AN13483

SE050E - User Guidelines

Rev. 1.2 — 22 August 2022 Application note

Document information

Information	Content
Keywords	Secure element, SE050E, User Guidelines, Plug & Trust, EdgeLock SE050E
Abstract	This document provides the guidelines for the usability and security recommendations for the new generation of SE050 products, SE050E. The guidance is valid for the IoT applet version 7.2.0.

Revision history

Revision history SE050E

Rev	Date	Description
1.2	2022-08-22	• Update Section 7.2.5 • Removed Crypto operations ECDAA
1.1	2022-05-25	• Update Section 4.1
1.0	2022-03-11	Initial version

1 Introduction

This document provides functional and security recommendations for the EdgeLock SE050E Security Module to system integrators and application developers. The recommendations are meant for developing a secure solution when the products is used according to those and under normal conditions.

This document refers to the EdgeLock Ready configuration of SE05x, further on named SE050E, these recommendations also apply to EdgeLock SE05x Custom configurations (see Section 6.2).

A difference will be made between single-tenant use and multi-tenant use:

- **Single-tenant** means the SE050E does not protect credentials separately for different users. No separation of users on SE050E is needed to use any of the credentials.
- **Multi-tenant** means the SE050E separates access to credentials based on a secret (= authentication object). Multi-tenant can be multiple (physical) users, but also multiple different applications or even multiple threads in the same application.

The guidelines in this document for single-tenant are always applicable, both for single-tenant and for multi-tenant use of the SE050E. Guidelines specific to multi-tenant use do not apply to single-tenant use.

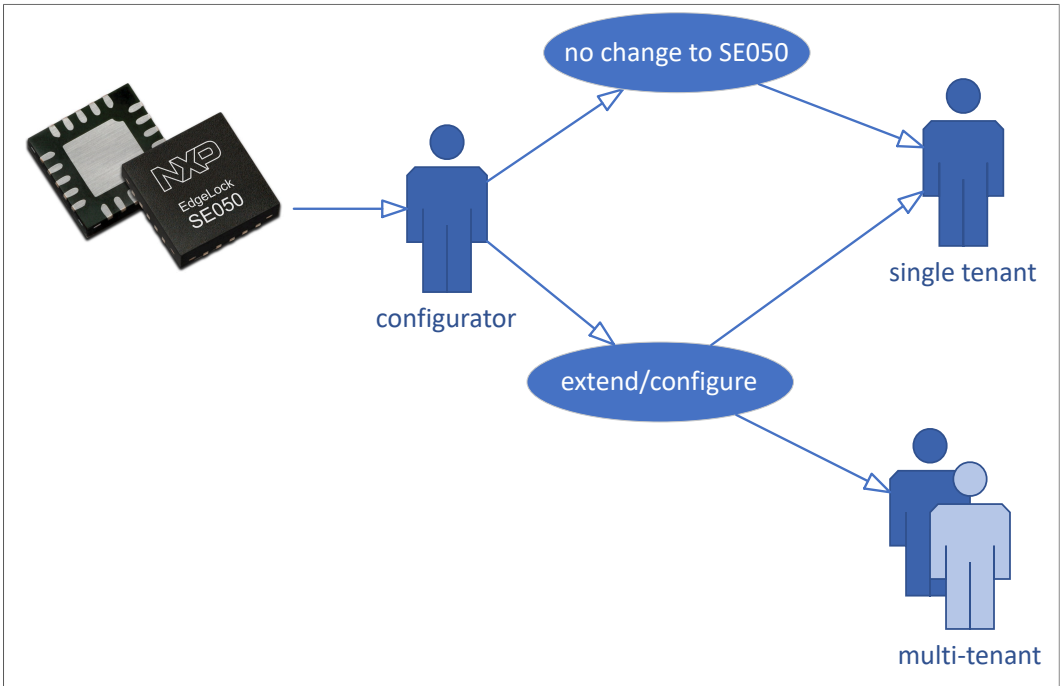

Figure 1. Single- and multi-tenant

The different chapters describe the different possible usages of the SE050E:

- **SE050E basics**
  - Describes the basics of the SE050E: what are Secure Objects and how they can be used.
- **SE050E Plug and Trust: Usage out of the box** (= use as-is as single-tenant)
  - describes how to use the SE050E Security Module straight out of the box, with one single entity using the SE050E. It provides general guidelines on the use cases which are feasible with the product variants off the shelf.

  - **Ease of Use Configuration** describes the generic SE050E variants which will be available in the market ready to plug and trust. These devices come with a specific set of credentials being trust-provisioned by NXP.
  - **Single-tenant Use Cases** provides an explanation of the most simple use cases applicable to the single-tenant usage of SE050E. In this context single-tenant means that the SE050E is operated in a single instance.
- **SE050E Plug and Trust: extendibility** (= configure the SE050E)
  - provides support to those users or system integrators who extend the Ease of Use Configuration with new provisioned credentials. This can apply for single-tenant use (e.g. adding additional credentials besides the Ease Of Use Configuration) or multi-tenant use (e.g. configure the SE050E for use by 2 different end users).
- **SE050E Plug and Trust: multi-tenant usage**
  - describes how to use the SE050E Security Module by multiple entities. It provides general guidelines on the use cases which are feasible with the turnkey product variants.
  - **Module Description Advanced**
    - Secure objects Advanced
    - Policies
    - Object Deletion
  - **Trust Provisioning**
  - **Multi-tenant System**
    - Authenticated Key Creation
    - Multi level SCP
  - **Security Recommendations**
  - **Functional Recommendations**

Note: *For the SE050F FIPS certified module UGM please refer to AN13482, available in Docstore under 7337xx.*

2 SE050E basics

This chapter explains some basics about the SE050E so users can start using the SE050E. It repeats definitions and concepts in a short form as described in the APDU Specification, see: [1].

2.1 Product Information

The SE050E product identification can be obtained out by sending a dedicated command to the secure element.

The Plug & Trust Middleware (nxp.com) includes a utility called ‘se05x_GetInfo’ to retrieve detailed product information from the connected SE050E derivative. It is available as a Windows binary (binaries\ex\VCOM-se05x_GetInfo.exe) and in source code. The html documentation included with the Plug & Trust Middleware package (section ‘Demo & Examples’ > ‘SE05X Get Info example’) provides additional information on using and compiling the utility. To setup the additional hardware required to execute the The Plug & Trust Middleware follow one of the EdgeLock™ SE05x Quick start guides, for example [13].

The information retrieved by se05x_GetInfo is a superset of what is required to determine whether an entry in the errata sheet is applicable to the product.

The exact product identification is covered by two parameters:

- The product OS configuration (Platform build ID) in the format JXXXXXXXXXXXXXXX. Example below : J3R351029B411100
- The version of the Applet in the format xx.xx.xx (major.minor.patch). Example below: 7.2.0

For information on the available features and configuration of the SE050E please refer to [2].

```
App   :INFO :PlugAndTrust_v04.00.01_20211214.0019.2
sss   :INFO :atr (Len=35)
      01 A0 00 00    03 96 04 03    E8 00 FE 02    0B 03 E8 00
      01 00 00 00    00 64 13 88    0A 00 65 53    45 30 35 31
      00 00 00

sss   :INFO :atr (Len=35)
      01 A0 00 00    03 96 04 03    E8 00 FE 02    0B 03 E8 00
      01 00 00 00    00 64 13 88    0A 00 65 53    45 30 35 31
      00 00 00
App
  :WARN :#####################################################
App   :INFO :uid (Len=18)
      04 00 50 01    CF 16 B2 06    12 D2 38 04    2C 02 21 B0
      00 00
App
  :WARN :#####################################################
App   :INFO :Applet Major = 7
App   :INFO :Applet Minor = 2
App   :INFO :Applet patch = 0
App   :INFO :AppletConfig = 3F9F
App   :INFO :With    ECDSA_ECDH_ECDHE
App   :INFO :With    EDDSA
App   :INFO :With    DH_MONT
App   :INFO :With    HMAC
App   :INFO :WithOut RSA_PLAIN
App   :INFO :WithOut RSA_CRT
App   :INFO :With    AES
App   :INFO :With    DES
App   :INFO :With    PBKDF
App   :INFO :With    TLS
App   :INFO :With    MIFARE
App   :INFO :With    I2CM
App   :INFO :Internal = FFFF
App
  :WARN :#####################################################
App   :INFO :Tag value - proprietary data 0xFE = 0xFE
App   :INFO :Length of following data 0x45 = 0x45
App   :INFO :Tag card identification data (Len=2)
      DF 28
App   :INFO :Length of card identification data = 0x42
App   :INFO :Tag configuration ID (Must be 0x01) = 0x01
App   :INFO :Configuration ID (Len=12)
      00 01 A9 21    89 0A 6F 56    4A 23 9C 41
App   :INFO :OEF ID (Len=2)
      A9 21
App   :INFO :Tag patch ID (Must be 0x02) = 0x02
App   :INFO :Patch ID (Len=8)
      00 00 00 00    00 00 00 01
App   :INFO :Tag platform build ID1 (Must be 0x03) = 0x03
```

```
App   :INFO :Platform build ID (Len=24)
      4A 33 52 33    35 31 30 32    39 42 34 31    31 31 30 30
      1A 08 FA 50    67 B5 F2 56
App   :INFO :JCOP Platform ID = J3R351029B411100
App   :INFO :Tag FIPS mode (Must be 0x05) = 0x05
App   :INFO :FIPS mode var = 0x00
App   :INFO :Tag pre-perso state (Must be 0x07) = 0x07
App   :INFO :Bit mask of pre-perso state var = 0x00
App   :INFO :Tag ROM ID (Must be 0x08) = 0x08
App   :INFO :ROM ID (Len=8)
      2E 5A D8 84    09 C9 BA DB
App   :INFO :Status Word (SW) (Len=2)
      90 00
App   :INFO :se05x_GetInfoPlainApplet Example Success !!!...
App
  :WARN :#####################################################
App   :INFO :cplc_data.IC_fabricator (Len=2)
      47 90
App   :INFO :cplc_data.IC_type1 (Len=2)
      D3 21
App   :INFO :cplc_data.Operating_system_identifier (Len=2)
      47 00
App   :INFO :cplc_data.Operating_system_release_date (Len=2)
      00 00
App   :INFO :cplc_data.Operating_system_release_level (Len=2)
      00 00
App   :INFO :cplc_data.IC_fabrication_date (Len=2)
      13 26
App   :INFO :cplc_data.IC_Serial_number (Len=4)
      00 00 08 95
App   :INFO :cplc_data.IC_Batch_identifier (Len=2)
      58 63
App   :INFO :cplc_data.IC_module_fabricator (Len=2)
      00 00
App   :INFO :cplc_data.IC_module_packaging_date (Len=2)
      00 00
App   :INFO :cplc_data.ICC_manufacturer (Len=2)
      00 00
App   :INFO :cplc_data.IC_embedding_date (Len=2)
      00 00
App   :INFO :cplc_data.IC_OS_initializer (Len=2)
      01 2C
App   :INFO :cplc_data.IC_OS_initialization_date (Len=2)
      02 30
App   :INFO :cplc_data.IC_OS_initialization_equipment (Len=4)
      30 30 30 38
App   :INFO :cplc_data.IC_personalizer (Len=2)
      00 00
App   :INFO :cplc_data.IC_personalization_date (Len=2)
      00 00
App   :INFO :cplc_data.IC_personalization_equipment_ID (Len=4)
      00 00 00 00
App   :INFO :cplc_data.SW (Len=2)
      90 00
App   :INFO :ex_sss Finished
```

2.2 Unauthenticated user

For any single-tenant use case, the user can use the SE050E functionality without authentication when both conditions are met:

- there is no interaction between (multiple) users
- no access control is needed to protect credentials against other users.

2.3 Platform SCP

By default, any delivered SE050E device has a SCP03 base key set that contains the same keys for each device-type per OEF (non-die-individual, keys for device types specified in: [2]). For the intended usage and details of the cryptographic keys used with Platform SCP please refer to [10].

Users who want to protect the communication between a host processor and the secure element can use SCP03 on platform level. This secure channel including the key management to update the base keys can be fully managed by GlobalPlatform commands and does not need any SE050E specific command.

2.4 Unbound user

Regardless of the authentication on platform level, the user will not apply any authentication to the applet. This is referred to as an ***unbound*** user. Section "Sessions" will detail *bound* users.

2.5 Secure Objects

Anything that is stored or generated inside the SE050E is a Secure Object.

2.5.1 Secure Object types

Supported Secure Object types are:

- **Keys**
  - ECKey = asymmetric key on any of the supported elliptic curves
  - RSAKey = asymmetric key for RSA (raw or CRT format) of 512, 1024, 1152, 2048, 3078 or 4096 bit
  - AESKey = symmetric key of 128, 192 or 256 bit; used for AES cipher operations
  - DESKey = symmetric key of 8, 16 or 24 byte; used for DES operations
  - HMACKey = symmetric key of 1 byte up to 256 byte length; used for HMAC and HKDF operations.
- **Files**
  - BinaryFile = a byte array (i.e. general purpose storage)
  - Counter = a monotonic counter
  - PCR = a hash value that can be extended with extra data
  - UserID = user identification string with the length of 4 to 16 bytes that can be used to group secure objects and allow their usage in an associated session (intended for use cases where a trusted operating system on a host MCU/MPU is isolating their applications based e.g. on their application ID).

See the [1] for more information.

2.5.2 Secure Object Attributes

Secure Object attributes are linked to any Secure Object. The attributes are:

- *Object identifier* = a unique identifier of the Secure Object
- *Type* = Secure Object type
- *Policy* = Access control applicable to the secure object
- *Origin* = Origin of the data, either external, internal or provisioned
- Additional attributes (only applies to multi-tenant; see Section 5)
  - *Authentication attribute*
  - *Object counter*
  - *Authentication object identifier*
  - *Maximum authentication attempts*
  - *Minimum output length*
  - *Minimum tag length for AEAD operations*

2.5.2.1 Object identifier

The object identifier cannot be modified during the object lifetime, so it remains the same until the object is deleted.

Object identifiers are always defined externally, the SE050E will not (automatically) assign object identifiers to objects. However, there is a set of reserved identifiers that are assigned to serve specific use cases. For more information, refer to [1] and [2].

All pre-provisioned credentials being trust-provisioned by NXP as part of the Ease Of Use Configuration have an identifier from the range “applet Reserved Area” or “NXP reserved region” in Table 1. Customers that will create their own Secure Objects are advised to use an identifier from the range “In field usage”.

Table 1. Identifier for applet reserved area or NXP reserved region

Address Range	IDs
0x00000000-0x7BFFFFFF	In field usage
0x7C000000-0x7CFFFFFF	Android Key Master area
0x7D000000-0x7DFFFFFF	Demo area
0x7FFF0000-0x7FFFFFFF	applet reserved area
0x80000000-0xFFFFFFFF	NXP reserved area

2.5.2.2 Type

See Secure object types.

2.5.2.3 Policy

A Secure Object policy defines the access control to a Secure Object by specifying the operations that each user can perform.

For access control the user must set the policy according to the use case of their system (see section Secure Object policy). For any Secure Object the minimum access control policy for each user has to be set up.

If no explicit policy is passed to a Secure Object at object creation, a default policy will apply as specified in [1] and accroding to the features available on the SE050E variant as described in [2].

Secure Object policies are assigned at object creation and cannot change afterwards, so they remain constant over the lifetime of a Secure Object.

2.5.2.4 Origin

The origin attribute indicates the origin of the content of a Secure Object: either externally generated, internally generated or if trust provisioned by NXP.

3 SE050E Plug and Trust: Usage out of the box

3.1 Ease of Use Configuration

All generic SE050E variants will be offered pre-provisioned according to a profile.

The variants currently available are: E, F

For more details, refer to [2].

Note: *For the SE050F FIPS certified module UGM please refer to AN13482, available in Docstore under 7337xx.*

3.2 Single-tenant protection

The configurator is responsible to bring the SE050E in a usable state for the end user's application.

The configurator and end user might be the same entity, e.g. a developer for prototyping purpose.

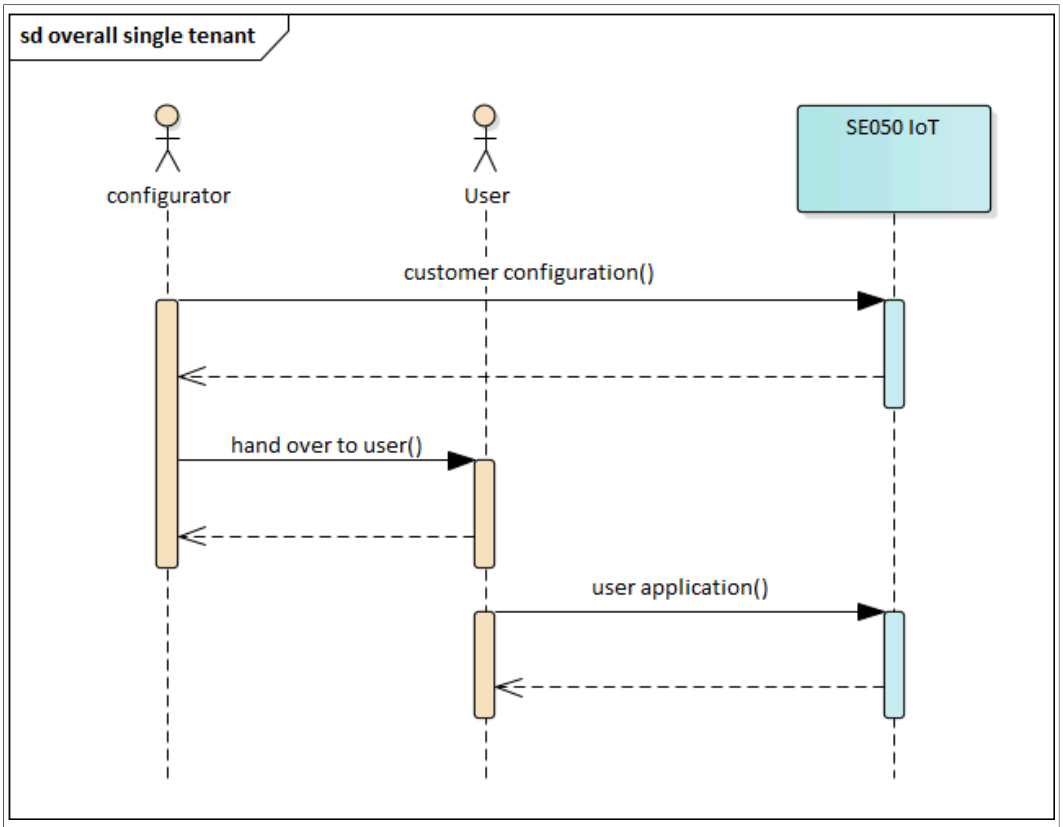

Figure 2. Overview single-tenant use

Note:

Configurator and User can be the same entity

3.3 How to update Platform SCP keys

The Platform default keys are available in [2].

SCP03 base keys can be updated as described in [10], using the existing DEK key as encryption key for the new keys to be set.

The Plug&Trust Middleware contains an example program to rotate (i.e. update) the Platform SCP03 keys.

The example program – and additional documentation - can be found in the demo folder.

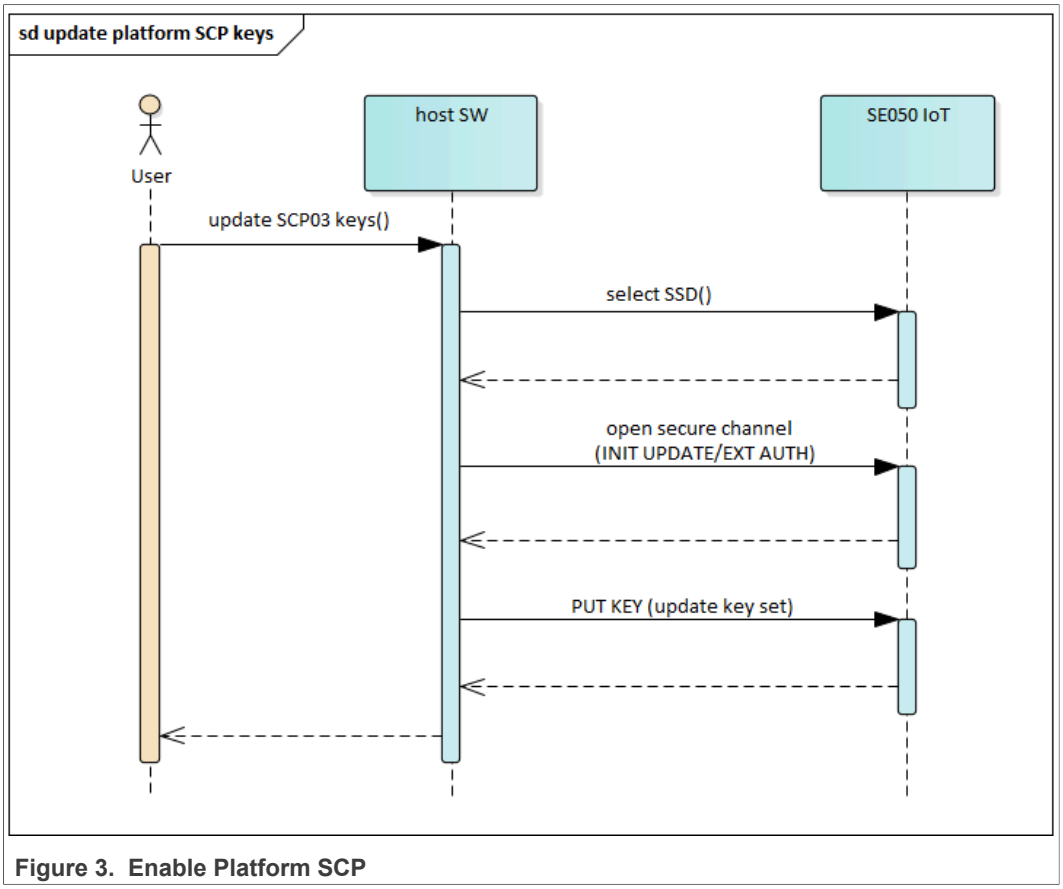

Figure 3. Enable Platform SCP

3.4 Attestation

Attestation is a means to prove that the data is within the secure element and for the case of attesting an I2C Controller response, that the data is from the attached I2C bus. The secure element “attests” the origin of the data by signing it with a trust provisioned attestation key by NXP. When key or file data are requested by the user, the user can request attestation for the returned data. Attestation is achieved by adding into the response of the requested data the chip unique identifier + freshness (i.e. a random value) + a timestamp (i.e. monotonic counter value) + a signature over the full payload (requested data + unique identifier + freshness + timestamp).

All the generic SE050 variants have an attestation key trust provisioned by NXP. Some of the SE050 variants also contain an NXP signed certificate associated to the attestation key. For more details on the configuration profiles of the SE050E refer to [2].

The certificate is signed by NXP Root of Trust entity. Attestation requires trust which is ensured by the issued certificate. To verify the validity of the attestation, the signature on the attested object is checked against the attestation certificate.

Security recommendations on attestation are detailed in Attestation”.

Use cases

1. Generated Key attestation
   SE050E can generate keys internally. The attestation mechanism is used to attest that the keys have been generated inside the SE050E.
2. External Data attestation

Customer might inject/provision data inside the SE050E. The attestation mechanism can be used to prove that the data has been stored in the secure element without modification.

For more information, see Attestation of provisioned objects.

4 SE050E configuration extendibility

This chapter provides information to those users and customers who desire to extend the SE050E product or a custom EdgeLock variant with customized keys and credentials besides the Ease Of Use configuration.

Security recommendations for extending SE050E Ease of Use configuration are provided in Extendibility and Multi-tenant.

4.1 Adding Secure Objects

Users can add Secure Objects to the Ease of Use configurations by creating new Secure Objects. During creation, the user needs to assign the object identifier (see Object identifier). For access control the user must set the policy according to the use case of their system (see section Secure Object policy). For any Secure Object the minimum access control policy for each user has to be set up.

Users have to choose between persistent and transient Secure Objects (in case both are supported; see [1]). Persistent Secure Objects value is always written to NVM while transient Secure Objects value is written into RAM.

For transient Secure Objects, it is possible to export the value (in encrypted form) of the Secure Object to the host controller and later on import the value again, as long as the Secure Object has not been deleted from the SE050E. Persistent Secure Objects cannot be exported or imported. Import and Export of a Secure Object requires the policy POLICY_OBJ_ALLOW_IMPORT_EXPORT to be set. To prevent re-import by unauthorized parties, POLICY_OBJ_ALLOW_IMPORT_EXPORT MUST be restricted to an authentication credential. To prevent modification of the Secure Objects attributes its deletion MUST be restricted by binding policy POLICY_OBJ_ALLOW_DELETE to an authentication credential.

4.2 Reserved identifiers

To prevent denial of service attacks reserved identifiers for secure objects, which are not pre-provisioned by NXP, MUST be created, preferrably to device individual values.

This is especially important for the following identifiers:

- RESERVED_ID_TRANSPORT
- RESERVED_ID_FACTORY_RESET
- RESERVED_ID_I2CM_ACCESS
- RESERVED_ID_RESTRICT

4.3 Creating Crypto Objects

By default, users have the possibility to do either cipher, signature or digest operations in one shot, meaning the input data are passed to the SE050E and the output data are returned directly. The SE050E does not keep any state in that case.

However, when users have the need to pass several blocks consecutively to the SE050E for one of those cipher, signature or digest operations, a Crypto Object can be allocated.

A Crypto Object will keep the state of a crypto operation and allow typically to do init/(n times) update/final operations.

4.4 Adding an attestation key

Customers can provide their own attestation key(s) (and related certificates) to perform the attestation as explained in Attestation. These keys must be injected or generated either in an secure environment or via a secure channel.

4.5 Adding Cloud Connection keys

SE050E Ease of Use configuration can be extended with credentials to onboard and connect securely to various clouds. Customers might decide to use their own PKI and CA.

More details on this use case can be found in [3] and [4].

4.6 Apply transport lock

Transport lock use provides security recommendations to securely use the transport lock.

4.6.1 Simple Use Case

The transport lock is a secure object which can be used to protect the modules on the logistic chain.

The transport lock MAY be used as tamper seal between entity A and entity B. Entity A applies a lock and share the key with entity B to give authorized access only to entity B. In this case entity B MAY be the final receiver of the devices.

4.6.2 Updatable Transport Lock

There might be more than two entities in the logistic chain. In this scenario each entity MAY be both a customer and a configurator.

In the case of a cascade logistic chain, entity A MAY make the Transport Lock updatable.

Receiving entity B can remove the lock of A and update the lock for further entities into the logistic chain.

Entity B MAY apply a specific lock for each entity which will receive the product.

4.7 Factory reset

Factory key reset allows to delete all objects except for those where the origin attribute is configured to "provisioned". This is the case for all keys belonging to the NXP Ease of Use configuration as well as mandatory secure objects such as UUID.

To prevent the unintended deletion of keys the secure object with ID RESERVED_ID_FACTORY_RESET MUST be set.

Note: *Certificates trust provisioned by NXP will be deleted after factory reset.*

Note: *Platform SCP keys are unaffected by the factory reset procedure.*

4.8 Object deletion

As described above, some of the credentials injected into the Ease of Use configuration, such as the Cloud Onboarding certificates, can be deleted by the customer if desired.

To delete them, the credentials must be overwritten first. This will change the origin from “provisioned” to either “internal” or “external” (depending on the write method) and will allow deletion either via individual deletion or via the factory reset.

Note: *To ensure the correct execution of the deleteAll command, a ReadIDList command or individual CheckObjectExists commands must be performed under the protection of a secure channel (with R-MAC) to ensure the proper deletion of the previously existing object(s). The response must indicate that the object has been correctly deleted.*

4.9 Importing external objects

Note: *The APDU “ImportExternalObject” must not be used without first contacting NXP to avoid potential problems. If you have used or plan to use the APDU “ImportExternalObject,” please make sure you contact your NXP representative.*

Users might import credentials using importExternalObject or writing to a new object using either applet-SCP03 or ECKey session.

ImportExternalObject, same as WriteSecureObject, can be performed by any party as long as not disabled by DisableSecureObjectCreation or TransportLock. The SE050E keypair (ID 0x7FFF0202, RESERVED_ID_EXTERNAL_IMPORT) is provisioned already by NXP as specified in [2]. The public key of the external party needs to be inserted as authentication object into any other chosen secure object ID, to use this feature.

Any command to write or update a credential can be sent. In addition to an unprotected command, ImportExternalObject commands are signed, encrypted and implicitly authenticated.

The APDUs for ImportExternalObject can be replayed. Access control via policies and/or versioning of the SecureObject can be used to restrict this.

Note that APDUs "WriteECKey" and "WriteRSAKey" do not check consistency of the components being written. Also, the APDUs do not check P1_KeyType when executed on an existing object.

APDU "WriteECKey" truncates the key components and does not return an error when writing an ECKey object on curve ID_ECC_MONT_DH_448 to an existing ECKey object on curve ID_ECC_ED_25519.

APDU "WriteSecureObject", when executed on an existing object, does not serve with attribute checks for "Authentication indicator", "Minimum tag length for AEAD operations", "Minimum output length" or "Maximum authentication attempts". The policy check of APDU "WriteECKey" does not cover verification of the existing ECKey object's curve.

4.10 Single-tenant use cases

4.10.1 Cloud Connection

The Ease of Use configuration can be used to onboard and connect securely to various clouds. More details can be found on the following Application Notes:

- SE05x for secure connection to Azure IoT Hub

- SE05x for secure connection to AWS IoT Core
- SE05x for secure connection to OEM cloud
- SE05x for secure connection to GCP
- SE05x for secure connection to IBM Watson IoT

4.10.2 Device to Device Authentication

Every SE050E product variant comes pre-provisioned with credentials which can be used for Device to Device authentication.

More details on the use case can be found in [8].

4.10.3 Attestation of provisioned objects

Note that for attestation, the key pair that performs the attestation (i.e. signing) needs to be part of a trusted certificate chain.

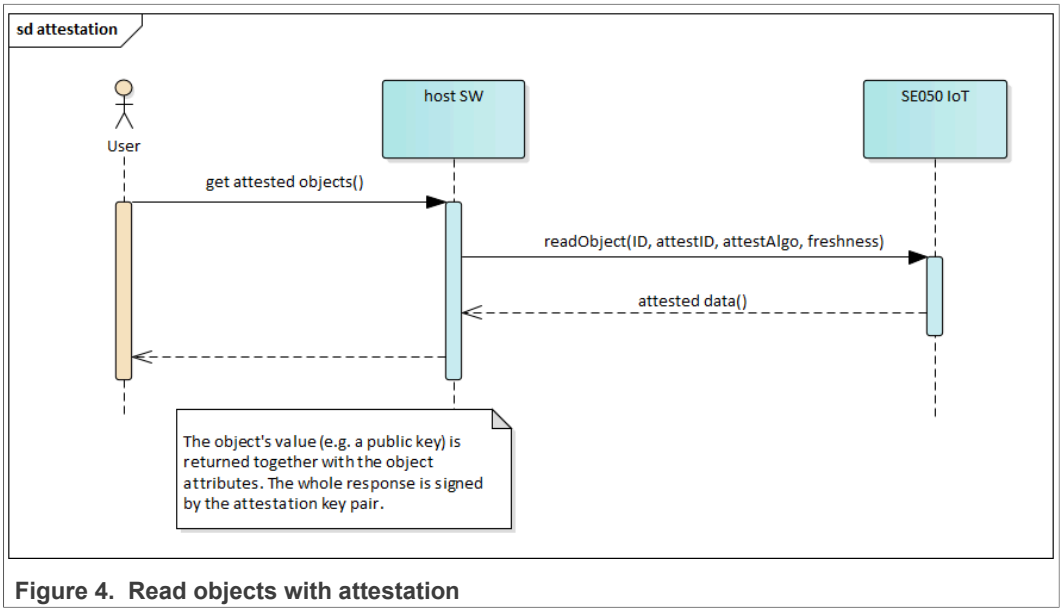

Figure 4. Read objects with attestation

4.10.4 User application

Any command can be sent in the default session (no authentication to the applet nor command wrapping are needed).

Data are encrypted and protected by Platform SCP.

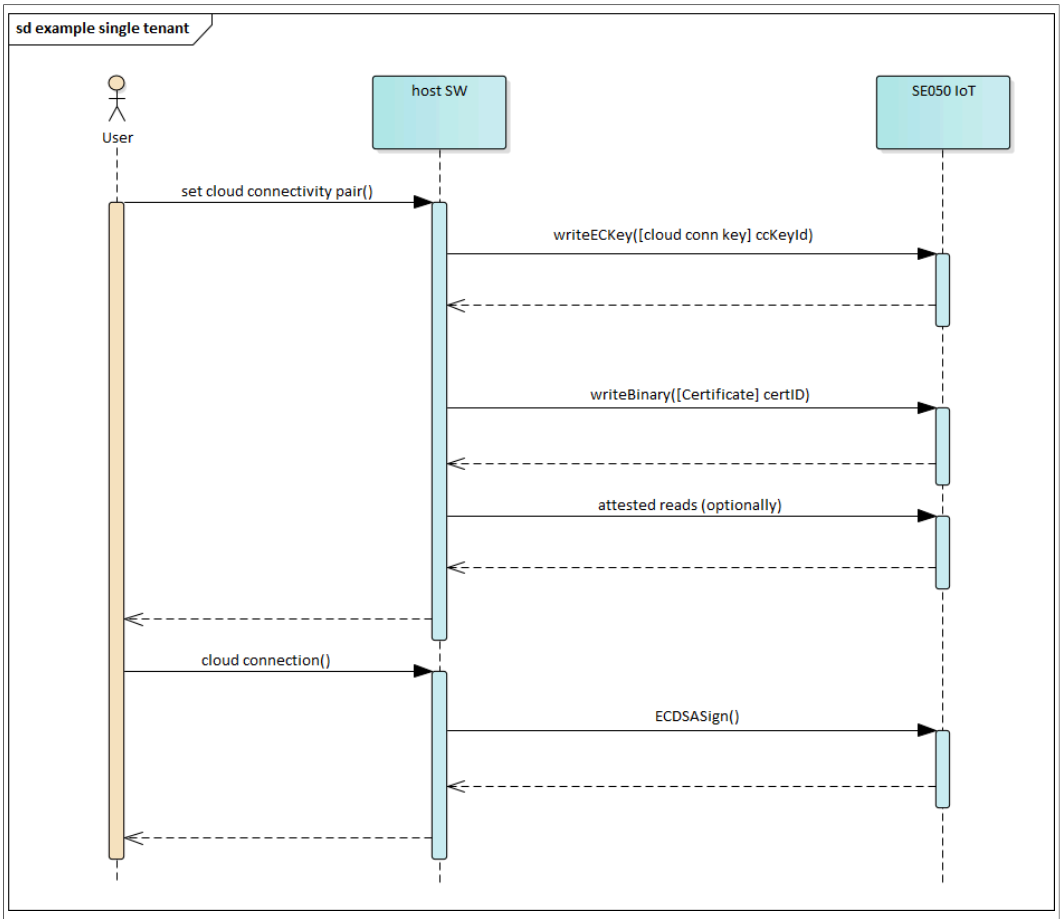

Figure 5. Single-tenant user application example

5 Multi-tenant use of SE050E

5.1 SE050E features for multi-tenant use

5.1.1 Authentication Objects

An Authentication Object is a specific Secure Object that allows users to mutually authenticate against the SE050E applet. In that sense the value of the object is protecting access to the SE050E.

Users who use an Authentication Object to authenticate against the SE050E applet are referred to as ***bound*** users (as opposed to the *unbound* user).

5.1.1.1 Authentication Object Creation

The entity that creates the Authentication Object is referred to as the ***authentication object owner***. The owner can be a single entity or multiple entities (whoever knows the value of the Authentication Object's value).

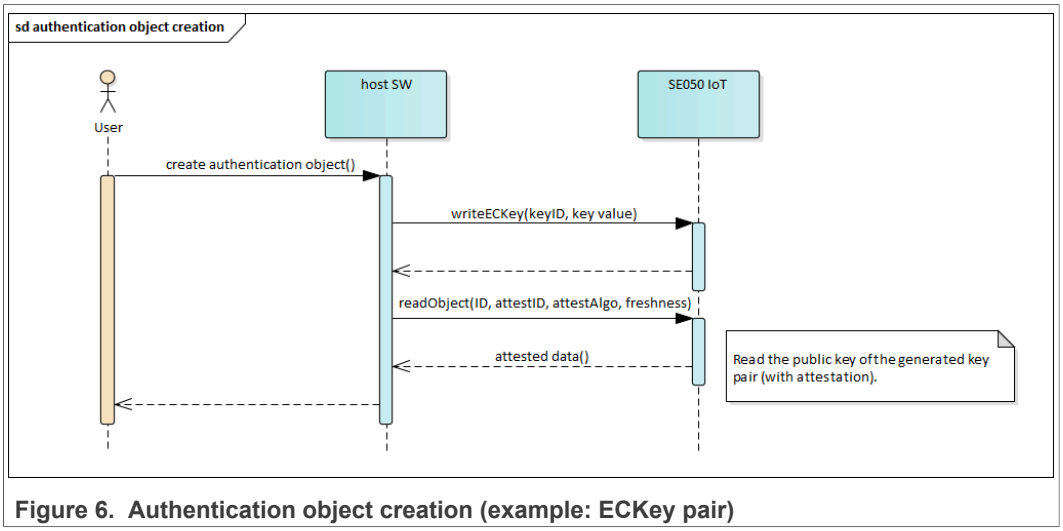

Figure 6. Authentication object creation (example: ECKey pair)

5.1.2 Sessions

The SE050E allows to open a **session** with any of the following Secure Objects:

- userID (to open a UserID session)
- AES128 key (to open a SCP03 session)
- ECKey pair or EC public key (to open a ECKey session)

UserID sessions are using communication in plain, whilst SCP03 or ECKey sessions rely upon SCP03 secure messenging and therefore provide end-to-end protection (see: security recommendation.

If a user opens a session:

- the access rights for the unbound user do not longer apply
- the user will become known by the Authentication Object ID that was used to open the session and becomes a ***bound*** user.

By default, if a SCP03 or ECKey session is established, **applet level SCP** will apply end-to-end for this particular session. On applet level SCP is using SCP03 secure messaging; the difference between an SCP03 and a ECKey session is the authentication method, where SCP03 is based on symmetric crypto and ECKey is using asymmetric crypto for the authentication.

Authenticated User Session provides recommendations for a secure use of sessions.

Note that in cases where Platform SCP is used, the applet level SCP is wrapped inside of the Platform SCP channel, see: [1].

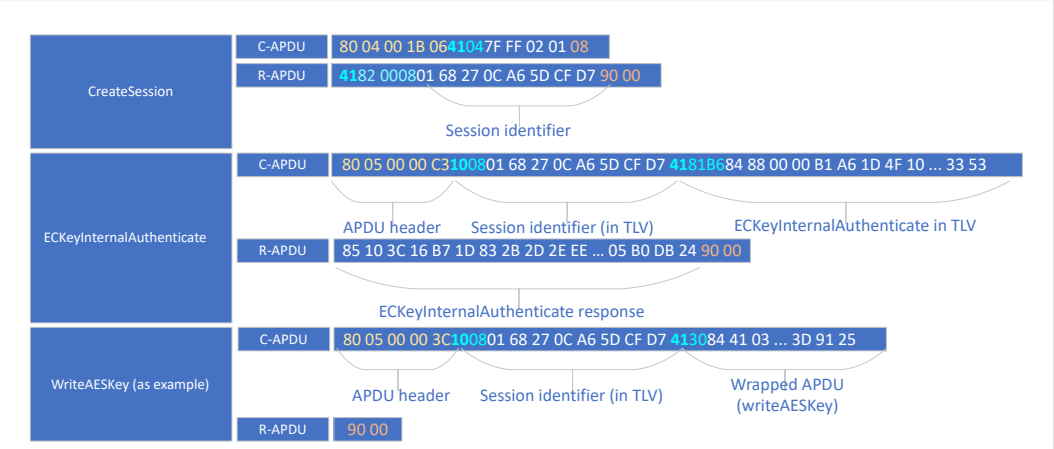

Figure 7. Example APDUs in ECKey session without Platform SCP

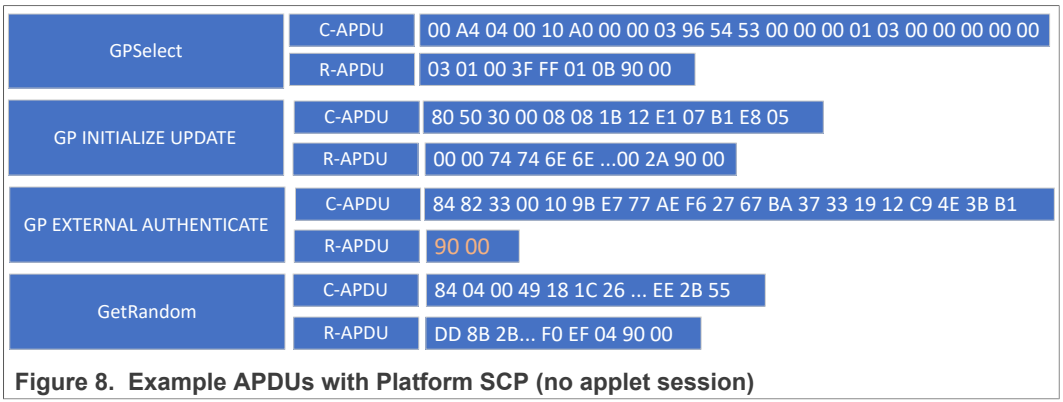

Figure 8. Example APDUs with Platform SCP (no applet session)

5.1.2.1 Session policies

Besides Secure Object policies, the user can also assign a policy to a session. If a policy is passed as argument during session creation, the session will be limited in its lifetime by the number of APDUs that are sent within the session. So the user passes the maximum number of APDUs and when this maximum is reached, the session is broken down and the user is no longer authenticated.

Note that the user can call SessionRefresh to extend the lifetime of a session.

5.1.2.2 Example UserID session

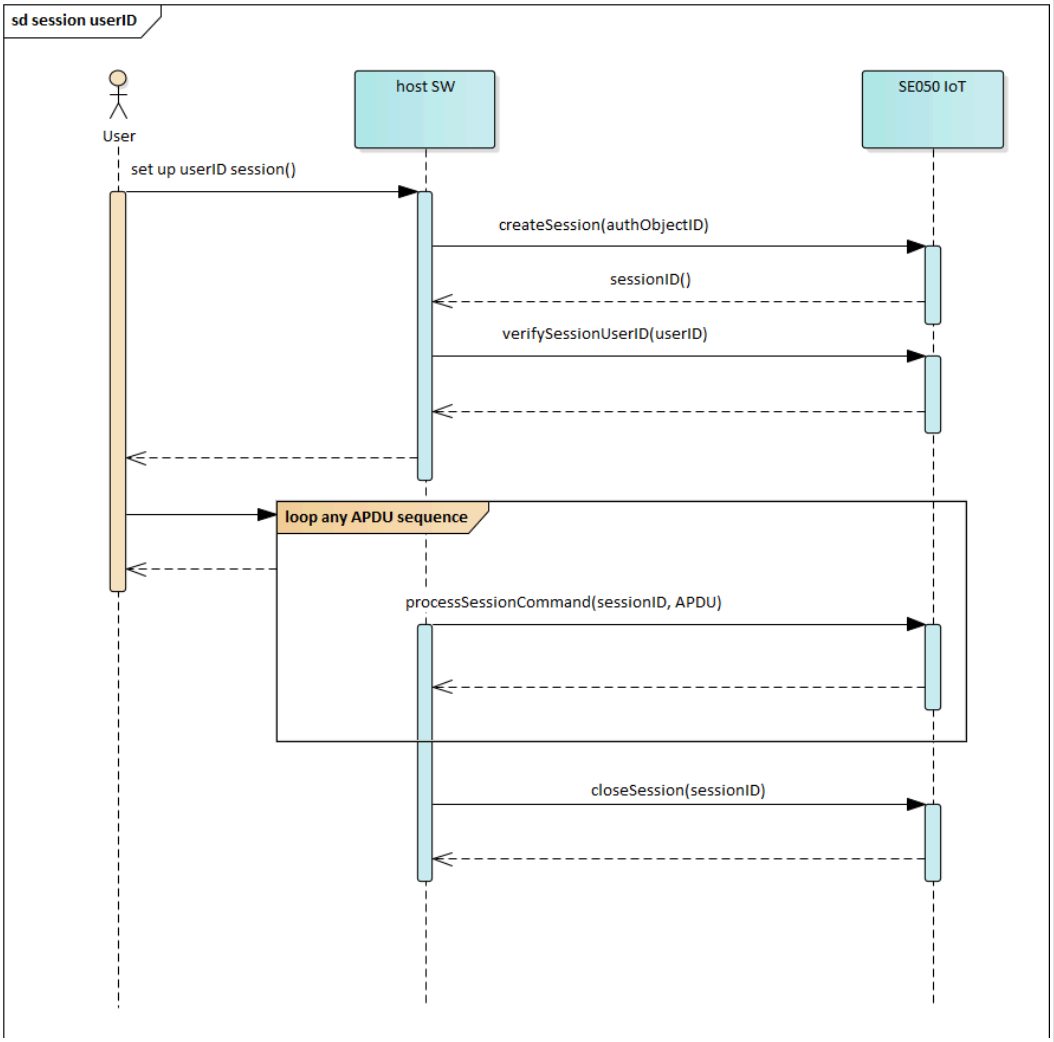

Figure 9. Example UserID session

Note: *Default session policy*

5.1.2.3 Example SCP03 session

Here the SCP03 protocol as defined in Global Platform (Card Specification v 2.2 – Amendment D) is used. The Global Platform SCP03 session is encapsulated within an applet session as shown in the picture below and is then called “applet SCP03 session”.

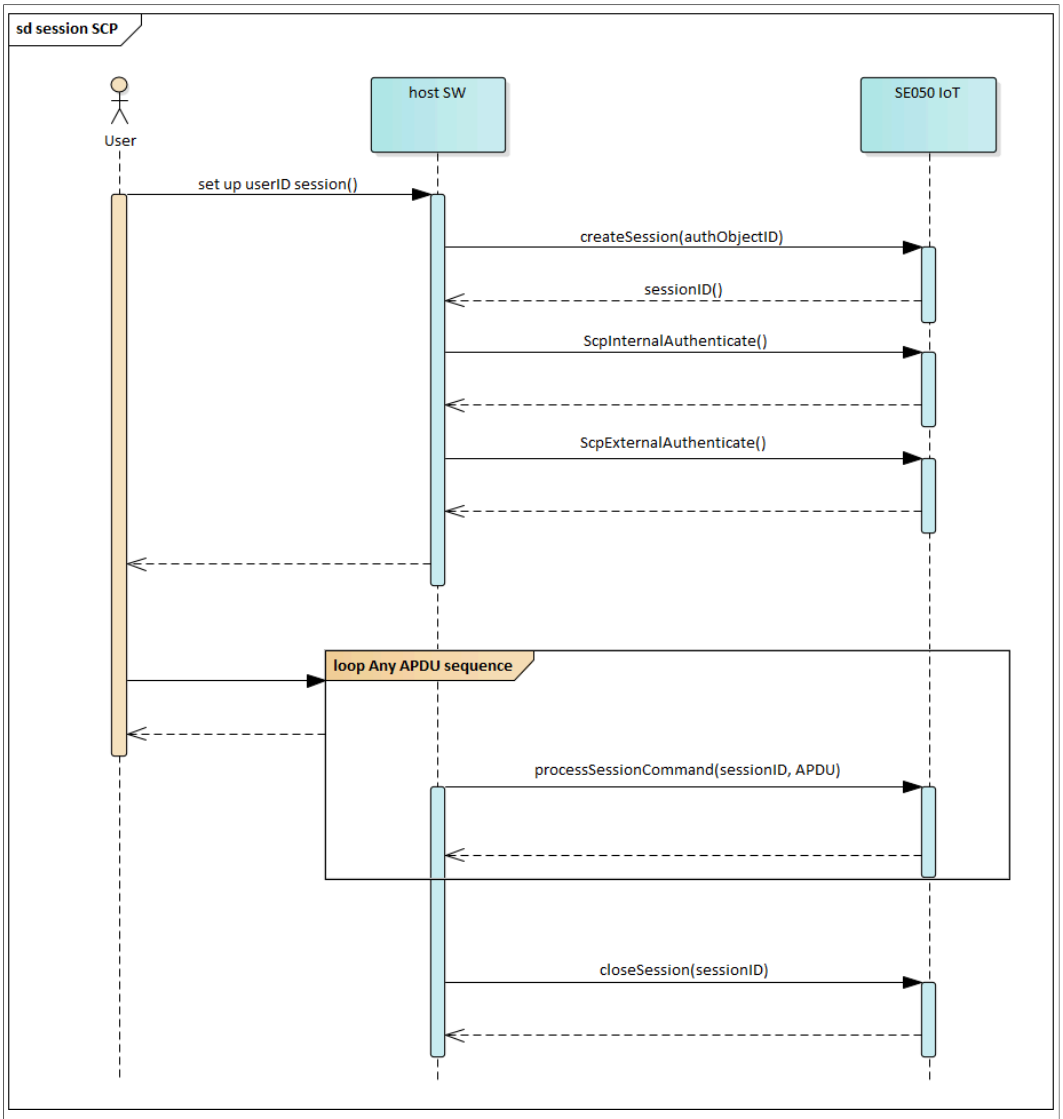

Figure 10. Example SCP session

Note: *Default session policy*

5.1.2.4 Example ECKey session

ECKey sessions uses ECKeys stored in the SE050E to open an bound user session. The authentication is done using the asymmetric ECKey and the session is encrypted using the SCP03 protocol. The ECKey authentication is defined in [1].

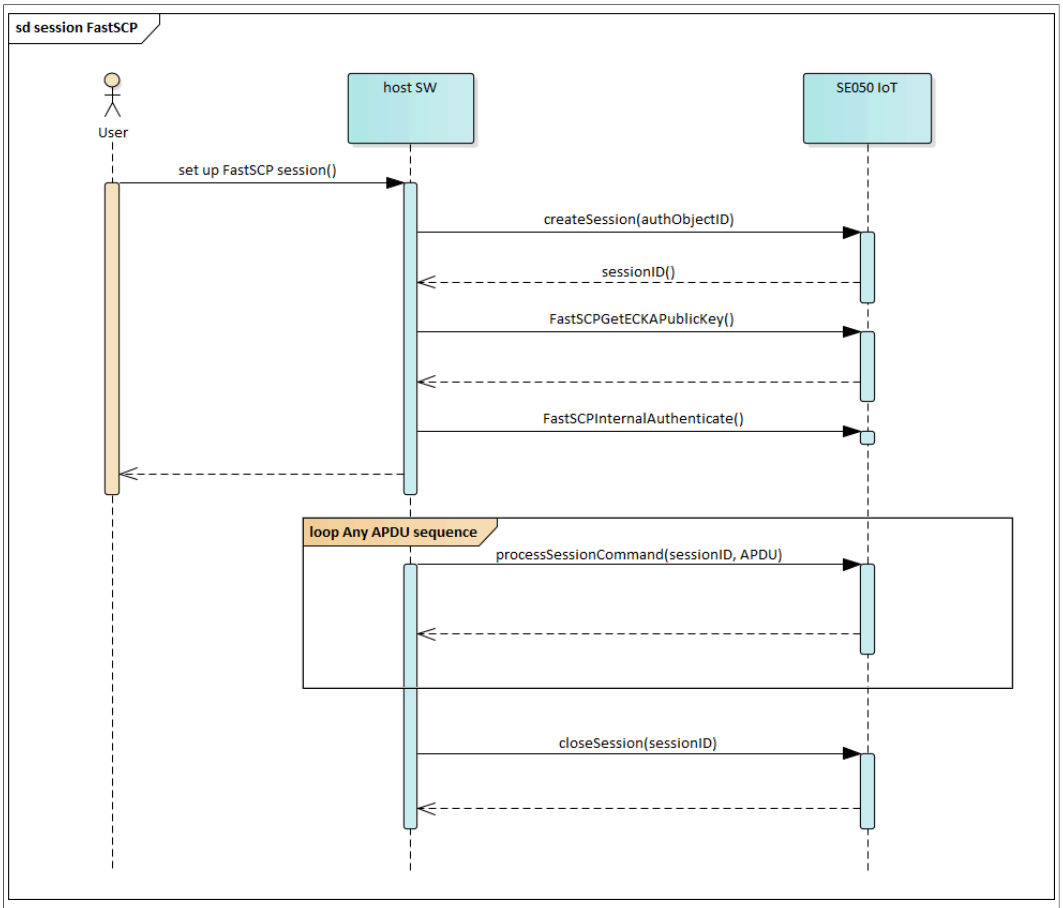

Figure 11. Example ECKey session

Note: *Default session policy*

5.1.3 Secure Object policies for multi-tenant use

When multiple users are configured or expected, the Secure Object policies need to be set up to allow the right users to perform the right operations (and forbid to the wrong user).

As a (simple) example, there could be a mapping of users to object policies as follows:

Table 2. Secure Object policies for multi-tenant use

	User A	User B
POLICY_OBJ_ALLOW_DELETE	Granted	Denied
POLICY_OBJ_ALLOW_READ	Granted	Granted
POLICY_OBJ_ALLOW_WRITE	Granted	Denied
POLICY_OBJ_ALLOW_SIGN	Denied	Granted

6 Trust Provisioning

This chapter focuses on the credentials provisioning.

Credentials provisioning provides recommendations on how to provision credentials in SE050E in a secure manner.

6.1 Trusted or untrusted environments

The provisioning phase of the device is critical to the security of the product, since sensitive data and key material are being generated on or injected into the SE050E.

A device can operate in different types of environments:

- **Trusted environment** – a trusted environment is a secured environment under control of a trusted party. The level of security depends on the environment and should be set appropriate to the threats and security objectives relevant to the device and its assets
- **Non-trusted environment** – a non-trusted environment is an unsecured environment and no control can be applied to it.

6.2 SE050E Trust Provisioning

The IoT device identity should be unique, verifiable and trustworthy so that device registration attempts and any data uploaded to the OEMs servers can be trusted. The SE050E is designed to provide a tamper-resistant platform to safely store keys and credentials needed for device authentication and registration to OEMs cloud service. Leveraging the SE050E security IC, OEMs can safely authenticate their devices without writing security code or exposing credentials or keys.

The following options are available for provisioning the EdgeLock SE050E security IC:

- EdgeLock 2GO Ready: Every EdgeLock SE050E product variant comes pre-provisioned with keys which can be used for all major use cases, including device-to-device authentication.
- EdgeLock 2GO Custom: NXP offers a customization service for injecting the credentials that you need during the SE050E IC manufacturing. Please contact NXP for more information on this service.
- EdgeLock 2GO Managed: NXP offers a cloud service for remotely configurating your SE050E. EdgeLock 2GO Managed is a secure and flexible way for provisioning the keys and certificates required on your devices and to manage the lifecycle of your device credentials. You can find more information and request an evaluation account at www.nxp.com/EdgeLock2GO .
- EdgeLock SE050E provisioning by OEMs, distributors or third-party partners: OEMs can provision EdgeLock SE050E on their own or select a distributor or third-party partner for provisioning the SE050E.

7 Security Recommendations

This chapter describes requirements and recommendations which have to be followed to use the production in a secure manner. Not complying bears a risk of security gaps.

“Must”, “should” and “may” are used in compliance with RFC2119 (see [9].)

- **Must** indicates an absolute security requirement

- **Should** indicates a security recommendation, meaning there may exist valid reasons in particular circumstances to ignore a particular item
- **May** mean that an item is optional

7.1 Generic recommendations (all use cases)

7.1.1 Platform and applet level SCP

Either Platform SCP or applet level SCP MUST be used to protect locally against eavesdropping and malicious command injection.

In operation stage the secure element MUST be configured to mandate platform SCP or mandate applet level SCP by secure object policy. In order to guarantee confidentiality and integrity on the APDU interface the full security level, which means command and response MAC and encryption (see APDU specification) MUST be enabled. The NXP PlugAndTrust MW uses the full security level by default.

Confidentiality, integrity and authenticity of the host SCP key set MUST be enforced as required during provisioning of the keys, outside of secure element, in the host and its memories.

- Access control on host keys MUST be enforced when available, or any mechanism that protects the keys from being disclosed
- Further security properties MUST be preserved by environmental measures.

Default SCP keys MUST be updated at first use of the product. It is recommended to use die individual keys to allow a mutual binding between the host and the secure element.

Confidentiality, integrity and authenticity of the SCP key set MUST be enforced as required during provisioning of the keys, outside of SE050E, in the host and its memories.

- SCP keys MUST be stored securely in the host. With PlatformSCP it is recommended to only have the encryption (ENC) and macing (MAC) keys stored on the host while having the data encryption (DEK) key, which is used to update the keyset within the SE050E, not stored on the host. For more information on the intended usage and details of the cryptographic keys used with Platform SCP please refer to [10].
- Access control on host keys MUST be enforced if available, or any mechanism that protects the keys from being disclosed.
- Further security properties MUST be preserved by environmental measures.

7.1.2 Initial State

Upon reception of SE050E, the authenticity of the provisioned Secure Objects MAY be checked by reading the Trust Provisioned flag of the Secure Object.

- The presence of the Trust Provisioned flag ensures the secure object has been securely provisioned by NXP.

During SE050E lifecycle, the authenticity of the provisioned secure objects MAY be checked by reading the Secure Object content with attestation mode.

7.1.3 Attestation

7.1.3.1 Attestation keys

Secure Objects used for attestation MUST have the POLICY_OBJ_ALLOW_ATTESTATION explicitly set and MUST NOT have the Policy rule POLICY_OBJ_ALLOW_SIGN or POLICY_OBJ_ALLOW_DECRYPT set.

When an attestation key is used the attestation key MUST be trusted (e.g. by validating the certificate chain associated with the public key)

It is recommended to use a pre-provisioned secure object for attestation and check the integrity of the key with an existing certificate. This is the case for credentials trust provisioned by NXP, indicated by the ORIGIN_PROVISIONED and related certificates.

Note: The product variant "C" comes with a certificate for the attestation key pre-provisioned.

7.1.3.2 Read with attestation

When reading with attestation, all returned fields MUST be checked for each attestation to prevent reuse of attestation.

- The attestation signature MUST be verified with a trusted attestation key.
- The timestamp field for consecutive attestations MUST be checked to be consecutive. Note: the timestamp must never have a value lower than the one from the previous attested read.
- The freshness (user input) in the C-APDU MUST be unique/random.
- The object id, type and object attributes MUST be compared against expectation.

The attested read to an RSAKey or ECKey object does not give evidence on correctness of the private key. The attested read to an ECKey object does not give evidence on correctness of the keys curve.

7.1.4 Secure Object policy

If access control to a Secure Object is required the user MUST set the policy of the object.

- NXP defined the default policy without considering any end use case application. It is solely responsibility of the developer to assess whether such policy can be used in their application. NXP recommend to set the policy according to needs and security of the end application.
- It is not recommended to use the default policy as NXP intended it for prototyping and it will therefore allow more access rights to credentials than necessary for the particular use case.
- For access control the user must set the policy according to the use case of their system (see section Secure Object policy). For any Secure Object the minimum access control policy for each user has to be set up.

7.1.5 Key usage

It is recommended to use a key only for one dedicated purpose (e.g. signature creation, encryption or decryption) and to not mix use cases such as:

- Signature of data

- Certificate signing
- key encipherment
- data encipherment
- key agreement

Example: A key used for message decryption shall not be used for signature generation. This is independent of the low level crypto operations allowed for the key, which can be the same operation.

Example: An AES key used for data encipherment shall not be used for signing data using CMAC.

7.1.6 Key Derivation Functions

The iteration count for PBKDF2 MUST be chosen accordingly for the respective use case. If execution with lower count may affect the security of the use case, the access to the relevant HMACKey must be protected at least one of the following:

- setting POLICY_OBJ_REQUIRE_SM
- configuring an Authentication Object for the operation
- mandating Platform SCP

When a function allows optionally output to be stored into a target object instead of returning via the R-APDU, the POLICY_OBJ_FORBID_DERIVED_OUTPUT can be applied on the source object to prevent output being returned to an external party and as such mandate the use of a target object on the SE050E. For more details see [1]

When a Key Agreement and a Key Derivation Function are combined in succession, while the intermediate result remains on the SE050E, (e.g. ECDHGenerateSharedSecret followed by an HKDFExtractAndExpand) to avoid manipulation as well as execution of different intermediate commands during the entire processing, it MUST be executed within a session.

A target object used in TLSCalculatePreMasterSecret with key exchange algorithm RSA_PSK or ECDHE_PSK cannot be protected against manipulations by setting ALLOW_DERIVED_INPUT, which is verified against only one of the two source objects. Protection of such target object against manipulations could instead be achieved with POLICY_OBJ_REQUIRE_SM, with restricting ALLOW_DERIVED_INPUT to an authentication object or by mandatory Platform SCP.

In case function HKDF resp. PDKDF2 shall return a derived secret into a target object, related source object can be assigned with a minimum output length in its attributes to preserve confidentiality of this derived secret.

An ECKeyPair used as source object in TLSCalculatePreMasterSecret for key exchange algorithm ECDH or ECDHE_PSK can be assigned with POLICY_OBJ_FORBID_DERIVED_OUTPUT to prevent its misuse in ECDHGenerateSharedSecret for retrieval of related shared secret in its response. (As it shares ALLOW_KA with APDU ECDHGenerateSharedSecret.)

7.1.7 Crypto Operation Cross-Usage

7.1.7.1 Crypto Operation Policies

All modes of the AES crypto operations use the same cryptographic primitive for encryption and for modes CTR, CCM and GCM//GMAC encryption and decryption are mathematically equal. Therefore it is not possible to prevent a decryption operation in mode CTR, CCM or GCM/GMAC by omitting the policy POLICY_OBJ_ALLOW_DEC while POLICY_OBJ_ALLOW_ENC is present.

FORBID_EXTERNAL_IV can be used in combination with POLICY_OBJ_ALLOW_ENC to generate the IV on the SE050E and return it, thereby making a decryption in AES CTR, CCM or GCM/GMAC mode not practical as the IV cannot be chosen.

There is no mode out of ECB, CBC, CTR, CCM and GCM/GMAC for which encryption operations could be prevented by omitting the policy POLICY_OBJ_ALLOW_ENC while POLICY_OBJ_ALLOW_DEC is set.

7.1.7.2 Crypto operations in AEAD modes

The internal authentication keys in Authenticated Encryption with Associated Data modes AES CCM and AES GCM/GMAC can be constructed for their return by using the same cipher key in modes:

- AES CTR in ENC/DEC
- AES ECB in ENC
- AES CBC in ENC

Therefore to protect confidentiality of the internal authentication keys in AES CCM and AES GCM/GMAC when POLICY_OBJ_ALLOW_ENC is set, it SHALL be combined with FORBID_EXTERNAL_IV. When the policy POLICY_OBJ_ALLOW_DEC is set, or POLICY_OBJ_ALLOW_ENC without FORBID_EXTERNAL_IV, access to the cipher key MUST be restricted by setting at least one of the following:

- setting POLICY_OBJ_REQUIRE_SM
- configuring an Authentication Object for the operation
- mandating Platform SCP

7.1.8 Transport Layer Security

A target object used in TLSCalculatePreMasterSecret with key exchange algorithm RSA_PSK or ECDHE_PSK cannot be fully protected against manipulations by setting ALLOW_DERIVED_INPUT, which is verified against only the key pair but not the HMACKey source object. Protection of such target object against manipulations could instead be achieved with POLICY_OBJ_REQUIRE_SM, with binding ALLOW_DERIVED_INPUT to an authentication object or by mandatory Platform SCP. For more details see [1]

7.1.9 MIFARE DESFire EV2 Support Functionality

The command DFChangeKey is used to provision a key stored in the SE050E into an external MIFARE DESFire device, therefore the related policy POLICY_OBJ_ALLOW_DESFIRE_CHANGEKEY MUST only be applied to keys with this intended purpose. The policy POLICY_OBJ_ALLOW_DESFIRE_CHANGEKEY requires the DESFire authentication key identifier as extension, this key has to be DESFire authenticated at the time the DFChangeKey is invoked. It is strongly recommended to not set POLICY_OBJ_ALLOW_DESFIRE_DUMP_SESSION_KEY on such DESFire authentication key. If dumping of session keys is required for other use cases of the key,

the host MUST prevent disclosure of the session keys from authentication sessions used for changekey execution. The following options can be considered:

- Configure the DESFire key twice:
  - Once with POLICY_OBJ_ALLOW_DESFIRE_CHANGEKEY authentication key and without POLICY_OBJ_ALLOW_DESFIRE_DUMP_SESSION_KEY, to be used for DFChangeKey command execution.
  - And once as DESFire authentication key without POLICY_OBJ_ALLOW_DESFIRE_CHANGEKEY and with POLICY_OBJ_ALLOW_DESFIRE_DUMP_SESSION_KEY, for other DESFire functinoality.
- Protect access to the SE050E, e.g. by a secure session to ensure the session keys do not get dumped.
- Protect confidentiality of dumped session keys in the host and ensure they are erased immediately after the authentication session.

For more details and explanations on other DESFire related commands and policies see [1]

7.2 Extendibility and Multi-tenant

7.2.1 Transport lock use

7.2.1.1 Transport lock

An entity A can apply a lock on SE050E and share the key with entity B to give authorized access only to entity B. In this case entity B MAY be the final receiver of the devices

If a transport lock is expected in SE050E configuration, customer MUST verify that the lock is still applied upon receipt of SE050E.

- In locked state, only GetVersion, GetUniqueID, GetRandom and CreateSession commands are allowed. Command ReadIDList should fail with response SW_COMMAND_NOT_ALLOWED.
- If an unexpected behavior is noticed, this MUST be reported to the entity which applied the transport lock.

If a transport lock is applied, SE050E MAY be unlocked. Unlocking response MUST be SW_NO_ERROR.

- Unlocking is achieved by authenticating to the reserved authentication object with identifier 0x7FFF0200. If this would fail or unexpected behavior is noticed, this MUST be reported to NXP.

7.2.1.2 Transport Lock Provisioning

These recommendations apply to customers or 3rd Party programming facilities who need transport lock to perform device provisioning.

The transport lock MAY be used as a tamper seal to distribute devices to other parties in a cascade logistic chain.

- In this scenario, the transport lock can be considered as seal, which hampers manipulations to the product during transport.

If more than one customer is intended to perform provisioning in the supply chain, each customer MUST update the transport lock.

- In this case the transport lock MUST be configured with write access policy.

7.2.2 UserID sessions

UserID sessions are not providing authentication functionality but are there to logically group Secure Objects.

7.2.2.1 UserID Secure Object

For secure use of UserID Secure Objects, the maximum authentication attempts TAG_MAX_ATTEMPTS MUST be set to a value different from zero.

- A UserID Secure Object TAG_MAX_ATTEMPTS with a value of zero means infinite authentication attempts. The UserID can be compromised by brute-force attack.
- Note that a TAG_MAX_ATTEMPTS with a value different from zero will cause a flash write at each UserID verification due to counter pre-decrement.

7.2.2.2 Security claims on user sessions

UserID sessions MUST NOT be used alone if confidentiality or integrity of communications are required.

- UserID sessions are not secure intrinsically as the UserID can be eavesdropped, and following communications are not encrypted.
- To ensure confidentiality and integrity of communications SCP03 or ECKey sessions MUST be used.

7.2.3 Secure messaging

If confidentiality is required on a secure object, the Secure Object policy MUST either have

- the rule POLICY_OBJ_REQUIRE_SM set or
- the Authentication Object ID referring to an existing key authentication object (AES128 key for an SCP03 session or ECCKey for a ECKey session) or
- Platform SCP has to be configured mandatorily.
- The highest security level MUST be set to enable C-ENC, C-MAC, R-ENC and R-MAC.

The secure channel concept and the used security levels of the secure channel MUST be tailored to the use case, ideally selecting always the highest possible security level.

7.2.4 ECKey sessions

The ephemeral key to establish a secure session with ECKey MUST be secured at a similar level as the static authentication private key of the host. Therefore, it MUST be destroyed when the secure channel is no longer needed. Furthermore, a newly created ephemeral key MUST be used in the following cases:

- for every new established secure channel with ECKeySessionInternal Authenticate
- for every new import of a secure object using ImportExternalObject

To ensure fresh authentication of the SE050E, one must enable R-MAC for the secure channel and validate the received MACs.

It is recommended to use attested read to retrieve the public key for the authentication of the SE or validate the public key with a certificate.

7.2.5 Credentials provisioning

These recommendations apply to customers or 3rd Party programming facilities who perform provisioning

Note: Provisioning can be protected/restricted by establishing authenticated session with restricted access rights.

7.2.5.1 Remote provisioning

For transferring secret key during remote provisioning, applet level SCP or Secure Object Import MUST be used.

- Use of applet level SCP (SCP03 or ECKey sessions) or Secure Object Import in addition to Platform SCP is mandatory to ensure end-to-end confidentiality and integrity of secrets during remote provisioning.

7.2.5.2 Asymmetric keys and key pairs

Confidentiality, integrity and authenticity of key pairs that are provisioned into SE050E MUST be enforced as required for their use during provisioning and outside of SE050E.

- Key pairs MAY be generated on-chip so that private keys can stay in SE050E.
- Further security properties MUST be preserved by environmental measures.

On-chip key genererated EC keys MUST always be generated as key pairs, by setting P1KeyType to P1_KEY_PAIR.

If only integrity and authenticity of key pairs that are provisioned into SE050E is required, attestation of the Secure Object with a provisioned attestation key MAY be used.

Key pairs provisioned into SE050E MUST be die-individual.

- Device individual key pairs hamper the exploitation of successful attacks on other devices.

For RSA keys a public exponent equal to or larger than 0x010001 (2^16+1) MUST be chosen.

7.2.5.3 Symmetric keys

Confidentiality, integrity and authenticity of symmetric secrets that are provisioned into SE050E MUST be enforced as required for their use also during provisioning and outside SE050E.

- SE050E supports Symmetric Keys with write of the wrapped key value according to RFC3394. Related unwrapping key must have policy POLICY_OBJ_ALLOW_RFC3394_UNWRAP set and MUST NOT have POLICY_OBJ_ALLOW_DEC set.
- Further security properties MUST be preserved by environmental measures.

If only integrity of symmetric keys that are provisioned into SE050E is required the attestation of the Secure Object with a provisioned attestation key MAY be used.

- The timestamp and freshness fields of the attestation must be checked according to Attestation.

When the use case allows it, symmetric secrets provisioned into SE050E SHOULD be die-individual.

- Symmetric Keys hamper exploitation of successful attacks on other devices.

7.2.6 General purpose storage

Integrity and authenticity of GP data that are provisioned into SE050E MUST be enforced as required for their use during provisioning and outside of SE050E.

- Integrity of GP data that are provisioned into SE050E is supported by attestation of the GP data with a provisioned attestation key.
- Further security properties MUST be preserved by environmental measures.

8 Functional Recommendations

8.1 Wear-out prevention

NVM writes have the risk to wear out the flash and thus permanently make the device unusable).

The default configuration of the secure element avoids as much as possible NVM writes: only when storing keys or files permanently into the device, flash write operations are done.

Creation and deletion of any Secure Object or Crypto Object is causing flash write operations. For transient Secure Objects and for Crypto Objects, any update of the value of the Secure Object is not causing additional flash write operations. For persistent Secure Objects, any update of the value of the Secure Object causes flash write operations.

Additional flash writes are done when users opt for putting a maximum number of authentication attempts on Authentication Objects. In that case, any authentication attempt is logged and causing additional flash write operations.

An exception to the general rules above is the shared secret generation in case the EC Montgomery curve 25519 is used: the externally provided public key will in that case be stored in NVM as well, so each shared secret generation will cause additional NVM write operations as well to store the external public key that is used in the shared secret generation.

8.2 Power modes of SE050E

SE050E supports the following kinds of power saving operations:

- “Off”: For this scenario, Vin is not supplied anymore. As a consequence, the IC looses all its internal states that are not yet persisted in NV memory. A full startup sequence needs to be executed.

- “Deep Power Down” via ENA pin: This mode is entered if the ENA pin is set to low potential. The behavior from IC point of view is identical to the power down mode described above. All transient states are lost.
- “Power Down”: When using I^2C interface, a command can be sent on the I^2C link to bring the device into a sleep mode. In Power Down mode, all transient states are kept and the communication can continue with the next APDU. When using the GlobalPlatform APDU Transport over I2C protocol refer to the S(RELEASE request) block in [11] as well as the Power Saving Timeout value (PST) as part of the CIP. When the NXP SE05x T=1 Over I2C protocol is used refer to the End of APDU session request S-Block in [12]
- Active mode: This mode is automatically entered when waiting for next command apdu.

Depending on the startup performance and power saving requirements one of the modes above should be chosen when the SE050E is not actively used.

8.2.1 Application Circuit Basic I^2C usage

Configuration used:

- I^2C from host to SE050E
- SE050E turned off via V_{cc}
- Contactless and I^2C controller not part of application schematic below
- Alternatively the V_{cc}-pin can be connected to the V_{in}-pin instead of the V_{out}-pin. The V_{out}-pin is not connected in this case.

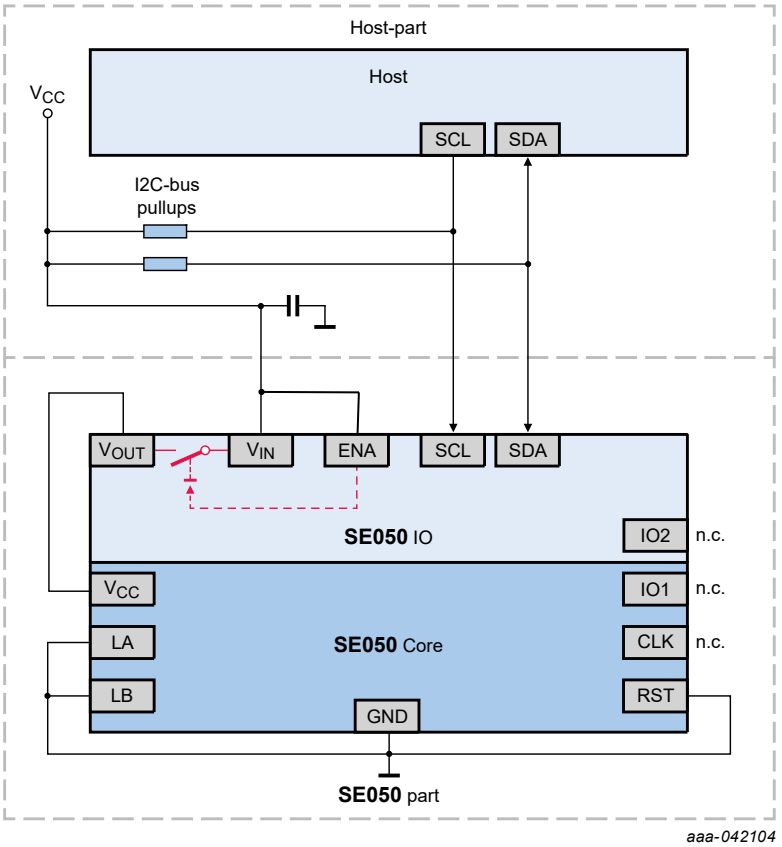

Figure 12. Application Circuit I^2C

8.2.2 Application Circuit I²C with Deep Power Down

Configuration used:

- I²C from host to SE050E
- SE050E turned off using Deep Power Down mode (ENA pin low)
- Contactless and I²C controller not part of application schematic below

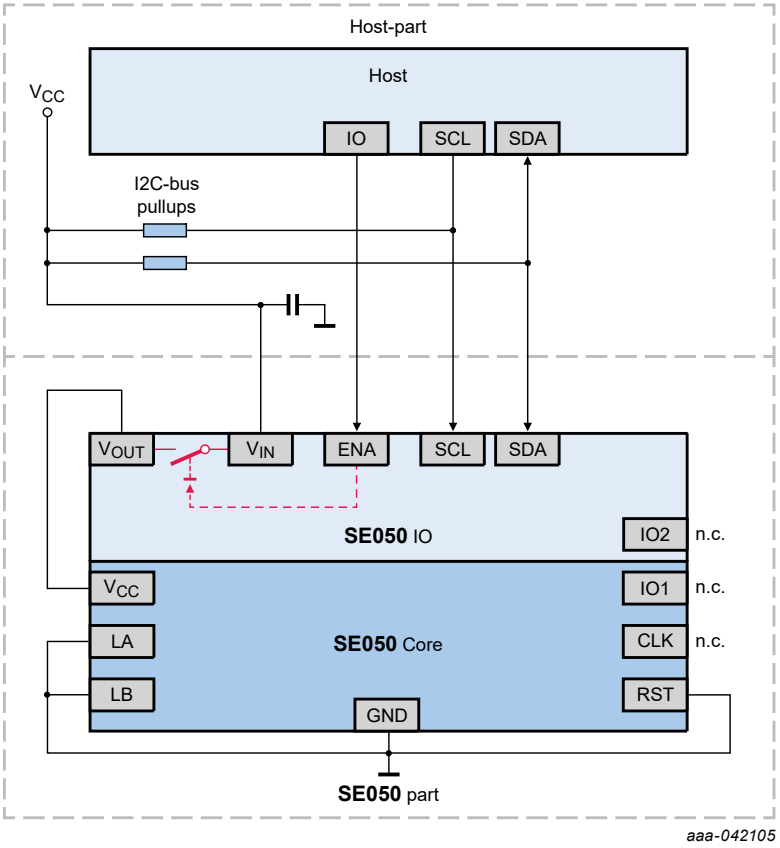

Figure 13. Application circuit I2C with Deep Power Down

No extra capacitor to be placed on the connection between V_{out} and V_{cc}.

8.2.3 Application Circuit I²C Controller (with Deep Power Down)

Configuration used:

- I²C from host to SE050E
- SE050E turned off using Deep Power Down mode (ENA pin low)
- I²C controller interface connected, in the below application schematic external sensor supplied by V_{out} of SE050E
- Contactless and I²C controller not part of application schematic below

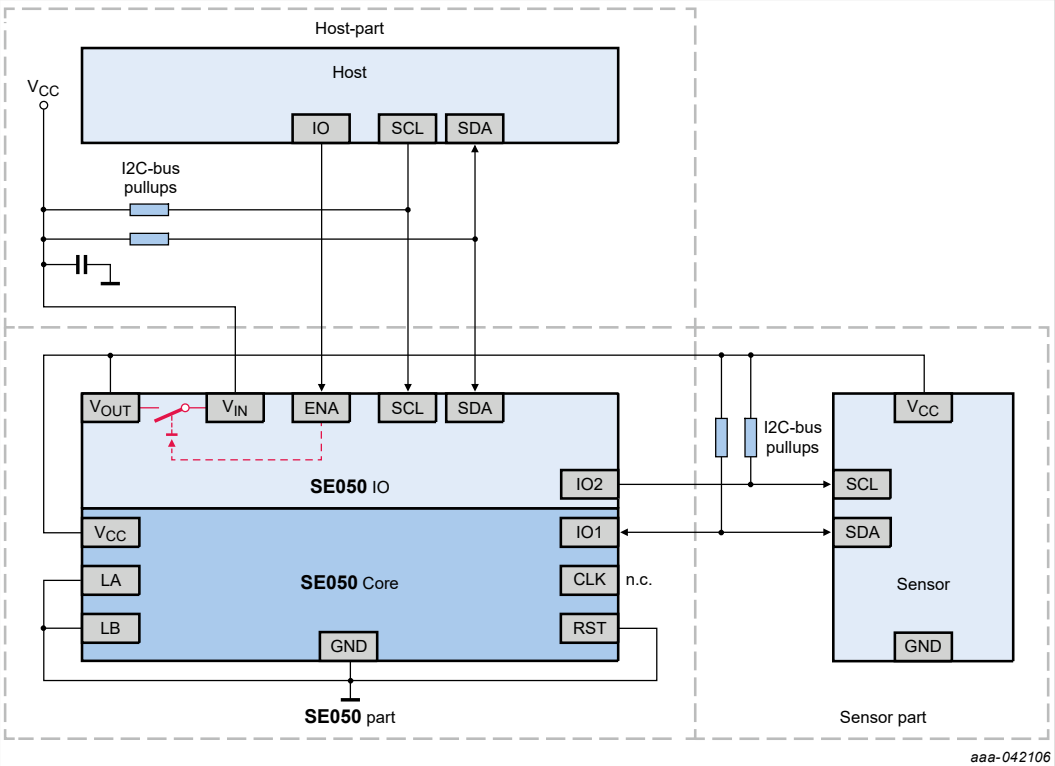

Figure 14. Reference Schematic for Smart Sensor

9 References

[1] Application Note: SE05x IoT Applet APDU Specification, AN12543.

[2] Application Note: SE050 Configurations, AN12436. Available under: https://www.nxp.com/docs/en/application-note/AN12436.pdf

[3] Application Note: SE05x for secure connection to Azure IoT Hub, AN12402. Available under: https://www.nxp.com/docs/en/application-note/AN12402.pdf

[4] Application Note: SE05x for secure connection to AWS IoT Core, AN12404. Available under https://www.nxp.com/docs/en/application-note/AN12404.pdf

[5] Application Note: SE05x for secure connection to OEM cloud, AN12400. Available under https://www.nxp.com/docs/en/application-note/AN12400.pdf

[6] Application Note: SE05x for secure connection to GCP, AN12401. Available under: https://www.nxp.com/docs/en/application-note/AN12401.pdf

[7] Application Note: SE05x for secure connection to IBM Watson IoT, AN12403. Available under: https://www.nxp.com/docs/en/application-note/AN12403.pdf

[8] Application Note: SE05x for device-to-device authentication, AN12399. Available under: https://www.nxp.com/docs/en/application-note/AN12399.pdf

[9] RFC2119. Available under: https://tools.ietf.org/html/rfc2119

[10] GlobalPlatform Card Specification Version 2.3.1, GPC_SPE_034. Available under: https://globalplatform.org/specs-library/card-specification-v2-3-1

[11] GlobalPlatform APDU Transport over SPI/I2C, Version 1.0, GPC_SPE_172. Available under: https://globalplatform.org/specs-library/apdu-transport-over-spi-i2c-v1-0-gpc_spe_172

[12] NXP SE05x T=1 Over SPI/I2C Specification, UM11225. Available under: https://www.nxp.com/webapp/Download?colCode=UM11225

[13] Application Note: EdgeLock™ SE05x Quick start guide with Visual Studio project examples, AN12398. Available under: https://www.nxp.com/docs/en/application-note/AN12398.pdf

10 Legal information

10.1 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.

10.2 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.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://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.

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, 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.

10.3 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.

MIFARE — is a trademark of NXP B.V.

Tables

Tab. 1. Identifier for applet reserved area or NXP reserved region 8
Tab. 2. Secure Object policies for multi-tenant use 21

Figures

Fig. 1. Single- and multi-tenant 3
Fig. 2. Overview single-tenant use 10
Fig. 3. Enable Platform SCP 11
Fig. 4. Read objects with attestation 15
Fig. 5. Single-tenant user application example 16
Fig. 6. Authentication object creation (example: ECKey pair) 17
Fig. 7. Example APDUs in ECKey session without Platform SCP 18
Fig. 8. Example APDUs with Platform SCP (no applet session) 18
Fig. 9. Example UserID session 19
Fig. 10. Example SCP session 20
Fig. 11. Example ECKey session 21
Fig. 12. Application Circuit I2C 31
Fig. 13. Application circuit I2C with Deep Power Down 32
Fig. 14. Reference Schematic for Smart Sensor 33

Contents

1 Introduction 3
2 SE050E basics 4
2.1 Product Information 4
2.2 Unauthenticated user 7
2.3 Platform SCP 7
2.4 Unbound user 7
2.5 Secure Objects 7
2.5.1 Secure Object types 7
2.5.2 Secure Object Attributes 8
2.5.2.1 Object identifier 8
2.5.2.2 Type 8
2.5.2.3 Policy 8
2.5.2.4 Origin 9
3 SE050E Plug and Trust: Usage out of the box 9
3.1 Ease of Use Configuration 9
3.2 Single-tenant protection 9
3.3 How to update Platform SCP keys 10
3.4 Attestation 11
4 SE050E configuration extendibility 12
4.1 Adding Secure Objects 12
4.2 Reserved identifiers 12
4.3 Creating Crypto Objects 12
4.4 Adding an attestation key 13
4.5 Adding Cloud Connection keys 13
4.6 Apply transport lock 13
4.6.1 Simple Use Case 13
4.6.2 Updatable Transport Lock 13
4.7 Factory reset 13
4.8 Object deletion 14
4.9 Importing external objects 14
4.10 Single-tenant use cases 14
4.10.1 Cloud Connection 14
4.10.2 Device to Device Authentication 15
4.10.3 Attestation of provisioned objects 15
4.10.4 User application 15
5 Multi-tenant use of SE050E 16
5.1 SE050E features for multi-tenant use 16
5.1.1 Authentication Objects 16
5.1.1.1 Authentication Object Creation 16
5.1.2 Sessions 17
5.1.2.1 Session policies 18
5.1.2.2 Example UserID session 19
5.1.2.3 Example SCP03 session 19
5.1.2.4 Example ECKey session 20
5.1.3 Secure Object policies for multi-tenant use 21
6 Trust Provisioning 22
6.1 Trusted or untrusted environments 22
6.2 SE050E Trust Provisioning 22
7 Security Recommendations 22
7.1 Generic recommendations (all use cases) 23
7.1.1 Platform and applet level SCP 23
7.1.2 Initial State 23
7.1.3 Attestation 24
7.1.3.1 Attestation keys 24
7.1.3.2 Read with attestation 24
7.1.4 Secure Object policy 24
7.1.5 Key usage 24
7.1.6 Key Derivation Functions 25
7.1.7 Crypto Operation Cross-Usage 25
7.1.7.1 Crypto Operation Policies 25
7.1.7.2 Crypto operations in AEAD modes 26
7.1.8 Transport Layer Security 26
7.1.9 MIFARE DESFire EV2 Support Functionality 26
7.2 Extendibility and Multi-tenant 27
7.2.1 Transport lock use 27
7.2.1.1 Transport lock 27
7.2.1.2 Transport Lock Provisioning 27
7.2.2 UserID sessions 28
7.2.2.1 UserID Secure Object 28
7.2.2.2 Security claims on user sessions 28
7.2.3 Secure messaging 28
7.2.4 ECKey sessions 28
7.2.5 Credentials provisioning 29
7.2.5.1 Remote provisioning 29
7.2.5.2 Asymmetric keys and key pairs 29
7.2.5.3 Symmetric keys 29
7.2.6 General purpose storage 30
8 Functional Recommendations 30
8.1 Wear-out prevention 30
8.2 Power modes of SE050E 30
8.2.1 Application Circuit Basic I2C usage 31
8.2.2 Application Circuit I2C with Deep Power Down 32
8.2.3 Application Circuit I2C Controller (with Deep Power Down) 32
9 References 34
10 Legal information 35

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

Date of release: 22 August 2022
Document identifier: AN13483