S32K3xx / MWCT2xxxS

SESIP Security Target

1.1.1

Rev. 1.0 — March 2026
Evaluation document

Document information

Information	Content
Keywords	SESIP Security Target, S32K312, MWCT2016S, S32K322, MWCT2D16S, S32K341, S32K342, MWCT2L16S, S32K314, MWCT2017S, S32K324, MWCT2D17S, S32K344, MWCT2L17S, S32K310, MWCT2014S, S32K311, MWCT2015S, S32K328, S32K338, S32K348, S32K358, S32K364, S32K366, S32K374, S32K376, S32K394, S32K396, S32K388
Abstract	Security target for evaluation of the S32K3xx / MWCT2xxxS developed and provided by NXP Semiconductors, according to SESIP Assurance Level 2 (SESIP2) based on SESIP methodology, version 1.2

Revision History

Rev.	Date	Description
0.1	August 28, 2024	Initial release
0.2	October 16, 2024	Removed Secure External Storage claim, updated FW versions
0.3	November 14, 2024	Minor changes to address Riscure comments
0.4	January 10, 2025	Fixed incorrect references and other minor changes
0.5	February 5, 2025	Finalized Residual Information Purging SFR, added MWCT document references, other minor corrections
0.6	March 7, 2025	Removed S32K389, minor updates based on Keysight comments
1.0	March 9, 2026	Minor updates based on Keysight comments. Final Release

1 Introduction

This Security Target describes the S32K3xx / MWCT2xxxS platform and the exact security properties of the platform that are evaluated against GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2, SESIP Assurance Level 2 (SESIP2) [1].

2.1 ST Reference

S32K3xx / MWCT2xxxS, SESIP Security Target, Revision 1.0, NXP Semiconductors, 09 March 2026.

2.2 SESIP Profile Reference and Conformance Claims

Table 1. SESIP Profile Reference and Conformance Claims

Reference	Value
SP Name	SESIP Profile for WPC Qi Secure Storage Subsystem [2]
SP Version	1.0
Assurance Claim	SESIP Assurance Level 2 (SESIP2)

SP Name	GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs [3]
SP Version	Version 1.0
Assurance Claim	SESIP Assurance Level 2 (SESIP2)
Package Claim	Base SP, Package Security Services, Package Software Isolation

2.3 Platform Reference

S32K3xx / MWCT2xxxS

Table 2. Platform Reference

Reference	Value
Platform Name and Version	S32K3xx / MWCT2xxxS, Rev 1.0
Platform Identification	S32K312, MWCT2016S, S32K322, MWCT2D16S, S32K341, S32K342, MWCT2L16S, S32K314, MWCT2017S, S32K324, MWCT2D17S, S32K344, MWCT2L17S, S32K310, MWCT2014S, S32K311, MWCT2015S, S32K328, S32K338, S32K348, S32K358, S32K364, S32K366, S32K374, S32K376, S32K394, S32K396, S32K366, S32K388
Platform Type	Vehicle microcontrollers
Flash Memory Configuration	FULL_MEM

2.4 Guidance Documents

The following documents are included with the platform:

Table 3. Guidance Documents

Document	Reference
Product Reference Manual	S32K3xx Reference Manual [6]

Firmware Reference Manual	HSE_B Firmware Reference Manual [4], HSE_B Firmware Reference Manual for GM [5]
Product Data Sheet	S32K3xx Datasheet [7]
Firmware API Reference Manual	[8]
SESIP Security Target	S32K3xx / MWCT2xxxS, SESIP Security Target, Revision 1.0, NXP Semiconductors, 09 March 2026.
Application Note	AN649711, Selecting and using cryptographic algorithms and protocols [9]
Product Reference Manual	MWCT2xxxS Reference Manual [10]
Product Data Sheet	MWCT2xxxS Product Data Sheet [11]
Application Note	AN6259, Common Trust Provisioning Conceptional Overview, Rev 1.1 [12]

2.5 Other Certification

S32K3xx / MWCT2xxxS development process has followed Business Creation and Management (BCaM) framework and is subject to Product Security Incident Response Process (PSIRP). The latest NXP (BCaM and PSIRP) processes have been certified as compliant following ISO/SAE 21434:2021 Road vehicles - cybersecurity engineering [13]. See more in Section 4.2.1.

Item	Content
Scheme	ISO/SAE 21434:2021 [13]
Certification Body	TUV SUD Product Service GmbH
Certification Number	Q4B 109577 0002 Rev. 00
Certification Date	2024-09-02

The Deterministic Random Bit Generator (DRBG) implemented in the S32K3xx / MWCT2xxxS has been CAVP (Cryptographic Algorithm Validation Program) validated according to NIST SP800-90A [14].

Item	Content
Scheme	Cryptographic Algorithm Validation Program
Certification Body	National Institute of Standards and Technology (NIST)
Certification Number	A4154
Certification Date	07-10-2023

2.6 Platform Overview and Description

The S32K3xx / MWCT2xxxS vehicle microcontroller product series possesses an Arm Cortex- M0 core within the Secure Enclave, an ARM Cortex-M7 core, flash memory, ASIL-B and D rating and advanced security module. The product series devices are well suited to a wide range of applications in electrical harsh environments, and are optimized for cost-sensitive applications offering new, space saving package options. The product series offers a broad range of memory, peripherals and performance options. Devices in this series share common peripherals and pin-out, allowing developers to migrate easily within a chip series or among other chip series to take advantage of more memory or feature integration.

S32K3xx / MWCT2xxxS offers compliance to WPC requirements for support of the Qi authentication protocol v.3.x.

NXP S32K3xx / MWCT2xxxS devices feature:

- An application domain, also referred to as the host, which comprises various system resources including one or several CPU subsystems; on-chip memory resources; several peripheral subsystems such as communication interfaces, timers, encoders/decoders, etc; interfaces to external memory resources; a system bus that is interconnecting all system resources together
- A security domain, which is the Hardware Security Engine (HSE) subsystem, also refered as HSE_B. It has its own exclusive system resources and connects to the host via a dedicated interface.

Specifically for flash loadable image, in the security domain, the flash loadable HSE firmware are:

- The HSE firmware executable, hereafter referred to as **FW-IMG**. For instance, crypto library is included in FW-IMG.
- The HSE system image that contains public and private (secret) keys and configuration data (aka HSE system attributes), hereafter referred to as **SYS-IMG**

Any additional firmware, OS or application software is stored in the application domain on the platform, and it is not in scope of this evaluation, and hereafter referred as application image.

Table 4. HSE Firmware feature

HSE firmware feature	Standard
AES	NIST FIPS 197
SHA	NIST FIPS 180-4
CMAC GMAC HMAC	NIST SP800-38B NIST SP800-38D NIST FIPS 198-1
CCM GCM	NIST SP800-38C NIST SP800-38D
RSA	NIST FIPS 186-4
ECDSA P256, P384, P521	NIST FIPS 186-4
EdDSA 25519	NIST FIPS 186-5
RSA ECDSA	NIST SP800-56A
RSA	PKCS #1

1.6.1 Platform Security Features

The Hardware Security Engine (HSE_B) is a subsystem that implements the security functions for the device. It provides cryptographic services to host CPUs, and fully meets the functional goals and objectives of the WPC requirements.

The HSE_B subsystem is responsible for establishing the root of trust on the device during the boot process and includes the following features:

- Trusted and Secure boot support
- Highly featured symmetric and asymmetric accelerators
- Support for various cryptographic functions (see Section 4.3)
- Arm Cortex-M0+ CPU

- True Random Number Generator (TRNG)
- Pseudo Random Number Generator (PRNG)
- Firmware Over-the-Air (FOTA) support.
- Secure Debug

Secure Boot Assist Flash (aka SBAF) is a software component programmed in devices by NXP during production. This software component resides in the HSE code flash area. The features provided by this software component are:

- HSE firmware installation
- HSE firmware restoration
- Debug authorization
- Partition swapping enablement
- Support in firmware update
- Secure and JTAG based recovery mode

1.6.2 Platform Logical Scope

The platform logical scope is the S32K3xx / MWCT2xxxS on-chip SBAF and the flash loadable updatable HSE firmware (i.e. FW-IMG and SYS-IMG) (either standard version or premium version). The versions for each component are as listed in Table 5. Note SYS-IMG contains keys and configurable data which is not a static image hence not listed in the table. All security and user guidance listed in Table 3 is also included in the TOE.

Any additional firmware, OS or application software stored on the platform (i.e. application image) is not in scope of this evaluation.

1.6.3 Platform Physical Scope

The platform physical scope is the microcontroller silicon chip including the on-chip ROM. The hardware components and interfaces are listed in Section 2.3 of [6] and Figure 1 shows the block diagram of the S32K3xx / MWCT2xxxS family.

Figure 1. S32K3xx / MWCT2xxxS Block Diagram

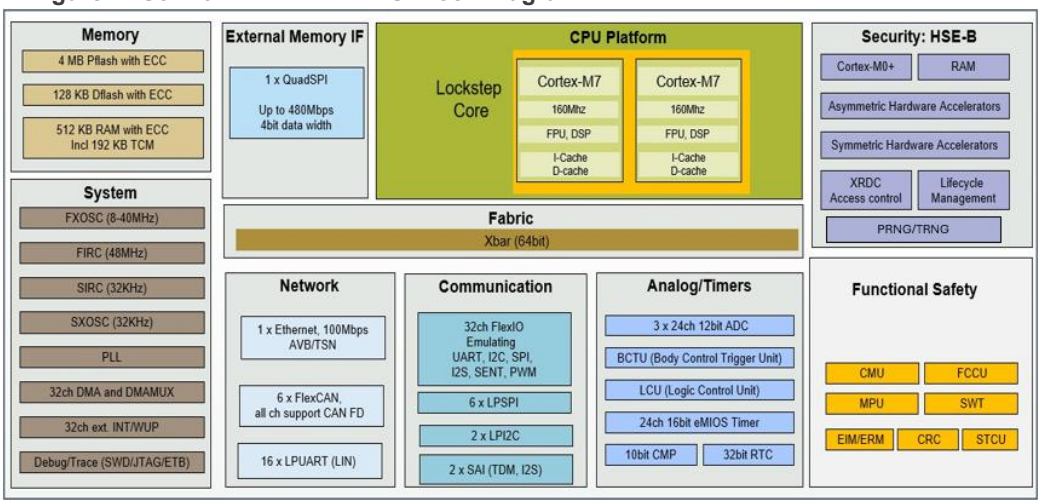
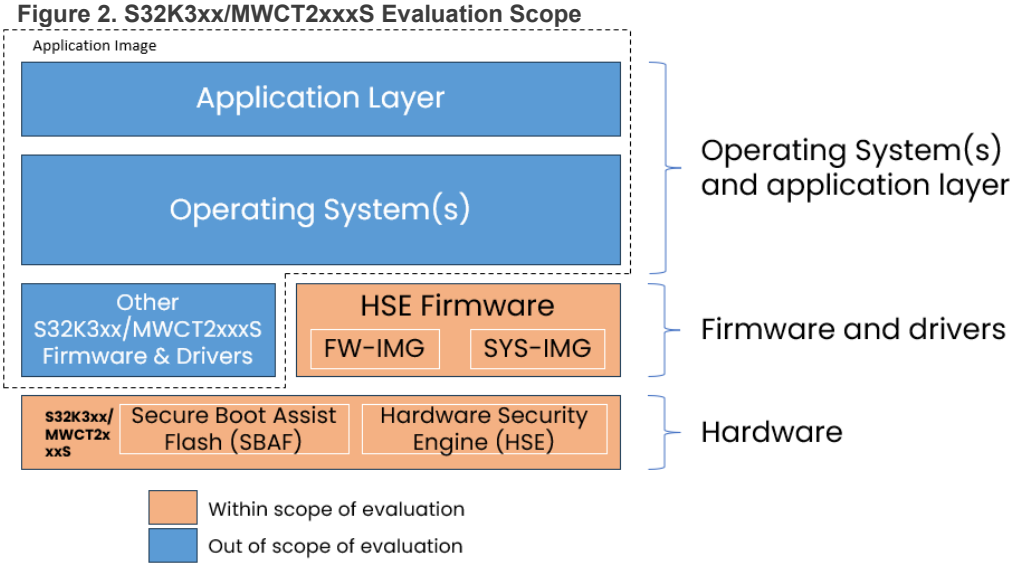


Table 5. Platform Deliverables

Type	Name	Release	Form of delivery
IC Hardware	S32K3xx MWCT2xxxS	Rev 1.0 Major mask = 0000 Rev 1.0 Major mask = 0000	Silicon Chip and On Chip ROM
HSE Firmware	S32k3xx / MWCT2xxxS HSE Firmware	x.2.6.0 and x.2.40.0	Software package
SBAF	S32K3xx / MXCT2xxxS SBAF Firmware	00 0D 08 00 00 15 00 01	Software package

Figure 2. S32K3xx/MWCT2xxxS Evaluation Scope



1.6.4 Required Non-Platform Hardware/Software/Firmware

There is no required non-platform hardware, software or firmware.

1.6.5 Life Cycle

The life cycle (LC) is managed by the HSE subsystem, see Section 3.3.8 of [4] for further information. The LC states are as Table 6:

Table 6. Life Cycle States

LC State	Description
NXP Internal	NXP manufacture and test state
CUST_DEL	Device (i.e. NXP's IC) delivered to system integrator (i.e. NXP's customer) for ECU manufacturing and initial configuration
OEM_PROD	ECU (device) delivered to the OEM for vehicle integration and final configuration
IN_FIELD	ECU integrated in the vehicle and operating; this is the state of normal device use (and most secure state)
FA	ECU (device) failure; this is the state for functional testing of the IC

NXP ensures secure provisioning of the NXP credentials and secure life cycle configuration. NXP's customer (also referred as OEM) will receive the device in CUST_DEL state, and shall perform software installation and configuration and OEM credential provision in CUST_DEL and OEM_PROD states and then configure the device to IN_FIELD state in their technical and/or procedural secure environment. The IN_FIELD state is the normal device use state and the only state it can switch into is FA which needs both OEM and NXP credential authentication.

1.6.6 Configurations

Trusted execution (base product)

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

Security services (extended product)

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

1.6.7 Use Case

[trusted user only]

The final device is expected to be installed and operated inside a vehicle within a secured enclosure, hence not expecting any unauthorized user to have physical access to the device.

[any code]

It cannot be excluded that the product executes code which is unknown to the product developer.

3 Security Objectives for the Operational Environment

3.1 Platform Objectives for the Operational Environment

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

Table 7. Platform Objectives for the Operational Environment

Title	Description	Reference
Platform Verification	The operating system or application code are expected to verify the correct version of all platform components it depends on, and it shall match the corresponding information from the guidance document.	Section 7 of [4]
Secure Boot	The operating system or application code are expected to make use of the Secure Boot Mode by setting IVT Boot Configuration Word and Memory Verification Services.	Section 7.10 of [4]
Protection from Attacker's Physical Access	The operational environment must protect the TOE against physical access of attackers. Note: The TOE protects itself against LIMITED physical attacker resistance.	Section 4.3.5
Secure Debug	The integrating environment is expected to configure the debug functionality as described in Chapter 82 of [6] to meet the extra physical attacker resistance.	Chapter 82 of [6], Chapter 75 of [10]
Ensure UID Uniqueness	The platform has a 64-bit UID and NXP ensures uniqueness across platform instances. Although the probability is low to have the same UID for a platform instance with another type of device, the actors in charge of platform management shall ensure there is no UID confliction, and hence the UID is unique to the platform instance depending on use case.	Section 2.2.3 of [4]
Key Management out of the Platform	Cryptographic keys and certificates outside of the Platform are subject to secure key management procedures. Keys shall be provisioned for corresponding security functions, including: attestation, memory authentication and encryption, secure debug.	Section 6 of [4]
SW Integration	The operating system or application code are expected to ensure the correct version of the HSE firmware is integrated and configured	Sections 3 and 4 of [4]
Memory Protection	For IP and data that needs protection and prevent dump, it shall use memory verification function	Section 7 of [4]

Secure Update	The operating system or application code are expected to enable secure communication for security update, and in case of update, the update image is expected to be properly signed and distributed in secure manner as well. The operating system or application code are expected to use the anti-roll back feature.	Section 11 of [4]
Lifecycle Management	The operating system or application code are expected to configure the LC state according the stage of product development and deployment.	Section 2.3.8 of [4]
Cryptographic Algorithm and Key Length	The operating system or application code are expected to select an appropriate algorithm and key length set to fulfill the security requirement for the intended use case, including ECDSA P256 and SHA 256	[9]
Product Usage	The device manufacturer is expected to respect integration and usage manual and security guidance described in the SOC Reference Manual.	[6], [10]

4 Security Requirements and Implementation

4.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP Assurance Level 2 (SESIP2)** as defined in Chapter 4 of GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 [1].

4.1.1 Flaw Reporting Procedures (ALC_FLR.2)

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

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

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

The hardware and firmware located in the on-chip ROM of S32K3xx / MWCT2xxxS cannot be updated due to their immutable nature. The HSE FW has the capability of change and the platform's Secure Boot feature is able to verify the authenticity of HSE FW during the initial boot and outside of the boot sequence. See Section 4.3.2.1 for further information.

The platform's Secure Boot feature further supports to verify the authenticity of customer code, providing an appropriate mechanism for supporting the update of customer code. The update mechanism beyond of the scope of has to be provided by the customer, and such mechanism as well as the customer code is not in scope of this evaluation.

4.2 Security Process Packages

4.2.1 Secure Development

For the development of the platform, secure product development process according to NXP BCaM framework have been applied, and this process has been certified for

compliance to ISO/SAE 21434:2021 Road vehicles - cybersecurity engineering [9].

Conformance rationale:
This product was designed for maximum compliance with ISO/SAE 21434:2021 Road vehicles - cybersecurity engineering [13].

Some work products have been created retrospectively, i.e. after product planning and development, based on process artefacts sourced from NXP's Security Maturity Process (SMP) and other processes defined in the Business Creation and Management (BCaM) product development framework.

The project started before the standard ISO/SAE 21434 was available. An initial security relevance assessment, followed by a security risk assessment was performed according to existing NXP BCaM processes. During the development, when the DIS/FDIS of ISO/SAE 21434 became available, the project ensured that the existing work products could be mapped onto the work products expected by the standard.

The NXP-wide BCaM framework is a product development process framework that covers all harmonized processes to successfully launch new products, including new technologies and/or software. It was built on best practices and now serves as NXP's platform for continuous improvements. This process framework applies to all of NXP's R&D projects and enables NXP to work together more efficiently and effectively worldwide.

The BCaM framework includes a Security Module, with the Security Maturity Process (SMP) at its centre. This process is designed to ensure that product security is given due consideration throughout the development cycle beginning with incorporating security in the product architecture – in a concept of 'Security-by-Design' - and then approving Security Milestones during development. Security Milestones align with the BCaM product development project gates and milestones with the aim to ensure that security related deliverables and reviews are planned accordingly, and eventually successfully completed for each Security Milestone, and hence for each product development gate/ milestone.

NXP's BCaM process and its Product Security Incident Response Process (PSIRP), introduced in this section, are certified as compliant with the new standard ISO/SAE 21434:2021 Road vehicles - cybersecurity engineering [13].

See https://www.nxp.com/docs/en/company-information/TUV-SUV-ISO21434-CERTIFICATE.pdf.

4.3 Security Functional Requirements

In the following Security Functional Requirements, the term **platform** covers the **S32K3xx / MWCT2xxxS physical and logical scope**, and the term **application** refer to any additional firmware, OS or application software which is out of evaluation scope. It represents a part of the final connected device.

S32K3xx / MWCT2xxxS fulfils the following security functional requirements:

4.3.1 Identification and Attestation of Platforms and Applications

4.3.1.1 Verification of Platform Identity

Requirement

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

Refinement

Assets and protections related to this SFR are:

Table 8. Refinement Operations

Asset	Protection required
Secure Storage Subsystem (SSS) module Platform Identity	Integrity

Conformance rationale:

The hardware identification and version protected in integrity can be obtained as follows:

- Via JTAG as described in "System Integration Unit Lite2 (SIUL2)" of SOC reference manual (chapter 10.6.2 of [6], chapter 9.6.2 of [10]). The register name where this info is stored is “SIUL2 MCU ID Register #1 (MIDR1)”.
- HSE Firmware version is readable by using HSE Get Attribute Services and hseAttrFwVersion_t.64 bit
- SBAF version number can be read through HSE GPR register at address 0x4039C020

Please refer to Table 5 above for the expected identification and version numbers.

The identification is hardcoded (i.e. burned in OTP)

4.3.1.2 Verification of Platform Instance Identity

Requirement

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

Refinement

Assets and protections related to this SFRs are:

Table 9. Refinement Operations

Asset	Protection required
SSS module Platform Instance Identity	Integrity

Conformance rationale:

A 64-bit unique device identifier (UID) is provisioned to identify the SSS module platform identity. It can be read from the location 0x1B000040 in UTEST area and is protected in integrity. See Section 2.2.3 of [4] and 32.4.2 of [6].

The identification information is hardcoded (i.e. burned in OTP)

4.3.1.3 Attestation of Platform Genuineness

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

Conformance rationale:

Attestation of the platform genuineness is provided by UID for the HW and SHE-UID in conjunction with HSE status for FW and SBAF. Within those unique identifiers, data identifying the hardware platform uniquely with its different versions of SBAF and HSE can be retrieved by the user for assessment of genuineness against the

documentation. See [8].

For more information on UID, see section 2.2.3 of [4], for more information on SHE-UID and HSE status see sections 8.4 & 6.3 of [4].

HSE FW provides SHE-UID retrieve function where HSE return the UID and the 8 bit of HSE status with CMAC calculated over the concatenation of input challenge, UID and status using MASTER_ECU_KEY, where both the platform instance identity and the status are attested.

4.3.1.4 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 *reset state*.

Refinement

Assets and protections related to this SFRs are:

Table 10. Refinement Operations

Asset	Protection required
SSS module firmware	Integrity, authenticity

Conformance rationale:

SBAF has the responsibility to authenticate, decrypt and load HSE Firmware during firmware installation. Once the HSE FW is installed, SBAF passes the control to HSE firmware to perform a secure boot operation by authenticating the application images. SBAF ensures in particular the integrity and authenticity of the firmware. The complete initialization flow is described in HSE FW Reference Manual. See Chapter 2.6.1.2 of [4].

4.3.1.5 Attestation of Platform State

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

Conformance rationale:

See Section 4.3.1.3, 8 bit of HSE status is returned with CMAC protection.

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

4.3.2.1 Secure Update of Platform

Requirement

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

Refinement

Assets and protections related to this SFRs are:

Table 11. Refinement Operations

Asset	Protection required
SSS module Firmware and Software	Integrity
SSS module Firmware and Software	Monotonic

Conformance rationale:

The host can update FW-IMG via the service defined by the structure hseFirmwareUpdateSrv_t. This functionality ensures a monotonic update as well as maintaining its integrity.

New FW-IMG delivered by NXP is encrypted by Firmware Delivery Key (FDK) RSA 2048 at NXP's Trust Centre. FDK is stored in HSE-B OTP Storage area.

While performing the Secure Update, HSE reads the FDK to decrypt the new FW-IMG. This is how, confidentiality of the new FW-IMG is ensured in the update process.

New FW-IMG is signed by NXP's Private key at NXP's Trust Centre. New IMG is checked by the public key during the secure update process. The said public key is part of New FW IMG.

Hash of the public key is stored in OTP area of SoC during NXP's production

Above mechanisms establish authenticity and Integrity.

More details can be found in Chapter 11 “HSE Firmware Update” of [4] and in Chapter 4.7 “HSE Info Block” of [5].

4.3.3 Cryptographic Functionality

4.3.3.1 Cryptographic Operation – WPC Qi

Requirement

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

Refinement

Table 12. Cryptographic Operations – WPC Qi

Operation	Algorithm	Specification	Key Lengths / Message Lengths	Modes
Hashing	SHA 256	NIST FIPS 180-4	256 (message)	NA
Signature Generation	ECDSA P256	NIST FIPS 186-4	256 (key)	NA

Conformance rationale:

Cryptographic operations SHA256 and ECDSA256 are provided by HSE and HSE FW. See Section 6 of [4].

4.3.3.2 Cryptographic Operation – General MCU/MPU

Requirement

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

Table 13. Cryptographic Operations – General MCU/MPU

Operation	Algorithm	Specification	Key Lengths	Modes
Encryption/Decryption	AES	NIST FIPS 197	128	ECB, CBC, CTR, CFB, OFB
Hashing	SHA	NIST FIPS 180-4	160 224 256 384 512 224 256	SHA1 SHA224 SHA256 SHA384 SHA512 SHA512-224 SHA512-256
MAC Generation	CMAC, GMAC, HMAC	NIST SP800-38B NIST SP800-38D NIST FIPS 198-1	128 128 Max 512	NA
Authenticated Encryption	CCM, GCM	NIST SP800-38C NIST SP800-38D	128 128	NA
Signature Generation	RSA	NIST FIPS 186-4	1024, 2048, 3072, 4096	PKCS V1.5/PSS
Signature Generation	ECDSA P256, P384, P521	NIST FIPS 186-4	≥ 192 and ≤ 640	NA
Signature Generation	EdDSA 25519	NIST FIPS 186-5	255	NA
Key Exchange	RSA, ECDSA	NIST SP800-56A	1024, 2048, 3072, 4096 ≥ 192 and ≤ 640	NA
Encryption/Decryption	RSA	PKCS #1	1024, 2048, 3072, 4096	PKCS V1.5
Encryption/Decryption	RSA	PKCS #1	1024, 2048, 3072, 4096	OAEP

Conformance Rationale

Cryptographic operations are provided by HSE and HSE FW. See Section 6 of [4].

4.3.3.3 Cryptographic Key Generation – WPC Qi

Requirement

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

Refinement

Table 14. Cryptographic Key Generation – WPC Qi

ID	Algorithm	Specification	Key Lengths
ECC key generation	ECDSA P256	FIPS 186-4	256

Conformance rationale

Cryptographic key generations for ECC are provided by HSE and HSE FW. See Section 6 of [4].

4.3.3.4 Cryptographic Key Generation – General MCU/MPU

Requirement

The platform provides a way to generate cryptographic keys for use in *algorithms in* Table 15 as specified in *specifications in* Table 15 for key lengths *described in* Table 15

Refinement

Table 15. Cryptographic Key Generation – General MCU/MPU

ID	Algorithm	Specification	Key Lengths
RSA key generation	RSA	FIPS 186-4	1024, 2048, 3072, 4096
AES key generation	AES	NIST FIPS 197	128, 256
HMAC key generation	HMAC	NIST FIPS 198-1	Max 512
DH key agreement	DH	NIST SP800-56A	1024, 2048, 3072, 4096

Conformance rationale

Cryptographic key generation for RSA, AES, HMAC and DH are provided by HSE and HSE FW. See Section 6 of [4].

4.3.3.5 Cryptographic KeyStore – WPC Qi

Requirement

The platform provides a way to store *Qi private key ECDSA-P256* such that not even the application can compromise the *authenticity, integrity, confidentiality* of this data. This data can be used for the cryptographic operations *Qi authentication support of the Power Transmitter by the Power Receiver*.

Refinement

Table 16. Cryptographic KeyStore – WPC Qi

Assets	Security Property	List of Operations
Qi private key ECDSA-P256	Authenticity, integrity and confidentiality	Qi authentication support of the Power Transmitter by the Power Receiver

Conformance rationale

HSE provides key management functions. NVM and RAM key properties and values are stored and updated within SYS-IMG and saved securely in secure data flash . Furthermore, policies and access right authentications are implemented, and key access right is determined by execution rights, Host Identity (HID), and key attributes. This covers in particular the Qi private key ECDSA-P256. See Sections 6.1 to 6.3 of [4].

4.3.3.6 Cryptographic KeyStore – General MCU/MPU

Requirement

The platform provides a way to store *AES and HMAC secret keys, RSA and DH Key Pairs* such that not even the application can compromise the *authenticity, integrity, confidentiality* of this data. This data can be used for the cryptographic operations *Encrypt/Decryption, Mac generation, Signature generation and key exchange*.

Refinement

Table 17. Cryptographic KeyStore – General MCU/MPU

Assets	Security Property	List of Operations
AES Secret Key	Authenticity, integrity and confidentiality	Encryption/Decryption
HMAC Secret Key	Authenticity, integrity and confidentiality	MAC generation
RSA Key Pair (public and private)	Authenticity, integrity and confidentiality	Signature generation
DH Key Pair (public and private)	Authenticity, integrity and confidentiality	Key exchange

Conformance rationale

HSE provides key management functions. NVM and RAM key properties and values are stored and updated within SYS-IMG and saved securely in secure data flash . Furthermore, policies and access right authentications are implemented, and key access right is determined by execution rights, Host Identity (HID), and key attributes. This covers in particular the AES and HMAC Secret keys and RSA and DH key pairs. See Sections 6.1 to 6.3 of [4].

4.3.3.7 Cryptographic Random Number Generation

Requirement

The platform provides a way based on *DRBG* to generate random numbers to as specified in *NIST.SP.800-90A Hash-DRBG with SHA256*

Conformance rationale:

In the HSE, the source of entropy is provided by the physical true random number generator, and the generation function is part of a Deterministic Random Number Generator (DRNG, aka DRBG or PRNG) module as defined in NIST SP 800-90A and CAVP certified (refer to Section 2.5).

- TRNG is capable to pass AIS 31 statistical tests T0-T8
- DRNG is capable to pass AIS 20 statistical tests T1-T5

See more in Section 6.5 of [4].

4.3.4 Compliance Functionality

4.3.4.1 Residual Information Purging

The platform ensures that *user cryptographic keys*, with the exception of *none*, are erased using internal functions to clear temporary buffers before the memory is (re)used by the platform or application again and before an attacker can access it.

Conformance rationale:

Internal functions are used throughout the code to clear user keys and other temporary values stored in buffers.

4.3.4.2 Reliable Index

The platform implements a strictly increasing function.

Conformance rationale:

HSE FW provides Monotonic Counters Services. The HSE monotonic counters are 64-bit integers that can be read and only incremented until saturation. See more in Section 9.1 of [4].

4.3.4.3 Secure Debugging

Requirement

The platform only provides *JTAG interface* authenticated as specified in *Section 2.6.1.3.2 of [4]* with debug functionality.

The platform ensures that all user data stored, with the exception of data stored in external (outside SoC) storage is made unavailable.

Refinement

All assets defined in other Security Functional Requirements and accessible through the Secure Debugging mechanism shall be protected against unauthorized access. For debug functionality authentication, device specific credentials shall be used.

Conformance rationale

The debugging of the HSE subsystem and associated firmware is restricted to NXP engineering teams.

The host debug has a configuration option, wherein it can either protected or permanently disabled in OEM_PROD and IN_FIELD LC states.

In case of "protected", JTAG can be accessed by challenge Response Mechanism.

In case of permanently disabled, then even challenge-response does not give access. Hence, no debug is possible for such Chips.

The application can choose which configuration option needs to be used for their specific use cases.

See more in Section 2.6.1.3.2 of [4], Chapter 84 of [6] and Chapter 77 of [10].

4.3.5 Extra Attacker Resistance

4.3.5.1 Limited Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises *Secure Initialization of Platform, Secure Update of Platform, Cryptographic Operations – Qi Authentication, and Secure Debugging.*

Conformance rationale:

Countermeasures are implemented to harden the HSE firmware, SBAF, and IPs . These

countermeasures provide resistance against physical attacks.

4.3.5.2 Software Attacker Resistance: Isolation of Platform

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

Conformance Rationale:

The Hardware Security Engine (HSE) is the security subsystem, which enforces security measures for the application during system start-up and run-time, safekeeps security sensitive information (e.g. secret key values) for the application, and offloads the application from processing cryptographic operations with dedicated coprocessors. It has its own exclusive system resources and connects to the host via a dedicated interface, hence it is isolated from the host.

4.4 Trust Provisioning

The Trust Provisioning system ensures the secure management in a trusted environment of Qi Authentication keys and their loading into the platform for the following use cases: Authentication compliant with Qi Authentication.

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

Conformance Rationale:

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 an OEM for secure provisioning of their own assets. In a nutshell, 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 (2048 bits) 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 [12].

5 Mapping and Sufficiency Rationales

5.1 SESIP Sufficiency

Table 18. SESIP2 Sufficiency

Assurance Class	Assurance Family	Covered By	Rationale
ASE: Security target evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in Section 1.1, the TOE reference in Section 1.3, the TOE overview and description in Section 1.6.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in Section 2 refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	Section 3	All SFRs in this ST are taken from [1]. SFR "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	Section 3	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in the SFR.
ADV: Development	ADV_FSP.4 Complete functional specifications	Section 1.4	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_FLR.2 Flaw reporting procedures	Section 3.1.1	The flaw reporting and remediation procedure is described.
ATE: Test	ATE_IND.1 Independent testing: conformance	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.

AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	N.A. A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.	The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Basic.

6 Bibliography

6.1 Evaluation Documents

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

[2] SESIP Profile for WPC Qi Secure Storage Subsystem, Version 1.0

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

6.2 Developer Documents

[4] HSE_B Firmware Reference Manual, Rev 2.4, NXP Semiconductors, February 2025.

[5] HSE_B Firmware Reference Manual for GM, Rev 2.0, NXP Semiconductors, June 2022.

[6] S32K3xx Reference Manual, Rev 11, NXP Semiconductors, July 2025.

[7] S32K3xx Datasheet, Rev 5.2, NXP Semiconductors, October 2022.

[8] HSE Service API Reference Manual for S32K3x1, v0.2.40.0, Revision 12af7554cd, NXP Semiconductors, July 2022.

[9] AN649711, Selecting and using cryptographic algorithms and protocols, Rev 1.1, NXP Semiconductors, February 2024.

[10] MWCT2xxxS Reference Manual, Rev. 3, 09/2024

[11] MWCT2xxxS Product Data Sheet, Rev. 4, 09/2024

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

6.3 Standards

[13] ISO/SAE 21434:2021 Road vehicles - cybersecurity engineering, edition 1.0, 2021, ISO/SAE.

[14] NIST Special Publication 800-90A Revision 1 – Recommendation for Random Number Generation using Deterministic Random Bit Generators

7 Legal information

7.1 Definitions

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

7.2 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.

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

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

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

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

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

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

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

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

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

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

7.3 Trademarks

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

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

8 Tables

Figures

9 Contents

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

Date of release: 09 March 2026