i.MX93 EdgeLock Secure Enclave

SESIP Security Target

Rev. 1.2 — 27 May 2024

Document information

Information	Content
Keywords	SESIP, Security Target, S401, i.MX93 EdgeLock Secure Enclave
Abstract	Evaluation of the I.MX93 S401 EdgeLock Secure Enclave developed and provided by NXP Semiconductors, according to SESIP Assurance Level 3 (SESIP3), based on SESIP methodology, version 1.2, and PSA L3.

Revision History

Rev.	Date	Description
0.1	15 September 2023	Initial draft
0.2	23 November 2023	Update of Secure Update Security Objective to include fuse blown requirement for security releases. Update of Figure 1 with the correct scope. Update of Table 7 with additional recommendation for Secure Update OOE and removal of Physical protection OOE. Update of TOE identification. Added IEC62443 mapping (tentative). Added NIST 8425 mapping (tentative).
0.3	19 December 2023	Updated IEC62443 mapping. Updated NIST IR8425 mapping. Added ETSI EN303645 mapping.
1.0	29 January 2024	Updated a few wording in the IEC62443 mapping (mapping unchanged). Updated the title of the Security Target. Updated 2 references [10] and [12] in section 6.2.
1.1	14 May 2024	Updated the title of the Security Target. Clarified TOE reference. Updated Cryptographic Random Number Generation SFR claim.
1.2	27 May 2024	Harmonized TOE name

1 Introduction

This Security Target describes the core security features provided by the S401 EdgeLock Secure Enclave to be embedded in a SoC. For the current evaluation, the S401 has been integrated into the i.MX93 System-on-Chip (SoC).

The S401 can indeed be integrated in different System-on-Chips (SoCs), in which it will be the Root-of-Trust (RoT) and will act as an Hardware Security Module (HSM), implementing trust-based services for the SoC modules. In particular, OEM applications will be able to use the S401 to ensure their own security.

The target of evaluation is the S401 EdgeLock Secure Enclave on the i.MX93 and is referred as “S401” or “platform” into the rest of this document. The term “application” refers to the rest of the SoC modules (the A55 and M33 domains), which can invoke the S401 features.

The current Security Target is covering the SESIP Secure MCU/MPU profile for the SESIP scheme and the SESIP Profile for PSA Certified™ for the PSA Verified scheme.

1.1 ST Reference

i.MX93 EdgeLock Secure Enclave, SESIP Security Target, Revision 1.2, NXP Semiconductors, 27 May 2024.

1.2 SESIP Profile Reference and Conformance Claims

This Security Target claims conformance to the two following SESIP Profiles:

Table 1. SESIP Profile for Secure MCUs and MPUs Conformance Claims

Reference	Value
SP Name	SESIP Profile for Secure MCUs and MPUs [2]
SP Version	Version 1.0
Assurance Claim	SESIP Assurance Level 3 (SESIP3)
Package Claim	Base SP, Package Secure Services, Package Software Isolation of Platform

Table 2. SESIP Profile for PSA Certified Level 2 Conformance Claims

Reference	Value
SP Name	SESIP Profile for PSA Certified Level 3 [3]
SP Version	V1.0
Assurance Claim	SESIP Assurance Level 3 (SESIP3)
Optional and Additional SFRs	Base profile with optional Secure Debugging SFR

1.3 Platform Reference

Table 3. Platform Reference

Reference	Value
Platform Name	S401
Platform Version	S401 ROM: A1 - See components details in Section 3.2.1.1 S401 FW: 00.01.00 - See hash value in Section 3.2.1.1

Table 3. Platform Reference*...continued*

Reference	Value
Platform Identification	i.MX93 EdgeLock Secure Enclave
Platform Type	Secure Subsystem on SoC

1.4 Included Guidance Documents

The following documents are included with the platform:

Table 4. Guidance Documents

Document	Reference
SESIP Security Target	i.MX93 EdgeLock Secure Enclave, SESIP Security Target, Revision 1.2, NXP Semiconductors, 27 May 2024.
Reference Manual	i.MX 93 Applications Processor Reference Manual [5]
Security Reference Manual	i.MX 93 Applications Processor Security Reference Manual [6]
Core API Reference Manual	IMX93ELEAPI Edgelock Secure Enclave (ELE) API Reference Guide [7]
HSM API Reference Manual	EdgeLock Enclave API Bridge detailed implementation FW v0.0.11 [8]

1.5 Platform Overview and Description

1.5.1 Platform Security Features and scope

The S401 services in the scope of the evaluation are the following:

- Secure unique identification
- Secure initialization of the S401 and SoC components, with OEM image encryption
- Secure Updates of S401 and SoC firmware's
- Signature based Authenticated Debug for SoC domain access
- HSM Crypto Key storage and Operations (AES, RSA, ECC, SHA2, HMAC/CMAC, RNG)
- Remote Attestation of S401 and SoC components
- Isolation of S401 towards rest of the SoC
- Physical attacker protection (e.g. glitch detector to protect against glitch/physical attacks)

The S401 subsystem consists of hardware and firmware: the physical scope includes the S401 processing unit, and the logical scope includes the S401 firmware in ROM and the loadable firmware stored in external NVM.

In the current evaluation, the S401 has been integrated into the i.MX93 SoC, as represented in the figure below (the S401 subsystem, evaluation scope, is in red square):

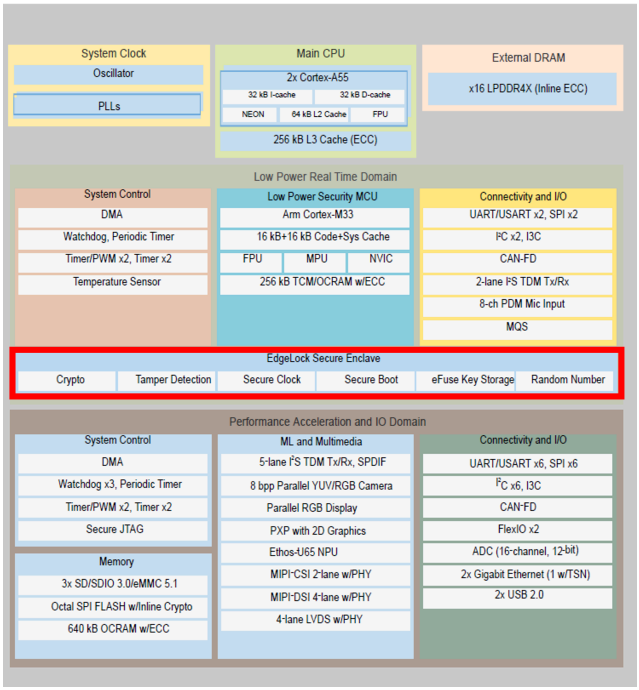

Figure 1. i.MX93 EdgeLock Secure Enclave scope

In this SoC, the S401 is integrated into the Real Time domain and is accessible by both the CM33 and A55 (Application domain) cores (LPAV domain is a slave domain only). The platform boundaries include the following hardware components and interfaces:

Table 5. Hardware components and interfaces

Component/interface	Description
CPU	32 bit RISC-V
Communication ports	Message Units, Trust Bus, SoC Bus
Debug port	JTAG
Fuse Status Block	Read of public fuses
Memories	DMEM, IMEM RAMs, PKC RAM, SRAM-PUF, ROM
GPIO Signals/Interrupts	See [6]
Crypto module	Public Key Coprocessor (PKC) Symmetric Crypto Accelerator (SGI)

The platform boundaries include the following software components and interfaces:

Table 6. Software components and interfaces

Component/interface	Description
ROM Firmware	Includes secure boot, secure update, life cycle management, attestation features for S401
Loadable Firmware image (in external NVM)	Includes key management, cryptographic operations, RNG, attestation features for OEM firmware
Firmware APIs	Interfaces to the S401 services from ROM and loadable firmware

1.5.2 Required Non-Platform Hardware/Software/Firmware

The platform is meant to be integrated into an SoC with a Flash memory in which the platform will be able to store its own data.

1.5.3 Life Cycle

The S401 life cycle steps are as follows:

- **NXP Design**: hardware and firmware design of S401, integration into the SoC design; preparation for manufacturing.
- **NXP Manufacturing**: manufacturing of the SoC integrating the S401; the unique identification information is injected.
- **NXP Packaging**: final testing and packaging of the SoC integrating the S401.
  - NXP secrets and root-of-trust related keys are injected; debug access to NXP area is closed, debug access to OEM area remains opened.
- **OEM Manufacturing**: integration of the SoC integrating the S401 into the OEM product.
  - Customer secrets are provisioned and debug access to OEM secure part must be closed.
- **In-field**: usage of the device integrating the SoC and its S401 subsystem. SoC Debug access is protected by ECC authentication, for S401 Debug is closed.
- **Field-return**:
  - The device integrating the SoC and its S401 subsystem is sent back to the OEM; the OEM changes the life-cycle state of the SoC (handled by S401, after OEM authentication) to “OEM Field-Return” and erase its own secrets.
  - The OEM sends back the SoC to NXP who change the life-cycle state of the SoC (handle by S401, after NXP authentication).
- **Destruction**: the destruction of the SoC can be done from any state; this is handled by S401. In this state, all secrets become unavailable by the zeroization of related encryption keys or related fuses.

Each step corresponds to one or several life-cycle states of the SoC, each of these states being associated to restricted to specific security restrictions.

The life-cycle state machine is handled by the S401 subsystem (see LMDA descriptions in section 7.1 of [6]).

1.5.4 Use Case Environments

The S401 is to be part of SoCs which will be integrated into devices requiring a Hardware Root-of-Trust to ensure the security of the final device use. In particular, the i.MX93 integrating it is expected to be used in home and general embedded control, wearables, portable healthcare or printing, IoT edge, SOM board solutions, etc.

[Any code] The S401 can be integrated into different SoCs and/or with different cores firmware and software implementation, thanks to the implementation of the secure isolation of the S401 security subsystem against the rest of the SoC modules (see Section 3.2.3.1).

[Trusted users] The S401 can be used into public environment, where it could be physically accessed by attackers (with enhanced-basic attack capacities), thanks to the implementation of physical protections (see Section 3.2.4.1).

2 Security Objectives for the Operational Environment

2.1 Platform Objectives for the Operational Environment

For the platform to fulfill its security requirements, the operational environment (technical or procedural) must meet the following objectives:

Table 7. Platform Objectives for the Operational Environment

Title	Description	Reference
Platform Acceptance	When receiving the platform, the user is expected to verify the correct version of all platform components that it depends on, as described in Section 3.2.1.1 of this document.	This document
Key Management	Cryptographic keys and certificates outside of the platform are subject to secure key management procedures.	This document
Trust Provisioning	Any secret to be provisioned into the platform is generated securely (e.g., via a standard compliant HSM) and subject to secure key management procedures. The provisioning process is done in secure sites with physical, logical security and organizational policies in place.	This document
Trusted Users	Actors in charge of TOE management, for instance for signature of firmware update, are trusted.	This document
Secure Boot	The operating system or application code is expected to make use of the AHAB feature as described in guidance manuals (see Section 1.4).	[6] chapter 5
Secure Update	Actors in charge of executing update of the platform firmware or applications are expected to securely initiate the update process. The update image is expected to be properly signed and distributed in secure manner to ensure its confidentiality and authenticity. In case of a security update, the actors in charge must also, as part of the update process, set up the "minimum version allowed" (see Section 3.2.1.3) to the new image version to ensure that no rollback to a previous version with security flaws is possible.	This document
Secure use	Users shall ensure secure and correct use of the platform according to guidance listed in Section 1.4. Note that there is only one user role allowing to access all the interfaces of the platform with the same privilege and in a unique mode of operation; also all features are accessible in only one configuration of the platform.	This document

3 Security Requirements and Implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP Assurance Level 3 (SESIP3)** as defined in Chapter 4 of Security Evaluation Standard for IoT Platforms (SESIP) [1].

3.1.1 Flaw Reporting Procedures (ALC_FLR.2)

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

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

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

The platform's secure boot feature is able to verify the authenticity of its loadable firmware part and of the customer code; it also provides an appropriate mechanism for the update of its own loadable firmware and support for the update of the customer code, the update mechanism itself being to be provided by the customer, most likely at the operating system level (not in scope of this evaluation).

3.2 Security Functional Requirements

The platform fulfills the following security functional requirements:

3.2.1 Base SP Security Functional Requirements

3.2.1.1 Verification of Platform Identity

The S401 unique identification information is injected into the S401 subsystem during the SoC manufacturing in NXP sites. This information can be retrieved through the following APIs described in detail in chapters 3.10 and 3.31 of [7]:

- Message *Get Info*: the response fields *Soc_rev*, *Soc_id*, *Fw_hash* and *Sha256 ROM patch* allow identifying the version of the silicon and the loadable firmware. In the current integration into the i.MX93 SoC, the expected values are:

Table 8. *Get Info* expected values

Field	Meaning	Expected value
Soc_rev	SoC revision number	0xA100
Soc_id	SoC identity	0x00009300
Fw_hash	Firmware hash	0xfbda7429410ac4a67f542c1b58e37993669826ba194a5cc2775ff07fdcfe0a71
Sha 256 ROM patch	ROM patch sha	0x48335e7264869e3402939bb7222e8d0e333fd87338a79efd9999ce1c9abe6fdf

- Message *Get FW version*: the response fields *FW version* and *Commit SHA1* are identifying the firmware. In the current integration into the i.MX93 SoC, the expected values are:

Table 9. *Get FW version* expected values

Field	Expected value
FW version	00.01.00
Commit SHA1	0xe943c57c

3.2.1.2 Secure Initialization of Platform

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

Conformance rationale:

Secure initialization (authenticity and integrity checks) of the S401, A55 and CM33 domains is ensured by the Advance High Assurance Boot (AHAB) feature implemented in the S401.

As part of this process, the authenticity and integrity of firmware to be run on S401 is checked by the S401 ROM based on a signature verification with NXP dedicated ECDSA P256 bits key and SHA-256. The other domains firmware are also checked by the S401 ROM or FW based on an OEM dedicated asymmetric key that can be ECDSA P256/384/521 bits or RSA 2048/3072/4096 bits.

Hashes SHA 256bits of asymmetric public keys are securely handled in S401 fuses (public keys are in firmware image container headers), initially generated in NXP HSMs.

Note that S401 firmware are always encrypted while this is optional for other domains firmware. Encryption is done with an AES-256 bits key, and decryption is handled withing the S401. Decryption keys are securely handled by the S401, derived by secrets in the S401 ROM and fuses.

For secure initialization purpose, the S401 is also in charge of all initial secure configuration of other SoC domains according to the life-cycle state; in particular:

- the domain controllers (RDCs) which set access policies for their domain including access to data and resources;
- the debug and test interfaces access.

In case of a general failure or firmware authentication during secure boot process, e.g. driver failure, secure disabling and cleaning of security settings and memory are performed to reach an abort mode, a failure state entering an endless loop in which accessible services are restricted and resetting after a timeout. After the warm reset, the access to the firmware authentication is restricted by a growing time delay, and to many attempt will block the boot; only a hard reset it possible.

3.2.1.3 Secure Update of Platform

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

Conformance rationale:

The authenticity and integrity of the updated firmware image is check during the secure boot process as described in Section 3.2.1.2. To protect against rollback of firmware, those are associated to a version number and the S401 manage a “minimum allowed firmware version” in fuses. This version can be updated through a specific customer command, however only security relevant update requires the fuse update.

Regarding ROM update, the S401 ROM can be patched, and the handling of those patches is fully handled by the S401. ROM patches can be part of OTP (called early patches) or be part of the S401 loadable firmware (called late patches).

In the first case, OTP patches can only be done during NXP manufacturing (through ECDSA P256 signed messages).

In the second case, the patches are part of the S401 loadable firmware and their authenticity and integrity is checked along with the overall firmware verification. Note that late patches loading feature is disabled by default and can only be enable by an early patch.

3.2.1.4 Secure Debugging

The platform only provides *JTAG* authenticated as specified in *[10]* with debug functionality.

The platform ensures that all data stored by the application, with the exception of *debugging information depending of the configured access level*, is made unavailable.

Conformance rationale:

The S401 debug access is disabled by default in all states; there is no service to re-enable it.

3.2.1.5 Residual Information Purging

The platform ensures that *user data*, with the exception of *none*, is erased using the method specified in *the rational below* before the memory is (re)used by the platform or application again and before an attacker can access it.

Conformance rationale:

User data handled by the S401 are the OEM keys or data in secure storage which are stored in SoC memory, external to S401, but encrypted by the S401. Those data need to be erased in case of field return or decommissioning processes which involve a life cycle change; encrypted containers in which those user data are stored are life cycle dependent i.e. the encryption key will be automatically changed during the life cycle change process. The encrypted containers then cannot be accessed anymore after this life cycle change, making the user data unavailable.

3.2.2 Package ‘Security Services’ Security Functional Requirements

3.2.2.1 Cryptographic Operation

The platform provides the application with *list of cryptographic operations specified in Table 10* functionality with *list of algorithms in Table 10* as specified in *specifications in Table 10* for key lengths *defined in Table 10* and modes *defined in Table 10*.

Table 10. Cryptographic Operations by S401

Algorithm	Operations	Specification	[Key] Lengths	Modes
AES	Encryption Decryption	FIPS 197 (AES) NIST SP 800-38A	128, 192, 256 bits	ECB, CBC, CFB, OFB, GCM
AEAD	Authentication Encryption Authenticated decryption	NIST SP 800-38C	128, 192, 256 bits	CCM
SHA2	Hash	FIPS-180-4	224, 256, 384, 512 bits	
HMAC	Mac	FIPS PUB 198-1	224, 256, 384, 512 bits	With SHA-256, SHA-384
CMAC	Mac	FIPS 197 (AES) NIST SP 800-38B	128, 192, 256 bits	CMAC
ECDSA	Signature generation Signature verification	FIPS 186-4	Brainpool R1 and T1 256, 320, 384 bits SECP R1 224, 256, 384, 521 bits	
RSA	Encryption, decryption Signature Generation and Verification	PKCS#1 v2.2	From 512 to 4096 bits	OAEP encoding and verification, PKCS #1 v1.5 generation and verification PSS encoding and verification, PKCS #1 v1.5 generation and verification

Conformance rationale:

The S401 implements symmetric (SGI) and asymmetric (PKC) cryptographic accelerator to provide cryptographic operations services to the application. Those resources are dedicated and only accessible by the S401 domain

3.2.2.2 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in *list of cryptographic algorithms in Table 11* as specified in *specifications in Table 11* for key lengths *described in Table 11*

Table 11. Cryptographic Key Generation

Algorithm	Specification	Key Lengths
ECC	ANSI X9.63 NIST FIPS 186-4	From 128 to 640 bits
AES	NIST FIPS 197 SP800-38C	128, 192, 256 bits
HMAC	NIST FIPS 198-1	224, 256, 384, 512 bits
RSA	PKCS #1 V2.2	From 512 to 4096 bits

Conformance rationale:

S401 implements cryptographic key generation services for the application based on cryptographic resources dedicated and accessible only by the S401 domain.

Persistent keys generated are then securely stored as described in Section 3.2.2.3.

3.2.2.3 Cryptographic KeyStore

The platform provides the application with a way to store *cryptographic keys* such that not even the application can compromise the *authenticity, integrity, confidentiality* of this data. This data can be used for the cryptographic operations *encryption, decryption, key derivation, signature generation, key exchange, signature verification (see complete list in [8])*.

Conformance rationale:

The S401 provides the application level an API for AES, ECC and RSA key storage. The application keys are sent via the API encrypted by an AES 256 bits pre-shared key.

Persistent keys can be generated or imported in S401 and are stored in SoC memory, encrypted by S401. Blobs are associated to a version (monotonic counter) stored in S401 fuses used for anti-rollback protection and blobs are die unique.

The S401 ensures the secure storage of the persistent keys (versus transient keys not stored) generated for the application.

More details are provided in sections 3.3 and 3.4 of [8].

3.2.2.4 Cryptographic Random Number Generation

The platform provides the application with a way based on *physical noise and DRBG* to generate random numbers to as specified in *[9] and NIST.SP.800-90A CTR-DRBG with AES-256*.

Conformance rationale:

The S401 provides random number to the application level by implementing in software a DRBG as defined in NIST SP 800-90A using a physical TRNG (on-chip entropy source) for the initialization and reseeding with fresh entropy (see more in [9]).

The S401 has a physical true random number generator and internal DRBG module as defined in NIST SP 800-90A. See more in [9].

3.2.3 Package 'Software Isolation' Security Functional Requirements

3.2.3.1 Software Attacker Resistance: Isolation of Platform

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

Application Note:

PSA profile specific requirements:

- The PSA-RoT is isolated from the NSPE.
- The PSA-RoT is isolated from the Application RoT Services.

Conformance rationale:

All SFRs are fully implemented by the S401 domain with hardware dedicated resources.

Access to those SFRs, and to any S401 service can only be done through a set of interfaces called Message Unit (MU) receiving the SoC requests to be transmitted to S401 domain. There is one MU per domain, A55 and CM33, and a third MU is used for SoC general requests e.g., life-cycle states handling. Messages parsing is fully handled by the S401, and their format is carefully checked.

From S401, out of internal S401 memory and dedicated S401 RAM regions, access to other SoC memory areas is done through DMA or CPU; in such case, format of retrieved data from those memories is carefully checked.

From PSA requirements perspective, this covers the isolation between S401 platform (SPE) and other SoC domains A55 and CM33 (NSPE). S401 is not handling Application RoT Services.

3.2.4 Package “Hardware Protections ” Security Functional requirements

3.2.4.1 Physical Attacker Resistance

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

Conformance rationale:

The cryptographic library has protections against fault injection and side channel analysis.

Software protections in ROM and loadable firmware implementation and hardware protections (glitch detectors) are in place against fault injections.

3.2.5 PSA specific Security Functional Requirements

3.2.5.1 Verification of Platform Instance Identity

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

Application Note:

The unique identification of platform must meet the attestation requirements of [4].

Conformance rationale:

The unique identification of a S401 instance is based on the UUID generated and fused into S401 during NXP manufacturing.

This information can be retrieved through the *UUID* field of the *Get Info* message (see chapter 3.31 of [7]).

3.2.5.2 Attestation of Platform Genuineness

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

Application Note:

See attestation mechanism of [4].

Conformance rationale:

The S401 implements an attestation of its genuineness building a payload including the S401 identity (as described in Section 3.2.1.1) and instance identity (as described in Section 3.2.5.1), as shown in section 3.32 of [7].

The payload is signed with ECDSA P256 key.

The nonce has been sent with the attestation request.

The payload preparation and signature are fully performed by the S401 in RROT mode.

3.2.5.3 Attestation of Platform State

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

Conformance rationale:

The S401 implements the attestation of its state by including this state (FW&patch hashes, life-cycle) as part of the attestation payload described in Section 3.2.5.2.

3.2.5.4 Secure External Storage

The platform ensures that all data stored outside the direct control of the platform, except for *none* is protected such that the *authenticity, integrity, confidentiality and binding to platform instance* is ensured.

Note: this SFR is named Secure Data Serialization in [1]

Conformance rationale:

The S401 implements the secure encrypted storage uses same encryption mechanism as for the persistent key storage (see Section 3.2.2.3). It is encrypted as specified in FIPS 197 and NIST SP 800-38A (AES GCM) with a platform instance unique key of key length 256 bits. See section 7.8 of [8].

3.3 Security Process Package (SPPs)

This package is extended from SESIP draft version to the CEN Enquiry (prEN 17927:2022) by CEN/JTC 13.

3.3.1 Secure development

For the development of the platform, the secure development process specified in IEC62443-4-1 *[17]* has been applied to the platform.

Conformance rationale:

NXP Security Maturity Process (SMP [12]) is designed to ensure that product security is given due consideration throughout the development cycle beginning with incorporating security in the product architecture – in a concept of ‘Security-by-Design’ - and then approving Security Milestones during development. This process is integrated into NXP Business Creation and Management (BCaM [11]) framework which covers all harmonized processes for launch, development, and release of a new product. NXP SMP ensures follow-up of Security Milestones, aligned with the BCaM product development gates, with the aim to ensure that security-related deliverables and reviews are planned and successfully completed for each Security Milestone and product development gates.

i.MX93 EdgeLock Secure Enclave development process has followed the BCaM framework (including SMP) and is subject to PSIRP process introduced in Section 3.1.1. The latest NXP BCAM and PSIRT processes have been certified against IEC 62443-4-1:2018 [17] as shown by [13]

4 Mapping and Sufficiency Rationales

4.1 SESIP3 Sufficiency

Assurance Class	Assurance Family	Covered By	Rationale
ASE: Security target evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in Section 1.1, the TOE reference in Section 1.3, the TOE overview and description in Section 1.5.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in Section 2 refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	Security Requirements and Implementation	All SFRs in this ST are taken from [2]. SFR "Identification of Platform Type" is included. SFR "Secure Update of Platform" is mentioned but refers to ALC_FLR.2.
	ASE_TSS.1 TOE Summary Specification	Security Requirements and Implementation	All SFRs are listed per definition, and for each SFR the implementation and verification is defined in the SFR.
ADV: Development	ADV_FSP.4 Complete functional specifications	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Section 1.4	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Section 1.4	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ALC_CMS.1 TOE CM Coverage	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ALC_FLR.2 Flaw reporting procedures	Section 3.1.1	The flaw reporting and remediation procedure is described.
ATE: Test	ATE_IND.1 Independent testing: conformance	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis	N.A. A vulnerability analysis is performed by the evaluator to ascertain	The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed

Assurance Class	Assurance Family	Covered By	Rationale
		the presence of potential vulnerabilities.	by the evaluator assuming an attack potential of Enhanced-Basic.

5 Appendix

5.1 IEC 62443 support

IEC 62443-4-1 compliance

IEC62443-4-2 requires component developed and supported following the secure product development process described in IEC 62443-4-1. This is covered by the current evaluation as described in Section 3.3.1.

IEC 62443-4-2 support

The table below shows how the platform under evaluation, i.MX93 EdgeLock Secure Enclave, described in this Security Target supports the final device, the component, to show compliance with the IEC 62443-4-2 security requirements (see [18]); it describes which part of each 62443-4-2 requirements are implemented at the i.MX93 EdgeLock Secure Enclave own level. Then, this is the responsibility of the component to use the security features described to implement the final requirement.

The descriptions below are checked by the independent security laboratory as part of the SESIP evaluation and provide evidences reusable in the context of end device compliance demonstration to 62443-4-2 standard.

Table 12. IEC 62443-4-2 security requirements support by i.MX93 EdgeLock Secure Enclave

62443-4-2 requirements	i.MX93 EdgeLock Secure Enclave supports
CR 1.1 - Human user identification and authentication CR 1.1(1) - Unique identification and authentication CR 1.1(2) - Multifactor authentication for all interfaces	Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation and Cryptographic KeyStore provide cryptographic functionalities that can be used to implement human user identification and authentication (including multifactor authentication).
CR 1.2 - Software process and device identification and authentication CR 1.2(1) - Unique identification and authentication	Verification of Platform Identity provides a unique and tamper-proof identification of the i.MX93 EdgeLock Secure Enclave type and version, that can be used for precise identification of the final component (by including subcomponent identification). Verification of Platform Instance Identity provides a unique and tamper-proof identity of each i.MX93 EdgeLock Secure Enclave instance, that can be used for precise identification of the final component (by including subcomponent identification). Attestation of Platform Genuineness provides an attestation for the i.MX93 EdgeLock Secure Enclave identity, that can be used for full authentication of the final component (by including subcomponent authentication). Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation and Cryptographic KeyStore provide cryptographic functionalities that can be used to implement identification and authentication to other components.
CR 1.3 - Account management	It is the component responsibility to properly implement account management. Cryptographic KeyStore provides secure storage for account credentials. Authentication is as per CR1.1 and 1.2.
CR 1.4 - Identifier management	Cryptographic Key Generation and Cryptographic Random Number Generation provide key generation and random number generation services which can be used for unique and unambigous identifier creation.
CR 1.5 - Authenticator management CR 1.5(1) - Hardware security for authenticators	Cryptographic Key Generation and Cryptographic Random Number Generation provides key generation and random number generation which can be used as authenticators. Cryptographic KeyStore provides secure storage of authenticators.

Table 12. IEC 62443-4-2 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

62443-4-2 requirements	i.MX93 EdgeLock Secure Enclave supports
	Physical Attacker Resistance provides protections of authenticators against physical attacks. Software Attacker Resistance: Isolation of Platform probides protection of authenticators against remote and local logical attacks.
CR 1.6 – Wireless access management	Cryptographic Operation. Cryptographic Key Generation and Cryptographic Random Number Generation provide cryptographic functionalities that can be used by network-components to implement authentication of all users engaged in wireless communication. Cryptographic KeyStore provides secure storage of cryptographic material used by network-components for identification and authentication of users engaged in wireless communication.
CR 1.7 – Strength of password-based authentication CR 1.7(1) – Password generation and lifetime restrictions for human users	It is the component responsibility to properly enforce the password policy. Cryptographic Operation, Cryptographic Key Generation, Cryptographic Random Number Generation provides cryptographic functionalities that can be used to enforce configurable password strength by meeting defined strength rules. Cryptographic KeyStore provides secure storage that can be used to enforce configurable password strength allowing their modifications and/or deletion to comply with defined number of use and lifetime restrictions.
CR 1.8 – Public key infrastructure certificates	Cryptographic Operation, Cryptographic Key Generation and Cryptographic Random Number Generation provide cryptographic functionlaities that can be used to interact and operate with PKI infrastructures. Cryptographic KeyStore provides secure storage of the cryptographic material (e.g. keys, certificates) involved in PKI infrastructures. Physical Attacker Resistance provides protections of cryptographic material and operations against physical attacks. Software Attacker Resistance: Isolation of Platform provides protections of cryptographic material and operations against remote and local logical attacks.
CR 1.9 – Strength of public key-based authentication CR 1.9(1) – Hardware security for public key-based authentication	Cryptographic Operation and Cryptographic Key Generation provide cryptographic features needed in public-key-based authentication in conformance with internationally recognized and proven security practices and recommendations. Cryptographic KeyStore provides secure storage for cryptographic material (e.g. keys, certificates) needed in public-key-based authentication. Physical Attacker Resistance provides protection of public-key-based authentication related material against physical attacks. Software Attacker Resistance: Isolation of Platform provides protection of public-key-based authentication related material against remote and local logical attacks.
CR 1.10 – Authenticator feedback	It is the component responsibility to obscure the authentication feedbacks sent back to the users. Human, Software, or Device Authentication is as per CR1.1 and CR1.2.
CR 1.11 – Unsuccessful login attempts	It is the component responsibility to limit the number of attempts and the reaction when the limit is reached. Human, Software, or Device Authentication is as per CR1.1 and CR1.2.
CR 1.12 – System use notification	It is the component responsibility to display a system use notification message before the authentication. Human, Software, or Device Authentication is as per CR1.1 and CR1.2.
CR 1.13 – Access via untrusted networks	It is the component responsibility to deny or accept requests based on the authentication results.

Table 12. IEC 62443-4-2 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

62443-4-2 requirements	i.MX93 EdgeLock Secure Enclave supports
CR 1.13(1) – Explicit access request approval	Human, Software, or Device Authentication is as per CR1.1 and CR1.2.
CR 1.14 – Strength of symmetric key-based authentication CR 1.14(1) – Hardware security for symmetric key-based authentication	Cryptographic Operation and Cryptographic Key Generation provide cryptographic functionalities conforment to internationally recognized and proven security best practices that can be used for symmetric-key-based authentication. Cryptographic KeyStore provides secure storage for cryptographic material (e.g. shared secret) involved in symmetric-key-based authentication. Physical Attacker Resistance provides protections of related material against physical attacks. Software Attacker Resistance: Isolation of Platform provides protections of related material against remote and local logical attacks.
CR 2.1 – Authorization enforcement	It is the component responsibility to properly implement authorization enforcement mechanism. Human, Software, or Device Authentication is as per CR1.1 and CR1.2. Software Attacker Resistance: Isolation of Platform provides logical isolation of the i.MX93 EdgeLock Secure Enclave subcomponent that can be leveraged to enforce authorization of properly authenticated entities.
CR 2.2 – Wireless use control	It is the component responsibility to properly implement wireless use control. Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation and Cryptographic KeyStore provide cryptographic functionalities that can be used to implement wireless network authentication.
CR 2.4 – Mobile code CR 2.4(1) – Mobile code authenticity check	Secure Initialization of Platform and Secure Update of Platform provide secure boot and secure update with integrity and authenticity verification of the i.MX93 EdgeLock Secure Enclave subcomponent and other SoC processing domains before their execution, which can include mobile code. Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation and Cryptographic KeyStore provide cryptographic functionalities that can be used to control the integrity and authenticity of mobile code, as well as to authenticate users that are allowed to transfer mobile code.
CR 2.5 – Session lock CR 2.6 – Remote session termination CR 2.7 – Concurrent session control	It is the component responsibility to properly implement session lock, remote session termination, and concurent session control mechanisms. Human user re-authentiction is as per CR1.1. Remote software processes or devices re-authentication is as per CR1.2 and CR1.6. Account and credential management are as per CR.13, CR1.4, CR1.5,
CR 2.8 – Auditable events CR 2.9 – Audit storage capacity CR 2.10 – Response to audit processing failures CR 2.11 – Timestamps	All SESIP SFRs provide output status which can be integrated to the component audit records. Secure External Storage provides secure storage service that can be used to securely store audit records, including the timestamps. Physical Attacker Resistance provides protections against physical attacks that could affect audit records overall management. Software Attacker Resistance: Isolation of Platform provides protections against remote and local logical attacks that could affect audit records overall management.
CR 2.12 – Non-repudiation CR 2.12 – Non-repudiation for all users	All SESIP SFRs provide output status which can be integrated to the component audit records as per CR2.8, CR2.9, CR2.10, CR2.11 and serve as a proof that an action has been performed. Cryptographic Operation, Cryptographic Key Generation, Cryptographic Random Number Generation and Cryptographic KeyStore provides

Table 12. IEC 62443-4-2 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

62443-4-2 requirements	i.MX93 EdgeLock Secure Enclave supports
	cryptographic functionalities that can be use to identify and authenticate a user and build the final non-repudiation solution.
CR 2.13 – Use of physical diagnostic and test interfaces	Secure Debugging provides protected access to the physical diagnostic and test interfaces of the entire SoC (including the i.MX93 EdgeLock Secure Enclave subcomponent).
CR 3.1 – Communication integrity CR 3.1(1) – Communication authenticity	Cryptographic Operation provides cryptographic operations that can be used to protect integrity and authenticity of transmitted information. Cryptographic Key Generation and Cryptographic Random Number Generation provides cryptographic functionalities that can be used to generate the cryptographic materiel necessary for the protection of transmitted information.. Cryptographic KeyStore provides secure storage that can be used to store cryptographic material (e.g. shared secret) on which such protections is be based. Physical Attacker Resistance provides protections of cryptographic services involved in secure communication integrity and authenticity enforcement against physical attacks. Software Attacker Resistance: Isolation of Platform provides protections of cryptographic services involved in secure communication integrity and authenticity enforcement against remote and local logical attacks.
CR 3.2 – Protection from malicious code	Secure Initialization of Platform provides protection against installation and execution of unauthorized software by checking the integrity and authenticity of the i.MX93 EdgeLock Secure Enclave own firmware, as well as the ones of other SoC processors, at each reset, as part of the secure boot. Software Attacker Resistance: Isolation of Platform provides isolation of the i.MX93 EdgeLock Secure Enclave subsystem against remote and local logical attacks that could be led from malicious code loaded into the rest of SoC. Note also that i.MX93 EdgeLock Secure Enclave is physically isolated from the rest of the SoC by design, using dedicated hardware.
CR 3.3 – Security functionality verification CR 3.3(1) – Security functionality verification during normal operation	The AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities support the components to verify the intended operation of the claimed security functions by requiring the execution of functional and penetration testing to those security functions. Secure Initialization of Platform provides integrity and authenticity verification of the i.MX93 EdgeLock Secure Enclave own firmware, as well as the ones of other SoC processors, ensuring a proper helth chack and security configuration at each reset, as part of the secure boot. Attestation of Platform State provides, on demand, the attestation of the state of the i.MX93 EdgeLock Secure Enclave subcomponent (including hashes of the firmware and patch, as well as life cycle state) that can be used to verify the state of the component during operation. Physical Attacker Resistance provides monitoring and detecting of physical attacks during operation.
CR 3.4 – Software and information integrity CR 3.4(1) – Authenticity of software and information CR 3.4(2) – Automated notification of integrity violations	Secure Initialization of Platform provides, as part of the secure boot, integrity and authenticity checks of the firmware, software and configuration data of i.MX93 EdgeLock Secure Enclave and/or other SoC processors before any execution. Secure Update of Platform additionally checks the version verification of the i.MX93 EdgeLock Secure Enclave firmware/software to be launched. Attestation of Platform State provides, on demand, the attestation of the state of the i.MX93 EdgeLock Secure Enclave subcomponent (including hashes of the firmware and patch, as well as life cycle state).

Table 12. IEC 62443-4-2 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

62443-4-2 requirements	i.MX93 EdgeLock Secure Enclave supports
	Physical Attacker Resistance ensures the protection of code and data integrity during boot and at runtime against physical attacks. Software Attacker Resistance: Isolation of Platform ensures the protection of code and data integrity during boot and at runtime against remote and local logical attacks. Detections of integrity violation are reported in registers accessible to the rest of the SoC, then in charge of automatic notification to other entities.
CR 3.5 – Input validation	The AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities support the validation of the syntax, length and content of input data by requiring such validation through code review and/or functional testing and/or penetration testing.
CR 3.6 – Deterministic output	The AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities support the verification of deterministic behaviour of the overall system by checking the correct and expected behavior of the i.MX93 EdgeLock Secure Enclave part.
CR 3.7 – Error handling	The AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities support the components to identify and handle error conditions by verifying that no sensitive information that could be used by attackers are outputted by the platform interfaces, in particular when related to cryptographic operations.
CR 3.8 – Session integrity	Cryptographic Random Number Generation provides random number that can be used to generate unique sessions identifiers. Cryptographic Operation provides cryptographic operations that can be used to protect integrity of session.
CR 3.9 – Protection of audit information	Physical Attacker Resistance and Software Attacker Resistance: Isolation of Platform provides protection of execution status of the i.MX93 EdgeLock Secure Enclave security services against remote and local, logical and physical attacks. Secure External Storage provides secure storage that can be used to protect audit information and logs from unauthorized access, modification and deletion.
CR 3.10 - Support for updates CR 3.10(1) - Update authenticity and integrity	Secure Initialization of Platform and Secure Update of Platform provides secure update of the i.MX93 EdgeLock Secure Enclave firmware/software parts through the checking of the its integrity, authenticity and version as part of the secure boot.
CR 3.11 - Physical tamper resistance and detection CR 3.11(1) Notification of a tampering attempt	Physical Attacker Resistance provides protections against physical attacks of the i.MX93 EdgeLock Secure Enclave; fault detections are notified into registers which can be read by the SoC for a notification at the component level.
CR 3.12 - Provisioning product supplier roots of trust	The i.MX93 EdgeLock Secure Enclave is implementing itself a root-of-trust from which supplier keys can be generated and protected by using the cryptographic services Cryptographic Key Generation, Cryptographic Operation, Cryptographic Random Number Generation and Cryptographic Key Store Physical Attacker Resistance provides protection of product supplier root-of-trust keys and data against physical attacks. Software Attacker Resistance: Isolation of Platform provides protection of product supplier root-of-trust keys and data against remote and local logical attacks.

Table 12. IEC 62443-4-2 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

62443-4-2 requirements	i.MX93 EdgeLock Secure Enclave supports
CR 3.13 - Provisioning asset owner roots of trust	Cryptographic Key Generation and Cryptographic Operation provides cryptographic services that can be used for the provisioning of asset owner root-of-trust. Cryptographic KeyStore provides secure storage (confidentiality, integrity, authenticity) that can be used to securely store provisioned supplier cryptographic material to be used as a root-of-trust. Physical Attacker Resistance provides protection of asset owner root-of-trust keys and data against physical attacks. Software Attacker Resistance: Isolation of Platform provides protection of asset owner root-of-trust keys and data against remote and local logical attacks.
CR 3.14 - Integrity of boot process CR 3.14(1) - Authenticity of the boot process	Secure Initialization of Platform provides, as part of the secure boot, integrity and authenticity checks of the firmware, software and configuration data of i.MX93 EdgeLock Secure Enclave and other SoC processors before any execution. Physical Attacker Resistance ensures the protection of code and data integrity during boot and at runtime against physical attacks. Software Attacker Resistance: Isolation of Platform ensures the protection of code and data integrity during boot and at runtime against remote and local logical attacks.
CR 4.1 - Information confidentiality	Secure External Storage and Cryptographic KeyStore provide the capability to protect the confidentiality of information at rest in the external NVM and in transit when imported in the i.MX93 EdgeLock Secure Enclave for use. Physical Attacker Resistance provides confidentiality protection of the information against physical attacks when manipulated by the i.MX93 Edge Lock Secure Enclave services. Software Attacker Resistance: Isolation of Platform provides confidentiality protection of the information against remote and local logical attacks when temporarily stored into the i.MX93 EdgeLock Secure Enclave services.
CR 4.2 - Information persistence	Residual Information Purging provides secure erasing of sensitive data when changing life-cycle state related to decommissioning or field return. Cryptographic KeyStore provides secure erasure of cryptographic material. Software Attacker Resistance: Isolation of Platform provides mediated access to information stored and manipulated inside the i.MX93 EdgeLock Secure Enclave subcomponent avoiding having to share critical memory ressources.
CR 4.3 - Use of cryptography	Cryptographic Operation, Cryptographic Key Generation, Cryptographic Random Number Generation and Cryptographic KeyStore provide cryptographic capbilities that can be used by the component. The AVA_VAN (vulnerability analysis) SESIP evaluation activity requires the verification that cryptographic algorithms, used in any security feature, are compliant with internationally recognized and proven security practices and recommendations.
CR 5.1 - Network segmentation CR 5.2 - Zone boundary protection CR 5.3 - General-purpose person-to-person communication restrictions	It is the component responsibility to properly implement network segmentation, zone boundary protection, and general-purpose person-to-person communication restrictions. The component may use security services claimed by i.MX93 EdgeLock Secure Enclave to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc., however this is to be determined case by case.
CR 6.1 – Audit log accessibility CR 6.1(1) - Programmatic access to audit logs	Secure External Storage provides secure storage in which the logs can be stored and accessed only to the authorized processor.

Table 12. IEC 62443-4-2 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

62443-4-2 requirements	i.MX93 EdgeLock Secure Enclave supports
	Cryptographic Operation, Cryptographic Key Generation, Cryptographic Random Number Generation and Cryptographic KeyStore provide cryptographic features needed to put in place authentication mechanism and granting access to audit log.
CR 6.2 – Continuous monitoring	It is the component responsibility to properly implement monitoring capabilities according to the system requirements. The component may use security services claimed by i.MX93 EdgeLock Secure Enclave to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc., however this is to be determined case by case.
CR 7.1 – Denial of service protection CR 7.1(1) – Manage communication load from component	It is the component responsibility to properly implement denial of service protection. The component may use security services claimed by i.MX93 EdgeLock Secure Enclave to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc., however this is to be determined case by case.
CR 7.2 – Resource management	It is the component responsibility to properly implement ressource management. The component may use security services claimed by i.MX93 EdgeLock Secure Enclave to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc., however this is to be determined case by case.
CR 7.3 – Control system backup CR 7.3(1) – Backup integrity verification	It is the component responsibility to properly implement backup. Cryptographic Operation, Cryptographic Key Generation, Cryptographic Random Number Generation and Cryptographic KeyStore provide cryptographic features that can be used to ensure confidentiality, integrity, and authenticity protection during backup and restore.
CR 7.4 – Control system recovery and reconstitution	It is the component responsibility to properly implement system recovery and reconstruction. The component may use security services claimed by i.MX93 EdgeLock Secure Enclave to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc. (e.g. as per CD7.3), however this is to be determined case by case.
CR 7.6 – Network and security configuration settings CR 7.6(1) – Machine-readable reporting of current security settings	It is the component responsibility to properly implement network and security configuration. The component may use security services claimed by i.MX93 EdgeLock Secure Enclave to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc., however this is to be determined case by case.
CR 7.7 – Least functionality	It is the component responsibility to provide capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services. The AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities support the components to specifically restrict the use of unecessary functions, ports. protocols and/or services by requiring for the i.MX93 EdgeLock Secure Enclave the verification that there is no unnecessary interface and/or code remaining in the final implementation.
CR 7.8 – Control system component inventory	It is the component responsibility to properly support a control system component inventoty. The component may use security services claimed by i.MX93 EdgeLock Secure Enclave to support this requirement, for instance in case Root-of-Trust

Table 12. IEC 62443-4-2 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

62443-4-2 requirements	i.MX93 EdgeLock Secure Enclave supports
	base, secure cryptography, or secure storage is needed, etc. (e.g. CR1.2), however this is to be determined case by case.

5.2 NIST 8425 support

The table below shows how the platform under evaluation, i.MX93 EdgeLock Secure Enclave, described in this Security Target supports the final IoT device (as defined in the NIST 8425 [14]; component of the IoT product), to show compliance with the NIST 8425 security requirements; it describes which part of each NIST 8425 requirements are implemented at the i.MX93 EdgeLock Secure Enclave own level. Then, this is the responsibility of the device to use the security features described to implement the final requirement.

The descriptions below are checked by the independent security laboratory as part of the SESIP evaluation and provide evidences reusable in the context of end device compliance demonstration to NIST 8425 standard.

NIST 8425 defines the IoT product as a system made of components like IoT device(s), mobile application(s), backend web application(s). In this context, the mapping provided below only holds for the IoT device.

Table 13. NIST 8425 security requirements support by i.MX93 EdgeLock Secure Enclave

NIST 8425 requirements	i.MX93 EdgeLock Secure Enclave supports
Asset Identification	
1. The IoT product can be uniquely identified by the customer and other authorized entities (e.g., the IoT product developer).	Verification of Platform Identity supports the IoT device to be uniquely identified by providing a unique and tamper-proof identification of the type and version of its i.MX93 EdgeLock Secure Enclave subcomponent. Verification of Platform Instance Identity supports the IoT device to be uniquely identified by providing a tamper-proof identity of its i.MX93 EdgeLock Secure Enclave subcomponent, and unique per IoT device instances. Attestation of Platform Genuineness supports the IoT device to be uniquely identified by providing identity information of its i.MX93 EdgeLock Secure Enclave subcomponent in a secure manner.
2. The IoT product uniquely identifies each IoT product component and maintains an up-to- date inventory of connected product components.	
Product Configuration	
1. Authorized individuals (i.e., customer), services, and other IoT product components can change the configuration settings of the IoT product via one or more IoT product components.	The authorization and configuration of the IoT device, as part of an IoT IoT product, shall be implemented by the operating system or application code. Cryptographic Key Generation, Cryptographic Random Number Generation and Cryptographic Operation provide the IoT device capability to implement the authorization and access control mechanism. Based on such mechanisms, the IoT device configuration settings can be changed by authorized individuals, services or other IoT product components. Cryptographic KeyStore additionally support the protection of the cryptographic secrets involved in the authorization mechanism described above. Secure Update of Platform allows the IoT device to update to a newer version in the filed in secure manner if this is needed for a configuration update.
2. Authorized individuals (i.e., customer), services, and other IoT product components have the ability to restore the IoT product to a secure default (i.e., uninitialized) configuration.	The authorization and configuration of the IoT device, as part of an IoT product, shall be implemented by the operating system or application code.

Table 13. NIST 8425 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

NIST 8425 requirements	i.MX93 EdgeLock Secure Enclave supports
	Residual Information Purging supports the ability to restore the IoT device to a secure default configuration by ensuring the secure erasing of sensitive data when changing life-cycle state.
3. The IoT product applies configuration settings to applicable IoT components.	The configuration of the IoT device, as part of an IoT product, shall be implemented by the operating system or application code. Secure Update of Platform allows the IoT device to update the configuration settings of its i.MX93 Edge Lock Secure Enclave subcomponent, as well as other processors of the SoC, to a newer version in the field in a secure manner if this is needed for a configuration update.
Data Protection	
1. Each IoT product component protects data it stores via secure means	Secure External Storage supports the IoT device to protect the storage of its data by providing an encrypted storage service. Cryptographic KeyStore supports the IoT device to protect the storage of its cryptographic data by providing a secure key store service. Other services also indirectly protect the IoT device data stored by the i.MX93 EdgeLock Secure Enclave subcomponent: Physical Attacker Resistance and Software Attacker Resistance: Isolation of Platform support the secure data storage by implementing protections against physical and logical, remote and local attacks. Secure Debugging supports the secure data storage by protecting unauthorized access to those data via debug features.
2. The IoT product has the ability to delete or render inaccessible stored data that are either collected from or about the customer, home, family, etc.	Residual Information Purging supports the ability to render inaccessible user data stored in the i.MX93 Edge Lock Secure Enclave subcomponent when changing life-cycle state.
3. When data are sent between IoT product components or outside the product, protections are used for the data transmission.	The communication function of the IoT device, as part of an IoT product, shall be fully facilitated by the operating system or application code. Cryptographic Key Generation, Cryptographic Random Number Generation and Cryptographic Operation supports the IoT device to implement protection of data transmission by providing secure cryptographic features on which such protections can rely. Cryptographic KeyStore additionally supports the protection of the cryptographic secrets involved in the data transmission protection mechanism described above.
Interface Access Control	
1. Each IoT product component controls access to and from all interfaces (e.g., local interfaces, whether externally accessible or not, network interfaces, protocols, and services) in order to limit	The design of final IoT device, as par of an IoT product, including the physical interface exposure and its usability, is by OEM. The access control, authentication, and communcation mechanism shall also

Table 13. NIST 8425 security requirements support by i.MX93 EdgeLock Secure Enclave *...continued*

NIST 8425 requirements	i.MX93 EdgeLock Secure Enclave supports
access to only authorized entities. At a minimum, the IoT product component shall: a. Use and have access only to interfaces necessary for the IoT product's operation. All other channels and access to channels are removed or secured. b. For all interfaces necessary for the IoT product's use, access control measures are in place (e.g., unique password-based multifactor authentication, physical interface ports inaccessible from the outside of a component). c. For all interfaces, access and modification privileges are limited.	be implemented by the operating system or application code. Cryptographic Key Generation, Cryptographic Random Number Generation and Cryptographic Operation support the IoT device to implement access control to its external interfaces by providing secure cryptographic features on which authentication mechanism can rely. Cryptographic KeyStore additionally supports the protection of the cryptographic secrets involved in the authentication mechanism described above. For the access to the i.MX93 EdgeLock Secure Enclave subcomponent interfaces: Software Attacker Resistance: Isolation of Platform implements protections of the i.MX93 EdgeLock Secure Enclave interfaces against illegal access to its resources (physically isolated by design), by restricting the access through Message Units dedicated per external processor. Secure Debugging supports the access control to the i.MX93 EdgeLock Secure Enclave interfaces by protecting unauthorized access to those interfaces in debug mode. Also, the AVA (vulnerability analysis), ADV (development) and ATE (functional testing) activities in SESIP evaluation verify that the interfaces provided at i.MX93 EdgeLock Secure Enclave level are restricted to only the necessary functions and privileges, and there is no unnecessary privilege, interface and/or code remained.
2. Some, but not necessarily all, IoT product components have the means to protect and maintain interface access control. At a minimum, the IoT product shall: a. Validate that data shared among IoT product components match specified definitions of format and content. b. Prevent unauthorized transmissions or access to other product components. c. Maintain appropriate access control during initial connection (i.e., onboarding) and when reestablishing connectivity after disconnection or outage.	
Software Update	
1. Each IoT product component can receive, verify, and apply verified software updates.	Secure Update of Platform implements the secure update of the i.MX93 EdgeLock Secure Enclave subcomponent, as well as of other processors of the SoC i.e. ensuring integrity and authentication verification. The software update development, distribution and customer notification are expected to be managed by OEMs and/or the network service providers.
2. The IoT product implements measures to keep software on IoT product components up to date (i.e., automatic application of updates or consistent customer notification of available updates via the IoT product).	
Cybersecurity State Awareness	
1. The IoT product securely captures and records information about the state of IoT components that can be used to detect cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.	The cybersecurity state awareness of the IoT device, as part of an IoT product, shall be designed and implemented by the operating system or application code. All SESIP SFRs support the components to provide the capability to manage audit records relevant to security by outputing status which can be integrated to the component audit records. Attestation of Platform Genuineness and Attestation of Platform State can attest the identity and state of the i.MX93 EdgeLock Secure Enclave subcomponent. Secure External Storage supports the IoT device to handle audit records by providing secure storage

Table 13. NIST 8425 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

NIST 8425 requirements	i.MX93 EdgeLock Secure Enclave supports
	service that can be used to securely store audit records, including the timestamps. Physical Attacker Resistance supports the IoT device to securely handle audit records by implementing protections against physical attacks that could affect audit records overall management. Software Attacker Resistance: Isolation of Platform supports the IoT device to securely handle audit records by implementing protections against remote and local logical attacks that could affect audit records overall management.
Documentation	
The IoT product developer creates, gathers, and stores information relevant to cybersecurity of the IoT product and its product components prior to customer purchase, and throughout the development of a product and its subsequent lifecycle.	NXP creates and stores documents related to the i.MX93 EdgeLock Secure Enclave cybersecurity all along its development and its subsequent lifecycle. The ASE (Security Target) SESIP evaluation activities (see [1]) ensures that information is provided related to expected use case (as defined in the SESIP profile for Secure MCUs and MPUs [2] and SESIP Profile for PSA Certified Level3 [3]) and security scope (like assurance level, assumptions on the operational environment, security functionalities,etc...) of the i.MX93 EdgeLock Secure Enclave subcomponent The AGD (Guidance) SESIP evaluation activities (see [1]) ensures that information is provided related to secure use of the i.MX93 EdgeLock Secure Enclave subcomponent.
Information and Query Reception	
The IoT product developer has the ability to receive information relevant to cybersecurity and respond to queries from the customer and others about information relevant to cybersecurity.	This requirement primarily address the OEMs and/or the network service providers. NXP also provides a flaw reporting procedure for its products. Flaw Reporting Procedure (ALC_FLR.2) SESIP evaluation activities (see also [1]) support the IoT device developer to respond to user queries about information relevant to cybersecurity by requiring for the i.MX93 EdgeLock Secure Enclave subcomponent, the implementation and the assessment of a flaw remediation process.
Information Dissemination	
The IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the IoT product ecosystem) information relevant to cybersecurity.	This requirement primarily address the OEMs and/or the network service providers. NXP also distributes information relevent to cybersecurity to its customer. The ASE (Security Target) and AGD (user guidance) SESIP evaluation activities (see [1]) support the IoT device developer disseminating information relevant to cybersecurity by providing information needed related to the i.MX93 EdgeLock Secure Enclave subcomponent. Flaw Reporting Procedure (ALC_FLR.2) SESIP evaluation activities (see also [1]) support the IoT device developer to respond to user queries about information relevant to cybersecurity by requiring for the i.MX93 EdgeLock Secure Enclave subcomponent,

Table 13. NIST 8425 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

NIST 8425 requirements	i.MX93 EdgeLock Secure Enclave supports
	the implementation and the assessment of a flaw remediation process.
Product Education and Awareness	
The IoT product developer creates awareness of and educates customers and others in the IoT product ecosystem about cybersecurity-related information (e.g., considerations, features) related to the IoT product and its product components.	This requirement primarily addresses the OEMs and/or the network service providers. NXP also distributes information relevent to cybersecurity to its customer. The ASE (Security Target) and AGD (user guidance) SESIP evaluation activities (see [1]) support the IoT device developer disseminating information relevant to cybersecurity by providing information needed related to the i.MX93 EdgeLock Secure Enclave subcomponent. Flaw Reporting Procedure (ALC_FLR.2) SESIP evaluation activities (see also [1]) support the IoT device developer to respond to user queries about information relevant to cybersecurity by requiring for the i.MX93 EdgeLock Secure Enclave subcomponent, the implementation and the assessment of a flaw remediation process.

5.3 ETSI EN 303645 support

ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements [15] is released by European Telecommunications Standard Institute (ETSI), and as its title suggests, it intends to prepare consumer IoT devices with a set of baseline requirements to address common cybersecurity threats. SESIP methodology is acknowledged as one of the schemes that aligns with EN 303 645.[1] GlobalPlatform also released a white paper on SESIP Applicability for EN 303 645 [16]. Yet at the time of writing, there is no recognized SESIP mapping to EN 303 645 released, hence NXP provides the following informative mapping and self-assessment towards EN 303 645 sufficiency rational from this evaluation. The mapping and rational is provided under each EN 303 645 provision entry, and for complete requirements by EN 303 645 provision, please refer to original text of [15].

This section refers to the claims and activities within this SESIP evaluation scope to demonstrate the sufficiency by SESIP methodology. Note EN 303 645 is targeting for consumer IoT device with full software stack mounted and physically designed, and connection to network-based services. The full software stack includes the operating system, communication stack and protocol, and/or application code, which is designed and owned by NXP (direct and indirect) customers, i.e. OEMs and the network service providers. So not all requirements are directly applicable to NXP product scope but more to OEMs and the network service providers. Thus, rationale on how i.MX93 EdgeLock Secure Enclave can support customers to meet EN 303 645 requirements are provided.

The descriptions below are checked by the independent security laboratory as part of the SESIP evaluation and provide evidences reusable in the context of end device compliance demonstration to ETSI EN 303645 standard.

Table 14. ETSI EN 303645 security requirements support by i.MX93 EdgeLock Secure Enclave

ETSI EN 303645 requirements	i.MX93 EdgeLock Secure Enclave supports
5.1-1 Unique device password	Password feature shall be implemented by the operating system or application code.

1 See more in https://www.etsi.org/technologies/consumer-iot-security

Table 14. ETSI EN 303645 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

ETSI EN 303645 requirements	i.MX93 EdgeLock Secure Enclave supports
	Yet, a default or other easy to manipulate password at i.MX93 Edge Lock Secure Enclave subcomponent hardware and firmware level can endeger security of operating system or application. The ADV (Development) and AVA (Vulnerability assessment) SESIP evaluation activities (see also [1]) support the requirement by providing full software source code access to the evaluator for vulnerability assessment, and it assures there is no such attack path identified within the evaluation scope and attack potential.
5.1-2 Password diversification	Verification of Platform Instance Identity can be used for password diversification per device.
5.1-3 Cryptography for user authentication	Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation and Cryptographic Random Number Generation provide the IoT device capability to implement user authentication.
5.1-4 Change of authentication value	Cryptographic KeyStore privides the IoT device secure key storage service for cryptographic data.
5.1-5 Authentication mechanism attack resilience	User authentication feature shall be implemented by the operating system or application code.
5.2-1 Vulnerability disclosure policy	Final product vulnerability disclosure policy shall be owned by OEMs. The ALC_FLR.2 (Flaw Reporting Procedure) SESIP evaluation activity (see also [1]) supports the requirement for the i.MX93 EdgeLock Secure Enclave subcomponent by providing a support portal and a Product Security Incident Response Team (PSIRT) committed to rapidly address security vulnerabilities in NXP products by responding and documenting reported vulnerabilities and by providing customers with clear guidance on the impact, severity and mitigation.
5.2-2 Timely response	
5.2-3 Vulnerability monitoring	
5.3-1 Secure Updatability	The software update development, distribution and customer notification are expected to be managed by OEMs and/or the network service providers. Secure Update of Platform implements the secure update of the i.MX93 EdgeLock Secure Enclave subcomponent, as well as of other processors of the SoC i.e. ensuring integrity and authentication verification.
5.3-2 Secure installation of updates	
5.3-3 Ease for update	Final product update mechanism shall be implemented by the operating system or application code. The AGD (Guidance document) SESIP evaluation activity (see also [1]) supports the requirement by providing full guidance documentation of the i.MX93 EdgeLock Secure Enclave subcomponent to the evaluator for assessment (and to the OEM).
5.3-4 Automatic update	Final product update mechanism shall be implemented by the operating system or application code. Secure Update of Platform implements the secure update of the i.MX93 EdgeLock Secure Enclave subcomponent, as well as of other processors of the SoC i.e. ensuring support for authomatic update and update failure detection/prevention. The AGD (Guidance document) SESIP evaluation activity (see also [1]) supports the requirement by providing full guidance documentation of the i.MX93 EdgeLock Secure Enclave subcomponent to the evaluator for assessment (and to the OEM), and by providing the corresponding tool chain for ease of use by the OEM.

Table 14. ETSI EN 303645 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

ETSI EN 303645 requirements	i.MX93 EdgeLock Secure Enclave supports
5.3-5 Check for update	Final product update mechanism shall be implemented by the operating system or application code.
5.3-6 Configurability for update	
5.3-7 Cryptography for update	Secure Update of Platform, Cryptographic Operation, Cryptographic Key Generation, Cryptographic KeyStore, and Cryptographic Random Number Generation implement the secure update of the i.MX93 Edge Lock Secure Enclave subcomponent, as well as of other processors of the SoC, using best practice cryptography, and provide cryptographic operations and secure storage for operating system or application code to implement other secure update mechanisms.
5.3-8 Timely update	Final product security update shall be owned by OEMs. The ALC_FLR.2 (Flaw Reporting Procedure) SESIP evaluation activity (see also [1]) supports the requirement for the i.MX93 EdgeLock Secure Enclave subcomponent by providing a support portal and a Product Security Incident Response Team (PSIRT) committed to rapidly address security vulnerabilities in NXP products by responding and documenting reported vulnerabilities and by providing customers with clear guidance on the impact, severity and mitigation.
5.3-9 Authenticity and Integrity of software update	Final product update mechanism shall be implemented by the operating system or application code. Secure Update of Platform, Cryptographic Operation, Cryptographic Key Generation, Cryptographic KeyStore, and Cryptographic Random Number Generation implement the secure update of the i.MX93 Edge Lock Secure Enclave subcomponent, as well as of other processors of the SoC, ensuring authenticity and integrity of the software update, and providing cryptographic operations and secure storage for operating system or application code to implement other secure update mechanisms.
5.3-10 Trust relationship for updates	
5.3-11 Security update communication	Final product security update shall be owned by OEMs. The ALC_FLR.2 (Flaw Reporting Procedure) SESIP evaluation activity (see also [1]) supports the requirement for the i.MX93 EdgeLock Secure Enclave subcomponent by providing a Support portal and a Product Security Incident Response Team (PSIRT) committed to rapidly address security vulnerabilities in NXP products by responding and documenting reported vulnerabilities and by providing customers with clear guidance on the impact, severity and mitigation.
5.3-12 Update notification	Final product update mechanism shall be implemented by the operating system or application code.
5.3-13 Defined support period	Support period of final product shall be defined by OEM. For the I.MX93 platform, this requirement is not covered by SESIP evaluation, yet NXP provides Product Longevity program where the I.MX93 shows a 15 years availability until April 2038.
5.3-14 Communication for constrained device	Final device updatability, end user communication and mitigation shall be defined by OEM
5.3-15 Isolatability and replaceability for constrained device	
5.3-16 Model recognizability	Final product model designation shall be defined by OEM. Verification of Platform Identity provides model designation for the i.MX93 EdgeLock Secure Enclave subcomponent (including firmware). The SESIP methodology (see also [1]) mandates unique identification of the platform under evaluation; conformance rational is provided.

Table 14. ETSI EN 303645 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

ETSI EN 303645 requirements	i.MX93 EdgeLock Secure Enclave supports
5.4-1 Security parameter storage	Software Attacker Resistance: Isolation of Platform Parts and Secure External Storage provide secure enclave and secure external storage to support operating system or application code to fulfil this provision requirement.
5.4-2 Tamper resistance of hard-coded identity	Verification of Platform Instance Identity , Software Attacker Resistance: Isolation of Platform Parts , and Physical Attacker Resistance provide an OTP based unique instance identity per device which can be used for security purposes. SESIP includes remote attack surface by default and the i.MX93 EdgeLock Secure Enclave subcomponent provides extra attacker resistance including software isolarion and physical attacker resistance for the secure enclave.
5.4-3 No hard-coded security parameters in software	The ADV (Development) and AVA (Vulnerability assessment) SESIP evaluation activities (see also [1]) support the requirement by providing full software source code access to the evaluator for vulnerability assessment, and it assures there is no such attack path identified within the evaluation scope and attack potential.
5.4-4 Device unique and diversified critical security parameters	Final product update and communication mechanism shall be implemented by the operating system or application code. Verification of Platform Instance Identity and Secure Update of Platform provide platform instance identity and secure update feature which support the operating system or application code to fulfil this requirement.
5.5-1 Best practice cryptography for communication	Final product communication shall be designed by OEM. Cryptographic Operation, Cryptographic Key Generation, Cryptographic KeyStore, and Cryptographic Random Number Generation provide cryptography support to implement secure communication protocol. Reference designs are also available yet it is not part of this evaluation.
5.5-2 Implementation review and evaluation	This SESIP evaluation is performed by 3rd party independent laboratory and certifier who are specialized in security including cryptography.
5.5-3 Cryptoagility	Secure Update of Platform, Cryptographic Operation, Cryptographic Key Generation, Cryptographic KeyStore, and Cryptographic Random Number Generation provide update capability where software based cryptography can be updated. Supported key sizes are clearly stated in cryptographic functionality sections.
5.5-4 Initialization state device access after authentication via network interface	Secure Initialization of Platform ensures secure initialization of the device before handling over control to operating system or application code when secure boot is configured. Secure Debugging ensures debug authentication. Cryptographic Operation, Cryptographic Key Generation, Cryptographic KeyStore, and Cryptographic Random Number Generation provide cryptographic support to implement authentication when the operating system or application code takes over control after boot up, hence up to the design by OEM.
5.5-5 Security configuration after authentication via network interface	Final product communication shall be designed by OEM. Cryptographic Operation, Cryptographic Key Generation, Cryptographic KeyStore, and Cryptographic Random Number Generation provide cryptography support to implement secure communication protocol.
5.5-6 Confidentiality for security parameter in transition	
5.5-7 Confidentiality for security parameter via network	

Table 14. ETSI EN 303645 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

ETSI EN 303645 requirements	i.MX93 EdgeLock Secure Enclave supports
5.5-8 Secure management process	The secure management process for OEM provisioned security parameters is owned by OEM. Cryptographic Key Generation, Cryptographic Operation and Cryptographic Random Number Generation support the provisioning and management of assets by providing cryptographic services which can be used for such secure provisioning and management. Cryptographic KeyStore supports the provisioning and storage of assets by implementing the secure storage (confidentiality, integrity, authenticity) of supplier cryptographic material.
5.6-1 Unused interface disablement	I.MX93 provides configurability and the enablement and disablement of interfaces is upon OEM's design.
5.6-2 Minimize disclosure during network interface initialization	Secure Initialization of Platform ensures secure initialization of the device before handling over control to operating system or application code when secure boot is configured. The operating system or application code will take over control after boot up, hence up to the design by OEM.
5.6-3 No unnecessary physical interface exposure	The design of final product including the physical interface exposure and its usability is by OEM
5.6-4 Debug disablement	Debug function of the i.MX93 EdgeLock Secure Enclave subcomponent, and of the I.MX93 SoC itself, can be disabled. i.MX93 EdgeLock Secure Enclave provides Secure Debugging, yet by provision requirement this feature shall be disabled if interface is physically accessible.
5.6-5 Least functionality	Software services of final product is defined by the operating system or application code.
5.6-6 Minimized code	The ADV (Development) and AVA (Vulnerability assessment) SESIP evaluation activities (see also [1]) support the requirement by providing full software source code access to evaluator for vulnerability assessment, and it assures that there is no unused code in the immutable part which could lead to attack path within the attack potential.
5.6-7 Least privilege	Software Attacker Resistance: Isolation of Platform Parts and Secure External Storage provide isolation of the i.MX93 EdgeLock Secure Enclave subcomponent ressources and of the memory allowing, in conjonction with other hardware based mechanisms not in the scope of this SESIP evaluation (like ARM TrustZone), management of privileged access by the operating system or application code.
5.6-8 Hardware-level memory access control	
5.6-9 Secure development process	Final product development process shall be defined and applied by OEM. i.MX93 EdgeLock Secure Enclave is part of NXP Edge Lock Assurance Program and secure development process is applied.
5.7-1 Secure boot for software verification	Secure Initialization of Platform provides secure boot feature and hardware root of trust.
5.7-2 Notification of unauthorized change.	This provision requirement shall be implemented by the operating system or application code.
5.8-1 Confidentiality of personal data transition between device and service	Final product communication shall be designed by OEM. Cryptographic Operation, Cryptographic Key Generation, Cryptographic KeyStore, and Cryptographic Random Number Generation provide cryptography support to implement confidentiality of personal data in transit.
5.8-2 Confidentiality of personal data transition between devices	

Table 14. ETSI EN 303645 security requirements support by i.MX93 EdgeLock Secure Enclave*...continued*

ETSI EN 303645 requirements	i.MX93 EdgeLock Secure Enclave supports
5.8-3 External sensing capability documented	Final product sensing capability and its document handling is up to OEM.
5.9-1 Resilience to outages	The resilience to outrages and recovery shall be designed by OEM and service provider. Secure Initialization of Platform and Attestation of Platform State provide secure initialization and attestation features which can support to fulfil the provision requirements.
5.9-2 Local function with loss of network	
5.9-3 Orderly reconnection	
5.10-1 Telemetry data examination	The use case and feature shall be defined by OEM of the final product. Secure Initialization of Platform and Attestation of Platform State provide secure initialization and attestation features which can support to fulfil the provision requirements.
5.11-1 Ease for user data deletion	The feature for user data management shall be defined by OEM of the final product. Residual Information Purging provides information purging mechanism which can support to fulfil the provision requirements.
5.11-2 Ease for user data deletion from service	These requirements shall be fulfilled by OEM and/or service provider.
5.11-3 Instruction for personal data deletion	
5.11-4 Deletion confirmation	
5.12-1 Ease of installation and maintenance	These requirements shall be fulfilled by OEM and/or service provider.
5.12-2 Guidance on setup	
5.12-3 Check on secure setup	This requirement shall be fulfilled by OEM and/or service provider. Secure Initialization of Platform and Attestation of Platform State provides secure initialization and attestation features which can support to fulfil the provision requirement.
5.13-1 Input Validation	The final product operating system or application code is responsible for their input validation. The ADV (Development) and AVA (Vulnerability assessment) SESIP evaluation activities (see also [1]) support the requirement by providing full software source code access to evaluator for vulnerability assessment, and it assures that there is no attack path identified including input manipulation within the attack potential.
6-1 Clear personal data usage	These requirements shall be fulfilled by OEM and/or service provider.
6-2 Consumer's consent	
6-3 Consent withdraw	
6-4 Minimum telemetry data collection	
6.5 Clear telemetry data collection and usage	

6 Bibliography

6.1 Evaluation Documents

[1] Security Evaluation Standard for IoT Platforms (SESIP), GlobalPlatform GP_FST_070, version 1.2.
[2] SESIP Profile for Secure MCUs and MPUs, GlobalPlatform Technology GPT_SPE_150.
[3] SESIP Profile for PSA Certified Level 3, PSA JSA JSADNE011, v1.0.
[4] Platform Security Model, Arm, ARM DEN 0079.

6.2 Developer Documents

[5] i.MX 93 Applications Processor Reference Manual, NXP Semiconductors, rev. 4.
[6] i.MX 93 Applications Processor Security Reference Manual, NXP Semiconductors, Rev. 4.
[7] IMX93ELEAPI Edgelock Secure Enclave (ELE) API Reference Guide, NXP Semiconductors, Rev. 3.
[8] EdgeLock Enclave API Bridge detailed implementation FW v0.0.11, NXP Semiconductors, Rev. 0.8.
[9] Design of the Entropy Source in the NXP RNG4 Random Number Generator, NXP Semiconductors, Rev. 1.23.
[10] NXP Debug Authentication Tools User Manual, NXP Semiconductors.
[11] BCAM framework, NXP Semiconductors, Release 7.5.
[12] Security Maturity Process, NXPOMS-1719007347-2172, NXP Semiconductors, 30 October 2022.
[13] Certificate No. IITS1 109577 0003 , TUV Sud, Rev. 00.

6.3 Standards

[14] NISTIR 8425: Profile of the IoT Core Baseline for Consumer IoT Products, September 2022, National Institute of Standards and Technology.
[15] ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI, v2.1.1, June 2020
[16] SESIP Applicability for EN 303 645, White Paper, GlobalPlatform, January 2022
[17] IEC 62443-4-1, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements, edition 1.0, 2018, the International Electrotechnical Commission (IEC).
[18] IEC 62443-4-2, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components, edition 1.0, 2019, the International Electrotechnical Commission (IEC).

Legal information

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.

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.

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 https://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.

Suitability for use in automotive applications — This NXP product has been qualified for use in automotive applications. If this product is used by customer in the development of, or for incorporation into, products or services (a) used in safety critical applications or (b) in which failure could lead to death, personal injury, or severe physical or environmental damage (such products and services hereinafter referred to as "Critical Applications"), then customer makes the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. As such, customer assumes all risk related to use of any products in Critical Applications and NXP and its suppliers shall not be liable for any such use by customer. Accordingly, customer will indemnify and hold NXP harmless from any claims, liabilities, damages and associated costs and expenses (including attorneys' fees) that NXP may incur related to customer's incorporation of any product in a Critical Application.

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.

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.

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: https://www.nxp.com

Date of release: 27 May 2024
Document identifier: i.MX93 EdgeLock Secure Enclave