SE050

SESIP Security Target

Rev. 1.6 — 19 December 2019

Evaluation document
COMPANY PUBLIC

Document information

Information	Content
Keywords	SESIP, Security Target, ICA, SE050
Abstract	Evaluation of the SE050 developed and provided by NXP Semiconductors, BL STI, according to SESIP Assurance Level 4 (SESIP4), and compliant to ICA IoT Security Level 3

Revision History

Rev.	Date	Description
1.0	2019-09-25	First version.
1.1	2019-10-23	Added AVA_VAN.4 in Methodical Vulnerability Analysis (AVA_VAN.4) per evaluator feedback.
1.2	2019-11-07	Updated to cope with updated SESIP ICA PP (including Methodical Vulnerability Analysis (AVA_VAN.4) Section Removed) from Security Target.
1.3	2019-11-19	Updated with evaluator feedback.
1.4	2019-12-04	Updated with evaluator feedback; added compliancy to SESIP PPs [3] and [4].
1.5	2019-12-18	Updated with certifier feedback.
1.6	2019-12-19	Updated with certifier and evaluator feedback.

1 Introduction

This Security Target describes the SE050 platform that is evaluated according to Security Evaluation Standard for IoT Platforms, version 1.3 [1], SESIP Profile: ICA IoT Security requirements level 3 [2], SESIP Profile: ICs SOGIS-CC certified against PP0084 [3], and SESIP Profile: platforms SOGIS-CC certified against JavaCard 3.0.5 [4]. The security properties are described in Section 3 of this document, and will be uphold by the platform when the objectives for the environment (described in Section 2) are fulfilled by the platform consumer.

1.1 ST Reference

SE050, SESIP Security Target, Revision 1.6, NXP Semiconductors, 19 December 2019.

1.2 Platform Reference

Table 1. Platform Reference

Reference	Value
Platform Name	SE050
Platform Version	N7121 B1 Test Software 9.2.3 Booth Software 9.2.3 Firmware 9.2.3 Library Interface 9.2.3 Flashloader OS 1.2.5 System mode OS 13.2.3 Crypto Library 0.7.6 JCOP 4 SE050 v4.7 R2.00.11
Platform Identification	SE050
Platform Type	Secure Element with Java Card Operating System with GlobalPlatform Framework

1.3 Guidance Documents

The following documents are included with the platform:

Table 2. Guidance Documents

Document	Reference
User Manual	JCOP 4 SE050, User manual for JCOP 4 SE050, Rev. 1.2, DocNo 500312, 20190531, NXP Semiconductors [7]
SESIP ST	SE050, SESIP Security Target, Revision 1.6, NXP Semiconductors, 19 December 2019.
GP Card Specification	GlobalPlatform Card Specification 2.3, GPC_SPE_034, GlobalPlatform Inc., October 2015 [11]

Document	Reference
JavaCard Specifications	Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., Oracle, May 2015 [12] Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.5., Oracle, May 2015 [13] Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0.5., Oracle, May 2015 [14]

1.4 Platform Overview and Description

The EdgeLock SE050 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 Micro Controller and a software stack which is stored on the Micro Controller and which can be executed by the Micro Controller. A block diagram of the IC hardware is depicted in Figure 2.

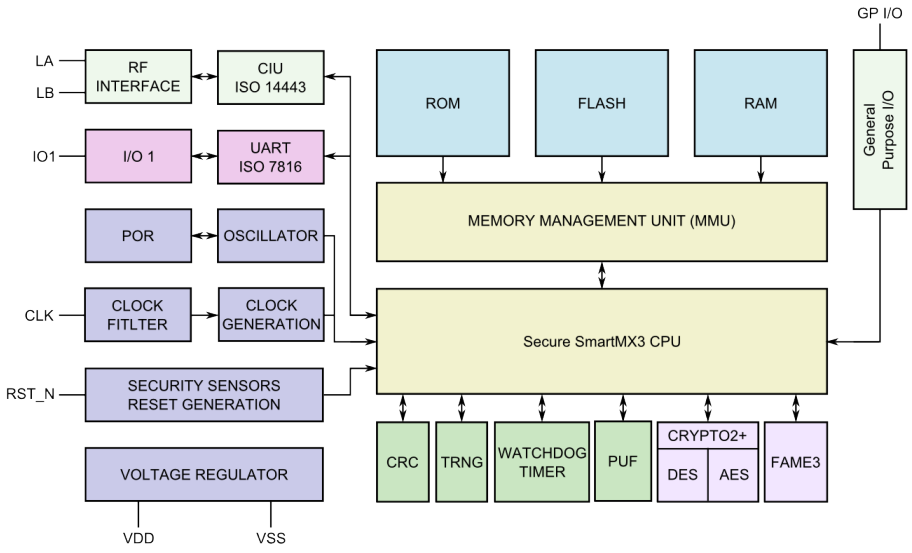

Figure 1. Components of the platform

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

- Firmware for booting and low level functionality of the Micro Controller (MC FW) like writing to flash memory. This includes software for implementing cryptographic operations, called Crypto Library.
- Software for implementing a Java Card Virtual Machine [13], a Java Card Runtime Environment [14] and a Java Card Application Programming Interface [12], called JCVM, JCRE and JCAPI.
- Software for implementing content management according to GlobalPlatform [11], called GlobalPlatform (GP) Framework.

- Software for executing native libraries, called Secure Box.

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 Micro Controller Firmware (MC FW). The platform uses one or more communication interfaces to communicate with its environment.

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 Librarys 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.

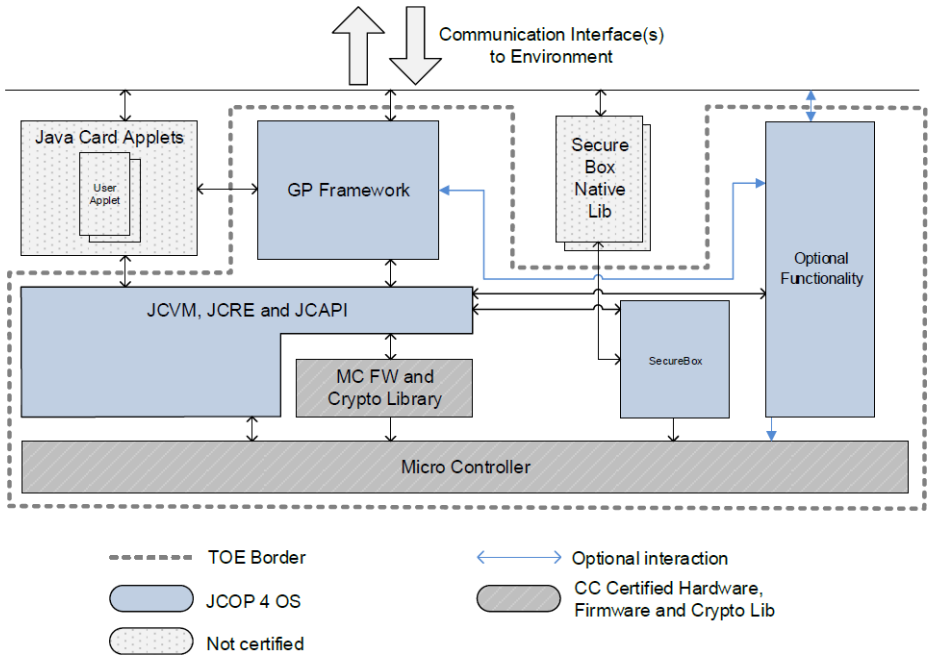

Figure 2. Components of the platform

The main security features of the platform are listed in Section 3 of this document.

1.4.1 Physical Scope of the Platform

The physical scope is the SE050 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.

1.4.2 Logical Scope of the Platform

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

1.4.3 Required non-Platform Hardware/Software/Firmware

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

1.4.4 Additional Information (Required by ICA, not covered by SESIP)

The platform provides the following hardware communication interfaces as required by Ref. [5] section 6.2 Hardware Communication Interface Requirements:

- ISO/IEC 7816 [8]
- ISO/IEC 14443 Type A [9]
- T1 over I2C [10]

The platform provides the cryptographic (security) algorithms as required by [5] in section 6.3 Chip Security Algorithm Requirements, see the SFRs Section 3.2.5.1.

The platform provides the following reliability as required by [5] section 6.4 Chip Reliability Requirements:

- Working temperature: Standard: -25 ~ 85 °C; Extended -40 ~ 105 °C.
- FLASH data retention time: min 25 years[1].
- Intrinsic FLASH endurance: min 1×10^5; typical 5×10^5.
- Electrostatic discharge voltage (Human Body Model) ± 2.0 kV.

1 T_{amb} = 55 °C

2 Security Objectives for the Operational Environment

In order for the platform to fulfil its security requirements, the operational environment (technical or procedural) must fulfil the following objectives as described in Section 6 of the User Manual [7] and this section:

- No applet loaded post-issuance shall contain native methods.
- All the bytecodes are expected verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time (see Section 6.3 of [7]). Additionally, the applet shall follow all the recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform.
- For application code loaded pre-issuance, evaluated technical measures implemented by the platform or audited organizational measures must ensure that loaded application has not been changed since the code verifications required (see Section 6.3 of [7]).
  For application code loaded post-issuance and verified off-card according to the code verification requirements, the verification authority shall provide digital evidence to the platform that the application code has not been modified after the code verification and that he is the actor who performed code verification.
  For application code loaded post-issuance and partially or entirely verified on-card, technical measures must ensure that the verification required are performed. On-card bytecode verifier is not in the scope.
- The operational environment is expected to support and use the secure communication protocols offered by the platform (see Section 6.2 of [7]).
- The keys which are stored outside the platform and which are used for secure communication and authentication between platform and environment are expected to be protected for confidentiality and integrity in their own storage environment (see Section 6.2 of [7]).
- Security procedures are expected to be used after delivery of the platform by the platform Manufacturer up to delivery to the end consumer to maintain confidentiality and integrity of the platform and of its manufacturing and test data (see Section 6.2 of [7]).
- The application provider is expected as a trusted actor that provides basic or secure application, and responsible for his security domain keys (APSD keys) according to GlobalPlatform requirements [11].
- The verification authority is expected as a trusted actor who is able to verify bytecode of an application loaded on the card, guarantee and generate the digital signature attached to an application and ensure that its public key for verifying the application signature is on the platform according to GlobalPlatform requirements [11].
- Security domains can be dynamically created, deleted and blocked during usage phase in post-issuance mode.

Please refer to Section 1.3 for references to the guidance documentation mentioned above.

3 Security Requirements

3.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP4** as defined in [1]. The assurance requirements are as follows:

Table 3. Security Assurance Requirements for SESIP4

Assurance Class	Assurance Families
ASE: Security Target Evaluation	ASE_INT.1 ST Introduction ASE_OBJ.1 Security requirements for the operational environment ASE_REQ.3 Listed security requirements ASE_TSS.1 TOE summary specification
ADV: Development	ADV_ARC.1 Security architecture descriptiion ADV_FSP.4 Complete functional specification ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs
AGD: Guidance Documents	AGD_OPE.1 Operational user guidance AGD_PRF.1 Preparative procedures
ALC: Life-cycle Support	ALC_CMC.1 Labelling of the TOE ALC_CMS.1 TOE CM coverage ALC_FLR.2 Flaw reporting procedures ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_TAT.1 Well-defined development tools
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing ATE_IND.1 Independent testing: conformance
AVA: Vulnerability Assessment	AVA_VAN.4 Methodical vulnerability analysis

3.1.1 ALC: Life-cycle support

3.1.1.1 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 operating system of the platform cannot be updated or patched after issuance. The reason is to minimize the attacking surface; the possibility to abuse the operating system via the update mechanism is removed. The final product with application(s) still reserves the capability of change post issuance. 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 [11], with proper personalization before the product field delivery. The final product with application(s) is out of the scope of this document.

3.2 Security Functional Requirements

The platform fulfills the following security functional requirements:

3.2.1 Identification and Attestation of Platforms and Applications

3.2.1.1 Identification of platform type

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

Self-assessment:

The 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 the User Manual [7]. The IDENTIFY command also returns information about Modules present in the platform and allows to identify the platform configuration.

JCOP 4 SE050 v4.7 R2.00.11 is a friendly name for the platform which is unique amongst all JCOP variants at NXP.

3.2.1.2 Identification of individual platform

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

Self-assessment:

Card Production Life Cycle (CPLC) data of the platform include unique identification of individual platform as described in Section 8.1 of the User Manual [7].

3.2.1.3 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 a secure state.

Self-assessment:

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).

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.

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

3.2.2.1 Secure install of application

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

Self-assessment:

Card content management function is implemented as defined in [11], which supports secure install of application in the field.

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.~~

Self-assessment:

The platform does not support the update after issuance. It does offer features for off-card entity within a logically secure environment to manage the applets securely following GP Card Manager technical and procedure requirements [11]. According to [1] the absence of this functionality for the platform must be explained as part of ALC_FLR.2. Please see Section 3.1.1.1 for this explanation.

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* [11] and protects against attacks including *disclosure, modification, replay* of messages between the endpoints, using *Secure Channel Protocol (SCP) '02'*.

The secure communication channel authenticates *off-card entity within a logically secure environment* [11] and protects against attacks including *disclosure, modification, replay* of messages between the endpoints, using *Secure Channel Protocol (SCP) '03'*.

Self-assessment:

JCOP supports the secure channel protocols SCP02 and SCP03 as defined in GlobalPlatform 2.3 [11].

3.2.3.2 Secure communication enforcement

The platform ensures the application can only communicate with *card Issuer, application provider, controlling authority, or delegated offcard entity with token signed by security domain provider* [11] over the secure communication channel(s) supported by the platform.

Self-assessment:

JCOP enforces the secure channel protocols SCP02 and SCP03 as defined in GlobalPlatform 2.3 [11] *for GP content management.*

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 other functional requirements, ensuring that the other functional requirements are not compromised.

Guidance (required by ICA and covered by SESIP):

The developer self-assessment (section below) and evaluator vulnerability analysis reporting must include consideration of attacks using the chip surfaces (IOSESEC01), supply voltages and frequencies, temperatures (IOTSESEC02), reverse engineering (IOSESEC03), probing and side-channel attacks (IOSESEC04), on-chip test features (IOTSESEC05), voltage manipulation (IOTSESEC06) and EM (IOTSESEC08) and laser (IOTSESEC09) and other non-invasive attacks (IOTSESEC07), SPA (IOTSESEC010) and DPA (IOTSESEC011) and EMA (IOTSESEC012) and other side-channel attacks, DFA (IOTSESEC14), and interrupt handling attacks (IOTSESEC15)

Self-assessment:

Attacks using the chip surfaces (IOSESEC01) , reverse engineering (IOSESEC03), probing and side-channel attacks (IOSESEC04) are countered by various special features in the design and layout of the circuitry, i.e., mainly shielding and hiding of relevant design parts. This includes:

- *security routing that adds unused lines between active ones to fill the topmost layers,*
- *route thick supply lines over interface areas,*
- *cover memory blocks and sensitive analogue parts with meshes and tiles, and*
- *using active lines (dummy lines with controlled signals) to cover important signal lines.*

There is no common bus, only local dedicated data, code and address lines interconnect the different memories and the CPU. All interfaces, including the data, code and address encryption logic for the memories are part of the 'Glue Logic'. Therefore it is never possible to observe any clear data by tapping local memory buses.

Beside the measures mentioned above, the general CPU Functions, the hardware components, the memory management unit with all memory interfaces including the encryption functions are realized in so-called 'Glue Logic'. The glue logic is a sea of basic low level gates. These gates are placed and interconnected by using automated tools which provide random, heuristic and deterministic placement and routing procedures. The CPU bus is never leaving the 'Glue Logic' area. The five metal layer technology

allows routing on top of the cells. By this on one hand no routing channels can be found (and therefore also no bus structures can be found) and on the other hand even the cell structure itself is no longer visible.

These features also support all other SFRs because prevention of successful manipulation of security functionality is a pre-condition for the reliable work of all other functions.

Attacks using the supply voltages and frequencies, temperatures (IOTSESEC02)) are countered by sensors for the upper and lower threshold of the operating conditions temperature, clock frequency as well as voltage. The sensors detect whether one parameter is outside the specified range. Any detection of an attack will be signaled again by performing a reset which leads to the secure state.

Attacks using SPA (IOTSESEC010) and DPA (IOTSESEC011) and EMA (IOTSESEC012) and other side-channel attacks are countered by the countermeasures implemented in the cryptographic co-processors (AES, TDES, and FAME3) such as blinding and randomization are independent of the keys and plain- or ciphertext calculated by the co-processor. The same calculation time for the encryption and decryption function (for a single operation) with all operands is also ensured by the design of the co-processor.

The clock configuration allows the usage of internally generated clock signals for different components (e.g. the co-processor) on the platform to operate independent of the external clock. In addition the execution of instructions by the CPU is randomized to some extent to prevent the possibility to synchronize the internal behavior based on external signals (clock and power consumption) for leakage attacks. Security critical comparisons are protected by hardware and software countermeasures.

Other features like filtering and scrambling that are implemented to increase the robustness and confidentiality also contribute to counter leakage attacks.

The cryptographic coprocessors (TDES, AES and Fame3) as well as the cryptographic library implements countermeasures against fault injection and information leakage. For instance, these platform components implement integrity protection of processed data. They further implement randomization such as blinding, dummy calculations and random delay before and after calculations. A further implemented mechanism to protect User Data from unwanted disclosure is an automatic clean-up of relevant registers (key and data registers of the used coprocessor) after usage and before changing the platform mode.

Attacks using voltage manipulation (IOTSESEC06), EM (IOTSESEC08) and laser (IOTSESEC09), other non-invasive attacks (IOTSESEC07) and DFA (IOTSESEC14)are countered by a collection of functions that allows checking whether the platform has been physically manipulated, including aforementioned features in the design, layout of the circuitry and cryptographic coprocessors.

TSF also supports the integrity of the ROM, RAM and Flash. The Flash is able to perform error correction. The ROM, RAM and Flash provide parity protection. A parity error is interpreted as a fault injection and forces a reset that increments the error counter. This combination increases the likelihood to detect manipulations of single cells. In addition, the manipulation of program or data or other meaningful values is much more difficult.

Attacks using the on-chip test features (IOTSESEC05) are countered by integrity protection during start-up.The access to the IC Dedicated Test Software in the Super System Mode is provided by evaluating the related electronic fuses during the boot sequence. It assures that it is not possible to enable access to the IC Dedicated Test

Software after platform delivery. Moreover TSF prevents direct access to the Special Function Registers.

Attacks using the weak RNGs (IOTSESEC13, see also Section 3.2.5.5) are countered by hardware test functionality to detect faults in the circuitry of the RNG (total failure test), functionality provided by Crypto Lib, also aforementioned measures against physical manipulation.

Attacks using the interrupt handling attacks (IOTSESEC15) are countered interupt control. Interrupts force a jump to a specific fixed vector address in the ROM or Flash. Any interrupt can therefore be controlled and guided by a specific part of the Security IC Embedded Software.

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 the other functional requirements.

Self-assessment:

The platform implements the Java Card Virtual Machine [13], Java Card Runtime Environment [14], Java Card API [12], configuration management and Card Content Management [11] 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.

Self-assessment:

The platform implements the Java Card Virtual Machine [13], Java Card Runtime Environment [14], configuration management and Card Content Management [11] according to corresponding specifications, which ensures isolation of the platform parts.

Furthermore, TSF provides an environment to securely execute non-certified native code from third parties, namely secure box, It ensures that only program code and data contained in the secure box can be accessed from within this secure box and therefore cannot harm, manipulate, or influence other parts of the platform.

Native code executed in the Secure Box is executed in User Mode. Access to the CPU mode, memory outside the Secure Box, the MMU segment table, and Special Function Registers which allow configuration of the MMU and allow System Management is prohibited for code executed in the Secure Box.

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.

Self-assessment:

The platform implements the Java Card Virtual Machine [13], Java Card Runtime Environment [14], configuration management and Card Content Management [11] according to corresponding specifications, which ensures isolation of the application parts.

3.2.5 Cryptographic Functionality

3.2.5.1 Cryptographic operation (symmetrical and asymmetrical algorithms)

The platform provides the application with *encryption and decryption* functionality with *TDES* as specified in *NIST SP 800-67* [20] for key length *112 or 168 bit* and modes *ECB and CBC* [17].

The platform provides the application with *MAC generation and verification* functionality with *TDES* as specified in *NIST SP 800-67* [20] for key length *112 or 168 bit* and modes *Retail-MAC, CBC-MAC* [23] *and CMAC* [18] .

The platform provides the application with *encryption and decryption* functionality with *AES* as specified in *NIST FIPS 197* [16] for key length *128, 192 or 256 bit* and modes *ECB, CBC and CTR* [17].

The platform provides the application with *MAC generation and verification* functionality with *AES* as specified in *NIST FIPS 197* [16] for key length *128, 192 or 256 bit* and modes *CMAC* [18] *and CBC-MAC* [23].

The platform provides the application with *encryption, decryption, signature generation and verification* functionality with RSA as specified in *PKCS#1* [21] for key length *512 bits to 4096 bits* and modes *EME-OAEP and EMSA-PSS*.

The platform provides the application with *signature generation and verification* functionality with ECDSA as specified in *ISO/IEC 14888-3:2015* [22] for key length *160, 192, 224, 256, 384, 512, 521 bit* and modes *not applicable*.

The platform provides the application with *Diffie-Hellman* functionality with ECDH as specified in *NIST FIPS 800-56A* [19] for key length *160, 192, 224, 256, 384, 512, 521 bit* and modes *not applicable.*

Guidance (required by ICA and covered by SESIP):

Only the algorithms in [5] section 6.3 listed must be claimed. At least one (symmetrical or asymmetrical) algorithm must be selected.

Self-assessment:

The support for cryptographic operations is described in the User Manual [7].

3.2.5.2 Cryptographic operation (hash algorithms)

The platform provides the application with *hashing* functionality with *SHA1* as specified in *NIST FIPS 180-4* [15] for key lengths *block size of 512 bits and digests of 160 bits* and mode *not applicable*.

The platform provides the application with *hashing* functionality with *SHA-256* as specified in *NIST FIPS 180-4* [15] for key lengths *block size of 512 bits and digests of 256 bits* and mode *not applicable*.

The platform provides the application with *hashing* functionality with *SHA-384* as specified in *NIST FIPS 180-4* [15] for key lengths *block size of 1024 bits and digests of 384 bits* and mode *not applicable*.

The platform provides the application with *hashing* functionality with *SHA-512* as specified in *NIST FIPS 180-4* [15] for key lengths *block size of 1024 bits and digests of 512 bits* and mode *not applicable*.

Guidance (required by ICA and covered by SESIP):

Only the algorithms in [5] section 6.3 listed must be claimed.

Self-assessment:

The support for cryptographic operations is described in the User Manual [7].

3.2.5.3 Cryptographic key generation

The platform provides the application with a way to generate cryptographic keys for use in *TDES* as specified in [20] for key lengths *112, 168 bit*.

The platform provides the application with a way to generate cryptographic keys for use in *AES* as specified in [16] for key lengths *128, 192, 256 bit*.

The platform provides the application with a way to generate cryptographic keys for use in *RSA* as specified in [21] for key lengths *512, 736, 768, 896, 1024, 1280, 1536, 1984, 2048, 4096 bit and from 2000 bit to 4096 bit in one bit steps.*

The platform provides the application with a way to generate cryptographic keys for use in *ECC* as specified in [22] and [19] for key lengths *160, 192, 224, 256, 384, 512, 521 bit.*

Self-assessment:

The support for cryptographic key generation is described in the User Manual [7].

3.2.5.4 Cryptographic Keystore

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

Self-assessment:

Platform provides a secure data storage for confidential data. It is used to store cryptographic keys and to store PINs. All data stored is CRC32 integrity protected and AES encrypted.

3.2.5.5 Cryptographic random number generation

The platform provides the application with a way based on *deterministic* to generate random numbers to as specified in *AIS 20 DRG.3* [6].

The platform provides the application with a way based on *hybrid-deterministic* to generate random numbers to as specified in *AIS 20 DRG.4* [6].

Guidance (required by ICA and covered by SESIP):

The random number generator must conform to a well-known random number generation standard such as AIS31, NIST SP800-22, or GB/T 32915. The evaluator vulnerability analysis reporting shall include RNG Test (IOTSESEC13).

Self-assessment:

TSF 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.

3.2.6 Compliance Functionality

3.2.6.1 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 [14] before the memory is (re)used by the platform or application again and before an attacker can access it.

Self-assessment:

TSF 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 [14].

TSF also provides deletion of memory for transient arrays, global arrays, and logical channels according to the Java Card Runtime Environment Specification [14].

4 Mapping and Sufficiency Rationales

4.1 SESIP4 Sufficiency

Assurance Class	Assurance Familiy	Covered By	Rationale
ASE: Security target evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in Section 1.1, the platform reference in Section 1.2, the platform overview and description in Section 1.4.
	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_ARC.1 Security architecture description	Materials provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ADV_FSP.4 Complete functional specifications	Materials 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	Materials 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 and materials provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Section 1.3 and materials provided to evaluator.	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	Materials provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.

Assurance Class	Assurance Familiy	Covered By	Rationale
	ALC_CMS.1 TOE CM Coverage	Materials provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ALC_FLR.2 Flaw reporting procedures	Section 3.1.1.1 and materials provided to evaluator.	The flaw reporting and remediation procedure is described.
	ALC_DEL.1 Delivery procedures	Materials provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ALC_DVS.1 Identification of security measures	Materials provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ACL_TAT.1 Well-defined development tools	Materials provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
ATE:Test	ATE_COV.1 Evidence of coverage	Materials provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ATE_FUN.1 Functional Testing	Materials provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ATE_IND.1 Independent testing: conformance	Materials provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA: Vulerabilty assessment	AVA_VAN.4 Methodical vulnerablity 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 platform. Penetration testing is performed by the evaluator assuming an attack potential of Basic.

4.2 ICA IoT security assurance requirements sufficiency

ICA security carrier level	SESIP Level	Rationale
ICA Security carrier Level 3	SESIP3 (or higher) + SFR “Physical attacker resistance”	The vulnerability analysis explicitly includes the ICA attack methods, and the required attack rating is identical (at SESIP3 level) or higher (at SESIP4 level or higher).

4.3 ICA IoT security functional requirements sufficiency

ICA requirement	Specific requirement	Covered by	Rationale
IoTSESEC01	Chip surface preparation, inspection and analysis	Section 3.2.4.1	Section 3.2.4.1 already includes all the mentioned attack methods (within the SESIP level), however the need to explicitly report on them is added as a refinement. Hence the evaluator will explicitly (penetration) test these sensors. As part of any SESIP level, the developer must give an overview on the testing performed to ensure the SFRs are correctly implemented. The SFR “Physical attacker resistance” section “Self-assessment” describes the developer’s testing.
IoTSESEC02	Sensors functional tests	Section 3.2.4.1	As IoTSESEC01
IoTSESEC03	Physical security analysis	Section 3.2.4.1	As IoTSESEC01
IoTSESEC04	Internal communication security	Section 3.2.4.1	As IoTSESEC01
IoTSESEC05	On-chip test features	Section 3.2.4.1	As IoTSESEC01
IoTSESEC06	Voltage manipulation	Section 3.2.4.1	As IoTSESEC01
IoTSESEC07	Other non-invasive attacks	Section 3.2.4.1	As IoTSESEC01
IoTSESEC08	EM manipulation	Section 3.2.4.1	As IoTSESEC01
IoTSESEC09	Laser manipulation	Section 3.2.4.1	As IoTSESEC01

ICA requirement	Specific requirement	Covered by	Rationale
IoTSESEC10	Simple Side-channel power analysis	Section 3.2.4.1	As IoTSESEC01
IoTSESEC11	Differential power analysis	Section 3.2.4.1	As IoTSESEC01
IoTSESEC12	Side-challenge EM emissions analysis	Section 3.2.4.1	As IoTSESEC01
IoTSESEC13	RNG test	Section 3.2.5.5	The requirement to addresses compliance to a random number generation standard. Similar to IoTSESEC01, the vulnerability analysis will include attacks against the RNG
IoTSESEC14	Differential Fault Analysis	Section 3.2.4.1	As IoTSESEC01
IoTSESEC15	Interrupt processing	Section 3.2.4.1	As IoTSESEC01
IoTSESEC16	Hardware communication interface requirements	Section 1.4.4	This functionality is described in the platform functionality, but not a SFR hence not verified to be resistant to an attacker. This is considered sufficient by ICA as it is additionally verified in ICA.
IoTSESEC17	Security algorithm verification	Section 3.2.5.1	The ICA requirements are explicitly translated and fully covered.
IoTSESEC18	SE reliability requirements	Section 1.4.4	This functionality is described in the platform functionality, but not a SFR hence not verified to be resistant to an attacker. This is considered sufficient by ICA as it is additionally verified in ICA.

5 Bibliography

5.1 Evaluation Documents

[1] Security Evaluation Standard for IoT Platforms, version 1.3.
[2] SESIP Profile: ICA IoT Security Requirements level 3, version 1.0.
[3] SESIP Profile: ICs SOGIS-CC certified against PP0084, version 1.0.
[4] SESIP Profile: platforms SOGIS-CC certified against JavaCard 3.0.5, version 1.0.
[5] Entry Criteria for IoT Secure Element, ICA/T 2017-201-01, ICA, October 2017.
[6] 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.

5.2 Developer Documents

[7] JCOP 4 SE050, User manual for JCOP 4 SE050, Rev. 1.2, DocNo 500312, 20190531, NXP Semiconductors.

5.3 Standards

[8] ISO 7816-3: Part 3: Cards with contacts - Electrical interface and transmission protocols , Nov 2006..
[9] ISO/IEC 14443 Proximity Cards - Part 4: Transmission protocol - ISO/IEC 14443-2:2008..
[10] NXP Semiconductors. NXP T=1 Over SPI/I2C Specification, rev. 1.1, January 9 2019.
[11] GlobalPlatform Card Specification 2.3, GPC_SPE_034, GlobalPlatform Inc., October 2015.
[12] Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., Oracle, May 2015.
[13] Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.5., Oracle, May 2015.
[14] Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0.5., Oracle, May 2015.
[15] FIPS PUB 180-4: Secure Hash Standard (SHS), Federal Information Processing Standards Publication, Information Technology Laboratory, National Institute of Standards and Technology, August 2015.
[16] FIPS PUB 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/National Institute of Standards and Technology, 26 November 2001.
[17] NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Morris Dworkin, National Institute of Standards and Technology, December 2001.
[18] NIST SP 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, National Institute of Standards and Technology, May 2005.
[19] NIST Special Publication 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.

[20] NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised January 2012, National Institute of Standards and Technology.

[21] PKCS#1: RSA Cryptography Standard, Version 1.5.

[22] ISO/IEC 14888-3:2015: Information technology â€“ Security techniques â€“ Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms, 2016.

[23] ISO 9797-1: Information technology – Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 1999-12, ISO/IEC.

6 Legal information

6.1 Definitions

Draft — The document is a draft version only. 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 herein 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 — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and 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: 19 December 2019