i.MX RT700

SESIP Security Target

Rev. 1.0 — 25 June 2026 **Evaluation document**

Document information

Information	Content
Keywords	SESIP, PSA, NIST IR 8425, EN 18031, ETSI EN 303645, CRA, Security Target, i.MX RT700, i.MX RT735S, i.MX RT758S, i.MX RT798S
Abstract	Security target for evaluation of the i.MX RT700 developed and provided by NXP Semiconductors, according to SESIP Assurance Level 3 (SESIP3) with Physical Attacker Resistance, based on SESIP methodology version 1.2 and PSA Certified Level 3 . Applicable Essential Cybersecurity Requirements from Regulation (EU) 2024/2847 Annex I are mapped in to demonstrate CRA compliance. Applicable IEC60601-4-5 requirements are mapped in to demonstrate IEC60601 compliance. Applicable NIST 8425 requirements are mapped in to demonstrate NIST 8425 compliance. Applicable ETSI EN 303645 requirements are mapped in to demonstrate EN 303645 compliance. Applicable EN 18031 requirements are mapped in to demonstrate EN 18031 (Radio Equipment Directive) compliance.

Revision History

Rev.	Date	Description
1.0	25 June 2026	First Public Release

1 Introduction

This Security Target describes the i.MX RT700 platform and the exact security properties of the platform that are evaluated against GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2, SESIP Assurance Level 3 (SESIP3) [1].

This Security Target also complies with the CEN norm EN 17927:2023 [2]

1.1 ST Reference

i.MX RT700, SESIP Security Target, Revision 1.0, NXP Semiconductors, 25 June 2026.

1.2 SESIP Profile Reference and Conformance Claims

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

Reference	Value
SP Name	GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs [3]
SP Version	Version 1.1
Assurance Claim	SESIP Assurance Level 3 (SESIP3)
Package Claim	Base SP, Package Secure Services, Package Software Isolation, Package Hardware Protection

See Section 1.6.6 for rationale on the Package Claim.

Table 2. SESIP Profile for PSA Certified Level 3 Conformance Claims

Reference	Value
SP Name	SESIP Profile for PSA Certified Level 3 [4]
SP Version	Version 1.0
Assurance Claim	SESIP Assurance Level 3 (SESIP3)
Optional and Additional SFRs	See Section 4.3

1.3 Platform Reference

i.MX RT700

Table 3. Platform Reference

Reference	Value
Platform Name and Version	i.MX RT700, B0
Platform Identification	i.MX RT735S, i.MX RT758S, i.MX RT798S
Platform Type	Microcontroller platform for IoT application
Trusted Subsystem Identification	ELE-CP (S50)

1.4 Included Guidance Documents

The following documents are included with the platform:

Table 4. Guidance Documents

Document	Reference
SESIP Security Target	i.MX RT700 SESIP Security Target, Revision 1.0, NXP Semiconductors, 25 June 2026.
Reference Manual	i.MX RT700 Crossover Microcontrollers Reference Manual [5]
Sescurity Reference Manual	i.MX RT700 Security Reference Manual [6]
Datasheet	i.MX RT700 Crossover Microcontroller Data Sheet [7]
User Manual	User Manual of Crypto Library Normal Secure (CLNS) [11]
Application Note	AN6497, Selecting and using cryptographic algorithms and protocols [13]
Software Development Kit	MCUXpresso SDK for i.MX RT700-EVK with ELE-CP (S50) FW [10]
Tool User Guidance	Secure Provisioning SDK (SPSDK) Application User Guides [12]

1.5 Other Certification

The RNG IP implemented in i.MX RT700 has also been CAVP validated according to NISP SP 800-90A Hash-DRBG with SHA256 [15].

Table 5. NIST CAVP compliance

Item	Content
Scheme	Cryptographic Algorithm Validation Program (CAVP)
Certification body	National Institute of Standards and Technology (NIST)
Certification number	DRBG 348
Certification date	2013-06-20

1.6 Platform Overview and Description

The i.MX RT series of crossover MCUs are part of the EdgeVerse™ edge computing platform and feature Arm® Cortex®-M cores, high performance real-time functionality and MCU usability at a cost-effective price.

The i.MX RT700 crossover MCU family includes a main-compute domain with an Arm Cortex M33 and an HiFi-4 DSP both running at 325MHz, a low-energy sense-compute domain with an Arm Cortex M33 and an HiFi-1 DSP both running at 100MHz, an NXP proprietary machine learning inference core, a high-efficiency GPU, an EdgeLock Secure Enclave (Core Profile) ELE-CP (S50), a broad range of connectivity, 7.5 MBytes of shared low-power SRAM, and an always-on domain with real time clock and wake-up signaling on events.

The i.MX RT700 is supported by an extensive developer ecosystem, featuring MCUXpresso software and tools, for an optimal microcontroller design experience.

1.6.1 Platform Security Features

The i.MX RT700 employs a security subsystem, EdgeLock Secure Enclave (Core Profile) (ELE-CP (S50), legacy names CSS or CSSv2), which together with its driver provides the following security features:

- Hardware root of trust (RoT)
- Hardware cryptography accelerators (symmetric, asymmetric, secure hash, KDF, etc.)
- True Random Number Generator (TRNG) and Deterministic Random Bit Generator (DRBG)

On top of ELE-CP (S50), i.MX RT700 provides the following security features at the SoC level:

- NXP EdgeLock™ Assurance

- ARM Trustzone enabled
- Secure boot, update and debug authentication
- Physical Unclonable Function (PUF) that can generate, store and reconstruct key sizes from 64 to 4096 bits, and directly fed to ELE-CP (S50)
- OTP-based device configuration and life cycle management
- 128 bit unique device serial number for identification (UUID)
- Secure GPIO
- Intrusion and tamper detection and response sub-system
- On-chip tamper detection for voltage level, glitch, light, temperature and reset
- Device Identifier Composition Engine (DICE)

Specific to Secure Boot and Update, i.MX RT700 supports:

- Secure boot using ECDSA P-256/384 signed images
- Custom certificate format to validated image public keys
- Up to four revocable Root of Trust (RoT) or Certificate Authority keys, Root of Trust establishment by storing the SHA-2 hash digest of the hashes of up to four RoT public keys
- Anti-rollback feature for firmware update and revocable image signing keys/certificates
- Image authentication APIs and authentication of XIP images
- Recovery booting from Serial NOR flash and ISP (UART, I2C, SPI, USB)
- SB commands to program flash, OTP-eFuse, QSPI flash programming, write to RAM and execute RAM (after image authentication)
- SB3 firmware update APIs
- Boot ROM supports Device Attestation with support of Device Identifier Composition Engine (DICE)

For more product feature beyond security, refer to Chapter 2 of [5].

1.6.2 Platform Physical Scope

The physical scope is the i.MX RT700 microcontroller silicon chip as shown in Figure 1.

The hardware components and interfaces are listed in Chapter 2 of [5].

The security functionalities are expressed through the SFRs listed in Section 3. .

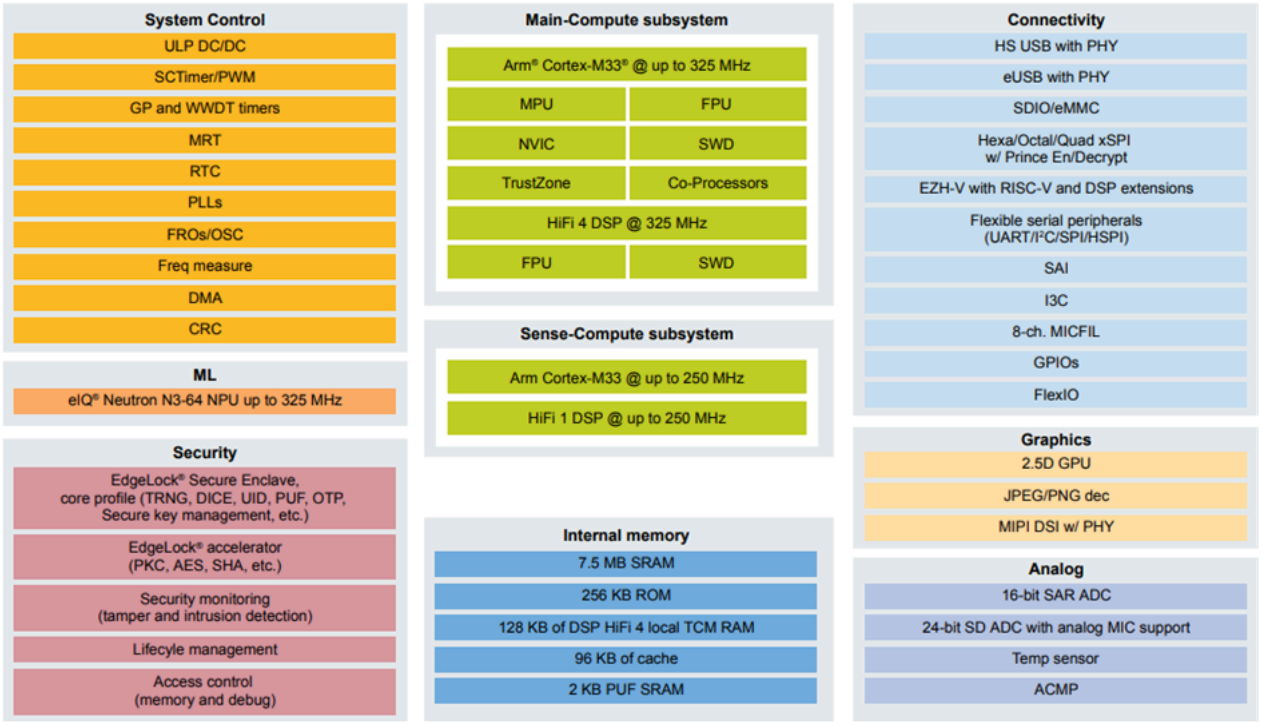

Figure 1. i.MX RT700 Family Superset Block Diagram

1.6.3 Platform Logical Scope

The logical scope includes the ROM firmware, and the optional flash loadable updatable platform root of trust (RoT) as illustrated in Figure 2 and listed in Table 6. Any additional firmware, OS or application software stored on the platform is not in scope of this evaluation. See Table 4 for a list of applicable guidance documents.

Table 6. Platform Deliverables

Type	Name	Release	Form of delivery
IC Hardware	i.MX RT700	B0	Silicon Chip
System ROM Firmware	i.MX RT700 ROM	T2.0.32	Onchip ROM Firmware
System ROM Firmware Patch	i.MX RT700 ROM Patch	N/A	Onchip Firmware
Secure Enclave	EdgeLock Secure Enclave (Core Profile) (ELE-CP (S50))	3.10.0	Onchip Hardware Subsystem
Secure Enclave ROM	ELE-CP (S50) Microcode	2.10.0	Onchip ROM Firmware
Updatable Platform RoT	ELE-CP (S50) SDK	SDK_25.12.00_ MIMXRT700-EVK (RFP 2.0 B0)	Software Package
Crypto Library	Crypto Library Normal Secure fori.MX RT700 SDK	SDK_V2.0.0	included in Software Package

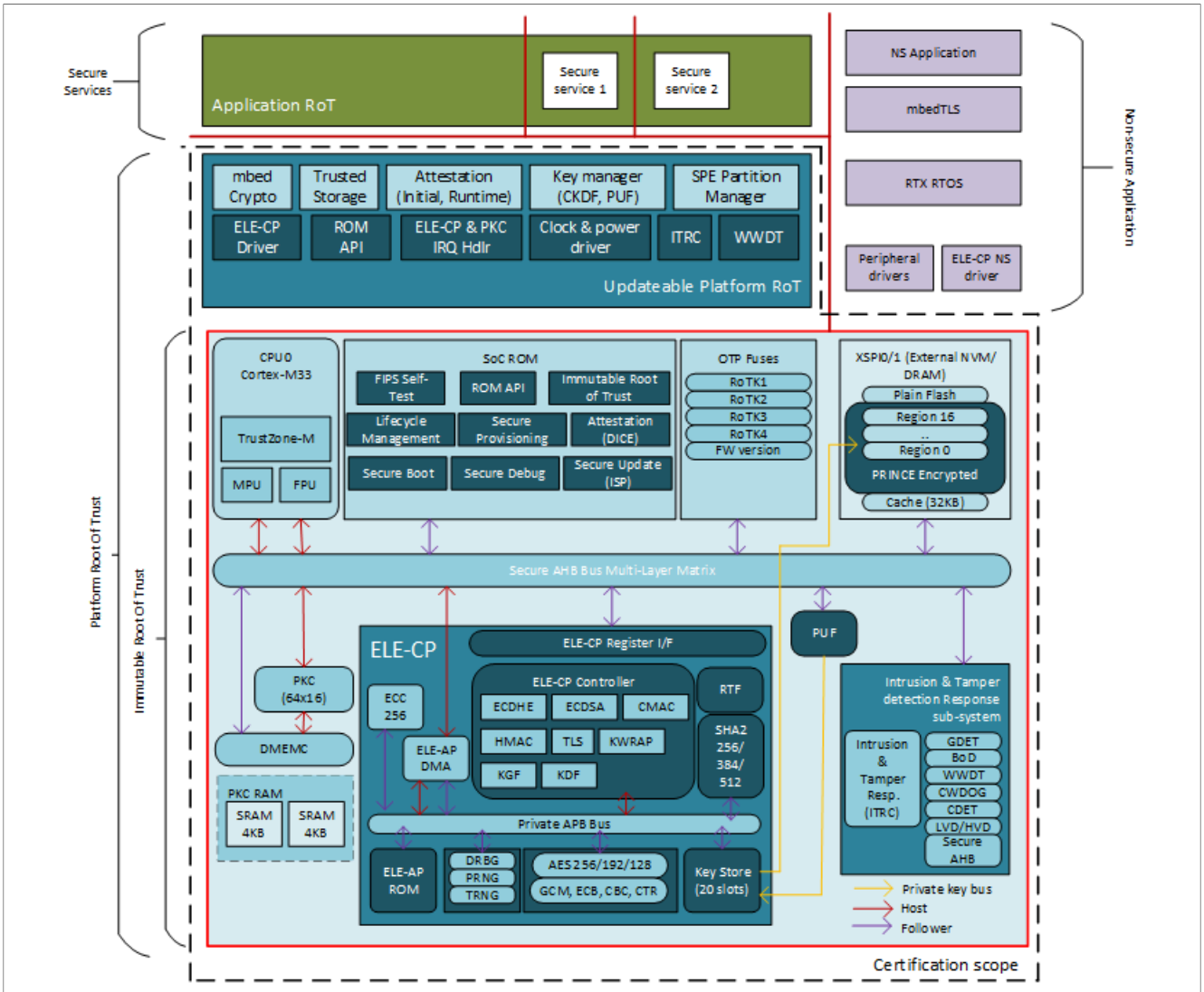

Figure 2. i.MX RT700 Logical Architecture and Certification Scope

1.6.4 Required Non-Platform Hardware/Software/Firmware

i.MX RT700 has no internal flash, hence compatible external non-volatile memory shall be deployed via FlexSPI for image storage with sufficient size. See Chapters 8 and 41 of [5].

1.6.5 Life Cycle

This device supports a security Life-Cycle state model. The current Life-Cycle state determines the device functionality, debug and test port availability, and asset accessibility. The LC_STATE fuse value controls the Life-Cycle state. The state values are selected so that additional fuse bits are burned to advance the state. Because fuses control the Life-Cycle state, moving to a more advanced state is an irreversible and permanent process. The Life-Cycle can only be advanced and cannot return to a previous state.

The boot ROM is responsible for checking the Life-Cycle state. Based on the Life-Cycle state, the ROM determines what boot flow is used, including whether control is passed to application code or not. The ROM also handles the opening of test and debug ports based on the Life-Cycle state. If the part is in the Bricked state or any invalid life cycle state, then the ROM will lock the part.

See more in Chapter 3 of [6].

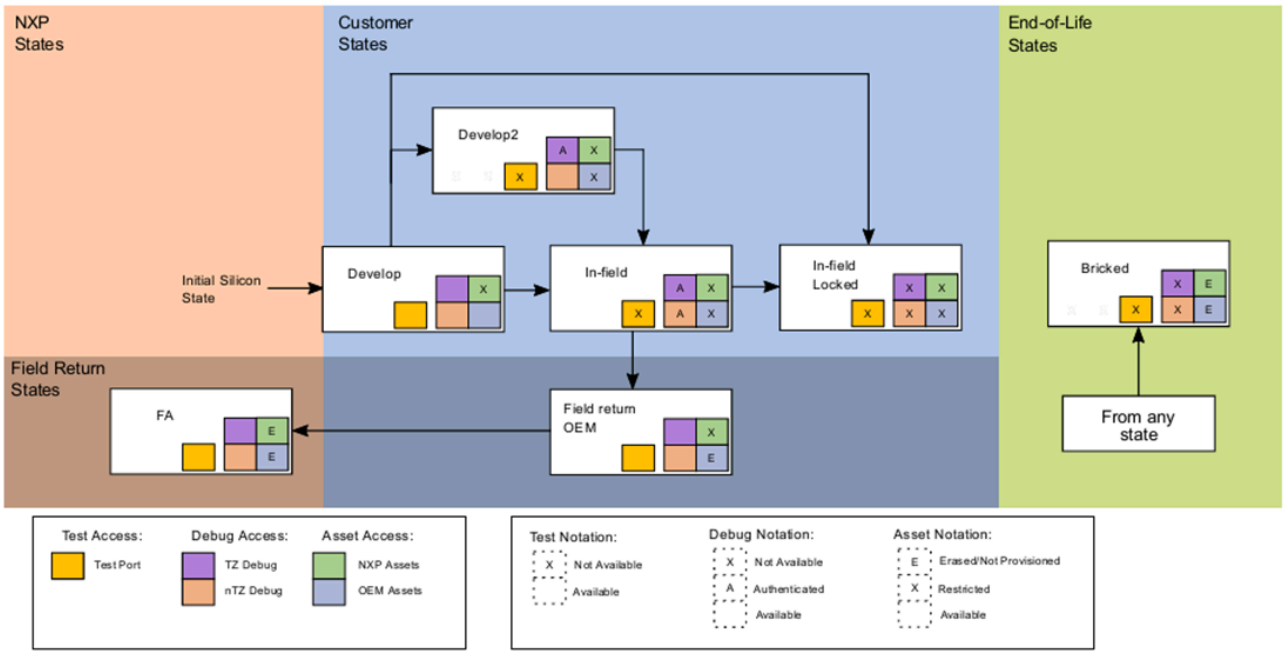

Figure 3. i.MX RT700 OEM Chip Life Cycle states

1.6.6 Configurations

Base SP Security Functional Requirements

The MCU/MPU ensures the execution of platform trusted code, particularly the functions related to secure boot, updatability, and code isolation.

Security services

The base security features are complemented by security services intended to be used by the higher software layers to implement a full-fledged Root of Trust and operating system.

Software Isolation

The Platform provides isolation between itself and the Application.

Secure Enclave

A Secure Enclave is used to ensure isolation between Platform parts .

Hardware Protection

The SoC is protected against physical attacks

1.6.7 Use Case

[any user]

The product may be physically accessed by an unknown or untrusted user, in an environment where access to the product cannot be sufficiently controlled or even in a more hostile environment.

[any code]

It cannot be excluded that the product will execute code that is unknown to the product developer.

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 fulfill the following objectives:

Table 7. Platform Objectives for the Operational Environment

Title	Description	Reference
Follow Secure Guidance	Users shall ensure secure and correct use of the platform according to guidance listed in Section 1.4.	This document Section 1.4
Platform Verification	The operating system or application code 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 Section 3.2.1.1
Key Management	Cryptographic keys and certificates outside of the Platform are subject to secure key management procedures.	This document
OEM 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 platform management, for instance for signature of firmware update, are trusted.	This document
Secure Boot	The operating system or application code are expected to make use of theSecure Boot feature as described in Chapter 7 of [6]	Chapter 7 of [6] and[9]
Secure Update and Key Revoke	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. The operating system or application code are expected to update an image with proper remedy solution and version increased and/or revoke key in case of security incidence occurrence of the image and/or the key.	Chapter 7 of [6]
Secure Debug	The integrating environment is expected to configure the debug functionality as described in Chapter 10 of [6] and [8] to meet the extra physical attacker resistance.	Chapter 10 of [6], and [8]
SW Integration	The operating system or application code are expected to ensure the correct version of SDK drivers are integrated and configured.	This document
Lifecycle Management	The operating system or application code are expected to provide lifecycle states and secure mechanism of lifecycle state transition according to the use case, and the operational environment is expected to configure the platform accordingly for lifecycle state transitions. In general, the operating system or application code are expected to configure the platform to In-field or In-field locked state.	Chapter 3 of [6]
Software isolation	i.MX RT700 provides two different isolation mechanisms: ELE-CP (S50) vs rest of SoC, and TrustZone Secure vs Non-secure. The operating system or application code are expected to configure and utilize at least one mechanism for isolation between platform and application.	Chapter 17 of [6], Chapter 7 of [5]
Physical attacker resistance configurations	If local physical attack is applicable for the use cases, the following configurations shall be kept after boot by the operating system or application code: • The operating system or application code are expected to configure the `compute_main_clk` to one of the internal clock sources;	This document, Chapters 12, 13, 14 and 24 of [6]

Table 7. Platform Objectives for the Operational Environment*...continued*

Title	Description	Reference
	• The operating system or application code are expected to configure the appropriate trigger source events in the ITRC controler; • The operating system or application code are expected to enable the glitch detectors • ARM CM33 CPU is not hardened against physical attacks, e.g., voltage glitching or EMFI. It is therefore recommended to harden secure application against such attacks using software-based countermeasures and leverage code watchdog offered by i.MX RT700;	

3 Security Requirements and Implementation

3.1 Security Assurance Requirements

The claimed assurance requirements packages are the following as defined in Chapter 4 of GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 [1]:

- **SESIP Assurance Level 3 (SESIP3)** .

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).

i.MX RT700'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). See Section 3.2.2.1 for further information.

3.2 Security Functional Requirements

In the following Security Functional Requirements, the term **platform** covers the **i.MX RT700 physical and logical scope**, and the term **application** refers to any additional firmware, OS or application software which is out of evaluation scope. It represents a part of the final connected device.

i.MX RT700 fulfils the following security functional requirements:

3.2.1 Identification and Attestation of Platforms and Applications

3.2.1.1 Verification of Platform Identity

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

Conformance rationale:

The ELE-CP (S50) Hardware and Software (microcode) versions are available from `ELS_VERSION` register as per chapters 17.3.2.22 and 17.4.21 of [6] and shall match the versions indicated in Section 1.6.3.

The ROM version can be read using the `GetProperty` command in ISP mode with tag 18h (Target ROM build version) as per chapters 9.5.2 and 9.5.16 of [6] and shall match the value in Section 1.6.3. The ROM version can also be read from `SYSCON0=>ELS_AS_CFG3` register as per chapter 13.6.1.72 of [6].

The ROM patch version can be read from `SYSCON0=>ELS_AS_CFG3` register as per chapter 13.6.1.72 of [6] and shall match the value in Section 1.6.3.

The SoC hardware version can be read using the `GetProperty` command in ISP mode with tag 10h as per chapters 9.5.2 and 9.5.16 of [6] and shall match the value in Section 1.6.3. The SoC hardware version can also be read from the `SYSCON3=>SILICONREV_ID` register as per chapter 13.6.4.10 of [6].

The CryptoLib version can be read using the `mcuxCl_GetVersion()` API. See "mcuxCl_GetVersion" in "mcuxCl_clns.h" section of [11].

The production validation process ensures that the SFR behaves correctly.

3.2.1.2 Verification of Platform Instance Identity

The platform provides a unique identification of that specific instantiation of the platform.

Conformance rationale:

The platform stores a 128-bit Universally Unique Identifier (UUID) in `SYSCON0=>ELS_AS_UUID0..ELS_AS_UUID3` registers (see Chapter 13.6.1.69 of [6]). One way to read out UUID is to use `GetProperty` command in ISP mode with tag 12h as specified in Chapters 9.5.2 and 9.5.16 of [6].

Furthermore, i.MX RT700 supports Device Identifier Composition Engine (DICE) Specification specified by Trusted Computing Group, which provides another way to uniquely identify a product instance (see Section 3.2.1.3 for more details).

The production validation process ensures that the SFR behaves correctly.

3.2.1.3 Attestation of Platform Genuineness

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

Conformance rationale:

Secure Attestation is a mechanisms used to provide evidence on the device’s genuine identity. Device Identity Composition Engine (DICE), as defined by Trusted Computing Group, uses Immutable RoT during boot time to create a signed attestation of platform UUID/ECID, hardware version, ROM version, and ROM patch (See chapters 7.2.2 and 7.15 of [6]). The PROVE_GENUINITY command can be used to read the attesation record from RAM (see chapter 9.5.15.8 of [6]).

In addition to DICE, Runtime Fingerprint (RTF) is an NXP-proprietary attestation mechanism, which measures the device’s software and hardware state during boot-time and run-time as well. See more in Chapters 2.10, 17.3.2.18 of [6] and [14].

Trust provisioning is a process used for creation of initial Device Identity keys. Its major objective is to provide a cryptographic proof of the device’s origin and to offer a set of tools to OEM for secure provisioning of their own assets. A device-unique private-public key pair is created on every device, the public portion of which is collected and signed by NXP. That signed public key is installed back onto every device in a form of device-unique certificate, which serves the actual proof of the device’s origin. The corresponding private key, together with other pre-installed key, is then used for authentication and secure connection to the device, enabling secure provisioning of OEM assets. See chapters 2.12, 7.11, 9.5.15, 17.3.2.3.6, 17.3.2.19 in [6].

The production validation process ensures that the SFR behaves correctly.

3.2.1.4 Secure Initialization of the Platform

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

Conformance rationale:

The secure part of the ROM bootloader of i.MX RT700 provides secure boot operation. Secure boot prevents unauthorized code from being executed on a given product. To ensure this level of security, secure boot always leaves the device ROM in an executing mode when coming out of a reset. The ROM can then assess the first user executable image resident in the flash memory and determine the authenticity of that code. The control is transferred to authentic code only. A chain of trusted code from the ROM to the user boot code is established. And the chain can be further extended through the verification of digital signatures associated with additional code layers.

The Elliptic Curve Digital Signature Algorithm (ECDSA) is used in this architecture to verify the authenticity of the boot code. The boot code is always signed with ECDSA P-256 or P-384 private keys. The corresponding ECDSA public keys used for signature verification (Root of Trust Keys) are contained in the certificate block included in the signed image. Support is provided for up to four Root of Trust keys.

The boot ROM supports different kind of boot based on pin allocation (see Chapters 6.3 of [6]): Prime boot from external NOR, NAND or eMMC Flash memories and ISP (In System Programming). In case of Prime boot failure, Recovery boot from NOR Flash is possible when enabled in fuse (See Chapters 6.2 and 6.8 of [6]). In case the Recovery boot fails, ISP can still be used.

The production validation process ensures that the SFR behaves correctly.

3.2.1.5 Attestation of Platform State

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

Conformance rationale:

See Section 3.2.1.3.

The production validation process ensures that the SFR behaves correctly.

3.2.1.6 Attestation of Application Genuineness

The platform provides an attestation of the application, in a way that ensures that the application has not been cloned or changed without detection.

Conformance rationale:

See Section 3.2.1.3.

The production validation process ensures that the SFR behaves correctly.

3.2.1.7 Attestation of Application State

The platform provides an attestation of state of the application.

Conformance rationale:

See Section 3.2.1.3.

The production validation process ensures that the SFR behaves correctly.

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

3.2.2.1 Secure Update of Platform

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

Conformance rationale:

The secure part of the ROM bootloader of i.MX RT700 provides a secure firmware update operation. Secure Update is the process used to securely update the firmware image in the field. The firmware image is encrypted using AES-128 or AES-256 and signed using ECDSA P-256, following the SB3.1 firmware image format. Secure Update guarantees authenticity and confidentiality of the new image. It also ensures that the new image is up-to-date, preventing the rollback to an older image. Running firmware is in charge of receiving and verifying the new firmware image. The follow-up Secure Boot verifies the new firmware image again, making sure the Immutable RoT is still in charge of ensuring authenticity of the latest firmware.

The anti-rollback is achieved by OTP fusewords SEC_FW_VER0..SEC_FW_VER3. The OTP fusemap also contains monotonic counter DCFG_CC_VU and IMAGE_KEY_REVOKE revocation field that can be updated as these are implemented as redundant 16-bit fusewords. See more in I.MX700_Fusemap.xlsx attached in [6].

The dual image boot and secure boot from the FlexSPI interface provides recovery capability for the device. See more in Section 3.2.1.4 and Section 3.2.5.6.

Furthermore, a trust provisioned private key, together with other pre-installed key material, is then used for authentication and secure connection to the device, enabling secure provisioning of OEM assets in manufacturing environment the OEM may not fully trusts. See also Section 3.2.1.3.

3.2.2.2 Decommission of Platform

The platform can be decommissioned.

Conformance rationale:

The End-of-Life security life cycle state, also called Bricked State, can be used by customers or NXP to remove a chip permanently from regular use and erase/block access to secrets inside the chip. Bricked is the final life cycle state, so the device cannot be advanced to any other states from Bricked and is locked unusable. See more in Chapter 3.6 of [6].

The production validation process ensures that the SFR behaves correctly.

3.2.2.3 Field Return of Platform

The platform can be returned to the vendor without user data.

Conformance rationale:

i.MX RT700 provides a secure Field Return feature.

In the Field Return OEM state, OEM assets are wiped (keys rotated), test and debug ports are open, and ROM does not pass execution to application code. The debug port is used to load and execute diagnostic program. This mechanism protects leakage of any residual data left during life-cycle state transition. See more in Chapters 3.2 and 3.3 of [6]

It can further move to FA life cycle state if the device is being returned to NXP for testing and failure analysis. In this state, NXP assets are wiped (keys rotated) and on every boot the ROM checks and erases key storage. Here also the ROM does not pass execution to application code and the debug port must be used to load and execute diagnostic program. See more in Chapters 3.2, 3.3 and 3.5 of [6].

The production validation process ensures that the SFR behaves correctly.

3.2.3 Extra Attacker Resistance

3.2.3.1 Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other functional requirements.

Conformance rationale:

i.MX RT700 is equipped with Intrusion and Tamper Response Controller (ITRC). ITRC provides a mechanism to configure the response action in case of intrusion event detected by on-chip security sensors. Intrusion Response is the action a device performs in order to prevent misuse of the device or disclosure of critical assets (cryptographic keys, personal data) that are generated or stored within the device. The response mechanism is typically triggered by either a signal from an on-chip sensor designed to detect that the device is in a threat condition or by an explicit command provided by the software. See more in Chapters 24 and 26 of [6].

Also, the software components including ROM leverage the code watchdog. For code watchdog, see more in Chapter 25 of [6]. The crypto coprocessor and library are securely hardened against potential physical attacks.

Furthermore, this device has one instance of the independent real time clock, RTC. This block is a low power module that provides time keeping and calendaring functions, protection against spurious memory/register updates and battery operation. See Chapter 35 of [5]. This function provides another layer of protection yet needs further HW support at board level, hence, not in the evaluation scope.

The internal vulnerability analysis process ensures that the SFR behaves correctly.

3.2.3.2 Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)

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

Conformance rationale:

There are multiple isolation features presented in the platform.

The ELE-CP (S50) module is a security subsystem supporting a wide range of cryptographic algorithms and providing strong key isolation from the rest of the system. When embedded in an SoC, ELE-CP (S50) serves as the main building block of the SoC's immutable Root of Trust. It is used as part of the trust anchor during secure boot, secure debug access, life-cycle management, and trust provisioning. ELE-CP (S50) has its own controller and exclusive system resources with enforced access control, hence it is isolated from the rest of the platform. See more in Chapter 17 of [6].

The SoC is segmented in several domains (Compute, Sense, Media) with separate security configured bus controllers. See more in Chapter 2.9 of [6].

PRINCE-based memory encryption also ensures Secure Isolation between multiple IP vendors. Initial Vector (IV) is derived by secure-privilege and a different value is used for every independent memory region, ensuring the isolation between each other. See more in Chapters 2.8 and 18.3.14.16 of [6].

ARM TrustZone enables Secure Isolation during run-time by providing four distinct levels of privilege: secure-privilege, secure-user, non-secure-privilege, non-secure user. Every peripheral is equipped with Peripheral Protection Checker (PPC) that can be programmed to control access to that peripheral, following the ARM TrustZone philosophy. Every memory is equipped with Memory Protection Checker (MPC) that can also be programmed in the same way as the PPC. Secure AHB Controller is in charge of programming all PPC and MPC blocks and only the highest level of privilege, which is secure-privilege, is allowed to do that. See more in Chapter 2.9 of [6].

Additional isolation is provided using Armv8-M architecture as both CPU0 and CPU1 Cortex-M33 cores have 8 MPU (Memory Protection Unit) and 8 SAU (Security Attribute Unit). See more in Chapter 2.9 of [6].

The production validation process ensures that the SFR behaves correctly.

3.2.3.3 Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services

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

Conformance rationale:

The isolation between PSA-RoT and Application Root of Trust Services is included in Section 3.2.3.2.

Also see more in Section 3.2.4.4 about key isolation.

The production validation process ensures that the SFR behaves correctly.

3.2.3.4 Software Attacker Resistance: Isolation of Platform Parts

The platform provides isolation between platform parts, such that an attacker able to run code in *the platform parts outside of the ELS ELE-CP (S50)* can compromise neither the *confidentiality and* integrity of *the ELS ELE-CP (S50)* nor the provision of any other Security Functional Requirements.

Conformance rationale:

The ELE-CP (S50) subsystem is a security subsystem supporting a wide range of cryptographic algorithms and providing strong key isolation from the rest of the system. When embedded in an SoC, ELE-CP (S50) serves as the main building block of the SoC's immutable Root of Trust. It is used as part of the trust anchor during secure boot, secure debug access, life-cycle management, and trust provisioning.

ELE-CP (S50) has its own controller and exclusive system resources with enforced access control, hence it is isolated from the rest of the platform. See more in Chapter 17 of [6].

The production validation process ensures that the SFR behaves correctly.

3.2.4 Cryptographic Functionality

3.2.4.1 Cryptographic Operation

The platform provides the *operations in Table 8* functionality with *algorithms in Table 8* as specified in *specifications in Table 8* for key lengths *described in Table 8* and modes *described in Table 8* .

Table 8. Cryptographic Operations by ELE-CP (S50)

Operation	Algorithm	Specification	Key Lengths	Modes
Encryption and decryption	AES	FIPS-197 NIST SP 800 38A	128, 192, 256	ECB, CBC, CTR
Authenticated encryption, authenticated decryption	AES	FIPS-197 NIST SP 800-38D	128, 192, 256	GCM
Hashing	SHA2	FIPS 180-4	224, 256, 384, 512	N/A
MAC generation and verification	HMAC	FIPS 198-1	256	SHA-256
MAC generation and verification	CMAC	NIST SP 800-38B	128, 256	AES

Table 8. Cryptographic Operations by ELE-CP (S50)...*continued*

Operation	Algorithm	Specification	Key Lengths	Modes
Signature generation and verification	ECDSA	FIPS PUB 186-4	256	SECP256R1

Conformance rationale:

The cryptographic operations listed in this SFR are handled by ELE-CP (S50). ELE-CP (S50) provides symmetric encryption/decryption, hashing, and asymmetric functions. See more in Chapters 17 of [6] and "mcuxClEls" section of [11].

The production validation process ensures that the SFR behaves correctly. Additionally, the SFR is validated by NXP ACVP lab against NIST CAVP.

3.2.4.2 Cryptographic Operation (PKC)

The platform provides the *operations in Table 9* functionality with *algorithms in Table 9* as specified in *specifications in Table 9* for key lengths *described in Table 9* and modes *described in Table 9* .

Table 9. Cryptographic Operations by ELE-CP (S50)

Operation	Algorithm	Specification	Key Lengths	Modes
Signature generation and verification	ECDSA	NIST FIPS 186-5	384	secp384r1

Conformance rationale:

The cryptographic operations listed in this SFR are handled outside the ELE-CP (S50), and rely on the Public-Key crypto Coprocessor (PKC) of the i.MX RT700. See Chapter 21 of [6]) and "mcuxClEcc" and "mcuxClPkc" sections of [11].

The production validation process ensures that the SFR behaves correctly. Additionally, the SFR is validated by NXP ACVP lab against NIST CAVP.

3.2.4.3 Cryptographic Key Generation

The platform provides a way to generate cryptographic keys for use in *algorithms in Table 10* as specified in *specifications in Table 10* for key lengths *Key Lenghts in Table 10*

Table 10. Cryptographic Key Generation

Algorithm	Specification	Key Lengths
ECDSA	NiST FIPS 186-5 ANSI X9.62 SEC2	SECP R1 256
HKDF	RFC5869 with HMAC (FIPS PUB 198-1) NIST SP 800-56C with SHA-256 (FIPS 180-4)	128, 256
CKDF	NIST SP 800-108 with CMAC (NIST SP 800-38B) NIST SP 800-56C	128, 256
TLS Master Key Derivation	IETF RFC5246 TLS 1.2	256

Table 10. Cryptographic Key Generation*...continued*

Algorithm	Specification	Key Lengths
TLS Session Key Derivation	IETF RFC5246 TLS 1.2	128 & 256
ECDH	IETF RFC8418	256

Conformance rationale:

The cryptographic key generations listed in this SFR are handled by the ELE-CP (S50). See more in Chapter 17 of [6] and "mcuxClEls" section of [11].

The production validation process ensures that the SFR behaves correctly. Additionally, the SFR is validated by NXP ACVP lab against NIST CAVP.

3.2.4.4 Cryptographic KeyStore

The platform provides 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, signature generation and verification, MAC generation and verification, key derivation, shared secret generation*.

Conformance rationale:

The ELE-CP (S50) provides key store function. Keys are stored inside the ELE-CP (S50) in a bank of internal 128-bit registers (each register is called a "key slot") and can be exported to external memory wrapped in encrypted blobs according to the RFC3394 standard. Keys cannot be accessed by the system. Keys in KeyStore can be imported (from OTP of PUF), derived (see Section 3.2.4.3), or unpacked from an RFC3394 wrapped key stored in system memory. Each Keystore Key has associated properties and ELE-CP (S50) enforces usage rules based on the properties of keys. See more in Chapters 17 and 22 of [6] and "mcuxClEls" section of [11].

The production validation process ensures that the SFR behaves correctly.

3.2.4.5 Cryptographic Random Number Generation

The platform provides a way based on *physical noise and DRBG* to generate random numbers as specified in *NIST.SP.800-90B and NIST.SP.800-90B CTR-DRBG with AES-128*.

Conformance rationale:

ELE-CP (S50) has a physical True Random Number Generator (TRNG) compliant with NIST SP 800-90B. This TRNG is used to seed an internal DRBG module as defined in NIST SP 800-90A.

Furthermore:

- The TRNG is capable to pass AIS 31 statistical tests T0-T8

See more in Chapters 17 of [6] and "nxpClEls" section of [11].

The production validation process ensures that the SFR behaves correctly. Additionally, the SFR is validated by NXP ACVP lab against NIST CAVP.

3.2.5 Compliance Functionality

3.2.5.1 Secure Data Serialization

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

Conformance rationale:

XSPI0 (Flash) and XSPI1 (Flash/DRAM) support inline PRINCE encryption/decryption in CTR, GCM, and XEX modes to achieve authenticity, integrity and confidentiality (see more in Chapters 2.3.3.3 and 41.3 of [5], and Chapters 6.5.2.4 and 18.3.14 to 18.3.16 of [6]). The key is stored in ELE-CP (S50) and derived from PUF which also provides binding to platform instance. See more in Chapter 22 of [6].

The production validation process ensures that the SFR behaves correctly.

3.2.5.2 Residual Information Purging

The platform ensures that *key store areas*, with the exception of *none*, is erased using the method specified in *document and section specified in the Conformance Rationale below* before the memory is used by the platform or application again and before an attacker can access it.

Conformance rationale:

ELE-CP (S50) provides `KDELETE` command which zeroizes the selected keystore on demand. See more in Chapter 17.3.2.3.9 of [6].

The production validation process ensures that the SFR behaves correctly.

3.2.5.3 Residual Information Purging (SoC)

The platform ensures that *PUF derived data, RAMs*, with the exception of *none*, is erased using the method specified in *the conformance rationale below* before the memory is used by the platform or application again and before an attacker can access it.

Conformance rationale:

The PUF zeroization operation scrambles the PUF, removes all the key material from PUF Engine / SRAM and will disable the PUF from outputting keys. It can be triggered by the hardware on threat detection or on demand by software.

The RAM zeroization (PKC RAM & SRAM Partition 4-5) removes all material from the RAM. It can be triggered by the hardware on threat detection or on demand by software.

See sections 22 and 24 of [6]. See also Section 3.2.2.3.

The production validation process ensures that the SFR behaves correctly.

3.2.5.4 Reliable Index

The platform implements a strictly increasing function.

Conformance rationale:

ELE-CP (S50) provides 14 fuse words of 32 bits each, for customer definition and usage which can be used as reliable index or monotonic counters due to the irreversible nature. The fuse programming and readout is achieved by ROM API. See more in Chapters 8.2.3, 9.5.11 and 9.5.12 of [6] and "i.MXRT700_Fusemap.xls" file included in [6] (fuse words 460 to 481).

The production validation process ensures that the SFR behaves correctly.

3.2.5.5 Secure Debugging

The platform only provides *SWD/JTAG interface* authenticated as specified in *the guidance document referenced in the Conformance rationale below* with debug functionality.

The platform ensures that all data stored, with the exception of *the guidance document referenced in the Conformance rationale below*, is made unavailable.

Conformance rationale:

The SWD/JTAG interface authentication is specified in [8]

In "In-field Locked" life cycle state the debug is blocked. In "In-field" life cycle states the chip forces a debug authentication protocol.

The debug authentication is a challenge-response scheme and assures that only the debugger in possession of the required debug credentials (approved by the product manufacturer) can successfully authenticate over the debug interface and access restricted parts of the device. The debug session is initiated by the debugger. The device responds by a Debug Authenitcation Challenge (DAC) with debug access information preconfigured in OTP (DCFG_CC) and a random challenge. The debugger sends back the Debug Authentication Response (DAR) signed with the manufacturer ROT private key (ECDSA) and containing the debugger access permission certificate, manufacturer ROT public key, and the random challenge. The device then compares the hash of the manufacturer ROT public key with the provisioned value in OTP, checks the DAR signature, and imports the debugger access permission certificate which can be used for secure debug.

Furthermore, the debug subsystem is sub-divided into multiple debug domains to allow finer access control.

See more in Chapter 16 of [5], Chapter 10 of [6] and [8].

The production validation process ensures that the SFR behaves correctly.

3.2.5.6 Secure Recovery

The platform detects anomalies *image authentication failure* and recovers to reach back a known state *application*.

Conformance rationale:

The Boot ROM supports recovery boot from an external serial NOR flash. See more in Chapter 6.8 of [6].

Also, see Section 3.2.1.4 and Section 3.2.2.1.

The production validation process ensures that the SFR behaves correctly.

4 Mapping and Sufficiency Rationales

4.1 SESIP3 Sufficiency

Table 11. 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 1.6.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in Section 2 refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	Section 3	All SFRs in this ST are taken from [1]. SFR "Verification of Platform Identity" is included. SFR "Secure Update of Platform" is included. The SARs are an exact SESIP assurance level. No multiple assurance level is claimed.
	ASE_TSS.1 TOE Summary Specification	Section 3	All SFRs are listed per definition, and for each SFR the implementation and verification is defined in the SFR.
ADV: Development	ADV_FSP.4 Complete functional specifications	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Section 1.4	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	The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in

Table 11. SESIP3 Sufficiency *...continued*

Assurance Class	Assurance Family	Covered By	Rationale
		evaluator to ascertain the presence of potential vulnerabilities.	the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Enhanced-Basic.

4.2 Conformance Mapping to SESIP Profile for Secure MCUs and MPU

This section provides rationales of conformance claimed in Section 1.2

Table 12. SESIP Profile for Secure MCUs and MPUs Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.2.1.1
	Secure Initialization of Platform	Section 3.2.1.4
	Secure Updated of Platform	Section 3.2.2.1
	Residual Information Purging	Section 3.2.5.2 Section 3.2.5.3
	Secure Debugging	Section 3.2.5.5
Security Services	Cryptographic Operation	Section 3.2.4.1 Section 3.2.4.2
	Cryptographic Key Generation	Section 3.2.4.3
	Cryptographic KeyStore	Section 3.2.4.4
	Cryptographic Random Number Generation	Section 3.2.4.5
Software Isolation	Software Attacker Resistance: Isolation of Platform	Section 3.2.3.2 Section 3.2.3.3
Hardware Protection	Physical Attacker Resistance	Section 3.2.3.1
Secure Enclave	Software Attacker Resistance: Isolation of Platform Parts	Section 3.2.3.4
Additional SFRs (Optional)	Verification of Platform Instance Identity	Section 3.2.1.2
	Attestation of Application Genuineness	Section 3.2.1.6
	Attestation of Application State	Section 3.2.1.7
	Attestation of Platform Genuineness	Section 3.2.1.3
	Attestation of Platform State	Section 3.2.1.5
	Decommission of Platform	Section 3.2.2.2
	Field Return of Platform	Section 3.2.2.3
	Reliable Index	Section 3.2.5.4
	Secure Data Serialization	Section 3.2.5.1
	Secure Recovery	Section 3.2.5.6

4.3 Conformance Mapping for SESIP Profile for PSA Certified Level 3

This section provides rationales of conformance claimed in Section 1.2

Table 13. SESIP Profile for PSA Certified Level 3 Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.2.1.1

Table 13. SESIP Profile for PSA Certified Level 3 Sufficiency*...continued*

Package Claimed	Security Functional Requirements	Covered By
	Verification of Platform Instance Identity	Section 3.2.1.2
	Attestation of Platform Genuineness	Section 3.2.1.3
	Secure Initialization of Platform	Section 3.2.1.4
	Attestation of Platform State	Section 3.2.1.5
	Secure Updated of Platform	Section 3.2.2.1
	Physical Attacker Resistance	Section 3.2.3.1
	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Section 3.2.3.2
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	Section 3.2.3.3
	Cryptographic Operation	Section 3.2.4.1 Section 3.2.4.2
	Cryptographic Random Number Generation	Section 3.2.4.5
	Cryptographic Key Generation	Section 3.2.4.3
	Cryptographic KeyStore	Section 3.2.4.4
Optional SFR	Secure Debugging	Section 3.2.5.5
	Secure Data Serialization	Section 3.2.5.1

5 Appendix

5.1 IEC 60601 support

IEC 60601-4-5 support

The table below shows how the platform under evaluation (i.MX RT700 described in this Security Target) supports the component that is built on top of that platform, demonstrating compliance with the IEC 60601-4-5 requirements (see [19]). The table describes which parts of each 60601-4-5 requirement are implemented at platform level or supported by the platform. Then, it is the responsibility of the component developer to make appropriate use of the platform security features to entirely implement the 60601-4-5 requirements. The platform provides all the mechanisms needed for development of a component compliant with SL-C 3.

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 60601-4-5 standard. By construction, 60601-4-5 is based on (and very close to) 62443-4-2. The delta from 62443-4-2 is identified below by ***Bold Italic*** text.

Table 14. IEC 60601-4-5 security requirements support by i.MX RT700

60601-4-5 requirements	i.MX RT700 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 Cryptographic Operation (SoC) Cryptographic Key Store will provide cryptographic functionalities that can be used to implement human user identification and authentication.
CR 1.2 - Software process and device identification and authentication ***CR 1.2 RE(1) - Unique identification and authentication***	Verification of Platform Identity will provide a unique and tamper-proof identification of the i.MX RT700 type and version, that can be used for precise identification of the component (by including subcomponent identification). Verification of Platform Instance Identity will provide a unique and tamper-proof identity of each i.MX RT700 instance, that can be used for precise identification of the component (by including subcomponent identification). Attestation of Platform Genuineness will provide an attestation for the i.MX RT700 identity, that can be used for full authentication of the component (by including subcomponent authentication). Cryptographic Key Generation Cryptographic Random Number Generation Cryptographic Operation Cryptographic Operation (SoC) Cryptographic Key Store will provide cryptographic functionalities that can be used to implement identification and authentication to any other components.
CR 1.3 - Account management	Cryptographic Key Generation Cryptographic Random Number Generation Cryptographic KeyStore will provide random number generation, key generation, and key storage services which can be used for account creation and management.
CR 1.4 - Identifier management	Cryptographic Key Generation Cryptographic Random Number Generation Cryptographic KeyStore will provide random number generation, key generation, and key storage services which can be used for unique identifier creation and management.
CR 1.5 - Authenticator management CR 1.5(1) - Hardware security for authenticators	Cryptographic Key Generation Cryptographic Random Number Generation Cryptographic KeyStore will provide random number generation, key generation, and key storage services which can be used for authenticator creation and management. Physical Attacker Resistance will provide protections of authenticators against physical attacks.

Table 14. IEC 60601-4-5 security requirements support by i.MX RT700*...continued*

60601-4-5 requirements	i.MX RT700 supports
	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) Software Attacker Resistance: Isolation of Platform Parts will provide protection of authenticators against remote and local logical attacks.
CR 1.6 – Wireless access management	Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation, Cryptographic Operation (SoC) Cryptographic Key Store, will provide cryptographic functionalities that can be used by network-components to implement 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 CR 1.7(2) – Password lifetime restrictions for all users (human, software process, or device)	Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic KeyStore, will provide random number generation, key generation, and key storage that can be used to generate and manage passwords in compliance with defined rules. Reliable Index, will provide time references and monotonic counters allowing password lifetime restriction management.
CR 1.8 – Public key infrastructure certificates	Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation, Cryptographic Operation (SoC) Cryptographic Key Store, will provide cryptographic functionlaities that can be used to interact and operate with PKI infrastructures.
CR 1.9 – Strength of public key-based authentication CR 1.9(1) – Hardware security for public key-based authentication	Cryptographic Key Generation Cryptographic Random Number Generation Cryptographic Operation Cryptographic Operation (SoC) Cryptographic Key Store will provide cryptographic features that can be used for public key-based authentication according to defined strength rules. Physical Attacker Resistance will provide protection of public key-based authentication related material against physical attacks. Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) Software Attacker Resistance: Isolation of Platform Parts will provide protection of public key-based authentication related material against remote and local logical attacks.
CR 1.10 – Authenticator feedback	
CR 1.11 – Unsuccessful login attempts	
CR 1.12 – System use notification	
CR 1.14 – Strength of symmetric key-based authentication CR 1.14(1) – Hardware security for symmetric key-based authentication	Cryptographic Key Generation Cryptographic Random Number Generation Cryptographic Operation Cryptographic Operation (SoC) Cryptographic Key Store will provide cryptographic features that can be used for symmetric key-based authentication according to defined strength rules. Physical Attacker Resistance will provide protection of symmetric key-based authentication related material against physical attacks. Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) Software Attacker Resistance: Isolation of Platform Parts will provide protection of symmetric key-based authentication related material against remote and local logical attacks.
CR 2.1 – Authorization enforcement CR 2.1(1) – Authorization enforcement for all users (humans, software processes and devices)	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) Software Attacker Resistance: Isolation of Platform Parts will provide logical isolation of the i.MX RT700 internals that can

Table 14. IEC 60601-4-5 security requirements support by i.MX RT700*...continued*

60601-4-5 requirements	i.MX RT700 supports
CR 2.1(2) – Permission mapping to roles CR 2.1(3) – Supervisor override CR 2.1(4) – Dual approval	be leveraged to enforce authorization ***and privileges*** of properly authenticated entities.
CR 2.2 – Wireless use control	Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation, Cryptographic Operation (SoC) and Cryptographic KeyStore, will 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 will provide secure boot and secure update with integrity and authenticity check of mobile code. Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation, Cryptographic Operation (SoC) Cryptographic Key Store, will 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. will provide mobile code authenticity check prior to the code being executed.
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. will provide session management based on user or entity authentication. 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 2.9(1) – Warn when audit record storage capacity threshold reached CR 2.10 – Response to audit processing failures CR 2.11 – Timestamps CR 2.11(1) – Time synchronization CR 2.11(2) – Protection of time source integrity	All SESIP SFRs provide output status which can be integrated to the component audit records. will provide audit logs management. Secure Data Serialization, will provide secure storage service that can be used to securely store audit records, including the timestamps. Reliable Index will provide a time base that can be used to create time stamps for use in audit records. Physical Attacker Resistance will provide protections against physical attacks that could affect audit records overall management. Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) and Software Attacker Resistance: Isolation of Platform Parts will provide protections against remote and local logical attacks that could affect audit records overall management.
CR 2.12 – Non-repudiation CR 2.12(1) – 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. will provide non-repudiation proof based on user or entity authentication. Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation, Cryptographic Operation (SoC) and Cryptographic KeyStore, will provide 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 CR 2.13(1) – Active monitoring	Secure Debugging will provide protected access to the physical diagnostic and test interfaces of the i.MX RT700 with active monitoring. Field Return of Platform, Decommission of Platform, will provide enablement / disablement of physical diagnostic and test interfaces depending on the life cycle state.
CR 3.1 – Communication integrity	will provide communication integrity and authenticity.

Table 14. IEC 60601-4-5 security requirements support by i.MX RT700*...continued*

60601-4-5 requirements	i.MX RT700 supports
CR 3.1(1) – Communication authenticity	Cryptographic Operation, Cryptographic Operation (SoC) will provide cryptographic operations that can be used to protect integrity and authenticity of transmitted information. Cryptographic Key Generation, and Cryptographic Random Number Generation, will provide cryptographic functionalities that can be used to generate the cryptographic materiel necessary for the protection of transmitted information. Cryptographic KeyStore, will provide secure storage that can be used to store cryptographic material (e.g. shared secret) on which such protections is be based. Physical Attacker Resistance will provide protections of cryptographic services involved in secure communication integrity and authenticity enforcement against physical attacks. Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) and Software Attacker Resistance: Isolation of Platform Parts will provide 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 Secure Update of Platform will provide protection against installation and execution of unauthorized software by checking the integrity and authenticity of the i.MX RT700 own firmware, as well as the ones of other SoC processors, at each reset, as part of the secure boot. will provide protection against installation or update of unauthorized application software by checking the integrity and authenticity of the i.MX RT700 application before installation or update. Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) and Software Attacker Resistance: Isolation of Platform Parts will provide isolation of the i.MX RT700 internals against remote and local logical attacks that could be led from malicious code loaded into the rest of SoC. Note also that i.MX RT700 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 will provide integrity and authenticity verification of the i.MX RT700 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 will provide, on demand, the attestation of the state of the i.MX RT700 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 will provide protections of cryptographic services involved in secure communication integrity and authenticity enforcement against physical attacks. provides monitoring and detection of physical attacks during operation.
CR 3.4 – Software and information integrity	Secure Initialization of Platform will provide, as part of the secure boot, integrity and authenticity checks of the firmware, software and configuration data of i.MX RT700 and/or other SoC processors before any execution.

Table 14. IEC 60601-4-5 security requirements support by i.MX RT700*...continued*

60601-4-5 requirements	i.MX RT700 supports
CR 3.4(1) – Authenticity of software and information CR 3.4(2) – Automated notification of integrity violations	Attestation of Platform Genuineness will provide, on demand, the attestation of the genuineness of the i.MX RT700 subcomponent. Attestation of Platform State will provide, on demand, the attestation of the state of the i.MX RT700 subcomponent (including hashes of the firmware and patch, as well as life cycle state). Attestation of Application Genuineness will provide, on demand, the attestation of the genuineness of the application. Attestation of Application State will provide, on demand, the attestation of the state of the application. Secure Update of Platform will additionally check the version verification of the i.MX RT700 firmware/software to be launched. Physical Attacker Resistance will ensure the protection of code and data integrity during boot and at runtime against physical attacks. Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) and Software Attacker Resistance: Isolation of Platform Parts will ensure 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 Secure Development (see Security Process Packages (SPPs)) and the AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities ensure the proper validation of the syntax, length and content of input by design and by validation (code review and/or functional testing and/or penetration testing).
CR 3.6 – Deterministic output	will provide mechanisms ensuring deterministic behaviour. 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.MX RT700 part.
CR 3.7 – Error handling	The Secure Development (see Security Process Packages (SPPs)) and 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	will provide session management for secure communication. Cryptographic Random Number Generation, will provide random number that can be used to generate unique sessions identifiers. Cryptographic Operation, Cryptographic Operation (SoC) will provide cryptographic operations that can be used to protect integrity of session.
CR 3.9 – Protection of audit information	will provide protection of audit information. Physical Attacker Resistance , Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) and Software Attacker Resistance: Isolation of Platform Parts will provide protection of execution status of the i.MX RT700 security services against remote and local, logical and physical attacks. Secure Data Serialization will provide secure storage that can be used to protect audit information and logs from unauthorized access, modification and deletion.

Table 14. IEC 60601-4-5 security requirements support by i.MX RT700*...continued*

60601-4-5 requirements	i.MX RT700 supports
CR 3.10 - Support for updates CR 3.10(1) - Update authenticity and integrity	Secure Initialization of Platform and Secure Update of Platform will provide secure update of the i.MX RT700 firmware/software parts through the checking of the its integrity, authenticity and version as part of the secure boot. will provide secure update of the i.MX RT700 application through the checking of the its integrity, authenticity and version as part of the secure application update process.
CR 3.11 - Physical tamper resistance and detection CR 3.11(1) Notification of a tampering attempt	Physical Attacker Resistance will provide detection and reaction against physical attacks of the i.MX RT700; fault detections are notified into registers which can be read by the SoC for a notification at the component level. On detection of a physical attack i.MX RT700 will go into a secure state based on the programed reaction. will provide notification of tampering attempt.
CR 3.12 - Provisioning product supplier roots of trust	The i.MX RT700 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 Random Number Generation, Cryptographic Operation, Cryptographic Operation (SoC) and Cryptographic KeyStore, Physical Attacker Resistance will provide protection of product supplier root-of-trust keys and data against physical attacks. Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) and Software Attacker Resistance: Isolation of Platform Parts will provide protection of product supplier root-of-trust keys and data against remote and local logical attacks. See also Trust provisioning for Trust Provisioning.
CR 3.13 - Provisioning asset owner roots of trust	Cryptographic Key Generation, and Cryptographic Operation Cryptographic Operation (SoC) will provide cryptographic services that can be used for the provisioning of asset owner root-of-trust. Cryptographic KeyStore will provide 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 will provide protection of asset owner root-of-trust keys and data against physical attacks. Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) and Software Attacker Resistance: Isolation of Platform Parts will provide protection of asset owner root-of-trust keys and data against remote and local logical attacks. See also Trust provisioning for Trust Provisioning.
CR 3.14 - Integrity of boot process CR 3.14(1) - Authenticity of the boot process	Secure Initialization of Platform will provide, as part of the secure boot, integrity and authenticity checks of the firmware, software and configuration data of i.MX RT700 and other SoC processors before any execution. Physical Attacker Resistance will ensure the protection of code and data integrity during boot and at runtime against physical attacks. Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) and Software Attacker Resistance: Isolation of Platform Parts will ensure the protection of code and data integrity during boot and at runtime against remote and local logical attacks.
CR 4.1 - Information confidentiality	Secure Data Serialization and Cryptographic KeyStore will provide the capability to protect the information stored internally or in the external NVM and in transit when imported in the i.MX RT700 for use.

Table 14. IEC 60601-4-5 security requirements support by i.MX RT700*...continued*

60601-4-5 requirements	i.MX RT700 supports
CR 4.1 new RE(1) - health data de-identification	will provide the capability to protect the information in transit. Physical Attacker Resistance will provide confidentiality protection of the information against physical attacks when manipulated by the i.MX RT700 services. Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) and Software Attacker Resistance: Isolation of Platform Parts will provide confidentiality protection of the information against remote and local logical attacks when temporarily stored into the i.MX RT700 services. ***Residual Information Purging Residual Information Purging (SoC) Decommission of Platform will provide secure erasing of patient's stored health data when changing life-cycle state related to decommissioning or field return.***
CR 4.2 - Information persistence	Residual Information Purging Residual Information Purging (SoC) Decommission of Platform will provide secure erasing of sensitive data when changing life-cycle state related to decommissioning or field return. Cryptographic KeyStore will provide secure erasure of cryptographic material. Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) and Software Attacker Resistance: Isolation of Platform Parts will provide mediated access to information stored and manipulated inside the i.MX RT700 subcomponent avoiding having to share critical memory ressources.
CR 4.3 - Use of cryptography	Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation, Cryptographic Operation (SoC) and Cryptographic KeyStore, will 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	It is the component responsibility to properly implement network segmentation, zone boundary protection, and general-purpose person-to-person communication restrictions. will provide mechanisms ensuring network segmentation. ***Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation, Cryptographic Operation (SoC) and Cryptographic KeyStore, will provide cryptographic capbilities that can be used for configuration interface encryption.*** ***will provide secure communication for configuration interface.*** The component may use security services claimed by i.MX RT700 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 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.MX RT700 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.

Table 14. IEC 60601-4-5 security requirements support by i.MX RT700*...continued*

60601-4-5 requirements	i.MX RT700 supports
CR 6.1 – Audit log accessibility CR 6.1(1) - Programmatic access to audit logs	will provide programtic access to audit logs. Secure Data Serialization will provide secure storage in which the logs can be stored and accessed only to the authorized processor. Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation, Cryptographic Operation (SoC) and Cryptographic KeyStore, will 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.MX RT700 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. Attestation of Platform State will provide on demand, the attestation of the security state of the i.MX RT700 subcomponent (including hashes of the firmware and patch, as well as life cycle state). Attestation of Application State will provide, on demand, the attestation of the security state of the application. will provide log of the security relevent events.
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.MX RT700 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. will maintain essential functions of the i.MX RT700 when operating in a degraded mode.
CR 7.2 – Resource management	It is the component responsibility to properly implement ressource management. The component may use security services claimed by i.MX RT700 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. will ensure limit of use of ressources by security functions.
CR 7.3 – Control system backup CR 7.3(1) – Backup integrity verification CR 7.4 – Control system recovery and reconstitution	It is the component responsibility to properly implement backup and recovery. The component may use security services claimed by i.MX RT700 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. will ensure secure backup and backup integrity verification. Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation, Cryptographic Operation (SoC) and Cryptographic KeyStore, will provide cryptographic features that can be used to ensure confidentiality, integrity, and authenticity protection during backup and restore.
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.MX RT700 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. will provide mechanisms ensuring network and security configuration settings.

Table 14. IEC 60601-4-5 security requirements support by i.MX RT700*...continued*

60601-4-5 requirements	i.MX RT700 supports
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 Secure Developement (see Security Process Packages (SPPs) and 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.MX RT700 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.MX RT700 to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc. (e.g. CR1.2), however this is to be determined case by case. Verification of Platform Identity, will provide a unique and tamper-proof identification of the i.MX RT700 type and version, that can be used for precise identification of the final component (by including subcomponent identification). Verification of Platform Instance Identity, will provide a unique and tamper-proof identity of each i.MX RT700 instance, that can be used for precise identification of the final component (by including subcomponent identification).

5.2 NIST 8425 support

The mapping below shows how the platform under evaluation (i.MX RT700, a Subcomponent of the IoT Device as defined in the NIST 8425 [20]) supports the final IoT Device (a Component of the IoT Product as defined in the NIST 8425 [20]), demonstrating compliance with the NIST 8425 security requirements. It describes which part of each NIST 8425 requirement is implemented at the i.MX RT700 level. Then, this is the responsibility of the IoT Device to use the i.MX RT700 security features to implement the final requirement.

This mapping is compliant with GlobalPlatform SESIP to NIST IR 8425 mapping GPS_NOT_025 [21].

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 15. NIST 8425 security requirements support by i.MX RT700

NIST 8425 requirements	i.MX RT700 supports
Asset Identification	
1. The IoT product can be uniquely identified by the customer and other authorized entities (e.g., the IoT product developer).	Attestation of Application Genuineness will provide an attestation of the IoT Device Application identity and authenticity. Attestation of Platform Genuineness will provide an attestation of the Plateform identity and authenticity that can be used by the IoT Device for attesting its identity and authenticity. Verification of Platform Identity will provide model designation and version of the Platform that can be used by the IoT Device for its identification.
2. The IoT product uniquely identifies each IoT product component and maintains an up-to- date inventory of connected product components.	

Table 15. NIST 8425 security requirements support by i.MX RT700*...continued*

NIST 8425 requirements	i.MX RT700 supports
	Verification of Platform Instance Identity will provide unique identifier of the Platform instance that can be used by the IoT Device for its identification.
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.	Secure Update of Platform will provide secure update capabilities of the platform that can be used by the IoT Product Component for field upgrade and/or configuration change. Cryptographic Keystore will provide cryptographic configuration (crypto assets management) capabilities of the Platform that can be used by the IoT Device to change its cryptographic configuration. Field Return of Platform will provide security configuration change and critical assets erasure capabilities of the Platform when the IoT Device changes its life cycle to FIELD RETURN. Most security services claimed in Section 3.2 offer configuration capabilities to a certain degree. See the security servoices claims for more details.
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.	Residual Information Purging Residual Information Purging (SoC) will provide erasure of critical assets on demand that can be used by the IoT Device Application software to restore the IoT Device into a secure default (i.e. uninitialized) configuration.
3. The IoT product applies configuration settings to applicable IoT components.	The configuration of other IoT Components, as part of an IoT product, shall be implemented by the operating system or application code of the IoT Device.
Data Protection	
1. Each IoT product component protects data it stores via secure means	Cryptographic Keystore will provide cryptographic key storage service of the Platform that can be used by the IoT Device to securely store cryptographic keys. Physical Attacker Resistance will provide detection and prevention of physical attacks on the Platform for protection of the IoT Device data. Secure Data Serialization will provide secure storage outside the Platform that can be used by the IoT Device to securely store cryptographic keys Secure Debugging will provide authenticated test mode entry of the Platform (with data erasure on test mode entry) for protection of the IoT Device data. Secure Initialization of the Platform will ensure that data is secured during intialization operations. Secure Update of Platform will ensure that data is secured during update of the Platform firmware. Software Attacker Resistance: Isolation of Platform (Between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (Between PSA ROT and Application Root of Trust Services) will provide isolation of the Platform's security services from the IoT Device Applicative domain. Software Attacker Resistance: Isolation of Platform Parts will provide isolation of the Platform's most sensitive

Table 15. NIST 8425 security requirements support by i.MX RT700*...continued*

NIST 8425 requirements	i.MX RT700 supports
	security services from other domains of the Platform and from the IoT Device Applicative domain. Verification of Platform Identity Verification of Platform Instance Identity will ensure that the model designation, the version, and unique identifier of the Platform (that can be used by the IoT Device for its identification) are protected (temper-proof). Security Target Requirements and Guidance Documentation Requirements will ensure that Security Objectives for the Operational Environment are defined in the Security Target and that Guidance is provided to secure data protection. The ASE (Security Target) and AGD (Guidance) SESIP evaluation activities (see [1]) verify that the Security Target and the Guidance Documentation of the Platform are compliant with the requirements.
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.	The Platform itself does not collect and store data collected from or about the customer, but provide services for such data storage and deletion. Decommission of Platform will ensure that the Platform can be moved to its end-of-life state with no possible way back to operational state and destruction of all data (including user data) when the IoT Device triggers end of life mode. Field Return of Platform will ensure deletion of user data stored by the Platform when the IoT Device trigers the field return mode. Residual Information Purging Residual Information Purging (SoC) will ensure deletion of selected data from the Platform on request of the IoT Device Application.
3. When data are sent between IoT product components or outside the product, protections are used for the data transmission.	Cryptographic Operation Cryptographic Operation (SoC) Cryptographic Key Generation Cryptographic Random Number Generation Cryptographic Keystore will provide cryptographic services of the Platform that can be used by the IoT Product Component for data protection during transmission.
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 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.	The design of final IoT Device, as part of an IoT product, including the physical interface exposure and its usability, is by the platform integrator. Secure Debugging will provide protected (by disablement or authentication) test interface of the Platform that can be leveraged by the IoT Device.
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).	Cryptographic Operation Cryptographic Operation (SoC) Cryptographic Key Generation Cryptographic Random Number Generation Cryptographic Keystore will provide cryptographic services of the Platform that can be used by the IoT Device for interface access control.

Table 15. NIST 8425 security requirements support by i.MX RT700*...continued*

NIST 8425 requirements	i.MX RT700 supports
	Secure Debugging will provide protected (by disablement or authentication) test interface of the Platform that can be leveraged by the IoT Device.
c. For all interfaces, access and modification privileges are limited.	Software Attacker Resistance: Isolation of Platform (Between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (Between PSA ROT and Application Root of Trust Services) will support IoT Device provileges management by protecting against illegal Application domain access to Platform ressources. Software Attacker Resistance: Isolation of Platform Parts will support IoT Device provileges management by protecting against illegal access between Platform domains.
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.	The Development Requirements, Test Requirements, and Vulnerability Assessment Requirements that the interfaces provided at Platform level are restricted to only the necessary functions and privileges, and that there is no unnecessary privilege, interface and/or code remaining. The ADV (development), ATE (functional testing) and AVA (vulnerability analysis) SESIP evaluation activities (see [1]) verify that the Development, the Independent Testing, and the resistance of the Platform are compliant with the requirements.
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.	Secure Initialization of the Platform will ensure start up of the Platform and IoT Device to maintain appropriate access control during initial connection or reconnection after disconnection or outage. Secure Recovery will ensures recovery service of the Platform that can be used by the IoT Device to maintain appropriate access control during initial connection or reconnection after disconnection or outage.
Software Update	
1. Each IoT product component can receive, verify, and apply verified software updates.	Attestation of Application Genuineness will provide an attestation of the IoT Device Application identity and authenticity. Attestation of Application State will provide an attestation of the Application state that can be used by the IoT Device for attesting its security state. Attestation of Platform Genuineness will provide an attestation of the Plateform identity and authenticity that can be used by the IoT Device for attesting its identity and authenticity. Attestation of Platform State will provide an attestation of the Plateform state that can be used by the IoT Device for attesting its security state. Physical Attacker Resistance will ensure that the Platform detects or prevents physical attacks and

Table 15. NIST 8425 security requirements support by i.MX RT700*...continued*

NIST 8425 requirements	i.MX RT700 supports
	reacts by itself or let the IoT Device choose the most appropriate action, with secure handling of audit logs. Software Attacker Resistance: Isolation of Platform (Between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (Between PSA ROT and Application Root of Trust Services) will support IoT Device provileges management by protecting against illegal Application domain access to Platform ressources. Software Attacker Resistance: Isolation of Platform Parts will support IoT Device provileges management by protecting against illegal access between Platform domains.
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).	The software update development, distribution and customer notification are expected to be managed by platform integrator and/or the network service providers. The Development Requirements, Guidance Documents Requirements, and Life-cycle Support Requirements (ALC_FLR.2 Flaw Reporting Procedure) ensure that the Platform implements measures to keep software up to date that can be used by the IoT Device Application. The ADV (Development), AGD (Guidance) and ALC_FLR.2 (Flaw Reporting Procedure) SESIP evaluation activities (see [1]) verify that the Development, Guidance Documentation, and Flaw Reporting Procedure of the Platform are compliant with the requirements. Secure Update of Platform will ensure that the software of the Platform can be updated securely using the Platform secure update mechanism
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 Application Genuineness will provide an attestation of the IoT Device Application identity and authenticity. Attestation of Application State will provide an attestation of the Application state that can be used by the IoT Device for attesting its security state. Attestation of Platform Genuineness will provide an attestation of the Plateform identity and authenticity that can be used by the IoT Device for attesting its identity and authenticity. Attestation of Platform State will provide an attestation of the Plateform state that can be used by the IoT Device for attesting its security state. Physical Attacker Resistance will ensure that the Platfrom detect or prevents physical attacks by reacting

Table 15. NIST 8425 security requirements support by i.MX RT700*...continued*

NIST 8425 requirements	i.MX RT700 supports
	itslef or leting the IoT Product Component choose the most appropriate action, and by securely handling the audit logs. Software Attacker Resistance: Isolation of Platform (Between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (Between PSA ROT and Application Root of Trust Services) will ensure that the Platform detects or prevents attempts of privilage violation and reacts by itslef or let the IoT Device choose the most appropriate action, with secure handling of audit logs. Software Attacker Resistance: Isolation of Platform Parts will ensure that the Platform detects or prevents attempts of privilage violation and reacts by itslef or let the IoT Product Component choose the most appropriate action, with secure handling of audit logs. The Guidance Documents Requirements ensure that the error messages sent back from the Platform to the IoT Device Application are described. The AGD (Guidance) SESIP evaluation activities (see [1]) verify that the Guidance Documents of the Platform are compliant with the requirements.
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.	This requirement primarily address the platform integrators and/or the network service providers. NXP creates and stores documents related to the Platform cybersecurity all along its development according to the Security Target Requirements, Development Requirements, Guidance Documents Requirements, Tests Requirements, Life-cycle Requirements, Vulnerability Assessment Requirements. The ASE (Security Tager), ADV (development), AGD (Guidance), ATE (functional testing), ALC (Life-cycle) and AVA (Vulnerability Assessment) SESIP evaluation activities (see [1]) verify that the documentation of the Platform is compliant with the requirements.
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 platform integrators and/or the network service providers. In compliance with the Life Cycle Requirements, NXP provides a flaw reporting procedure for its products. ALC_FLR.2 (Flaw Reporting Procedure) SESIP evaluation activities (see [1]) verify that the Flaw Reporting Procedure is compliant with the requirements.
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 platform integrators and/or the network service providers. In compliance with the Life Cycle Requirements, NXP provides a flaw reporting procedure for its products. ALC_FLR.2 (Flaw Reporting Procedure) SESIP evaluation activities (see [1]) verify that the flaw

Table 15. NIST 8425 security requirements support by i.MX RT700*...continued*

NIST 8425 requirements	i.MX RT700 supports
	remediation procedure is compliant with the requirements.
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 address the platform integrators and/or the network service providers. In compliance with the Guidance Documentation Requirements, NXP provides Guidance Documents for its products. The AGD (Guidance Documents) SESIP evaluation activities (see [1]) verify that the Guidance Documents are compliant with the requirements.

5.3 ETSI EN 303645 support

ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements [16] 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 [17]. 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 [16].

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.MX RT700 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 16. ETSI EN 303645 security requirements support by i.MX RT700

ETSI EN 303645 requirements	i.MX RT700 supports
5.1-1 Unique device password	Password feature shall be implemented by the operating system or application code. Yet, a default or other easy to manipulate password at i.MX RT700 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.

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

Table 16. ETSI EN 303645 security requirements support by i.MX RT700*...continued*

ETSI EN 303645 requirements	i.MX RT700 supports
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, Cryptographic Operation (PKC) 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.MX RT700 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.MX RT700 firmware image (including application software) 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.MX RT700 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.MX RT700 firmware image (including application software), 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.MX RT700 to the evaluator for assessment (and to the OEM), and by providing the corresponding tool chain for ease of use by the OEM.
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 Operation (PKC), Cryptographic Key Generation, Cryptographic Key Store, and Cryptographic Random Number Generation implement the secure update of the i.MX RT700 firmware image (including the application software), 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.

Table 16. ETSI EN 303645 security requirements support by i.MX RT700*...continued*

ETSI EN 303645 requirements	i.MX RT700 supports
	The ALC_FLR.2 (Flaw Reporting Procedure) SESIP evaluation activity (see also [1]) supports the requirement for the i.MX RT700 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 Operation (PKC), Cryptographic Key Generation, Cryptographic Key Store, and Cryptographic Random Number Generation implement the secure update of the i.MX RT700 firmware image (including the application software), 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.MX RT700 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. NXP provides Product Longevity program where the i.MX RT700 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.MX RT700 (including firmware). The SESIP methodology (see also [1]) mandates unique identification of the platform under evaluation; conformance rational is provided.
5.4-1 Security parameter storage	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform Parts, and Secure Data Serialization 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 (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), 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.MX RT700

Table 16. ETSI EN 303645 security requirements support by i.MX RT700*...continued*

ETSI EN 303645 requirements	i.MX RT700 supports
	provides extra attacker resistance including software isolarion and physical attacker resistance.
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 Operation (PKC), 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 Operation (PKC), 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 Operation (PKC), 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 Operation (PKC), 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	
5.5-8 Secure management process	The secure management process for OEM provisioned security parameters is owned by OEM. Cryptographic Key Generation, Cryptographic Operation , Cryptographic Operation (PKC) 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.

Table 16. ETSI EN 303645 security requirements support by i.MX RT700*...continued*

ETSI EN 303645 requirements	i.MX RT700 supports
	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.MX RT700 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.MX RT700 can be disabled. i.MX RT700 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 (between SPE and NSPE) , Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application ROot of Trust) , Software Attacker Resistance: Isolation of Platform parts and Secure External Storage provide isolation of the ELE-CP (S50) subcomponent ressources and of the memory allowing (in conjonction with other hardware based mechanisms 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.MX RT700 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 the 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 Operation (PKC), 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	
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.
5.9-2 Local function with loss of network	

Table 16. ETSI EN 303645 security requirements support by i.MX RT700*...continued*

ETSI EN 303645 requirements	i.MX RT700 supports
5.9-3 Orderly reconnection	Secure Initialization of the Platform and Attestation of Platform State provide secure initialization and attestation features which can support to fulfil the provision requirements.
5.10-1 Telemetry data examination	The use case and feature shall be defined by OEM of the final product. Secure Initialization of the 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 the 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	

5.4 CRA Essential Cybersecurity Requirements support

The table below shows how the platform under evaluation (i.MX RT700 described in this Security Target) supports the final product, demonstrating compliance with Regulation (EU) 2024/2847 Annex I (see [18]).It describes which part of each Essential Cybersecurity Requirment (ECR) are implemented at the platform level. Then, this is the responsibility of the final product software (the OEM application) to use the platform security features to implement the complete ECR at final product level. The rationale in the table uses SESIP language: the "platform" in the rationale is to be understood as "the certified security functionalities of the digital element".

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 (EU) 2024/2847 regulation.

Table 17. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT700

Requireme ID	Requirement from CRA	i.MX RT700 supports
1(1)	Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;	The set of security requirements included in this Security Target (see Section 3.2) has been identified from a generic risks assessment done by the chip manufacturer community inside the Protection Profile(s) referenced in Section 1.2. Based on NXP-wide Business Creation and Management (BCaM) development framework and the Security Maturity Process (SMP) applicable for security products, different context of risks have been considered and are described in Section 1.6.7 for which the appropriate assurance level has been determined and described in Section 4. The AVA_VAN SESIP security evaluation activity requires a security vulnerability analysis of the implementation and testing on the final product ensuring an adequate level of security of the platform with regards to the claimed use case and assurance level.
1(2)	On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:	
	(a) be made available on the market without known exploitable vulnerabilities;	The NXP BCaM development framework and SMP process enforce secure by default development, secure implementation rules, design reviews and extensive validation testing before mass production of the platform, minimizing the risc of exploitable vulnerability remaining in the platform. The AVA_VAN SESIP security evaluation activity includes verification that no known exploitable vulnerabilities in the platform exist, or that any such vulnerability can be covered by the upper layer based on security guidelines for the integrator. The AGD_PRE and AGD_OPE SESIP security evaluation activity assesses the existance and sufficiency of the security guidance for the integrator to ensure the secure preparation and use of the platform.
	(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;	The AGD_PRE and AGD_OPE SESIP security evaluation activity assesses the existance and sufficiency of the security guidelines for the integrator to ensure the secure configuration of the platform after integration and to be put in the field. The AVA_VAN SESIP security evaluation activity includes verification of the platform implementation related to the secure configuration. Residual Information Purging Residual Information Purging (SoC) will ensure that sensitive data can be erased on demand and that critical information is systematically erased from memory on memory dealocation.
	(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification	Secure Update of Platform will ensure that the platform loadable software can be securely updated after deployment. ALC_FLR.2 evaluation activity ensures the existence of a process for the handling of security incidents, including

Table 17. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT700*...continued*

Requireme ID	Requirement from CRA	i.MX RT700 supports
	of available updates to users, and the option to temporarily postpone them;	the efficient development, deployment, and distributions of updates. Note: 1. The automaticity and user opt-out mechanism is not covered at the platform level and must be handled at the upper sofware layer where applicable. 2. There is the possibility for the developer to claim no security update by providing a rationale that is assessed to be acceptable.
	(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access	Software Attacker Resistance: Isolation of Platform (Between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (Between PSA ROT and Application Root of Trust Services) Software Attacker Resistance: Isolation of Platform Parts will protect against unauthorized acces to sensitive data and services by specifying an isolated security domain and by specifying segmentation of memory arrays and peripherals into Secure or Non-Secure areas. Physical Attacker Resistance will protect against aunauthorized acces via physical attacks. Any other access control mechanism is to be implemented by the upper software layer. All those SFRs will return execution status (via the corresponding APIs) or generate an alarm (in case of anomaly) that can be recorded by the integrator software in an audit log to report possible unauthorized access.
	(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;	Secure Initialization of Platform will ensure the integrity, authenticity (and confidentiality) of the platform configuration and loadable software at boot, and the security of all other SFRs implementation including the related protections for data confidentiality and integrity. Secure Update of Platform will ensure the integrity, authenticity (and confidentiality) of platform loadable software during update. Software Attacker Resistance: Isolation of Platform (Between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (Between PSA ROT and Application Root of Trust Services) Software Attacker Resistance: Isolation of Platform Parts will protect the confidentiality of data stored or manipulated inside the isolated security domain and secure area against logical attacks from the non-security domain and non-secure area. Secure Data Serialization will ensure that sensitive data stored outside the platform is protected with confidentiality, integrity, authenticity and binding to the platform instance. Cryptographic KeyStore will ensure confidentiality, integrity and binding to the platform instance of cryptogrphic sensitive material stored inside the platform or in external NVM. Cryptographic Operation Cryptographic Operation (SoC) will provide the integrator software with cryptographic services that can be used to encrypt relevant data at rest or in transit

Table 17. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT700*...continued*

Requireme ID	Requirement from CRA	i.MX RT700 supports
		Physical Attacker Resistance will protect the confidentiality of data stored or manipulated inside the platform against physical attacks.
	(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;	Secure Initialization of Platform will ensure that integrity, authenticity and confidentiality of the platform configuration and loadable software are maintained during the secure boot process. Secure Update of Platform will ensure that the platform loadable software can be securely updated after deployment such that Authenticity, Integrity and Confidentiality is maintained. Software Attacker Resistance: Isolation of Platform (Between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (Between PSA ROT and Application Root of Trust Services) Software Attacker Resistance: Isolation of Platform Parts will protect the integrity of data stored or manipulated inside the platform against logical attacks. Secure Data Serialization will ensure that sensitive data stored outside the platform is protected with confidentiality, integrity, authenticity and binding to the platform instance. Cryptographic KeyStore will ensure confidentiality, integrity and binding to the platform instance of cryptogrphic sensitive material stored inside the platform or in external NVM. Cryptographic Operation Cryptographic Operation (SoC) will provide cryptographic services that can be used to encrypt relevant data at rest or in transit Physical Attacker Resistance will protect the integrity of data stored or manipulated inside the product against physical attacks. All those SFRs will return execution status (via the corresponding APIs) or generate an alarm (in case of anomaly) that can be included in an audit log to report corruption.
	(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);	AVA_VAN: this SESIP security evaluation activity requires a security vulnerability analysis of the implementation which includes the verification of minimisation of data
	(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;	AVA_VAN: this SESIP security evaluation activity requires a security vulnerability analysis of the implementation which includes the verification that essential and basic functions remains available and that no known exploitable vulnerabilities are part of the implementation. The AGD_PRE and AGD_OPE SESIP security evaluation activity assesses the existance and sufficiency of the security guidelines for the integrator, to ensure the secure configuration of the platform and protect the availability of essential and basic functions. Secure Initialization of Platform Secure Update of Platform will ensure the integrity of the platform loadable software

Table 17. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT700*...continued*

Requireme ID	Requirement from CRA	i.MX RT700 supports
		and therefore the availability of the essential and basic functions at startup. Software Attacker Resistance: Isolation of Platform (Between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (Between PSA ROT and Application Root of Trust Services) Software Attacker Resistance: Isolation of Platform Parts will ensure the availabiliy of essential security processes from external nonessential applications or from other processes by offering an isolated security domain and secure area. Physical Attacker Resistance will protect the availability of essential and basic functions against physical attacks.
	(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;	AVA_VAN: this SESIP security evaluation activity requires a security vulnerability analysis of the implementation which includes the verification that impact of the device on the availability of services provided by other devices or services will be minimal and that no such known exploitable vulnerabilities are part of the implementation. The AGD_PRE and AGD_OPE SESIP security evaluation activity assesses the existance and sufficiency of the security guidelines for the integrator, to ensure the secure configuration of the platform and minimze the impact of the product. Verification of Platform Identity Verification of Platform Instance Identity will ensure the secure and unique identification of the platform to other devices or networks, allowing those to determine the expected behavior of the platform. Attestation of Platform Genuineness will ensure that the platform can attest about its identity on demand. Attestation of Application Genuineness will ensure that the application can attest about its identity and its security state on demand. Secure Initialization of Platform will ensure the integrity and authenticity of the platform loadable software at boot and therefore prevent its inappropriate use against other devices or network. Secure Update of Platform ensure the integrity and authenticity of the platform loadable software when updated and therefore prevent its inappropriate use against other devices or network. Software Attacker Resistance: Isolation of Platform (Between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (Between PSA ROT and Application Root of Trust Services) Software Attacker Resistance: Isolation of Platform Parts will ensure the availabiliy of essential security processes from external nonessential applications or from other processes by offering an isolated security domain and secure area. Physical Attacker Resistance will protect the availability of essential and basic functions against physical attacks.

Table 17. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT700*...continued*

Requireme ID	Requirement from CRA	i.MX RT700 supports
	(j) be designed, developed and produced to limit attack surfaces, including external interfaces;	AVA_VAN: the SESIP security evaluation activity requires a security vulnerability analysis of the implementation which includes the evaluation of the attack surface. Secure Debuging will disable debug interface when the platform is moved to the operational life cycle state.
	(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	The AVA_VAN SESIP security evaluation activity includes verification that the implementation ensures the security of the assets against attacks, including the appropriate mitigation mechanism and techniques. Software Attacker Resistance: Isolation of Platform (Between SPE and NSPE) Software Attacker Resistance: Isolation of Platform (Between PSA ROT and Application Root of Trust Services) will mitigate the impact of logical attacks or incidents happening in the nonsecure world by offering an isolated security domain and secure area. Software Attacker Resistance: Isolation of Platform Parts will mitigate the impact of logical attacks or incidents happening in subparts of the platform by offering isolation and segmentation between subparts of the platform. Physical Attacker Resistance will mitigate the impact of physical attacks or incidents by offering detection and reaction to physical attack.
	(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;	Security services claimed in Section 3 will return execution status (via the corresponding APIs) or generate an alarm (in case of anomaly) that can be monitored and recorded by the upper software layer to integrate into the reporting to the user.
	(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	Residual Information Purging Residual Information Purging (SoC) will ensure the correct and robust implementation of a secure erasing service of user data settings.
2(1)	Manufacturers of the products with digital elements shall identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;	The outputs of the platform SESIP evaluation can be reused and integrated to the software bill of material of the final product.
2(2)	Manufacturers of the products with digital elements shall in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;	Secure Update of Platform will ensure that the platform loadable software can be updated with verified integrity and authanticity. ALC_FLR: this SESIP evaluation activity assesses that the element under evaluation implements a process of flaw remediation allowing the monitoring, the reporting and the correction of security issues which could be found in the field, and which would trigger the use of the secure update mechanism to mitigate the security issue (see Section 3.1.1.

Table 17. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT700*...continued*

Requireme ID	Requirement from CRA	i.MX RT700 supports
2(3)	Manufacturers of the products with digital elements shall apply effective and regular tests and reviews of the security of the product with digital elements;	All SESIP evaluations requires the performance of a full vulnerability analysis (AVA_VAN) of the components integrated into the final product; the evaluation outputs are reusable by any security review at the final product level.
2(4)	Manufacturers of the products with digital elements shall once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;	All SESIP security evaluations require that the element under evaluation implement a flaw remediation process (assessed by ALC_FLR evaluation activity, see Section 3.1.1). The NXP Product Security Incident Response Team (PSIRT) is in charge of collecting reported vulnerabilities or documentation flaws via a dedicated portal, coordinating responsible vulnerability disclosure, evaluating the soundness and impact of the reported vulnerability or flaw, communicating with affected customers about the impact/severity/mitigation, triggering the technical teams in charge of developing a solution to mitigate the reported vulnerability or in charge or correcting the documentation flaw, and organizing the distribution of firmware update or documentation update. This is to be used by the final product manufacturer to put in place and enforce a policy on coordinated vulnerability disclosure, to facilitate the sharing of information about potential vulnerabilities and ensure the final distribution of security patches and/or updates to end users.
2(5)	Manufacturers of the products with digital elements shall put in place and enforce a policy on coordinated vulnerability disclosure;	
2(6)	Manufacturers of the products with digital elements shall take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	
2(7)	Manufacturers of the products with digital elements shall provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;	
2(8)	Manufacturers of the products with digital elements shall ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	

5.5 EN 18031 (RED) support

The table below shows how the platform under evaluation, i.MX RT700, described in this Security Target supports the RED compliance ([22]); it describes which part of each RED requirements are implemented at the

i.MX RT700 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 RED standard.

Table 18. RED security requirements support by i.MX RT700

RED requirements	Description	RED Article d: network assets e: privacy assets f: financial assets	Supported by i.MX RT700 and assessed by SESIP
ACM-1	Applicability of access control mechanisms	d/e/f	Cryptographic Operation Cryptographic Operation (PKC) Cryptographic Key Generation Cryptographic Keystore Cryptographic Random Number Generation : those SESIP security claims assess the implementation of secure cryptographic services, which ones can be used by the equipment to implement an access control mechanism. An explicit refinement of the requirement can require the validation of authenticator, the ability to change the authenticator, the preventing of static and default values. Protection against brute force and other cryptographic attack is part of the SESIP vulnerability analysis (AVA_VAN.SESIP) evaluation activity.
ACM-2	Appropriate access control mechanisms	d/e/f	Same as above
ACM-3	Default access control for children in toys	e	Same as above
ACM-4	Default access control to children's privacy assets for toys and childcare equipment	e	Same as above
ACM-5	Parental/Guardian access controls for children in toys	e	Same as above
ACM-6	Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys	e	Same as above
AUM-1	Applicability of authentication mechanisms	d/e/f	Same as above
AUM-2	Appropriate authentication mechanisms	d/e/f	Same as above
AUM-3	Authenticator validation	d/e/f	Same as above
AUM-4	Changing authenticators	d/e/f	Same as above
AUM-5	Password strength	d/e/f	Same as above
AUM-6	Brute force protection	d/e/f	Same as above
SUM-1	Applicability of update mechanisms	d/e/f	Secure Update of Platform : this SESIP security claims assess the implementation of a secure update mechanism of the mutable part of the equipment

Table 18. RED security requirements support by i.MX RT700*...continued*

RED requirements	Description	RED Article d: network assets e: privacy assets f: financial assets	Supported by i.MX RT700 and assessed by SESIP
			element under evaluation, including the integrity and authenticity verification of the image to be installed/ loaded. ALC_FLR: this SESIP evaluation activity assesses that for the equipment element under evaluation a process of flaw remediation is in place to allow the monitoring, the reporting and the correction of security issues which could be found in the field, and which would trigger the use of the secure update mechanism to mitigate the security issue.
SUM-2	Secure updates	d/e/f	Same as above
SUM-3	Automated updates	d/e/f	Same as above
SSM-1	Applicability of secure storage mechanisms	d/e/f	Secure Data Serialization : those SESIP security claims assess the implementation of secure storage mechanisms, including authenticity, integrity and/or confidentiality protections depending on the related stored assets protection needed.
SSM-2	Appropriate integrity protection for secure storage mechanisms	d/e/f	Same as above
SSM-3	Appropriate confidentiality protection for secure storage mechanisms	d/e/f	Same as above
SCM-1	Applicability of secure communication mechanisms	d/e/f	
SCM-2	Appropriate integrity and authenticity protection for secure communication mechanisms	d/e/f	Same as above
SCM-3	Appropriate confidentiality protection for secure communication mechanisms	d/e/f	Same as above
SCM-4	Appropriate replay protection for secure communication mechanisms	d/e/f	Same as above
LGM-1	Applicability of logging mechanisms	e/f	All those SFRs will return execution status (via the corresponding APIs) or generate an alarm (in case of anomaly) that can be included in an audit log to report corruption.
LGM-2	Persistent storage of log data	e/f	Same as above
LGM-3	Minimum number of persistently stored events	e/f	Same as above
LGM-4	Time-related information of persistently stored log data	e/f	Same as above

Table 18. RED security requirements support by i.MX RT700*...continued*

RED requirements	Description	RED Article d: network assets e: privacy assets f: financial assets	Supported by i.MX RT700 and assessed by SESIP
DLM-1	Applicability of deletion mechanisms	e	Descommission of Platform Field Return of Platform : those SESIP security claims assess that user data is securely erased before some life cycle change which could involve ownership reset or change. Residual Information Purging Residual Information Purging (SoC) : this SESIP security claim assesses the implementation of a secure erasing mechanism or user data handled by the equipment element which can be triggered upon need by the equipment upper layers.
RLM-1	Applicability and appropriateness of resilience mechanisms	d	
NMM-1	Applicability and appropriateness of network monitoring mechanisms	d	Cryptographic Operation Cryptographic Operation (SoC) Cryptographic Key Generation Cryptographic Keystore Cryptographic Random Number Generation : those SESIP security claims assess the implementation of secure cryptographic services, which ones could be needed by the equipment to support or implement a network monitoring mechanism.
TCM-1	Applicabilityand appropriateness of traffic control mechanisms	d	Cryptographic Operation Cryptographic Operation (SoC) Cryptographic Key Generation Cryptographic Keystore Cryptographic Random Number Generation : those SESIP security claims assess the implementation of secure cryptographic services, which ones could be needed by the equipment to support or implement a traffic control mechanism.
UNM-1	Applicability of user notification mechanisms	e	
UNM-2	Appropriate user notification content	e	
CKK-1	Appropriate CCKs	d/e/f	All SESIP security services claim involving cryptographic keys (cryptographic services, secure initialization, secure update, secure communication, secure storage, etc.) are assessed to verify that those keys are securely handled and adhere to best practice cryptography. Explicit refinement of such security services claim can require that no hard-coded values nor static defaults values are used for confidential cryptographic keys.
CCK-2	CCK generation mechanisms	d/e/f	Same as above
CCK-3	Preventing static default values for preinstalled CCKs	d/e/f	Same as above

Table 18. RED security requirements support by i.MX RT700*...continued*

RED requirements	Description	RED Article d: network assets e: privacy assets f: financial assets	Supported by i.MX RT700 and assessed by SESIP
GEC-1	Up-to-date software and hardware with no publicly known exploitable vulnerabilities	d/e/f	AVA_VAN.SESIP: this SESIP security evaluation activity requires the vulnerability analysis of the claimed security services implementation, during which: • it is verified that the implementation under evaluation does not include publicly known exploitable vulnerabilities and that only needed interfaces are exposed for each life-cycle state. • it is checked that necessary input validation are performed. AGD_OPE/PRE: these SESIP security evaluation activities require the documentation of security services exposed to the users.
GEC-2	Limit exposure of services via related network interfaces	d/e/f	Same as above
GEC-3	Configuration of optional services and the related exposed network interfaces	d/e/f	Same as above
GEC-4	Documentation of exposed network interfaces and exposed services via network interfaces	d/e/f	Same as above
GEC-5	No unnecessary external interfaces	d/e/f	Same as above
GEC-6	Input validation	d/e/f	Same as above
GEC-7	Documentation of external sensing capabilities	e	Same as above
GEC-8	Equipment Integrity	f	Same as above
CRY-1	Best practice Cryptography	d/e/f	All SESIP security services claim assessment involving cryptographic keys (cryptographic services, secure initialization, secure update, secure communication, secure storage, etc.) verify that those keys are securely handled and adhere to best practice cryptography

6 Bibliography

6.1 Evaluation Documents

[1] GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2, GP_FST_070.
[2] Security Evaluation Standard for IoT Platforms (SESIP), CEN, EN 17927:2023.
[3] GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs, Version 1.1, GPT_SPE_150.
[4] SESIP Profile for PSA Certified Level 3, Version 1.0, GPS_SPE_111, November 2025, PSA JSA.

6.2 Developer Documents

[5] i.MX RT700 Crossover Microcontrollers Reference Manual, Rev. 5, Date 2025-10-31, NXP Semiconductors.
[6] i.MX RT700 Security Reference Manual, Rev. 5.1, Date 2026-06-04, NXP Semiconductors.
[7] i.MX RT700 Crossover Microcontroller Data Sheet, Rev. 6, Date 2025-10-30, NXP Semiconductors.
[8] AN14825 Secure Debug on i.MX RT700, Rev. 1.0, Date 2025-11-10, NXP Semiconductors
[9] AN14821 Secure Boot on i.MX RT700, Rev. 1.0, Date 2025-11-10, NXP Semiconductors
[10] MCUXpresso SDK for i.MX RT700-EVK with ELE-CP (S50) FW , SDK_25.12.00_MIMXRT700-EVK (RFP 2.0 B0), NXP Semiconductors
[11] User Manual of Crypto Library Normal Secure (CLNS), components\els_pkc\doc folder of SDK_25.12.00_MIMXRT700-EVK (RFP 2.0 B0), NXP Semiconductors.
[12] Secure Provisioning SDK (SPSDK) Application User Guides, Rev. 2facbebd, NXP Semiconductors, https://spsdk.readthedocs.io/
[13] AN6497, Selecting and using cryptographic algorithms and protocols, Rev 1.2, NXP Semiconductors, April 2025.

6.3 Standards

[14] ARM Platform Security Architecture Firmware Framework 1.0, ARM Limited, DEN 0063 Issue number 0, June 2019.
[15] NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology, January 2012.
[16] ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI, v2.1.1, June 2020
[17] SESIP Applicablity for EN 303 645, White Paper, GlobalPlatform, January 2022
[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).
[19] IEC TR 60601-4-5, Medical electrical equipment - Part 4-5: Guidance and interpretation - Safety-related technical security specifications, edition 1.0, 2021-01, the International Electrotechnical Commission (IEC).
[20] NIST IR 8425 Profile of the IoT Core Baseline for Consumer IoT Products, September 2022, NIST.
[21] GlobalPlatform Technology SESIP to NIST IR 8425 mapping, version 1.0, GP_NOT_025.
[22] EN 18031 Common security requirements for radio equipment, August 2024, CEN EN.

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.

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

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at 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.

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

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.

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

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

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.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell 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