050 pinout description

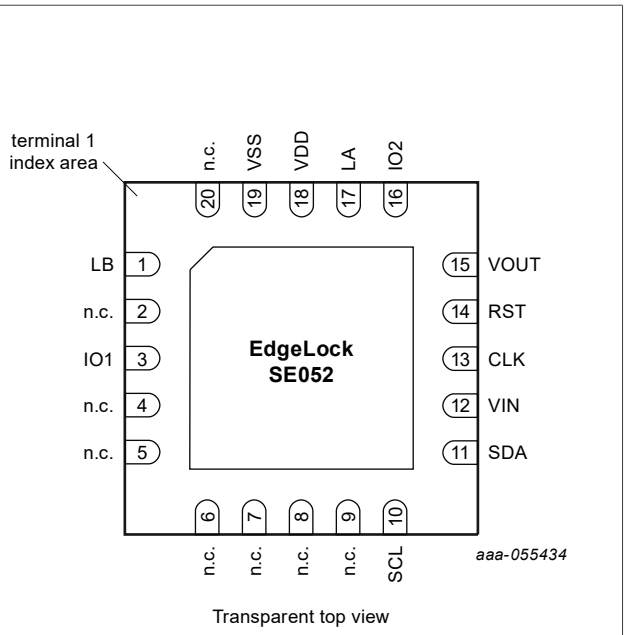

Figure 2. SE052 pinout description

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

- SE050F: clockstretching enabled
- SE052F: clockstretching disabled

This limits the maximum available SCL clock frequency on EdgeLock SE052F to 1 MHz (see data sheet section "Supported I^2C frequencies".

2.1.1 Deep Power Down Configuration

The Deep Power Down feature uses a internal switch between V_{in} and V_{out} to cut power to the core of the IC to be able to turn the IC off to save power. The HW prerequisite for this mode is identical:

The ICs V_{CC}/V_{DD} pin needs to be connected to V_{out} only. In this way the internal switch can turn off power to V_{CC}/V_{DD}.

With EdgeLock SE052F the Deep Power Down mode is not entered via a pin (ENA pin), but instead it can be triggered via an I^2C command. Sending a T1oI2C S-Block with PCB 0xDF triggers this mode. Deep Power Down mode will be entered after the response to this command was fetched and will be left when the IC detects any I^2C read or write request with its target address on the I^2C bus. The IC then boots again and start to process the next command.

2.1.2 Chip Reset

Resetting EdgeLock SE050F with a signal line is done using the Deep Power Down mode with the ENA pin. On EdgeLock SE052F the IC can be reset via pulling down the RST_N pin. The RST_N pin's voltage domain is V_{DD}, so in case of Deep power Down mode used the RST_N high voltage should follow

2.2 IoT applet integration considerations

The EdgeLock SE052F 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 SE050F. For more information on the features affected by the changes please refer to the SE05x IoT Applet APDU specification.

Table 1. EdgeLock SE052F IoT applet backward compatibility issues

Feature	Applet 3.6 (SE050F)	SE051 Applet 7.2.22 (SE052F)
ECKeySessionGet ECKAPublicKey	ECKeySessionGetECKPublicKey and Read Object 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 SE05x IoT Applet 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.
Secure object attributes	No version attribute available.	Version added (not incompatible, but this needs to be considered on attestation).
	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
Attestation	Initial Attestation format	Updated Attestation format used on commands • ReadObject • ReadAttributes • I2CMExecuteCommandSet • TriggerSelfTest
ReadAtributes/Read Size/ReadType:	Does not require ALLOW_READ on secure object	Requires ALLOW_READ on Secure Object
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 Key Derivation Functions:	ALLOW_KDF only	Access rule ALLOW_KDF split into four destinct access rules: • ALLOW_HKDF • ALLOW_PBKDF • ALLOW_TLS • ALLOW_HKDF

Table 1. EdgeLock SE052F IoT applet backward compatibility issues...*continued*

Feature	Applet 3.6 (SE050F)	SE051 Applet 7.2.22 (SE052F)
		The previous value of ALLOW_KDF is now interpreted as ALLOW_HKDF.
Default Policy	ALLOW_RFC3394_UNWRAP included in default policy	ALLOW_RFC3394_UNWRAP not included in default policy
DESKey secure objects	3DES available	Not available
Error Code on memory full when creating new objects	SW_CONDITIONS_NOT_SATISFIED	SW_FILE_FULL
ECDAASign	Available	Not available
GetFreeMemory	Free memory reported as 2 byte field.	Free memory reported as 4 byte field.

In case your existing application based on SE050F relies on the features listed in Table 1, you may need to revisit your software implementation to accommodate the updated IoT applet features.

2.2.1 New features

Comparing SE052F with the predecessor SE050F, these features got added:

- ECDH(E)
- RSA with plain keys and RSA 4k key generation
- AES CCM / GCM (GCM encrypt only wih internal IV generation)
- PBKDF2
- TLS KDF, PSK (additional functions for TLS 1.2 handshake, TLS authentication always supported)

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 SE052F 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 SE052F, 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.

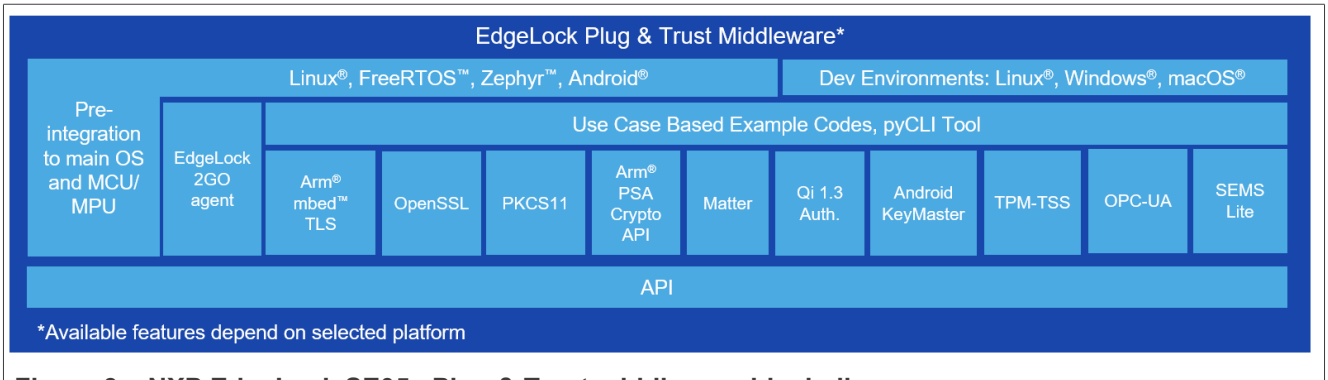

Figure 3. NXP EdgeLock SE05x Plug & Trust middleware block diagram

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 to EdgeLock SE052F, you need to use EdgeLock SE05x Plug & Trust middleware **version 04.05.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. The SE052 is to be compiled with same settings as SE051C. For SE052F variant PlatformSCP is already mandated by FIPS and need to be activated at compilation time.

Table 2. EdgeLock SE052F 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

Table 3. CMake-settings for SE052F

CMake Setting	Required value	Comment
PTMW_Applet	SE05X_C	Include all algorithms in middleware
PTMW_FIPS	None	Setting only required for SE050F to limit example scope, no effect on middleware

Table 3. CMake-settings for SE052F*...continued*

CMake Setting	Required value	Comment
PTMW_SCP	SCP03_SSS	SE050F has PlatformSCP secure channel always on - Include the secure channel in the library
PTMW_Auth	PlatformSCP	Configures the default authentication used by the middleware examples.
PTMW_SE05X_Ver	07_02	Iot Applet version 7.2 used

The SE052F uses like SE050F a mandated PlatformSCP connection. The compiled in default key can be selected in `fsl_sss_ftr.h`. For SE052F set:

```
#define SSS_PFSCP_ENABLE_SE052_B501 1
```

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.

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.

2.3.1 APDU Throughput

The SE052F uses an APDU throughput limitation. In case more than 1 million APDUs are received within 34 days the SE052F will respond with status word 66A6 until the IC gets reset.

The component access manager (starting with MW 04.05.00) which allows multiple applications to access the secure element on Linux based platforms detects this situation and resets the IC automatically using a reset command sent over I2C. This reset clears all transient objects and closes any opened applet level session. They needs to be opened again by the application. Default sessions (sessions without any user level authentication) will only lose the one operation which hits the limit, the next operation will succeed again.

3 Revision history

Table 4. Revision history

Document ID	Release date	Description
AN14028 v.1.0	02 April 2024	• Initial version

Legal information

Definitions

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

Disclaimers

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Trademarks

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

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

Contents

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

Date of release: 2 April 2024
Document identifier: AN14028