MCX N94x / 54x / 23x

SESIP Security Target

Rev 1.1 — 14 October 2024 **Security Target**

Document information

Info	Content
Keywords	SESIP, PSA, Security Target, MCX N94x, MCX 54x, and MCX N23x
Abstract	Evaluation of the MCX N94x, MCX N54x and MCX N23x developed and provided by NXP Semiconductors, according to SESIP Assurance Level 3 (SESIP3), based on SESIP methodology, version 1.2 and PSA level 3

Revision history

Rev	Date	Description
0.1	2024-15-01	Initial Draft
0.2	2024-25-03	Minor edits
0.3	2024-09-04	Updated to reflect SESIP methodology version 1.2, updated PSA SESIP Profile version, removed TP claim, fixed errors, added attestation and Secure Recovery
0.4	2024-07-05	Minor edits in response to Riscure comments
0.5	2024-13-06	Updated naming convention and included MCX N23x, minor edits
0.6	2024-02-07	New block diagrams, updated guidance documents list, minor edits
1.0	2024-30-08	Final Release
1.1	2024-14-10	Final Release plus NIST 8425 and IEC 62443-4-2 mappings

Contact information

For more information, please visit: http://www.nxp.com

Introduction

This Security Target describes the MCX N94x / 54x / 23x and the core 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].

1.1 ST Reference

MCX N94x / 54x / 23x, SESIP Security Target, Revision 1.1, NXP Semiconductors, 10-14-2024

1.2 Protection Profile Reference and Conformance Claims

Table 1. Protection Profiles Reference and Conformance Claims

Reference	Value
SP Name	GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs [2]
SP Version	Version 1.0
Assurance Claim	SESIP Assurance Level 3 (SESIP3)
Package Claim	Base SP, Package Security Services, Package Software Isolation, Package Hardware Protection, Package Secure Enclave

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

Reference	Value
SP Name	SESIP Profile for PSA Certified Level 3 [3]
SP Version	Version 2.0 BETA 01
Assurance Claim	SESIP Assurance Level 3 (SESIP3)
Optional and Additional SFRs	See Section 4.3

1.3 Platform Reference

Table 3. Platform Reference

Reference	Value	
Platform Name and Version	MCX N94x/54x A1 and MCX N23x A0	
Platform Identification	Chip name and version	See IC hardware in Table 5
	PSA-RoT name and version	See updatable platform RoT in Table 5
Platform Type	Microcontroller platform for IoT applications	
Trusted Subsystem Identification	See security enclave and its software in Table 5	

1.4 Included Guidance Documents

The following documents are included with the platform:

Table 4. Guidance Documents

SESIP Security Target	MCX N94x/54x/23x SESIP Security Target, Revision 1.1, NXP Semiconductors, 14 October 2024
Security Reference Manual	MCX Nx4x Security Reference Manual [4]
Reference Manual	MCXNx4x RM [5]
Datasheet	MCXNx4x DS [6]
API Reference Manual	User Manual of Crypto Library Normal Secure (CLNS) [7]
Application Note	AN969001 - AN14086 Encryption and Decryption for External Memory on SPSDK Tool for MCX N Series (0.1) [8]
Application Note	AN970001 - Encryption and decryption for Internal Memory on SEC tool for MCX N Series (0.1) [9]
Application Note	AN970101 - Enabling Secure Boot and Trust Provisioning on MCX N Series (0.1) [10]
Application Note	AN970201 - Enabling Debug Authentication on MCX N Series for In-field Analysis(0.1) [11]
Application Note	AN970301 - Secure Provisioning Guidelines for MCX N Series MCUs(0.1) [12]
Application Note	AN970601 - Encryption and decryption for External Memory on SEC tool for MCX N Series(0.1) [13]
Application Note	AN970801 - AN14087 Encryption and Decryption for Internal Memory on SPSDK Tool for MCX N Series(0.1) [14]
Tool User Guidance	MCUXpresso Config Tools User’s Guide (IDE) [15]
Security Reference Manual	MCX N23x Security Reference Manual [22]
Reference Manual	MCX N23x RM [23]
Datasheet	MCXN23x DS [24]
Application Note	AN14145 Flash Memory Swap Feature on MCX N Series (Rev. 2) [25]
Application Note	AN14179 - Migration Guide for MCXNx4x to MCXN23x (Rev. 1) [26]

1.5 Other Certifications

The MCX N94x / 54x / 23x development process has followed the 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 62443-4-1:2018 Security for Industrial Automation and Control Systems.

Item	Content
Scheme	IEC 62443-4-1:2018
Certification Body	TÜV SÜD Product Service GmbH
Certification Number	IITS1 109577 0003 Rev. 00
Certification Date	2021-12-10

The entropy source implemented in MCX N94x / 54x / 23x has been ESV (Entropy Source Validation) validated according to NIST SP800-90B [18].

Item	Content
Scheme	Entropy Source Validation
Certification Body	National Institute of Standards and Technology (NIST)
Certification Number	E184
Certification Date	2024-09-03

1.6 Platform Overview and Description

The MCX N94x / 54x are based on dual high-performance Arm® Cortex®-M33 cores running up to 150 MHz, with 2MB of Flash with optional full ECC RAM, a DSP co-processor and an integrated eIQ Neutron NPU. The NPU delivers up to 30x faster machine learning (ML) throughput compared to a CPU core alone enabling it to spend less time awake and reducing overall power consumption.

The multicore design delivers improved system performance and reduced power consumption by enabling smart, efficient distribution of workloads to the analog and digital peripherals. The devices are supported by the MCUXpresso Developer Experience to optimize, ease and help accelerate embedded system development.

The MCX N94x family is geared toward industrial applications with a wider set of analog and motor control peripherals, while the MCX N54x family targets consumer and IoT applications with peripherals ranging from high-speed USB with a PHY to secure digital (SD) and smart card interfaces.

The MCX N23x is based on a high-performance Arm® Cortex®-M33 running up to 150 MHz, with 1MB of Flash, 352 KB ECC RAM and SmartDMA. The MCX N23x is optimized for cost, memory and system performance and offers a single core option with efficient distribution of workloads to the analog and digital peripherals.

1.6.1 Platform Security Features

MCX N94x / 54x / 23x employs a security subsystem, EdgeLock System S50 (ELS S50, legacy names CSS or CSSv2), which together with its driver provides the following security features:

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

On top of ELS S50, MCX N94x / 54x / 23x provides the following security features at the SoC level:

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

Specific to Secure Boot and Update, MCX N94x / 54x / 23x supports:

- Secure boot using ECDSA P-256/384 or CMAC (128 or 256 bits) signed images
- Custom certificate format to validated image public keys
- Up to four revocable Root of Trust (RoT) or Certificate Authority keys, Root of Trust establishment by storing the SHA-2 hash digest of the hashes of up to four RoT public keys
- Anti-rollback feature for firmware update and revocable image signing keys/certificates
- PFR authentication using OTP-eFuse and CMAC computed using DUK (Device Unique Key)
- Image authentication APIs and authentication of XIP images
- Recovery booting of SB3.1 signed and AES encrypted images over serial interfaces (SPI-slave)
- SB commands to program flash, OTP-eFuse, PFR, PUF provisioning, QSPI flash programming (only on MCX N94x/54x), write to RAM and execute RAM (after image authentication), SB commands in recovery boot supports commands including flash/PFR/OTP programming
- SB3 firmware update APIs
- Boot ROM supports Device Identifier Composition Engine (DICE) Specification (version Family 2.0, Level 00 Revision 69) specified by Trusted Computing Group

For more product feature beyond security, refer to Chapter 2 of [5] and [23].

1.6.2 Platform Type

Processor with internal hardware isolation with Arm TrustZone technology for Cortex M, secure memory, and a secure subsystem for use within industrial and consumer IoTapplications.

1.6.3 Platform Physical Scope

The physical scope is the MCX N94x / 54x and MCX N23x microcontroller silicon chip as shown in Figure 1 and Figure 2.

The hardware components and interfaces are listed in Chapter 2 of [5] and [23].

Fig 1. MCX N94x/54x Block Diagram

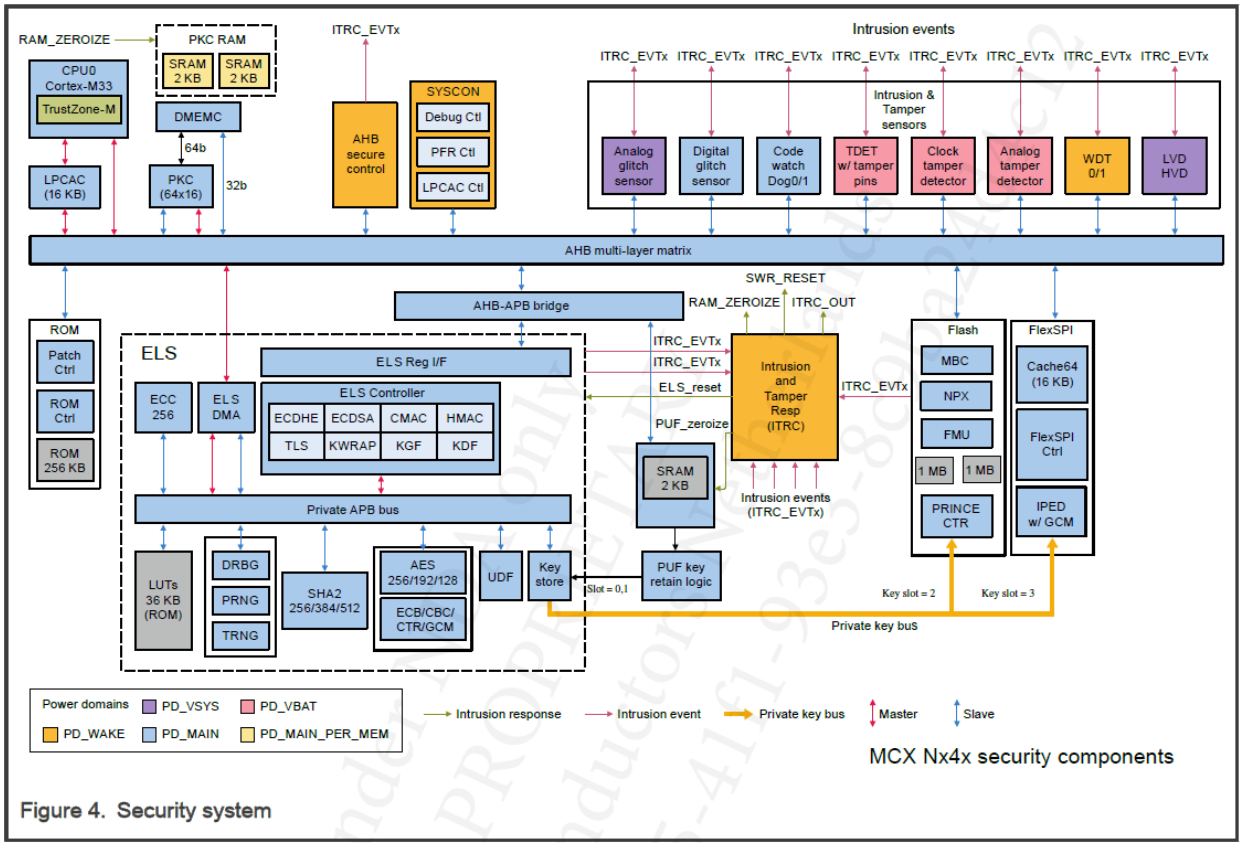

Figure 4. Security system

Fig 2. MCX N23x Block Diagram

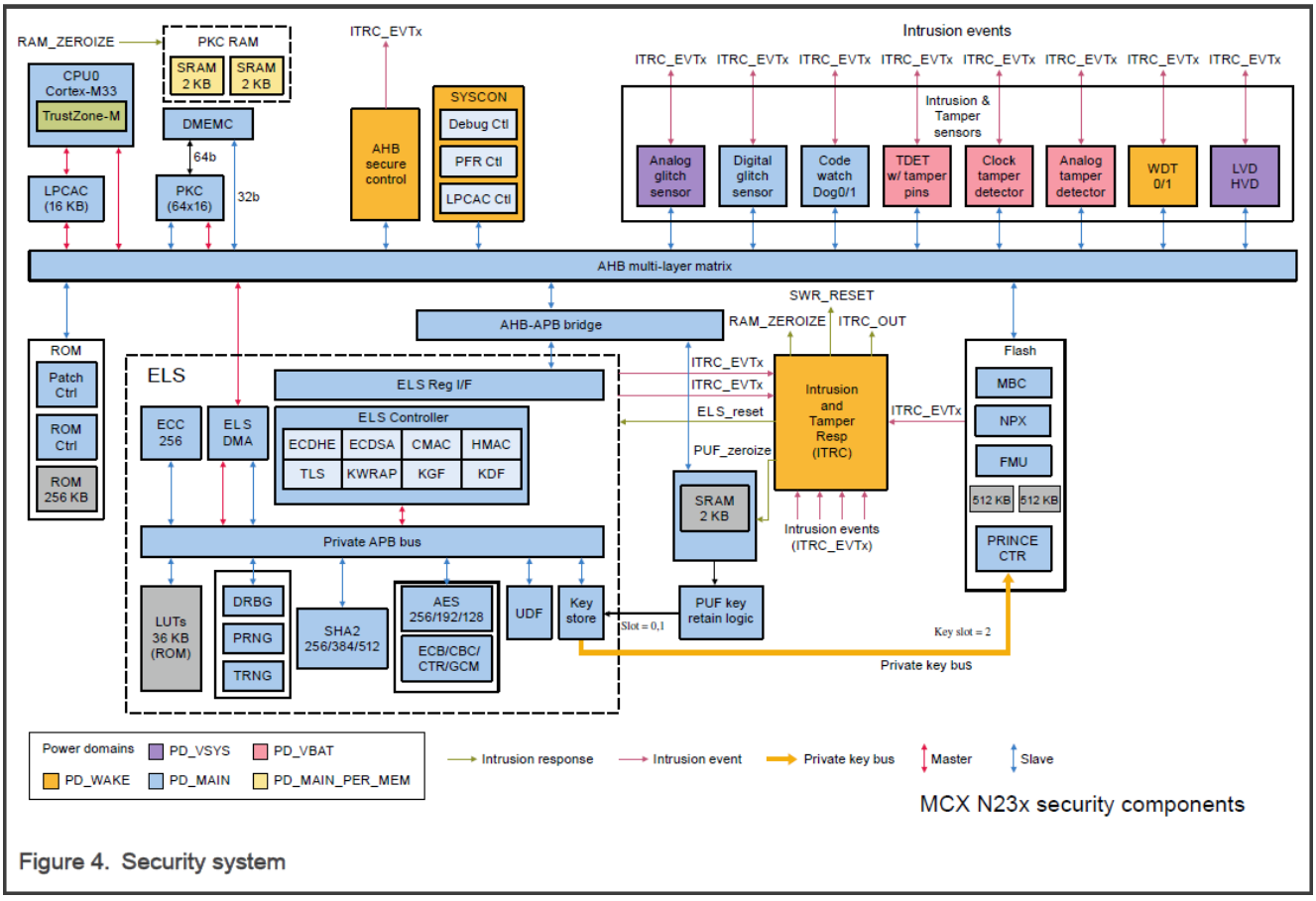

Figure 4. Security system

1.6.4 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 5. Any additional firmware, OS or application software stored on the platform is not in scope of this evaluation. Please see Table 4 for a list of applicable guidance documents.

Table 5. Platform Deliverables

Type	Name	Release	Form of Delivery
IC Hardware	MCX N94x/54x MCX N23x	A1 A0	Silicon Chip
ROM Firmware	MCX N94x/54x ROM MCX N23x ROM	K3.2.0 K3.2.0	Onchip Firmware
ROM Firmware Patch	MCX N94x/54x ROM Patch	T1.1.4 T1.0.4	Onchip Firmware

	MCX N23x ROM Patch		
Security Enclave	MCX N94x/54x EdgeLock System S50 (ELS 50) MCX N23x EdgeLock System S50 (ELS 50)	3.04.6 3.09.1	Onchip Hardware Subsystem
Security Enclave Software	MCX N94x/54x/23x ELS S50 software (microcode)	2.04.0	Onchip ROM firmware
Updatable Platform RoT	MCX N94x/54x SDK MCX N23x SDK	SDK_2_14_0_FRDM-MCXN947 with Attestation Demonstration SDK_2_14_0_FRDM-MCXN236	Software Package
Crypto Library	Crypto Library Normal Secure for MCX N94x/54x SDK Crypto Library Normal Secure for MCX N23x SDK	Clns-SDK_v1.7.0 Clns-SDK_v1.7.0	Included in Software Package

Fig 3. Logical Architecture and Certification Scope

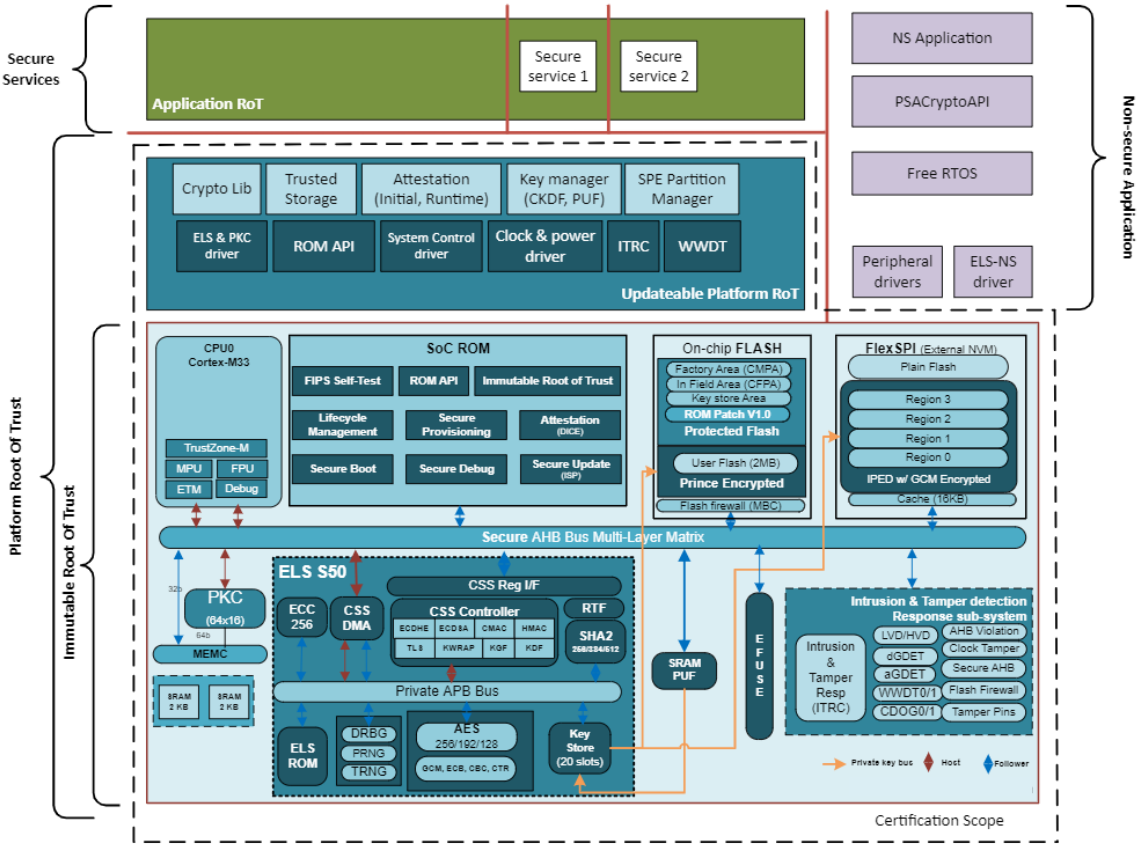

*Figure 3 depicts MCX N94x/54x only. Refer to Figure 1 and Figure 2 in Section 1.6.3 for differences between MCX N94x/54x and MCX N23x.

1.6.5 Required Non-Platform Hardware/Software/Firmware

No additional non-platform hardware, software or firmware is required for the correct functioning of the security claims described in this document except for Section 3.3.5.3. For security claim of Section 3.3.5.3, compatible external non-volatile memory shall be deployed via FlexSPI for MCX N94x and N54x. See Chapter 4.3 of [6] for more information. External non-volatile memory is not required for MCX N23x.

1.6.6 Life Cycle

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

The boot ROM is responsible for checking the Life-Cycle state. Based on the Life-Cycle state, the ROM determines what boot flow is used, including whether control is passed to application code or not. The ROM

also handles the opening of test and debug ports based on the Life-Cycle state. If the part is in the Bricked state or any invalid life cycle state, then the ROM will lock the part.

See more in Chapter 5 of [4] and [22].

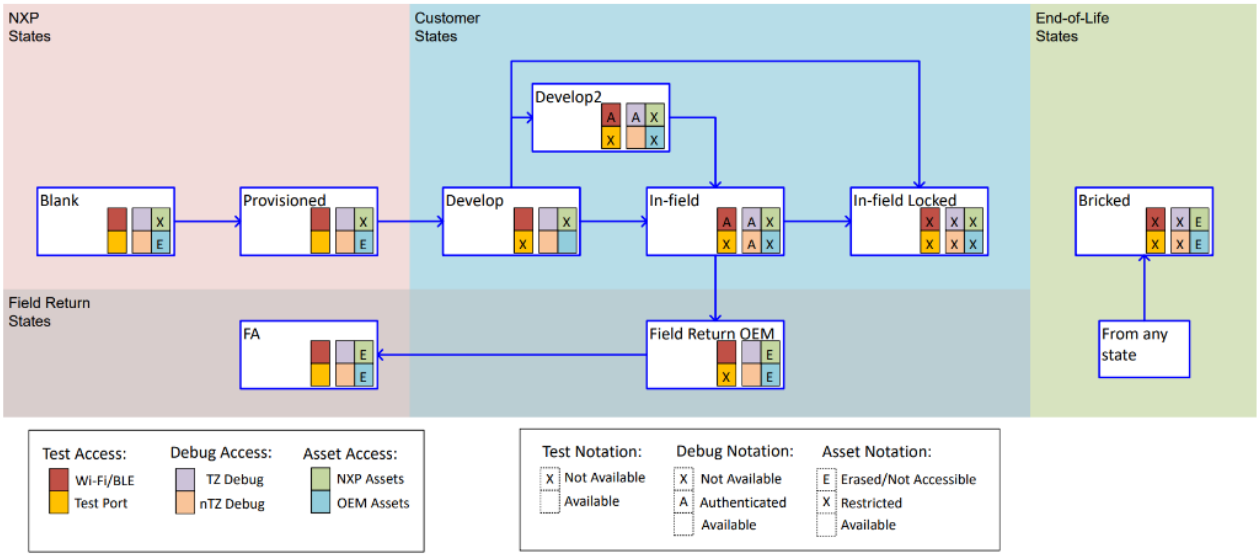

Fig 4. MCX N94x / 54x / 23x Security Life-Cycle States

1.6.7 Configurations

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

The security features discussed above 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

A Secure Enclave is used to fulfil the following security features as described in Section 3.2.

1.6.8 Use Case

[any user]

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

[any code]

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

Security Objectives for the Operational Environment

2.1 Platform Objectives for the Operational Environment

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

Table 6. Platform Objectives for the Operational Environment

Title	Description	Reference
Platform Verification	The operating system or host application code is expected to verify the correct version of all platform components that it depends on, as described in Section 3.4.1 in of this document.	Section 3.4.1
Secure Boot	The operating system or host application code is expected to make use of the feature as described in Chapter 9 of [4] and [23].	Chapter 9 of [4], [22] and [10]
Secure Debug	The integrating environment is expected to configure the debug functionality as described in Chapter 16 of [5] and [11] to meet the extra physical attacker resistance.	Chapter 16 of [5], Chaper 13 of [23] and [11]
Key Management	Cryptographic keys and certificates outside of the Platform are subject to secure key management procedures.	This document
Trusted Users	Actors in charge of platform management, for instance for signature of firmware update, are trusted.	This document
SW Integration	The operating system or application code are expected to ensure the correct version of the crypto library and SDK drivers are integrated and configured.	This document
Secure Update and Key Revoke	The operating system or application code are expected to update an image with proper remedy solution and version increased and/or revoke key in case of security incidence occurrence of the image and/or the key.	Chapter 9 of [4], [22]
Lifecycle Management	The operating system or application code are expected to provide lifecycle states and secure mechanism of lifecycle state transition according to the use case, and the operational environment is expected to configure the platform accordingly for lifecycle state transitions. In general, the operating system or application code are expected to configure the platform to Infield or in-field locked state.	Chapter 5 of [4], [22]
Software Isolation	MCX N94x / 54x / 23x provides two different isolation mechanisms: S50 vs rest of SoC, and TrustZone Secure vs Non-secure. The operating system or application code are expected to configure and utilize at least one mechanism for isolation between platform and application.	Chapters 13 of [4], [22] and [19]
Physical Attacker Resistance Configurations	If local physical attack is applicable for the use cases, the following configurations shall apply: • The operating system or application code are expected to configure the `main_clk` to one of the internal clock sources; • The operating system or application code are expected to keep the ITRC output configured to `CHIP_RESET`; • The operating system or application code are expected to configure the security sensor settings as the `helloworld` example in SDK at application initialization; • The operating system or application code are expected not to be executed from external flash with XIP mode. • The operating system or application code are expected not to use printf or any external console output functions in secure partition. • ARM CM33 CPU is not hardened against physical attacks, e.g., voltage glitching or EMFI. It is therefore recommended to harden secure application	This document, [15], Chapters 33.1, 33.2 and 42 of [5], Chapters 24.1, 24.2 and 32 of [23], MCX Nx4x SDK_2_14_0_FRDM-MCXN947 with Attestation Demonstration, and SDK_2_14_0_FRDM-MCXN236

	against such attacks using software-based countermeasures and leverage code watchdog offered by MCX N94x / 54x / 23x.	

Security Requirements and Implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is: SESIP3 as defined in Chapter 4 of GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 [1].

3.1.1 Flaw Reporting Procedures (ALC_FLR.2)

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

NXP has defined a Product Security Incident Response Process (PSIRP), implemented by a dedicated team (PSIRT). This process provides a publicly available interface (https://nxp.com/psirt), and includes 4 steps:

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

The platform's secure boot feature is able to verify the integrity of its loadable firmware part; it also provides an appropriate mechanism for the update of its own loadable firmware. The firmware update mechanism will prevent the rollback of flash firmware by ensuring that the major version number of the firmware download is numerically greater than or equal to the existing firmware major version (indicating a "newer" firmware version has been downloaded).

3.2 Security Functional Requirements for Security Enclave

MCX N94x / 54x / 23x employs a security enclave: EdgeLock System S50 (ELS S50), which fulfills the following security functional requirements:

3.2.1 Identification and Attestation of Platforms and Applications

3.2.1.1 Verification of Platform Identity

Requirement

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

Conformance rationale:

The ELS S50 version is available from `ELS_VERSION`. The values shall match the versions indicated in Table 5. See more in Chapter 13 of [4], [22].

3.2.2 Extra Attacker Resistance

3.2.2.1 Software Attacker Resistance: Isolation of Platform Parts

Requirement

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

Conformance rationale:

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

ELS S50 has its own controller and exclusive system resources with enforced access control, hence it is isolated from the rest of platform. See more in Chapter 13 of [4], [22].

3.2.3 Cryptographic Functionality

3.2.3.1 Cryptographic Operation

Requirement

The platform provides operations in Table 7 functionality with algorithms in Table 7 as specified in specifications in Table 7 for key lengths described in Table 7 and modes described in Table 7.

Table 7. Cryptographic Operations by ELS S50

Operation	Algorithm	Specification	Key Lengths	Modes
Encryption and decryption	AES	NIST FIPS 197	128, 192, 256	ECB, CBC, CTR
Authenticated Encryption, Authenticated Decryption	AES	NIST SP800-38D	128, 192, 256	GCM
Hashing	SHA2	NIST FIPS 180-4	224, 256, 384, 512	N/A
MAC generation and verification	HMAC	RFC2104	Up to 512	SHA-256
MAC generation and verification	CMAC	RFC4493	128, 256	AES
Signature generation and verification	ECDSA	NIST FIPS 186-5	256	Secp256r1

Conformance Rationale

The crypto coprocessors are located in ELS S50. ELS S50 provides symmetric encryption/decryption, hashing, and asymmetric functions. See more in Chapter 13 of [4], [22].

3.2.3.2 Cryptographic Key Generation

Requirement

The platform provides a way to generate cryptographic keys for use in algorithms in Table 8 as specified in specifications in Table 8 for key lengths described in Table 8.

Table 8. Cryptographic Key Generation

ID	Algorithm	Specification	Key Lengths
ECDSA	ECDSA	NIST FIPS 186-5	256
HKDF	HKDF	RFC5869	128, 256
CKDF	CKDF	NIST SP800-108	128, 256
TLS KDF	TLS Master Key Derivation	TLS 1.2	N/A
TLS KDF	TLS Session Key Derivation	TLS 1.2	N/A
ECDH	ECDH	NIST SP800-56A	256

Conformance Rationale

The ELS S50 also provides key generation service. See more in Chapter 13 of [4], [22].

3.2.3.3 Cryptographic KeyStore

Requirement

The platform provides a way to store cryptographic keys such that not even the application can compromise the *confidentiality, integrity, authenticity* of this data. This data can be used for the cryptographic operations *encryption, decryption, signature generation, MAC generation, key derivation, shared secret generation*.

Conformance Rationale

ELS S50 provides key store function. Keys can be stored in ELS in a bank of internal 128-bit registers (each register is called a "key slot"). Specifically, their values (the key material) cannot be accessed by the system. Keys in KeyStore can be created by key exchange and key derivation functions in Section 3.3.3.2, key generation function in Section 3.3.3.2, unwrapping externally wrapped key per NIST SP 800-38F, or imported from unique key derived from PUF. Each Keystore Key has associated properties and ELS S50 enforces usage rules based on the properties of keys. See more in Chapter 13 of [4], [22].

3.2.3.4 Cryptographic Random Number Generation

Requirement

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

ELS S50 has physical true random number generator used to seed an internal DRBG module as defined in NIST SP 800-90A. The TRNG achieves NIST SP 800-90B compliance.

Furthermore:

- TRNG is capable of passing AIS 31 statistical tests T0-T8

See more in Chapters 13 of [4], [22].

3.2.4 Compliance Functionality

3.2.4.1 Residual Information Purging

Requirement

The platform ensures that *key store areas*, with the exception of *none*, is erased using the method specified in Chapter 13 of [4], [22] before the memory is (re)used by the platform or application again and before an attacker can access it.

Conformance Rationale

ELS S50 provide KDELETE command which removes the key and zeroizes the register. See more in Chapter 13 of [4], [22].

3.3 Security Functional Requirements for SoC

In the following Security Functional Requirements, the term **platform** covers the **MCX N94x / 54x / 23x physical and logical scope**, and the term **application** refers to any additional firmware, OS or application software which is outside of the evaluation scope. It represents a part of the final connected device.

MCX N94x / 54x / 23x fulfils the following security functional requirements:

3.3.1 Identification and Attestation of Platforms and Applications

3.3.1.1 Verification of Platform Identity

Requirement

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

Conformance Rationale

Besides reading out ELS S50 HW and driver version as introduced in Section 3.3.1.1, SoC Hardware and ROM identifier and revision number can be read from `CHIP_INFO` register and one way to do so is to use `GetProperty` command in ISP mode as specified in Section 7.5.16 of [4], 7.5.2 and 7.5.3 of [22],14.5.15 of [5] and 11.5.15 of [23] with tag 10h. The return value shall match the value in Chapter 17.4.1.132 of [5] and 14.4.1.91 of [23] and the version shall match the value indicated in Section 1.6.4.

The ROM patch revision is stored in protected flash, which can be read via ISP mode or ROM API, and the return value shall be the same as Section 1.6.4.

The Updatable Platform RoT Firmware is delivered in logical format as a software library. One can identify the version in a readme file and verify the commit hash as defined in Section 1.6.4.

3.3.1.2 Verification of Platform Instance Identity

Requirement

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

Conformance Rationale

The platform stores a 128-bit IETF RFC4122 compliant non-sequential Universally Unique Identifier (UUID). It can be read from protected flash (address 0x0110_0000 - 0x0110_000F). One way to read out UUID is to use `GetProperty` command in ISP mode with tag 12h as specified in Chapter 7.5.16 of [4] and 7.5.2 of [22].

Furthermore, MCX N94x / 54x / 23x supports Device Identifier Composition Engine (DICE) Specification (version Family 2.0, Level 00 Revision 69) specified by Trusted Computing Group, which provides another way to uniquely identify a product instance.

NXP also provide trust provisioning service, where a certificate is injected during NXP manufacturing which can be used to verify the platform instance identity and genuineness. See more in [16].

3.3.1.3 Attestation of Platform Genuineness

Requirement

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

Conformance Rationale

Secure Attestation is a set of mechanisms used to provide evidence to a remote party on the device’s genuine identity, its software and firmware versions, as well as its integrity and lifecycle state. Device Identity Composition Engine (DICE), as defined by Trusted Computing Group, uses Immutable RoT during boot time to create a unique Device Identity which takes into account Unique Device Secret (UDS), hardware state of the device and its firmware. Runtime Fingerprint (RTF) is the NXP-proprietary attestation mechanism, which measures the device’s state during boot-time and run-time as well. See more in [19].

Trust provisioning is a process used for creation of initial Device Identity keys. Its major objective is to provide a cryptographic proof of the device’s origin and to offer a set of tools to OEM for secure provisioning of their own assets. A device-unique private-public key pair is created on every device, the public portion of which is collected and signed by NXP. That signed public key is installed back onto every device in a form of device-unique certificate, which serves the actual proof of the device’s origin. See more in [16].

3.3.1.4 Attestation of Platform State

Requirement

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

Conformance Rationale

See Section 3.3.1.3.

3.3.1.5 Attestation of Application Genuineness

Requirement

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

Conformance Rationale

See Section 3.3.1.3.

3.3.1.6 Attestation of Application State

Requirement

The platform provides an attestation of the state of the application.

Conformance Rationale

See Section 3.3.1.3.

3.3.1.7 Secure Initialization of Platform

Requirement

The platform ensures its integrity and authenticity during the platform initialization. If the platform integrity or authenticity cannot be ensured, the platform will go to a limited availability mode in which only Test or Download modes, subject to further authentication, can be entered.

Conformance Rationale

The secure part of the ROM bootloader of MCX N94x / 54x / 23x provides secure boot operation. Secure boot prevents unauthorized code from being executed on a given product. To ensure this level of security, secure boot always leaves the device ROM in an executing mode when coming out of a reset. The ROM can then assess the first user executable image resident in the flash memory and determine the authenticity of that code. The control is transferred to authentic code only. A chain of trusted code from the ROM to the user boot code is established. And the chain can be further extended through the verification of digital signatures associated with additional code layers.

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

The operating system or application code has the option to further enable built-in selftests in Secure Boot ROM to ease the certification of NIST CMVP. See more in Chapter 3.5 of [4] and [22].

The boot ROM supports dual image boot for internal flash memory. This means that two boot images can be placed in the flash memory region. The boot ROM decides which image to boot first based on the image version. It boots the one with the newer image version first, and in case of a failure, it boots the older one. See Chapter 8.3.1 of [4] and [22].

MCX N94x and N54x also support secure boot from the FlexSPI interface, which can be used for external flash boot as well as ease for the OEM manufacturer. The FlexSPI interface is not supported in N23x.

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

3.3.2.1 Secure Update of Platform

Requirement

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

Conformance rationale:

The secure part of the ROM bootloader of MCX N94x / 54x / 23x provides a secure firmware update operation. Secure Update is the process used to securely update the firmware image in the field. The firmware image is encrypted using AES-128 or AES-256 and signed using ECDSA P-256 or ECDSA P-384, following the SB3.1 firmware image format. Secure Update guarantees authenticity and confidentiality of the new image. It also ensures that the new image is up-to-date, preventing the rollback to an older image. Running firmware is in charge of receiving and verifying the new firmware image. The follow-up Secure Boot verifies the new firmware image again, making sure the Immutable RoT is still in charge of ensuring authenticity of the latest firmware.

The anti-rollback is achieved by OTP fuseword. The OTP fusemap contains monotonic counters or ROTKH revocation fields that can be updated as these are implemented as redundant 16-bit fusewords. See more in 3.6 of [4] and [22].

The dual image boot and secure boot from the FlexSPI interface provides recovery capability for the device. See more in Section 3.3.1.7. Note that FlexSPI is not support in N23x.

Furthermore, a trust provisioned private key, together with other pre-installed key material, is then used for authentication and secure connection to the device, enabling secure provisioning of OEM assets even in the manufacturing environment OEM may not fully trust. See more in [16].

3.3.2.2 Field Return of Platform

Requirement

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

Conformance Rationale

MCX N94x / 54x / 23x provides a secure Field Return feature.

In the Field Return OEM state, every boot ROM verifies that the customer key store (0x0100_4000 - 0x0100_5FFF) is blank. If not, erases before opening debug access. PUF and ELS S50 modules are put in FA mode which will re-key all application usage keys including memory encryption Prince keys. This mechanism protects leakage of any residue data left during life-cycle state transition.

It can further move to FA life cycle state if the device is being returned to NXP for testing and failure analysis, and further sensitive information is erased. See more in Chapters 5.1.5.1 of [4] and [22].

3.3.2.3 Decommission of Platform

Requirement

The platform can be decommissioned.

Conformance Rationale

The End-of-Life security life cycle state, or Bricked State, can be used by customers or NXP to remove a chip permanently from regular use and erase/block access to secrets inside the chip. Bricked is the final life cycle state, so the device cannot be advanced to any other states from Bricked. See more in Chapter 5.1.6 in [4] and [22].

3.3.3 Extra Attacker Resistance

3.3.3.1 Physical Attack Resistance

Requirement

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

Conformance Rationale

MCX N94x / 54x / 23x is equipped with Intrusion and Tamper Response Controller (ITRC). ITRC provides mechanism to configure the response action for an intrusion event detected by an on chip security sensors. Intrusion Response is the action a device performs in order to prevent misuse of the device or disclosure of critical assets (cryptographic keys, personal data) that are generated or stored within the device. The response mechanism is typically triggered by either a signal from an on-chip sensor designed to detect that the device is in a threat condition or by an explicit command provided by the software. See more in Chapter 20 of [4] and [22].

Also, the software components including ROM leverage the code watchdog. For code watchdog, see more in Chapter 18 of [4] and [22]. The crypto coprocessor and the library are secure hardened against potential physical attacks.

Furthermore, this device has one instance of the independent real time clock, RTC. This block is a low power module that provides time keeping and calendaring functions, protection against spurious memory/register updates and battery operation. See Chapter 56 of [5] and Chapter 42 of [23]. This function provides another layer of protection yet needs further HW support at board level, hence, not in the evaluation scope.

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

Requirement

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 security functional requirements.

Conformance Rationale

There are multiple isolation features presented in the platform.

The ELS S50 module is a security subsystem supporting a wide range of cryptographic algorithms and providing strong key isolation from the rest of the system. When embedded in an SoC, ELS S50 serves as the main building block of the SoC's immutable Root of Trust. It is used as part of the trust anchor during secure boot, secure debug access, life-cycle management, and trust provisioning. ELS S50 has its own controller and exclusive system resources with enforced access control, hence it is isolated from the rest of platform. See more in Chapter 13 of [4] and [22].

PRINCE-based memory encryption also ensures Secure Isolation between multiple IP vendors. Initial Vector (IV) is derived by secure-privilege and a different value is used for every independent memory region, ensuring the isolation between each other. See more in Chapter 3.8 of [4] and [22].

Furthermore, MCX N94x / 54x / 23x provides Protected Flash Region (PFR) and ROM API to flash firewall setup and access control. See more Chapter 8.5 of [4] and [22].

ARM TrustZone enables Secure Isolation during run-time by providing four distinct levels of privilege: secure-privilege, secure-user, non-secure-privilege, non-secure user. Every peripheral is equipped with Peripheral Protection Checker (PPC) that can be programmed to control access to that peripheral, following the ARM TrustZone philosophy. Every memory is equipped with Memory Protection Checker (MPC) that can also be programmed in the same way as the PPC. Secure AHB Controller is in charge of programming all PPC and MPC blocks and only the highest level of privilege, which is secure-privilege, is allowed to do that. See more in Chapter 3.9 of [4] and [22].

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

Requirement

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 security functional requirements.

Conformance rationale:

The isolation between PSA-RoT and Application Root of Trust Services is included in Section 3.3.3.2.

Also see more in Section 3.4.4.3.

3.3.3.4 Software Attacker Resistance: Isolation of Platform Parts

See Section 3.3.2.1.

3.3.4 Cryptographic Functionality

3.3.4.1 Cryptographic Operation

Requirement

The platform provides operations in Table 10 and Table 11 functionality with algorithms in Table 10 and Table 11 as specified in specifications in Table 10 and Table 11 for key lengths described in Table 10 and Table 11 and modes described in Table 10 and Table 11.

Table 9. Cryptographic Operations provided outside of ELS S50

Operation	Algorithm	Specification	Key Lengths	Modes
Signature generation and verification	EdDSA	NIST FIPS 186-5	255	Ed25519
Signature generation and verification	ECDSA	NIST FIPS 186-5	192, 224, 256, 384, 521	secpXXXr1, XXX = key length
			192, 224, 256	secpYYYk1, YYY = key length
			160, 192, 224, 256, 320, 384, 512	brainpoolPZZZr1, ZZZ = key length
Signature generation and verification	RSA	PKCS v1.5 and RSA PSS	2048, 3072, 4096	N/A

Conformance rationale:

On top of ELS S50 security coprocessor introduced in Section 3.3.3.3, MCX N94x / 54x / 23x also deploys Public-Key Crypto Coprocessor (PKC, Chapter 16 of [4] and [22]). The Crypto Library has been developed leveraging ELS S50 and PKC.

3.3.4.2 Cryptographic Key Generation

Requirement

The platform provides a way to generate cryptographic keys for use in algorithms in Table 8 as specified in specifications in Table 8 for key lengths described in Table 8.

Table 10. Cryptographic Key Generation

ID	Algorithm	Specification	Key Lengths

AES	AES	NIST SP800-133	128, 192, 256
ECC	ECC	ANSI X9.62	160, 192, 224, 255, 256, 320, 384, 512, 521
RSA	RSA	PKCS#1	2048, 3072, 4096
ECDH	ECDH	NIST SP800-56A	255 (Curve25519), 448 (Curve448)
			192, 224, 256, 384, 521 (secpXXXr1, XXX = key length)
			192, 224, 256 (secpYYYk1, YYY = key length)
			160, 192, 224, 256, 320, 384, 512 (brainpoolPZZZr1, ZZZ = key length)

Conformance rationale:

The crypto library also provides a key generation service leveraging the coprocessors.

3.3.4.3 Cryptographic Key Store

Requirement

The platform provides a way to store cryptographic keys such that not even the application can compromise the *confidentiality, integrity, authenticity* of this data. This data can be used for the cryptographic operations *encryption*, *decryption*, *signature generation*, *MAC generation and verification*, *key derivation*, *shared secret generation*.

Conformance rationale:

ELS S50 provides key store function. The input key is one of the following:

1. The device unique key (DUK), a master key which is transferred from PUF via a dedicated hardware interface.

2. An encrypted (wrapped) key in system memory. KeyIn unwraps these keys before writing them to keystore. ELS S50 key wrapping uses the algorithm defined in the RFC3394 standard.

See more in Chapter 13.4.2.7 of [4] and [22].

One can further use Physically Unclonable Function (PUF) for keystore. See more in Chapter 14 of [4] and [22].

3.3.4.4 Cryptographic Random Number Generation

Requirement

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

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

Conformance rationale:

There is one RNG instance in MCX N94x / 54x /23x located inside ELS S50 as stated in Section 3.3.3.4.

3.3.5 Compliance Functionality

3.3.5.1 Secure Data Serialization

Requirement

The platform ensures that all data stored outside the direct control of the platform, except for *data not stored in the configured address area,* is protected such that the *confidentiality, integrity, authenticity and binding to platform instance* is ensured.

Conformance rationale:

External flash storage can also be encrypted by PRINCE algorithm GCM mode using IPED engine to achieve authenticity and confidentiality (see more in Chapter 12 in [5], and Chapters 7.3 and 7.4 of [4]. The key is stored in ELS S50 and derived from PUF which also provides binding to platform instance. See more in Chapter 10.9.3 of [4].

Note that external flash storage is not applicable for MCX N23x therefore, Secure Data Serialization does not apply to MCX N23x.

3.3.5.2 Secure Debugging

Requirement

The platform only provides *Arm's Serial Wire Debug (SWD) interface* authenticated as specified in Section 1 of [11] with debug functionality.

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

Conformance rationale:

The fundamental principles of debugging, which require access to the system state and system information, conflict with the principles of security, which require the restriction of access to assets. Thus, many products disable debug access completely before deploying the product. This causes challenges for product design teams to do proper Return Material Analysis (RMA). To address these challenges, the chip offers a debug authentication protocol as a mechanism to authenticate the debugger (an external entity) has the credentials approved by the product manufacturer before granting debug access to the device.

The debug authentication is a challenge-response scheme and assures that only the debugger in possession of the required 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 Chapter 16 of [5], Chapter 13 of [23], and [11].

3.3.5.3 Secure Recovery

Requirement

The platform detects anomalies <image authentication failure> and recovers to return to a known state <application>.

Conformance rationale:

The Boot ROM supports recovery boot from an external 1-bit SPI flash memory device or an image loaded into IFR0. See more in Chapter 8.3.3 in [4] and [22].

Also, see Section 3.3.1.7 and Section 3.3.2.1.

3.3.5.4 Residual Information Purging

Requirement

The platform ensures that *key store areas*, with the exception of *none*, is erased using the method specified in *Chapter 13.4.2.9 of [4] and [22]* before the memory is (re)used by the platform or application again and before an attacker can access it.

The platform ensures that *PUF derived data, ELS stored keys and IPED protected memory*, with the exception of *none*, is erased using the method specified in *Section Chapters 5.1.5.1 and Chapter 5.1.6 of [4] and [22]* before the memory is (re)used by the platform or application again and before an attacker can access it.

Conformance rationale:

ELS S50 provide KDELETE command which removes the key and zeroizes the register. See more in Chapter 13.4.2.9 of [4] and [22].

Entering the FA Mode or Bulk Erase Flash purges sensitive data. See more in Section 3.3.2.2 and Section 3.3.2.3.

3.3.5.5 Reliable Index

Requirement

The platform implements a strictly increasing function.

Conformance rationale:

MCX N94x / 54x / 23x provides fuses for customer definition and usage which can be used as reliable index due to the irreversible nature. The fuse programming and readout is achieved by ROM API. MCX N94x / 54x / 23x also provides several monotonic counter and monotonic flag fields in CFPA (customer Field Programmable protected flash Area). See more in Section 13 of [5], and Chapter 10 of [23].

Mapping and Sufficiency Rationales

4.1 SESIP3 Sufficiency

Table 11. Rationale for SESIP3 Sufficiency

Assurance Class	Assurance Family	Covered by	Rationale
ASE: Security Target Evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in Section 1.1, the platform reference is in Section 1.3 and the platform overview and description is 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 guidance documents.
	ASE_REQ.3 Listed Security requirements	Security Requirements and Implementation	All SFRs in this ST are taken from [1]. SFR "Identification of Platform Type" is included. SFR "Secure Update of Platform" is mentioned but

			refers to ALC_FLR.2.
	ASE_TSS.1 TOE Summary Specification	Security Requirements and Implementation	All SFRs are listed per definition, and for each SFR the implementation and rationale are provided in the SFR.
ADV: Development	ADV_FSP.4 Complete functional specification	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: Tests	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_VAN.2	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 platform. Penetration testing is performed by the evaluator assuming an attack potential of Enhanced-Basic.

4.2 Conformance Mapping for SESIP Profile for Secure MCUs and MPUs

This section provides rationales of conformance claimed in Section 1.2

Table 12. SESIP Profile for Secure MCUs and MPUs Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.3.1.1
	Secure Initialization of Platform	Section 3.3.1.7
	Secure Update of Platform	Section 3.3.2.1
	Residual Information Purging	Section 3.3.5.4
	Secure Debugging	Section 3.3.5.2
Security Services	Cryptographic Operation	Section 3.3.4.1
	Cryptographic Key Generation	Section 3.3.4.2
	Cryptographic Key Store	Section 3.3.4.3
	Cryptographic Random Number Generation	Section 3.3.4.4
Software Isolation	Software Attacker Resistance: Isolation of Platform	Section 3.3.3.2 and Section 3.3.3.3
Hardware Protections	Physical Attacker Resistance	Section 3.3.3.1
Secure Enclave	Software Attacker Resistance: Isolation of Platform Parts and SFRs per Section 3.3	Section 3.2.2.1 and Section 3.3
Additional Security Functional Requirements (Optional)	Verification of Platform Instance Identity	Section 3.3.1.2
	Verification of Platform Genuineness	Section 3.3.1.3
	Attestation of Platform State	Section 3.3.1.4
	Decommission of Platform	Section 3.3.2.3
	Field Return of Platform	Section 3.3.2.2
	Secure Data Serialization	Section 3.3.5.1

4.3 Conformance Mapping for SESIP Profile for PSA Certified Level 3

This section provides rationales of conformance claimed in Section 1.2

Table 13. SESIP Profile for PSA Certified Level 3 Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.3.1.1
	Verification of Platform Instance Identity	Section 3.3.1.2
	Verification of Platform Genuineness	Section 3.3.1.3

	Secure Initialization of Platform	Section 3.3.1.7
	Attestation of Platform State	Section 3.3.1.4
	Secure Update of Platform	Section 3.3.2.1
	Physical Attacker Resistance	Section 3.3.3.1
	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Section 3.3.3.2
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	Section 3.3.3.3
	Cryptographic Operation	Section 3.3.4.1
	Cryptographic Key Generation	Section 3.3.4.2
	Cryptographic Key Store	Section 3.3.4.3
	Cryptographic Random Number Generation	Section 3.3.4.4
Optional SFR	Secure Debugging	Section 3.3.5.2
	Secure Data Serialization	Section 3.3.5.1

4.4 ETSI EN 303 645 Mapping and Sufficiency

ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements [20] is released by European Telecommunications Standard Institute (ETSI), and as its title suggests, it intends to prepare consumer IoT devices with a set of baseline requirements to address common cybersecurity threats. SESIP methodology is acknowledged as one of the schemes that aligning with EN 303 645.2 GlobalPlatform also released a white paper on SESIP Applicability for EN 303 645 [21]. Yet at the time of writing, there is no recognized SESIP mapping to EN 303 645 released, hence NXP provides the following informative mapping and self-assessment towards EN 303 645 sufficiency rational from this evaluation. The mapping and rational is provided under each EN 303 645 provision entry, and for complete requirements by EN 303 645 provision, please refer to original text of [20].

This section refers to the claims and activities within this SESIP evaluation scope to demonstrate the sufficiency by SESIP methodology. Note EN 303 645 is targeting for consumer IoT device with full software stack mounted and physically designed, and connection to network-based services. The full software stack includes the operating system, communication stack and protocol, and/or application code, which is designed and owned by NXP (direct and indirect) customers, i.e. OEMs and the network service providers. So not all requirements are directly applicable to NXP product scope but more to OEMs and the network service providers. Thus, rationale on how MCX N94x / 54x / 23x can support customers to meet EN 303 645 requirements are provided.

Table 14. EN 303 645 Mapping and Sufficiency

EN 303 645 Provisions	Covered/Supported By	Rationale
5.1-1 Unique device password	ADV: Development; AVA: Vulnerability assessment	Password feature shall be implemented by the operating system or application code.

5.1-2 Password Diversification	Verification of Platform Instance Identity	Password feature shall be implemented by the operating system or application code. The OEM can leverage platform instance identity for unique per device password diversification.
5.1-3 Cryptography for user authentication	Cryptographic Functionality	User authentication feature shall be implemented by the operating system or application code. MCX N94x / 54x / 23x provides cryptographic operations and secure storage which can be leveraged to fulfil this requirement.
5.1-4 Change of Authentication value 5.1-5 Authentication mechanism and attack resilience	N/A	User authentication feature shall be implemented by the operating system or application code.
5.2-1 Vulnerability disclosure policy 5.2-2 Timely response 5.2-3 Vulnerability monitoring	Flaw Reporting Procedures	Final product vulnerability disclosure policy shall be owned by OEMs. For NXP product, the NXP Product Security Incident Response Team (PSIRT) is committed to rapidly address security vulnerabilities in NXP products by responding and documenting reported vulnerabilities and by providing customers with clear guidance on the impact, severity and mitigation.
5.3-1 Secure Updatability 5.3-2 Secure installation of updates	Secure Update of Platform	MCX N94x / 54x / 23x provides secure update capabilities
5.3-3 Ease for update	AGD: Guidance document	Guidance documentation for secure update of platform is part of SESIP evaluation
5.3-4 Automatic update	Secure Update of Platform; AGD: Guidance document	Final product update mechanism shall be implemented by the operating system or application code. MCX N94x / 54x / 23x provides guidance document and corresponding tool chain for ease of use for OEM.
5.3-5 Check for update 5.3-6 Configurability for update	N/A	Final product update mechanism shall be implemented by the operating system or application code.
5.3-7 Cryptography for update	Secure Update of Platform; Cryptographic Functionality	MCX N94x / 54x / 23x secure update feature employs best practice cryptography. MCX N94x / 54x / 23x provides cryptographic operations and secure storage for operating system or application code to implement other secure update mechanisms.
5.3-8 Timely update	Flaw Reporting Procedures	Final product security update shall be owned by OEMs. For NXP product, the NXP Product Security Incident Response Team (PSIRT) is committed to rapidly address security vulnerabilities in NXP products by responding and documenting reported vulnerabilities and by providing customers with

		clear guidance on the impact, severity and mitigation.
5.3-9 Authenticity and Integrity of software update 5.3-10 Trust relationship for updates	Secure Update of Platform; Cryptographic Functionality	MCX N94x / 54x / 23x secure update feature ensures authenticity and integrity. MCX N94x / 54x / 23x provides cryptographic operations and secure storage for operating system or application code to implement other secure update mechanisms. Final product update mechanism shall be implemented by the operating system or application code.
5.3-11 Security update communication	Flaw Reporting Procedures	Final product security update shall be owned by OEMs. For NXP product, the NXP Product Security Incident Response Team (PSIRT) is committed to rapidly address security vulnerabilities in NXP products by responding and documenting reported vulnerabilities and by providing customers with clear guidance on the impact, severity and mitigation.
5.3-12 Update notification	N/A	Final product update mechanism shall be implemented by the operating system or application code.
5.3-13 Defined support period	N/A	Support period of final product shall be defined by OEM. For MCX N94x / 54x / 23x, this requirement is not covered by SESIP evaluation, yet NXP provides a Product Longevity program where MCX N94x / 54x / 23x will be included.
5.3-14 Communication for constrained device 5.3-15 Isolatability and replaceability for constrained device	N/A	Final device updatability, end user communication and mitigation shall be defined by OEM
5.3-16 Model recognizability	Verification of Platform Identity	Final product model designation shall be defined by OEM. SESIP methodology mandates unique identification of the platform under evaluation, MCX N94x / 54x / 23x conformance rational is provided.
5.4-1 Security Parameter Storage	Isolation of Platform Parts; Isolation of Platform (between SPE and NSPE); Secure Data Serialization	MCX N94x/ 54x/ 23x provides multiple security mechanism including TEE, secure enclave and secure external storage to support operating system or application code to fulfil this provisioning requirement.
5.4-2 Tamper resistance of hard-coded identity	Verification of Platform Instance Identity; Extra Attacker Resistance	Platform instance identity is unique per device and OTP based which can be used for security purposes. SESIP includes remote attack surface by default and MCX N94x / 54x / 23x provides extra attacker resistance including physical attacker resistance.

5.4-3 No hard-coded security parameters in software	ADV: Development; AVA: Vulnerability assessment	This evaluation provides full software source code access to evaluator for vulnerability assessment, and it assures that there is no hard-coded security parameter which leads to attack path within the attack potential.
5.4-4 Device unique and diversified critical security parameters	Verification of Platform Instance Identity; Secure Update of Platform	Final product update and communication mechanism shall be implemented by the operating system or application code. MCX N94x / 54x / 23x provides platform instance identity and a secure update feature which supports the operating system or application code to fulfil this requirement.
5.5-1 Best practice cryptography for communication	Cryptographic Functionality	Final product communication shall be designed by OEM. MCX N94x / 54x / 23x provides cryptography support to implement secure communication protocols. Reference designs (e.g. mbedTLS) are also available yet it is not part of this evaluation.
5.5-2 Implementation review and evaluation	SESIP methodology and certification	This SESIP evaluation is performed by a 3rd party independent laboratory and certifier who specialize in security including cryptography.
5.5-3 Cryptoagility	Secure Update of Platform, Cryptographic Functionality	MCX N94x / 54x / 23x provides an update capability where software based cryptography can be updated. Supported key sizes are clearly stated in cryptographic functionality sections.
5.5-4 Initialization state device access after authentication via network interface	Secure Initialization of Platform; Secure Debugging	The operating system or application code will take over control after MCX N94x / 54x / 23x boot up, hence it is up to the design by OEM. MCX N94x / 54x / 23x ensures secure initialization of the device before handing over control to the operating system or application code when secure boot is configured. MCX N94x / 54x / 23x also supports debug authentication.
5.5-5 Security configuration after authentication via network interface	Cryptographic Functionality	Final product communication shall be designed by OEM. MCX N94x / 54x / 23x provides cryptography support to implement secure communication protocols.
5.5-6 Confidentiality for security parameter in transition		
5.5-7 Confidentiality for security parameter via network		
5.5-8 Secure management process	N/A	The secure management or key management process for OEM provisioned security parameters is owned by OEM.
5.6-1 Unused interface disablement	N/A	MCX N94x / 54x / 23x provides configurability and the enablement and disablement of interfaces is dependent upon OEM's design.
5.6-2 Minimize disclosure during in initialization	Secure Initialization of Platform	The operating system or application code will take over control after MCX N94x / 54x / 23x boot up, hence it is up to the design by OEM. MCX N94x /

		54x / 23x ensures secure initialization of the device before handing over control to operating system or application code when secure boot is configured.
5.6-3 No unnecessary physical interface exposure	N/A	The design of final product including the physical interface exposure and its usability is by OEM.
5.6-4 Debug disablement	N/A	The debug function of MCX N94x / 54x / 23x can be disabled. Note MCX N94x / 54x / 23x provides Secure Debugging, yet by provision requirement this feature shall be disabled if the interface is physically accessible.
5.6-5 Least functionality	N/A	Software services of the final product is defined by the operating system or application code.
5.6-6 Minimized code	ADV: Development; AVA: Vulnerability assessment	This evaluation provides full software source code access to the evaluator for vulnerability assessment, and it assures that there is no unused code in the immutable part which could lead to attack path within the attack potential.
5.6-7 Least privilege	Isolation of Platform (between SPE and NSPE)	MCX N94x / 54x / 23x provides different hardware based privilege levels and isolation mechanisms which can be used to fulfil these requirements.
5.6-8 Hardware-level memory access control		
5.6-9 Secure development process	N/A	Final product development process shall be defined and applied by OEM. MCX N94x / 54x / 23x is part of the NXP Edge Lock Assurance Program and secure development process is applied.
5.7-1 Secure boot for software verification	Secure Initialization of Platform	MCX N94x / 54x / 23x provides secure boot feature and hardware root of trust.
5.7-2 Notification of unauthorized change	N/A	This provision requirement shall be implemented by the operating system or application code.
5.8-1 Confidentiality of personal data transition between device and service	Cryptographic Functionality	Final product communication shall be designed by OEM. MCX N94x / 54x / 23x provides cryptography support to implement the provisioning requirements.
5.8-2 Confidentiality of personal data transition between devices		
5.8-3 External sensing capability documented	N/A	Final product sensing capability and its document handling is up to OEM.
5.9-1 Resilience to outages	Secure Initialization of Platform; Attestation of Platform State	The resilience to outages and recovery shall be designed by OEM and service provider. MCX N94x / 54x / 23x provides secure initialization and attestation features which can support fulfillment of the provisioning requirements.
5.9-2 Local function with loss of network		
5.9-3 Orderly reconnection		
5.10-1 Telemetry data examination	Secure Initialization of Platform; Attestation of Platform State	The use case and feature shall be defined by OEM of the final product. MCX N94x / 54x / 23x provides secure initialization and attestation features which can support fulfillment of the provisioning requirements.

5.11-1 Ease for user data deletion	Residual Information Purging	The feature for user data management shall be defined by OEM of the final product. MCX N94x / 54x / 23x provides an information purging mechanism which can support fulfillment of the provisioning requirements.
5.11-2 Ease for user data deletion from service	N/A	These requirements shall be fulfilled by OEM and/or service provider.
5.11-3 Instruction for personal data deletion		
5.11-4 Deletion confirmation		
5.12-1 Ease of installation and maintenance	N/A	These requirements shall be fulfilled by OEM and/or service provider.
5.12-2 Guidance on setup		
5.12-3 Check on secure setup	Secure Initialization of Platform; Attestation of Platform State	This requirement shall be fulfilled by OEM and/or service provider. MCX N94x / 54x / 23x provides secure initialization and attestation features which can support fulfillment of the provisioning requirement.
5.13-1 Input Validation	ADV: Development; AVA: Vulnerability assessment	The final product operating system or application code is responsible for their input validation. The SESIP evaluation ensures there is no attack path identified including input manipulation within the attack potential in MCX N94x / 54x / 23x scope.
6-1 Clear personal data usage	N/A	These requirements shall be fulfilled by OEM and/or service provider.
6-2 Consumer's consent		
6-3 Consent withdraw		
6-4 Minimum telemetry data collection		
6.5 Clear telemetry data collection and usage		

4.5 NIST IR 8425 Mapping and Sufficiency

NIST has developed Profile of the IoT Core Baseline for Consumer IoT Products as NIST IR 8425 [27], which identifies cybersecurity capabilities commonly needed for the consumer IoT sector.

This section refers to the claims and activities within this SESIP evaluation scope to demonstrate the sufficiency by SESIP methodology towards compliance of NIST IR 8425. Note NIST IR 8425 is targeting for consumer IoT products with full software stack mounted and physically designed, and connection to network-based services. The full software stack includes the operating system, communication stack and protocol, and/or application code, which is designed and owned by NXP (direct and indirect) customers, i.e. the consumer IoT product manufactures (aka OEMs), and the network service providers. So not all requirements are directly applicable to NXP product scope but more to OEMs and the network service providers. Thus, rationale on how MCX N94x / 54x / 23x can support customers to meet NIST IR 8425 requirements are provided.

The descriptions below are checked by the independent security laboratory as part of the SESIP evaluation and provide evidences reusable in the context of consumer IoT product towards compliance to NIST IR 8425 when the corresponding security features are leveraged.

Table 15. NIST IR8425 Mapping and Sufficiency

NIST IR 8425	Covered/Supported by	Rationale
Asset Identification - 1 & 2	Verification of Platform Identity; Verification of Platform Instance Identity; Attestation of Platform Genuineness	MCX N94x / 54x / 23x provides identifications for its internal parts and their versions, and unique instance identification, which OEM can leverage for IoT Device identification. Attestation APIs further support to get the identity information in a secure manner.
Product Configuration - 1	Cryptographic Functionality; Secure Update of Platform	The authorization and configuration of the IoT device shall be implemented by the operating system or application code. MCX N94x / 54x / 23x cryptographic functionalities provide the IoT products capability to implement the authorization and access control mechanisms. Based on such mechanisms, the IoT product configuration settings can be changed by authorized individuals, services or other IoT product components. Cryptographic KeyStore additionally supports the protection of the cryptographic secrets involved in the authorization mechanism described above. Secure Update of Platform allows the IoT devices to update to a newer version in the field in secure manner if this is needed for a configuration update.
Product Configuration - 2	Residual Information Purging	The authorization and configuration of the IoT device shall be implemented by the operating system or application code. MCX N94x / 54x / 23x provides Residual Information Purging functions, which can erase corresponding data when the IoT product is returned to a secure default configuration.
Product Configuration - 3	Secure Update of Platform	The way the IoT product applies configuration to IoT components depends on the IoT product architecture, and the IoT device operating system or application shall be implemented accordingly. MCX N94x / 54x / 23x Secure Update of Platform function allows the IoT Device to update to a newer version in the field in secure manner if this is needed for a configuration update.
Data Protection - 1	Cryptographic Key Store; Physical Attack Resistance; Isolation of Platform Parts; Secure Debugging; Verification of Platform Identity; Verification of Platform Instance Identity	MCX N94x / 54x / 23x provides various mechanisms to protect data it stores. The Cryptographic KeyStore function protects the storage of the cryptographic data. Physical Attacker Resistance and Software Attacker Resistance: Isolation of Platform support the secure data storage by implementing protections against physical and logical, remote and local attacks. Secure Debugging supports the secure data storage by not protecting unauthorized access to those data via debug features. The platform identity and instance identity are also stored securely.

Data Protection – 2	Residual Information Purging; Field Return of Platform; Decommission of Platform	MCX N94x / 54x / 23x Residual Information Purging function supports the ability to delete or render inaccessible user data stored in MCX N94x / 54x / 23x. Field Return of Platform and Decommission of Platform can be leveraged by IoT devices to delete or render inaccessible stored data when changing life-cycle state.
Data Protection – 3	Cryptographic Functionality	The communication function of the IoT device shall be fully facilitated by the operating system or application code. MCX N94x / 54x / 23x provides cryptographic functionalities by which the IoT device can implement protection of data transmission. Cryptographic KeyStore additionally supports the protection of the cryptographic secrets involved in the data transmission protection mechanism.
Interface Access Control – 1 & 2	Cryptographic Functionality; Extra Attacker Resistance; Secure Debugging; VA: Vulnerability Assessment; ADV: Development; ATE: Test	The design of final device including the physical interface exposure and its usability is by OEM. The access control, authentication, and communication mechanism shall also be implemented by the operating system or application code of the IoT device. MCX N94x / 54x / 23x provides cryptographic functionalities by which the IoT devices can implement access control and authentication mechanism. Cryptographic KeyStore additionally supports the protection of the cryptographic secrets involved in the authentication mechanism described above. Software Attacker Resistance: Isolation of Platform and Software Attacker Resistance: Isolation of Platform Part implement protections against illegal access to resources (physically isolated by design), by restricting the access between Secure and Non Secure domain of trust zone, and between the security enclave and the rest of system. Secure Debugging supports the access control to MCX N94x / 54x / 23x debug interfaces only for authorized party. Also, the AVA (vulnerability assessment), ADV (development) and ATE (Test) activities in SESIP evaluation verify that the interfaces provided at MCX N94x / 54x / 23x platform level are restricted to only the necessary functions and privileges, and there is no unnecessary privilege, interface and/or code remained.
Software Update – 1 & 2	Secure Update of Platform	Secure Update of Platform implements the secure update ensuring integrity and authentication verification. The software update development, distribution and customer notification are expected to be managed by OEMs and/or the network service providers.

Cybersecurity State Awareness - 1	Attestation of Platform Genuineness; Attestation of Platform State; Physical Attack Resistance; Isolation of Platform Parts	The cybersecurity state awareness of the IoT device shall be designed and implemented by the operating system or application code. MCX N94x / 54x / 23x provides various services that can facilitate such mechanisms: The attestation function can attest the identity and platform state. Software Attacker Resistance: Isolation of Platform can capture attempts of privilege violation. Physical Attacker Resistance also provide protections on secure audit record handling.
Documentation	ASE: Security Target; AGD: Guidance document; SESIP Methodology [1]; SESIP Profile for Secure MCUs and MPUs [2]; SESIP Profile for PSA Certified Level 3 [3]; Flaw Reporting Procedures	NXP provides MCX N94x / 54x / 23x documents related to cybersecurity. The ASE (Security Target) and AGD (user guidance) activities in SESIP evaluation (see [1]) evaluates the documents to ensure information is provided related to security including security scope, functions, assurance level, secure use of the platform, etc. Flaw Reporting Procedure (ALC_FLR.2) in SESIP evaluation ensures that it is clear that how a customer get informed.
Information and Query Reception	Flaw Reporting Procedures	This is a requirement to OEMs and/or the network service providers. At NXP level, we have Flaw Reporting Procedure defined, and as part of SESIP evaluation (see also [1]), such procedure is verified that flaw reporting process is in place and allows the efficient tracking of flaws, and users get notifications on a flaw and how to handle it.
Information Dissemination	ASE: Security Target; AGD: Guidance document; Flaw Reporting Procedures	This is a requirement to OEMs and/or the network service providers. NXP provides MCX N94x / 54x / 23x documents related to cybersecurity. See more in rational in Documentation and Information and Query Reception entry.
Product Education and Awareness	ASE: Security Target; AGD: Guidance document	This is a requirement to OEMs and/or the network service providers. NXP provides MCX N94x / 54x / 23x documents related to cybersecurity. The ASE (Security Target) and AGD (user guidance) activities in SESIP evaluation (see [1]) evaluates the documents to ensure information is provided related to security including security scope, functions, assurance level, secure use of the platform, etc.

4.6 IEC 62443-4-2 Mapping and Sufficiency

The table below shows how the platform under evaluation, MCX N94x / 54x / 23x, described in this Security Target supports the final device, the component, to show compliance with IEC 62443-4-2 security requirements (see [28]). It describes which part of the each 62443-4-2 requirements are implemented by MCX N94x / 54x / 23x. Then, it 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 evidence reusable in the context of the end device compliance demonstration to the 62443-4-2 standard.

Table 16. IEC 62443-4-2 Security Requirements supported by MCX N94x / 54x / 23x

62443-4-2	Covered/Supported By	Rationale
CR 1.1 - Human user identification and authentication CR 1.1(1) - Unique identification and authentication CR 1.1(2) – Multifactor authentication for all interfaces	Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Operation; Cryptographic Key Store	MCX N94x / 54x / 23x provide cryptographic functionalities that can be used to implement human user identification and authentication (including multifactor authentication).
CR 1.2 - Software process and device identification and authentication CR 1.2(1) - Unique identification and authentication	Verification of Platform Identity; Verification of Platform Instance Identity; Attestation of Platform Genuineness; Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Operation; Cryptographic Key Store	Verification of Platform Identity provides a unique and tamper-proof identification of the MCX N94x / 54x / 23x 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 MCX N94x / 54x / 23x 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 MCX N94x / 54x / 23x 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	Cryptographic Key Store	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; Cryptographic Random Number Generation	Cryptographic Key Generation and Cryptographic Random Number Generation provide key generation and random number generation services which can be used for unique and unambiguous identifier creation.
CR 1.5 - Authenticator management CR 1.5(1) - Hardware security for authenticators	Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Key Store; Physical Attacker Resistance; Software Attacker Resistance	Cryptographic Key Generation and Cryptographic Random Number Generation provides key generation and random number generation which can be used as authenticators. Cryptographic KeyStore provides secure storage of authenticators. Physical Attacker Resistance provides protections of authenticators against physical attacks. Software Attacker Resistance: Isolation of Platform provides protection of authenticators against remote and local logical attacks.
CR 1.6 – Wireless access management	Cryptographic Operation; Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Key Store	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. It is the component responsibility to properly implement wireless access management. 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	Cryptographic Operation; Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Key Store	It is the component responsibility to properly enforce the password policy. Cryptographic Operation, Cryptographic Key Generation, Cryptographic Random Number Generation provides cryptographic functionalities that can be used to enforce configurable password strength by meeting defined strength rules. Cryptographic KeyStore provides secure storage that can be used to enforce configurable password strength allowing their modifications and/or deletion to comply with defined number of use and lifetime restrictions.
CR 1.8 – Public key infrastructure certificates	Cryptographic Operation; Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Key Store; Physical Attacker Resistance; Software Attacker Resistance	Cryptographic Operation, Cryptographic Key Generation and Cryptographic Random Number Generation provide cryptographic functionalities that can be used to interact and operate with PKI infrastructures. Cryptographic KeyStore provides secure storage of the cryptographic material (e.g. keys, certificates) involved in PKI infrastructures. Physical Attacker Resistance provides protections of cryptographic material and operations against physical attacks. Software Attacker Resistance: Isolation of Platform provides protections of cryptographic material and operations against remote and local logical attacks.

CR 1.9 – Strength of public key-based authentication CR 1.9(1) – Hardware security for public key-based authentication	Cryptographic Operation; Cryptographic Key Generation; Cryptographic Key Store; Physical Attacker Resistance; Software Attacker Resistance	Cryptographic Operation and Cryptographic Key Generation provide cryptographic features needed in public-key-based authentication in conformance with internationally recognized and proven security practices and recommendations. Cryptographic KeyStore provides secure storage for cryptographic material (e.g. keys, certificates) needed in public-key-based authentication. Physical Attacker Resistance provides protection of public-key-based authentication related material against physical attacks. Software Attacker Resistance: Isolation of Platform provides protection of public-key-based authentication related material against remote and local logical attacks.
CR 1.10 – Authenticator feedback	N/A	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	N/A	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	N/A	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	N/A	It is the component responsibility to deny or accept requests based on the authentication results.

CR 1.13(1) – Explicit access request approval		
CR 1.14 – Strength of symmetric key based authentication CR 1.14(1) – Hardware security for symmetric key-based authentication	Cryptographic Operation; Cryptographic Key Generation; Cryptographic Key Store; Physical Attacker Resistance; Software Attacker Resistance	Cryptographic Operation and Cryptographic Key Generation provide cryptographic functionalities conformant to internationally recognized and proven security best practices that can be used for symmetric-key-based authentication. Cryptographic KeyStore provides secure storage for cryptographic material (e.g. shared secret) involved in symmetric-key-based authentication. Physical Attacker Resistance provides protections of related material against physical attacks. Software Attacker Resistance: Isolation of Platform provides protections of related material against remote and local logical attacks.
CR 2.1 – Authorization enforcement	Software Attacker Resistance	It is the component responsibility to properly implement authorization enforcement mechanism. Human, Software, or Device Authentication is as per CR1.1 and CR1.2. Software Attacker Resistance: Isolation of Platform provides logical isolation of the MCX N94x / 54x / 23x subcomponent that can be leveraged to enforce authorization of properly authenticated entities.
CR 2.2 – Wireless use control	Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Operation; Cryptographic Key Store	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	Software Attacker Resistance; Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Operation; Cryptographic Key Store	Isolation of Platform provides an isolated processing environment which can include the 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 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	N/A	It is the component responsibility to properly implement session lock, remote session termination, and concurrent session control mechanisms. Human user re-authentication is as per CR1.1. Remote software processes or devices re-authentication is as per CR1.2 and CR1.6. Account and credential management are as per CR.13, CR1.4, CR1.5.
CR 2.8 – Auditable events CR 2.9 – Audit storage capacity CR 2.10 – Response to audit processing failures CR 2.11 – Timestamps	Physical Attacker Resistance; Software Attacker Resistance	All SESIP SFRs provide output status which can be integrated to the component audit records. It is the component responsibility to properly implement audit logging capabilities. Physical Attacker Resistance provides protections against physical attacks that could affect audit records overall management. Software Attacker Resistance: Isolation of Platform provides protections against remote and local logical attacks that could

		affect audit records overall management.
CR 2.12 – Non-repudiation CR 2.12 – Non-repudiation for all users	Cryptographic Operation; Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Key Store	All SESIP SFRs provide output status which can be integrated to the component audit records as per CR2.8, CR2.9, CR2.10, CR2.11 and serve as a proof that an action has been performed. Cryptographic Operation, Cryptographic Key Generation, Cryptographic Random Number Generation and Cryptographic KeyStore provides cryptographic functionalities that can be used 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	Secure Debugging provides protected access to the physical diagnostic and test interfaces of the MCX N94x / 54x / 23x.
CR 3.1 – Communication integrity CR 3.1(1) – Communication authenticity	Cryptographic Operation; Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Key Store; Physical Attacker Resistance; Software Attacker Resistance	Cryptographic Operation provides cryptographic operations that can be used to protect integrity and authenticity of transmitted information. Cryptographic Key Generation and Cryptographic Random Number Generation provides cryptographic functionalities that can be used to generate the cryptographic material necessary for the protection of transmitted information. Cryptographic KeyStore provides secure storage that can be used to store cryptographic material (e.g. shared secret) on which such protections is be based. Physical Attacker Resistance provides protections of cryptographic services involved in secure communication integrity

		and authenticity enforcement against physical attacks. Software Attacker Resistance: Isolation of Platform provides protections of cryptographic services involved in secure communication integrity and authenticity enforcement against remote and local logical attacks.
CR 3.2 – Protection from malicious code	Secure Initialization of Platform; Software Attacker Resistance	Secure Initialization of Platform provides protection against installation and execution of unauthorized software by checking the integrity and authenticity of the MCX N94x / 54x / 23x firmware at each reset, as part of the secure boot. Software Attacker Resistance: Isolation of Platform provides isolation of the MCX N94x / 54x / 23x against remote and local logical attacks that could be led from malicious code loaded into the SoC.
CR 3.3 – Security functionality verification CR 3.3(1) – Security functionality verification during normal operation	Secure Initialization of Platform; Attestation of Platform State; Physical Attacker Resistance	Secure Initialization of Platform provides integrity and authenticity verification of the MCX N94x / 54x / 23x firmware ensuring a proper health check 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 MCX N94x / 54x / 23x (including hashes of the firmware and patch, as well as life cycle state) that can be used to verify the state of the component during operation. Physical Attacker Resistance provides monitoring and detecting of physical attacks during operation.

CR 3.4 – Software and information integrity CR 3.4(1) – Authenticity of software and information CR 3.4(2) – Automated notification of integrity violations	Secure Initialization of Platform; Secure Update of Platform; Attestation of Platform State; Physical Attacker Resistance; Software Attacker Resistance	Secure Initialization of Platform provides, as part of the secure boot, integrity and authenticity checks of the firmware, software and configuration data MCX N94x / 54x / 23x before any execution. Secure Update of Platform additionally checks the version verification of the MCX N94x / 54x / 23x firmware/software to be launched. Attestation of Platform State provides, on demand, the attestation of the state of the MCX N94x / 54x / 23x (including hashes of the firmware and patch, as well as life cycle state). Physical Attacker Resistance ensures the protection of code and data integrity during boot and at runtime against physical attacks. Software Attacker Resistance: Isolation of Platform ensures the protection of code and data integrity during boot and at runtime against remote and local logical attacks. Detections of integrity violation are reported in registers accessible to the SoC, then in charge of automatic notification to other entities.
CR 3.5 – Input validation	VA: Vulnerability Assessment; ATE: Test	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	VA: Vulnerability Assessment; ATE: Test	The AVA_VAN (vulnerability analysis) and ATE_IND (functional testing) SESIP evaluation activities support the verification of

		deterministic behavior of the overall system by checking the correct and expected behavior of the MCX N94x / 54x / 23x part.
CR 3.7 – Error handling	VA: Vulnerability Assessment; ATE: Test	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; Cryptographic Operation	Cryptographic Random Number Generation provides random number that can be used to generate unique sessions identifiers. Cryptographic Operation provides cryptographic operations that can be used to protect integrity of session.
CR 3.9 – Protection of audit information	Physical Attacker Resistance; Software Attacker Resistance	Physical Attacker Resistance and Software Attacker Resistance: Isolation of Platform provides protection of execution status of the MCX N94x / 54x / 23x security services against remote and local, logical and physical attacks.
CR 3.10 - Support for updates CR 3.10(1) - Update authenticity and integrity	Secure Initialization of Platform; Secure Update of Platform	Secure Initialization of Platform and Secure Update of Platform provides secure update of the MCX N94x / 54x / 23x firmware/software parts through the checking of the its integrity, authenticity and version as part of the secure boot.
CR 3.11 - Physical tamper resistance and detection CR 3.11(1) Notification of a tampering attempt	Physical Attacker Resistance	Physical Attacker Resistance provides protections against physical attacks of the MCX N94x / 54x / 23x; 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	Cryptographic Key Generation; Cryptographic Operation; Cryptographic Random Number Generation; Cryptographic Key Store; Physical Attacker Resistance; Software Attacker Resistance	The MCX N94x / 54x / 23x is implementing itself a root-of-trust from which supplier keys can be generated and protected by using the cryptographic services Cryptographic Key Generation, Cryptographic Operation, Cryptographic Random Number Generation and Cryptographic Key Store Physical Attacker Resistance provides protection of product supplier root-of-trust keys and data against physical attacks. Software Attacker Resistance: Isolation of Platform provides protection of product supplier root-of-trust keys and data against remote and local logical attacks.
CR 3.13 - Provisioning asset owner roots of trust	Cryptographic Key Generation; Cryptographic Operation; Cryptographic Key Store; Physical Attacker Resistance; Software Attacker Resistance	Cryptographic Key Generation and Cryptographic Operation provides cryptographic services that can be used for the provisioning of asset owner root-of-trust. Cryptographic KeyStore provides secure storage (confidentiality, integrity, authenticity) that can be used to securely store provisioned supplier cryptographic material to be used as a root-of-trust. Physical Attacker Resistance provides protection of asset owner root-of-trust keys and data against physical attacks. Software Attacker Resistance: Isolation of Platform provides protection of asset owner root-of-trust keys and data against remote and local logical attacks.
CR 3.14 - Integrity of boot process CR 3.14(1) - Authenticity of the boot process	Secure Initialization of Platform; Secure Update of Platform; Cryptographic Key Store; Physical	Secure Initialization of Platform and Secure Update of Platform provides secure update of the

	Attacker Resistance; Software Attacker Resistance	MCX N94x / 54x / 23x firmware/software parts through the checking of the its integrity, authenticity and version as part of the secure boot. Cryptographic KeyStore provide the capability to protect the confidentiality of information at rest in transit when imported in the MCX N94x / 54x / 23x for use. Physical Attacker Resistance provides confidentiality protection of the information against physical attacks when manipulated by the MCX N94x / 54x / 23x services. Software Attacker Resistance: Isolation of Platform provides confidentiality protection of the information against remote and local logical attacks when temporarily stored into the MCX N94x / 54x / 23x services.
CR 4.1 - Information confidentiality	Cryptographic KeyStore; Physical Attacker Resistance; Software Attacker Resistance	Cryptographic KeyStore provides the capability to protect the confidentiality of information at rest in the external NVM and in transit when imported in the MCX N94x / 54x / 23x for use. Physical Attacker Resistance provides confidentiality protection of the information against physical attacks when manipulated by the MCX N94x / 54x / 23x services. Software Attacker Resistance: Isolation of Platform provides confidentiality protection of the information against remote and local logical attacks when temporarily stored into the MCX N94x / 54x / 23x services.
CR 4.2 - Information persistence	Residual Information Purging; Cryptographic Key Store; Software Attacker Resistance	Residual Information Purging provides secure erasing of sensitive data when changing life-cycle state related to decommissioning or field return.

		Cryptographic KeyStore provides secure erasure of cryptographic material. Software Attacker Resistance: Isolation of Platform provides mediated access to information stored and manipulated inside the MCX N94x / 54x / 23x avoiding having to share critical memory resources.
CR 4.3 - Use of cryptography	Cryptographic Operation; Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Key Store	Cryptographic Operation, Cryptographic Key Generation, Cryptographic Random Number Generation and Cryptographic KeyStore provide cryptographic capabilities that can be used by the component. The AVA_VAN (vulnerability analysis) SESIP evaluation activity requires the verification that cryptographic algorithms, used in any security feature, are compliant with internationally recognized and proven security practices and recommendations.
CR 5.1 - Network segmentation CR 5.2 - Zone boundary protection CR 5.3 - General-purpose person-to-person communication restrictions	N/A	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 MCX N94x / 54x / 23x 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	Cryptographic Operation; Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Key Store	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	N/A	It is the component responsibility to properly implement monitoring capabilities according to the system requirements. The component may use security services claimed by MCX N94x / 54x / 23x to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc., however this is to be determined case by case.
CR 7.1 – Denial of service protection CR 7.1(1) – Manage communication load from component	N/A	It is the component responsibility to properly implement monitoring capabilities according to the system requirements. The component may use security services claimed by MCX N94x / 54x / 23x 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	N/A	It is the component responsibility to properly implement monitoring capabilities according to the system requirements. The component may use security services claimed by MCX N94x / 54x / 23x 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	Cryptographic Operation; Cryptographic Key Generation; Cryptographic Random Number Generation; Cryptographic Key Store	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	N/A	It is the component responsibility to properly implement system recovery and reconstruction. The component may use security services claimed by MCX N94x / 54x / 23x 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 7.6 – Network and security configuration settings CR 7.6(1) – Machine-readable reporting of current security settings	N/A	It is the component responsibility to properly implement monitoring capabilities according to the system requirements. The component may use security services claimed by MCX N94x / 54x / 23x to support this requirement, for instance in case Root-of-Trust base, secure cryptography, or secure storage is needed, etc., however this is to be determined case by case.
CR 7.7 – Least functionality	VA: Vulnerability Assessment; ATE: Test	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 unnecessary functions, ports. protocols and/or services by requiring for the MCX N94x / 54x / 23x the verification that there is no unnecessary interface and/or code remaining in the final implementation.

CR 7.8 – Control system component inventory	N/A	It is the component responsibility to properly implement monitoring capabilities according to the system requirements. The component may use security services claimed by MCX N94x / 54x / 23x 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.

Bibliography

5.1 Evaluation Documents

[1] GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2, GP_FST_070.

[2] GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs, Version 1.0, GPT_SPE_150.

[3] SESIP Profile for PSA Certified Level 3, V2.0 BETA 01, PSA JSA, 20/02/2024.

5.2 Developer Documents

[4] MCX Nx4x Security Reference Manual, Rev 3, 01/2024, NXP Semiconductors

[5] MCXNx4xRM, Rev 4, 01/2024, NXP Semiconductors

[6] MCXNx4x Data Sheet Rev. 4

[7] User Manual of Crypto Library Normal Secure (CLNS)

[8] AN969001-AN14086 Encryption and Decryption for External Memory on SPSDK Tool for MCX N Series (Rev. 1)

[9] AN970001-Encryption and decryption for Internal Memory on SEC tool for MCX N Series (Rev. 1)

[10] AN970101-Enabling Secure Boot and Trust Provisioning on MCX N Series (Rev. 1)

[11] AN970201-Enabling Debug Authentication on MCX N Series for In-field Analysis (Rev. 1)

[12] AN970301-Secure Provisioning Guidelines for MCX N Series MCUs (Rev. 1)

[13] AN970601-Encryption and decryption for External Memory on SEC tool for MCX N Series (Rev. 1)

[14] AN970801-AN14087 Encryption and Decryption for Internal Memory on SPSDK Tool for MCX N Series (Rev. 1)

[15] MCUXIDECTUG – MCUXpresso Config Tools User’s Guide (IDE) (Rev. 7)

[16] AN6259 - Common Trust Provisioning Conceptional Overview, Rev 1.1, NXP Semiconductors, March 2021

[22] MCX N23x Security Reference Manual, Rev. 1, 11/2023

[23] MCX N23x Reference Manual, Rev. 3, 05/2024

[24] MCXN23x Data Sheet, Rev. 2, 05/2024

[25] AN14145 Flash Memory Swap Feature on MCX N Series (Rev. 2)

[26] AN14179 - Migration Guide for MCXNx4x to MCXN23x (Rev. 1)

5.3 Standards

[17] NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology, January 2012

[18] NIST SP800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, National Institute of Standards and Technology, January 2018

[19] ARM Platform Security Architecture Firmware Framework 1.0, ARM Limited, DEN 0063. Issue number 0, Jun 2019

[20] ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI, v2.1.1, June 2020

[21] SESIP Applicability for EN 303 645, White Paper, GlobalPlatform, January 2022

[27] NIST IR 8425 Profile of the IoT Core Baseline for Consumer IoT Products, National Institute of Standards and Technology, September 2022, https://csrc.nist.gov/pubs/ir/8425/final

[28] 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

6.1 Definitions

Draft — The document is a draft version only. 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 herein and shall have no liability for the consequences of use of such information.

6.2 Disclaimers

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

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

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

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

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

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

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

provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

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

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 is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

6.3 Trademarks

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

<Name> — is a trademark of NXP Semiconductors N.V.

List of figures

List of tables

Contents

Date of release: 14 October 2024
Document identifier: 1.1

Date of release: 14 October 2024
Document identifier: 1.1