i.MX RT1180

SESIP Security Target

Rev. 1.3 — 11 December 2025 **Evaluation document**

Document information

Information	Content
Keywords	SESIP, IEC 62443, PSA, Security Target, i.MX RT1180, i.MX RT1181, i.MX RT1182, i.MX RT1186, i.MX RT1187, i.MX RT1189
Abstract	Security target for evaluation of the i.MX RT1180 developed and provided by NXP Semiconductors. The TOE targets compliance to SESIP Assurance Level 3 (SESIP3) with Limited Physical Attacker Resistance on the Secure Enclave, based on SESIP methodology version 1.2 , PSA Certified Level 3 . The Secure Enclave targets compliance to SESIP Assurance Level 3 (SESIP3) with Physical Attacker Resistance , PSA Certified Level 3 iSE/SE and RoT Component. Applicable IEC62443-4-2 requirements are mapped in to demonstrate IEC62443 compliance.

Revision History

Rev.	Date	Description
1.3	11 December 2025	First public release.

1 Introduction

This Security Target describes the i.MX RT1180 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 RT1180, SESIP Security Target, Revision 1.3, NXP Semiconductors, 11 December 2025.

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 1.0
Assurance Claim	Secure Enclave: SESIP Assurance Level 3 (SESIP3) Entire SoC: SESIP Assurance Level 3 (SESIP3)
Package Claim	Secure Enclave: Base SP, Package Secure Services, Package Software Isolation, Package Hardware Protection Entire SoC:Base SP, Package Secure Services, Package Software Isolation, Package Secure Enclave

See Section 1.5.7 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	This Profile applies to the Secure Enclave only: SESIP Assurance Level 3 (SESIP3)
Optional and Additional SFRs	See Section 4.5

Table 3. SESIP Profile for PSA Certified Level 3 iSE/SE and RoT Components Conformance Claims

Reference	Value
SP Name	SESIP Profile for PSA Certified Level 3 iSE/SE and RoT Component [5]
SP Version	Version 2.0 BETA
Assurance Claim	This Profile applies to the Secure Enclave only: SESIP Assurance Level 3 (SESIP3)
Optional and Additional SFRs	See Section 4.6

1.3 Platform Reference

i.MX RT1180

Table 4. Platform Reference

Reference	Value	
Platform Name and Version	See Table 6	
Platform Identification	Chip name and version	See IC hardware in Table 6
	PSA-RoT name and version	See updatable platform RoT in Table 6
Platform Type	See Section 1.5.2	
Trusted Subsystem Identification	See security enclave and its software in Table 6	

1.4 Included Guidance Documents

The following documents are included with the platform:

Table 5. Guidance Documents

Document	Reference
SESIP Security Target	i.MX RT1180, SESIP Security Target, Revision 1.3, NXP Semiconductors, 11 December 2025.
Reference Manual	i.MX RT1180 Reference Manual [6] i.MX RT1180 Reference Manual - Schneider Electric [7]
Sescurity Reference Manual	i.MX RT1180 Security Reference Manual [8] i.MX RT1180 Security Reference Manual - Schneider Electric [9]
Datasheets	Industrial [10] Schneider [11] Extended Industrial [12] Automotive [13]
ELE-AP API Reference Manual	UG10192 EdgeLock Secure Enclave i.MX RT1180 B0C0 User Guide (FW version v1.1.0 d5a78cba) [14]
Software Development Kit	MCUXpressor SDK for MIMXRT1180-EVK with ELE S401 FW v1.1.0 [16]
Secure Provisionning Tool User Guidance	Secure Provisioning SDK (SPSDK) Application User Guides [20]
Application notes	AN6259, Common Trust Provisioning Conceptional Overview [21]
Application notes	Application Notes, AN14227 Secure Boot on i.MX RT118x [17]
Application notes	Application Notes, AN14579 Secure Debug on ELE-AP based i.MX SoCs [18]
Application notes	Application Notes, AN13023 Selecting and using cryptographic algorithms and protocols [19]

1.4.1 Other Certification

i.MX RT1180 development process has followed Business Creation and Management (BCaM) framework and is subject to Product Security Incident Response Process (PSIRP). The latest NXP (BCaM and PSIRP) processes have been certified as compliant following IEC 62443-4-1, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements[24]. See more in Section 3.2.1.

Item	Content
Scheme	IEC 62443-4-1:2018 [24]
Certification body	TÜV SÜD Product Service GmbH

Item	Content
Certification number	No. IITS1 109577 0003 Rev. 00
Certification date	2021-12-10

The RNG IP implemented in i.MX RT1180 has also been CAVP validated accoridng to NISP SP 800-90A Hash-DRBG with SHA256 [22].

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

1.5 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 RT1180 crossover MCU family includes a Gb time sensitive networking (TSN) switch to enable real-time rich networking integration that handles both time-sensitive and industrial real-time communication. The i.MX RT1180 supports multiple protocols, bridging communications between real-time Ethernet and industry 4.0 systems. This family includes a state-of-the-art EdgeLock secure enclave, a dual core architecture with both an 800 MHz Cortex-M7 and a 240 MHz Cortex-M33 for ultimate design flexibility. The i.MX RT1180 is supported by an extensive developer ecosystem, featuring MCUXpresso software and tools, for an optimal microcontroller design experience.

1.5.1 Platform Security Features

The i.MX RT1180 security system includes following features:

- Advanced High Assurance Boot (AHAB) feature in the system boot
- EdgeLock Secure Enclave (Advanced Profile) (ELE-AP as hardware root of trust (RoT)
  - Microsoft Azure Sphere compliance
  - Symmetric Crypto Accelerators
  - Asymmetric Crypto Accelerators
  - Random number generator
  - One-Time Programmable electrical fuse used for security keys and configuration of other security related functions.
  - Physically Unclonable Function based master secrets as an option.
- On-the-fly decryption (FlexSPI OTFAD) of the encrypted application code or data stored in external flash device
- Battery Backed Secure/Non-Secure Module (BBSM/BBNSM) with security monitor, key storage, various tamper detections, monotonic counter, and real-time clock.
- Resource domain controller (TRDC) for complete peripheral & memory isolation.

1.5.2 Platform Type

Dual Core Crossover MCU with Time Sensitive Networking Switch and Integrated EdgeLock® Secure Enclave.

1.5.3 Platform Physical Scope

The physical scope is the i.MX RT1180 microcontroller silicon chip as shown in Figure 1.

The security functionalities are expressed through the SFRs listed in Section 3. Most SFRs are implemented by the Secure Enclave (see Figure 1) and are listed in Section 3.3. A few SFRs are implemented outside the Secure Enclave (i.e. by the rest of the SoC); those SFRs are explicitly identified as such by there naming ending by "(SoC)" and are provided in Section 3.4.

The hardware components and interfaces are listed in Chapter 2 of [6] / [7].

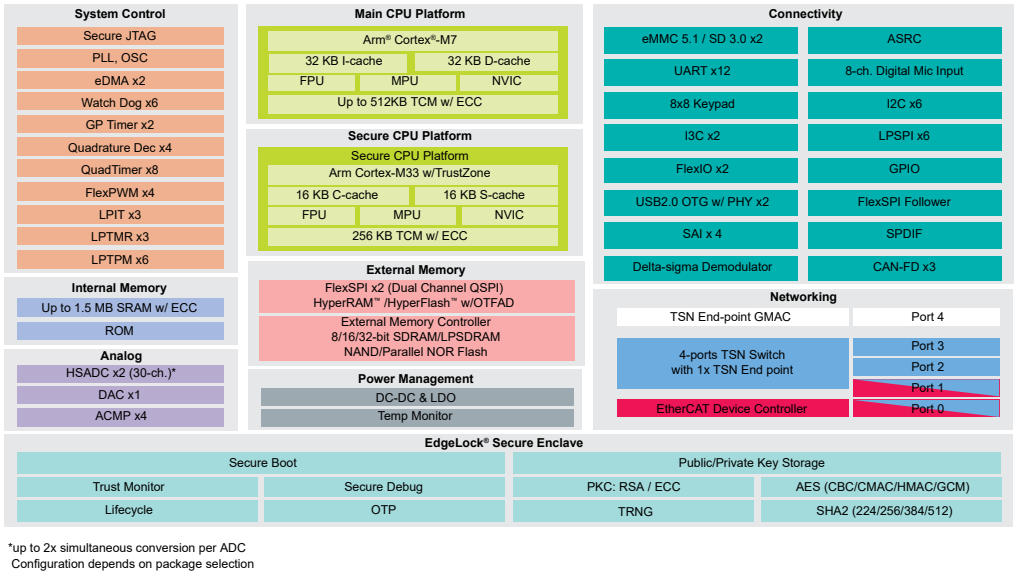

Figure 1. i.MX RT1180 Family Superset Block Diagram

1.5.4 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.

Table 6. Platform Deliverables

Type	Name	Release	Form of delivery
IC Hardware	i.MX RT1180	C0	Silicon Chip
System ROM Firmware	i.MX RT1180 System ROM	3.0 RC1.2	Onchip ROM Firmware
System ROM Firmware Patch	i.MX RT1180 ROM Patch	N/A	Onchip Firmware
Secure Enclave	EdgeLock Secure Enclave (Advanced Profile) (ELE-AP)	S401	Onchip Hardware Subsystem
Secure Enclave ROM	ELE-AP ROM	C0 RC3 (8d2c3a87)	Onchip ROM Firmware
Updatable Platform RoT	ELE-AP Firmware	1.1.0 (d5a78cba)	Software Binary Package
Software Development Kit	i.MX RT1180 SDK	25.03.00	Software Package

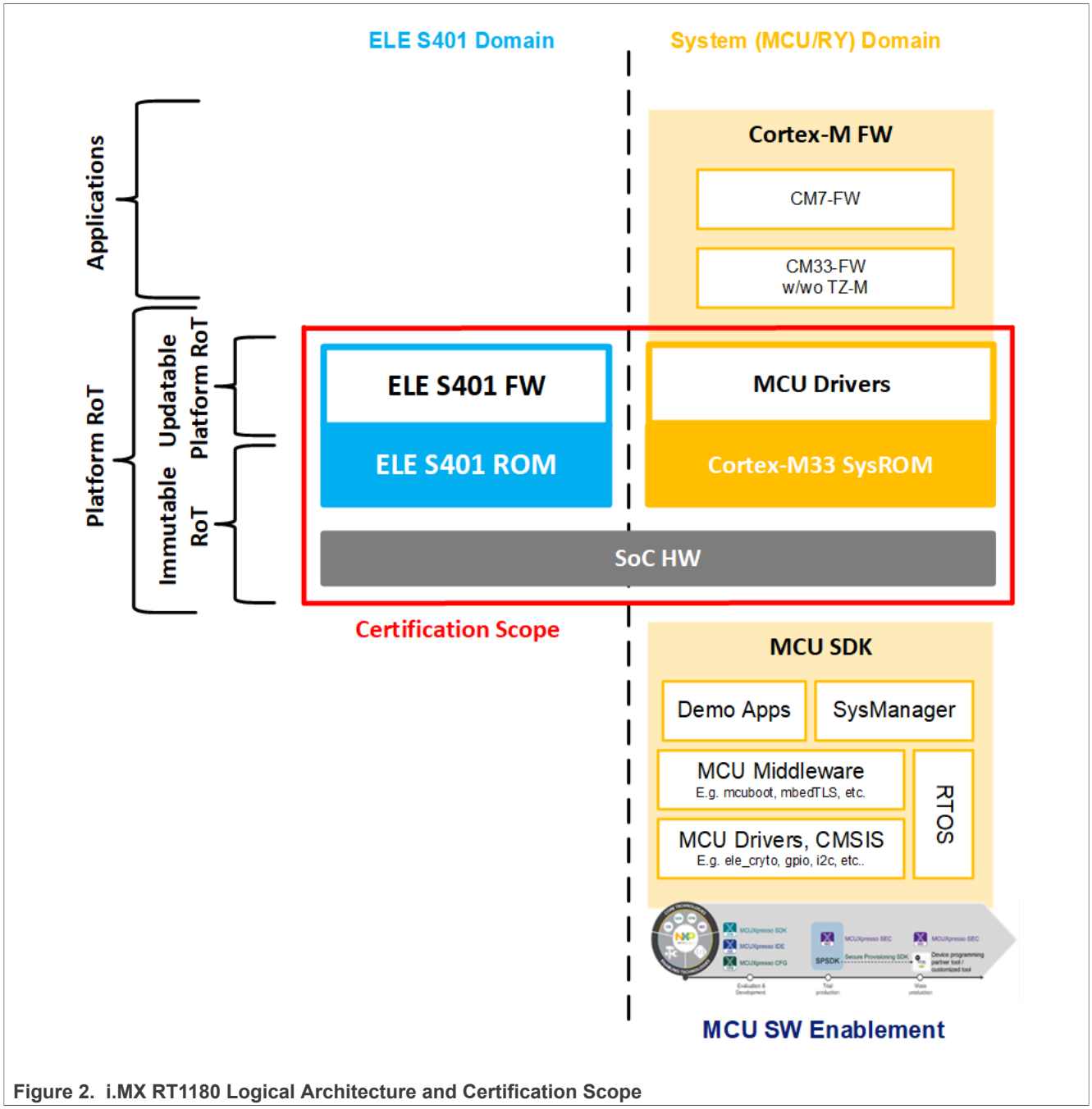

Figure 2. i.MX RT1180 Logical Architecture and Certification Scope

The TOE is available in 5 declinations, all available in the Indusctrial, Extended-Industrial, and Automotive grades (see [10], [12] and [13]):

- I.MX1181 & I.MX1182 in 144BGA package: with no Cortex M7 core, 1MB RAM & reduced number of connectivity ports
- I.MX1186 in 196 BGA package with Cortex M7, 1.5MB RAM, reduced numner of connectivity ports
- I.MX1197 & I.MX1189 in 289BGA package with Cortex M7, 1.5MB RAM, and full connectivity

In addition to that, the I.MX1181_S & I.MX1187_S are varients of the I.MX1181 & I.MX1187 with customer application specific IP activated by Fuse, and available in Industrial and Extended-Industrial grades (see [11]).

All these variants are strictly identical from a security services point of view and the current security target applies to all of them.

The logical scope also includes the following midleware drivers for the Real Time host provided in the SDK:

Table 7. SDK drivers

Driver	Implmentation in SDK ("devices/MIMXRT1180/drivers"
NETC drivers	fsl_netc_* netc_hw/fsl_netc_hw*
clock/clock tree drivers	fsl_clock*
The ANATOP drivers if applicable	spread in clock/power related drivers
The Sentinel IP drivers	in Sentinel IP
The cache drivers (if any)	cm7/fsl_cache cm33/fsl_cache
The DCDC drivers	fsl_dcdc*
The GPIO drivers	fsl_rgpio*
The I²C drivers	fsl_lpi2c* cmsis_drivers/fsl_lip2ic*
The UART drivers	fsl_lpuart* cmsis_drivers/fsl_lpuart*
The SPI Drivers	fsl_lpspi* cmsis_drivers/fsl_lpspi*
The Messaging unit drivers	fsl_mu*
The Shared memory drivers	middleware/multicore
The Power management drivers	fsl_gpc* fsl_misc* fsl_pmu* fsl_soc_src*
The temperature sensor drivers	fsl_tempsensor*
The watchdogs drivers	fsl_rtwdog*
The OCOTP drivers	in Sentinel IP
TRDC: TrustZone Driver	fsl_trdc*

1.5.5 Required Non-Platform Hardware/Software/Firmware

i.MX RT1180 has no internal flash, hence compatible external non-volatile memory shall be deployed via FlexSPI for image storage with sufficient size. See Chapters 31 of [6] / [7] for compatible external flash.

To have Battery Backed Secure / Non-Secure Module (BBSM/BBNSM) working as expected, battery shall be integrated to provide power to VDD_BBSM_IN domain, and have sufficient power for the intended use case. See more in Chapter 24 BBNSM and Chapter 27 SRC of [6] / [7] and Chapter 8 of [8] / [9].

1.5.6 Life Cycle

The i.MX RT1180 life cycle states for OEM are shown as Figure 3. ELE-AP manage the life cycle state fuses, and the current life cycle state determines the device functionality, debug and test port availability, and asset accessibility for both the EdgeLock secure enclave and the rest of SoC. The life cycle can only be advanced and cannot return to a previous state. See more in Chapter 2.5 Life Cycle Management of [8] / [9]

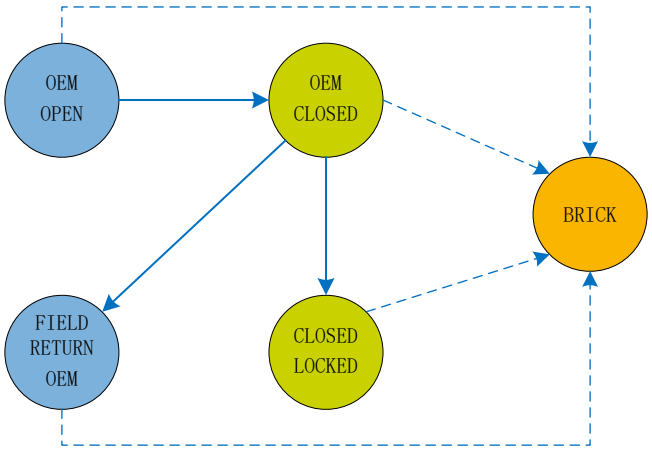

Figure 3. i.MX RT1180 OEM Chip Life Cycle states

1.5.7 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 and the Secure Enclave is protected aginst physical attacks.

Hardware Protection

The Secure Enclave is protected aginst physical attacks

1.5.8 Use Case

[trusted user]

In general, i.MX RT1180 is expected to be deployed in a controlled evniroment where users who can have physical access are trusted. Yet in case that 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, i.MX RT1180 offers ELE-AP protection mechanisms to provide extra attacker resistance including physical attackers.

[any code]

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

1.5.9 IEC62443-4-2 Considerations

IEC62443 series [23] includes several standards and technical reports addressing Industrial Automation and Control Systems (IACS). Its Part 4-2: Technical security requirements for IACS components [25] provides detailed technical control system component requirements. It defines 4 security levels of control system component capability (SL-C 1~4), and 4 types of components of IACS: software applications, host devices, embedded devices and network devices.

i.MX RT1180 is desigined to be used as a part of system for industiral use cases, or in IEC62443-4-2 term, a subcomponent. This document also serves as a guidance on correct integration of an IEC62443-4-2 compliant IACS component. As a subcomponent, i.MX RT1180 fulfills subset of IEC62443-4-2 requirements which can keep aligned with the overall component requirements, and more importantly, provides services which support the overall component fulfilling IEC62443-4-2 requirements in a secure and ready-to-use way.

i.MX RT1180 targets compliance to Capability Security Level 3 (SL-C 3). The mapping and rationales are provided in IEC62443-4-2 Mapping.

In Section 3, we have not only provided the security functions in SESIP language, also provided further specifications if an IEC62443-4-2 requirement has finer granularity. One can refer to [25] for the original text of the requrirement, yet the reader should be aware there is difference and connection on the terminology between IEC62443-4-2 and SESIP. For instance, component or its type (e.g. embedded device) in IEC62443 may refer to the platform under evaluation in SESIP, and this document intends to keep this usage to provide a clear scope of the certification.

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 8. 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
Platform Acceptance	When receiving the platform, the user shall verify the correct version of all platform components that it depends on, as described in Section 3.3.1.1 and Section 3.4.1.1 of this document. Note that one of the loadable firmware identified in Section 3.3.1.1 must be loaded for the product to be in a certified configuration.	Section 3.3.1.1 Section 3.4.1.1
Key Management	Management of cryptographic keys and certificates outside of the Platform shall follow secure key management procedures.	This document
OEM Trust Provisioning	Any secret to be provisioned into the platform shall be generated securely (e.g., via a standard compliant HSM) and subject to secure key management procedures. The provisioning process shall be 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, shall be trustworthy.	This document
Secure Boot	The operating system or application code shall make use of the Advanced High Assurance Boot (AHAB) feature as per Section 3.9 Secure Boot of [8] / [9]	Section 3.9 Secure Boot of [8] / [9]
Secure Update and Key Revoke	Actors in charge of executing update of the platform firmware or applications shall securely initiate the update process. The update image shall be properly signed and distributed in secure manner to ensure its confidentiality and authenticity. The operating system or application code shall 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.	Section 3.6 Program Image and Section 3.9 Secure Boot of [8] / [9]
Secure Debug	The integrating environment shall configure the debug functionality as described in Section 5 Secure Debug of [8] / [9] to meet the extra physical attacker resistance.	Section 5 Secure Debug of [8] / [9]
SW Integration	The operating system or application code shall ensure that the correct version of SDK drivers are integrated and configured.	This document
Lifecycle Management	The integrating OEM shall ensure that the platform life cycle is set to OEM CLOSED or CLOSED LOCKED state at the end of product manufacturing before deployment in the field.	Section 3.11 Forward Lifecycle of [14]
Physical attacker resistance configurations	If local physical attack is applicable for the use cases, the integrating OEM shall make sure that GDET is activated before deployment in the field, and that assets and security sensitve parameter are protected by ELE-AP. In particular, for critical security operations requiring physical attack resistance, the crypto operation shall be performed with the key from the keystore and the IV shall be internally generated by ELE when applicable.	Sections 1.6 and 4.4.23 of [14] Sections 3.19 and 5.1.8.1 of [14] Sections 4.4 of [14]
Untrusted code	Deployment of untrusted code on the end product shall not be permitted in the same execution domain(s) as the vendor application. Execution domain is characterized by the execution Core ID, the privileged level within that Core, and the TrustZone (if applicable)	Sections 1.6 of [14]

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]:

- Secure Enclave (Section 3.3): **SESIP Assurance Level 3 (SESIP3)** .
- The entire SoC (Section 3.4): **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 RT1180's Advanced High Assurance Boot (AHAB) 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 3.3.2.1 for further information.

3.2 Security Process Packages (SPPs)

The claimed Security Process Packages are the following:

- IEC 62443-461 Secure Development (Section 3.2.1): **SESIP Assurance Level 3 (SESIP3)** .
- Trust Provisionning (Section 3.2.2): **SESIP Assurance Level 3 (SESIP3)** .

3.2.1 IEC 62443-4-1 Secure Development

For the development of the platform, the secure development process specified in *IEC62443-4-1 [24]* has been applied to the platform.

Conformance rationale:

NXP Security Maturity Process (SMP) is designed to ensure that product security is given due consideration throughout the development cycle beginning with incorporating security in the product architecture – in a concept of 'Security-by-Design' - and then approving Security Milestones during development. This process is integrated into NXP Business Creation and Management (BCaM) framework which covers all harmonized processes to successfully launch New Products, and Security Milestones align with the BCaM product development project gates and milestones with the aim to ensure that security-related deliverables and reviews are planned accordingly, and eventually successfully completed for each Security Milestone, and hence for each product development gate/milestone.

BCaM process including SMP which focuses on Security by Design together with PSIRP process introduced in Section 3.1.1 has been certified against Security for Industrial Automation and Control Systems - Part 4-1: Secure Product Development Lifecycle Requirements (IEC 62443-4-1:2018) [24] (See Section 1.4.1).

For the development of i.MX RT1180, the abovementioned IEC62443-4-1 certified NXP processes have been applied.

3.2.2 Trust provisioning

A trust provisioning process ensures the secure management in a trusted environment of *Data in Table 9* and its/their loading into the platform for the following use cases *Use Case in Table 9* as specified in *Specification in Table 9*.

Both the trusted environment and the platform protect the *access, confidentiality, integrity* of provisioned data.

Table 9. Trust provisioning

Data	Use Case	Specification
Cryptographic Keys	OEM Secure Provisioning	[21]
Cryptographic Keys	EdgeLock2Go	[21]
Customer Data	Customer Customized Provisioning by NXP	[21]

Conformance rationale:

Trust Provisioning (TP) describes the process of establishing a trust anchor in NXP devices that can be used by customers. This trust anchor could be a cryptographic key (or a set of keys), a unique identifier, or customer specific content. See more in [21], Section 3.3.2.1 and Section 3.3.5.2.

3.3 Security Functional Requirements for the Secure Enclave

In the following Security Functional Requirements, the term **platform** covers the **i.MX RT1180 physical and logical scope**, and the term **application** refer 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 RT1180 employs a secure enclave (ELE-AP), which fulfills the following security functional requirements:

3.3.1 Identification and Attestation of Platforms and Applications

3.3.1.1 Verification of Platform Identity

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

Conformance rationale:

The ELE-AP unique identification information is injected into the ELE-AP subsystem during the SoC manufacturing in NXP sites or programed into the ROM/Loadable FW release. This information can be retrieved

through the "GET INFO" and "Get EdgeLoc Secure Enclave FIRMWARE VERSION" commands described in detail in [14] section 3.30 and 3.13 respectively:

Command "GET INFO": the response fields `Soc_rev`, `Soc_id`, `Fw_hash` and `Sha256 ROM patch` allow identifying the version of the silicon and the loadable firmware. In the current integration into the i.MX RT1180 SoC, the return values shall match the versions indicated in the table below. This information will also be part of the attestation information (see Section 3.3.1.3). Due to limited ELE-AP RAM space, the ELE-AP Loadable FW is made of four binaries for four different use cases which can be identified individually:

1. The "base" FW that conatains features that are mainly used at boot
2. The "alt" FW that contains the "HSM" features (keystore / opaque key support, crypto)
3. The "EL2Go" FW that can be used to enable the EL2Go product manufacturing
4. The "OEM provisioning" FW that can be used to provision the customer keystore by enabling some key exchange features

Table 10. *Get Info* expected values

Field	Meaning	Expected value
Soc_rev	Soc revision number	0xC000
Soc_id	Soc identity	0x1180
Sha 256 ROM patch	Sha256 of Edge Lock Secure Enclave rom patch fuses	2a2fb57ebe246cf9e388346f320b3c55a127b38350a7c0bb9d1a449350af0372[1]
Sha FW (base)	First 256 bits of installed fw sha	1d2cb66c28111ae53db789944c64732850bc8178fc030b5a2671c93aebcba588[1]
Sha FW (alt)	First 256 bits of installed fw sha	f417f4c3add1924a9ae18aaa0579ba7e087a345b46d4231da8f7648676d2d41f[1]
Sha FW (EL2Go)	First 256 bits of installed fw sha	b539b23b0c55399a63d8def2990bb4f04c8f38711796329a11f8ee9a49b766da[1]
Sha FW (OEM prov)	First 256 bits of installed fw sha	d37ba4f7dfe258fd4bc5e6f6d0197c816b2d8a7598565fb23de3e54e6f1acaf1[1]

[1] Byte stream representation. GET INFO output is Little Endien 32bits based on ARM Cortex-M architecture.

Command "Get EdgeLoc Secure Enclave FIRMWARE VERSION": the response fields `FW version` / `FW Commit SHA1` allows identifying the version of the installed loadable firmware. In the current integration into the i.MX RT1180 SoC, the return values shall match the versions indicated in table below.

Table 11. *Get EdgeLock Secure Enclave FIRMWARE VERSION* expected values with installed loadable firmware

Field	Expected value
FW version (FW)	1.1.0
Commit SHA1 (FW)	d5a78cba

The production validation process ensures that the SFR behaves correctly.

3.3.1.2 Verification of Platform Instance Identity

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

Conformance rationale:

The unique identification of a i.MX RT1180 instance is based on the UUID generated and fused into ELE-AP during NXP manufacturing in NXP sites.

This information can be retrieved through the "GET INFO" API described in detail in [14] section 3.30. This information will also be part of the attestation information (see Section 3.3.1.3).

The production validation process ensures that the SFR behaves correctly.

3.3.1.3 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 cannot be cloned or changed without detection.

Conformance rationale:

The ELE-AP implements a challenge-response attestation of its genuineness building a payload including the information provided by the Get Info API : ELE-AP identity (as described in Section 3.3.1.1), ELE-AP instance identity (as described in Section 3.3.1.2), ELE-AP lifecycle state, OEM SRK Hash, ELE-AP state, and a nonce that is received with the attestation request. See section 3.31 "DEVICE ATTESTATION" API of [14]. The payload is signed with ECDSA p384 NXP DIE ATTEST AUTH key. The payload preparation and signature are fully performed by the ELE-AP in RROT (Runtime Root Of Trust) mode.

The production validation process ensures that the SFR behaves correctly.

3.3.1.4 Secure Initialization of 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:

Secure initialization (authenticity and integrity checks) of the ELE-AP, CM7 and CM33 domains is ensured by the Advanced High Assurance Boot (AHAB) feature implemented in the ELE-AP.

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

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

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

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

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

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

The production validation process ensures that the SFR behaves correctly.

3.3.1.5 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:

The ELE-AP implements the attestation of its state by including this state (FW&patch hashes, life-cycle) as part of the attestation payload described in Section 3.3.1.3.

The production validation process ensures that the SFR behaves correctly.

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

3.3.2.1 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 authenticity and integrity of the updated firmware image is checked during the secure boot process as described in Section 3.3.1.4. To protect against rollback of firmware, those are associated to a version number and the ELE-AP manage a “minimum allowed firmware version” in fuses.

Regarding ROM update, the ELE-AP ROM can be patched, and the handling of those patches is fully handled by the ELE-AP. ROM patches can be part of OTP (called early patches) or be part of the ELE-AP loadable firmware (called late patches). In the first case, OTP patches can only be done during NXP manufacturing (through ECDSA P256 signed messages). In the second case, the patches are part of the ELE-AP loadable firmware and their authenticity and integrity is checked along with the overall firmware verification. Note that late patches loading feature is disabled by default and can only be enabled by an early patch.

The production validation process ensures that the SFR behaves correctly and supports the ALC_FLR.2 procedures as referenced in Section 3.1.1

3.3.2.2 Decommission of Platform

The platform can be decommissioned.

Conformance rationale:

i.MX RT1180 provides BRICK life-cycle state. BRICK life cycle state completely disables ELE-AP from any use or testing (see Chapter 3.5 of [8] / [9] and Section 3.14 of [14]).

In this state the ELE-AP and the SoC CPUs are disabled preventing any access to user data, fuses, and debug functionalities.

The production validation process ensures that the SFR behaves correctly.

3.3.2.3 Field Return of Platform

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

Conformance rationale:

i.MX RT1180 enters FIELD RETURN OEM (/NXP) state when a dedicated commend signed by OEM (/NXP) SRK is sent to ELE-AP (Section 3.14 of [14]). In that state, access to user sensitive data is made impossible as key blobs created in CLOSED or CLOSED LOCKED life cycle states are diversified unsing the lifecycle, ensuring that keystores blobs generated in CLOSED or CLOSED LOCKED cannot be unwrapped in FIELD RETURN OEM (/NXP) life cycle state (see Section 3.4 of [8] / [9], and Section 4.1.5.5, 4.4.11, 4.4.16 of [14]).

The production validation process ensures that the SFR behaves correctly.

3.3.3 Secure Communication

3.3.3.1 Secure Communication Support

The platform provides the application with one or more secure communication channel(s).

The secure communication channel authenticates *Host Platform* and protects against *disclosure, modification, replay, erasure* of messages between the endpoints, using *physical isolation, command integrity verification, seesion handle, payload signing or encryption*.

Conformance rationale:

Each CPU of the SoC Domain is physically and exclusively connected to the ELE-AP via a dedicated Message Unit (ELE-MU). ELE-MUs are buffereded gates allowing the SoC CPUs and the ELE-AP to exchange commands and responses using a formally defined protocol, ensuring a complete mediation of the commands as no ressources from the ELE-AP can be accessed directly by the SoC CPUs (see section 11 of [8] / [9]).

The protocol ensures commands integrity using a CRC (see section 11 of [8] / [9]). Cryptographic command sequences and secure store access command sequences are done inside sessions with a session handle ensuring binding to the requestor and to the physical characteristics of the ELE-MU used to transmit the command (see HSM commands in section 4.4 of [14]). Keystore access also requires knowledge of a Nonce as authentication data (see section 4.4.5 of [14]). Most critical commands are signed (see section 2.6, 3.14.1 and 4.4.8 of [14]) or use encrypted payload (see section 4.4.16 and 4.4.46 of [14]).

3.3.4 Extra Attacker Resistance

3.3.4.1 Limited Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises *Verification of Platform Identity, Verification of Platform Instance Identity, Attestation of Platform Genuineness, Secure Initialization of Platform, Attestation of Platform State, Secure Update of Platform, Descomissioning of Platform, Filed Return of Platform, Secure Communication Support, 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), Cryptographic Operation, Cryptographic Operation (with provisioned key), Cryptographic Key Generation, Cryptographic KeyStore, Cryptographic Random Number Generation, Secure Data Serialization, Residual Information Purging, Reliable Index and Secure Debugging.*

Conformance rationale:

The ELE-AP is equipped with Voltage, Temperature, Frequency, and Glitch detectors. The System Reset Controler (SRC) module provides mechanism to configure the response action in case of unexpected enviromental conditions (See chapter 27 of [6] / [7]).

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

The ELE-AP software component including ROM and loadable firmware implements software protection technics and the cryptographic library has dedicated protections against fault injection and side channel analysis.

Note: Limitied Physical Attacker Resistance deviates from SESIP Profile for PSA Certified Level 3 [4] and SESIP Profile for PSA Certified Level 3 iSE/SE and RoT Component [5] but includes all the SFRs for the Secure Enclave which is the scope of the SESIP Profile for PSA Certified Level 3 [4] and SESIP Profile for PSA Certified Level 3 iSE/SE and RoT Component [5] claim.

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

3.3.4.2 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:

The ELE-AP domain is equiped of hardware dedicated resources which is solated from the rest of the SoC.

Access to any ELE-AP service can only be done through a set of interfaces called Message Unit (MU) receiving the SoC requests to be transmitted to ELE-AP domain. There is one MU per domain, CM7 and CM33, and a third MU is used for SoC general requests e.g., life-cycle states handling. Message validation and parsing is fully handled by the ELE-AP.

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

From PSA requirements perspective, one can regard the ELE-AP as Secure Processing Environment (SPE) and the rest of SoC domains CM7 and CM33 as Non-Secure Processing Environment (NSPE).

3.3.4.3 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 ensured inside the ELE-AP (see also Section 3.3.4.2.

ELE-AP stored PSA-RoT is protected and isolated from Application RoT services by ownership management of the objects stored inside the ELE-AP. See more in Section 3.3.5.4 about key isolation.

3.3.5 Cryptographic Functionality

3.3.5.1 Cryptographic Operation

The platform provides the *operations in Table 12* functionality with *algorithms in Table 12* as specified in *specifications in Table 12* for key lengths *described in Table 12* and modes *described in Table 12*.

Table 12. Cryptographic Operations by ELE-AP

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

Table 12. Cryptographic Operations by ELE-AP*...continued*

Operation	Algorithm	Specification	Key Lengths	Modes
Signature generation and verification	ECDSA	NIST FIPS 186-5	SECP R1 224, 256, 384, 521	SHA224, SHA256, SH384, SHA512
			BrainpoolP R1 224, 256, 384	SHA224, SHA256, SH384, SHA512
	RSA	PKCS#1 v2.2 NIST FIPS 186-5	2048, 3072, 4096	PKCS1 V1.5 SHA224 PKCS1 V1.5 SHA256 PKCS1 V1.5 SHA384 PKCS1 V1.5 SHA512 PKCS1 PSS MGF1 SHA224 PKCS1 PSS MGF1 SHA256 PKCS1 PSS MGF1 SHA384 PKCS1 PSS MGF1 SHA512

Conformance rationale:

The ELE-AP implements symmetric (SGI) and asymmetric (PKC) cryptographic accelerator to provide cryptographic operations services to the application. Those resources are dedicated and only accessible by the ELE-AP domain. See Chapters 4.1 and 4.2 of [14].

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

3.3.5.2 Cryptographic Operation (with provisioned key)

The platform provides the *operations in Table 13* functionality with *algorithms in Table 13* as specified in *specifications in Table 13* for key lengths *described in Table 13* and modes *described in Table 13*.

Table 13. Cryptographic Operations

Operation	Algorithm	Specification	Key Lengths	Modes
Signature Generation	ECDSA	ANSI X9.62	256	NIST P-256
Key unwrapping	AES	RFC3394	256	-

Conformance rationale:

The trust provisioning service also provide provision for EdgeLock2Go root-of-trust keys, hence their cryptographic operations are available to the platform which can enable secure communication establishment with EdgeLock2Go infrastructure and hence EdgeLock2Go Services. See more in Section 4.6 of [21] and Section 3.2.2.

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

3.3.5.3 Cryptographic Key Generation

The platform provides a way to generate cryptographic keys for use in *algorithms in Table 14* as specified in *specifications in Table 14* for key lengths *Key Lenghts in Table 14*

Table 14. Cryptographic Key Generation

Algorithm	Specification	Key Lengths
ECC	NiST FIPS 186-5 ANSI X9.62 SEC2 Brainpool v1.0	SECP R1 224, 256, 384, 521 BrainpoolP R1 224, 256, 384
RSA	NiST FIPS 186-5 PKCS#1 v2.2	2048, 3072, 4096
AES	NIST FIPS 197	128, 192, 256
HMAC	NIST FIPS 198-1	224, 256, 384, 512

Conformance rationale:

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

See Chapters 4.1 and 4.2 of [14]. Persistent keys generated are then securely stored as described in Section 3.3.5.4.

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

3.3.5.4 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-AP provides the application level an API for symmetric or asymmetric key storage and management. The application keys are imported via the API using an AES 256 bits pre-shared key.

Persistent keys (generated by the ELE-AP or imported in ELE-AP) are stored in NVM, inside Blobs encrypted by the ELE-AP. The Blobs are encrypted and authenticated using AES-GCM with a 256bit key, and binded to the platform instance, life cycle state, and version stored in fuses (anti rollback counter).

More details are provided in sections 3.4 of [8] / [9] and 4.4.9 to 4.4.16 of [14].

The production validation process ensures that the SFR behaves correctly.

3.3.5.5 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.800-90A CTR-DRBG (with AES-128)*.

Conformance rationale:

ELE-AP has a physical True Random Number Generator (TRNG) compliant with NIST SP 800-90B and internal DRBG module as defined in NIST SP 800-90A.

Furthermore:

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

See more in Chapters 4.4.41 of [14] and in [15].

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

3.3.6 Compliance Functionality

3.3.6.1 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:

The ELE-AP implements the secure encrypted data storage using same encryption mechanism as for the persistent key storage (see Section 3.3.5.4).

Persistent data are stored in NVM, inside Blobs encrypted by the ELE-AP. The Blobs are encrypted and authenticated using AES-GCM with a 256bit BEK that is binded to the platform instance, the life cycle state, and a storage counter (anti rollback).

More details are provided in sections 4.4.31 to 4.4.35 of [14]

The production validation process ensures that the SFR behaves correctly.

3.3.6.2 Residual Information Purging

The platform ensures that *key store areas, user data, sensitive transient data*, with the exception of *none*, is erased using the method specified in *the guidance document referenced 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:

Keys handled by the ELE-AP are erased (see *Chapter 4.4.15 of [14]*) by overwriting the keys with zero.

Data handled by the ELE-AP are erased (see *Chapter 4.4.35 of [14]*) by clearing the data chunk stored outside of the ELE-AP.

Sensitive transisent data (e.g. Cryptolib work area or root keys used to derive other keys) are cleared using a secure memeset function.

The production validation process ensures that the SFR behaves correctly.

3.3.6.3 Reliable Index

The platform implements a strictly increasing function.

Conformance rationale:

The ELE-AP implements an hardware OTP based Monotonic Counter that is used for Key management operations to prevent rollback (see sections 4.1.4.1, 4.4.5, 4.4.8, 4.4.11, 4.4.12, 4.4.13, 4.4.15, 4.4.16, and 5.2.3 of [14]).

The value of the ELE-AP Monotonic Counter can be read using the GET INFO APÏ command as per Section 4.4.4 of [14].

The production validation process ensures that the SFR behaves correctly.

3.3.6.4 Secure Debugging

The platform only provides *SWD/JTAG interface* authenticated as specified in *Chapter 7 of [8] / [9]* with debug functionality.

The platform ensures that all data stored, with the exception of *data in the authorised domain and Debug Enable Group as defined in the rationale below*, is made unavailable.

Conformance rationale:

In LOCKED life cycle state the debug is blocked. In OEM CLOSED life cycle state the SoC debug domains is accessible via OEM authentication (see sections 3.4 and 3.5 [8] / [9]). The debug blocked or authenticated access is enforced by the ELE-AP. The bebug authentication is a challenge-response scheme and assures that only the debugger in possession of the OEM debug credentials can successfully authenticate over the debug interface and access restricted parts of the device.

Debug acces to ELE-AP domain is reserved to NXP during production or field return analysis and is not reachable from any OEM life cycle state. See section 5.1.3 of [14].

See also Chapter 7 of [8] / [9] and Chapter 8 of [6] / [7].

The production validation process ensures that the SFR behaves correctly.

3.4 Security Functional Requirements for the SoC

In the following Security Functional Requirements, the term **platform** covers the **i.MX RT1180 physical and logical scope**, and the term **application** refer to any additional firmware, OS or application software which is out of evaluation scope. It represents a part of the final connected device.

The security functional requirements for the ELE-AP secure enclave are provided in Section 3.3. The following security functional requirements are implemented by the rest of the SoC outside the ELE-AP secure enclave:

3.4.1 Identification and Attestation of Platforms and Applications

3.4.1.1 Verification of Platform Identity (SoC)

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

Conformance rationale:

Besides reading out ELE-AP HW and driver version as introduced in Section 3.3.1.1, the SoC can also be identified by reading the JTAG ID register as per [6] / [7] section 9.8.3 (Part Revision Number PRN, Design Center DC, Part Identification Number PIN, and Manufacturer Identity Code MIC).

The SoC variant can be determined by reading the CHIP_ID fuse. The expected value is 0x009Y_8XC0 where

- X encodes the part number and can be 1/2/6/7/9 for i.MX RT1181/1182/1186/1187/1189
- Y encodes the operating temperature grade and General Market/Schneider varient and can be 0/1/2/3/4/5 for General Market and 6/7 for Schneider

See section 26.3 of [6] / [7] for more details.

The production validation process ensures that the SFR behaves correctly.

3.4.2 Extra Attacker Resistance

3.4.2.1 Software Attacker Resistance: Isolation of Platform (SoC)

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

Conformance rationale:

There are multiple isolation features presented in the platform.

The ELE-AP isolation is introduced in Section 3.3.4.3 and Section 3.3.4.2.

IEE-based and OTFAD-based memory encryption ensures Secure Isolation between the multiple memory contexts and the two physical QuadSPI Flash as introduced in Section Section 3.4.3.1 and Section 3.4.3.2.

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. At boot, the Trusted Ressource Domain Control (TRDC) is initialized and configured by the ELE-AP for the secure initialization and secure boot of the Platform, before passing the TRDC control to the authenticated OEM software for customer configuration (only secure-privilege code can do so). TRDC allows software to assign chip resources (processor cores, non-core bus masters, memory regions, and slave peripherals) to processing domains, to define access control policies for the individual domains, and to enforce access control to ressources per domain following the ARM TrsutZone philosophy. See more in Chapter 43 of [6] / [7] and chapter 3.10 of [8] / [9].

The production validation process ensures that the SFR behaves correctly.

3.4.2.2 Software Attacker Resistance: Isolation of Platform Parts (SoC)

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

Conformance rationale:

The ELE-AP is physically isolated from the rest of the platform and communication between ELE-AP and the rest of the platform is done through a set of interfaces called Message Units. See Section 3.3.4.2.

The production validation process ensures that the SFR behaves correctly.

3.4.3 Compliance Functionality

3.4.3.1 Secure Data Serialization (IEE) (SoC)

The platform ensures that all data stored outside the direct control of the platform, except for *Data outside of the eight memory contexts defined accross the external SPI Fash space and SDRAM space* is protected such that the *confidentiality, binding to the platform instance* is ensured.

Conformance rationale:

The Inline Encryption Engine (IEE) of the SoC provides for encryption and decryption supporting up to eight independent memory contexts, each having a unique 128-bit key. It can be used for SDRAM encryption/ decription with AES XTS and 128bit key, QuadSPI Flash decrition with AES CTR and 128bit key (similar to OTFAD). The context for each region is configured in the IEE.

The keys are stored in ELE-AP and distributed to IEE on demand via a dedicated bus, ensuring binding to platform instance and life cycle state. See more in Chapters 11 and 12 of [8] / [9].

The production validation process ensures that the SFR behaves correctly.

3.4.3.2 Secure Data Serialization (OTFAD) (SoC)

The platform ensures that all data stored outside the direct control of the platform, except for *Data outside of the eight memory context defined across the external SPI Flash space (2 FlexSPI interfaces)* is protected such that the *confidentiality, binding to the platform instance* is ensured.

Conformance rationale:

The SoC supports on-the-fly decryption (OTFAD) of Application code and data stored encrypted (AES CTR with 128bits key) in up to two external QuadSPI Flash (accessible via two FlexSPI interfaces) via two OTFAD interfaces, in complete transparency (“on-the-fly”) for the host and with zero latency (no additional read cycles). Each OTFADn supports up to four independent memory contexts, each context having a unique 128-bit key. The four keys of OTFADn are stored in the corresponding Flash inside an encrypted blob and unwrapped using KEKs generated from OTFADn_KEY (OTP), OTFADn_KEY_SCRAMBLE (OTP), and the context number. See Sections 5 and 10 of [8] / [9].

The production validation process ensures that the SFR behaves correctly.

3.4.3.3 Residual Information Purging (SoC)

The platform ensures that *PUF derived data, ELE-AP stored keys and used data, and OTFAD/IEE protected memory*, with the exception of *none*, is erased using the method specified in *Section 3.4 of [8] / [9]* before the memory is used by the platform or application again and before an attacker can access it.

Conformance rationale:

The keys and user data erasure in ELE-AP is introduced in Section 3.3.6.2.

Entering the FA Mode or Bulk Erase Flash purges sensitive data like OTFAD/IEE memory encrytion keys rendering the memory content inaxessible. See more in Section 3.3.2.3 and Section 3.3.2.2.

The production validation process ensures that the SFR behaves correctly.

3.4.3.4 Reliable Index (SoC)

The platform implements a strictly increasing function.

Conformance rationale:

Battery Backed Secure / Non-Secure Module (BBSM/BBNSM) is in the low power section VDD_BBSM_IN domain, which can be battery backed. This enables it to keep this data valid and continue to increment the time counter when the power goes down in the rest of the device. The always-powered up part of the module is isolated from the rest of the logic to ensure that it does not get corrupted when the device is powered down.

The BBSM provides a Monotonic Counter and a Secure Real Time clock as described in Section 2.2, 3.3, 9.2, 9.3 of [8] / [9].

The production validation process ensures that the SFR behaves correctly.

3.4.3.5 Secure Debugging (SoC)

The platform only provides *SWD/JTAG interface* authenticated as specified in *Chapter 7 of [8] / [9]* with debug functionality.

The platform ensures that all data stored, with the exception of *subdomain(s) debug access enabled*, is made unavailable.

Conformance rationale:

In LOCKED life cycle state the debug is blocked. In OEM CLOSED life cycle states the chip forces a debug authentication protocol for the OEM SoC (non-ELE) domain.

The debug blocked or authenticated access is enforced by the ELE-AP. The debug authentication is a challenge-response scheme and assures that only the debugger in possession of the OEM debug credentials can successfully authenticate over the debug interface and access restricted parts of the device. Furthermore, the debug subsystem is sub-divided into multiple debug domains to allow finer access control.

See more in Chapters 3.5 and 7 of [8] / [9].

The production validation process ensures that the SFR behaves correctly.

4 Mapping and Sufficiency Rationales

4.1 SESIP3 Sufficiency for the SoC

Table 15. SESIP3 Sufficiencyfor the SoC

Assurance Class	Assurance Family	Covered By	Rationale
ASE: Security target evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in Section 1.1, the TOE reference in Section 1.3, the TOE overview and description in Section 1.5.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in Section 2 refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	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 15. SESIP3 Sufficiencyfor the SoC*...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 SESIP3 Sufficiency for the Secure Enclave

Table 16. SESIP3 Sufficiency for the Secure Enclave

Assurance Class	Assurance Family	Covered By	Rationale
ASE: Security target evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in Section 1.1, the TOE reference in Section 1.3, the TOE overview and description in Section 1.5.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in Section 2 refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	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.

Table 16. SESIP3 Sufficiency for the Secure Enclave*...continued*

Assurance Class	Assurance Family	Covered By	Rationale
ATE: Test	ATE_IND.1 Independent testing: conformance	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis	N.A. A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.	The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Enhanced-Basic.

4.3 Conformance Mapping to SESIP Profile for Secure MCUs and MPU for the SoC

This section provides rationales of conformance claimed in Section 1.2

Table 17. SESIP Profile for Secure MCUs and MPUs Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.3.1.1 Section 3.4.1.1
	Secure Initialization of Platform	Section 3.3.1.4
	Secure Updated of Platform	Section 3.3.2.1
	Residual Information Purging	Section 3.3.6.2 Section 3.4.3.3
	Secure Debugging	Section 3.3.6.4 Section 3.4.3.5
Security Services	Cryptographic Operation	Section 3.3.5.1 Section 3.3.5.2
	Cryptographic Key Generation	Section 3.3.5.3
	Cryptographic KeyStore	Section 3.3.5.4
	Cryptographic Random Number Generation	Section 3.3.5.5
Software Isolation	Software Attacker Resistance: Isolation of Platform	Section 3.3.4.2 Section 3.3.4.3 Section 3.4.2.1
Secure Enclave	Software Attacker Resistance: Isolation of Platform Parts , and SFRs per Section 3.3	Section 3.4.2.2 Section 3.3
	Limited Physical Attacker Resistance	Section 3.3.4.1
Additional Security Functional Requirements (Optional)	Verification of Platform Instance Identity Attestation of Platform Genuineness Attestation of Platform State Decommission of Platform Field Return of Platform Reliable Index Secure Communication Support Secure Data Serialization	Section 3.3.1.2 Section 3.3.1.3 Section 3.3.1.5 Section 3.3.2.2 Section 3.3.2.3 Section 3.3.6.3 Section 3.3.3.1 Section 3.3.6.1 Section 3.4.3.1 Section 3.4.3.2

4.4 Conformance Mapping to SESIP Profile for Secure MCUs and MPUs for the Secure Enclave

This section provides rationales of conformance claimed in Section 1.2

Table 18. SESIP Profile for Secure MCUs and MPUs Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.3.1.1
	Secure Initialization of Platform	Section 3.3.1.4
	Secure Updated of Platform	Section 3.3.2.1
	Residual Information Purging	Section 3.3.6.2
	Secure Debugging	Section 3.3.6.4
Security Services	Cryptographic Operation	Section 3.3.5.1 Section 3.3.5.2
	Cryptographic Key Generation	Section 3.3.5.3
	Cryptographic KeyStore	Section 3.3.5.4
	Cryptographic Random Number Generation	Section 3.3.5.5
Software Isolation	Software Attacker Resistance: Isolation of Platform	Section 3.3.4.2 Section 3.3.4.3
Hardware Protections	Physical Attacker Resistance: All the SFRs of the Secure Enclave are covered by the Limited Physical Attacker Resistance	Section 3.3.4.1
Additional Security Functional Requirements (Optional)	Verification of Platform Instance Identity Attestation of Platform Genuineness Attestation of Platform State Decommission of Platform Field Return of Platform Secure Communication Support Secure Data Serialization Reliable Index	Section 3.3.1.2 Section 3.3.1.3 Section 3.3.1.5 Section 3.3.2.2 Section 3.3.2.3 Section 3.3.3.1 Section 3.3.6.1 Section 3.3.6.3

4.5 Conformance Mapping for SESIP Profile for PSA Certified Level 3

This section provides rationales of conformance claimed in Section 1.2

Table 19. SESIP Profile for PSA Certified Level 3 Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.3.1.1
	Verification of Platform Instance Identity	Section 3.3.1.2
	Attestation of Platform Genuineness	Section 3.3.1.3
	Secure Initialization of Platform	Section 3.3.1.4
	Attestation of Platform State	Section 3.3.1.5
	Secure Updated of Platform	Section 3.3.2.1
	Physical Attacker Resistance: All the SFRs of the Secure Enclave are covered by the Limited Physical Attacker Resistance	Section 3.3.4.1 which covers all the SFRs mapped in this table
	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Section 3.3.4.2
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	Section 3.3.4.3

Table 19. SESIP Profile for PSA Certified Level 3 Sufficiency*...continued*

Package Claimed	Security Functional Requirements	Covered By
	Cryptographic Operation	Section 3.3.5.1 Section 3.3.5.2
	Cryptographic Key Generation	Section 3.3.5.3
	Cryptographic KeyStore	Section 3.3.5.4
	Cryptographic Random Number Generation	Section 3.3.5.5
Optional SFR	Secure Debugging	Section 3.3.6.4
	Secure External Storage	Section 3.3.6.1

4.6 Conformance Mapping for SESIP Profile for PSA Certified Level 3 iSE/SE and RoT Component

This section provides rationales of conformance claimed in Section 1.2

Table 20. SESIP Profile for PSA Certified Level 3 iSE/SE and RoT Component Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.3.1.1
	Secure Initialization of Platform	Section 3.3.1.4
	Secure Updated of Platform	Section 3.3.2.1
	Physical Attacker Resistance: All the SFRs of the Secure Enclave are covered by the Limited Physical Attacker Resistance	Section 3.3.4.1 which covers all the SFRs mapped in this table
	Cryptographic Operation	Section 3.3.5.1 Section 3.3.5.2
	Cryptographic Random Number Generation	Section 3.3.5.5
	Cryptographic Key Generation	Section 3.3.5.3
	Cryptographic KeyStore	Section 3.3.5.4
Optional SFR	Verification of Platform Instance Identity	Section 3.3.1.2
	Attestation of Platform Genuineness	Section 3.3.1.3
	Attestation of Platform State	Section 3.3.1.5
	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Section 3.3.4.2
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	Section 3.3.4.3
	Secure Communication Support	Section 3.3.3.1
	Secure Debugging	Section 3.3.6.4
	Secure Data Serialization	Section 3.3.6.1

5 Appendix

5.1 IEC 62443 support

IEC 62443-4-1 compliance

IEC62443-4-2 requires component developed and supported following the secure product development process described in IEC 62443-4-1. This is covered by the current evaluation as described in Section 3.2.

IEC 62443-4-2 support

The table below shows how the platform under evaluation (i.MX RT1180 described in this Security Target) supports the final device (known as the component), demonstrating compliance with the IEC 62443-4-2 security requirements (see [25]).It describes which part of each 62443-4-2 requirements are implemented at the i.MX RT1180 own level. Then, this is the responsibility of the component to use the security features described to implement the final requirement.

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

Table 21. IEC 62443-4-2 security requirements support by i.MX RT1180

62443-4-2 requirements	i.MX RT1180 supports
CR 1.1 - Human user identification and authentication CR 1.1(1) - Unique identification and authentication	It is the component responsibility to implement human user identification and authentication[1]. Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation and Cryptographic KeyStore provide cryptographic functionalities that can be used to implement human user identification and authentication.
CR 1.2 - Software process and device identification and authentication CR 1.2(1) - Unique identification and authentication	Verification of Platform Identity and Verification of Platform Identity (SoC) provide a unique and tamper-proof identification of the i.MX RT1180 type and version, that can be used for precise identification of the final component (by including subcomponent identification). Verification of Platform Instance Identity provides a unique and tamper-proof identity of each i.MX RT1180 instance, that can be used for precise identification of the final component (by including subcomponent identification). Attestation of Platform Genuineness provides an attestation for the i.MX RT1180 identity, that can be used for full authentication of the final component (by including subcomponent authentication). Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation and Cryptographic KeyStore provide cryptographic functionalities that can be used to implement identification and authentication to other components.
CR 1.3 - Account management	It is the component responsibility to properly implement account management. Cryptographic KeyStore provides secure storage for account credentials. Authentication is as per CR1.1 and 1.2.
CR 1.4 - Identifier management	Cryptographic Key Generation and Cryptographic Random Number Generation provide key generation and random number generation services which can be used for unique and unambigous identifier creation.
CR 1.5 - Authenticator management CR 1.5(1) - Hardware security for authenticators	Cryptographic Key Generation and Cryptographic Random Number Generation provide key generation and random number generation which can be used as authenticators. Cryptographic KeyStore provides secure storage of authenticators.

Table 21. IEC 62443-4-2 security requirements support by i.MX RT1180*...continued*

62443-4-2 requirements	i.MX RT1180 supports
	Limited Physical Attacker Resistance provides protections of authenticators against physical attacks. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide protection of authenticators against remote and local logical attacks.
CR 1.6 – Wireless access management	Cryptographic Operation, Cryptographic Key Generation and Cryptographic Random Number Generation provide cryptographic functionalities that can be used by network-components to implement authentication of all users engaged in wireless communication. Cryptographic KeyStore provides secure storage of cryptographic material used by network-components for identification and authentication of users engaged in wireless communication.
CR 1.7 – Strength of password-based authentication CR 1.7(1) – Password generation and lifetime restrictions for human users	It is the component responsibility to properly enforce the password policy. Cryptographic Operation, Cryptographic Key Generation and Cryptographic Random Number Generation provide cryptographic functionalities that can be used to enforce configurable password strength by meeting defined strength rules. Cryptographic KeyStore provides secure storage that can be used to enforce configurable password strength allowing their modifications and/or deletion to comply with defined number of use and lifetime restrictions. Reliable Index and Reliable Index (SoC) provide time references and monotonic counters allowing lifetime restriction management.
CR 1.8 – Public key infrastructure certificates	Cryptographic Operation, Cryptographic Key Generation and Cryptographic Random Number Generation provide cryptographic functionlaities that can be used to interact and operate with PKI infrastructures. Cryptographic KeyStore provide secure storage of the cryptographic material (e.g. keys, certificates) involved in PKI infrastructures. Limited Physical Attacker Resistance provides protections of cryptographic material and operations against physical attacks. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide protections of cryptographic material and operations against remote and local logical attacks.
CR 1.9 – Strength of public key-based authentication CR 1.9(1) – Hardware security for public key-based authentication	Cryptographic Operation and Cryptographic Key Generation provide cryptographic features needed in public-key-based authentication in conformance with internationally recognized and proven security practices and recommendations. Cryptographic KeyStore provides secure storage for cryptographic material (e.g. keys, certificates) needed in public-key-based authentication. Limited Physical Attacker Resistance provides protection of public-key-based authentication related material against physical attacks. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide protection of public-key-based authentication related material against remote and local logical attacks.

Table 21. IEC 62443-4-2 security requirements support by i.MX RT1180*...continued*

62443-4-2 requirements	i.MX RT1180 supports
CR 1.10 – Authenticator feedback	It is the component responsibility to obscure the authentication feedbacks sent back to the users. Human, Software, or Device Authentication is as per CR1.1 and CR1.2.
CR 1.11 – Unsuccessful login attempts	It is the component responsibility to limit the number of attempts and the reaction when the limit is reached. Human, Software, or Device Authentication is as per CR1.1 and CR1.2.
CR 1.12 – System use notification	It is the component responsibility to display a system use notification message before the authentication. Human, Software, or Device Authentication is as per CR1.1 and CR1.2.
CR 1.13 – Access via untrusted networks CR 1.13(1) – Explicit access request approval	It is the component responsibility to deny or accept requests based on the authentication results. Human, Software, or Device Authentication is as per CR1.1 and CR1.2.
CR 1.14 – Strength of symmetric key-based authentication CR 1.14(1) – Hardware security for symmetric key-based authentication	Cryptographic Operation and Cryptographic Key Generation provide cryptographic functionalities conforment to internationally recognized and proven security best practices that can be used for symmetric-key-based authentication. Cryptographic KeyStore provides secure storage for cryptographic material (e.g. shared secret) involved in symmetric-key-based authentication. Limited Physical Attacker Resistance provides protections of related material against physical attacks. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide protections of related material against remote and local logical attacks.
CR 2.1 – Authorization enforcement	It is the component responsibility to properly implement authorization enforcement mechanism. Human, Software, or Device Authentication is as per CR1.1 and CR1.2. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide logical isolation of the i.MX RT1180 internals that can be leveraged to enforce authorization of properly authenticated entities.
CR 2.2 – Wireless use control	It is the component responsibility to properly implement wireless use control. Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation and Cryptographic KeyStore provide cryptographic functionalities that can be used to implement wireless network authentication.
CR 2.4 – Mobile code CR 2.4(1) – Mobile code authenticity check	Secure Initialization of Platform and Secure Update of Platform provide secure boot and secure update with integrity and authenticity verification of the i.MX RT1180 subcomponent and other SoC processing domains before their execution, which can include mobile code. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide isolation mechanisms for controlled execution of mobile code. Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation and Cryptographic KeyStore provide cryptographic functionalities that can be used to control the integrity and authenticity of

Table 21. IEC 62443-4-2 security requirements support by i.MX RT1180*...continued*

62443-4-2 requirements	i.MX RT1180 supports
	mobile code, as well as to authenticate users that are allowed to transfer mobile code.
CR 2.5 – Session lock CR 2.6 – Remote session termination CR 2.7 – Concurrent session control	It is the component responsibility to properly implement session lock, remote session termination, and concurent session control mechanisms. Human user re-authentiction is as per CR1.1. Remote software processes or devices re-authentication is as per CR1.2 and CR1.6. Account and credential management are as per CR.13, CR1.4, CR1.5,
CR 2.8 – Auditable events CR 2.11 – Timestamps	The interfaces implementing the SFRs provide execution status response which can be integrated to the component audit records. It is the component responsibility to implement audit storage, warn on audit record storage capacity threshold reached and response to audit processing failure[2][3]. Secure Data Serialization, Secure Data Serialization (OTFAD) (SoC) and Secure Data Serialization (IEE) (SoC) provide secure storage service that can be used to securely store audit records, including the timestamps. Reliable Index (SoC) provides a time base that can be used to create time stamps for use in audit records. Limited Physical Attacker Resistance provides protections against physical attacks that could affect audit records overall management. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide protections against remote and local logical attacks that could affect audit records overall management.
CR 2.12 – Non-repudiation CR 2.12 – Non-repudiation for all users	Cryptographic Key Generation, Cryptographic Random Number Generation, Cryptographic Operation and Cryptographic KeyStore 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	Secure Debugging and Secure Debugging (SoC) provide protected access to the physical diagnostic and test interfaces of the entire SoC (including the i.MX RT1180 subcomponent). Field Return of Platform and Decommission of Platform provide enablement / disablement of physical diagnostic and test interfaces depending on the life cycle state.
CR 3.1 – Communication integrity CR 3.1(1) – Communication authenticity	Cryptographic Operation provides cryptographic operations that can be used to protect integrity and authenticity of transmitted information. Cryptographic Key Generation and Cryptographic Random Number Generation provide cryptographic functionalities that can be used to generate the cryptographic materiel necessary for the protection of transmitted information.. Cryptographic KeyStore provides secure storage that can be used to store cryptographic material (e.g. shared secret) on which such protections is be based. Limited Physical Attacker Resistance provides protections of cryptographic services involved in secure communication integrity and authenticity enforcement against physical attacks. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide protections of cryptographic services involved in secure communication integrity and authenticity enforcement against remote and local logical attacks.

Table 21. IEC 62443-4-2 security requirements support by i.MX RT1180*...continued*

62443-4-2 requirements	i.MX RT1180 supports
CR 3.2 – Protection from malicious code	Secure Initialization of Platform and Secure Update of Platform provide protection against installation and execution of unauthorized software by checking the integrity and authenticity of the i.MX RT1180 own firmware, as well as the ones of other SoC processors, at each reset, as part of the secure boot. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide isolation of the i.MX RT1180 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 RT1180 is physically isolated from the rest of the SoC by design, using dedicated hardware.
CR 3.3 – Security functionality verification CR 3.3(1) – Security functionality verification during normal operation	The AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities support the components to verify the intended operation of the claimed security functions by requiring the execution of functional and penetration testing to those security functions. Secure Initialization of Platform provides integrity and authenticity verification of the i.MX RT1180 own firmware, as well as the ones of other SoC processors, ensuring a proper helth chack and security configuration at each reset, as part of the secure boot. Attestation of Platform State provides, on demand, the attestation of the state of the i.MX RT1180 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. Limited Physical Attacker Resistance provides monitoring and detecting of physical attacks during operation.
CR 3.4 – Software and information integrity CR 3.4(1) – Authenticity of software and information CR 3.4(2) – Automated notification of integrity violation	Secure Initialization of Platform provides, as part of the secure boot, integrity and authenticity checks of the firmware, software and configuration data of i.MX RT1180 and/or other SoC processors before any execution and will automatically report integrity/authenticity violation through related API. Secure Update of Platform additionally checks the version verification of the i.MX RT1180 firmware/software to be launched and will automatically report versioning violation through related API. Attestation of Platform State and Attestation of Platform Genuineness provide, on demand, the attestation of the state of the i.MX RT1180 subcomponent (including hashes of the firmware and patch, as well as life cycle state). Limited Physical Attacker Resistance ensures the protection of code and data integrity during boot and at runtime against physical attacks. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) ensures the protection of code and data integrity during boot and at runtime against remote and local logical attacks.
CR 3.5 – Input validation	The AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities support the validation of the syntax, length and content of input data by requiring such validation through code review and/or functional testing and/or penetration testing.
CR 3.6 – Deterministic output	The AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities support the verification of deterministic behaviour of the

Table 21. IEC 62443-4-2 security requirements support by i.MX RT1180*...continued*

62443-4-2 requirements	i.MX RT1180 supports
	overall system by checking the correct and expected behavior of the i.MX RT1180 part.
CR 3.7 – Error handling	The AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities support the components to identify and handle error conditions by verifying that no sensitive information that could be used by attackers are outputted by the platform interfaces, in particular when related to cryptographic operations.
CR 3.8 – Session integrity	Cryptographic Random Number Generation provides random number that can be used to generate unique sessions identifiers. Cryptographic Operation provides cryptographic operations that can be used to protect integrity of session.
CR 3.9 – Protection of audit information	Limited Physical Attacker Resistance, Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide protection of execution status of the i.MX RT1180 security services against remote and local, logical and physical attacks. Secure Data Serialization, Secure Data Serialization (OTFAD) (SoC) and Secure Data Serialization (IEE) (SoC) provide secure storage that can be used to protect audit information and logs from unauthorized access and modification.
CR 3.10 - Support for updates CR 3.10(1) - Update authenticity and integrity	Secure Initialization of Platform and Secure Update of Platform provide secure update of the i.MX RT1180 firmware/software parts through the checking of the its integrity, authenticity and version as part of the secure boot.
CR 3.11 - Physical tamper resistance and detection CR 3.11(1) Notification of a tampering attempt	Limited Physical Attacker Resistance provides protections against physical attacks of the i.MX RT1180; fault detections are notified into registers which can be read by the SoC for a notification at the component level.
CR 3.12 - Provisioning product supplier roots of trust	The i.MX RT1180 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 and Cryptographic KeyStore. Limited Physical Attacker Resistance provides protection of product supplier root-of-trust keys and data against physical attacks. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide protection of product supplier root-of-trust keys and data against remote and local logical attacks. Trust Provisionning process is described in Section 3.2.2
CR 3.13 - Provisioning asset owner roots of trust	Cryptographic Key Generation and Cryptographic Operation provides cryptographic services that can be used for the provisioning of asset owner root-of-trust. Cryptographic KeyStore provides secure storage (confidentiality, integrity, authenticity) that can be used to securely store provisioned supplier cryptographic material to be used as a root-of-trust. Limited Physical Attacker Resistance provides protection of asset owner root-of-trust keys and data against physical attacks.

Table 21. IEC 62443-4-2 security requirements support by i.MX RT1180*...continued*

62443-4-2 requirements	i.MX RT1180 supports
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide protection of asset owner root-of-trust keys and data against remote and local logical attacks. Trust Provisionning process is described in Section 3.2.2
CR 3.14 - Integrity of boot process CR 3.14(1) - Authenticity of the boot process	Secure Initialization of Platform provides, as part of the secure boot, integrity and authenticity checks of the firmware, software and configuration data of i.MX RT1180 and other SoC processors before any execution. Limited Physical Attacker Resistance ensures the protection of code and data integrity during boot and at runtime against physical attacks. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) 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, Secure Data Serialization (OTFAD) (SoC), Secure Data Serialization (IEE) (SoC) and Cryptographic KeyStore provide the capability to protect the confidentiality of information at rest in the external NVM and in transit when imported in the i.MX RT1180 for use. Limited Physical Attacker Resistance provides confidentiality protection of the information against physical attacks when manipulated by the i.MX RT1180 services. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide confidentiality protection of the information against remote and local logical attacks when temporarily stored into the i.MX RT1180 services.
CR 4.2 - Information persistence CR 4.2(1) - Erase of shared memory resources	Residual Information Purging and Residual Information Purging (SoC) provide automatic secure erasure of sensitive data when memory is dealicated. Field Return of Platform and Decommission of Platform enrure that sensitive data is made unaccessible when life-cycle state is changed to FIELD RETURN or BRICK state. Cryptographic KeyStore provides secure erasure of cryptographic material. Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust), Software Attacker Resistance: Isolation of Platform (between SPE and NSPE), Software Attacker Resistance: Isolation of Platform (SoC) and Software Attacker Resistance: Isolation of Platform Parts (SoC) provide mediated access to information stored and manipulated inside the i.MX RT1180 subcomponent avoiding having to share critical memory ressources.
CR 4.3 - Use of cryptography	Cryptographic Operation, Cryptographic Key Generation, Cryptographic Random Number Generation and Cryptographic KeyStore provide cryptographic capbilities that can be used by the component. The AVA_VAN (vulnerability analysis) SESIP evaluation activity requires the verification that cryptographic algorithms, used in any security feature, are compliant with internationally recognized and proven security practices and recommendations.

Table 21. IEC 62443-4-2 security requirements support by i.MX RT1180*...continued*

62443-4-2 requirements	i.MX RT1180 supports
CR 5.1 - Network segmentation CR 5.2 - Zone boundary protection CR 5.3 - General-purpose person-to-person communication restrictions	It is the component responsibility to properly implement network segmentation, zone boundary protection, and general-purpose person-to-person communication restrictions. The component may use security services claimed by i.MX RT1180 to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc., however this is to be determined case by case.
CR 6.1 – Audit log accessibility CR 6.1(1) - Programmatic access to audit logs	Secure Data Serialization, Secure Data Serialization (OTFAD) (SoC) and Secure Data Serialization (IEE) (SoC) provide secure storage in which the logs can be stored and accessed only to the authorized processor. Cryptographic Operation, Cryptographic Key Generation, Cryptographic Random Number Generation and Cryptographic KeyStore provide cryptographic features needed to put in place authentication mechanism and granting access to audit log.
CR 6.2 – Continuous monitoring	It is the component responsibility to properly implement monitoring capabilities according to the system requirements. The component may use security services claimed by i.MX RT1180 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 and Attestation of Platform Genuineness provide, on demand, the attestation of the state of the i.MX RT1180 subcomponent (including hashes of the firmware and patch, as well as life cycle state).
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 RT1180 to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc., however this is to be determined case by case.
CR 7.2 – Resource management	It is the component responsibility to properly implement ressource management. The component may use security services claimed by i.MX RT1180 to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc., however this is to be determined case by case.
CR 7.3 – Control system backup CR 7.3(1) – Backup integrity verification	It is the component responsibility to properly implement backup. Cryptographic Operation, Cryptographic Key Generation, Cryptographic Random Number Generation and Cryptographic KeyStore provide cryptographic features that can be used to ensure confidentiality, integrity, and authenticity protection during backup and restore.
CR 7.4 – Control system recovery and reconstitution	It is the component responsibility to properly implement system recovery and reconstruction. The component may use security services claimed by i.MX RT1180 to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc. (e.g. as per CD7.3), however this is to be determined case by case.
CR 7.6 – Network and security configuration settings CR 7.6(1) – Machine-readable reporting of current security settings	It is the component responsibility to properly implement network and security configuration. The component may use security services claimed by i.MX RT1180 to support this requirement, for instance in case Root-of-Trust base, secure cryptography,

Table 21. IEC 62443-4-2 security requirements support by i.MX RT1180*...continued*

62443-4-2 requirements	i.MX RT1180 supports
	or secure storage is needed, etc., however this is to be determined case by case.
CR 7.7 – Least functionality	It is the component responsibility to provide capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services. The AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities support the components to specifically restrict the use of unecessary functions, ports. protocols and/or services by requiring for the i.MX RT1180 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 RT1180 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, Verification of Platform Identity (SoC) and Verification of Platform Instance Identity, provide identification and unique identity of each i.MX RT1180 instance that can be used for component inventory.

[1] CR 1.1(2) "Multifactor authentication for all interfaces" has been removed from the mapping as the platform does not support multifactor authentication. Multifactor authentication must be implemented by the final application based on cryptographic services provided by the platform.
[2] CR 2.9 "Audit storage capacity" has been removed from the mapping because the platform does not provide audit storage. The audit storage must be implemented by the application by collecting the status from platform services execution.
[3] CR 2.10 "Response to audit processing failures" has been removed because the platform does not support audit log generation

5.2 CRA Essential Cybersecurity Requirements support

The table below shows how the platform under evaluation (i.MX RT1180 described in this Security Target) supports the final product, demonstrating compliance with Regulation (EU) 2024/2847 Annex I (see [25]).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 22. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT1180

Requireme ID	Requirement from CRA	i.MX RT1180 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) 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 1.5.8 for which the appropriate assurance level has been determined and described in Section 4.

Table 22. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT1180*...continued*

Requireme ID	Requirement from CRA	i.MX RT1180 supports
		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 of available updates to users, and the option to temporarily postpone them;	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 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	Software Attacker Resistance: Isolation of Platform (SoC) Software Attacker Resistance: Isolation of Platform

Table 22. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT1180*...continued*

Requireme ID	Requirement from CRA	i.MX RT1180 supports
	not limited to authentication, identity or access management systems, and report on possible unauthorised access	(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 (SoC) 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. Limited 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 (SoC) 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 (SoC) 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. Secure Data Serialization (IEE) will ensure confidentiality and binding to the platform instance of data stored in external SDRAM or SPI Flash. Secure Data Serialization (OTFAD) will ensure confidentiality and binding to the platform instance of data stored in external SPI Flash. 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 (with provisioned key) will provide the integrator software with cryptographic services that can be used to encrypt relevant data at rest or in transit

Table 22. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT1180*...continued*

Requirement ID	Requirement from CRA	i.MX RT1180 supports
		Limited 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 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 (SoC) 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 (SoC) 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 (with provisioned key) will provide the integrator software with cryptographic services that can be used to encrypt relevant data at rest or in transit Limited Physical Attacker Resistance will protect the confidentiality of data stored or manipulated inside the platform 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

Table 22. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT1180*...continued*

Requireme ID	Requirement from CRA	i.MX RT1180 supports
		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 and therefore the availability of the essential and basic functions at startup. Software Attacker Resistance: Isolation of Platform (SoC) 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 (SoC) 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. Limited 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 Identity (SoC) 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. 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 (SoC) 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 (SoC) 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.

Table 22. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT1180*...continued*

Requireme ID	Requirement from CRA	i.MX RT1180 supports
		Limited Physical Attacker Resistance will protect the availability of essential and basic functions against physical attacks.
	(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 Secure Debuging(SoC) 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 (SoC) 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 (SoC) 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. Limited 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 Security Requirements and Implementation 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	Secure Update of Platform: this SESIP security claim assesses the implementation of a secure update mechanism of the implementation under evaluation. ALC_FLR: this SESIP evaluation activity assesses that the element under evaluation implements a process of

Table 22. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT1180*...continued*

Requirement ID	Requirement from CRA	i.MX RT1180 supports
	security updates shall be provided separately from functionality updates;	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.
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.	

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 1.0, GPT_SPE_150.
[4] SESIP Profile for PSA Certified Level 3, Version 1.0, PSA JSA, Oct 2022.
[5] SESIP Profile for PSA Certified Level 3 iSE/SE and RoT Component, Version 2.0 BETA, PSA JSA, July 2024

6.2 Developer Documents

[6] i.MX RT1180 Reference Manual, Rev. 8 - 29/06/2025, NXP Semiconductors.
[7] i.MX RT1180 Reference Manual - Schneider Electric, Rev. 9, 2025-07-18, NXP Semiconductors.
[8] i.MX RT1180 Security Reference Manual, Rev. 5 - 2025-07-23, NXP Semiconductors.
[9] i.MX RT1180 Security Reference Manual - Schneider Electric, Rev. 3 - 06/2024, NXP Semiconductors.
[10] i.MX RT1180 Crossover Processors Data Sheet for Industrial Products, Rev. 5 Draft B - 05/2024, NXP Semiconductors.
[11] i.MX RT1180_S High-Performance Processors Data Sheet for Automotive Products, Rev. 2 - 12/2024, NXP Semiconductors.
[12] i.MX RT1180 Crossover Processors Data Sheet for Extended Industrial Products, Rev. 2 Draft B - 12/2024, NXP Semiconductors.
[13] i.MX RT1180 Crossover Processors Data Sheet for Automotive Products, Rev. 1 - 05/2024, NXP Semiconductors.
[14] UG10192 EdgeLock Secure Enclave i.MX RT1180 B0C0 User Guide (FW version v1.1.0 d5a78cba), Rev. 1.2 - 19 November 2025, NXP Semiconductors.
[15] Placeholder, Design of the Entropy Source in the NXP RNG4 Random Number Generator, NXP Semiconductors.
[16] MCUXpressor SDK for MIMXRT1180-EVK with ELE S401 FW v1.1.0, v2.16.000, NXP Semiconductors
[17] Application Notes, AN14227 Secure Boot on i.MX RT118x, Rev. 1.0 - 7 June 2024, NXP Semiconductors
[18] Application Notes, AN14579 Secure Debug on ELE-AP based i.MX SoCs, Rev. 1.0 - 24 February 2025, NXP Semiconductors
[19] Application Notes, AN13023 Selecting and using cryptographic algorithms and protocols, Rev. 1.2 - 16 April 2025, NXP Semiconductors
[20] Secure Provisioning SDK (SPSDK) Application User Guides, Rev. 2.6.0, NXP Semiconductors, https://spsdk.readthedocs.io/
[21] AN6259, Common Trust Provisioning Conceptional Overview, Rev 1.1, NXP Semiconductors, March 2021.

6.3 Standards

[22] NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology, January 2012.
[23] IEC TS 62443-1-1, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, edition 1.0, 2009, the International Electrotechnical Commission (IEC).
[24] IEC 62443-4-1, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements, edition 1.0, 2018, the International Electrotechnical Commission (IEC).

[25] IEC 62443-4-2, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components, edition 1.0, 2019, the International Electrotechnical Commission (IEC).

Legal information

Definitions

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

Disclaimers

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

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

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

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

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

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

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

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

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

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

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

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

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

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

Trademarks

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

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

Tables

Tab. 1. SESIP Profile for Secure MCUs and MPUs Conformance Claims 3
Tab. 2. SESIP Profile for PSA Certified Level 3 Conformance Claims 3
Tab. 3. SESIP Profile for PSA Certified Level 3 iSE/SE and RoT Components Conformance Claims 3
Tab. 4. Platform Reference 4
Tab. 5. Guidance Documents 4
Tab. 6. Platform Deliverables 6
Tab. 7. SDK drivers 8
Tab. 8. Platform Objectives for the Operational Environment 11
Tab. 9. Trust provisioning 13
Tab. 10. Get Info expected values 14
Tab. 11. Get EdgeLock Secure Enclave FIRMWARE VERSION expected values with installed loadable firmware 14
Tab. 12. Cryptographic Operations by ELE-AP 18
Tab. 13. Cryptographic Operations 19
Tab. 14. Cryptographic Key Generation 20
Tab. 15. SESIP3 Sufficiencyfor the SoC 26
Tab. 16. SESIP3 Sufficiency for the Secure Enclave 27
Tab. 17. SESIP Profile for Secure MCUs and MPUs Sufficiency 28
Tab. 18. SESIP Profile for Secure MCUs and MPUs Sufficiency 29
Tab. 19. SESIP Profile for PSA Certified Level 3 Sufficiency 29
Tab. 20. SESIP Profile for PSA Certified Level 3 iSE/SE and RoT Component Sufficiency 30
Tab. 21. IEC 62443-4-2 security requirements support by i.MX RT1180 31
Tab. 22. (EU) 2024/2847 Annex I Essential Cybersecurity Requirements support by i.MX RT1180 39

Figures

Fig. 1. i.MX RT1180 Family Superset Block Diagram 6
Fig. 2. i.MX RT1180 Logical Architecture and Certification Scope 7
Fig. 3. i.MX RT1180 OEM Chip Life Cycle states 9

Contents

1 Introduction 3
1.1 ST Reference 3
1.2 SESIP Profile Reference and Conformance Claims 3
1.3 Platform Reference 3
1.4 Included Guidance Documents 4
1.4.1 Other Certification 4
1.5 Platform Overview and Description 5
1.5.1 Platform Security Features 5
1.5.2 Platform Type 5
1.5.3 Platform Physical Scope 6
1.5.4 Platform Logical Scope 6
1.5.5 Required Non-Platform Hardware/Software/Firmware 8
1.5.6 Life Cycle 8
1.5.7 Configurations 9
1.5.8 Use Case 9
1.5.9 IEC62443-4-2 Considerations 10
2 Security Objectives for the Operational Environment 11
2.1 Platform Objectives for the Operational Environment 11
3 Security Requirements and Implementation 12
3.1 Security Assurance Requirements 12
3.1.1 Flaw Reporting Procedures (ALC_FLR.2) 12
3.2 Security Process Packages (SPPs) 12
3.2.1 IEC 62443-4-1 Secure Development 12
3.2.2 Trust provisioning 13
3.3 Security Functional Requirements for the Secure Enclave 13
3.3.1 Identification and Attestation of Platforms and Applications 13
3.3.1.1 Verification of Platform Identity 13
3.3.1.2 Verification of Platform Instance Identity 14
3.3.1.3 Attestation of Platform Genuineness 15
3.3.1.4 Secure Initialization of Platform 15
3.3.1.5 Attestation of Platform State 16
3.3.2 Product Lifecycle: Factory Reset / Install / Update / Decommission 16
3.3.2.1 Secure Update of Platform 16
3.3.2.2 Decommission of Platform 16
3.3.2.3 Field Return of Platform 16
3.3.3 Secure Communication 17
3.3.3.1 Secure Communication Support 17
3.3.4 Extra Attacker Resistance 17
3.3.4.1 Limited Physical Attacker Resistance 17
3.3.4.2 Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) 18
3.3.4.3 Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) 18
3.3.5 Cryptographic Functionality 18
3.3.5.1 Cryptographic Operation 18
3.3.5.2 Cryptographic Operation (with provisioned key) 19
3.3.5.3 Cryptographic Key Generation 19
3.3.5.4 Cryptographic KeyStore 20
3.3.5.5 Cryptographic Random Number Generation 20
3.3.6 Compliance Functionality 21
3.3.6.1 Secure Data Serialization 21
3.3.6.2 Residual Information Purging 21
3.3.6.3 Reliable Index 21
3.3.6.4 Secure Debugging 22
3.4 Security Functional Requirements for the SoC 22
3.4.1 Identification and Attestation of Platforms and Applications 22
3.4.1.1 Verification of Platform Identity (SoC) 22
3.4.2 Extra Attacker Resistance 23
3.4.2.1 Software Attacker Resistance: Isolation of Platform (SoC) 23
3.4.2.2 Software Attacker Resistance: Isolation of Platform Parts (SoC) 23
3.4.3 Compliance Functionality 23
3.4.3.1 Secure Data Serialization (IEE) (SoC) 23
3.4.3.2 Secure Data Serialization (OTFAD) (SoC) 24
3.4.3.3 Residual Information Purging (SoC) 24
3.4.3.4 Reliable Index (SoC) 24
3.4.3.5 Secure Debugging (SoC) 24
4 Mapping and Sufficiency Rationales 26
4.1 SESIP3 Sufficiency for the SoC 26
4.2 SESIP3 Sufficiency for the Secure Enclave 27
4.3 Conformance Mapping to SESIP Profile for Secure MCUs and MPU for the SoC 28
4.4 Conformance Mapping to SESIP Profile for Secure MCUs and MPUs for the Secure Enclave 28
4.5 Conformance Mapping for SESIP Profile for PSA Certified Level 3 29
4.6 Conformance Mapping for SESIP Profile for PSA Certified Level 3 iSE/SE and RoT Component 30
5 Appendix 31
5.1 IEC 62443 support 31
5.2 CRA Essential Cybersecurity Requirements support 39
6 Bibliography 46
6.1 Evaluation Documents 46
6.2 Developer Documents 46
6.3 Standards 46
Legal information 48