SE051

SESIP Security Target

Rev. 1.0 — 18 December 2020 **Evaluation document**

Document information

Information	Content
Keywords	SESIP, Security Target, SE051, IEC 62443-4-2
Abstract	Evaluation of the SE051 developed and provided by NXP Semiconductors, according to SESIP Assurance Level 3 (SESIP3), and fulfilling subset of requirement of IEC62443-4-2

Revision History

Rev.	Date	Description
1.0	2020-12-18	First release version

1 Introduction

This Security Target describes the SE051 platform and the exact security properties of the platform that are evaluated against GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.0, SESIP Assurance Level 3 (SESIP3) [1].

1.1 ST Reference

SE051, SESIP Security Target, Revision 1.0, NXP Semiconductors, 18 December 2020.

1.2 Platform Reference

SE051

Table 1. Platform Reference

Reference	Value
Platform Name	SE051
Platform Version	N7121 B1 Test Software 9.2.3 Boot Software 9.2.3 Firmware 9.2.3 Library Interface 9.2.3 Crypto Library 0.7.6 JCOP 4 SE051 v4.7 R3.01.11 SE051 IoT Applet v6.0.0 SE05x Perso Applet 0.0.2 SEMS Lite Applet - 1.4.0.11
Platform Identification	SE051
Platform Type	Secure Element with Java Card Operating System with GlobalPlatform Framework and IoT applets

1.3 Included Guidance Documents

The following documents are included with the platform:

Table 2. Guidance Documents

Document	Reference
JCOP User Manual	JCOP 4.7 SE051, User manual for JCOP 4.7 SE051, Rev. 1.2, DocNo 581812, NXP Semiconductors [9]
Applet User Manual and Specification	AN12543 SE051 IoT applet APDU Specification, Rev. 2.0, NXP Semiconductors [10] SE05xConfig APDU specification, API description SE05x Config Applet, Rev 1.0, NXP Semiconductors [13] SEMS Lite v1.x.x.11JxR Secure Element Management Service Lite Application, User Manual Rev 0.3, NXP Semiconductors [14]
User Guidelines	AN12730 SE051 - User Guidelines, Rev 1.0, NXP Semiconductors [11]
SESIP Security Target	SE051, SESIP Security Target, Revision 1.0, NXP Semiconductors, 18 December 2020.

Table 2. Guidance Documents*...continued*

Document	Reference
GP Card Specification	GlobalPlatform Card Specification 2.3, GPC_SPE_034, GlobalPlatform Inc., October 2015 [16] Executable Load File Upgrade, GPCS 2.3 - Amendment H v1.1, GPC_SPE_120, GlobalPlatform Inc., March 2018 [17] Secure Element Management Service, GPCS 2.3 - Amendment I, GPC_SPE_121, GlobalPlatform Inc., March 2018 [18]
JavaCard Specifications	Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., Oracle, May 2015 [19] Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.5., Oracle, May 2015 [20] Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0.5., Oracle, May 2015 [21]

1.4 Other Certification

The underlying Java Card Operating System and Hardware has previously been evaluated following SOG-IS CC EAL6+ [3].

Item	Content
Scheme	Java Card System - Open Configuration Protection Profile, December 2017, Version 3.0.5, published by Oracle, Inc. (BSI-CC-PP-0099-2017). [5]
Certification Body	The Netherlands Scheme for Certification in the Area of IT Security
Certification number	NSCIB-CC-0095534-CR
Certification date	2020-07-07

Item	Content
Scheme	Security IC Platform Protection Profile with Augmentation Packages, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014 [4]
Certification Body	Bundesamt für Sicherheit in der Informationstechnik
Certification number	BSI-DSZ-CC-1040
Certification date	2019-06-14

SE051 development process has followed Business Creation and Management (BCaM) framework and is subject to Product Security Incident Response Process (PSIRP). BCaM and PSIRP have been certified following Security for Industrial Automation and Control Systems - Part 4-1: Secure Product Development Lifecycle Requirements (IEC 62443-4-1:2018) [7]. See more in Section 3.1.

Item	Content
Scheme	IEC 62443-4-1: 2018 [7] PPP15002A:2018 (IEC62443-4-1 Full Process Profile)
Certification Body	TÜV SÜD Product Service GmbH
Certification number	IITS1 109577 0001 Rev. 00
Certification date	2020-09-18

1.5 Platform Overview and Description

The EdgeLock SE051 product family of Plug & Trust devices offers enhanced security for unprecedented protection against the latest attack scenarios. This ready-to-use secure element for IoT devices provides a root of trust at the IC level.

The product configurations support the latest IoT security use cases such as sensor data protection, secure access to IoT services, IoT device commissioning, and personalization and Wi-Fi credential protection. This support is in addition to the already known use cases, including secure cloud onboarding, device-to-device authentication, device integrity protection, and attestation as well as device traceability and proof-of-origin.

The platform consists of the microcontroller and a software stack which is stored on the microcontroller and which can be executed by the microcontroller. A block diagram of the IC hardware is depicted in Figure 1.

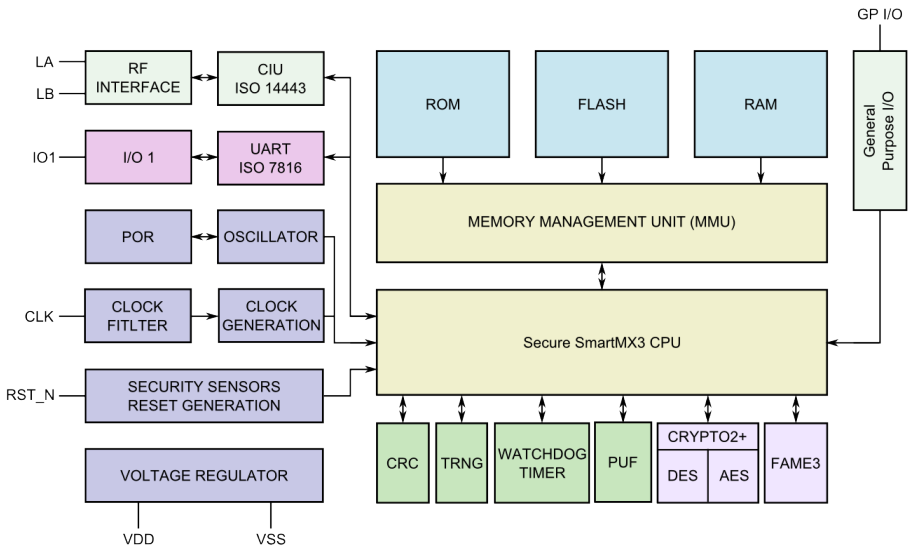

Figure 1. Block Diagram of the IC

The software stack can be further split into the following components:

- Firmware for booting and low level functionality of the microcontroller like writing to flash memory. This includes software for implementing cryptographic operations, called Crypto Library.
- Software for implementing a Java Card Virtual Machine [20], a Java Card Runtime Environment [21] and a Java Card Application Programming Interface [19], called JCVM, JCRE and JCAPI.

- Software for implementing content management according to GlobalPlatform [16], called GlobalPlatform (GP) Framework.
- Software for IoT application and application configuration and maintanence.

The Operating System in the platform is also referred to as JCOP 4. JCOP 4 OS consists of the software stack without the Crypto Library (Crypto Lib) and without the microcontroller firmware. The platform uses one or more communication interfaces to communicate with its environment. The Application Software includes IoT applet, Perso applet and SEMS Lite applet, which supports IoT application and application configuration and maintanence.

The complete platform is depicted in Figure 2. The platform includes Hardware, Firmware, Crypto Library, the JCVM, JCRE, JCAPI and the GP Framework. Also included is optional functionality and the Secure Box mechanism. The Secure Box Native Libraries provide native functions for untrusted third parties and are not part of the platform. The figure shows Java Card applets which are small programs in Java language that can be executed by the platform, but are not part of the platform.

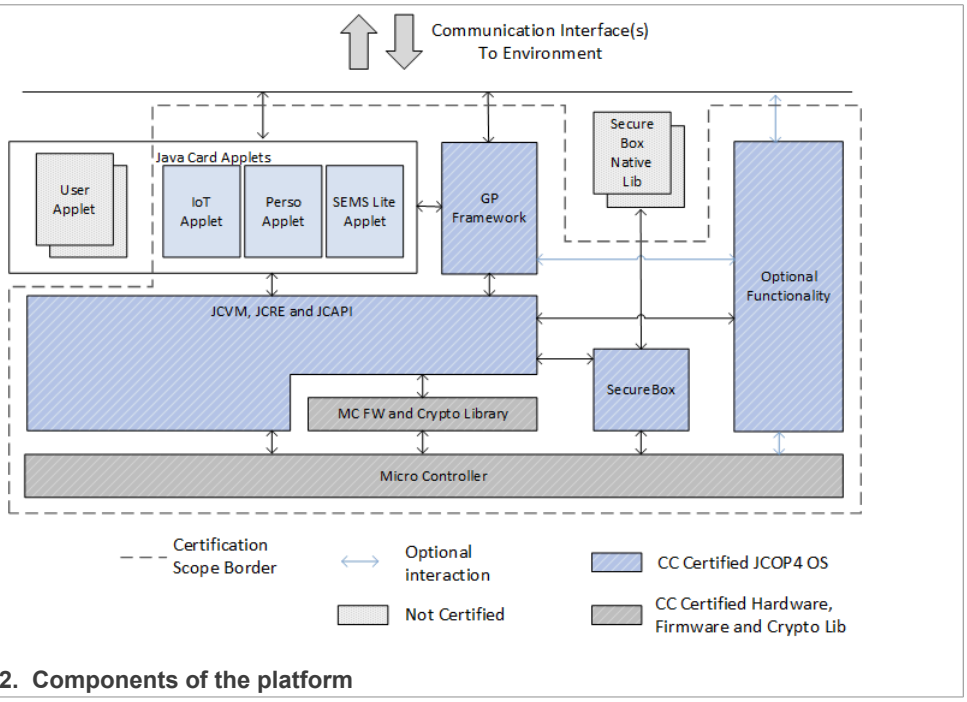

Figure 2. Components of the platform

SE051 is designed to be used as a part of an IoT system. It works as an auxiliary security device attached to a host controller. The host controller communicates with SE051 through an I²C interface (with the host controller being the master and the SE051 being the slave). Besides the mandatory connection to the host controller, the SE051 device can optionally be connected to a sensor node or similar element through a separate I²C interface. In this case, the SE051 device is the master and the sensor node the slave. Lastly, SE051 has a connection for a NFC contactless antenna, providing a wireless interface to an external device such as a smartphone. A reference solution is depicted in Figure 3. Noted the blue part of Figure 3 is not in the scope of the certification.

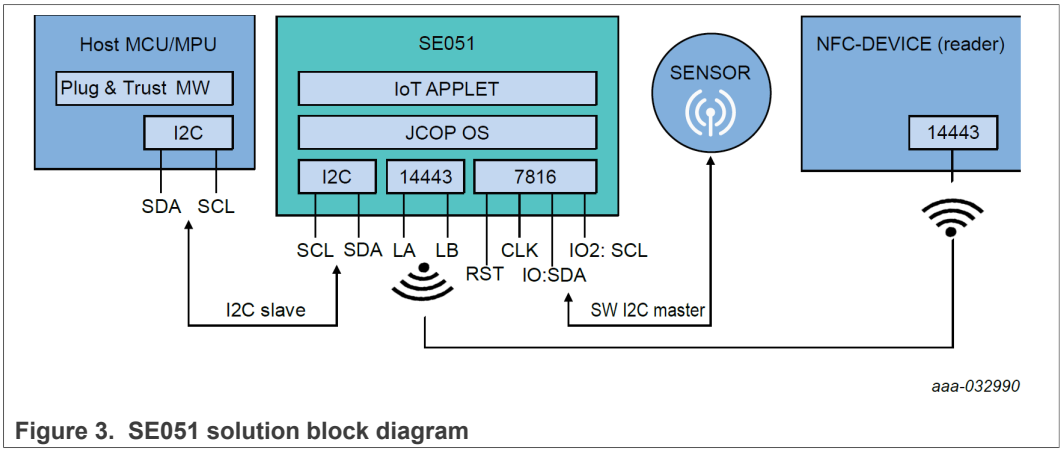

Figure 3. SE051 solution block diagram

1.5.1 Platform Security Features and Scope

The SE051 IoT applet supports:

- Generic module management support
  - Lifecycle management
  - Session management
  - Timer functionality
  - Access control
  - Secure import/export of keys or files
- Applet Secure Channel management
  - AESKey sessions
  - ECKey sessions
- Random number generation
- Key management (ECC, RSA, AES, DES, etc.): write, read, lock, delete
- Elliptic curve cryptographical operations
- RSA cryptographical operations
- AES/DES cryptographical operations (AES ECB, CBC, CTR)
- AES GCM and GMAC (128, 192 and 256 bit).
- Binary file creation and management
- UserID creation and management
- Monotonic counter creation and management
- Platform Configuration Register (PCR) creation and management
- Hash operations
- Message authentication code generation
  - CMAC
  - HMAC
- Key derivation functionality
  - HKDF
  - PBKDF2
- Specific use case support
  - TLS PSK master secret calculation
  - MIFARE DESFire protocol support
  - I2C Master support

Also, the JCOP operating system supports:

- Java Card 3.0.5 Classic
- GlobalPlatform 2.3
- Various Cryptographic Functionality (Session 4.1 of [9])
- Additional JCOP 4.7 SE051 APIs (Section 5.4 of [9])

The physical scope is the SE051 microcontroller as identified in Table 1 and whose functional blocks are identified in Figure 1.

Platform also provides a general purpose I/O interface which is directly connected to the internal SFR bus. This interface is connected to an I2C interface. The Security Functionality of the platform does not rely on the communication interface connected to this interface. However, the platform implements countermeasures against misuse.

The logical scope includes the microcontroller and the software stack which is stored on the microcontroller as identified in Table 1 and Figure 2

No additional non-platform hardware, software or firmware is required for the correct functioning of the security claims described in this document.

1.5.2 IEC62443-4-2 Considerations

IEC62443 series [6] includes several standards and technical reports addressing Industrial Automation and Control Systems (IACS). Its Part 4-2: Technical security requirements for IACS components [8] provides detailed technical control system component requirements. It defines 4 security levels of control system component capability (SL-C 1~4), and 4 types of components of IACS: software applications, host devices, embedded devices and network devices.

SE051 is designed to be used as a part of system as depicted in Figure 3, or in IEC62443-4-2 term, a subcomponent. This document also serves as a guidance on correct integration of an IEC62443-4-2 compliant IACS component. As a subcomponent, SE051 fulfills subset of IEC62443-4-2 requirements which can keep aligned with the overall component requirements, and more importantly, provides services which support the overall component fulfilling IEC62443-4-2 requirements in a secure and ready-to-use way.

The mapping and rationales are provided in Section 4.2.

In Section 3.2, we have not only provided the security functions in SESIP language, also provided further refinement if an IEC62443-4-2 requirement has finer granularity. The refinement refers to the original text from [8] to keep the flavor, yet the reader should be aware there is difference and connection on the terminology between IEC62443-4-2 and SESIP. For instance, component or its type (e.g. embedded device) in IEC62443 may refer to the platform under evaluation in SESIP, and this document intends to keep this usage to provide a clear scope of the certification.

2 Security Objectives for the Operational Environment

2.1 Platform Objectives for the Operational Environment

This section details guidance and information that the user of the SE051 must take into account when integrating the SE051. For SE051 to fulfill its security requirements, the operational environment (technical or procedural) must fulfill the following objectives (Section 7.1 of [11]).

- The configurator shall verify the correct version of JCOP, IoT applet, Perso applet and SEMS Lite Applet as provided in Section 1.2, by selecting the applet if applicable and obtaining the version information as described in Section 3.2.1.1.
- Either Platform SCP or SCP user session MUST be used (Section 7.1 of [11]).
- Platform SCP key MUST be updated or specifically TrustProvisioned (for a specific customer) at first use of the product. (Section 7.1 of [11]).
- Confidentiality, integrity and authenticity of the Platform SCP key set MUST be enforced as required during provisioning of the keys, outside of SE051, in the host and its memories. (Section 7.1 of [11]).
- When reading with attestation, the timestamp and freshness fields MUST be checked for each attestation to prevent reuse of attestation(Section 7.1 of [11]).
- If access control on Secure Object is required the user MUST set the policy of the object (Section 7.2 of [11]).
- If a transport lock is expected in SE051 configuration, customer MUST verify that the lock is still applied upon receipt of SE051 (Section 7.2 of [11]).
- If more than one customer is intended to perform provisioning in the supply chain, each customer MUST update the transport lock (Section 7.2 of [11]).
- For secure use of UserID Secure Objects, the maximum authentication attempts TAG_MAX_ATTEMPTS MUST be set to a value different from zero (Section 7.2 of [11]).
- UserID sessions MUST NOT be used alone if confidentiality or integrity of communications are required (Section 7.2 of [11]).
- If confidentiality is required on a secure object, the Secure Object policy MUST either have the rule POLICY_OBJ_REQUIRE_SM set, or have the Authentication Object ID referring to an existing key authentication object (AES128 key for an AESKey session or ECKey for a ECKey session) or Platform SCP has to be configured mandatorily (Section 7.2 of [11]).
- If customer or 3rd party prgramming facilities perform credentials provisioning (Section 7.2 of [11]).
  - For transferring secret key during remote provisioning, applet level SCP or Secure Object Import MUST be used.
  - Confidentiality, integrity and authenticity of key pairs that are provisioned into SE051 MUST be enforced as required for their use during provisioning and outside of SE051.
  - Confidentiality, integrity and authenticity of symmetric secrets that are provisioned into SE051 MUST be enforced as required for their use also during provisioning and outside SE051
- Integrity and authenticity of GP data that are provisioned into SE051 MUST be enforced as required for their use during provisioning and outside of SE051 (Section 7.2 of [11]).

- Users and customers who desire to extend the SE051 product variants by importing external objects besides the Ease Of Use configuration MUST first contact their NXP representative to avoid potential problems (Section 4.5 of [11] and [12]).

2.2 Inherited Objectives for the Operational Environment

SE051 includes platform parts that have previously been evaluated under *CC EAL 6+*. That platform part defined objectives for its own operational environment, which have been handled by the platform as defined in Section 6 of [9]. SE051 has a few options of configurations including credentials provisioned by NXP and/or enabling extention of other applets. For the product with only credentials provisioned by NXP and no other applet loadable (i.e. closed product), there is no other objectives other than Section 2.1; otherwise, all objectives for the Operational Environment in Section 6 of [9] applies.

2.3 Additional Platform Objectives for the Operational Environment for IEC62443-4-2 Compliance

For SE051 to fulfill an additional security requirement defined by IEC62443-4-2, the operational environment (technical or procedural) must fulfill the following objectives but such objectives are optional or recommended only for non-IEC62443 usage:

- CR1.11: the operational environment shall configure a proper number of maximum authentication attempts other than unlimited (see Section 3.3.3 of [10]).

3 Security Requirements and Implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP3** as defined in Chapter 4 of GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.0 [1].

3.1.1 Flaw Reporting Procedures (ALC_FLR.2)

In accordance with the requirement for flaw reporting procedures (ALC_FLR.2), the developer has defined the following procedure:

NXP has defined a Product Security Incident Response Process (PSIRP), implemented by a dedicated team (PSIRT). This process provides a publicly available interface (https://nxp.com/psirt), and includes 4 steps:

- **Reporting**. The process begins when the PSIRT becomes aware of a potential security vulnerability in an NXP product. The reporter receives an acknowledgment and updates throughout the handling process.
- **Evaluation**. The PSIRT confirms the potential vulnerability, assesses the risk, determines the impact and assigns a processing priority. If the vulnerability is confirmed, the priority determines how the issue is handled throughout the remaining steps in the process.
- **Solution**. Working with PSIRT, the product team develops a solution that mitigates the reported security vulnerability. Solutions will take different forms based on the vulnerability. Because of the nature of NXP products – mostly silicon products where the firmware is in ROM -, very often the solution can only be provided in a next version of the chips and the short-term solution will consist of recommending security measures to be applied in systems using the NXP product.
- **Communication**. As said above, because of the nature of the NXP products, the solution to systems using the affected products often needs to be found in additional countermeasures in those systems. The communication on the vulnerability and solutions will in most cases be done directly towards the affected customers. For previously unknown or unreported issues, NXP will acknowledge the reporter of the issues (unless the reporter requests otherwise).

The hardware and firmware located in the on-chip ROM of SE051 cannot be updated due to their immutable nature. The JCOP operating system of the platform cannot be updated or patched after issuance. The reason is to minimize the attack surface; the possibility to abuse the operating system via the update mechanism is removed. The final product with applications has the capability of change post issuance (See Section 3.2.2). The installation of applet procedure verifies the authenticity of applet code, providing an appropriate mechanism for supporting the management of this code. The management mechanism is defined by GlobalPlatform [17][18], with proper personalization before the product field delivery.

3.1.2 Security by Design

NXP Security Process in Product Development, also referred to as the Security Maturity Process (SMP), is designed to ensure that product security is given due consideration throughout the development cycle beginning with incorporating security in the product architecture – in a concept of ‘Security-by-Design’ - and then approving Security Milestones during development. This process is integrated into NXP Business Creation

and Management (BCaM) framework which covers all harmonized processes to successfully launch New Products, and Security Milestones align with the BCaM product development project gates and milestones with the aim to ensure that security-related deliverables and reviews are planned accordingly, and eventually successfully completed for each Security Milestone, and hence for each product development gate/milestone.

BCaM process including SMP which focuses on Security by Design together with PSIRP process introduced in Section 3.1.1 has been certified against Security for Industrial Automation and Control Systems - Part 4-1: Secure Product Development Lifecycle Requirements (IEC 62443-4-1:2018) [7] (See Section 1.4).

3.2 Security Functional Requirements

SE051 fulfills the following security functional requirements:

3.2.1 Identification and Attestation of Platforms and Applications

3.2.1.1 Verification of Platform Identity

The platform provides a unique identification of the platform, including all its parts and their versions.

Conformance rationale:

RESERVED_ID_UNIQUE_ID is a BinaryFile Secure Object which holds the device unique ID in IoT Applet. This file cannot be overwritten or deleted. Furthermore, IoT Applet provides GetVersion APDU in Section 4.20 of [10]. SEMS Lite Applet version can be obtained by GET DATA APDU with tag '00DE' (see Section 3.1 of [14]). Perso Applet version can be obtained when the applet is selected by sending GP SELECT command. The JCOP platform can be identified by using the Platform ID, the FLASH ID and the Patch ID. The IDENTIFY command and the identification output for this platform are described in detail in Section 5 of [9]. The formats of version information return value are described in the corresponding guidance documents, and the return value shall match the version number provided in Section 1.2.

3.2.1.2 Verification of Platform Instance Identity

The platform provides a unique identification of that specific instantiation of the platform, including all its parts and their versions.

Conformance rationale:

SE051 provides RESERVED_ID_UNIQUE_ID secure object which cannot be overwritten or deleted as described in Section 3.3.6.6 of [10].

3.2.1.3 Attestation of Platform Genuineness

The platform provides an attestation of the “Verification of Platform Identity” and “Verification of Platform Instance Identity”, in a way that cannot be cloned or changed without detection.

Conformance rationale:

The secure channel establishment proves the possession of the authentication credential on the platform, and the version information for JCOP and the applets can be obtained with secure channel established and its authenticity is ensured (See Section 3.2.3.1).

The user can request attestation for the key or file data requested. Attestation means that the response will have a chip unique identifier, freshness, a timestamp (i.e., monotonic counter value) and a signature over the full payload (requested data, unique identifier, freshness and timestamp) in addition to the requested data as described in Section 3.3.8.2 of [10].

The signature algorithm is configurable and by default either 2048-bit RSA or 256-bit ECC, and it can be secure provisioned by NXP.

3.2.1.4 Secure Initialization of Platform

The platform ensures its authenticity and integrity during the platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to *reset*.

Refinement for IEC62443-4-2 EDR/NDR 3.14 (1) - Authenticity of the boot process [8].

Conformance rationale:

The Boot Software is executed after each reset of the platform, i.e. every time when the platform starts. It sets up the platform and does some basic configuration of the hardware based on the settings stored in memories assigned to the Super-System Mode (SSM). It is not possible to communicate with the device until this process is complete.

The Boot Software is stored in ROM memories assigned to the SSM.

The correct configuration of the platform during the boot sequence is supported by all security features. In this way the self-protection aspect and the protection from interference and tampering are implemented. The protection applies to all configuration values that are relevant.

Regarding EDR/NDR 3.14 (1), various mechanisms, e.g. code signature, apply in the boot process to verify the authenticity of the image.

3.2.1.5 Attestation of Platform State

The platform provides an attestation of the state of the platform, such that it can be determined that the platform is in a known state.

Refinement for IEC62443-4-2 CR 3.3 - Security functionality verification [8]**.**

Refinement for IEC62443-4-2 CR 3.3 (1) - Security functionality verification during normal operation [8].

Refinement for IEC62443-4-2 CR 3.4 - Software and information integrity [8].

Refinement for IEC62443-4-2 CR 3.4 (1) - Authenticity of software and information [8].

Conformance rationale:

SE051 JCOP implemented GP state defined by [16] and TriggerSelfTest and ReadState APDU are provided in Section 4.6 of [10].

Regarding CR 3.3, CR 3.3 (1), CR 3.4, CR 3.4 (1) on demand self check can be triggered (See Section 4.6.6 of [10]).

3.2.2 Product Lifecycle: Factory Reset / Install / Update / Decommission

3.2.2.1 Factory Reset of Platform

The platform can be reset to the state in which it exists when the composite product embedding the platform is delivered to the user, before any personal user data, user credentials, or user configuration is present on the platform.

Conformance rationale:

DeleteAll APDU deletes all Secure Objects, all curves and Crypto Objects except Secure Objects that are trust provisioned by NXP is as described in Section 4.20.5 of [10].

3.2.2.2 Secure Update of Platform

The platform can be updated to a newer version in the field such that the integrity, authenticity and confidentiality of the platform is maintained.

Refinement for IEC62443-4-2 EDR 2.4 - Mobile code [8].

Refinement for IEC62443-4-2 EDR 2.4 (1) - Mobile code authenticity check [8].

Refinement for IEC62443-4-2 CR 7.6 - Network and security configuration settings: [8].

Refinement for IEC62443-4-2 CR 7.6 (1) - Machine-readable reporting of current security settings: [8].

Refinement for IEC62443-4-2 CR 7.7 - Least functionality [8].

Conformance rationale:

The JCOP operating system of the platform cannot be updated or patched after issuance to minimize the attack surface. Please also refer to Section 3.1.1 for flaw reporting procedures.

The install, update and uninstall procedure of applet verifies the authenticity of applet code, providing an appropriate mechanism for supporting the management of this code. SEMS Lite Applet provides the management mechanism adapted from GlobalPlatform [17][18]

Regarding CR 7.6, CR 7.6 (1) and CR 7.7, technically it is not the application update, but the update of the application configuration, and it can be achieved by updating the policy. The applied policy can be read out by ReadAttributes APDU.

Furthermore, the Perso Applet allows secure removal of unused JCOP module.

3.2.2.3 Secure Install of Application

The application can be installed in the field such that the integrity, authenticity *and confidentiality* of the application is maintained.

Conformance rationale:

SE051 is able to install, update and uninstall applet if necessary for an application. SEMS Lite Applet provides the management mechanism adapted from GlobalPlatform [17][18]

3.2.2.4 Secure Update of Application

The application can be updated to a newer version in the field such that the integrity, authenticity and confidentiality of the application is maintained.

Conformance rationale:

See Section 3.2.2.3.

3.2.2.5 Secure Uninstall of Application

The application can be uninstalled in the field such that all application data *with the exception of TrustProvisioned Objects* is destroyed.

Conformance rationale:

See Section 3.2.2.3.

Furthermore, the Perso Applet allows secure removal of unused JCOP module.

3.2.3 Security Communication

3.2.3.1 Secure Communication Support

The platform provides the application with one or more secure communication channel(s).

The secure communication channel authenticates *off-card entity within a logically secure environment* [16] and protects against attacks including *disclosure, modification, replay* of messages between the endpoints, using *AESKey Session*.

The secure communication channel authenticates *off-card entity within a logically secure environment* and protects against attacks including *disclosure, modification, replay* of messages between the endpoints, using *ECKey Session* [22].

Conformance rationale:

SE051 supports the secure channel protocols AESKey Session and ECKey Session.

3.2.3.2 Secure Communication Enforcement

The platform ensures the application can only communicate with *offcard entities with possession of authentication credential* over the secure communication channel(s) supported by the platform using *SCP02, SCP03 and FastSCP*.

Refinement for IEC62443-4-2 CR 1.9 - Strength of public key authentication [8].

Refinement for IEC62443-4-2 CR 1.10 - Authenticator feedback [8].

Refinement for IEC62443-4-2 CR 1.11 - Unsuccessful login attempts [8].

Refinement for IEC62443-4-2 CR 1.14 - Strength of symmetric key-based authentication [8].

Refinement for IEC62443-4-2 CR 2.6 - Remote session termination [8].

Refinement for IEC62443-4-2 CR 2.7 - Concurrent session control [8].

Refinement for IEC62443-4-2 CR 3.5 - Input validation [8].

Refinement for IEC62443-4-2 CR 3.7 - Error handling [8].

Refinement for IEC62443-4-2 CR 3.8 - Session integrity [8].

Conformance rationale:

SE051 enforces the secure channel protocols SCP02 and SCP03 as defined in GlobalPlatform 2.3 [16] for GP content management.

SE051 also enforces Applet Secure Channel with SCP03 or FastSCP according to the policy configured and can be mandated by calling SetPlatformSCPRequest as described in Section 3.14 of [10]. This fulfills CR3.8.

Regarding CR 1.9, FastSCP employs public key authentication with 256-bit ECC to setup session key with AES128 bits .

Regarding CR 1.10 and CR 3.7, in case of authentication failure or error, returned error code will not disclose exploitable information. (see Section 4.3.1 and Section 4.5.1.1 of [10])

Regarding CR1.11, The maximum authentication attempt can be configured (see Section 3.3.3 of [10]).

Regarding CR 1.14, SCP03 employs AES for authentication.

Regarding CR 2.6, Session closure conditions are described in Section 3.7.5 of [10].

Regarding CR 2.7, The maximum number of applet sessions is two. (see Section 4.3.2 of [10])

Regarding CR 3.5, the input is APDU based and APDU format is introduced in Section 4.1 of [10] and invalid input will yield error code return.

3.2.4 Extra Attacker Resistance

3.2.4.1 Physical Attack Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the functional requirements, ensuring that the functional requirements are not compromised.

Conformance rationale:

Various special features for physical attack resistance have been implemented in the design and layout of the circuitry, for instance shielding, glue logic, sensors, secure hardened components with side channel and fault injection protection, etc. All above mentioned functions and effectiveness against attacks are comprehensively tested by NXP and independent 3rd party evaluator.

3.2.4.2 Software Attacker Resistance: Isolation of Platform

The platform provides isolation between the application and itself, such that an attacker able to run code as an application on the platform cannot compromise any other claimed security functional requirements.

Conformance rationale:

The platform implements the Java Card Virtual Machine [20], Java Card Runtime Environment [21], Java Card API [19], configuration management and Card Content Management [16] according to corresponding specifications, where firewall policy is defined along with other security measures, which ensures isolation between the operating system and the application

3.2.4.3 Software Attacker Resistance: Isolation of Platform Parts

The platform provides isolation between platform parts, such that an attacker able to run code in *Secure box* can compromise neither the integrity and confidentiality of *JCRE* nor the provision of any other security functional requirements.

Refinement for IEC62443-4-2 CR 2.1 (2) - Permission mapping to roles [8].

Conformance rationale:

The platform implements the Java Card Virtual Machine [20], Java Card Runtime Environment [21], configuration management and Card Content Management [16] according to corresponding specifications, which ensures isolation of the platform parts.

The JCOP also introduce module concept and a module can be removed without compromising security and function of others.

Furthermore, the IoT Applet in SE051 implements policies and access rules to defined restrictions and working conditions for objects and sessions. (Section 3.8 of [10]).

Regarding to CR2.1 (2), the policies can be assigned to UserID.

3.2.4.4 Software Attacker Resistance: Isolation of Application Parts

The platform provides isolation between parts of the application, such that an attacker able to run code as one of the *applet* cannot compromise the integrity and confidentiality of the other application parts.

Conformance rationale:

The platform implements the Java Card Virtual Machine [20], Java Card Runtime Environment [21], configuration management and Card Content Management [16] according to corresponding specifications, which ensures isolation of the application parts when new applications and its parts are implemented by installing new applet.

3.2.5 Cryptographic Functionality

3.2.5.1 Cryptographic Operation

The platform provides the application with *encryption and decryption* functionality with *DES* as specified in *NIST SP 800-67* for key length *56,112, 168 bit* and modes *ECB, CBC*.

The platform provides the application with *encryption and decryption* functionality with *AES* as specified in *NIST FIPS 197* for key length *128, 192, 256 bit* and modes *ECB, CBC, CTR, GCM, CCM*.

The platform provides the application with *signature generation and verification* functionality with *ECDSA* as specified in *ANSI X9.62* for key length *160, 192, 224, 256, 384, 512, 521 bit* and modes *none*.

The platform provides the application with *signature generation and verification* functionality with *EdDSA* as specified in *RFC8032* for key length *255 bit* and modes *none*.

The platform provides the application with *signature generation* functionality with *ECDAA* as specified in *TPM rev 2.00* for key length *256 bit* and modes *none*.

The platform provides the application with *shared secret* functionality with ECDH as specified in *NIST FIPS 800-56A* for key length *160, 192, 224, 256, 384, 512, 521 bit* and modes *none.*

The platform provides the application with *encryption, decryption, signature generation and verification* functionality with *RSA* as specified in *PKCS#1* for key length *512, 1024, 1152, 2048, 3072, 4096 bits* and modes *EME-OAEP and EMSA-PSS*.

The platform provides the application with *hashing* functionality with *SHA 1, SHA 224, SHA 256, SHA 384, SHA 512* as specified in *FIPS180-4* for key length *160, 224, 256, 384, 512* and modes *none*.

The platform provides the application with *MAC generation and verification* functionality with *SHA 1, SHA 256, SHA 384, SHA 512* as specified in *RFC2104* for key length *1-2048 bits* and modes *none*.

The platform provides the application with *MAC generation and verification* functionality with *AES* as specified in *RFC4493* for key length *128 bits* and modes *CMAC*.

The platform provides the application with *MAC generation and verification* functionality with *DES, TDES* as specified in *ISO 9797-1* for key length *56 or 112 bits* and modes *Retail-MAC, CBC-MAC and CMAC*.

The platform provides the application with *key derivation* functionality with *SHA 1, SHA 256, SHA 384, SHA 512* as specified in *RFC5869* for key length *1-2048 bits* and modes *HKDF*.

The platform provides the application with *key derivation* functionality with *xxxx* as specified in *RFC8018* for key length *1-2048 bits* and modes *PBKDF2*.

The platform provides the application with *key derivation* functionality with *SHA 1, SHA 256, SHA 384, SHA 512* as specified in *RFC5246* for key length *128, 256, 384, 512 bits* and modes *TLS PRF*.

The platform provides the application with *key derivation* functionality with *AES* as specified in [15] for key length *128 bits* and modes *MIFARE DESFire EV2 (S mode)*.

Operation	Algorithm	Specification	Key Lengths	Modes
Encryption and decryption	DES, TDES [1]	NIST SP 800-67	56, 112, 168	ECB, CBC
Encryption and decryption	AES	NIST FIPS 197	128, 192, 256	ECB, CBC, CTR,
Authenticated encryption with associated data (AEAD)	AES	ISO/IEC 19772	128, 192, 256	GCM, CCM
Signature generation and verification	ECDSA	ANSI X9.62	160, 192, 224, 256, 384, 512, 521	-
Signature generation and verification	EdDSA [2]	RFC8032	255	-
Signature generation	ECDAA	TPM rev 2.00	256	-
Shared secret	ECDH	NIST FIPS 800-56A	160, 192, 224, 256, 384, 512, 521	-
Encryption, decryption, signature generation and verification	RSA	PKCS#1	512, 1024, 1152, 2048, 3072, 4096	EME-OAEP, EMSA-PSS

Operation	Algorithm	Specification	Key Lengths	Modes
Hashing	SHA 1 [3], SHA 224, SHA 256, SHA 384, SHA 512 [4]	FIPS 180-4	160, 224, 256, 384, 512	-
MAC generation and verification	SHA 1 [3], SHA 256, SHA 384, SHA 512	RFC2104	1-2048	HMAC
MAC generation and verification	AES	RFC4493	128	CMAC
MAC generation and verification	DES [1]	ISO 9797-1	56, 112	CMAC, CBC-MAC, Retail MAC
Key derivation	SHA 1 [3], SHA 256, SHA 384, SHA 512	RFC5869	1-2048	HKDF
Key derivation	SHA 1 [3]	RFC8018	1-2048	PBKDF2
Key derivation	SHA 1 [3], SHA 256, SHA 384, SHA 512	RFC5246	128, 256, 384, 512	TLS PRF
Key derivation	AES	[15]	128	MIFARE DESFire EV2 (S mode)

[1] The DES encryption algorithm is deprecated by many sources due to its small key size and further reduction in complexity under certain conditions. The TDEA (Triple Data Encryption Algorithm), also known as Triple DES (3DES), is considered to provide only 80 bits security (when used with 2 keys) or 112 bits (when used with 3 keys). It has been deprecated by NIST in 2017.

[2] Recent research has concluded that deterministic signature algorithms, such as EdDSA (RFC 8032), by construction, have theoretical weaknesses against certain instances of side-channel and fault injection attacks and that the attacks are practically feasibly in some environments.

[3] The SHA-1 hash algorithm is deprecated by various sources. As of 2020, a chosen-prefix collision can be found with a complexity of $2^{63.4}$. Due weaknesses in the utilized SHA-1 algorithms, the use of HMAC in conjunction with these functions (HMAC-SHA1) is not recommended.

[4] Members of the SHA-2 family of hash functions (SHA-224, SHA-256, SHA-384, SHA-512) are, under certain circumstances, susceptible to length extension attacks. Such attacks may be applicable if SHA-2 is used in (non-recommended) keyed hash constructions. If SHA-2 is used in a HMAC construction (RFC 2104), length extension attacks are deemed non-applicable.

Conformance rationale:

The various cryptographic operations supported by SE051 is documented in Section 4 of [10].

Footnotes are provided to indicate primitives/algorithms with known limitation, customers are expected to consider various information sources for up-to-date recommendations and/or deprecations of cryptographic algorithms and protocols, to select security features and key lengths that best meet rules, regulations, and standards of the intended end application.

3.2.5.2 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in *RSA* as specified in *PKCS#1* for key lengths *512, 1024, 1152, 2048, 3072, 4096 bits.*

The platform provides the application with a way to generate cryptographic keys for use in *ECC* as specified in *ANSI X9.62* for key lengths *160, 192, 224, 256, 384, 512, 521 bit.*

Conformance rationale:

WriteECKey and WriteRSAKey APDU with key value absent will trigger key generation (see Section 4.7.1 of [10]).

Also, shared secret and key derivation algorithms are supported as described in Section 3.2.5.1.

3.2.5.3 Cryptographic KeyStore

The platform provides the application with a way to store *cryptographic keys, PINs* such that not even the application can compromise the *authenticity, integrity, confidentiality* of this data. This data can be used for the cryptographic operations *encryption, decryption, signature generation, MAC generation, key derivation, shared secret generation*.

Refinement for IEC62443-4-2 CR 1.1 - Human user identification and authentication [8].

Refinement for IEC62443-4-2 CR 1.1 (1) - Unique identification and authentication [8].

Refinement for IEC62443-4-2 CR 1.1 (2) - Multifactor authentication for all interfaces [8].

Refinement for IEC62443-4-2 CR 1.3 - Account management [8].

Refinement for IEC62443-4-2 CR 1.4 - Identifier management [8].

Refinement for IEC62443-4-2 CR 1.5 - Authenticator management [8].

Refinement for IEC62443-4-2 EDR/NDR 3.12 - Provisioning product supplier roots of trust [8].

Refinement for IEC62443-4-2 EDR/NDR 3.13 - Provisioning asset owner roots of trust [8].

Conformance rationale:

Cryptographic keys are stored as Secure Objects in SE051 (see Section 3.3 of [10]).

Regarding CR1.1 and CR 1.1 (1), SE051implements UserID (see Section 3.3.1.9 of [10]) which logically group secure objects and policy can be configured that authentication is needed to open a session. UserID is up to 16 bytes which supports Unique Identification.

Regarding CR 1.1 (2), different credentials can be stored including keys and PINs, and furthermore SE051 can be used as a MIFARE DESFire card reader and store the master key.

Regarding CR 1.3 and 1.4, security objects includes UserID can be created, managed and deleted and UserID is up to 16 bytes. (see Section 4.7 of [10]).

Regarding CR 1.5, authenticator stored in SE051 is secure objects and can be managed.

Regarding EDR/NDR 3.12 and 3.13, SE051 has trust provision service.

3.2.5.4 Cryptographic Random Number Generation

The platform provides the application with a way based on *physical noise* to generate random numbers to as specified in *AIS31 PTG.2* [2].

The platform provides the application with a way based on *deterministic* to generate random numbers to as specified in *AIS 20 DRG.3* [2].

The platform provides the application with a way based on *hybrid-deterministic* to generate random numbers to as specified in *AIS 20 DRG.4* [2].

Conformance rationale:

SE051 provides deterministic random number generator that implements DRG.3 and hybrid deterministic random number generator that implements DRG.4. The random seed is from Hardware RNG implements PTG.2. GetRandom APDU is defined in Section 4.20.4 in [10].

3.2.6 Compliance Functionality

3.2.6.1 Secure Encrypted Storage

The platform ensures that all data stored by the application, except for *none*, is encrypted as specified in *proprietary algorithm* with a platform instance unique key of key length *proprietary information*.

Conformance rationale:

All types of memory in SE051 are encrypted by hardware mechanism with address scrambling and integrity protection.

3.2.6.2 Residual Information Purging

The platform ensures that *class instances (objects), transient arrays, and global arrays*, with the exception of *none*, is erased using the method specified in [21] before the memory is (re)used by the platform or application again and before an attacker can access it.

Refinement for IEC62443-4-2 CR 4.2 (2) - Erase verification [8].

Conformance rationale:

SE051 provides the object management for Java objects which are processed by JCVM. It provides object creation and garbage collection according to the Java Card Runtime Environment Specification [21].

SE051 also provides deletion of memory for transient arrays, global arrays, and logical channels according to the Java Card Runtime Environment Specification [21].

Also see Section 3.2.2.1 for DeleteAll APDU.

Regarding CR 4.2 (2), Various APDU can verify the erasure of an object, e.g. ReadIDList, CheckObjectExists, ReadObject, ReadAttributes.

3.2.6.3 Reliable Index

The platform implements a strictly increasing function.

Conformance rationale:

Applet provides GetTimestamp APDU as described in Section 4.20.2 of [10].

4 Mapping and Sufficiency Rationales

4.1 SESIP3 Sufficiency

Assurance Class	Assurance Family	Covered By	Rationale
ASE: Security target evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in Section 1.1, the TOE reference in Section 1.2, the TOE overview and description in Section 1.5.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in Section 2 refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	Section 3	All SFRs in this ST are taken from [1]. SFR "Identification of Platform Type" is included. SFR "Secure Update of Platform" is mentioned but refers to ALC_FLR.2.
	ASE_TSS.1 TOE Summary Specification	Section 3	All SFRs are listed per definition, and for each SFR the implementation and verification is defined in the SFR.
ADV: Development	ADV_FSP.4 Complete functional specifications	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Section 1.3	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Section 1.3	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ALC_CMS.1 TOE CM Coverage	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.

Assurance Class	Assurance Family	Covered By	Rationale
	ALC_FLR.2 Flaw reporting procedures	Section 3.1.1	The flaw reporting and remediation procedure is described.
ATE: Test	ATE_IND.1 Independent testing: conformance	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis	N.A. A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.	The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Enhanced-Basic.

4.2 IEC62443-4-2 Mapping

The IEC62443-4-2 Sufficiency Mapping has been organized in the following way:

- SE051 as a subcomponent, fulfills subset of IEC62443-4-2 requirements;
- SE051 provides services which support the overall component fulfilling IEC62443-4-2 requirements.

4.2.1 Sufficiency of Subset of IEC62443-4-2 Requirements

SE051, as a subcomponent of a targeted IACS component, thus it fulfills subset of the IEC62443-4-2 requirements, which provides support for the component.

Note SE051 is not targeted as a standalone device and therefore not targeted to comply with the whole set of IEC62443-4-2. The applicable requirements and the mapping of SFR is provided to Table 3.

IEC62443-4-2 requires component developed and supported following the secure product development process described in IEC 62443-4-1. The development of SE051 follows BCaM which is IEC62443-4-1 Certified.

Table 3. IEC62443-4-2 requirements Sufficiency

Req.	Description	SL-C				Covered by
		1	2	3	4	
CCSC 4	Software development process: IEC62443-4-1 Compliance	x	x	x	x	Security Assurance Requirements
CR 1.1	Human user identification and authentication	x	x	x	x	Cryptographic KeyStore [1]
CR 1.1 (1)	Unique identification and authentication		x	x	x	Cryptographic KeyStore [1]
CR 1.1 (2)	Multifactor authentication for all interfaces			x	x	Cryptographic KeyStore [1]

Table 3. IEC62443-4-2 requirements Sufficiency...*continued*

Req.	Description	SL-C				Covered by
		1	2	3	4	
CR 1.2	Software process and device identification		x	x	x	Verification of Platform Identity & Attestation of Platform Genuineness
CR 1.2 (1)	Unique identification and authentication			x	x	Verification of Platform Instance Identity & Attestation of Platform Genuineness
CR 1.3	Account management	x	x	x	x	Cryptographic KeyStore [1]
CR 1.4	Identifier management	x	x	x	x	Cryptographic KeyStore [1]
CR 1.5	Authenticator management	x	x	x	x	Cryptographic KeyStore [1]
CR 1.5 (1)	Hardware security for authenticators			x	x	Physical Attack Resistance & Cryptographic KeyStore [1]
NDR 1.6	Wireless access management	x	x	x	x	Verification of Platform Identity & Attestation of Platform Genuineness
NDR 1.6 (1)	Unique identification and authentication		x	x	x	Verification of Platform Instance Identity & Attestation of Platform Genuineness
CR 1.9	Strength of public key-based authentication		x	x	x	Secure Communication Enforcement [1]
CR 1.9 (1)	Hardware security for public key based authentication			x	x	Physical Attack Resistance & Secure Communication Enforcement [1]
CR 1.10	Authenticator feedback	x	x	x	x	Secure Communication Enforcement [1]
CR 1.11	Unsuccessful login attempts	x	x	x	x	Secure Communication Enforcement [1]
CR 1.14	Strength of symmetric key based authentication		x	x	x	Secure Communication Enforcement
CR 1.14 (1)	Hardware security for symmetric key based authentication			x	x	Physical Attack Resistance & Secure Communication Enforcement [1]
CR 2.1	Authorization enforcement	x	x	x	x	Secure Communication Enforcement
CR 2.1 (1)	Authorization enforcement for all users		x	x	x	Secure Communication Enforcement
CR 2.1 (2)	Permission mapping to roles		x	x	x	Software Attacker Resistance: Isolation of Application Parts [1]
EDR 2.4	Mobile code	x	x	x	x	Secure Install of Application
EDR 2.4 (1)	Mobile code authenticity check		x	x	x	Secure Install of Application
CR 2.6	Remote session termination		x	x	x	Secure Communication Enforcement [1]
CR 2.7	Concurrent session control			x	x	Secure Communication Enforcement [1]
CR 3.1	Communication integrity	x	x	x	x	Secure Communication Enforcement
CR 3.1 (1)	Communication authentication		x	x	x	Secure Communication Enforcement
EDR 3.2	Protection from malicious code	x	x	x	x	Secure Install of Application
CR 3.3	Security functionality verification	x	x	x	x	Attestation of Platform State [1]
CR 3.3 (1)	Security functionality verification during normal operation				x	Attestation of Platform State [1]

Table 3. IEC62443-4-2 requirements Sufficiency*...continued*

Req.	Description	SL-C				Covered by
		1	2	3	4	
CR 3.4	Software and information integrity	x	x	x	x	Attestation of Platform State [1]
CR 3.4 (1)	Authenticity of software and information		x	x	x	Attestation of Platform State [1]
CR 3.5	Input validation	x	x	x	x	Secure Communication Enforcement [1]
CR 3.7	Error handling	x	x	x	x	Secure Communication Enforcement
CR 3.8	Session integrity		x	x	x	Secure Communication Enforcement [1]
EDR/NDR 3.10	Support for updates	x	x	x	x	Secure Update of Platform & Secure Update of Application
EDR/NDR 3.10 (1)	Update authenticity and integrity		x	x	x	Secure Update of Platform & Secure Update of Application
EDR/NDR 3.11	Physical tamper resistance and detection		x	x	x	Physical Attack Resistance
EDR/NDR 3.12	Provisioning product supplier roots of trust		x	x	x	Cryptographic KeyStore [1]
EDR/NDR 3.13	Provisioning asset owner roots of trust		x	x	x	Cryptographic KeyStore [1]
EDR/NDR 3.14	Integrity of the boot process	x	x	x	x	Secure Initialization of Platform
EDR/NDR 3.14 (1)	Authenticity of the boot process		x	x	x	Secure Initialization of Platform [1]
CR 4.1	Information confidentiality	x	x	x	x	Secure Communication Enforcement
CR 4.2	Information persistence		x	x	x	Residual Information Purging
CR 4.2 (2)	Erase verification			x	x	Residual Information Purging [1]
CR 4.3	Use of cryptography	x	x	x	x	Security Communication & Cryptographic Functionality
CR 7.6	Network and security configuration settings	x	x	x	x	Secure Update of Platform [1]
CR 7.6 (1)	Machine-readable reporting of current security settings			x	x	Secure Update of Platform [1]
CR 7.7	Least functionality	x	x	x	x	Secure Update of Platform [1] & Secure Uninstall of Application

[1] Corresponding refinement applies for the security functional requirement to fulfill the IEC62443 requirement.

4.2.2 Features for Final Product towards IEC62443-4-2 Compliance

SE051 is deigned to be used as a part of system, or in IEC62443-4-2 terms, as a subcomponent of an IEC62443-4-2 component. The following table provides mapping of SE051 features described in SESIP terms towards IEC62443-4-2 compliance for a product with SE051 integrated, or in other words, the features described in the SESIP SFR can be safely utilized as part of the IEC62443-4-2 compliance of the final product.

Note it is up to the integrator on whether a feature is used for IEC62443-4-2 compliance and correct utilization of the feature, and this session is for guidance and informative purpose, but not in the scope of the SESIP evaluation. For example, SE051 has unique identification as described in Verification of Platform Instance Identity and can be used to fulfill CR 1.2 (1), but the integrator may use another identifier available from another subcomponent of the product. Taking CR 2.12 Non-repudiation mapping to Cryptographic Functionality for another instance, a component can use ECDSA as described in Cryptographic Operation to sign a log with keys protected by Cryptographic KeyStore and random nonce from Cryptographic Random Number Generation implicitly, but the integrator may implement other non-repudiation mechanism and/or not use all SE051 features to perform a sub task. The integrator is responsible on how to design and architecture a component to fulfill IEC62443 requirements leveraging SE051 integrated to fit the purpose and security requirements.

Table 4. SE051 Services for Final Product towards IEC62443-4-2 Compliance

Req.	Description	SL-C				Supported by
		1	2	3	4	
CR 1.2	Software process and device identification		x	x	x	Verification of Platform Identity & Attestation of Platform Genuineness
CR 1.2 (1)	Unique identification and authentication			x	x	Verification of Platform Instance Identity & Attestation of Platform Genuineness
CR 1.5	Authenticator management	x	x	x	x	Cryptographic KeyStore
CR 1.5 (1)	Hardware security for authenticators			x	x	Physical Attack Resistance & Cryptographic KeyStore [1]
NDR 1.6	Wireless access management	x	x	x	x	Cryptographic Operation: PBKDF2
NDR 1.6 (1)	Unique identification and authentication		x	x	x	Verification of Platform Instance Identity & Attestation of Platform Genuineness
CR 1.7	Strength of password-based authentication	x	x	x	x	Cryptographic Operation: SHA & PBKDF2
CR 1.8	Public key infrastructure certificates		x	x	x	Cryptographic Functionality; Secure Encrypted Storage
CR 1.9	Strength of public key-based authentication		x	x	x	Cryptographic Functionality
CR 1.9 (1)	Hardware security for public key based authentication			x	x	Physical Attack Resistance & Cryptographic Functionality
CR 1.10	Authenticator feedback	x	x	x	x	Secure Communication Enforcement [1]
CR 1.11	Unsuccessful login attempts	x	x	x	x	Secure Communication Enforcement [1]; Reliable Index
CR 1.14	Strength of symmetric key based authentication		x	x	x	Cryptographic Functionality
CR 1.14 (1)	Hardware security for symmetric key based authentication			x	x	Physical Attack Resistance & Cryptographic Functionality
EDR 2.4	Mobile code	x	x	x	x	Cryptographic Functionality
EDR 2.4 (1)	Mobile code authenticity check		x	x	x	Cryptographic Functionality
CR 2.8	Auditable events	x	x	x	x	Reliable Index

Table 4. SE051 Services for Final Product towards IEC62443-4-2 Compliance *...continued*

Req.	Description	SL-C				Supported by
		1	2	3	4	
CR 2.9	Audit storage capacity	x	x	x	x	Secure Encrypted Storage
CR 2.12	Non-repudiation	x	x	x	x	Cryptographic Functionality
CR 2.12 (1)	Non-repudiation for all users				x	Cryptographic Functionality
CR 3.1	Communication integrity	x	x	x	x	Cryptographic Functionality
CR 3.1 (1)	Communication authentication		x	x	x	Cryptographic Functionality
EDR 3.2	Protection from malicious code	x	x	x	x	Cryptographic Functionality
CR 3.4	Software and information integrity	x	x	x	x	Cryptographic Functionality; Secure Encrypted Storage
CR 3.4 (1)	Authenticity of software and information		x	x	x	Cryptographic Functionality; Secure Encrypted Storage
CR 3.4 (2)	Automated notification of integrity violations			x	x	Cryptographic Functionality
CR 3.8	Session integrity		x	x	x	Cryptographic Functionality
CR 3.9	Protection of audit information		x	x	x	Cryptographic Functionality; Secure Encrypted Storage
EDR/NDR 3.10 (1)	Update authenticity and integrity		x	x	x	Cryptographic Functionality
EDR/NDR 3.11	Physical tamper resistance and detection		x	x	x	Physical Attack Resistance
EDR/NDR 3.12	Provisioning product supplier roots of trust		x	x	x	Cryptographic KeyStore [1]
EDR/NDR 3.13	Provisioning asset owner roots of trust		x	x	x	Cryptographic KeyStore [1]
EDR/NDR 3.14	Integrity of the boot process	x	x	x	x	Cryptographic Functionality; Secure Encrypted Storage
EDR/NDR 3.14 (1)	Authenticity of the boot process		x	x	x	Cryptographic Functionality; Secure Encrypted Storage
CR 4.1	Information confidentiality	x	x	x	x	Cryptographic Functionality; Secure Encrypted Storage
CR 4.2	Information persistence		x	x	x	Residual Information Purging
CR 4.2 (2)	Erase verification			x	x	Residual Information Purging[1]
CR 4.3	Use of cryptography	x	x	x	x	Cryptographic Functionality
CR 7.3 (1)	Backup integrity verification		x	x	x	Cryptographic Functionality

[1] Security functional requirement with corresponding refinement supports final product towards IEC62443 compliance.

5 Bibliography

5 . 1 Evaluation Documents

[1] GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.0, GP_FST_070.

[2] A proposal for: Functionality classes for random number generators, Wolfgang Killmann, T-Systems GEI GmbH, Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, 18 September 2011.

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017.

[4] Security IC Platform Protection Profile with Augmentation Packages, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014.

[5] Java Card System - Open Configuration Protection Profile, December 2017, Version 3.0.5, published by Oracle, Inc. (BSI-CC-PP-0099-2017)..

[6] IEC TS 62443-1-1, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, edition 1.0, 2009, the International Electrotechnical Commission (IEC).

[7] IEC 62443-4-1, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements, edition 1.0, 2018, the International Electrotechnical Commission (IEC).

[8] IEC 62443-4-2, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components, edition 1.0, 2019, the International Electrotechnical Commission (IEC).

5 . 2 Developer Documents

[9] JCOP 4.7 SE051, User manual for JCOP 4.7 SE051, Rev. 1.2, DocNo 581812, NXP Semiconductors.

[10] AN12543 SE051 IoT applet APDU Specification, Rev. 2.0, NXP Semiconductors.

[11] AN12730 SE051 - User Guidelines, Rev 1.0, NXP Semiconductors.

[12] SE051 - User Guideline Addendum, Rev 1.0, NXP Semiconductors.

[13] SE05xConfig APDU specification, API description SE05x Config Applet, Rev 1.0, NXP Semiconductors.

[14] SEMS Lite v1.x.x.11JxR Secure Element Management Service Lite Application, User Manual Rev 0.3, NXP Semiconductors.

5 . 3 Standards

[15] AN10922 Symmetric key diversifications, rev 2.2, NXP Semiconductors..

[16] GlobalPlatform Card Specification 2.3, GPC_SPE_034, GlobalPlatform Inc., October 2015.

[17] Executable Load File Upgrade, GPCS 2.3 - Amendment H v1.1, GPC_SPE_120, GlobalPlatform Inc., March 2018.

[18] Secure Element Management Service, GPCS 2.3 - Amendment I, GPC_SPE_121, GlobalPlatform Inc., March 2018.

[19] Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., Oracle, May 2015.

[20] Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.5., Oracle, May 2015.

[21] Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0.5., Oracle, May 2015.

[22] 'FastSCP' Secure Channel Protocol, Rev 1.0, 2015, Doc ID 327810,NXP Semiconductors.

6 Legal information

6.1 Definitions

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

6.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

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

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

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

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.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

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.

Non-automotive qualified products — Unless this data sheet 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 is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

6.3 Trademarks

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

Tables

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: 18 December 2020