NXP NSN4XX2M0 Series - Secure Element

Security Target Lite

Rev. 1.4 — 27 April 2026 **Product evaluation document**

EUCC-2500173-01

Document information

Information	Content
Keywords	NXP, ASE, NSN4XX2M0 Single Chip Secured (NFC) Controller Series, Single Chip Secure Element and NFC Controller, Common Criteria, EAL5+
Abstract	This document is the Security Target of the NSN4XX2M0 Series - 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 CC:2022 with augmentations.

Revision History

Revision history

Revision number	Date	Description
1.4	2026-04-27	This ST-lite is derived from the full Security Target v1.4. It contains an identical TOE introduction in accordance with EUCC Implementing Regulation Annex V.2, item 3(a).

1 ST Introduction (ASE_INT)

1.1 ST Reference

"NXP NSN4XX2M0 Series - Secure Element", Security Target Lite, Revision 1.4, 27 April 2026.

1.2 TOE Reference

Table 1. TOE Reference

Content	Version
Product Type	Secure Element subsystem of the IC hardware platform NSN4XX2M0 with IC Dedicated Support Software and documentation describing usage of the TOE
TOE name	NXP NSN4XX2M0 Series - Secure Element (In this document, the TOE name is abbreviated as "*NSN4XX2M0_SE*")
TOE version(s)	*NSN4XX2M0_SE* ***B1.1.000 J6***

1.3 TOE Type

The TOE is classified as a Security IC Platform providing a hardware-based security environment for Security IC Embedded Software. The TOE comprises only the security-relevant hardware of the NSN4XX2M0 Secure Element subsystem and implements security features required for resistance against physical, environmental, and logical attacks.

1.4 TOE Overview

The TOE is the Embedded Secure Element subsystem (NSN4XX2M0_SE) of the NSN4XX2M0 Single Chip Secured (NFC) Controller Series. The TOE is defined as the NSN4XX2M0_SE Secure IC hardware platform together with its IC Dedicated Software and constitutes the only TOE configuration. The TOE is not available or provided without Security IC Embedded Software.

The overall product is implemented as a monolithic integrated circuit integrating multiple functional subsystems:

- NSN4XX2M0_SE – Embedded Secure Element (part of the TOE)
- NSN4XX2M0_NFC – NFC Controller subsystem (not part of the TOE)
- NSN4XX2M0_PMU – shared Power Management Unit (not part of the TOE)

The NSN4XX2M0_SE is a secure microcontroller integrating a high-frequency ARM Cortex-M33 core and dedicated cryptographic hardware accelerators. It provides secure memory structures, hardware-supported mechanisms addressing information leakage and faulty behavior, as well as sensors and tamper-detection and response mechanisms. The NSN_SE serves as a secure hardware platform for Security IC Embedded Software, supporting the confidentiality and integrity of data and code when operated in environments where an attacker may have physical access to the device.

The TOE is designed to support secure execution and secure storage functions and to provide resistance against logical attacks, environmental manipulation, and physical attacks, including semi-invasive and invasive methods, in accordance with the threat model, assumptions, and security objectives defined in this Security Target and the

applicable Protection Profile [10]. The TOE boundary is illustrated in Figure 1. The following sections describe the TOE architecture and interfaces in more detail.

Only the NSN4XX2M0_SE subsystem and its IC Dedicated Software are included within the TOE boundary.

A separate Security Target will address the composite product consisting of the NSN4XX2M0_SE hardware platform and Security IC Embedded Software.

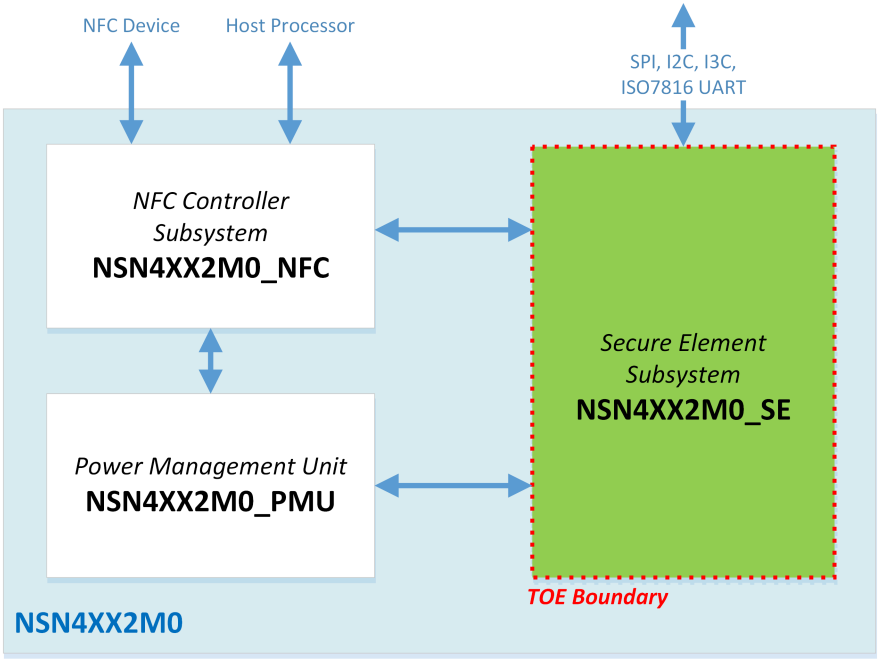

Figure 1. Place in the system

1.5 TOE Description

1.5.1 TOE Hardware Description

The toplevel block diagram of the NSN4XX2M0 Secure Element subsystem is depicted in Figure 2. The hardware part of the NSN4XX2M0_SE is referred to as Secure Element Hardware in the following.

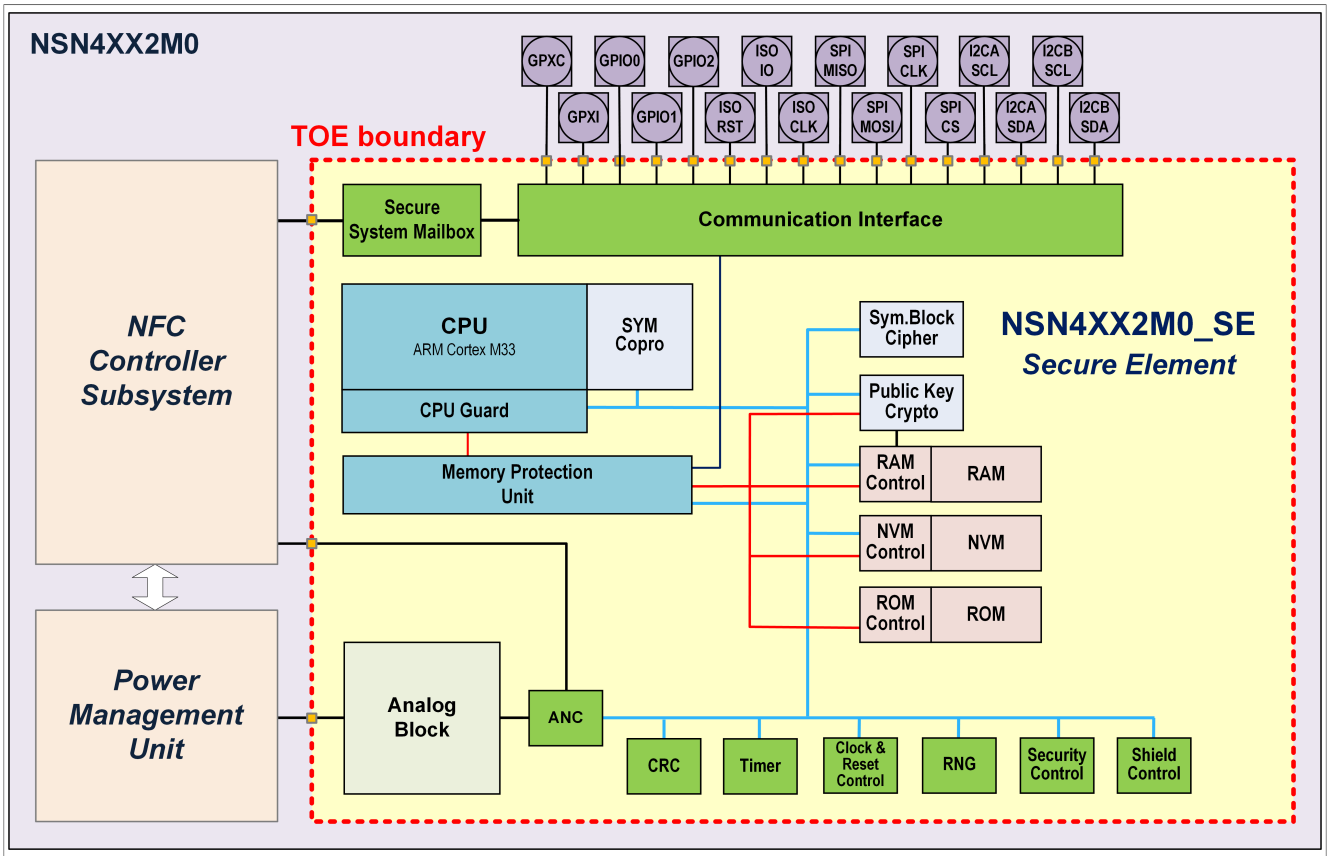

Figure 2. Block Diagram of the Secure Element Hardware

Secure Element Hardware Architecture

The TOE incorporates a high-frequency clocked ARM Cortex-M33 processor augmented by dedicated coprocessors for cryptographic and security-related processing, and connected through a secure internal bus system. The internal bus system provides controlled access to on-chip memories, cryptographic and computational hardware peripherals, and communication interfaces.

The secure internal bus system associates context information with each bus transaction, enabling hardware-enforced access restrictions and the detection of invalid or unauthorized accesses.

The TOE integrates dedicated hardware accelerators to support symmetric-key, public-key, and post-quantum cryptographic operations, as well as a hardware true random number generator.

The memory subsystem of the TOE comprises read-only memory (ROM); non-volatile memory implemented as resistive RAM (RRAM); and volatile memory resources, including System RAM, dedicated PKC RAM, and Buffer RAM. Access to memory resources is enforced by hardware mechanisms.

Cryptographic and Computational Hardware

The TOE provides dedicated cryptographic and security-related hardware functionality through a set of tightly integrated accelerators and coprocessors. These hardware components support symmetric-key cryptographic operations, public-key cryptographic

operations, and post-quantum cryptographic computations, as well as hardware-based random number generation.

The TOE further integrates a symmetric coprocessor operating under the control of the main processor to support secure processing of sensitive data and protected data movement within the Secure Element.

Security Mechanisms Supporting Protection Against Physical Attacks

The TOE implements a range of hardware-based security mechanisms designed to maintain correct operation of the security functionality and to preserve the confidentiality and integrity of data and code during processing and storage, including in scenarios where an attacker has physical access to the device.

These security mechanisms include, in particular:

- hardware mechanisms supporting the confidentiality of stored and processed data, such as memory encryption and masking,
- hardware mechanisms supporting data and code integrity, including error detection and correction,
- environmental monitoring mechanisms observing operating conditions such as voltage, frequency, temperature, and light exposure,
- active shielding structures
- monitoring and control mechanisms such as watchdog counters and CPU Guard functionality, and
- hardware mechanisms supporting resistance against fault injection, glitching, and tamper attempts.

The integrated IC hardware is protected by shielding structures and monitored by dedicated sensors to increase resistance against physical manipulation.

Scope of Security Functionality

The security functionality of the TOE is designed to act as part of an integral security system composed of the Secure Element Hardware platform and Security IC Embedded Software. Certain security mechanisms are completely implemented in and controlled by the TOE hardware, while other security mechanisms rely on correct use by the Security IC Embedded Software and are outside the scope of the TOE defined in this Security Target.

This Security Target addresses only the Secure Element Hardware platform together with the IC Dedicated Software. The IC Dedicated Software is limited to low-level functionality supporting configuration, initialization, and controlled operation of the hardware security mechanisms.

Cryptographic functionality provided by the hardware accelerators is evaluated with respect to resistance against physical manipulation at the hardware level as described in chapter 5 of [9]. The correct and secure usage of this cryptographic functionality by higher-level Security Services requires the availability of a Cryptographic Library, which is not part of the TOE. **Such Security Services and Security Features are outside the scope of this Security Target and will be evaluated as part of a separate Security Target for the composite product including Security IC Embedded Software.**

No access control policy as defined by the optional package of the Protection Profile [10] is claimed by the TOE; memory protection is realized solely by fixed hardware mechanisms supporting resistance against physical manipulation.

1.5.2 IC Dedicated Software

The TOE includes IC Dedicated Software that is executed on the NSN4XX2M0_SE during secure initialization, testing, and transitions between operational states. This software supports the correct operation of the TOE hardware and enables secure configuration and lifecycle control of the Secure Element.

The IC Dedicated Software comprises the following components:

BootOS

The BootOS is executed at each reset or power-on. It is responsible for:

- secure initialization of the Secure Element,
- configuration of security-relevant hardware components,
- establishment of a trusted operational state, and
- controlled transition to Mission Mode or (if enabled) Test Mode.

FactoryOS

The FactoryOS is executed during manufacturing and, if applicable, during controlled field-return analysis. It provides functionality for:

- secure loading of software into non-volatile memory,
- controlled access to test functionality,
- production testing features (full capabilities under NXP control)
- restricted diagnostics in field-return scenarios,
- protection mechanisms preventing disclosure of confidential data, and
- basic functional tests and reading of TOE identification data (if enabled via OEF)

Firmware Library

The Firmware Library provides hardware abstraction functions supporting essential non-volatile memory operations required during Boot Mode and Test Mode. It ensures controlled access to non-volatile memory prior to entering Mission Mode.

The BootOS, FactoryOS, and Firmware Library are primarily stored in ROM. In order to support corrective maintenance, patches to the BootOS may be stored in non-volatile memory (NVM). Execution of patched functionality is controlled by hardware mechanisms of the TOE. The IC Dedicated Software remains defined by the ROM-resident code together with hardware-controlled patches, without modifying the TOE boundary.

The TOE does not include communication software drivers. The Secure Element hardware provides hardware-implemented physical and electrical communication interfaces (e.g. I2C, SPI). Any communication functionality requiring software support, including communication drivers and protocol handling, is implemented by Security IC Embedded Software as part of the composite product and is outside the scope of this Security Target.

1.6 TOE Boundary

1.6.1 Physical TOE Boundary

The TOE is a hardware-based Secure Element platform implemented within a single monolithic integrated circuit. The physical TOE boundary encompasses all hardware components that form the NSN4XX2M0_SE subsystem and that contribute to the implementation of the TSF.

. The physical TOE boundary includes, in particular:

- the main processing unit of the TOE subsystem and its associated coprocessors,
- cryptographic and security-related hardware accelerators,
- on-chip non-volatile and volatile memory components belonging to the NSN4XX2M0_SE subsystem,
- the secure internal bus system interconnecting the TOE hardware components,
- hardware-based security sensors and monitoring mechanisms,
- hardware mechanisms supporting tamper detection and resistance, and
- secure peripheral and interface logic belonging to the TOE subsystem.

All hardware components belonging to the NSN4XX2M0_SE subsystem that contribute to the TSF are part of the TOE.

Excluded from the TOE, although implemented on the same integrated circuit, are:

- the NSN4XX2M0_NFC subsystem, and
- the NSN4XX2M0_PMU subsystem

as introduced in Section Section 1.4 of this Security Target. These subsystems are physically and logically separated from the NSN4XX2M0_SE subsystem and do not contribute to the TSF.

1.6.2 Logical TOE Boundary

The logical TOE boundary is defined by the TSF provided by the Secure Element platform and evaluated according to the Protection Profile [10].

The TSF are primarily enforced by dedicated hardware mechanisms of the NSN4XX2M0_SE subsystem. IC Dedicated Software supports the correct configuration, initialization, and controlled operation of these hardware security mechanisms but does not implement higher-level security services or protocols.

The TSF provided by the TOE include, in particular:

- hardware-implemented cryptographic functions supporting symmetric-key, public-key, and post-quantum cryptographic operations, evaluated with respect to resistance against physical manipulation,
- hardware-enforced memory isolation and protection mechanisms preventing unauthorized physical access, modification, or observation of on-chip non-volatile and volatile memories,
- generation of random numbers by a dedicated hardware true random number generator (TRNG),
- hardware mechanisms for detection of abnormal operating conditions, fault injection attempts, and tamper events,
- protective hardware mechanisms supporting the confidentiality and integrity of user data and TSF data, and
- hardware-based active shielding and monitoring mechanisms.

Excluded from the logical TOE boundary are:

- Security IC Embedded Software, providing higher-level security services, including communication drivers and protocol handling,
- cryptographic libraries implementing higher-level use of cryptographic primitives,
- Firmware associated with NSN4XX2M0_NFC, and
- Firmware associated with NSN4XX2M0_PMU.

The TOE provides hardware-implemented physical and electrical communication interfaces (e.g. I2C, SPI). Communication functionality requiring software support, such as communication drivers and protocol handling, is provided by Security IC Embedded Software as part of the composite product and does not form part of the TSF of this TOE.

Higher-level Security Services and Security Features making use of the evaluated Secure Element platform are outside the scope of this Security Target and are intended to be assessed as part of a separate Security Target for the composite product.

1.6.3 Required non-TOE Hardware/Software/Firmware

Besides the NSN4XX2M0_SE subsystem, the NSN4XX2M0 Single Chip Secured (NFC) Controller comprises a NFC controller subsystem (NSN4XX2M0_NFC) and a shared Power Management Unit (NSN4XX2M0_PMU).

The NSN4XX2M0_SE requires the full functionality of the NSN4XX2M0_PMU in order to power-up and operate correctly. Power-up and power management control of the NSN4XX2M0_PMU are performed by software executed on the NSN4XX2M0_NFC subsystem. These components are therefore required for correct operation of the TOE but do not provide security functionality claimed by this Security Target. An overview of these components is provided in Figure 1.

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

1.6.4 Evaluated Package Types

The TOE, as integral part of the NSN4XX2M0 IC, is delivered as a packaged device. The security of the TOE does not depend on how the pads are connected to the package; therefore, the security functionality is not influenced by the specific package type used.

The device is available exclusively in a Wafer Level Chip Scale Package (WLCSP), a thin fine-pitch ball-grid array package in which all enabled pins of the TOE are externally accessible. Any additional physical protection that might be provided by the plastic encapsulation is not taken into account for the security of the TOE.

1.7 TOE Interfaces

The TOE provides interfaces that support controlled interaction with the Secure Element hardware for initialization, configuration, and normal operation. These interfaces are used by IC Dedicated Support Software and by Security IC Embedded Software to access hardware functionality in accordance with the hardware-enforced restrictions and operational conditions of the TOE.

External interaction with the TOE is performed exclusively through chip-external interfaces of the integrated circuit. All external interfaces are mediated by dedicated

hardware mechanisms and are subject to the current operational state and execution context of the TOE.

Electrical Interfaces

The electrical interfaces of the TOE comprise the signal lines between the I/O interface logic of the NSN4XX2M0_SE subsystem and the external communication pads that are exclusively assigned to the TOE.

The TOE supports communication via the following electrical interfaces:

- a Serial Peripheral Interface (SPI),
- two I2C interfaces,
- an I3C interface, sharing physical pins with one of the I2C interfaces,
- an ISO/IEC 7816 compliant interface using ISO/IEC 7816 UART, and
- a GPIO interface accessed via Special Function Registers.

Internal electrical connections exist between the TOE and the following subsystems implemented on the same integrated circuit:

- the NSN4XX2M0_PMU subsystem (power, ground), and
- the NSN4XX2M0_NFC subsystem (clock, reset, Secure System Mailbox signals).

Logical Interfaces

Figure 3 illustrates the logical interface between the TOE and the Security IC Embedded Software. Internal logical interfaces within the TOE are not shown.

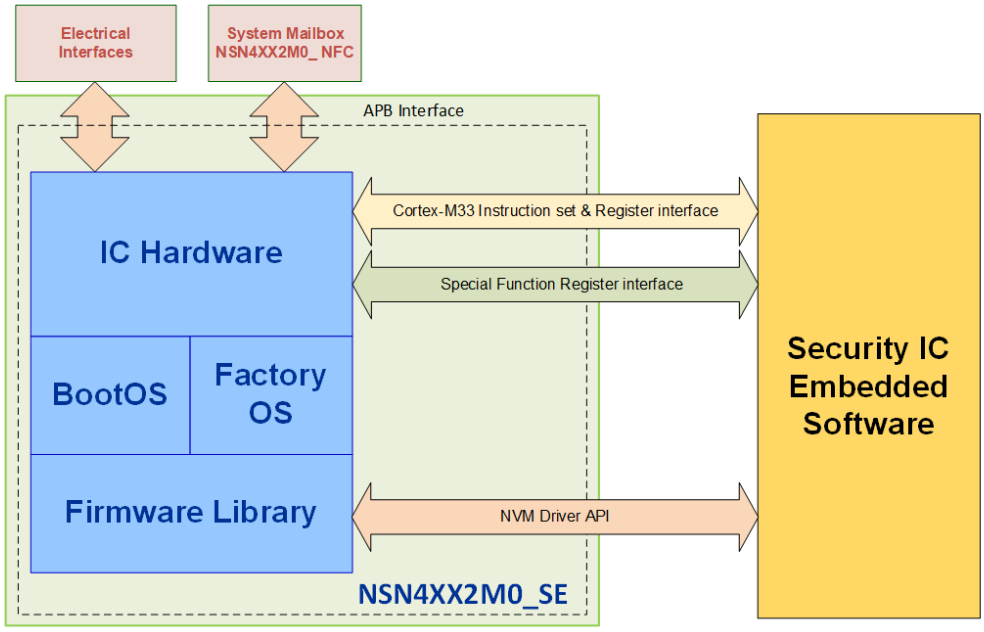

Figure 3. Logical interface of the TOE

The logical interface of the TOE accessible to the Security IC Embedded Software implements the mediation between the Security IC Embedded Software and the TOE hardware resources and provides the following logical interface channels:

- Secure System Mailbox interface for controlled data exchange with NSN4XX2M0_NFC subsystem,
- CPU Instruction set and Register interface acc. to [15]
- access to Special Function Registers acc. to [14]
- access to non-volatile memory control functionality via an NVM driver interface.

All logical interfaces, with exception of the Secure System Mailbox interface, are accessible through the electrical interfaces SPI, I2C, I3C, UART, and GPIO.

Physical interfaces

The surface of the integrated circuit is considered a physical interface of the TOE and is exposed to potential physical manipulation attempts. The TOE incorporates multiple hardware-based tamper-resistance and monitoring mechanisms to protect this physical interface.

1.8 TOE Identification

1.8.1 Evaluated Hardware Configurations

Each evaluated configuration of the TOE is defined by a specific physical and logical configuration.

The physical configuration comprises the Secure Element hardware components, including the ROM-resident code forming the IC Dedicated Software and the associated documentation.

The logical configuration comprises configuration data and, where applicable, hardware-controlled patches to the IC Dedicated Software stored in non-volatile memory (NVM). No higher-level Security IC Embedded Software functionality is included in the TOE configuration.

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

Table 2. Configuration identifiers of the TOE

Name	Symbol	Description
Series	*srs*	Series identifier within the NXP product family
IC version	*xy.z.zzz*	Composite identifier of the IC version, where: *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 the NSN4XX2M0 Series)
NXP hardware configuration	*v*	Version identifier of the NXP hardware configuration, identifying the version of configuration data stored in NVM, including 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*_SE *xy.z.zzz wv* [1]

Evaluated **physical** configuration of the TOE is

- *NSN4XX2M0_SE* ***B1.1.000***

All components of NSN4XX2M0_SE B1.1.000 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 NVM memory is

- *NSN4XX2M0_SE B1.1.000* ***J6***

All components that are specific for NSN4XX2M0_SEB1.1.000 J6 are listed in Table 4 with their respective version numbers.

TOE identification methods are described in [13].

Table 3. Components of NSN4XX2M0_SE B1.1.000 common for any logical configuration

Category	Component	Identification	Delivery form
IC Hardware	base layer and fixed metal masks	B1.1.000 [1]	Package WLCSP
IC Dedicated Software	FactoryOS	9.8.6	On-chip software. Stored to the ROM of the TOE
	BootOS	9.8.6	On-chip software. Stored to the ROM of the TOE
	Firmware Library	9.14.11	On-chip software. Stored to the ROM of the TOE
Documentation, User Guidance	NSN4XX2M0_SE Information on Guidance and Operation	[11]	Electronic Document (PDF via NXP Docstore)
Documentation, Product Data Sheet	NSN4XX2M0 Integration manual	[12]	Electronic Document (PDF via NXP Docstore)
	NSN4XX2M0_SE TOE Identification, Data sheet addendum	[13]	Electronic Document (PDF via NXP Docstore)
Documentation, Application Note	NSN4XX2M0_SE Programmer's Manual (for revision B1), Application Note	[14]	Electronic Document (NXP internal Document)
	ARM® Cortex®-M33 Processor Technical Reference Manual	[15]	Electronic Document (www.arm.com)

[1] Note that the NSN4XX2M0_SE IP is identical for NSN4XX2M0 B0/B1 IC and will identify itself as B0.1 for both silicon versions. Please check [13] section 4.3 for details.

Table 4. Components of NSN4XX2M0_SE B1.1.000 specific for J6 configuration

Category	Component	Identification	Delivery form
Configuration Data	Factory Page	250818	On-chip configuration page. Stored to the NVM area of the TOE

1 This naming scheme is reflected in the Type ID for TOE identification given in [13]: "*srs xy.z.zzz*" refers to byte 0 of the Type ID, "*w*" to byte 1 and "*v*" to byte 2.

Table 4. Components of NSN4XX2M0_SE B1.1.000 specific for J6 configuration ***...continued***

Category	Component	Identification	Delivery form
	System Control Page	250818	On-chip configuration page. Stored to the NVM area of the TOE
	System Update Page	250611	On-chip configuration page. Stored to the NVM area of the TOE
	System Patch Page	v985_ s5_v0	On-chip configuration page. Stored to the NVM area of the TOE

Information on how to identify the logical configuration options of the NSN4XX2M0_SE after TOE Delivery and the delivery method used for NSN4XX2M0 IC are described in [13].

1.9 Security During Development and Production

The TOE product life cycle follows the phases defined in the Protection Profile [10]. This Security Target covers the following phases:

- Phase 2 - IC Development
- Phase 3 - IC Manufacturing
- Phase 4 - IC Packaging

TOE Delivery takes place at the end of Phase 4.

The development environment for the TOE extends from Phase 2 (IC Development) up to TOE Delivery. All remaining phases belong to the operational environment. This complies with Application Note 1 of the Protection Profile [10].

Phase 2 - IC Development

During this phase, access to all sensitive design data of NSN4XX2M0_SE subsystem is strictly restricted to personnel directly involved in the development activities. Appropriate organizational and technical measures ensure the confidentiality and integrity of design artefacts throughout the development process.

Phase 3 - IC Manufacturing

In this phase, the TOE - as integral part of the NSN4XX2M0 IC - is manufactured and tested at wafer level. NXP also acts as Composite Product Manufacturer, optionally programming Security IC Embedded Software into the NVM of the NSN4XX2M0_SE.

The NXP Trust Provisioning Service ensures

- confidentiality and integrity of customer data,
- secure handling and injection of customer-provided code and data, and
- protection of any random or derived data generated by NXP for personalization.

All manufacturing-test access is performed under strictly controlled conditions. FactoryOS enforces security policies that prevent unauthorized disclosure or modification of confidential NVM regions, also in the context of field-return analysis.

Phase 4 - IC Packaging

In Phase 4 NSN4XX2M0 ICs containing the TOE are assembled into their final packages. All inter-site delivery and handling processes ensure:

- traceability of each die,
- accountability between manufacturing and packaging sites, and
- protection against substitution and tampering.

Authentic TOE delivery is supported by the NXP Trust Provisioning Service.

2 Conformance Claims (ASE_CCL)

2.1 CC Conformance Claim

This Security Target claims conformance to Common Criteria for Information Technology Security Evaluation CC:2022 which comprises of:

- Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC:2022 Revision 1, November 2022, CCMB-2022-11-001 [1].
- Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CC:2022 Revision 1, November 2022, CCMB-2022-11-002 [2].
- Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CC:2022 Revision 1, November 2022, CCMB-2022-11-003 [3].
- Part 5: Common Criteria for Information Technology Security Evaluation, Part 5: Predefined packages of security requirements, CC:2022 Revision 1, November 2022, CCMB-2022-11-005 [4].

The TOE is evaluated against this Security Target in consideration of the methodology in

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CEM:2022, Revision 1, November 2022, CCMB-2022-11-006 [5].

In accordance with the Common Criteria Portal requirements, this ST applies the latest mandatory Errata and Interpretations for CC:2022 and CEM:2022

- Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, October 2025, CCMB-2025-001 [6]

This Security Target claims to be CC Part 2 extended and CC Part 3 conformant. Chapter 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

- AVA_VAN.5 “Advanced methodical vulnerability analysis”
- ALC_DVS.2 “Sufficiency of security controls”
- ALC_FLR.2 “Flaw reporting procedures”
- ASE_TSS.2 “TOE summary specification with architectural design summary”

As demonstrated in Section 7.1, 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-CC-PP-0084-V2-2026)

This Security Target claims strict conformance to Security IC Platform Protection Profile [10].

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 of this Security Target. Its components are detailed in TOE Description of this Security Target. These descriptions are consistent with the TOE description in section 1.3.2 of the Protection Profile [10] .

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 [10], 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 [10] .

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 [10] .

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 [10] 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 memory areas
- 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 memory areas
- SC3 - Correct operation of the security services provided by the TOE for the 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 [10] are listed in Table 5. They entirely apply to this Security Target.

Table 5. 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 [10].

3.1.3 OSPs related to the IC Protection Profile

The organizational security policies defined in section 3.3 of the Protection Profile [10] are listed in Table 6. They entirely apply to this Security Target.

Table 6. 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 [10] are listed in Table 7. They entirely apply to this Security Target.

Table 7. 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 NSN4XX2M0 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 [10]. They are listed in Table 8 and apply entirely to this Security Target.

Table 8. 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 [10].

4.2 Security Objectives for the Security IC Embedded Software

4.2.1 Security Objectives for the Security IC Embedded Software related to the IC Protection Profile

The security objective for the Security IC Embedded Software defined in section 4.2 of the Protection Profile [10] is listed in Table 9. It entirely applies to this Security Target.

Table 9. 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.

4.3 Security Objectives for the Operational Environment

4.3.1 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 [10] are listed in Table 10. They entirely apply to this Security Target.

Table 10. Security objectives for the operational environment defined in the Protection Profile

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

4.4 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 4.3 are traced back to the assumptions they uphold.

4.4.1 Security Objective Rationale related to the IC Protection Profile

4.4.1.1 Rationale for Threats

Table 11 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 11. 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 [10]). It is clear from the description of each objective (refer to Section 4.1 of PP [10]), 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	

4.4.1.2 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 supports 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 shall support the integrity of the generated unique identification. The technical and organisational security controls that ensure the security of the development environment and production environment are evaluated based on the assurance controls that are part of the evaluation. For a list of material produced and processed by the TOE Manufacturer refer to paragraph 68 (page 19) of the Protection Profile [10]. All listed items 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 controls are concerned.

4.4.1.3 Rationale for Assumptions

This section traces the security objectives for the Security IC Embedded Software in Section 4.2.1 and the security objectives for the operational environment in Section 4.3.1 back to the assumptions they uphold.

A.Resp-Appl

Name of security objective	Rationale
OE.Resp-Appl	This security objective taken from Protection Profile [10] 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 [10] are listed in Table 12. They entirely apply to this Security Target.

Table 12. Extended components defined in the Protection Profile

Name	Title
FAU_SAS	FAU_SAS Audit data storage

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 [10] 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 13 lists the security functional requirements for the TOE, which are defined in section 6.1 of the Protection Profile [10]. They entirely apply to this Security Target.

Table 13. 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 10 in the Protection Profile [10]. Considering Application Note 11 in the Protection Profile [10], the TOE does not generate audit data for FRU_FLT.2 and/or FPT_FLS.1.

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. These responses are enforced by security feature SF.PHY as described in Section 8.2. This addresses Application Note 15 in the Protection Profile [10].

On some further Security Functional Requirements from the Protection Profile [10] operations are made. Table 14 gives an overview on the Security Functional Requirements that were subject to refinement, selection, assignment and/or iteration operations in this Security Target.

Table 14. 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	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. 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 13 in the Protection Profile [10].

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*[2] in the *NVM*[3].

This Security Target performs one assignment operation on FDP_SDC.1 as requested by the Protection Profile [10].

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 *all user data* [4] while it is stored in the *temporary memory and persistent memory* [5].
Refinement:	Temporary memory" refers to all TSF-managed volatile memory (RAM). "Persistent memory" refers to all TSF-managed non-volatile memory (NVM). ROM is excluded, as it contains only IC Dedicated Software and immutable data and cannot store user data.

This Security Target performs two assignment operations on FDP_SDI.2 according to Application Note 14 in the Protection Profile [10].

FDP_SDI.2	**Stored data integrity monitoring and action**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.

2 [selection: *the Initialisation Data, Pre-personalisation Data, [assignment: other data]*]
3 [assignment: *type of persistent memory*]
4 [selection: *all user data, the following user data* [assignment: *list of user data*]]
5 [selection: *temporary memory, persistent memory, any memory*]

FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for *modification, deletion, 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 NVM, the ROM, the System RAM, the PKC RAM and the Buffer RAM* [7].
FDP_SDI.2.2	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. It also performs two assignment operations according to Application Note 17 in the Protection Profile [10]. The operations follow the guidance in section 11.2. of the Protection Profile [10] in consideration of the updated documents [8] and [7].

FCS_RNG.1/PTG.2	**Random number generation - PTG.2**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Note:	This security functional requirement is compliant with Class PTG.2 in [7]
FCS_RNG.1.1/PTG.2	The TSF shall provide a *physical* [9] random number generator that implements: *(PTG.2.1)The TSF shall generate raw random numbers that can be viewed as realizations of a (time-local) stationary stochastic process R_1, R_2, ...* *(PTG.2.2) The internal random numbers shall be interpreted as realizations of random variables Y_1, Y_2, ... If the random variables Y_j are binary-valued, it shall be Prob(Y_j) ∈ (0.493, 0.507). If the random variables Y_j assume binary vectors, this condition shall be met by the projections onto the particular bits. Furthermore, it shall be guaranteed that the Shannon entropy per internal random number bit is greater than or equal to 0.9998.* [10] *(PTG.2.3) The start-up test shall be applied after the RNG has been started. It shall be designed to detect a total failure of the physical noise source and severe statistical weaknesses. The TSF shall not output any internal random numbers before the start-up test has been passed.* *(PTG.2.4) The online test shall check the quality of the raw random numbers while the RNG is in operation. The*

6 [assignment: *integrity errors*]
7 [assignment: *user data attributes*]
8 [assignment: *action to be taken*]
9 [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]
10 [selection: *the Shannon entropy per internal random number bit is greater than or equal to 0.9998, the min-entropy per internal random number bit is greater than or equal to 0.98, the Shannon entropy per internal random number bit is greater than or equal to 0.9998 and the min-entropy per internal random number bit is greater than or equal to 0.98]*]

	online test shall detect non-tolerable entropy defects of the raw random numbers sufficiently soon. The TSF shall not output any internal random numbers if a non-tolerable entropy defect has been detected. *(PTG.2.5) The total failure test shall detect if a total failure of the physical noise source occurs while the PTRNG is in operation. The total failure test shall prevent the output of internal random numbers that depend on any raw random number that has been generated after the total failure of the physical noise source. If the PTRNG applies a cryptographic post-processing algorithm (with memory) that is compliant with functionality classes DRG.2 or DRG.3, then this relaxes this requirement: After the total failure has occurred, the output of internal random numbers bits whose entropy per bit is not close to 1 shall be prevented.* [11]
FCS_RNG.1.2/PTG.2	The TSF shall provide *octets of bits*[12] that meet: *(PTG.2.6) The internal random numbers shall pass test suite T_{im}.* [13]

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 15 .

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 15. 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, FPT_FLS.1
	FPT_PHP.3
	FDP_ITT.1, FPT_ITT.1, FDP_IFC.1
O.Phys-Probing	FPT_PHP.3
	FDP_SDC.1

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

Table 15. 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
O.Phys-Manipulation	FDP_SDI.2
	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
	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 15 show how the Protection Profile [10] maps its security objectives for the TOE to the Security Functional Requirements for the TOE, see section 6.3.1 of the Protection Profile [10]. that also provides the rationale for these mappings.

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 16.

Table 16. 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 [10]
FAU_SAS.1	none	N/A
FDP_SDC.1	none	N/A
FDP_SDI.2	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 [10] 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 17. These Security Assurance Requirements are augmented from the Protection Profile [10] to EAL5 augmented with Security Assurance Requirements ALC_DVS.2, ALC_FLR.2, AVA_VAN.5 and ASE_TSS.2.

Table 17. Security Assurance Requirements for the Secure Element Hardware

Name	Title	compared to PP [10]
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 controls	as in PP
ALC_FLR.2	Flaw reporting procedures	as in PP
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 to EAL5
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 [10] to security assurance requirements in Table 17, which are augmented from the Protection Profile, are discussed below in their applicability to this Security Target. This addresses Application Note 19 in the Protection Profile [10].

Refinements regarding ADV_FSP

Refinement to ADV_FSP.4 in the Protection Profile [10] paragraph 207 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 paragraph 11 on page 9 of the Protection Profile [10]. 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. 208, no. 209 and no. 210 to ADV_FSP.4 in the Protection Profile [10] 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. 190 to ALC_CMS.4 in the Protection Profile [10] 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.2 to cover policies and procedures that are applied to track, evaluate, correct and process communication of 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 5 [4]. 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.2 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 18. 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 18. 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 NSN4XX2M0 Secure Element

The TOE Security Functionality (TSF) of the NSN4XX2M0 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 19 and described in Section 8.2.1. The Security Features of the TOE are summarized in Table 20 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 19. Security Services of the NSN4XX2M0 Secure Element

Security Services	Name
SS.RNG	Random Number Generator

Table 20. Security Features of the NSN4XX2M0 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 NSN4XX2M0 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 [7]. 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 Deterministic Random Number Generator (DRNG).

The Random Number Generator fulfills the online test requirements defined in [7] and embeds hardware test functionality to detect hardware defects and quality issues of the random numbers.

This security functionality covers:

- FPT_PHP.3
- FCS_RNG.1/PTG.2

8.2.2 Security Features of the NSN4XX2M0 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 stimulation 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.

A watchdog on error detection codes runs in the background over code and data stored to System RAM and data stored to PKC RAM, and the Security IC Embedded Software can configure and enable Secure Fetch Plus on code and data read from RRAM and ROM. In addition, Security IC Embedded Software may protect its program flow by use of a code signature watchdog that computes signatures over executed CPU instructions, and by use of a security counter to check the correctness of the code execution.

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 NVM.

This security functionality covers:

- FDP_SDI.2
- FPT_FLS.1
- FPT_PHP.3
- FRU_FLT.2

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 NVM 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 implementation of security critical logic (e.g. CPU, Sym Copro) and 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 self-tests that run during start-up of the device.

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

This security functionality covers:

- FDP_IFC.1
- FDP_ITT.1
- FDP_SDC.1
- FPT_FLS.1
- FPT_ITT.1
- FPT_PHP.3
- FRU_FLT.2

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.

Sym Copro provides secure general purpose operations over sensitive data outside the CPU. Secure data transfers from memory to memory or from memory to peripherals on the data bus are also managed by the Sym Copro. All such transfers are fully masked from source to destination across the bus infrastructure.

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).

This security functionality covers:

- FDP_IFC.1
- FDP_ITT.1
- FPT_ITT.1

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 NVM 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.

This security functionality covers:

- FAU_SAS.1
- FMT_LIM.1
- FMT_LIM.2

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, CC:2022 Revision 1, November 2022, CCMB-2022-11-001

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CC:2022 Revision 1, November 2022, CCMB-2022-11-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CC:2022 Revision 1, November 2022, CCMB-2022-11-003

[4] Common Criteria for Information Technology Security Evaluation, Part 5: Predefined packages of security requirements, CC:2022 Revision 1, November 2022, CCMB-2022-11-005

[5] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CEM:2022, Revision 1, November 2022, CCMB-2022-11-006

[6] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, October 2025, CCMB-2025-001

[7] A Proposal for Functionality Classes for Random Number Generators, Matthias Peter and Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 3.0, 10 September 2024.

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

[9] Application of attack potential to smartcards and similar devices, EUCC Scheme State-of-the-art document, Version 2, February 2025

[10] Security IC Platform Protection Profile including Functional Packages, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-V2-2026, Version 2.0, 16 December 2025.

9 . 2 Developer documents

[11] NSN4XX2M0_SE Information on Guidance and Operation, Revision 1.0, 23.03.2026, NXP Semiconductors

[12] NSN4XX2M0 Integration manual , UM10955, Revision 1.1, 18.12.2025, NXP Semiconductors

[13] NSN4XX2M0_SE TOE Identification, Data sheet addendum , AD00091, Revision 1.3, 24.03.2026, NXP Semiconductors

[14] NSN4XX2M0_SE Programmer's Manual (for revision B1), Application Note , RM00308, Revision 1.02, 24.03.2026, NXP Semiconductors

[15] ARM® Cortex®-M33 Processor Technical Reference Manual, Revision r1p0, ARM Limited

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: 27 April 2026