NXP SE310 Series - Secure Element

Security Target Lite

Rev. 0.1.1 — 22 May 2023 Preliminary evaluation document
NSCIB-2200031-01 COMPANY PUBLIC

Document information

Information	Content
Keywords	NXP, ASE, SE310 Single Chip Secure Element , Single Chip Secure Element , Common Criteria, EAL5 augmented
Abstract	This document is the Security Target of the SE310 Secure Element, developed and provided by NXP Semiconductors. The TOE complies with Evaluation Assurance Level 5 of the Common Criteria for Information Technology Security Evaluation Version 3.1 with augmentations.

Revision History

Revision history

Revision number	Date	Description
0.1.0	2023-05-09	Derived from full Security Target 0.1.0
0.1.1	2023-05-22	Derived from full Security Target 0.1.1

1 ST Introduction (ASE_INT)

1.1 ST Reference

"SE310 Secure Element", Security Target Lite, Revision 0.1.1, 22 May 2023.

1.2 TOE Reference

Table 1. TOE Reference

Content	Version
Product Type	Secure Element subsystem of the IC hardware platform SE310 with IC Dedicated Support Software and documentation describing usage of the TOE
TOE name	NXP SE310 Series - Secure Element
TOE version(s)	SE310_SE A0.1.000 J2

1.3 TOE Overview

1.3.1 Usage and Major Security Features of the TOE

The SE310 Single Chip Secure Element combines on a single die an Embedded Secure Element and a SYS Domain. The two subsystems are called "SE310_SE" and "SE310_SYS". The SYS Domain is not part of the TOE. The Embedded Secure Element SE310_SE is based on a Flash-based secure microcontroller platform. A high frequency clocked ARM Cortex M33 core along with state of the art cryptographic hardware coprocessors brings secured applications to a new level in performances and security. The TOE is integral part of the SE310 IC. Note that SE310 without any Security IC Embedded Software for the TOE is available for NXP internal use only.

Secure Element Hardware:

The TOE incorporates an high frequency clocked ARM Cortex M33 processor augmented with its dedicated coprocessor (SYM-lite), a secure copy machine (SMA), and a Public-Key Cryptography (PKC) coprocessor, which are all connected to a bus system. This bus system gives access to memories, hardware peripherals and communication interfaces. The PKC coprocessor provides large integer arithmetic operations, which can be used by Security IC Embedded Software for asymmetric-key cryptography. Hardware peripherals include coprocessors for symmetric-key cryptography and for calculation of error-detecting codes, and also a random number generator. On-chip memories are Flash memory, ROM and RAMs. The Flash memory can be used to store data and code of Security IC Embedded Software. It is designed for reliable non-volatile storage.

The security functionality of the TOE is designed to act as an integral part of a security system composed of hardware and Security IC Embedded Software to strengthen it as a whole. Several security mechanisms of the TOE are completely implemented in and controlled by the SE310 Secure Element. Other security mechanisms must be treated by Security IC Embedded Software. All security functionality is targeted for use in a potential insecure environment, in which the TOE maintains

- correct operation of the security functionality
- integrity and confidentiality of data and code stored to its memories and processed in the device

This is ensured by the construction of TOE and its security functionality.

The following list contains the main features of the TOE:

- hardware to perform computations on multiprecision integers, which are suitable for public-key cryptography
- hardware to calculate the Data Encryption Standard with up to three keys
- hardware to calculate the Advanced Encryption Standard (AES) with different key lengths
- hardware to support Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR) modes of operation for symmetric-key cryptographic block ciphers
- hardware to support Galois/Counter Mode (GCM) of operation for symmetric-key cryptographic block ciphers
- hardware to calculate Cyclic Redundancy Checks (CRC)
- hardware to serve with True Random Numbers

In addition, the hardware embeds sensors, which ensure proper operating conditions of the device. Integrity protection of data and code involves error correction and error detection codes, EMFI detector, light sensing and other security functionality. Memory encryption and masking mechanisms are implemented to preserve confidentiality of data. The IC hardware is shielded against physical attacks.

Note that this Security Target addresses only the hardware part of an integral security system. The secure operation of cryptographic functionality given above requires availability of the Cryptographic Library which is not part of this TOE. Therefore Security Services and Security Features using this cryptographic functionality **need to be evaluated in the composite product together with Cryptographic Library as part of the Security IC Embedded Software**. As a consequence, for the cryptographic functionality the scope of this evaluation is confined to protection against physical manipulation.

All security functional requirements applicable to this Security Target are given in Section 6.

1.3.2 TOE Type

The TOE is a Security Integrated Circuit Platform for operating systems and applications with high security requirements.

1.3.3 Security During Development and Production

The Security IC product life cycle is scheduled in phases, which are defined in the Protection Profile [7].

Phase 2 IC Development, phase 3 IC Manufacturing as well as phase 4 IC Packaging of this life cycle are part of this Security Target. The TOE Delivery is at the end of phase 4.

The development environment of SE310_SE always ranges from phase 2 IC Development to TOE Delivery. All other phases are part of the operational environment. This addresses Application Note 1 in in the Protection Profile [7].

In phase 2 IC Development of SE310_SE access to sensitive design data of SE310_SE is restricted to people, who are involved in the development of the product.

In phase 3 IC Manufacturing the TOE as integral part of SE310 IC are produced and tested on wafers. In this phase NXP also serves as Composite Product Manufacturer by optionally storing Security IC Embedded Software to the Flash of SE310_SE. The NXP Trust Provisioning Service ensures confidentiality and integrity of any customer data in this phase. This incudes secure treatment and insertion of data and code received from the customer as well as random or derived data, which are generated by NXP.

In phase 4 IC Packaging SE310 ICs including the TOE are embedded into packages.

The delivery processes between all involved sites provide accountability and traceability of the dies. Authentic delivery of the TOE is supported by its NXP Trust Provisioning Service.

1.3.4 Required non-TOE Hardware/Software/Firmware

Besides the SE310_SE the SE310 Single Chip Secure Element comprises a SYS Domain (SE310_SYS) and a shared Power Management Unit SE310_PMU).

For operation the SE310_SE requires full function of the SE310_PMU subsystem, that is controlled by software of the SE310_SYS subsystem Figure 1.

The TOE does not include communication drivers in the IC Dedicated Support Software. Those need to be part of the Security IC Embedded Software.

1.4 TOE Description

The SE310 Single Chip Secure Element is build upon two subsystems: "SE310_SE" and "SE310_SYS". Both subsystem use a shared Power Management Unit ("SE310_PMU").

All components and the TOE boundaries are depicted in Figure 1. The components are described in more detail in the following sections.

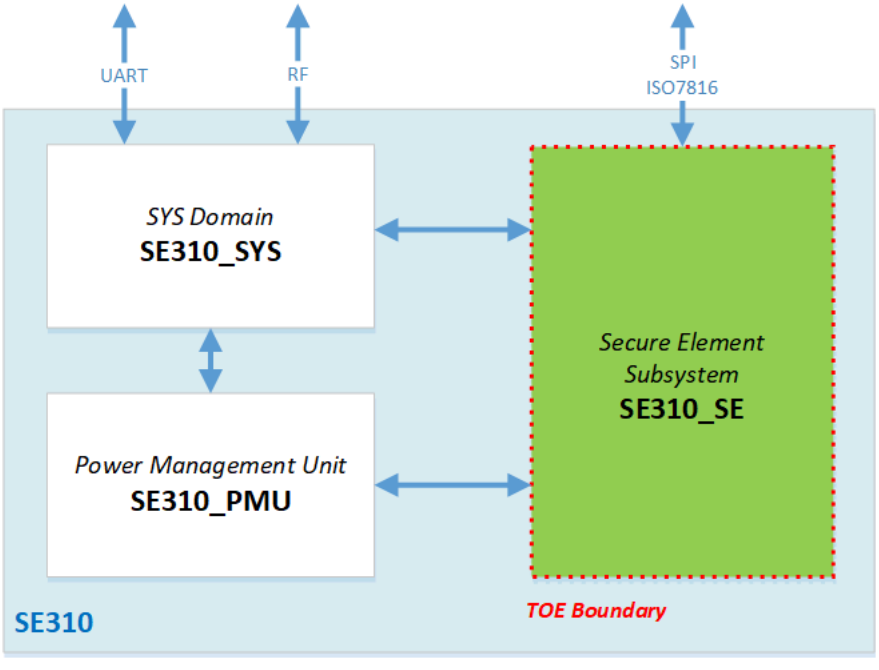

Figure 1. Components of the TOE

1.4.1 Secure Element Subsystem

The SE310 is a hardware platform designed to meet the developing needs of the mobile communications market. It embeds a Secure Element Subsystem (SE310_SE), supported by an integrated SYS Domain (SE310_SYS) and Power Management Unit (SE310_PMU).

The toplevel block diagram of the SE310_SE is depicted in Figure 2.

The hardware part of the SE310_SE is referred to as Secure Element Hardware in the following.

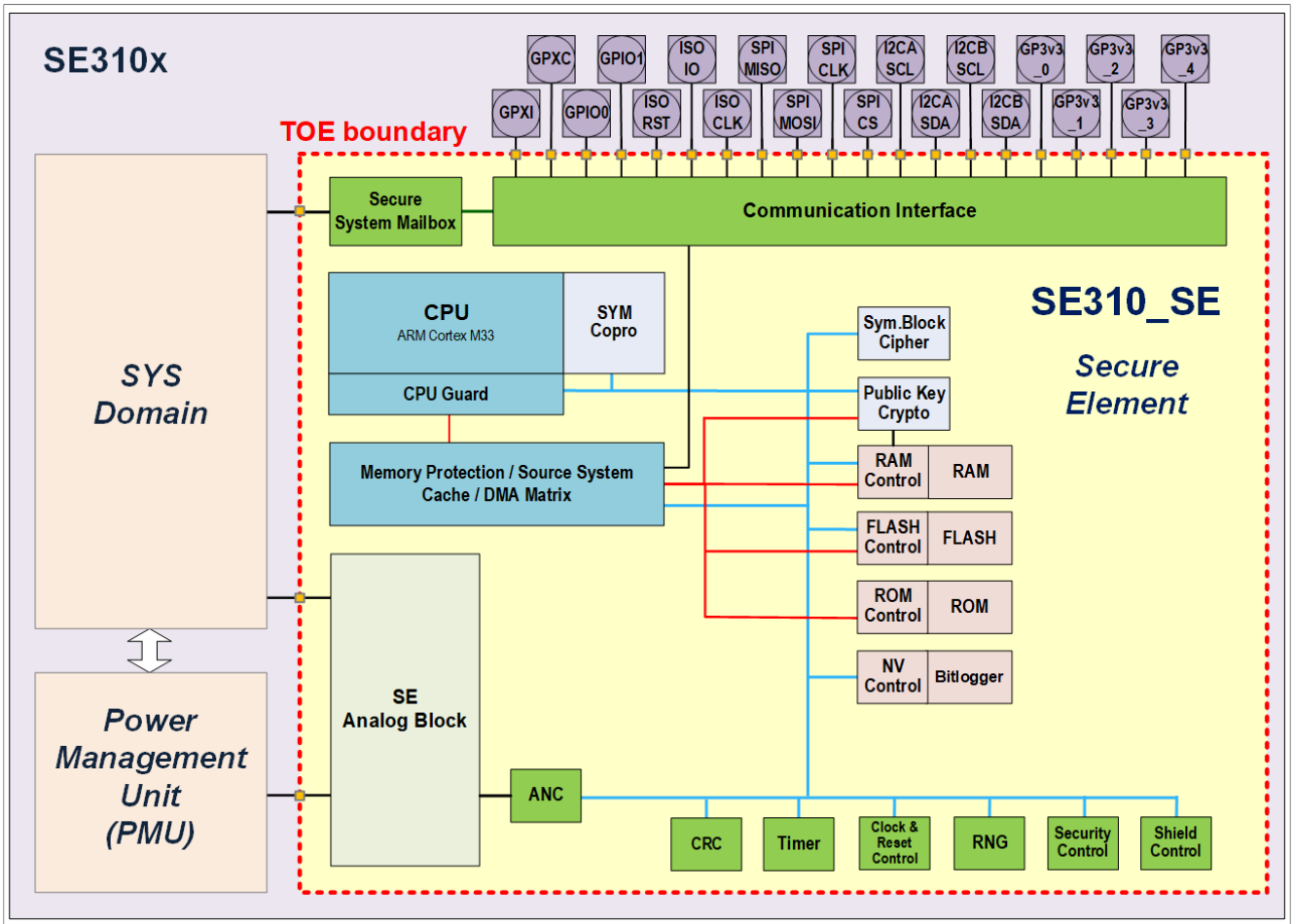

Figure 2. Block Diagram of the Secure Element Hardware

1.4.1.1 Hardware Description

The SE310 Secure Element implements ROM, Flash, System RAM, PKC RAM and a Buffer RAM for Flash erase/programming and for Flash read caching. All these memories are accessible over the bus system on data/address busses. The hardware controls write, read and execute access to the memories over the bus system against system operation modes. Context information is attached to all bus transactions throughout the whole system. Any peripheral on the bus can use the context information to check if access is allowed for the actual context, apply context specific cyphering or to assign associated errors or interrupts to a particular context.

The SE310 Secure Element implements a wide range of hardware components. It embeds the Fast Accelerator for Modular Exponentiation of 3rd Generation (Fame3.5), which can be utilized by the software to accelerate computations required for public-key cryptography like such related to RSA, Elliptic Curve Cryptography (ECC).

The Secure Generic Interface (SGI) is a symmetric crypto engine that serves the IC Security Embedded Software with interfacing to a DES coprocessor, an AES coprocessor and a GCM coprocessor.

The SYM-Lite is a CPU co-processor providing the IC Security Embedded Software with crypto-supporting general purpose operations over sensitive data, outside - but under control of - the CPU.

The Secure Copy Machine (SMA) is a secure DMA. Purpose of the SMA is to copy data between memories and between memories and peripherals in a secure way.

Two CRC coprocessors each serve with checksum computation based on CRC generation polynomials CRC-8, CRC-16 and CRC-32. The Random Number Generator generates true random numbers, which are compliant to AIS31 and FIPS 140-3[1].

SE310 Secure Element also implements a watchdog counter with time-out mechanism that can be utilized by the software to abort irregular program executions, and provides a CPU Guard with several security functionality, which can be utilized by the software to secure its execution.

The Hardware components can be controlled by the IC Security Embedded Software via Special Function Registers, which are accessible over the bus system on two separate busses. One peripheral control bus is provided for I/O communication. The secure peripheral bus serves protected internal communication.

The SE310 Secure Element implements complex security functionality to protect code and data during processing and while stored to the device. This includes appropriate memory encryptions and masking schemes to preserve confidentiality. This also includes error detection codes (the Flash Secure Fetch Plus) to protect the integrity of memory contents. Additionally, manifold light sensing with EMFI detector is integrated to detect perturbations which can lead to integrity violation. Active shielding is present and operating conditions are monitored by sensors on temperature, power supplies and frequencies.

The TOE hardware operates with a power supply provided by the shared Power Management Unit ("SE310_PMU"). The device can be set into sleep and power-down modes, which have different levels of reduced availability of hardware components with appropriately reduced power consumption.

1.4.1.2 IC Dedicated Support Software

The IC Dedicated Support Software of the SE310_SE comprises:

- Test software named *FactoryOS*
- Boot software named *BootOS*
- Memory Driver software named *Flash Driver Software*

BootOS, FactoryOS and Flash Driver Software are stored to ROM. Patches to the BootOS are stored to Flash.

1 Note: FIPS 140-3 compliance is not in scope of this Common Criteria evaluation.

The BootOS is executed during start-up after power-on or reset of the TOE. It sets up the device and its configuration, and finally jumps to a start address in either Mission Mode or Test Mode (if not finally locked).

The FactoryOS is used during manufacturing to load the whole software stack into Flash. The FactoryOS also provides controlled access to different levels of testing capabilities of SE310 Secure Element. Full testing capabilities are under restricted access to NXP for production testing of the TOE and also for in-depth analysis of field returns. In addition, limited testing capabilities are accessible to NXP for basic analysis of field returns, which target to preserve the product in its original condition. Beyond that, the FactoryOS provides some basic functional testing of the SE310 Secure Element and also with a readout of the TOE IC hardware identification flags (if enabled via OEF option). The FactoryOS implements security functionality to protect from unauthorized access and ensures that also authorized access cannot compromise confidentiality of content stored to access controlled Flash areas as well as System Pages. Factory OS implements security functionality against unauthorized access in the field.

Flash Driver Software provides a Hardware Abstraction Layer that is stored to ROM. It supports basic operation of the Flash memory to enable usage of the Flash during Boot Mode and Test Mode.

1.4.2 Interfaces of the TOE

Electrical interface

The electrical interface of the TOE are the lines between the I/O interface of the SE310_SE and the communication pads, that are exclusively used by the SE310_SE subsystem. The interface can be configured to establish communication with the TOE via the following interfaces:

- Serial Peripheral Interface (SPI)
- 2x I^2C interfaces
- GPIO interface by use of Special Function Registers
- 5x GP3v3 interfaces

The TOE also provides an electrical interface to the SE310_PMU subsystem, which connects power supply voltage input and ground as reference voltage, and an interface to the Power-Clock-Reset Module of the SE310_SYS subsystem. Communication between SE310_SE and SE310_SYS supported by System Mailbox interface.

Logical interface

Figure 3 illustrates the logical interface to the Security IC Embedded Software internal interfaces not drawn).

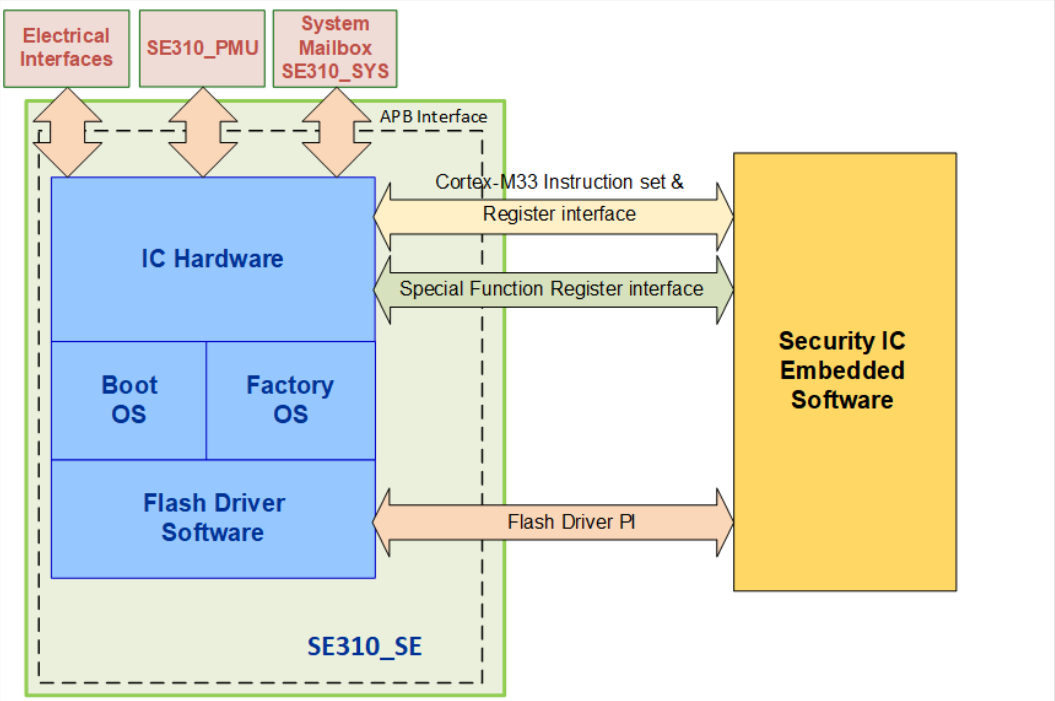

Figure 3. Logical interface of SE310

The logical interface of the TOE accessible to the Security IC Embedded Software provides the following communication channels:

- Secure System Mailbox interface for data exhange with SE310_SYS subsystem
- CPU Instruction set and Register interface acc. to [12]
- Special Function Registers interface acc. to [11]
- Flash Driver PI, which is accessible to Security IC Embedded Software

All logical interfaces other than the Secure System Mailbox interface are accessible via the electrical interfaces SPI, I^2C, GPIO and GP3v3.

Physical interface

The chip surface must be considered as an interface of the TOE as well. This interface could be exposed to environmental stress or physically manipulated by an attacker.

1.5 TOE Identification

1.5.1 Evaluated Hardware Configurations

Each configuration of the TOE consists of a physical configuration (i.e. hardware component incl. ROM code and related documentation) and a logical configuration (i.e. Software components and configuration data stored to Flash memory).

The definition of the configuration identifiers of SE310_SE is detailed in Table 2.

Table 2. Configuration identifiers of the TOE

Name	Symbol	Description
Series	*srs*	Series identifier in NXP product family
IC version	*xy.z.zzz*	*x*: base layer identifier of the development type *y*: fixed metal masks identifier of the development type *z.zzz*: customizable metal masks identifier of the development type, includes the IC Dedicated Software stored to ROM
NXP software	*w*	*w*: NXP software combination identifier of the development type (fixed to "J" for SE310 Series)
NXP hardware configuration	*v*	Version identifier of the NXP hardware configuration, identifies the version of configuration data stored to Flash (combination of Factory Page, System Control Page, System Update Page and System Patch Page)

The symbols in the second column in Table 2 build the product name of a TOE configuration according to the following rule:

- *srs xy.z wv* [2]

Evaluated **physical** configuration of the TOE is

- *SE310_SE **A0.1.000***

All components of SE310_SE A0.1.000 that are common for any logical configuration are listed in Table 3 with their respective version numbers.

Evaluated **logical** configuration of the TOE stored to flash memory is

- *SE310_SE A0.1.000 **J2***

All components that are specific for SE310_SE A0.1.000 J2 are listed in Table 4 with their respective version numbers.

TOE identification methods are described in [10].

Table 3. Components of SE310_SE A0.1.000 common for any logical configuration

Category	Component	Identification	Delivery form
IC Hardware	base layer and fixed metal masks	A0.1.000	Package
IC Dedicated Support Software	FactoryOS	3.4.4	On-chip software. Stored to the ROM of the TOE
	BootOS (ROM)	3.4.2	On-chip software. Stored to the ROM of the TOE
	Flash Driver Software	3.4.5	On-chip software. Stored to the ROM of the TOE
Documentation, User Guidance	SE310_SE Information on Guidance and Operation	[8]	Electronic Document (PDF via NXP Docstore)
Documentation, Product Data Sheet	SE310S Embedded Secure Element, Product data sheet	[9]	Electronic Document (PDF via NXP Docstore)
	SE310 TOE Identification (for A0), Data sheet addendum	[10]	Electronic Document (PDF via NXP Docstore)

2 This naming scheme is reflected in the Type ID for TOE identification given in [10]: "*srs xy.z*" refers to byte 0 of the Type ID, "*w*" to byte 1 and "*v*" to byte 2.

Table 3. Components of SE310_SE A0.1.000 common for any logical configuration ***...continued***

Category	Component	Identification	Delivery form
Documentation, Application Note	SE310_SE Programmers's Manual, Application Note	[11]	Electronic Document (NXP internal Document)
	ARM® Cortex®-M33 Processor Technical Reference Material	[12]	Electronic Document (www.arm.com)

Table 4. Components of SE310_SE A0.1.000 specific for J2

Category	Component	Identification	Delivery form
Configuration Data	Factory Page	220824	On-chip configuration page. Stored to the FLASH area of the TOE
	System Control Page	220427	On-chip configuration page. Stored to the FLASH area of the TOE
	System Update Page	220624	On-chip configuration page. Stored to the FLASH area of the TOE
	System Patch Page	v345_s5_v1	On-chip configuration page. Stored to the FLASH area of the TOE

Logical configuration options are provided for each physical configuration of SE310_SE, which do not modify the physical scope. Evaluated logical configuration options are all or a subset of the order entry options available in the electronic Order Entry Form [13].

Table 5 identifies these evaluated logical configuration options.

Table 5. Evaluated logical configuration options

Name of order entry option	Evaluated values
SNSE_SWOPT_RAM_INIT_SIZE	0..6144
SNSE_SWOPT_RECONSTRUCT_PUF	NO / RECON / RECON_LOCK
SNSE_SWOPT_USE_PUF	YES / NO
SNSE_SWOPT_ALLOW_SUP_TABLE	YES / NO
SNSE_SWOPT_ALLOW_SUP_SENSOR	YES / NO
SNSE_SWOPT_ENABLE_CHMODE	YES / NO
SNSE_SWOPT_ENABLE_AUTHCMD	YES / NO
SNSE_SWOPT_AUTH_REENABLE_TESTMODE	YES / NO

The TOE is integral part of the SE310 IC. Order information is given in [9].

Information on how to identify the logical configuration options of the SE310_SE after TOE Delivery and the delivery method used for SE310 are described in [10].

Note that SE310 without any Security IC Embedded Software for the TOE is available for NXP internal use only.

1.6 Evaluated Package Types

The TOE as integral part of SE310 IC is delivered as a packaged device. The security of the TOE does not rely on the way the pads are connected to the package. Therefore the security functionality of SE310 is not affected by the delivered package type.

The only available package type is "Wafer Level Chip Scale Package" (WLCSP). This package is a thin fine-pitch ball grid array package. All (enabled) pins of the TOE are externally accessible. Any additional security provided by the plastic package is ignored for the security of the TOE.

2 Conformance Claims (ASE_CCL)

This chapter is divided into the following sections: "CC Conformance Claim", "PP Claim", and "Conformance Claim Rationale".

2.1 CC Conformance Claim

This Security Target claims conformance to version 3.1 of Common Criteria for Information Technology Security Evaluation according to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017 [1].
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017 [2].
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017 [3].

The following methodology will be used for the evaluation:

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, CCMB-2017-04-004, April 2017 [4].

This Security Target claims to be CC Part 2 extended and CC Part 3 conformant. Section 6 of this Security Target defines the extended Security Functional Requirements, and also demonstrates that they are consistent with the above conformance claims.

This Security Target claims conformance to the assurance package **EAL5 augmented**. The augmentations to EAL5 are

- ASE_TSS.2 “TOE summary specification with architectural design summary”
- ALC_FLR.1 “Basic flaw remediation”
- ALC_DVS.2 “Sufficiency of security measures”
- AVA_VAN.5 “Advanced methodical vulnerability analysis”

As demonstrated in Section 7, this claim includes or exceeds the minimum assurance level for the Protection Profile identified in Section 2.2.

2.2 PP Claim

This Security Target claims conformance to the following Protection Profiles.

2.2.1 Security IC Platform (BSI-PP-0084-2014)

This Security Target claims strict conformance to Security IC Platform Protection Profile [7].

The TOE as defined in the Protection Profile is the Security IC including IC Dedicated Software without Security IC Embedded Software.

2.3 Conformance Claim Rationale

2.3.1 Security IC

Security IC is the type of TOE defined in Section 1.3.2 of this Security Target. Its components are detailed in Section 1.4 of this Security Target. These descriptions are consistent with the TOE definition in section 1.2.2 of the Protection Profile [7] .

2.3.1.1 SPD Statement for Security IC Component

The security problem definition in Section 3 of this Security Target includes all threats, organizational security policies and assumptions which are identified in the Protection Profile [7], and this without any restrictions or modifications.

2.3.1.2 Security Objectives Statement for Security IC Component

The statement of security objectives in the ST presented in Section 4 includes all security objectives as presented in the Protection Profile [7] .

2.3.1.3 Security Functional Requirements Statement for Security IC Component

The Security Functional Requirements for the Security IC component are copied from the Protection Profile [7] .

3 Security Problem Definition (ASE_SPD)

The following sections list the assets, threats, organisational security policies and assumptions of the TOE.

These are listed separately for each component to allow tracing of the conformance to the corresponding Protection Profile.

3.1 SPD related to the IC Protection Profile

3.1.1 Assets related to the IC Protection Profile

Assets are security-relevant elements to be directly protected by the TOE. Confidentiality of assets is always intended with respect to un-trusted people or software, as various parties are involved during the first stages of the smart card product life-cycle. Details concerning the threats are given in Section 3.1.2 hereafter.

Assets have to be protected, some in terms of confidentiality and some in terms of integrity or both integrity and confidentiality. These assets might get compromised by the threats that the TOE is exposed to.

The assets and emanating high-level security concerns SC1 to SC4 in section 3.1 of the Protection Profile [7] entirely apply to this Security Target.

- SC1 - Integrity of user data of the Composite TOE and of Security IC Embedded Software, while being executed/processed and while being stored in the TOE's protected memories
- SC2 - Confidentiality of user data of the Composite TOE and of Security IC Embedded Software, while being executed/processed and while being stored in the TOE's protected memories
- SC3 - Correct operation of the security services provided by the TOE for Security IC Embedded Software
- SC4 - Deficiency of Random Numbers

3.1.2 Threats related to the IC Protection Profile

The threats defined in section 3.2 of the Protection Profile [7] are listed in Table 6. They entirely apply to this Security Target.

Table 6. Threats defined in the Protection Profile

Name	Title
T.Malfunction	Malfunction due to Environmental Stress
T.Abuse-Func	Abuse of Functionality
T.Phys-Probing	Physical Probing
T.Phys-Manipulation	Physical Manipulation
T.Leak-Inherent	Inherent Information Leakage
T.Leak-Forced	Forced Information Leakage
T.RND_HW	Deficiency of Random Numbers

The threat T.RND_HW explicitly includes deficiencies of hardware (true) random numbers and corresponds to the thread T.RND in [7].

3.1.3 OSPs related to the IC Protection Profile

The organizational security policies defined in section 3.3 of the Protection Profile [7] are listed in Table 7. They entirely apply to this Security Target.

Table 7. Organizational security policies defined in the Protection Profile

Name	Title
P.Process-TOE	Identification during TOE Development and Production

3.1.4 Assumptions related to the IC Protection Profile

The assumptions defined in section 3.4 of the Protection Profile [7] are listed in Table 8. They entirely apply to this Security Target.

Table 8. Assumptions defined in the Protection Profile

Name	Title
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
A.Resp-Appl	Treatment of user data of the Composite TOE

The Security IC Embedded Software must ensure the appropriate “Treatment of user data of the Composite TOE” as specified in A.Resp-Appl. Note that SE310 without any Security IC Embedded Software is available for NXP internal use only. Furthermore, any Security IC Embedded Software is exclusively provided under control of NXP.

The Security IC Embedded Software might enable additional specific Security Services that are not defined in this Security Target. The corresponding requirements for the Security IC Embedded Software shall be defined in the Security Target of the Composite TOE.

4 Security Objectives

4.1 Security Objectives for the TOE

4.1.1 Security Objectives related to the IC Protection Profile

The security objectives for the Secure Element Hardware are defined in section 4.1 of the Protection Profile [7]. They are listed in Table 9 and apply entirely to this Security Target.

Table 9. Security objectives for the TOE defined in the Protection Profile

Name	Title
O.Malfunction	Protection against Malfunctions
O.Abuse-Func	Protection against Abuse of Functionality
O.Phys-Probing	Protection against Physical Probing
O.Phys-Manipulation	Protection against Physical Manipulation
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Leak-Forced	Protection against Forced Information Leakage
O.RND_HW	Random Numbers
O.Identification	TOE Identification

The objective O.RND_HW explicitly includes deficiencies of hardware (true) random numbers and corresponds to the objective O.RND in [7].

4.1.2 Security Objectives for the Security IC Embedded Software

The security objective for the Security IC Embedded Software defined in section 4.2 of the Protection Profile [7] is listed in Table 10. It entirely applies to this Security Target.

Table 10. Security objectives for the Security IC Embedded Software defined in the Protection Profile

Name	Title
OE.Resp-Appl	Treatment of user data of the Composite TOE

This Security Target does not add security objectives for the Security IC Embedded Software.

4.2 Security Objectives for the Operational Environment

4.2.1 Security Objectives for the Operational Environment related to the IC Protection Profile

The security objectives for the operational environment in section 4.3 of the Protection Profile [7] are listed in Table 11. They entirely apply to this Security Target.

Table 11. Security objectives for the operational environment defined in the Protection Profile

Name	Title
OE.Process-Sec-IC	Protection during composite product manufacturing

4.3 Security Objectives Rationale

In this section each threat, Organizational Security Policy, and assumption identified in Section 3 is traced to the security objectives with a rationale.

The security objectives for the TOE defined in Section 4.1 are traced back to the threats countered by them, and to the organisational security policies enforced by them. The security objectives for the operational environment defined in Section 4.2 are traced back to the assumptions they uphold.

4.3.1 Security Objective Rationale related to the IC Protection Profile

4.3.1.1 Rationale for Threats

Table 12 traces the security objectives for the TOE in Section 4.1.1 back to the threats countered by them and the organisational security policies enforced by them.

Table 12. Tracing of security objectives to threads

Name of threat	Name of security objective	Rationale
T.Malfunction	O.Malfunction	For all these threats the corresponding objectives are stated in a way, which directly corresponds to the description of the threat (refer to Section 3.2 of PP [7]). It is clear from the description of each objective (refer to Section 4.1 of PP [7]), that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds.
T.Abuse-Func	O.Abuse-Func	
T.Phys-Probing	O.Phys-Probing	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Inherent	O.Leak-Inherent	
T.Leak-Forced	O.Leak-Forced	
T.RND_HW	O.RND_HW	

4.3.1.2 Rationale for OSPs

This section traces the security objectives for the TOE in Section 4.1.1 back to the organizational security policies they uphold.

Organizational Security Policies for Secure Element Hardware:

P.Process-TOE

Objective	Rationale
O.Identification	O.Identification requires that the TOE has to support the possibility of a unique identification. The unique identification can be stored on the TOE. Since the unique identification is generated by the production environment the production environment must support the integrity of the generated unique identification. The technical and organisational security measures that ensure the security of the development environment and production environment are evaluated based on the assurance measures that are part of the evaluation. The material produced and processed by the TOE Manufacturer and the associated development and production environments are subject of the evaluation. Therefore, the organisational security policy P.Process-TOE is covered by this objective, as far as organisational measures are concerned.

4.3.1.3 Rationale for Assumptions

This section traces the security objectives for the Security IC Embedded Software in Section 4.1.2 and the security objectives for the operational environment in Section 4.2.1 back to the assumptions they uphold.

A.Resp-Appl

Name of security objective	Rationale
OE.Resp-Appl	This security objective taken from Protection Profile [7] requires the Security IC Embedded Software to implement the measures assumed in assumption A.Resp-Appl. That assumption is considered fulfilled, as the concrete requirements for the Security IC Embedded Software are defined in this Security Target.

A.Process-Sec-IC

Name of security objective	Rationale
OE.Process-Sec-IC	Since OE.Process-Sec-IC requires the Composite Product Manufacturer to implement those measures assumed in A.Process-Sec-IC, the assumption is covered by this objective.

5 Extended Components Definition (ASE_ECD)

5.1 Extended Components Definition related to the IC Protection Profile

The extended components defined in chapter 5 of the Protection Profile [7] are listed in Table 13. They entirely apply to this Security Target.

Table 13. Extended components defined in the Protection Profile

Name	Title
FCS_RNG	Generation of random numbers
FMT_LIM	Limited capabilities and availability
FAU_SAS	FAU_SAS Audit data storage
FDP_SDC	Stored data confidentiality

6 Security Functional Requirements (ASE_REQ)

6.1 Security Functional Requirements related to the IC Protection Profile

6.1.1 Security Functional Requirements

Security functional requirements from the Protection Profile [7] are applied to this Security Target as described in Section 6.1.1.1 .

6.1.1.1 Security Functional Requirements from Protection Profile

Table 14 lists the security functional requirements for the TOE, which are defined in section 6.1 of the Protection Profile [7]. They entirely apply to this Security Target.

Table 14. Security Functional Requirements from the Protection Profile

Name	Title
FRU_FLT.2	Limited fault tolerance
FPT_FLS.1	Failure with preservation of secure state
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FPT_PHP.3	Resistance to physical attack
FDP_ITT.1	Basic internal transfer protection
FPT_ITT.1	Basic internal TSF data transfer protection
FDP_IFC.1	Subset information flow control

FPT_FLS.1 requests the TSF to preserve a secure state when the TOE is exposed to operating conditions which may not be tolerated according to FRU_FLT.2. The TOE detects such operating conditions and forces itself into a secure state as long as these conditions are valid. This secure state is enforced by security feature SF.OPC as described in Section 8.2. This addresses Application Note 14 in the Protection Profile [7]. The TOE does not generate audit data for FRU_FLT.2 and/or FPT_FLS.1. This addresses Application Note 15 in the Protection Profile [7].

FPT_PHP.3 requests the TSF to resist physical manipulation and physical probing by responding automatically such that the security functional requirements are always enforced. The TOE implements two types of such automatic responses. One type of response is permanent and implicitly hampers exploitability or already incidence of physical attacks. The other type of response is conditional upon a failed check and explicitly detects physical attacks. Such type of response stops operation of the TOE or the attacked parts of it. This addresses Application Note 19 in the Protection Profile [7].

On some further Security Functional Requirements from the Protection Profile [7] operations are made. Table 15 gives an overview on the Security Functional Requirements that were subject to refinement, selection, assignment and/or iteration operations in this Security Target.

Table 15. Security Functional Requirements from the Protection Profile with operations done in this Security Target

Name	Title
FAU_SAS.1	Audit storage
FDP_SDC.1	Stored data confidentiality
FDP_SDI.2: • FDP_SDI.2/FLT	Stored data integrity monitoring and action
FCS_RNG.1: • FCS_RNG.1/PTG.2	Random number generation

Iteration operations are notified by a slash, which is appended to the name of the security functional requirement and followed by an identifier. Selection and assignment operations are denoted in italics. Refinements are denoted just as described in the Protection Profile [7]. Note that this convention only applies to the current chapter.

This Security Target performs selection and assignment operations on FAU_SAS.1 according to Application Note 17 in the Protection Profile [7].

FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the test process before TOE Delivery with the capability to store *the Initialisation Data, Pre-personalisation Data and other user data*[3] in the *Flash memory* [4].

This Security Target performs one assignment operation on FDP_SDC.1 according to Application Note 18 in the Protection Profile [7].

FDP_SDC.1	**Stored data confidentiality**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *Flash memory, the System RAM, the PKC RAM and the Buffer RAM* [5].

This Security Target performs one iteration operation on FDP_SDI.2, which complies with section 8.1 in CC Part 1 [1], and also performs two assignment operations on that iteration according to Application Note 18 in the Protection Profile [7].

FDP_SDI.2/FLT	**Stored data integrity monitoring and action - Faults**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1/FLT	The TSF shall monitor user data stored in containers controlled by the TSF for *modification, deletion,*

3 [selection: *the Initialisation Data, Pre-personalisation Data, [assignment: other data]*]
4 [assignment: *type of persistent memory*]
5 [assignment: *memory area*]

	repetition or loss of data [6] on all objects, based on the following attributes: *integrity check information associated with the data including code stored to the Flash memory, the ROM, the System RAM, the PKC RAM and the Buffer RAM* [7].
FDP_SDI.2.2/FLT	Upon detection of a data integrity error, the TSF shall *correct the error or trigger a security reset or raise a non-maskable interrupt* [8].

This Security Target performs an iteration operation on FCS_RNG.1, which complies with section 8.1 in CC Part 1 [1]. It also performs two assignment operations according to Application Note 21 in the Protection Profile [7]. The operations follow the example and its Application Note 44 in section 7.5.1 of the Protection Profile [7] in consideration of the updated documents [6] and [5].

FCS_RNG.1/PTG.2	**Random number generation - PTG.2**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Note:	This security functional requirement complies with PTG.2 in [5]
FCS_RNG.1.1/PTG.2	The TSF shall provide a *physical* [9] random number generator that implements: { *(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.* *(PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.* *(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.* *(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.* *(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the*

6 [assignment: *integrity errors*]
7 [assignment: *memory area*]
8 [assignment: *action to be taken*]
9 [selection: *physical, hybrid physical, hybrid deterministic*]

	statistical properties of the raw random numbers within an acceptable period of time. }[10]
FCS_RNG.1.2/PTG.2	The TSF shall provide *octets of bits or packages of 32 bits*[11] that meet { *(PTG.2.6) Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.* *(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.* }[12]

6.1.2 Security Requirements Rationale

6.1.2.1 Rationale for the Security Functional Requirements

The Security Objectives for the TOE are mapped to the Security Functional Requirements in Table 16 .

It indicates the sufficient necessity and rationality of security requirements, that is, each security objective has at least one security functional requirement corresponding to it, and each security functional requirement solves at least one security objective, which is sufficient and necessary for security objectives.

Table 16. Mapping of the Security Objectives for the TOE to the Security Functional Requirements for the TOE

Security Objective for the TOE	Security Functional Requirement of the TOE
O.Malfunction	FRU_FLT.2, FPT_FLS.1
O.Abuse-Func	FMT_LIM.1, FMT_LIM.2
	FRU_FLT.2, FTP_FLS.1
	FPT_PHP.3
	FDP_ITT.1, FPT_ITT.1, FDP_IFC.1
O.Phys-Probing	FPT_PHP.3
	FDP_SDC.1
O.Phys-Manipulation	FDP_SDI.2/FLT
	FPT_PHP.3
O.Leak-Inherent	FDP_ITT.1, FPT_ITT.1 , FDP_IFC.1
O.Leak-Forced	FRU_FLT.2, FPT_FLS.1
	FPT_PHP.3

10 [assignment: *list of security capabilities*]
11 [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*]
12 [assignment: *a defined quality metric*]

Table 16. Mapping of the Security Objectives for the TOE to the Security Functional Requirements for the TOE ***...continued***

Security Objective for the TOE	Security Functional Requirement of the TOE
	FDP_ITT.1, FPT_ITT.1, FDP_IFC.1
O.RND_HW	FCS_RNG.1/PTG.2
	FRU_FLT.2, FPT_FLS.1
	FPT_PHP.3
	FDP_ITT.1, FPT_ITT.1 , FDP_IFC.1
O.Identification	FAU_SAS.1

The green colored cells in Table 16 show how the Protection Profile [7] maps its security objectives for the TOE to the Security Functional Requirements for the TOE, see section 6.3.1 and section 7.4.2. of the Protection Profile [7]. Section 6.3.1 of the Protection Profile [7] also gives the rationale for the mappings colored in green.

6.1.3 Security Requirements Dependencies

6.1.3.1 Dependencies of Security Functional Requirements

The dependencies of the Security Functional Requirements for the TOE are given in Table 17.

Table 17. Dependencies of the Security Functional Requirements for the TOE

SFR of the TOE	Dependencies	Fullfilled by SFRs
FRU_FLT.2	FPT_FLS.1	FPT_FLS.1
FPT_FLS.1	none	N/A
FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
FPT_PHP.3	none	N/A
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1
FPT_ITT.1	none	N/A
FDP_IFC.1	FDP_IFF.1	N/A, see sec. 6.3.2 in PP [7]
FAU_SAS.1	none	N/A
FDP_SDC.1	none	N/A
FDP_SDI.2/FLT	none	N/A
FCS_RNG.1/PTG.2	none	N/A

6.1.3.2 Security Requirements are Internally Consistent

The statement on internal consistency of security requirements in section 6.3.4 of the Protection Profile [7] entirely applies to this Security Target.

7 Security Assurance Requirements (ASE_REQ)

7.1 Security Assurance Requirements related to the IC Protection Profile

The Security Assurance Requirements for the Secure Element Hardware are listed in Table 18. These Security Assurance Requirements are augmented from the Protection Profile [7] to EAL5+ with additional Security Assurance Requirements ASE_TSS.2, AVA_VAN.5, ALC_DVS.2 and ALC_FLR.1.

Table 18. Security Assurance Requirements for the Secure Element Hardware

Name	Title	compared to PP [7]
ADV_ARC.1	Security architectural description	as in PP
ADV_FSP.5	Complete semi-formal functional specification with additional error information	augmented from PP to EAL5
ADV_IMP.1	Implementation representation of the TSF	as in PP
ADV_INT.2	Well-structured internals	added for EAL5
ADV_TDS.4	Semiformal modular design	augmented from PP to EAL5
AGD_OPE.1	Operational user guidance	as in PP
AGD_PRE.1	Preparative procedures	as in PP
ALC_CMC.4	Production support, acceptance procedures and automation	as in PP
ALC_CMS.5	Development tools CM coverage	augmented from PP to EAL5
ALC_DEL.1	Delivery procedures	as in PP
ALC_DVS.2	Sufficiency of security measures	as in PP
ALC_FLR.1	Basic flaw remediation	not in PP, added for EAL5+
ALC_LCD.1	Developer defined life-cycle model	as in PP
ALC_TAT.2	Compliance with implementation standards	augmented from PP to EAL5
ASE_CCL.1	Conformance claims	as in PP
ASE_ECD.1	Extended components definition	as in PP
ASE_INT.1	ST introduction	as in PP
ASE_OBJ.2	Security objectives	as in PP
ASE_REQ.2	Derived security requirements	as in PP
ASE_SPD.1	Security problem definition	as in PP
ASE_TSS.2	TOE summary specification with architectural design summary	augmented from PP to EAL5+
ATE_COV.2	Analysis of coverage	as in PP
ATE_DPT.3	Testing: modular design	augmented from PP
ATE_FUN.1	Functional testing	as in PP
ATE_IND.2	Independent testing - sample	as in PP
AVA_VAN.5	Advanced methodical vulnerability analysis	as in PP

All refinements in section 6.2.1 of the Protection Profile [7] to security assurance requirements in Table 18, which are augmented from the Protection Profile, are discussed below in their applicability to this Security Target. This addresses Application Note 23 in the Protection Profile [7].

Refinements regarding ADV_FSP

Refinement no. 215 to ADV_FSP.4 in the Protection Profile [7] is not relevant for this Security Target since the TOE does not embed IC Dedicated Test Software.

The Factory OS is not considered as IC Dedicated Test Software but instead as IC Dedicated Support Software since it is **not** only used to support testing of the TOE during production and **does** provide security functionality to be used after TOE delivery, which both contradicts to abstract 12 on page 8 of the Protection Profile [7]. However, the Factory OS provides testing capabilities for production testing and analysis of field returns, which is under restricted access to NXP and not for usage by the Composite Product Manufacturer. Therefore, these testing capabilities are considered as "test tool", which don't have to be described in the Functional Specification, but only be evaluated against their abuse after TOE delivery. Apart from that the Factory OS provides some basic functional testing of Secure Element Hardware and also with a readout of the identification flags of Secure Element Hardware from System Page Common, which must be described in the Functional Specification.

Refinements no. 216, no. 217 and no. 218 to ADV_FSP.4 in the Protection Profile [7] are entirely applicable to ADV_FSP.5 since the refinements clarify the scope of the functional specification, and ADV_FSP.5 adds to this scope in accordance with the refinements.

Refinements regarding ALC_CMS

Refinement no. 199 to ALC_CMS.4 in the Protection Profile [7] is a clarification of the configuration item "TOE implementation representation". Although NXP as the TOE manufacturer is providing the Security IC Embedded Software, this item is not relevant for the configuration list, as the Security IC Embedded Software is developed independently from the TOE.

Compared to ALC_CMS.4 component ALC_CMS.5 only adds the requirement for a new configuration items to be included in the configuration list. (ALC_CMS.5.1C). Therefore the refinement in the PP regarding ADV_CMS.4 can be applied without changes and is valid for ADV_CMS.5.

7.2 Rationale for the Security Assurance Requirements

This Security Target augments from EAL4 to EAL5 in order to meet increasing assurance expectations on the resistance to attackers with high attack potential.

This Security Target augments EAL5 with ALC_FLR.1 to cover policies and procedures that are applied to track and correct flaws and to support surveillance of the TOE. Furthermore, ASE_TSS.2 is chosen to give architectural information on the security functionality of the TOE, which enhances comprehensibility.

The assurance level EAL5 is an elaborated pre-defined level of the CC, part 3 [3]. The assurance components in an EAL level are chosen in a way that they build a mutually supportive and complete set of components. The additional requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL5. Therefore, the components AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 and ALC_FLR.1 serve additional assurance to EAL5, but the mutual support of the requirements is still guaranteed.

7.3 Dependencies of Security Assurance Requirements

The dependencies of the Security Assurance Requirements are given in Table 19. They are derived from Appendix C of CC [3] . The table indicates whether the SAR is directly or indirectly required. Only applicable dependencies from the highest level assurance components are considered.

Table 19. Dependencies of the Security assurance requirements

Name	Directly required	Indirectly required
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	ADV_FSP.2
ADV_FSP.5	ADV_IMP.1, ADV_TDS.1	ADV_TDS.3, ALC_TAT.1
ADV_IMP.1	ADV_TDS.3, ALC_TAT.1	ADV_FSP.4
ADV_INT.2	ADV_IMP.1, ADV_TDS.3, ALC_TAT.1	ADV_FSP.4,
ADV_TDS.4	ADV_FSP.5	ADV_IMP.1
AGD_OPE.1	ADV_FSP.1	none
AGD_PRE.1	none	none
ALC_CMC.4	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	none
ALC_CMS.5	none	none
ALC_DEL.1	none	none
ALC_DVS.2	none	none
ALC_FLR.1	none	none
ALC_LCD.1	none	none
ALC_TAT.2	ADV_IMP.1	ADV_TDS.3
ASE_CCL.1	ASE_ECD.1, ASE_INT.1, ASE_REQ.1	none
ASE_ECD.1	none	none
ASE_INT.1	none	none
ASE_OBJ.2	ASE_SPD.1	none
ASE_REQ.2	ASE_ECD.1, ASE_OBJ.2	ASE_SPD.1
ASE_SPD.1	none	none
ASE_TSS.2	ADV_ARC.1, ASE_INT.1, ASE_REQ.1	ADV_FSP.1, ADV_TDS.1, ASE_ECD.1
ATE_COV.2	ADV_FSP.2, ATE_FUN.1	ADV_TDS.1
ATE_DPT.3	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1	ADV_FSP.5, ARE_COV.1
ATE_FUN.1	ATE_COV.1	ADV_FSP.2, ATE_FUN.1
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_ PRE.1, ATE_COV.1, ATE_FUN.1	ADV_TDS.1
AVA_VAN.5	ADV_ARC.1, ADV_FSP4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_ PRE.1, ATE_DPT.1	ALC_TAT.1, ATE_FUN.1

8 TOE summary specification (ASE_TSS)

8.1 Introduction

The Security Functions (SF) and Security Services (SS) introduced in this section realize the SFRs of the TOE. Each SF/SS consists of components spread over several TOE modules to provide a security functionality and fulfill SFRs.

8.2 Security Functionality of the SE310 Secure Element

The TOE Security Functionality (TSF) of the SE310 Secure Element is composed of Security Services (SS) and Security Features (SF). They together fulfill the Security Functional Requirements for the TOE, which are identified in Section 6.1.1.

The Security Services of the TOE are summarized in Table 20 and described in Section 8.2.1. The Security Features of the TOE are summarized in Table 21 and described in Section 8.2.2.

The TOE also implements security functionality, which is not part of its Security Services and Security Features, like the cryptographic coprocessors. Such security functionality isn't required to meet the Security Functional Requirements for the TOE. Instead, it can be used by Security IC Embedded Software to implement further Security Services and Security Features.

Table 20. Security Services of the SE310 Secure Element

Security Services	Name
SS.RNG	Random Number Generator

Table 21. Security Features of the SE310 Secure Element

Security Features	Name
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation
SF.LOG	Logical Protection
SF.FOS-USE	FactoryOS use restrictions

8.2.1 Security Services of the SE310 Secure Element

8.2.1.1 SS.RNG : Random Number Generator

SS.RNG serves Security IC Embedded Software with random numbers.

For this purpose SS.RNG implements a physical Random Number Generator, which claims functionality class PTG2 of the pre-defined RNG classes in [5]. This Security Service is suited e.g. for generation of signature key pairs, generation of session keys for symmetric encryption mechanisms, random padding bits, zero-knowledge proofs or generation of seeds for Digital Random Number Generation (DRNG).

The Random Number Generator fulfills the online test requirements defined in [5] and embeds hardware test functionality to detect hardware defects and quality issues of the random numbers.

8.2.2 Security Features of the SE310 Secure Element

8.2.2.1 SF.OPC : Control of Operating Conditions

SF.OPC controls operating conditions of the TOE. These are explicitly controlled by security functionality that simply hampers feeding certain electrical stimulations into the device. Such security functionality is composed of frequency filters and voltage limiters. Operating conditions of the device are explicitly controlled also by security functionality that actively monitors certain electrical parameters. These parameters are voltage levels of external supply from pad and internal supplies, frequencies of internal clocks and on-chip temperature. Such security functionality raises an error message whenever a monitored parameter drops out of its valid range. In addition, exposure of the device to light is explicitly controlled by security functionality that senses abnormal light over its whole surface, raising an error message when detected.

SF.OPC also controls operating conditions implicitly. This is done by security functionality that detects faults in code and data stored to memories and while processed in the device. Such faults might be inserted by electrical stimulations or by exposure of the device to energy or particles. Error detection codes are used to protect the memories as well as the access channels over the bus system to memories and to hardware peripherals on the control bus. Watchdogs on error detection codes run over code and data stored to RAM, and the Secure Fetch Plus on code and data read from Flash memory can be configured and enabled by Security IC Embedded Software.

Further on, Security IC Embedded Software can configure and enable a Secure Fetch on CPU code and/or data accesses over the bus system and also range checks on values in general purpose, stack pointers and link registers of the CPU as well as checks on predefined CPU instructions for zero values in their operands or in the addresses of their resulting data accesses to memory. In addition, Security IC Embedded Software may protect its program flow by use of a signature watchdog on CPU code accesses over the bus system, by use of a secure counter and by use of a watchdog timer.

In case an error message is raised the TOE either (i) aborts code execution and forces a reset or (ii) raises an exception, which interrupts code execution and jumps to an exception vector on which the Security IC Embedded Software can react with an appropriate exception handler. In case of reset the TOE returns to its initial state and provides information on the reset source to the Security IC Embedded Software. In case of an exception the TOE provides information on the exception source to the Security IC Embedded Software.

SF.OPC also implements security functionality that corrects errors in Flash memory.

8.2.2.2 SF.PHY : Protection against Physical Manipulation

SF.PHY protects the TOE from physical probing and physical manipulation of its hardware, its IC Dedicated Software, its TSF data and Security IC Embedded Software stored to its Flash memory including user data of the Composite TOE. This is achieved by appropriate shielding techniques for all elements in the physical design of the TOE, by redundant CPU core, by redundant routing of sensitive signals, by layout constraints on particular placements and routings.

Selected security functionality in analog design parts of the TOE is additionally checked for its basic operability by a built-in selftests that run during startup of the device.

Memories and their interfaces are additionally protected against probing by appropriate encryption of stored content and address scrambling mechanisms.

8.2.2.3 SF.LOG : Logical Protection

SF.LOG provides logical protection of the TOE that fights disclosure of confidential data stored to and processed in the TOE through tracing of power consumption or emanation and subsequent complex signal analysis.

Secure data transfers from memory to memory or from memories to peripherals on the control bus are managed by the secure copy engine (SMA). All such transfers are fully masked from source to destination across the bus infrastructure.

SYM-Lite coprocessor provides secure general purpose operations over sensitive data outside the CPU.

The cryptographic coprocessors implement functionality that effectively reduces side channel leakage by adding noise, inserting dummy activity and randomizations if used for implementation of security functions under control of the Security IC Embedded Software (not in scope of this Security Target).

8.2.2.4 SF.FOS-USE : FactoryOS use restrictions

SF.FOS-USE restricts use of the FactoryOS among three levels of testing capabilities of the TOE. Access to the lower level of testing capabilities is not blocked. Instead, its testing capabilities are very limited so that they cannot be exploited. The medium level of testing capabilities is blocked by an authentication procedure. After successful authentication to this level the TOE serves with testing capabilities to the extent that confidentiality of content stored to its memories cannot be compromised.

The upper level of testing capabilities is blocked by two authentication checks, of which the latter one also forces an erase of Flash windows as well as System Pages before full testing capabilities are provided.

Commands of the FactoryOS are conditionally installed in stages and commands with test functionality are cut to tests of basic functionality only.

SF.FOS-USE also ensures that even the corresponding administrator cannot modify the identification data of chip after the IC card chip enters the use stage.

8.3 TOE Summary Specification Rationale

Deleted here, only available in the full version of the Security Target.

9 Bibliography

9 . 1 Evaluation documents

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017

[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] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, CCMB-2017-04-004, April 2017

[5] 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.

[6] Evaluation of random number generators, Bundesamt für Sicherheit in der Informationstechnik, Version 0.10

[7] 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.

9 . 2 Developer documents

[8] SE310_SE Information on Guidance and Operation, Revision 0.3, 22.02.2023, NXP Semiconductors

[9] SE310S Embedded Secure Element, Product data sheet, Revision 3.1, 10.05.2023, DocID 737131, NXP Semiconductors

[10] SE310 TOE Identification (for A0), Data sheet addendum, Revision 1.0, 16.01.2023, DocID 761810, NXP Semiconductors

[11] SE310_SE Programmers's Manual, Application Note, Revision 0.1, DocID 761901, 22.08.2022, NXP Semiconductors

[12] ARM® Cortex®-M33 Processor Technical Reference Material, Revision r1p0, ARM Limited

[13] Order Entry Form, online document, NXP Semiconductors

10 Legal information

10.1 Definitions

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

10.2 Disclaimers

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

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

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

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

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

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

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

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

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

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

Suitability for use in 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, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

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

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

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

10.3 Trademarks

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

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

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: 22 May 2023
Document identifier: NXP-ST01-SE310-Jxxxx