S32R41

SESIP Security Target

Rev. 1.0 — 23 February 2026

Document information

Information	Content
Keywords	SESIP, Security Target, S32R41, S32R416, S32R418
Abstract	Security target for evaluation of the S32R41 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
1.0	23 February 2026	Public release

1 Introduction

This Security Target describes the S32R41 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) [2].

This Security Target also complies with the CEN norm EN 17927:2023 [1].

1.1 ST Reference

S32R41, SESIP Security Target, Revision 1.0, NXP Semiconductors, 23 February 2026.

1.2 SESIP Profile Reference and Conformance Claims

Table 1. SESIP Profile Reference and Conformance Claims

Reference	Value
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

1.3 Platform Reference

S32R41

Table 2. Platform Reference

Reference	Value
Platform Name and Version	S32R41, Rev 1.0 & 1.1 (Major_mask 0x00, Minor_mask 0x00) HSE Firmware for S32R41, RTM, v x.2.58.1, x=0/1
Platform Identification	S32R416, S32R418
Platform Type	Vehicle radar processor

1.4 Included Guidance Documents

The following documents are included with the platform:

Table 3. Guidance Documents

Document	Reference
SESIP Security Target	S32R41, SESIP Security Target, Revision 1.0, NXP Semiconductors, 23 February 2026.
Reference Manual	S32R41 Reference Manual [4]
Security Application Note	S32R41 Security application note [7]
Firmware Reference Manual	HSE_H/M Firmware Reference Manual [6]
Firmware API Reference Manual	HSE Service API Reference Manual for S32R41x [8]
Product Data Sheet	S32R41 Data Sheet [5]
Application Note	AN13023, Selecting and using cryptographic algorithms and protocols [9]

1.5 Other Certification

S32R41 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 [14]. See more in Section 3.2.1.

Item	Content
Scheme	ISO/SAE 21434:2021 [14]
Certification body	TÜV SÜD Product Service GmbH
Certification number	Q4B 109577 0002 Rev. 00
Certification date	2021-09-06

The RNG IP implemented in S32R41 has also been CAVP validated according to NISP SP 800-90A Hash-DRBG with SHA256 [13].

Item	Content
Scheme	Cryptographic Algorithm Validation Program (CAVP)
Certification body	National Institute of Standards and Technology (NIST)
Certification number	A5258 https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=17907
Certification date	22 April 2024

1.6 Platform Overview and Description

The Platform is the S32R41 automotive radar MPU which combines a high-performance radar accelerator, a powerfull processing unit, and an EVITA Full SHE+ ISO/SAE 21434 compliant hardware security engine. The S32R41 supports the needs for short, medium, and long range automative radar application in a compact form factor, developed in accrodance to ISO 26262 SEoOC methodology, and supporting ASIL B applications. The platform will be used by the application developer for final automotive use cases.

Security wise, NXP S32R41 provides:

- An application domain, also referred to as the host, which comprises various system resources including one Cortex-A53 (application & processing) and one Cortex-M7 (real time) 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 "M" variant of the Hardware Security Engine (HSE) subsystem, also referred as HSE in the rest of this document. It has its own exclusive system resources and connects to the host via a dedicated interface.
- A Radar domain with a radar processing accelerator and a DSP.

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

- 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 (i.e. HSE system attributes, CR/SMR entries, OTFAD contexts), hereafter referred to as **SYS-IMG**

NXP offers standard and premium versions for HSE firmware, which are all in evaluation scope, while the premium version provides expanded security capabilities. See Table 4 for the difference between the standard version and the premium version.

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

Table 4. HSE Firmware Difference: Standard vs Premium

HSE firmware variant	Standard	Premium
ECC max key size	256 bits	640 bits
RSA max key size	2048 bits	4096 bits
HMAC max key size	512 bits	1152 bits
Number of keys in RAM	20	User configurable
Number of symmetric keys in NVM	40	User configurable
Number of asymmetric keys in NVM	12	User configurable
SHA3, IPSec, Classic DH, and Burmester-Desmedt services	Not supported	Supported
SMR (Secure Memory Region)	8	32
CR (Core Reset)	4	16

1.6.1 Platform Security Features

The Hardware Security Engine (HSE_M) is a subsystem that implements the security functions for the device. It provides cryptographic services to the host CPUs and the network accelerators, and fully meets the functional goals and objectives of the common automotive security specifications Secure Hardware Extension (SHE+), Hardware Security Module (HSM), and E-safety Vehicle Intrusion Protected Application (EVITA) Full.

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

- Secure boot of customer code using asymmetric or symmetric keys
- Highly featured symmetric and asymmetric accelerators
- Support for various cryptographic functions (see Section 3.3.4.1)
- Arm Cortex-M7 CPU
- True Random Number Generator (TRNG)
- Pseudo Random Number Generator (PRNG)
- Firmware Over-the-Air (FOTA) support.
- Secure Debug

1.6.2 Platform Physical Scope

The physical scope is the S32R41 microcontroller silicon chip including the on-chip ROM. The hardware components and interfaces are listed in Section 2.4 of [4] and Figure 1 shows the superset block diagram of the S32R41 family.

Figure 1. S32R41 Family Superset Block Diagram

1.6.3 Platform Logical Scope

The Target Of Evaluation (TOE) is the hardware (including the on-chip ROM) and the flash loadable updatable HSE firmware (i.e. FW-IMG and SYS-IMG) (either standard version or premium version) as shown in Figure 2. The versions for each components 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.

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

Table 5. Platform Deliverables

Type	Name	Release	Form of delivery
IC Hardware	S32R41	Rev 1.0 & 1.1 (Major_mask 0x00, Minor_mask 0x00)	Silicon Chip and On Chip ROM
HSE Firmware	HSE Firmware for S32R41	RTM, v x.2.58.1 x=0, Standard Version x=1, Premium Version	Software package

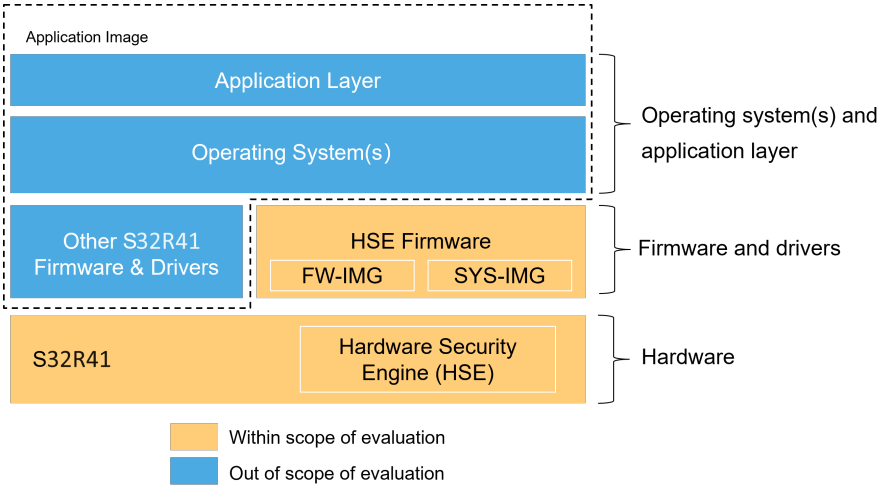

Figure 2. S32R41 Evaluation Scope

1.6.4 Required Non-Platform Hardware/Software/Firmware

S32R41 has no internal flash, hence compatible external non-volatile memory shall be deployed for image storage with sufficient size. See Chapter 37 of [4] for compatible external flash.

1.6.5 Life Cycle

The life cycle (LC) is managed by the HSE subsystem, see Section 3.3.8 of [6] and Section 8 of [7] for further information. The LC states after NXP manufacturing are as Table 6:

Table 6. Life Cycle States

LC State	Description
Production	Device (i.e. NXP's IC) is under development at NXP
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)
PRE_FA mode	Normal device usage. Additionally, it provides capabilities for failure analysis. This mode is available within OEM_PROD and IN_FIELD lifecycle.
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. The PRE_FA and FA states can be reached from the OEM_PROD and IN_FIELD states, and switching into FA needs both OEM and NXP credential authentication.

1.6.6 Configurations

Base SP Security Functional Requirements

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

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

Software Isolation

The base security features are complemented by mechanisms needed to cover the use case where the final IoT product allows the execution of untrusted code and/or requires access restrictions to the platform features by the upper level.

1.6.7 Use Case

[trusted user only]

The final product is expected to be installed and operated inside a vehicle within a secured enclosure, hence it is not expected to be physically accessible to unknown or untrusted users.

[any code]

The final product is expected to run only authorized code, but it cannot be excluded that the product executes code which is unknown to the product developer or which is unintentionally harmfull to the platform.

2 Security Objectives for the Operational Environment

2.1 Platform Objectives for the Operational Environment

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

Table 7. Platform Objectives for the Operational Environment

Title	Description	Reference
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 3.3.1.1
Secure Boot	The operating system or application code are expected to make use of the Secure Boot Mode by blowing the BOOT_CFGn, FUSE_SEL, FUSE_CFG_ LOCK and IVT_AUTH fuses, by setting the IVT Boot Configuration Word [BOOT_SEC], by configuring the Memory Verification Services, and by securely provisionning device-dependent ADPK.	Sections 4 and 5 of [7], Section 31 of [4], Section 8 of [6]
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 1.6.7
Secure Debug	In order to meet the physical attacker resistance, the integrating environment is expected to configure the debug functionality as described in Section 3.6.2 of [6] by securely provisionning a device-dependent ADPK.	Section 3.6.2 of [6].
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 2.1
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 7 of [6]
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. As a flash-less device, there is finite number of anti-roll back counter updates (fuses) and further procedure shall be taken once the counter limit is reached.	Sections 6.5 and 11 of [6]
SW Integration	The operating system or application code are expected to ensure the correct version of the HSE firmware is integrated and configured	Sections 4 and 5 of [6]
Memory Protection	For IP and data that needs protection in authenticity, integrity and confidentiality, memory verification function (SMR Authentication, SMR Decryption) and Flash encryption (OTFAD) shall be used.	Section 8 and 10.2 of [6]
Lifecycle Management	The operating system or application code are expected to configure the LC state according the stage of product development and deployment.	Section 3.3.8 of [6]
Cryptographic Algorithm and Key Length	A few well-established cryptographic algorithms supported by the platform is of known limitation, e.g. SHA1, and key length for each algorithm has a direct impact on the cryptographic strength. 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.	[9]

3 Security Requirements and Implementation

3.1 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 [2].

3.1.1 Flaw Reporting Procedures (ALC_FLR.2)

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

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

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

The hardware and firmware located in the on-chip ROM of S32R41 cannot be updated due to their immutable nature. The HSE Firmware has the capability of change and the platform's Secure Boot feature is able to verify the authenticity of HSE Firmware during the initial boot and outside of the boot sequence. See Section 3.3.2.1 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 has to be provided by the customer, and such mechanism as well as the customer code is not in scope of this evaluation.

3.2 Security Process Packages

3.2.1 Secure Development

For the development of the platform, the secure development process specified in ISO/SAE 21434:2021 Road vehicles - cybersecurity engineering [14] has been applied to the platform.

Conformance rationale:

This product was designed for maximum compliance with ISO/SAE 21434:2021 Road vehicles - cybersecurity engineering [14].

During the development, the project ensured that the existing work products could be mapped onto the work products expected by the DIS/FDIS of ISO/SAE 21434 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 Section 3.1.1, are certified as compliant with the new standard ISO/SAE 21434:2021 Road vehicles - cybersecurity engineering [14]. See https://www.nxp.com/docs/en/company-information/TUV-SUV-ISO21434-CERTIFICATE.pdf.

3.3 Security Functional Requirements

In the following Security Functional Requirements, the term **platform** covers the **S32R41 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.

S32R41 fulfils the following security functional requirements:

3.3.1 Identification and Attestation of Platforms and Applications

3.3.1.1 Verification of Platform Identity

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

Conformance rationale:

The hardware identification and version can be obtained by reading register SIUL2 MCU ID Register #1 (MIDR1) per Section 18.3.2 of [4]. The content shall match the value identified in Section 1.3 and Section 1.6.3.

The Platform Identification can be obtained using JTAG as per Section 63.6.2 of [4].

HSE Firmware version is readable by using HSE Get Attribute Services and `hseAttrFwVersion_t`. (See Section 9.1.3 of [6]).

The production validation process ensures that the SFR behaves correctly.

3.3.1.2 Verification of Platform Instance Identity

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

Conformance rationale:

A 64-bit unique device identifier (UID) is provisioned. See Section 3.2.3 of [6]. It can be retrieved via JTAG (see sections 63.26.6 and 63.26.7 of [4]) or via the service defined by the structure hseSheGetIdSrv_t (see section 9.6 of [6]).

The production validation process ensures that the SFR behaves correctly.

3.3.1.3 Attestation of Platform Genuineness

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

Conformance rationale:

HSE Firmware provides SHE-UID retrieve function via the service defined by the structure hseSheGetIdSrv_t. This function returns the UID and the HSE status with a CMAC value. The CMAC is calculated over the input challenge, the UID and the status, and the key used is `MASTER_ECU_KEY`. Hence both the platform instance identity and the status are attested. See Section 9.6 of [6].

The production validation process ensures that the SFR behaves correctly.

3.3.1.4 Attestation of Platform State

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

Conformance rationale:

See Section 3.3.1.3, 8 bit of HSE status is returned with CMAC protection.

3.3.1.5 Secure Initialization of Platform

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

Conformance rationale:

BootROM has the responsibility to authenticate, decrypt and load HSE Firmware when performing a secure boot operation. Then HSE Firmware will take over and is capable to authenticate the system image. The authentication scheme followed by BootROM to accomplish secure boot is shown in Sections 4 and 5 of [7], see also Section 8 of [6] for further information.

The production validation process ensures that the SFR behaves correctly.

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

3.3.2.1 Secure Update of Platform

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

Conformance rationale:

The host can update FW-IMG via the service defined by the structure `hseFirmwareUpdateSrv_t`. See Section 11 of [6].

The SYS-IMG is updatable. See Section 6.5 of [6].

Memory verification services by HSE provides capability of secure update of the application image. See Section 8 of [6].

An anti-rollback protection is provided on both FW-IMG and SYS-IMG, which prevents the possibility to use a previous version of those images when they have been replaced by newer versions. See Section 11.3 of [6].

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

3.3.2.2 Field Return of Platform

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

Conformance rationale:

Field Analysis Mechanism is available as described in Chapter 3.3.8 of [6]. Entering PRE_FA mode (from OEM_PROD or In_FIELD) requires both OEM credential (ADKP) and NXP credential and enables a limited set of test features while keeping the possibility to return to OEM_PROD or In_FIELD lifecycle state after a reset. Entering FA lifecycle state (from any state) requires NXP credential and is irreversible. Once entered in FA mode, device specific keys used to encrypt FW-IMG and SYS-IMG are irreversibly destroyed, hence all stored assets and information encrypted by the keys in HSE firmware are not accessible anymore.

The production validation process ensures that the SFR behaves correctly.

3.3.3 Extra Attacker Resistance

3.3.3.1 Limited Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises *Verification of Platform Identity, Verification of Platform Instance Identity, Attestation of Platform Genuineness, Attestation of Platform State, ecure Initialization of Platform, Secure Update of Platform, Field Return of Platform, Software Attacker Resistance:Isolation of Platform, Cryptographic Operation, Cryptographic Key Generation, Cryptographic KeyStore, Cryptographic Random Number Generator, Secure External Storage (FW-IMG, SYS-IMG and Secure Memory Region), Residual Information Purging, Reliable Index and Secure Debugging.*

Conformance rationale:

Countermeasures are implemented to harden the boot ROM and IPs and the functions provided by boot ROM provides resistant against physical attacks.

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

Software protections in ROM and loadable firmware, and hardware protections (voltage, temperature, frequency detectors) are in place against fault injections. See section 10 of [7].

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

3.3.3.2 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 is isolated from the host by having its own exclusive system resources and connecting to the host via a dedicated interface (Messaging Unit - MU). See Section 3.5.1 of [6].

The production validation and internal vulnerability analysis processes ensure that the SFR behaves correctly.

3.3.4 Cryptographic Functionality

3.3.4.1 Cryptographic Operation

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

Table 8. Cryptographic Operations

Operation	Algorithm	Specification	Key Lengths	Modes
Encryption and decryption	AES	NIST FIPS 197 NIST SP 800-38A	128, 192, 256	ECB, CBC, CTR, CFB, OFB
MAC generation and verification	AES	RFC 3566 NIST SP 800-38B NIST SP 800-38D	128	XCBC-MAC [1], CMAC, GMAC
MAC generation and verification	SHA 1, SHA 2 [2]	FIPS PUB 198-1	Up to 512 [3], or Up to 1152[1]	HMAC
MAC generation and verification	SipHash	[10]	64[2], 128	CMAC, CBC-MAC, Retail MAC
Hashing	SHA 1 [2]	NIST FIPS 180-4	160	-
Hashing	SHA 2 [2]	NIST FIPS 180-4	224, 256, 384, 512	-
Hashing	SHA 3[1]	NIST FIPS 202	224, 256, 384, 512	-
Hashing	Miyaguchi-Preneel Compression with AES	[11]	128	-
Authenticated encryption with associated data (AEAD) and authenticated decryption	AES	NIST SP 800-38D NIST SP 800-38C	128, 192, 256	GCM, CCM
Signature generation and verification	RSA	PKCS#1 v2.2	Up to 2048[3], or Up to 4096[1]	PKCS1 v1.5, PSS
Signature generation and verification	ECDSA	Standards for Efficient Cryptography 1 (SEC1)	Up to 256[3], or Up to 640[1]	-
Signature generation and verification	EdDSA [2]	RFC8032	256, 448	Ed25519, Ed448
Encryption, decryption	RSA	PKCS#1 v2.2	Up to 2048[3], or Up to 4096[1]	PKCS1 v1.5, OAEP padding
KDF	CKDF	NIST SP 800-108 NIST SP 800-56C R1	See CMAC and HMAC or Hashing	-
KDF	PBKDF2	RFC8018	See HMAC	-
KDF	TLS v1.2 PRF	RFC 5246, RFC 7627, RFC 4279, RFC 5489		

Table 8. Cryptographic Operations*...continued*

Operation	Algorithm	Specification	Key Lengths	Modes
KDF	HKDF	RFC 5869	See HMAC	
KDF	The internnet Key Exchange V2 (IKEv2) rekeying functions	RFC 4306		
KDF	Standards for Efficient Cryptography 1 (SEC1)	ANSI X9.63		
KDF	ISO18033 KDF1, KDF2	ISO/IEC 18033-2:2006		
Key Exchange	ECDH	NIST FIPS 800-56A	Up to 256[3], or Up to 512[1]	-
Key Exchange	Classic DH	[12]	Up to 2048[3], or Up to 4096[1]	-

[1] Only supported by HSE premium firmware.
[2] Refer to [9] for considerations on algorithm and key lengths.
[3] Supported by HSE standard firmware.

Conformance rationale:

Cryptographic operations are provided by HSE and HSE Firmware. See Section 7 of [6].

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

3.3.4.2 Cryptographic Key Generation

The platform provides a way to generate cryptographic keys for use in *algorithms in Table 9* as specified in *specifications in Table 9* for key lengths *described in Table 9*

Table 9. Cryptographic Key Generation

ID	Algorithm	Specification	Key Lengths
AES	Random Number Generator		128, 192, 256
HMAC	Random Number Generator		Up to 512[1], or Up to 1152[2]
SIPHASH	Random Number Generator		64, 128
ECC	ECC	ANSI X9.62	Up to 256[1], or Up to 640[2]
RSA	RSA	PKCS#1	Up to 2048[1], or Up to 4096[2]

[1] Supported by HSE standard firmware.
[2] Only supported by HSE premium firmware.

Conformance rationale:

Cryptographic key generations are provided by HSE and HSE Firmware. See Section 7.2 of [6].

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

3.3.4.3 Cryptographic KeyStore

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:

HSE Firmware provides key management functions. NVM and RAM key properties and values are stored and updated within SYS-IMG and saved securely in NVM by device specific keys. Furthermore, policies and access right authentications are implemented, and key access right is determined by execution rights, Host Identity (HID), and key attributes. See Sections 7.1 to 7.3 of [6].

The production validation process ensures that the SFR behaves correctly.

3.3.4.4 Cryptographic Random Number Generation

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

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 1.5).

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

See more in Section 7.5 of [6].

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

3.3.5 Compliance Functionality

3.3.5.1 Secure Data Serialization (FW-IMG, SYS-IMG and Secure Memory Region)

The platform ensures that all data stored outside the direct control of the platform, except for *non-secure memory regions* is protected such that the *confidentiality, integrity, authenticity, binding to the platform instance, versioning* is ensured.

Conformance rationale:

Both FW-IMG and SYS-IMG are encrypted and authenticated with device-dependent keys (See Section 3.3.7 of [6]).

A secure memory region (SMR) is defined by a start address and a size, associated to a proof of authenticity, either a MAC or RSA/ECC signature. The host can define up to 32 SMRs clustered into the SMR table which is stored in SYS-IMG. See Section 8 of [6].

An anti-rollback protection by fuses is provided on both FW-IMG and SYS-IMG, which prevents the possibility to use a previous version of those images when they have been replaced by newer versions. As SMR table is stored in SYS-IMG, its binding to platform instance and versioning is also achievable by SYS-IMG encryption, authentication and anti-rollback.

The production validation process ensures that the SFR behaves correctly.

3.3.5.2 Secure Data Serialization (On-the-fly AES decryption)

The platform ensures that all data stored outside the direct control of the platform, except for *data not in the protected regions*, is protected such that the *confidentiality* is ensured.

Conformance rationale:

Application code and data stored encrypted in an external Flash accessible via the QuadSPI can be decrypted via the On-the-fly AES decryption (OTFAD), in complete transparency (“on-the-fly”) for the host and with zero latency (no additional read cycles). See Section 10.2 of [6].

The production validation process ensures that the SFR behaves correctly.

3.3.5.3 Residual Information Purging

The platform ensures that *keys with matched host identity*, with the exception of *none*, is erased using the method specified in *FIPS 140-3 using overwriting with Zeros* before the memory is used by the platform or application again and before an attacker can access it.

Conformance rationale:

NVM and RAM key slots can be securely deleted by the host via a service defined by the structure `hseEraseKeysSrv_t`. See Section 7.2.9 of [6].

The production validation process ensures that the SFR behaves correctly.

3.3.5.4 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 10.1 of [6].

The production validation process ensures that the SFR behaves correctly.

3.3.5.5 Secure Debugging

The platform only provides *JTAG interface* authenticated as specified in *NIST FIPS 197 & NIST SP800-38A* with debug functionality.

The platform ensures that all data stored by the application, with the exception of *no data*, is made unavailable.

Conformance rationale:

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

In OEM_PROD, IN-FIELD, and PRE_FA lifecycle state, the host debug is protected by an AES ECB challenge/response authentication or permanently disabled by configuring the DEBUG_DISABLE OTP. See more in Section 3.6.2 of [6] and Chapter 63-66 of [4].

The production validation process ensures that the SFR behaves correctly.

4 Mapping and Sufficiency Rationales

4.1 SESIP2 Sufficiency

Table 10. 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 [2]. SFR "Verification of Platform Identity" is included. SFR "Secure Update of Platform is included". The SARs are an exact SESIP assurance level. No multiple assurance level is claimed.
	ASE_TSS.1 TOE Summary Specification	Section 3	All SFRs are listed per definition, and for each SFR the implementation and verification 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.

4.2 SESIP Profile Conformance Mapping

This section provides rationales of conformance claimed in Section 1.2

Table 11. 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 3.3.1.5
	Secure Updated of Platform	Section 3.3.2.1
	Residual Inforamtion Purging	Section 3.3.5.3
	Secure Debugging	Section 3.3.5.5
Security Services	Cryptographic Operation	Section 3.3.4.1
	Cryptographic Key Generation	Section 3.3.4.2
	Cryptographic KeyStore	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

4.3 Cybersecurity Assurance Level 4 (CAL4) Sufficiency Rationales (Informative)

This section provides the informative CAL4 sufficiency rational as introduced in Annex E of ISO/SAE 21434:2021 Road vehicles - cybersecurity engineering [14], where four levels of Cybersecurity Assurance Level (CAL) is described, and CAL4 is the highest level. Given the fact that the annex in [14] is informative and only examples are provided without rigorous definition, this section can only provide demonstration on how this SESIP evaluation can help to meet the requirements of CAL4, rather than rigorous conformance analysis.

Also, this section only refers to the activities performed during this SESIP evaluation. NXP has deployed internal processes and procedures for product development and governance, not necessarily to have external evaluation or certification, to ensure ISO21434 compliance and they are certified as stated in Section 3.2.1. This section will not map NXP internal process and deliverables, but only to demonstrate the sufficiency from this SESIP evaluation. The following tables provide the requirements from Annex E of [14] and sufficiency rationals.

Table 12. Cybersecurity Assurance Level 4 (CAL4) expected rigour in cybersecurity assurance measures and sufficiency rationales

	CAL4 Requirement	Covered by	Rationale
a) Methods to provide confidence that cybersecurity activities are performed with appropriate rigour	All combinations of interactions between components are tested	Section 3.2.1, SESIP Methodology and certification scheme, and AVA: Vulnerability assessment	The performance of cybersecurity activities are covered by this evaluation in several folds: As covered by the claim in Section 3.2.1, this evaluation verifies the ISO/SAE21434 certified process has applied to the product development. Furthermore, SESIP evaluation covers various cybersecurity actives. SESIP Methodology is of strong formalism as it is stated in the standard [2], and the certification scheme with lab and certifier setup further ensures that the certifier reviews the lab evaluation, and hence the evaluation meets the expected rigorous. For the testing coverage, the evaluated scope as illustrated in Figure 2 serves as a (sub)component for an embedded system inside a road vehicle. The security evaluation activities performed by an independent evaluator includes a review of the SAF85xx critical code (boot ROM, HSE Firmware), a vulnerability analysis, and penetration testing. Fuzz testing is part of the penetration testing that the evaluator can decide to apply based on its independent

Table 12. Cybersecurity Assurance Level 4 (CAL4) expected rigour in cybersecurity assurance measures and sufficiency rationales*...continued*

	CAL4 Requirement	Covered by	Rationale
			vulnerability analysis. Fuzzing with random vectors has been applied on other products of the same familly without reveling any issue.
b) Methods to provide confidence that unmanaged vulnerabilities do not remain	Activities such as analysis and/or testing to search for vulnerabilities by exploratory methods	AVA: Vulnerability assessment	Vulnerability assessment and further on penetration testing required by SESIP AVA assurance components are of exploratory nature.
c) Independence scheme to provide confidence that the cybersecurity activities performed are appropriate	Cybersecurity assessments are carried out by a person who is independent regarding management, resources and release authority from the originating department	SESIP Methodology and certification scheme	SESIP Methodology by nature is carried out by 3rd party evaluator and another 3rd party certifier further verifies the compliance to the methodology for the SESIP scheme used.

Table 13. Example of level of independence of cybersecurity activities and sufficiency rationales

Activity	CAL4 Requireme	Definition of required level	Covered by	Rationale
Verification of cybersecurity concept and design activities	I2	The activity is performed by a person who is independent from the team that is responsible for the creation of the considered work product(s), i.e. by a person reporting to a different direct superior.	ASE: Security target evaluation, and ADV: Development	The covered by column provides the corresponding activities in SESIP evaluation that map into ISO/SAE21434 activities. SESIP Methodology by nature is carried out by 3rd party evaluator and another 3rd party certifier further verifies the compliance to the methodology for the SESIP scheme used.
Verification of the implementation and integration of components			ATE: Test	
Cybersecurity validation			SESIP evaluation process, particularly AVA: Vulnerability assessment	
Cybersecurity assessment	I3	The activity is performed by a person who is independent, regarding management, resources and release authority, from the department responsible for the creation of the considered work product(s).	SESIP evaluation process and certification scheme setup	

Table 14. Example of parameters of testing methods and sufficiency rationales

Activity	CAL4 Requireme	Definition of required level	Covered by this evaluation	Rationale
Functional testing	T2	based on requirements and interactions between components	ATE: Test	The ATE component is for functional testing, and it is based on the requirements on this security target

Table 14. Example of parameters of testing methods and sufficiency rationales*...continued*

Activity	CAL4 Requireme	Definition of required level	Covered by this evaluation	Rationale
Vulnerability scanning	T1	for known vulnerabilities	AVA: Vulnerability assessment	Scanning for known vulnerabilities is mandated for the scheme used
Fuzz testing	T2	with an increased number of test case iterations and/or adaptive selection of inputs	AVA: Vulnerability assessment	Fuzz testing is part of the penetration testing that the evaluator can decide to apply based on its independent vulnerability analysis.
Penetration testing	T2	assuming higher attacker expertise, knowledge of the item or component and/or resources	ADV: Development, and AVA: Vulnerability assessment	The evaluator selected is well recognized in the industry and further vouched by the scheme used. NXP provided full software source code to the evaluator even this is not mandated for SESIP2 level.

5 Bibliography

5.1 Evaluation Documents

[1] Security Evaluation Standard for IoT Platforms (SESIP), CEN, EN 17927:2023.
[2] GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2, GP_FST_070.
[3] GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs, Version 1.0, GPT_SPE_150.

5.2 Developer Documents

[4] S32R41 Reference Manual, S32R41RM, Rev 2, NXP Semiconductors, November 2022.
[5] S32R41 Data Sheet, Rev 2, NXP Semiconductors, November 2022.
[6] HSE_H/M Firmware Reference Manual, HSEFWRM, Rev 2.6, NXP Semiconductors, March 2025.
[7] S32R41 Security application note, AN13926, Rev 1.0, NXP Semiconductors, 10 July 2023.
[8] HSE Service API Reference Manual for S32R41x, v1.2.58.1, Revision 4ecfd9522a, NXP Semiconductors, Feb 2025.
[9] AN13023, Selecting and using cryptographic algorithms and protocols, ref. 639712, Rev 1.2, NXP Semiconductors, 16 April 2025.

5.3 Standards

[10] J. Aumasson, et al, SipHash: A Fast Short-Input PRF, Progress in Cryptography - INDOCRYPT 2012, pp 489-508.
[11] Specification of Secure Hardware Extensions, Release R19-11, AUTOSAR, 2019.
[12] W. Diffie and M Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory. 22 (6): 644–654.
[13] NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology, January 2012.
[14] ISO/SAE 21434:2021 Road vehicles - cybersecurity engineering, edition 1.0, 2021, ISO/SAE.

Legal information

Definitions

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

Disclaimers

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Trademarks

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

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

Tables

Figures

Contents