S32G2

SESIP Security Target

Rev. 1.3 — 2 March 2022

Evaluation document

Document information

Information	Content
Keywords	SESIP, Security Target, S32G2, S32G274A, S32G254A, S32G233A, S32G234M
Abstract	Security target for evaluation of the S32G2 developed and provided by NXP Semiconductors, according to SESIP Assurance Level 2 (SESIP2) based on SESIP methodology, version 1.1

Revision History

Rev.	Date	Description
1.0	4 January 2022	Initial release
1.1	14 January 2022	Corrected an editorial error in Secure Update of Platform and product name
1.2	7 February 2022	Updated in Section 3.3.4 according to evaluator feedback
1.3	2 March 2022	Updated in Section 3.3.4.4 according to evaluator feedback

1 Introduction

This Security Target describes the S32G2 platform and the exact security properties of the platform that are evaluated against GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.1, SESIP Assurance Level 2 (SESIP2) [1].

1.1 ST Reference

S32G2, SESIP Security Target, Revision 1.3, NXP Semiconductors, 2 March 2022.

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 [2]
SP Version	Version 1.0
Assurance Claim	SESIP Assurance Level 2 (SESIP2)
Package Claim	Base SP, Package Secure Services, Package Software Isolation

1.3 Platform Reference

S32G2

Table 2. Platform Reference

Reference	Value
Platform Name and Version	S32G2, Rev 2.0 HSE Firmware for S32G2XX, v x.1.0.0, x=0/1
Platform Identification	S32G2, S32G274A, S32G254A, S32G233A, S32G234M
Platform Type	Vehicle network processor

1.4 Included Guidance Documents

The following documents are included with the platform:

Table 3. Guidance Documents

Document	Reference
Product Reference Manual	S32G2 Reference Manual [3]
Firmware Reference Manual	HSE_H Firmware Reference Manual [7]
Product Data Sheet	S32G2 Data Sheet [4]
Application Note	AN12978, S32G2 Support for Firmware Over The Air Updates [5]
Application Note	AN12422, S32G2 Boot Process [6]
Firmware API Reference Manual	HSE Service API Reference Manual for S32G2XX [8]
Firmware API Reference Manual	HSE Service API Reference Manual for S32G2XX [9]
SESIP Security Target	S32G2, SESIP Security Target, Revision 1.3, NXP Semiconductors, 2 March 2022.

Table 3. Guidance Documents*...continued*

Document	Reference
Application Note	AN13023, Selecting and using cryptographic algorithms and protocols [10]

1.5 Other Certification

S32G2 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 [15]. See more in Section 3.2.

Item	Content
Scheme	ISO/SAE 21434:2021 [15]
Certification body	TÜV SÜD Product Service GmbH
Certification number	Q4B 109577 0002 Rev. 00
Certification date	2021-09-06

The RNG IP implemented in S32G2 has also been CAVP validated accoridng to NISP SP 800-90A Hash-DRBG with SHA256 [14].

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

1.6 Platform Overview and Description

S32G2 vehicle network processors combine ASIL D safety, hardware security, high-performance real-time and application processing, and network acceleration. S32G2 supports the needs of new vehicle architectures: service-oriented gateways, domain controllers, zonal processors, safety processors and more. The platform will be used by the application developer for final automotive use cases.

NXP S32G2 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_H. 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**

NXP offers standard and premium versions for HSE firmware, which are all in evaluation scope, while the premium version 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, and it is not in scope of this evaluation, and hereafter referred as application image.

Table 4. HSE Firmware Difference: Standard vs Premium

HSE firmware variant	Standard	Premium
ECC max key size	256 bits	512 bits
RSA and DH max key size	2048 bits	4096 bits
HMAC max key size	512 bits	1152 bits
Number of keys in RAM	20	User configuratable
Number of keys in NVM	12 (asym) + 40 (sym)	User configuratable
SHA3	Not available	Supported
XCBC-MAC	Not available	Supported
Max number of memory regions verified	4	32
IPSec protocol offloads	Not available	Supported

1.6.1 Platform Security Features

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

The HSE_H 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 S32G2 microcontroller silicon chip including the on-chip ROM. The hardware components and interfaces are listed in Section 2.4 of [3] and Figure 1 shows the superset block diagram of the S32G2 family.

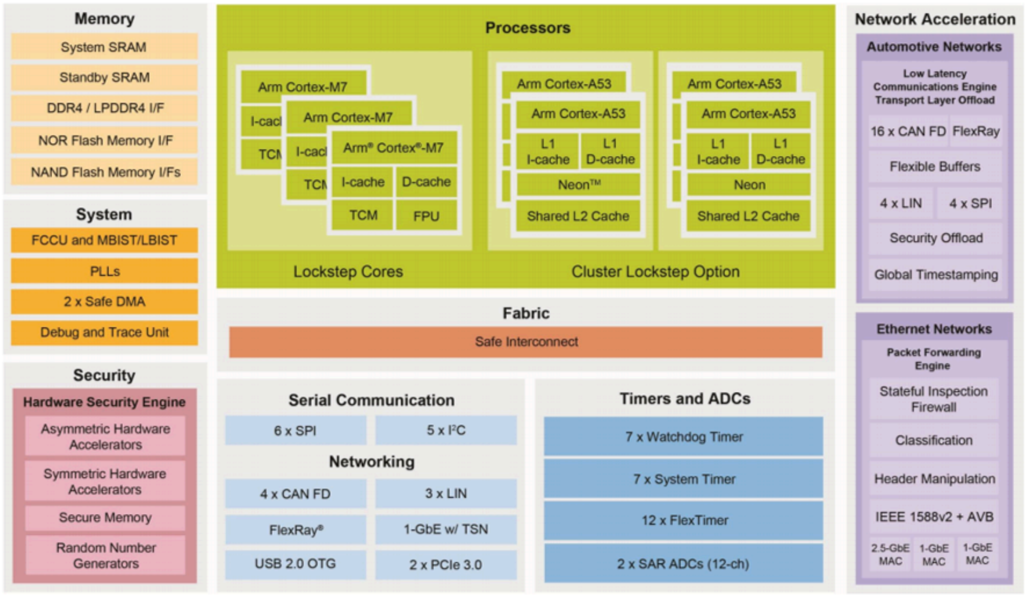

Figure 1. S32G2 Family Superset Block Diagram

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	S32G2	Rev 2.0	Silicon Chip and On Chip ROM

HSE Firmware	S32G2 HSE Firmware	x.1.0.0
		x=0, Standard Version
		x=1, Premium Version
			Software package

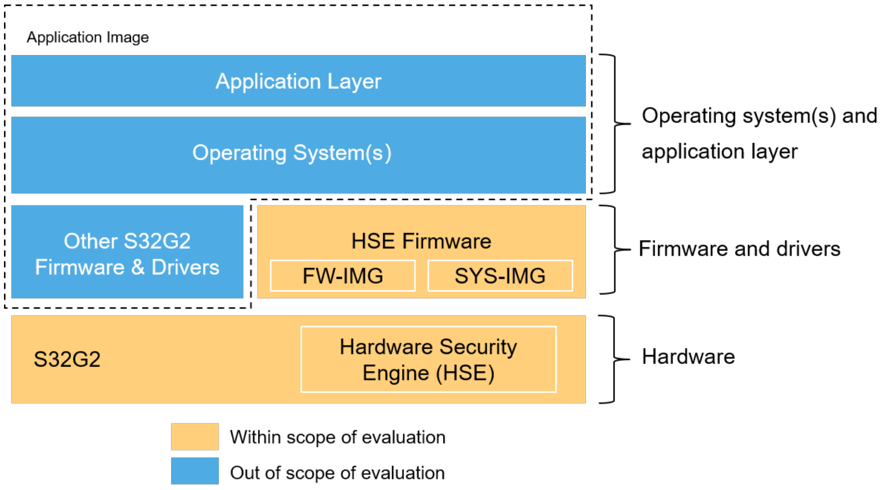
Application Image
Application Layer
Operating System(s)
Operating system(s) and application layer
Other S32G2 Firmware & Drivers
HSE Firmware
FW-IMG
SYS-IMG
Firmware and drivers
S32G2
Hardware Security Engine (HSE)
Hardware
Within scope of evaluation
Out of scope of evaluation

Figure 2. S32G2 Evaluation Scope

1.6.4 Required Non-Platform Hardware/Software/Firmware

S32G2 has no internal flash, hence compatible external non-volatile memory shall be deployed for image storage with sufficient size. See Sections 38, 39 of [3] for compatible external flash.

S32G2 also supports external DRAM (See Chapter 36 of [3]) but the functions in the evaluation scope only use internal SRAM hence the DRAM is not required.

1.6.5 Life Cycle

The life cycle (LC) is managed by the HSE subsystem, see Section 3.3.8 of [7] 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.

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 setting IVT Boot Configuration Word and Memory Verification Services.	Section 3.12-3.14 of [6], Section 30.11 of [3], Section 8 of [7]
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 2.1
Secure Debug	The integrating environment is expected to configure the debug functionality as described in Section 3.6.2 of [7] to meet the extra physical attacker resistance.	Section 3.6.2 of [7].
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 [7]
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.	Section 13.7 of [3], Section 6.5 of [7], Section 3.2 of [8][9]
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 & 5 of [7]
Memory Protection	For IP and data needs protection and prevent dump, it shall use memory verification function	Section 8 of [7]

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

Title	Description	Reference
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 [7]
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.	[10]

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 1.1 [1].

3.1.1 Flaw Reporting Procedures (ALC_FLR.2)

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

NXP has defined a Product Security Incident Response Process (PSIRP), implemented by a dedicated team (PSIRT). This process provides a publicly available interface (https://nxp.com/psirt), and includes 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 S32G2 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 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 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.

3.2 Security by Design and Process Compliance

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* [15].

Conformance rationale:

This product was designed for maximum compliance with ISO/SAE 21434:2021 Road vehicles - cybersecurity engineering [15].

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 securityrelated 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 [15]. 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 **S32G2 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.

S32G2 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 either obtained by JTAG per Section 76.5.3.1 of [3] or reading register SIUL2 MCU ID Register #1 (MIDR1) per Section 16.3.2 of [3].

HSE Firmware version is readable by using HSE Get Attribute Services and `hseAttrFwVersion_t`. (See Section 9.1.3 of [7])

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 and their versions.

Conformance rationale:

A 64-bit unique device identifier (UID) is provisioned. See Section 3.2.3 of [7].

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 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. See Section 9.6 of [7] and Section 7 of [8][9].

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

Conformance rationale:

BootROM has the responsibility to authenticate, decrypt and load HSM 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 table 7 of [6] and see Section 8 of [7] for further information.

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 integrity, authenticity and confidentiality 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 [7].

The SYS-IMG is updatable. See Section 6.5 of [7].

Memory verification services by HSM provides capability of secure update of the application image. See Section 8 of [7].

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 Sections 5.2, 6.5, 9.4 of [7].

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 61 of [3]. Entering FA mode needs both OEM credential (ADKP) and NXP credential, and once enterred, device specific keys used to encrypt FW-IMG and SYS-IMG are irrevisibly destropyed, hence all stored assets and information encrypted by the keys in HSE firmware are not accessible anymore.

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 *Secure Initialization of Platform, Secure Update of Platform 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.

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 has its own exclusive system resources and connects to the host via a dedicated interface, hence it is isolated from the host.

3.3.4 Cryptographic Functionality

3.3.4.1 Cryptographic Operation

The platform provides the application with *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	128, 192, 256	ECB, CBC, CTR, XTS, CFB
MAC generation and verification	AES	RFC4493	128	XCBC-MAC [1], CMAC, GMAC
MAC generation and verification	SHA 1, SHA 2,	RFC2104	Up to 512 [2], or Up to 1152[1]	HMAC
MAC generation and verification	SipHash	[11]	64, 128	CMAC, CBC-MAC, Retail MAC
Hashing	SHA 1	NIST FIPS 180-4	160	-
Hashing	SHA 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	[12]	128	-
Authenticated encryption with associated data (AEAD) and authenticated decryption	AES	ISO/IEC 19772	128, 192, 256	GCM, CCM
Signature generation and verification	RSA	PKCS#1 v1.5	Up to 2048[2], or Up to 4096[1]	-
Signature generation and verification	RSA	PKCS#1 v2.1	Up to 2048[2], or Up to 4096[1]	PSS
Signature generation and verification	ECDSA	ANSI X9.62	Up to 256[2], or Up to 512[1]	-
Signature generation and verification	EdDSA	RFC8032	255	-
Encryption, decryption	RSA	PKCS#1 v1.5	Up to 2048[2], or Up to 4096[1]	-
Encryption, decryption	RSA	PKCS#1 v2.1	Up to 2048[2], or Up to 4096[1]	OAEP padding
KDF	CKDF	NIST SP 800-108 NIST SP 800-56C	See CMAC and HMAC or Hashing	-
KDF	PBKDF2	RFC8018	See HMAC	-
Key Exchange	ECDH	NIST FIPS 800-56A	Up to 256[2], or Up to 512[1]	-

Table 8. Cryptographic Operations*...continued*

Operation	Algorithm	Specification	Key Lengths	Modes
Key Exchange	Classic DH	[13]	Up to 2048[2], or Up to 4096[1]	-

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

Conformance rationale:

Cryptographic operations are provided by HSE and HSE FW. See Section 7 of [7] and Sections 4 and 5 of [8][9].

3.3.4.2 Cryptographic Key Generation

The platform provides the application with 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
ECC	ECC	ANSI X9.62	Up to 256 [1], or Up to 512[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 FW. See Section 7.2 of [7].

3.3.4.3 Cryptographic KeyStore

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

Conformance rationale:

HSE provides key management functions. NVM and RAM key properties and valudes 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 [7].

3.3.4.4 Cryptographic Random Number Generation

The platform provides the application with 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).

- 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 7.5 of [7]. and Section 9.1 of [8][9].

3.3.5 Compliance Functionality

3.3.5.1 Secure External Storage (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-HSE image nor secure memory region* is protected such that the *authenticity, integrity, confidentiality, binding to the platform instance* and *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 [7]).

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 [7].

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.

3.3.5.2 Secure External Storage (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 [7].

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 *Section 7.2.9 of [7]* before the memory is (re)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 [7].

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 [7].

3.3.5.5 Secure Debugging

The platform only provides *JTAG interface* authenticated as specified in *Section 3.6.2 of [7]* with debug functionality.

The platform ensures that all data stored by the application, with the exception of *all data*, is made unavailable.

Conformance rationale:

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

The host debug is either protected or permanently disabled in OEM_PROD and IN_FIELD LC states. See more in Section 3.6.2 of [7] and Chapter 76-79 of [3].

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 [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.

Table 10. SESIP2 Sufficiency*...continued*

Assurance Class	Assurance Family	Covered By	Rationale
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

5 Bibliography

5 . 1 Evaluation Documents

[1] GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.1, GP_FST_070.

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

5 . 2 Developer Documents

[3] S32G2 Reference Manual, Rev 3, NXP Semiconductors, April 2021.

[4] S32G2 Data Sheet, Rev 3, NXP Semiconductors, April 2021.

[5] AN12978, S32G2 Support for Firmware Over The Air Updates, Rev 1, NXP Semiconductors, March 2021.

[6] AN12422, S32G2 Boot Process, Rev. 4, NXP Semiconductors, April 2021.

[7] HSE_H Firmware Reference Manual, HSEFWRM, Rev 1, NXP Semiconductors, Sept 2021.

[8] HSE Service API Reference Manual for S32G2XX, v0.1.0.0, Revision c36150e89, NXP Semiconductors, Oct 2021.

[9] HSE Service API Reference Manual for S32G2XX, v1.1.0.0, Revision c36150e89, NXP Semiconductors, Oct 2021.

[10] AN13023, Selecting and using cryptographic algorithms and protocols, Rev 1.0, NXP Semiconductors, November 2021.

5 . 3 Standards

[11] J. Aumasson, et al, SipHash: A Fast Short-Input PRF, Progress in Cryptography - INDOCRYPT 2012, pp 489-508.

[12] Specification of Secure Hardware Extensions, Release R19-11, AUTOSAR, 2019.

[13] W. Diffie and M Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory. 22 (6): 644–654.

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

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

6 Legal information

6.1 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.

6.2 Disclaimers

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

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

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

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

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.

6.3 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.

Tables

Figures

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

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

Date of release: 2 March 2022