NHS52S04 BLE Microcontroller

SESIP Security Target

Rev. 1.2 — 13 November 2024 Evaluation document

Document information

Information	Content
Keywords	SESIP, PSA, Security Target, NHS52S04
Abstract	Security target for evaluation of the NHS52S04 developed and provided by NXP Semiconductors, according to SESIP Assurance Level 2 (SESIP2) based on SESIP methodology, version 1.2, and PSA Certified Level 2

Revision History

Rev.	Date	Description
1.0	09 Oct 2024	Release Version
1.1	12 Nov 2024	Update MBedTLS version and add precisions to the steps for Field Return of Platform
1.2	13 Nov 2024	Update to rationale for Residual Information Purging.

1 Introduction

This Security Target describes the NHS52S04 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) [7].

1.1 ST Reference

NHS52S04, SESIP Security Target, Revision 1.2, NXP Semiconductors, 13 November 2024.

1.2 SESIP Profile Reference and Conformance Claims

Table 1. SESIP Profile for Secure MCUs and MPUs Conformance Claims

Reference	Value
SP Name	GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs [8]
SP Version	Version 1.0
Assurance Claim	SESIP Assurance Level 2 (SESIP2)
Package Claim	• Base SP • Package Security Services • Package Software Isolation

Table 2. SESIP Profile for PSA Certified Level 2 Conformance Claims

Reference	Value
SP Name	SESIP Profile for PSA Certified Level 2 [9]
SP Version	V1.0 REL 02
Assurance Claim	SESIP Assurance Level 2 (SESIP2)
Optional and Additional SFRs	• Secure Debugging • Secure Encrypted Storage (internal storage) See Section 4.3

1.3 Other Conformance Claims

NHS52S04 is compliant to the requirements from DIRECTIVE 2014/53/EU, Article 3 for radio equipments [19]. In particular, the following requirements are fulfilled by NHS52S04:

- Requirement 3.3 (d): radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;
- Requirement 3.3 (e): radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;
- Requirement 3.3 (f): radio equipment supports certain features ensuring protection from fraud;

1.4 Platform Reference

NHS52S04 has a single configuration, but is also marketed using a commercial name, MCX W23x, where the value of *x* indicates the diversified available memory capacity.

Table 3. Platform Reference

Reference	Value	
Platform Name and Version	See Table 7	
Platform Identification	• NHS52S04	T1.0.0 [1]
Platform Type	Ultra Low Power Health IoT Solution	
Packages	• WLCSP package: < 6.56 mm2 with 37 bumps • QFN package: 5mm x 5mm with 40 pins	
Commercial name	MCX W23x	Commercial name used in product marketing

[1] Silicon version is mapped to TargetVersion ISP property given in given in Table 10

1.4.1 Die Markings

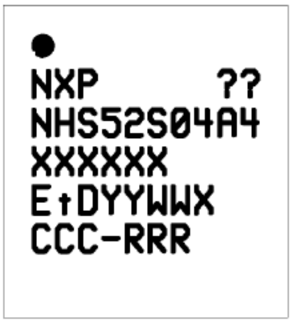

Figure 1. Wafer Laser Etch Markings

Table below details the die laser markings visible for WLCSP product

Table 4. Die markings

Row	Content	Description
1	DOT	Pin 1 marker
2	NXP	Company Name (fixed)
2	??	Wafer ID (variable)
3	NHS52S04A4	Product Type (fixed)
4	XXXXXX	NXP Internal (variable)
5	E	Fab Code
5	tD	Assembly Centre Code, RoHS Code (Dark Green)
5	YYWW	NXP Internal (variable)
5	X	Engineering build (not present in production product)
6	CCC-RRR	NXP Internal (variable)

1.4.2 QFN Package markings

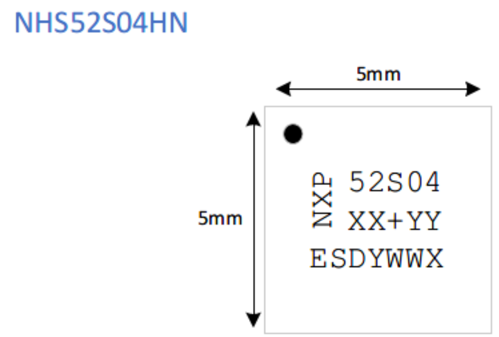

Figure 2. QFN Package Diagram

Table below details the QFN package markings

Table 5. QFN Marking details

Row	Content	Description
1	52S04	Product Identifier
2	XX + YY	NXP Internal (variable)
3	E S D Y WW X	Fab Id Test House ID RoHS Code (Dark Green) Year of Assembly (variable) Week of ASsembly (Variable) Pre-CQS (not present on production product)

1.5 Included Guidance Documents

The following documents are included with the platform:

Table 6. Guidance Documents

Document	Reference
User Guidance	NHS52S04 Getting started guide [11]
Software Development Kit	NHS52S04 SDK [12]
Secure Boot Guidance	AN13988: Getting started with secure boot on NHS52Sx4 [15]
User Manual	UM11461: NHS52S04 for healthcare IoT applications [14]
User Manual	UM11489 Ultra-low power, small footprint Bluetooth Low Energy solution with integrated flash and security for IoT [13]
User Manual	MCUXpresso Secure Provisioning Tool User Guide [16]
API Reference Manual	PSA Attestation API 1.0 [2]
API Reference Manual	PSA Cryptography API 1.1 [3]
API Reference Manual	PSA Storage API 1.0 [4]
API Reference Manual	Mbed TLS API [5]

Table 6. Guidance Documents*...continued*

Document	Reference
TF-M User Manual	Trusted Firmware M [6]

1.6 Platform Overview and Description

The NHS52S04 product family is a low-power, highly secure, single-chip wireless MCU that integrates a high performance Bluetooth Low Energy version 5.3 radio and flexible Power Management Unit facilitating extended battery lifetime for healthcare IoT applications.

The family integrates a state-of-the-art, scalable security architecture including Arm TrustZone-M, a resource domain controller, and dedicated Security functionality including a PUF, Crypto accelerators and a True Random Number Generator with support for Key generation and Secure Key Storage as well as approved Crypto Operations. Flash memory contents can optionally be stored as encrypted data and then decrypted on-the-fly enabling protection of sensitive data and algorithms.

1.6.1 Platform Security Features

NHS52S04 is an Arm Cortex-M33 with TrustZone, Floating Point Unit (FPU) and Memory Protection Unit (MPU) that includes a security subsystem, which together with its Crypto Library and firmware parts provides the following security features:

- Integrated Flash memory with Error Code Correction
- PRINCE module for real-time encryption of data being written to and decryption of encrypted flash data to support asset protection
- CASPER Crypto co-processor, enabling hardware acceleration for Crypto functions used in certain Assymmetric crypto algorithms, such as ECC
- Phycically Unclonable Function (PUF), which can generate, derivem store and reconstruct key sizes from 64 bits to 4096 bits, including Hardware for key extraction
- Hardware AES 128/192/256 accelerator with ECB, CBC and CTR with keys fed directly from PUF or software
- Cryptographic hash function (SHA-2) with dedicated DMA controller
- SHA-1, SHA-256 and HMAC
- Cryptographic True Random Number Generator (TRNG) - including full set of health tests and 512 bit entropy register
- Key storage services
- Secure GPIO
- Code Watchdog
- Universal Unique Identifier (UUID) - a 128-bit IETF RFC4122 compliant non-sequential universally unique identifier
- Protected Flash region (PFR) available to configure secure-boot, debug authentication, read UUID, Store PUF in Key Store and user defined fields for specific data storage
- Secure boot to ensure authenticity, integrity and confidentiality of the device bootloader, firmware, and other software during the boot process and that the intended secure life-cycle state is reached.
- Secure debug requiring Authentication
- Secure firmware update using SB2.1 file format guaranteeing authenticity, integrity and confidentiality.
- ARM Trust-Zone - Secure isolation to partition the platform into multiple functional/security domains with Access Right Management controlled by the Secure AHB Bus controller, Memory and Peripheral Controller (MPC and PPC)
- Secure attestation to provide proof to a remote party on the platform’s genuine identity, its software and firmware versions, as well as its integrity and lifecycle state.

Non Security related features include, but are not limited to :

- 2.4GHz transceiver supporting Bluetooth Low Energy 5.3
- Real Time Clock
- 5 Standard Timer/Counters and a WatchDog Timer
- Systick Timer, Micro-tick Timer, Free running OS Timer
- Flexible Power Management Unit (PMU) for multiple battery types

1.6.2 Platform Type

The platform consists of a micro-processor with internal hardware isolation with Arm TrustZone technology, secure memory, and a secure subsystem.

1.6.3 Platform Physical Scope

The physical scope is the NHS52S04 microcontroller silicon chip as shown in Figure 3.

The hardware components and interfaces are listed in [13].

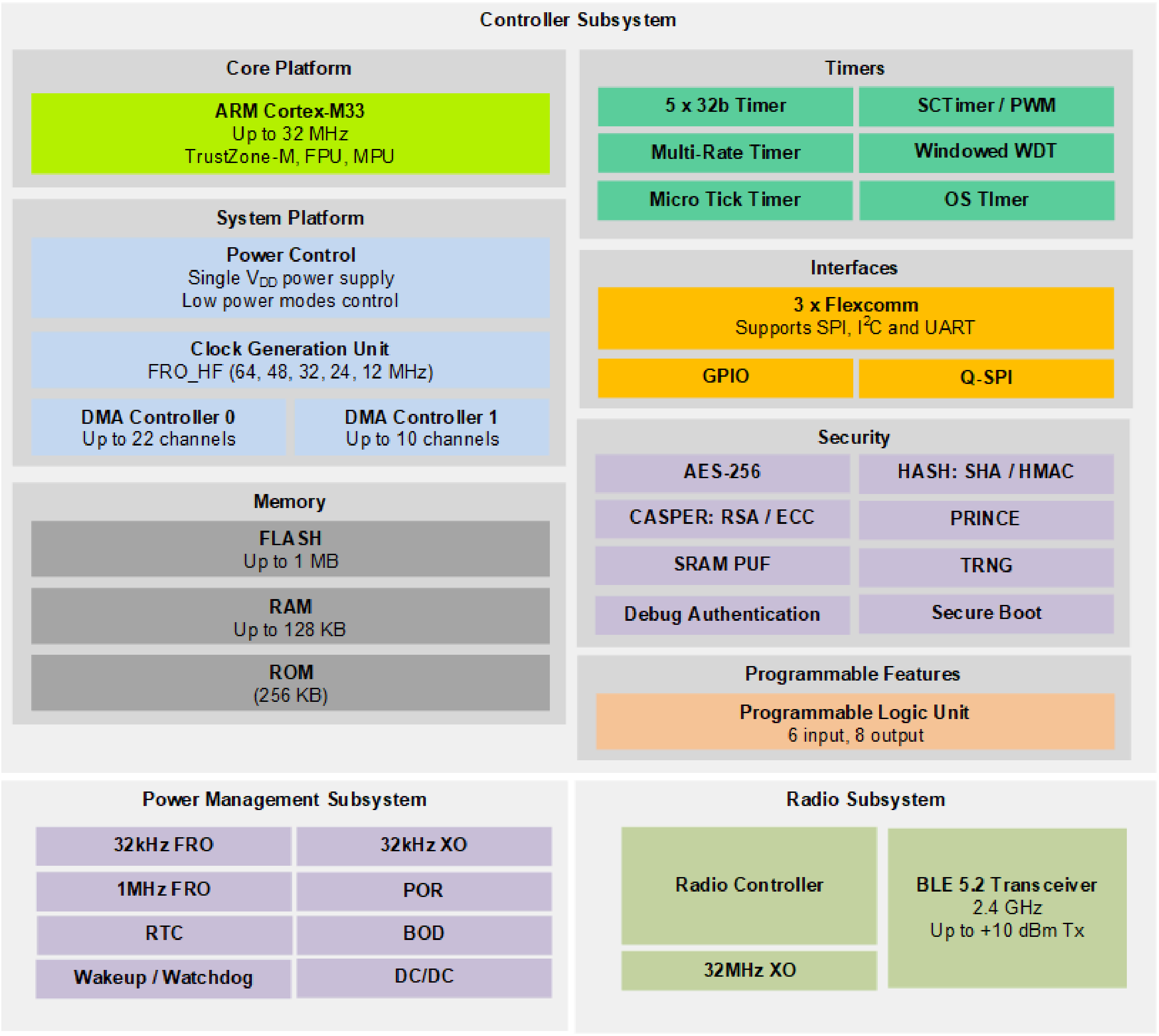

Figure 3. NHS52S04 Block Diagram

1.6.4 Platform Logical Scope

The logical scope includes:

- The IC itself with the ARM Cortex-M33
- The ROM firmware which resides in the platform's ROM and the ROM firmware patch. The ROM firmware includes the bootloader and other pieces of code to enforce security features including life-cyle state, secure boot, secure update, etc.
- The TF-M integration software package for implementing TF-M functionalities.

All the platform deliverables are listed in Table 7 below. Any additional firmware, OS or application software stored on the platform is not in scope of this evaluation.

Table 7. Platform Deliverables

Type	Name	Release	Form of delivery
IC Hardware	NHS52S04	T1.0.0. [1]	Silicon Chip
ROM Firmware	NHS52S04 ROM	3.1.0	Onchip ROM
MbedTLS ROM Integration	NHS52S04 ROM	2.28	Subset of crypto library integrated in Onchip ROM
ROM Patch	NHS52S04 ROM Patch	n/a	Onchip Firmware
TF-M Integration	NHS52S04TF-M Integration	1.6.0	Software Package (part of SDK)

[1] Silicon version is mapped to TargetVersion ISP property given in given in Table 10

For the guidance documents that shall be considered by the users, please refer to Section 1.5

1.6.5 Required Non-Platform Hardware/Software/Firmware

No additional non-platform hardware, software or firmware is required for the correct functioning of the security claims described in this document.

1.6.6 Life Cycle

The life cycle (LC) is managed by the platform, see Section 10.5 of UGM [14] for complete details of Lifcycles and transitions. The defined LC states are as Table 8:

Table 8. Life Cycle States

LC State	Description	Transitions		
		Fields to Write	**Next State**	**Notes**
NXP Provisioned	Final State at NXP facility before customer delivery	N/A	OEM Open	The Change in LC reflects the delivery from NXP facility to OEM facility
		N/A	Bricked	-
OEM Open / OEM Tier 1	Tier 1 software development • ROM opens debug ports, however debug access is disabled during ROM execution • If debug authentication fields (DCFG_CC_SOCU_xxx)are programmed, they are used to determine debug access • SECURE_BOOT_CFG field determines if secure boot flow is enabled or not, as well as other options for TrustZone, and boot seed.	• CMPA_DIGEST • DCFG_CC_SOCU_PIN • DCFG_CC_SOCU_DFLT • Secure World Debug should be restricted or disabled	OEM Tier 2	This state is intended for the case where Tier 1 develops a secure world application and transfers to Tier 2 OEM writing a non-secure world application
		• CMPA_DIGEST • DCFG_CC_SOCU_PIN • DCFG_CC_SOCU_DFLT	OEM Provisioned	This State transition is intended for when Tier 1 writes both secure world and non-secure world application
		N/A	Bricked	-
OEM Tier 2	Tier 2 development - Optional State, to enable module vendors to have SW IP running secure-world leaving non-secure open for customer code • Secure Debug ports closed - may be always closed or open by authentication • Non-Secure Debug ports enabled • Primary image enables TZ-M • CMPA cannot be written • ISP commands limited or disabled completely	N/A	Bricked	-
OEM-Provisioned	In field application State	N/A	Application Active	This change in lifecycle indicates the change of location from when device leaves OEM facility.
Application Active	State as leaving OEM facility towards the end-user	Same as "OEM Provisioned"	OEM Closed - No Return	-

Table 8. Life Cycle States*...continued*

LC State	Description	Transitions		
		Fields to Write	Next State	Notes
OEM Closed - No Return	End state at customer, device will not be use, nor will it be returned	N/A	Bricked	-
Failure Analysis	Returned (CQI): • ROM checks that the key store is emptyand blocks PUF key unwrapping functionality before enabling test/debug ports open. • ROM does not boot images in flash but remains in infinite loop • Part can only be used to run test patterns through SWD or to load and run code in RAM using the SW interface. • ISP command interface is disabled. • CMPA and CFPA cannot be written	N/A	Bricked	-
Bricked	Fail / End of Life state: • Debug ports are disabled • All Assets are removed	N/A	N/A	-

The Boot ROM is responsible for checking the life-cycle state. Based on the life-cycle state, the ROM determines what boot flow is used, including whether the control is passed to the application code or not. The ROM also handles the opening of test and debug ports based on the life-cycle state. If the platform is in any invalid life-cycle state, then the ROM locks the platform.

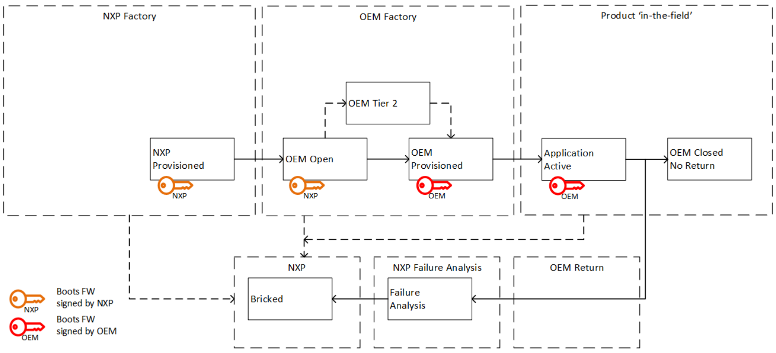

Figure 4. NHS52S04 Life Cycle Transitions

1.6.7 Use Case

[trusted user]

The platform is expected to be used by trusted users only.

[trusted code]

Only trusted code is expected to run the platform. The platform enforces this by secure boot feature. In the field, the platform firmware can be updated. However, the update process must be done in a secure manner which protects the confidentiality and integrity of the firmware.

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) shall fulfill the following objectives:

Table 9. 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, as described in Section 3.2.1.1 of this document.	Section 3.2.1.1
Secure Boot	The operating system or application code are expected to make use of the Secure Boot feature as described in [15] and [14].	[15], [14]
Secure Debug	The integrating environment is expected to configure the debug functionality as described in [14]	[14]
Key Management	Cryptographic keys and certificates outside of the Platform are subject to secure key management procedures.	This document
Trusted Users	Actors in charge of platform management, for instance for signature of firmware update, are trusted.	This document
SW Integration	The operating system or application code are expected to ensure the correct version of the crypto library and SDK drivers are integrated and configured.	This document
Secure Update and Key Revoke	The operating system or application code are expected to update an image with proper remedy solution and version increased and/or revoke key in case of security incidence occurrence of the image and/or the key.	[14]
Lifecycle Management	The operating system or application code are expected to provide lifecycle states and secure mechanism of lifecycle state transition according to the use case, and the operational environment is expected to configure the platform accordingly for lifecycle state transitions. In general, the operating system or application code are expected to configure the platform to OEM-Closed or OEM-Locked state.	[14]

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 [7].

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 platform’s Secure Boot feature is able to verify the authenticity of customer code, i.e., the OEM firmware, during the boot sequence. In addition, the platform also provide Secure Update feature to allows the update of the OEM firmware to a newer version. Once updated, it is not possible to revert back to any older version of the firmware. The update mechanism can also be used to update the TF-M software package provided by the platform since the TF-M package is an integrated part of the OEM firmware. See Section 3.2.2.1 for further information.

3.2 Security Functional Requirements

In the following Security Functional Requirements, the term **platform** covers the **NHS52S04 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.

NHS52S04 fulfils the following security functional requirements:

3.2.1 Identification and Attestation of Platforms and Applications

3.2.1.1 Verification of Platform Identity

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

Conformance rationale:

The identification for different parts of the platform can be done by using `GetProperty` command in ISP (In-System Programming) mode as specified in Chapter 8.5.2 [14].

Table 10. ISP Properties for TOE identification

Property	Tag	Value	Description
CurrentVersion	01	0x4B030100	Current Bootloader version (K3.1.0 in ASCII)
TargetVersion	18	0x54010000	ISP Property *Targetversion* ties the released firmware to specific Silicon Revision (A4). Any changes in the firmare or the Silicon version are reflected in this value. (T.1.0.0 in ASCII).

Table 11. Futher ISP Properties for TOE identification

Property	Tag	Description
AvailablePeripherals	02	Set of supported Peripherals
FlashStartAddress	03	Start address of Program Flash
FlashSizeInBytes	04	Size of Flash
AvailableCommands	07	Set of supported bootloader commands

The TF-M integration and Mbed TLS integration are delivered as software packages in the SDK for the platform. Packages included in the SDK can be identified via the `SW-Content-Register.txt` file that comes with the SDK.

3.2.1.2 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:

The platform stores a 128-bit IETF RFC4122 compliant non-sequential Universally Unique Identifier (UUID). It can be read out by using ISP command `GetProperty` to retrieve `UniqueDeviceId` property.

3.2.1.3 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:

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

NHS52S04 with TF-M Port also supports the PSA attestation API to produce an initial attestation token in IETF EAT format containing measurements of the firmware, which provides an attestation service which reports on the device identity, firmware measurements and run-time state of the device. The attestation can be verified by remote entities. The tokens are signed using attestation keys stored in the internal flash. See more in [1] and [2].

3.2.1.4 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 3.2.1.3.

3.2.1.5 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 *ISP mode for Secure Update (configurable) or a Bricked state*.

Conformance rationale:

Secure boot prevents unauthorized code from being executed on a given product. It achieves this level of security by always leaving the device's ROM in an executing mode when coming out of a reset. This allows the ROM to examine the first user executable image resident in internal flash memory to determine the authenticity of that code. If the code is authentic, then control is transferred to it. This establishes a chain of trusted code from the ROM to the user boot code. This chain can be further extended, through the verification of digital signatures associated with additional code layers.

The platform's ROM boot loader which is always executed after reset provides the secure boot operation. The image to be loaded is signed using the RSASSA-PKCS1-v1_5 scheme of the PKCS #1 standard; see RFC 3447. The platform supports only 2048-bit or 4096-bit RSA keysizes. To verify the authenticity of the RSA keys used for signing, X.509 V3 certificates are used. The image validation process is a two-step process, intially establishing trust in the Public Keys provided by the certificates before using the public key to verify the signature of the image. Please see [15] and [14] for more details.

The bootloader can boot images from three locations in memory. So, it can make up to three boot attempts. The bootloader tries the following boot attempts sequentially:

1. Primary boot
2. Redundant boot, if configured in CMPA
3. Recovery boot, if an external SPI NOR flash is connected to the platform and the option is enabled in CMPA

Finally, if none of these options succeed, the platform enters the ISP mode if the CMPA settings are set to allow it. Otherwise, the part bricks.

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

3.2.2.1 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:

Secure Update is the process used to securely update the OEM firmware to a newer version. The OEM firmware includes the TF-M package provided by the platform and thus this secure update process provides a mechanism to update the platform. Secure Update is required to guarantee the authenticity and confidentiality of the new image. In addition, it also ensures that the new image is up-to-date, preventing the rollback to an older image.

The platform's ROM boot loader provides secure firmware update operation. The Secure Update can be enabled when the platform is booted into ISP (In-System Programming) mode and the ReceiveSBFile command is available. This is not the case for all life-cycle states including Returned / FA mode or Bricked states. In these states, Secure Update is not possible.

3.2.2.2 Field Return of Platform

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

Conformance rationale:

NHS52S04 provides secure Field Return feature as part of its life-cycle management.

The following steps are recommended to transition a part to Returned / FA mode:

1. Erase Flash (Mass Erase except PFR)
2. Erase System SRAM
3. Erase PUF Key Store [1]
4. Set ENABLE_FA_MODE field
5. Trigger Reset

See also chapter 10.6 [14].

3.2.2.3 Decommission of Platform

The platform can be decommissioned.

Conformance rationale:

The OEM-Closed security life-cycle state can be used by customers or NXP to remove a chip permanently from regular use and erase all sensitive data stored on the chip, see Chapter 10.6 of [14]. When a part is decommissioned the user application functionality is disabled. The device can be moved to Failuer Analysis mode which will erase PUF and OEM Keystore data.

3.2.3 Extra Attacker Resistance

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

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

Conformance rationale:

There are multiple isolation features presented in the platform.

ARM defines 2 distinct levels for memory Access, Privileged and Un-Privileged, (also called 'User'). ARM TrustZone introduces 2 further levels of Secure and non-Secure - sometimes referred to as 'Secure World' and 'Normal World'.

These four distinct levels of Access enable secure code Isolation during run-time.

- secure, privileged
- secure, user
- non-secure, privileged
- non-secure, user

Every peripheral is equipped with Peripheral Protection Checker (PPC) that can be programmed to control access to that peripheral, following the ARM TrustZone philosophy. Every memory segment is equipped with Memory Protection Checker (MPC) that can also be programmed in the same way as the PPC. The Secure

[1] The ROM will enforce an erase on PUF Key Store

AHB Controller, operating with the highest level of Access (secure, privileged), programs all PPC and MPC blocks.

Additionally, PSA Level 2 Isolation is supported by TF-M integration which makes use of TrustZone and Memory Protection Unit (MPU) on the platform's ARM v8-M core.

The memory encryption with PRINCE cipher also ensures Secure Isolation between multiple IP vendors. The cipher's Initial Vector (IV) is derived by secure-privileged and a different value is used for every independent memory region, ensuring the isolation between each other.

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

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

Conformance rationale:

The isolation between PSA-RoT and Application Root of Trust Services is included in Section 3.2.3.1.

3.2.4 Cryptographic Functionality

3.2.4.1 Cryptographic Operation

The platform provides the application with *operations in Table 12*, *Table 13* functionality with *algorithms in Table 12*, *Table 13* as specified in *specifications in Table 12*, *Table 13* for keylengths *described in Table 12*, *Table 13* and modes *described in Table 12*, *Table 13* .

Table 12. Cryptographic Operations with Hardware Acceleration

Operation	Algorithm	Specification	Key Lengths (bits)	Modes
Encryption and decryption	AES	NIST FIPS 197	128, 192, 256	ECB, CBC, CTR
Hashing	SHA-1 [1] SHA-2	NIST FIPS 180-4	-	-
MAC generation and verification	HMAC	RFC2104	256	
Key Exchange	ECDH • secp256r1 • secp384r1 • secp512r1 ECDHE • secp256r1 • secp384r1 • secp512r1	NIST FIPS 800-56A	-	-
Signature generation and verification	ECDSA • secp256r1 • secp384r1 • secp512r1	ANSI X9.62	-	-
Signature generation and verification	EdDSA[2]	IETF RFC 8032	256	Curve25519
Key Exchange	MontDH[2]	IETF RFC 7748	256	Curve25519

[1] Not recommended for cryptographic purposes

[2] MBED TLS

Table 13. SDK Cryptographic Operations

Operation	Algorithm	Specification	Key Lengths (bits)	Modes
Signature generation and verification	EdDSA	IETF RFC 8032	256	Curve25519
Key Exchange	MontDH	IETF RFC 7748	256	Curve25519

Conformance rationale:

The specified cryptographic operations are available to users via Mbed TLS integration in ROM, see [5].

Supported algorithms are further enabled in the SDK TF-M port via PSA Crypto API, see [3].

3.2.4.2 Cryptographic Key Generation

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

Table 14. Cryptographic Key Generation

ID	Algorithm	Specification	Key Lengths
ECC	ECC	ANSI X9.62	256
Symmetric	AES	NIST FIPS 197	128, 192 and 256 bits

Conformance rationale:

The ECC key generation function is provided by the SDK Crypto Library. Users can access this function via Mbed TLS integration, see [5] as well as in the TF-M port via PSA Crypto API, see [3].

The AES key generation is provided by the PUF (Physically Unclonable Feature) see 41.2.5 of [14] for the AES Key Management.

3.2.4.3 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 and verification, key derivation, shared secret generation*.

Conformance rationale:

The platform provides a dedicated flash area for customer key storage, which can be provisioned during manufacture, See Chapter 10.2 of [14] The platform provides a mechanism for key wrapping with the PUF (Physically Unclonable Feature), which has an activiation code stored in the Protected Flash Region, along with up to 8 other key codes. See [14] Chapter 7.2.3 for details of Key storage in the protected flash region and Chapter 41.2 for details of the PUF.

3.2.4.4 Cryptographic Random Number Generation

The platform provides the application with a way based on *methods in Table 15* to generate random numbers to as specified in *specifications in Table 15*.

Table 15. Cryptographic Random Number Generation

Methods	Specifications
Physical Noise (TRNG)	NXP Standalone entropy source [10]
DRBG	• NIST SP800-90A CTR-DRBG with AES-128 or AES-256 [18] • NIST SP800-90A HMAC-DRBG [18]

Conformance rationale:

The platform integrates the NXP SA_TRNG_512, which is a Physical entropy source with a full set of health tests and 512-bit entropy register capable of passing AIS 31 statistical tests T0-T8.

Access to random number generators are enabled via the ROM Mbed TLS integration, see [5] as well as in the TF-M port via PSA Crypto API, see [3].

3.2.5 Compliance Functionality

3.2.5.1 Secure Encrypted Storage

The platform ensures that all data stored by the application, except for *data not stored in the configured address area*, is encrypted as specified in *PRINCE [17]* with a platform instance unique key of key length *128 bits*.

Conformance rationale:

This device offers support for real-time encryption and decryption for on-chip flash using the PRINCE encryption algorithm. For more details, see Chapter 41.1.9 of [14].

The keys used for the PRINCE encryption engine are generated by the on-chip SRAM PUF and are therefore unique for each individual die.

3.2.5.2 Secure Debugging

The platform provides *Arm's Serial Wire Debug (SWD) interface* with an authentication protocol as described in chapter 43.6 of *[14]*.

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

Conformance rationale:

The availability of debug functionality depends on the life-cycle state of the platform. This is enforced by life-cyle management of the platform as specified in chapter 10.6 of [14].

3.2.5.3 Residual Information Purging

The platform ensures that *key store area*, with the exception of *none*, is erased using the method specified in *hardware memory erase* before the memory is (re)used by the platform or application again and before an attacker can access it.

Conformance rationale:

As the key store area are in the platform's internal flash, the platform implements residual information purgingwhen transitioning to the Returned / FA Mode. See Section 3.2.2.2. This requires the following process to be followed:

1. Erase flash (mass erase, except PFR)
2. Erase System SRAM

3. Erase PUF Key Store [2]
4. Set ENABLE_FA_MODE field
5. Trigger reset

3.2.5.4 Reliable Index

The platform implements a strictly increasing function.

Conformance rationale:

The customer field programmable area (CFPA) page contains three monotonic counters, which support the anti-rollback mechanism claimed in Section 3.2.2.1. Refer to Chapter 7 of [14] for details of the Secure Boot ROM and the Customer Field Programmable Area, where the monotonic Counters are implemented. .

[2] enforced by the ROM

4 Mapping and Sufficiency Rationales

4.1 SESIP2 Sufficiency

Table 16. 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 ST Reference, the TOE reference in Section 1.4, 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	Security Requirements and Implementation	All SFRs in this ST are taken from [7]. SFR "Identification of Platform Type" is included. SFR "Secure Update of Platform" is mentioned but refers to ALC_FLR.2.
	ASE_TSS.1 TOE Summary Specification	Security Requirements and Implementation	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in the SFR.
ADV: Development	ADV_FSP.4 Complete functional specifications	Section 1.5	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Section 1.5	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Section 1.5	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 Conformance Mapping for SESIP Profile for Secure MCUs and MPUs

This section provides rationales of conformance claimed in Section 1.2

Table 17. SESIP Profile for Secure MCUs and MPUs Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.2.1.1

Table 17. SESIP Profile for Secure MCUs and MPUs Sufficiency*...continued*

Package Claimed	Security Functional Requirements	Covered By
	Secure Initialization of Platform	Section 3.2.1.5
	Secure Updated of Platform	Section 3.2.2.1
	Residual Information Purging	Section 3.2.5.3
	Secure Debugging	Section 3.2.5.2
Security Services	Cryptographic Operation	Section 3.2.4.1
	Cryptographic Key Generation	Section 3.2.4.2
	Cryptographic KeyStore	Section 3.2.4.3
	Cryptographic Random Number Generation	Section 3.2.4.4
Software Isolation	Software Attacker Resistance: Isolation of Platform	Section 3.2.3.1, Section 3.2.3.2
Additional Security Functional Requirements (Optional)	Verification of Platform Instance Identity Attestation of Platform Genuineness Attestation of Platform State Decommission of Platform Field Return of Platform Secure Encrypted Storage Reliable Index	Section 3.2.1.2 Section 3.2.1.3 Section 3.2.1.4 Section 3.2.2.3 Section 3.2.2.2 Section 3.2.5.1 Section 3.2.5.4

4.3 Conformance Mapping for SESIP Profile for PSA Certified Level 2

This section provides rationales of conformance claimed in Section 1.2

Table 18. SESIP Profile for PSA Certified Level 2 Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.2.1.1
	Verification of Platform Instance Identity	Section 3.2.1.2
	Attestation of Platform Genuineness	Section 3.2.1.3
	Secure Initialization of Platform	Section 3.2.1.5
	Attestation of Platform State	Section 3.2.1.4
	Secure Updated of Platform	Section 3.2.2.1
	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Section 3.2.3.1
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	Section 3.2.3.2
	Cryptographic Operation	Section 3.2.4.1
	Cryptographic Key Generation	Section 3.2.4.2
	Cryptographic KeyStore	Section 3.2.4.3
	Cryptographic Random Number Generation	Section 3.2.4.4
Optional SFR	Secure Debugging	Section 3.2.5.2
	Secure Encrypted Storage (internal storage)	Section 3.2.5.1

4.4 Conformance Rationales for DIRECTIVE 2014/53/EU (RED)

This section provides conformance rational for RED conformance claim described in Section 1.3.

Table 19. Conformance Rationales for RED

RED Requirement ID	Description	RED Article d: network assets e: privacy assets f: financial assets	Fulfilled By
ACM-1	Applicability of access control mechanisms	d/e/f	Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4 AVA_VAN
ACM-2	Appropriate access control mechanisms	d/e/f	Same as above
ACM-3	Default access control for children in toys	e	Same as above
ACM-4	Default access control to children's privacy assets for toys and childcare equipment	e	Same as above
ACM-5	Parental/Guardian access controls for children in toys	e	Same as above
ACM-6	Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys	e	Same as above
AUM-1	Applicability of authentication mechanisms	d/e/f	Same as above
AUM-2	Appropriate authentication mechanisms	d/e/f	Same as above
AUM-3	Authenticator validation	d/e/f	Same as above
AUM-4	Changing authenticators	d/e/f	Same as above
AUM-5	Password strength	d/e/f	Same as above
AUM-6	Brute force protection	d/e/f	Same as above
SUM-1	Applicability of update mechanisms	d/e/f	Section 3.2.2.1 Section 3.1.1
SUM-2	Secure updates	d/e/f	Same as above
SUM-3	Automated updates	d/e/f	Same as above
SSM-1	Applicability of secure storage mechanisms	d/e/f	Section 3.2.5.1
SSM-2	Appropriate integrity protection for secure storage mechanisms	d/e/f	Same as above
SSM-3	Appropriate confidentiality protection for secure storage mechanisms	d/e/f	Same as above

Table 19. Conformance Rationales for RED*...continued*

RED Requirement ID	Description	RED Article d: network assets e: privacy assets f: financial assets	Fulfilled By
SCM-1	Applicability of secure communication mechanisms	d/e/f	Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4
SCM-2	Appropriate integrity and authenticity protection for secure communication mechanisms	d/e/f	Same as above
SCM-3	Appropriate confidentiality protection for secure communication mechanisms	d/e/f	Same as above
SCM-4	Appropriate replay protection for secure communication mechanisms	d/e/f	Same as above
LGM-1	Applicability of logging mechanisms	e/f	Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4 Section 3.2.5.1
LGM-2	Logging mechanisms – Persistent storage	e/f	Same as above
LGM-3	Logging mechanisms – Minimum number of Events	e/f	Same as above
LGM-4	Logging mechanisms – Time related information	e/f	Same as above
DLM-1	Applicability of deletion mechanisms	e	Section 3.2.2.2 Section 3.2.2.3 Section 3.2.5.3
RLM-1	Applicability of resilience mechanisms	d	Section 3.2.1.5 Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4
NMM-1	Applicability of and appropriate network monitoring mechanisms	d	Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4
TCM-1	Applicability of and appropriate traffic control mechanisms	d	Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4
UNM-1	Applicability of user notification mechanisms	e	Not applicable

Table 19. Conformance Rationales for RED*...continued*

RED Requirement ID	Description	RED Article d: network assets e: privacy assets f: financial assets	Fulfilled By
UNM-2	Content of user notification	e	Not applicable
CCK-1	Appropriate Confidential cryptographic keys (CCKs)	d/e/f	Section 3.2.1.5 Section 3.2.2.1 Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4 Section 3.2.5.1 Section 3.2.5.2 Section 3.2.1.3 Section 3.2.1.4
CCK-2	Confidential cryptographic key generation mechanisms	d/e/f	Same as above
CCK-3	Preventing static default values for preinstalled CCKs	d/e/f	Same as above
GEC-1	Up-to-date software and hardware with no publicly known exploitable vulnerabilities	d/e/f	AVA_VAN AGD_PRE and AGD_OPE
GEC-2	Limit exposure of services via related network interfaces	d/e/f	Same as above
GEC-3	Configuration of optional services and the related exposed network interfaces	d/e/f	Same as above
GEC-4	Documentation of exposed network interfaces and exposed services via network interfaces	d/e/f	Same as above
GEC-5	No unnecessary external interfaces	d/e/f	Same as above
GEC-6	Input validation	d/e/f	Same as above
GEC-7	Documentation of external sensing capabilities	e	Same as above
GEC-8	Equipment Integrity	f	Same as above
CRY-1	Best practice Cryptography	d/e/f	Section 3.2.1.5 Section 3.2.2.1 Section 3.2.4.1 Section 3.2.4.2 Section 3.2.4.3 Section 3.2.4.4 Section 3.2.5.1 Section 3.2.5.2

5 Bibliography

5.1 Evaluation Documents

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

[2] PSA Attestation API 1.0, ARM Limited, IHI 0085, Issue Number 0, Jun 2019.

[3] PSA Cryptography API 1.1, ARM Limited, IHI 0086, Issue Number 0, Feb 2022

[4] PSA Storage API 1.0, ARM Limited, IHI 0087, Issue Number 0, Jun 2019.

[5] Mbed TLS API, ARM Limited, https://mbed-tls.readthedocs.io/.

[6] Trusted Firmware M, ARM Limited, https://tf-m-user-guide.trustedfirmware.org/releases/1.5.0.html, Release 1.5.0.

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

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

[9] SESIP Profile for PSA Certified Level 2, V1.0 REL 02, PSA JSA, 24th November 2022.

5.2 Developer Documents

[10] Design of the Entropy Source in the NXP RNG4 Random Number Generator, v1.24,NXP Semiconductors, 16 October 2023.

[11] NHS52S04 Getting started guide, NXP Semiconductors, MCUXpresso IDE, Rev 0.9 12 April 2024

[12] NHS52S04 SDK, NXP Semiconductors, Rev 2.1 12 April 2024

[13] UM11489 Ultra-low power, small footprint Bluetooth Low Energy solution with integrated flash and security for IoT, NXP Semiconductors, Rev. 1.04 — 19 June 2024

[14] UM11461: NHS52S04 for healthcare IoT applications, NXP Semiconductors, v1.06, 29 Aug 2024

[15] AN13988: Getting started with secure boot on NHS52Sx4 NXP Semiconductors, Rev. 1.0 24 September 2024

[16] MCUXpresso Secure Provisioning Tool User Guide , NXP Secure Provisioning Tool

5.3 Standards

[17] J. Borghoff, et al, PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications, Cryptology ePrint Archive, Report 2012/529.

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

[19] DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014L0053-20180911.

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: 13 November 2024