Technical note

STM32N65x Security Target for SESIP level 3 certification

Document information

This Security Target document is based on the GlobalPlatform® Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 (July 2023), GP_FST_070.

1 Introduction

This Security Target document describes the STM32N6 platform and the exact security properties of the platform that are evaluated against the GlobalPlatform® Security Evaluation Standard for IoT Platforms [SESIP].
The protection profile reference and conformance claims for this Security Target are described below.

Table 1. Protection Profile Reference and Conformance Claims

Reference	Value
Protection profile name	SESIP protection profile for secure MCUs and MPUs [SP1]
Protection profile version	1.0
Package claim	Base SP, Security Services, Software Isolation, Hardware Protections
Assurance claim	Refer to Section 3.1

Table 2. SESIP profile for PSA-certified RoT component level 3 conformance claims

Reference	Value
SP name	SESIP Profile for PSA Certified RoT Component Level 3 [SP2]
SP version	1.0
Optional and additional SFRs	Base profile
Assurance claim	Refer to Section 3.1

1.1 Security Target reference

This document: Technical note *STM32N65x Security Target for SESIP level 3 certification* (TN1562), revision 2, STMicroelectronics.

1.2 Platform reference

Table 3. Platform reference

Reference	Value
Platform name	STM32N65x Arm®-based 32-bit MCU
Platform version	ChipVersion = 0x486, CutVersion = 2.0, mask ID = 1, BootromVersion = 5.1
Platform identification	STM32N655, STM32N657(1)
Platform type	General-purpose microprocessor device for IoT, industrial, or consumer applications.

1. *The difference between STM32N655 and STM32N657 is that the NPU (neural processing unit) is available on STM32N657, whereas it is not available on STM32N655. However, this makes no difference to the security features on the device and does not impact any of the security software. STM32N645 and STM32N647 have cryptographic accelerators disabled and are therefore not intended for certification.*

1.3 Included guidance documents

The following documents are included with the platform:

Table 4. Guidance documents

Category	Name	Reference
User Manual	STM32N65x security guidance for SESIP level 3 certification (UM3451)	[SG]
Product reference manual	STM32N6xx Arm®-based 32-bit MCUs (RM0486)	[RM]
Errata sheet	STM32N6xxxx device errata (ES0620)	[ES]

1.4 Platform functional overview and description

1.4.1 Platform type

STM32N65x is a general-purpose microcontroller (MCU), consisting of an Arm® Cortex®-M55 microprocessor with an immutable ROM firmware and security hardware features such as TrustZone®, OTP fuse memory, crypto accelerators, and true RNG. It contains a high-performance neural processing unit for supporting advanced edge AI applications.

Note: Arm and TrustZone are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

1.4.2 Platform physical scope

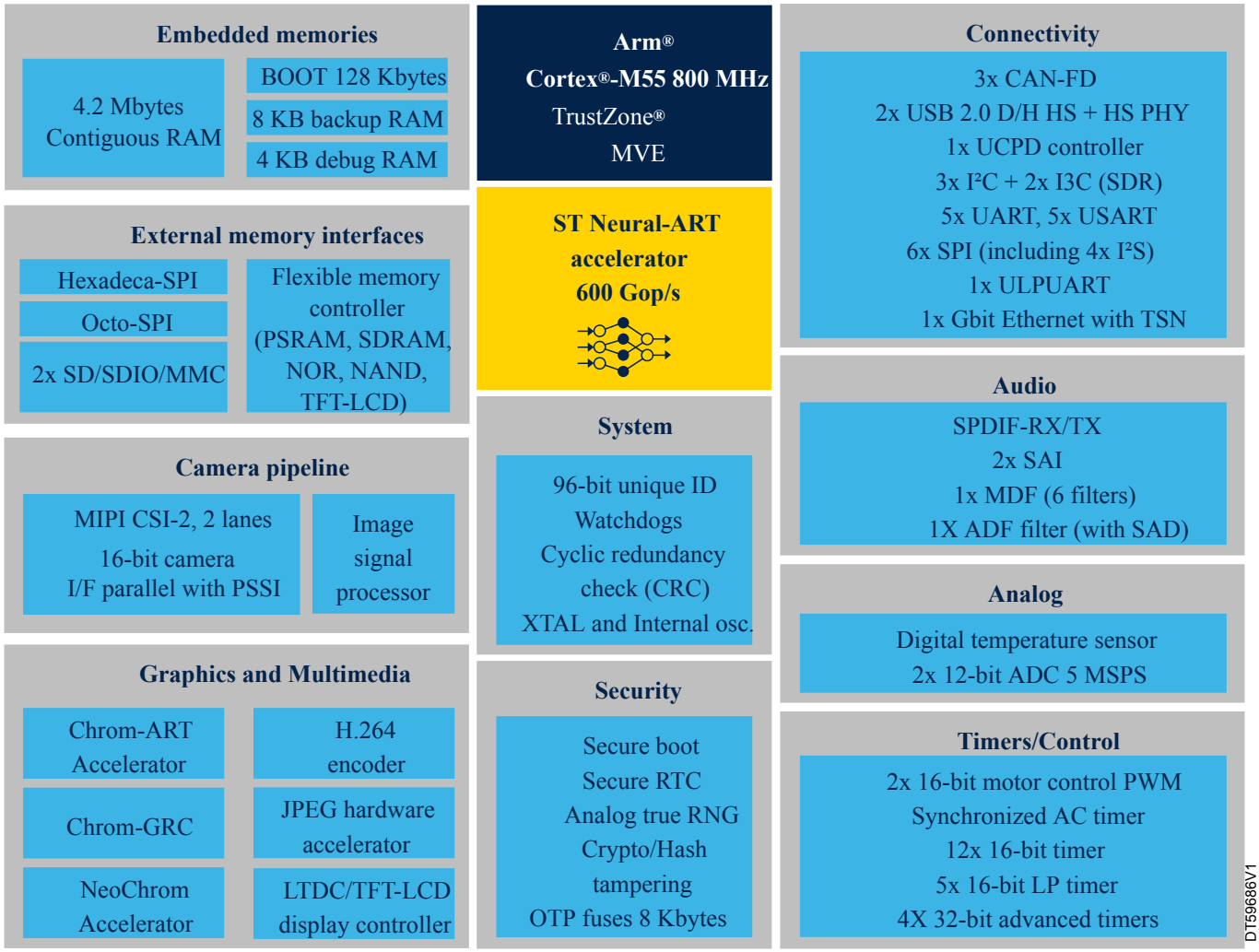
The STM32N65x microcontroller is designed with security features including:

- Resource isolation using privilege mode and Armv8-M mainline security extension of the Cortex®-M55, extended to securable I/Os, DMA channels, memories, and peripherals.
- Firewalls that are configurable by the secure firmware to restrict internal memory regions to particular bus controllers.
- Boot ROM, supporting the download of boot image through USART, USB, serial NOR/NAND flash (via Octo-SPI), parallel NAND flash (via FMC), SD card, or eMMC (via SDMMC).
- Nonvolatile storage (in BSEC), featuring:
  - ECC-protected OTP words, one-time programmable.
  - Redundancy-protected OTP words, bit-per-bit programmable.
  - Embedded life cycle management (such as sticky lock, permanent lock, tamper mode).
- Secure storage, featuring:
  - Battery-powered volatile secure storage, automatically erased in case of tampering (8-Kbyte RAM, 128-byte registers).
  - Write-only key registers in the AES engines.
  - Device 96-bit unique ID, readable via JTAG.
  - Provisioning of AES-wrapped keys in nonvolatile storage (for example external flash memory), encrypted with unreadable device-unique keys derived from nonvolatile hardware unique key (DHUK). These provisioned AES keys are never readable in the clear, are only usable on this device, and are only usable in the target AES accelerator (SAES or CRYP1).
- Set of hardware crypto blocks with symmetric crypto functions (SAES and CRYP), asymmetric crypto accelerator (PKA), and hash function (HASH).
- True random number generator (RNG), NIST SP800-90B certified.
- On-the-fly encryption/decryption of accesses to external flash memories.
- Secure life cycle management (secret provisioning, return material for analysis using customer-defined 128-bit key, default debug deactivation).
- Temporal isolation: boot levels are isolated by the HDPL (hide protect level) monotonic counter.
- Secure software monitoring using an independent watchdog.

- Active tampering and protection against temperature, voltage, and frequency attacks.
  - Up to 16 tamper pins for eight active output tamper pins.
  - The battery-backed volatile secrets are erased immediately upon confirmed tamper detection.

An overview of the STM32N65x microcontroller is shown in the block diagram below.

Figure 1. STM32N65x block diagram



The hardware components and interfaces that constitute the TOE are defined in Table 5. They are described in the reference manual [RM].

Table 5. Hardware components and interfaces of the TOE

Component/Interface	Description	Identification
CPU	Cortex®-M55 subsystem (includes memory protection unit)	Hardware ID
Communication ports	None (outside the platform)	
Memories	SYSRAM, RETRAM, TCM	
Infrastructure	RCC, PWR, BSEC, RIFSC, RISAF, IWDG, TAMP, SYSCFG, FMC, GPIO	
Cryptography	SAES, PKA, CRYP1, HASH, RNG	

1.4.3 Platform logical scope

The software components and interfaces that constitute the TOE are shown in Figure 2 and listed in Table 6. Any additional firmware, OS, or application software stored on the platform is not in the scope of this evaluation. They might be referenced using the term *application* in Section 3.

Figure 2. Platform logical architecture and certification scope

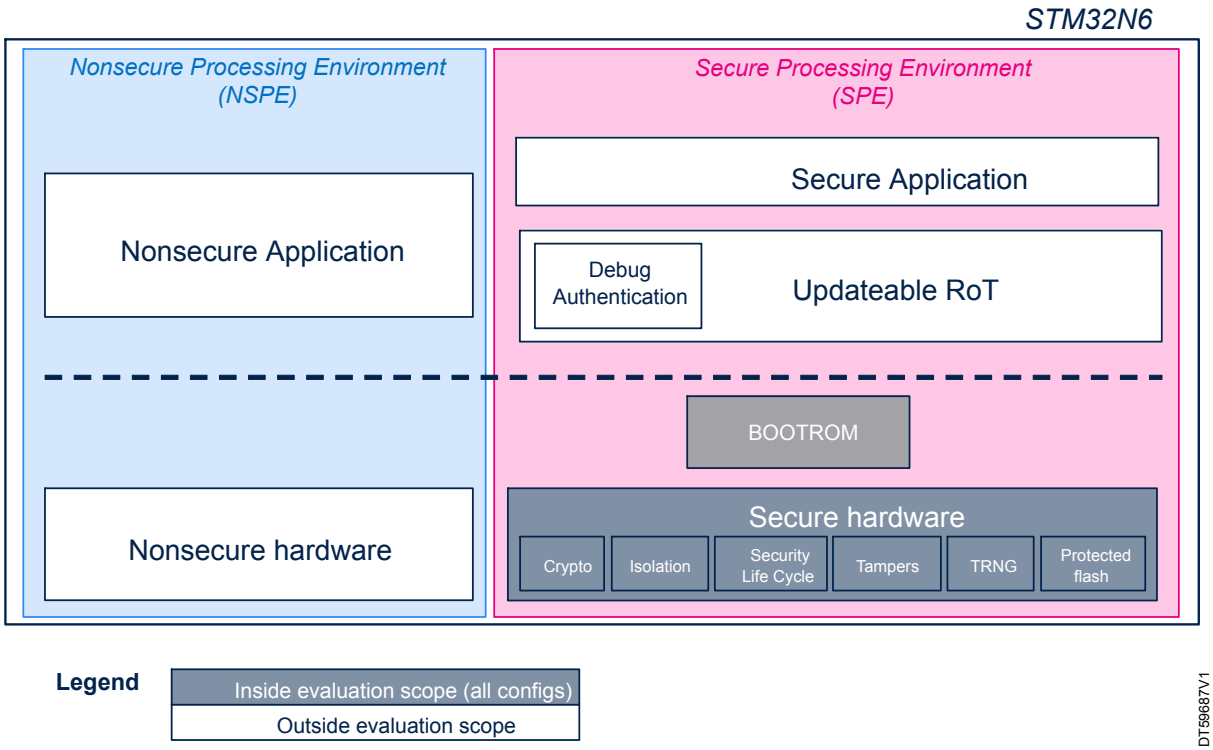


Table 6. Software components and interfaces of the TOE

Component/Interface	Description	Identification/Version
Boot ROM (secure)	Embedded ROM code, reserved to TrustZone® secure mode	0x00000501 (version 5.1)
APIs	*Not supported*	*Not applicable*

The boot ROM version is in the ROM code, readable in `0x1800 100C` for secure word reads, or `0x0800 100C` for nonsecure reads.

1.4.4 Platform security features and usage

The core security features of the platform, implemented as embedded ROM code running in the secure environment of the Cortex®-M55 processor, are:

- Secure initialization, to control the initialization sequence of the platform. At the end of the initialization, the platform has a secure trusted CPU that shall implement the necessary security measures to have a final secure IoT product.
- Residual information purging for life-cycle handling.

Optional packages in [SP1] and [SP2] are selected to accommodate the context of use of the platform:

- Cryptographic operations, based on hardware cryptographic accelerators.
- Hardware protection to handle hostile environments.
- Isolation mechanisms controlling access between certified and noncertified parts of the software building the product.

Regarding security features, note the following:

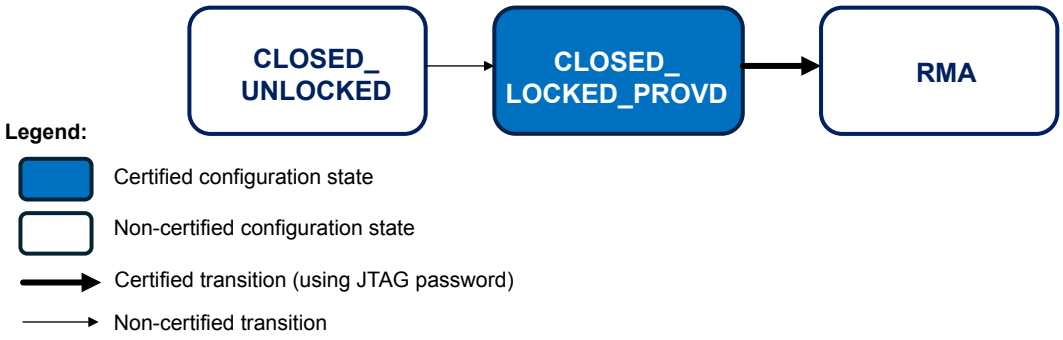
- Secure debugging of the platform is implemented but not accessible to the users. Debugging of the non-TOE application can be activated using an authenticated boot image in a certified configuration (no debug by default).
- Secure update of the platform is inapplicable since the platform does not support the patching of the embedded ROM.

The guidance documentation for the platform usage is listed in Table 4 in Section 1.3.

Life cycle

The product life cycle shown in Figure 3 is used in the SFRs when references to a life cycle are required. The product in-the-field must imperatively be configured in *Closed_Locked_Provd*, in accordance with [SG] Section 3.2.3.

Figure 3. Reference product life cycle



STMicroelectronics delivers *Closed_Unlocked* STM32N65x devices without RoT keys or RMA password provisioned. The provisioning of those is described in the [SG] Section 3.2.2.

The integrity and confidentiality of the platform during the life of the STM32N65x devices are ensured because the ROM part of the TOE and the TOE secrets are hidden from the integrator code or debugger.

The transition to the RMA state is initiated via the JTAG interface by the integrator using their 128-bit password. After X integrator-defined consecutive wrong password attempts (X<5), the RMA sequence always fails.

The integrator must store its security-sensitive information (secret AES keys, and private ECC or RSA keys) in OTP words 256 to 367 so that no secrets leak when the device goes to the RMA state.

Use case

The environmental conditions under which the TOE in certified configuration can be securely used are defined below:

- [**Any user**] the product may be physically accessed by an unknown or untrusted user, in an environment where access to the product cannot be sufficiently controlled or even in a more hostile environment.
- [**Any code**] it cannot be excluded that the product will execute code that is unknown to the product developer.

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.

- The operating system or application code is expected to verify the correct version of all platform components that it depends on, as described in Section 1.2.
- The operating system or application code is expected to use the secure boot feature described in Section 3.3.2.

Since the Security Target declares the "Hardware Protections" Package (Section 3.6), then as mandated in [SP1], the following objective related to the configuration of debug must be listed. However, note that, as mentioned in Section 1.4.4 and Section 3.3.5, the debug of the TOE is not available to the user, so in practice, the following objective is redundant.

The integrating environment is expected to configure the debug functionality as described in Section 3.3.5 to meet the additional physical resistance of the attacker.

2.2 Inherited Objectives for the Operational Environment

The platform does not include parts previously evaluated under any SESIP certification scheme.

3 Security requirements and implementation

3.1 Security assurance requirements

The claimed assurance requirements package is SESIP Assurance Level 3 (SESIP3), as defined in Chapter 4 of the GlobalPlatform® Technology Security Evaluation Standard for IoT Platforms [SESIP].

3.2 Flaw reporting procedure (ALC_FLR.2)

The "Secure Update of Platform" SFR is inapplicable since the platform does not support the patching of the immutable ROM firmware. Outside the platform, the integrator can implement their secure update mechanism in their code, leveraging the boot image revocation method (refer to [SG] Section 4.2.1 for details).

Following the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to generate any needed update and distribute it, the developer has defined the procedure described in https://www.st.com/content/st_com/en/security/report-vulnerabilities.html.

3.3 Base PP Security Functional Requirements

The platform fulfills the following Security Functional Requirements:

3.3.1 Verification of Platform Identity

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

Conformance rationale:

The platform referenced in Section 1.2 provides the identifiers listed in Table 7.

Table 7. Platform identifiers

Field	Address	Value	Interpretation
Device identifier (ChipVersion)	0x18001000	0x0000 8604	STM32N6 (0x486)
Cut identifier (CutVersion)	0x18001004	0x0000 0200	Cut2.0
Mask identifier (MaskVersion)	0x18001008	0x0000 0001	Mask 1
Boot ROM identifier (BootromVersion)	0x1800100C	0x0000 0501	5.1
Device part number	0x56009024	0x0000 2000 or 0x0000 6000	STM32N657 or STM32N655

Note: The above registers are accessible from Secure World software running on the CPU, or via the DAP when secure debug is enabled (for example, on a Closed_unlocked part).

An STM32N65x with the above settings is also referred to as revision ID *Rev B*.

3.3.2 Secure Initialization of Platform

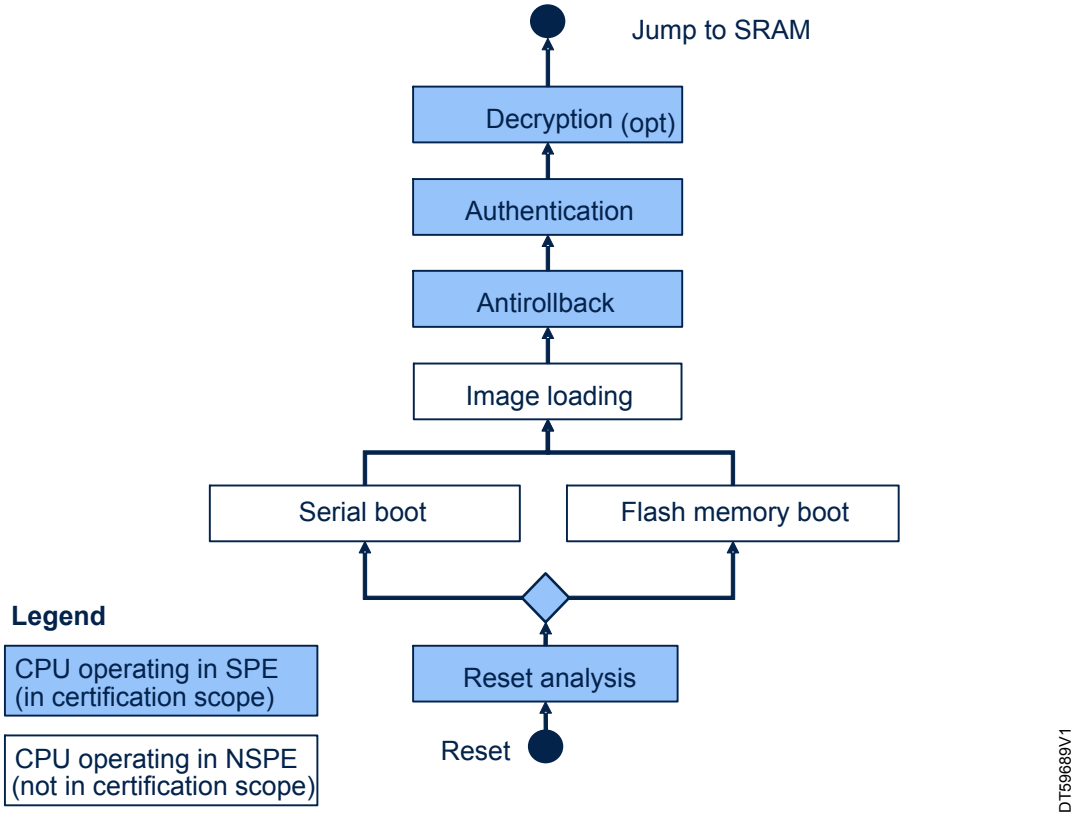
The platform ensures its authenticity and integrity during the platform initialization. If the authenticity or integrity of the platform cannot be ensured, the platform goes into a locked state.

Conformance rationale:

Following any device reset, the platform executes its embedded secure ROM code, ensuring the second stage of the microprocessor trusted boot chain.

ROM code uses immutable fuses provisioned by OEM to verify the authenticity and integrity of FSBL before executing it from the embedded SRAM. The FSBL's SHA-256 digest is always signed using an active 256-bit ECDSA private key, based on NIST prime256v1 or brainpoolP256t1 curves. The platform can choose one among eight ECDSA public keys when verifying the bootloader code signature. The selected key is provided text-clear in the boot image, with its SHA-256 digest protected in the platform on-chip fuses.

Figure 4. **Boot ROM overview**



The serial and flash memory boot steps, and the image loading processes, are performed by ROM code running in the nonsecure domain and are not considered part of the TOE. The antirollback, authentication, and decryption are performed by ROM code running in the secure domain and are considered part of the TOE.

Anytime during the platform ROM execution, any fuse perturbation prevents boot chain execution, forcing an application reset. This way, when the platform's authenticity or integrity cannot be ensured, it leads to a locked state where the application secrets stored in on-chip fuses are locked from any code, and debugger and test modes are disabled for any user until an application reset is done. Refer to Section 4.3 of BSEC peripheral in the reference manual [RM].

3.3.3 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 are maintained.~~

Non-conformance rationale:

The absence of this functionality is justified in Section 3.2: Flaw reporting procedure (ALC_FLR.2).

3.3.4 Residual Information Purging

The platform ensures that all the SRAM used by the platform is erased using the method specified in this section before the memory is used by the platform or application again and before an attacker can access it.

Conformance rationale:

- Following a reset, the platform erases the contents of SRAM used by the ROM.
- After usage the platform erases all the SRAM area and registers that contain secrets, using random values.
- Before jumping to the authenticated application, the platform clears all its allocated embedded SRAM by writing zeroes on each allocated SRAM address. The platform also sticky-reload-locks its secrets stored in BSEC.

3.3.5 Secure debugging

~~The platform only provides *<list of endpoints>* authenticated as specified in *<specification>* with debug functionality.~~

~~The platform ensures that all data stored by the application, with the exception of *<list of exceptions>*, is made unavailable.~~

Nonconformance rationale:

This SFR is removed because the feature is not available to the users. It is implemented but not accessible.

For the other debug features of the product, the platform is certified with all debug features disabled out of cold boot reset (refer to Section 1.4.4). This debug protection can be frozen anytime until the next reset by writing zero to the DBGCR register in the BSEC peripheral. The platform systematically does this when *debug_lock* fuses are burnt in OTP word 18 (refer to *Secure debug* in [SG] Section 4.2.1).

If the user activates any debug capability on the device following a cold boot defined in Section 3.3.2, the debugging of platform ROM code remains not accessible.

3.4 Package “Security Services” Security Functional Requirements

The platform fulfills the following Security Functional Requirements:

3.4.1 Cryptographic operation

The platform provides the application with side channel-resistant cryptographic operations such as encryption, decryption, and authentication, with a list of algorithms specified in Table 8.

Table 8. Platform cryptographic operations

Operations	Algorithm	Specification	Key lengths	Modes
Encryption, decryption	AES	FIPS PUB 197 NIST SP800-38A	128, 256 bits	ECB, CBC, CTR
Authenticated encryption or decryption		NIST SP800-38C NIST SP800-38D		GCM, CCM
Cipher-based message authentication code		NIST SP800-38D		GMAC
Protected modular exponentiation (signature, decryption, key agreement...)	RSA	IETF RFC 8017 NIST SP800-56B FIPS PUB 186-4	Up to 4096 bits	RSA 1024, 2048, 3072, 4096
Signature	ECDSA	ANSI X9.62 IETF RFC 7027 FIPS PUB 186-4 SEC 1, SEC 2	Up to 640 bits	Nist: P256, P384, P521 Brainpool: bp256r1, bp384r1, bp512r1 SEC 2(1): secp256k1, secp256r1, secp384r1, secp521r1
ECC scalar multiplication (public key generation, key agreement, shared secret generation...)	ECDH ECIES	ANSI X9.42 ANSI X9.63 FIPS PUB 186-4 SEC 1, SEC 2(1)		

1. *Standards for efficient cryptography: SEC1, SEC2 (1)*

Conformance rationale:

For more details refer to the reference manual [RM]:

- Section 48 secure AES coprocessor (SAES)
- Section 52 public key accelerator (PKA)

The STM32N65x device also provides useful cryptographic operations without special side-channel attack resistance, as listed in Table 9. They must not be used to manipulate SESIP assurance level 3 sensitive information.

For more details refer to the reference manual [RM]:

- Section 50 Hash processor (HASH)

Table 9. Cryptographic operations available outside the platform

Operations	Algorithm	Specification	Key lengths	Modes
Cryptographic hash	SHA-2	FIPS PUB 180-4	N/A	SHA-256, SHA-384, SHA-512
	SHA-3	FIPS PUB 202	N/A	SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256

3.4.2 Cryptographic KeyStore

The platform provides the application with a way to store secret keys such that not even the application can compromise the authenticity, integrity, or confidentiality of this data. This data can be used for the cryptographic operations listed in Table 10.

Table 10. Platform cryptographic operations available to KeyStore

Operations	Algorithm	Specification	Key lengths	Modes
Encryption, decryption	AES(1)	FIPS PUB 197 NIST SP800-38A	128, 256 bits	ECB, CBC, CTR
Authenticated encryption or decryption		NIST SP800-38C NIST SP800-38D		GCM, CCM
Cipher-based message authentication code		NIST SP800-38D		GMAC

1. *AES algorithm with key sizes of 128 and 256 bits running in SAES peripheral (with side-channel resistance).*

Conformance rationale:

The platform provides hardware mechanisms to protect the confidentiality of AES 128 or 256-bit keys. When the user encrypts those keys in the SAES peripheral using the DHUK, they can only be decrypted in this specific device, and the decrypted keys are only available in the SAES write-only key registers. Note that if the application tries to overwrite part of the key, the whole key is erased.

The DHUK is never disclosed to any application code or debugger and is only usable in the side-channel protected SAES peripheral. Refer to *SAES operation with wrapped keys* in [RM] Section 48 Secure AES coprocessor (SAES) for details.

3.4.3 Cryptographic Random Number Generation

The platform provides the application with a way based on a live entropy source (analog) to generate random numbers as specified in NIST [SP 800-90B].

Conformance rationale:

The platform includes an RNG peripheral that can be certified NIST SP800-90B. The application can use this peripheral to generate true random numbers. Refer to [RM] Section 47 for details.

3.5 Package “Software Isolation” Security Functional Requirements

The platform fulfills the following Security Functional Requirements:

3.5.1 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 the other Security Functional Requirements.

Conformance rationale:

As shown in Figure 2, no non-TOE code can alter any hardware, code, assets, platform secrets, or binary used to implement the SFRs claimed in this document.

The platform ROM code uses hardware runtime protections to enforce isolation between the platform and the application. More specifically:

- The platform ROM code and some nonvolatile assets in the BSEC peripheral are hidden from any application code following a cold boot. Refer to [RM] Section 4 for details.
- The platform secure ROM code manages the RIF configuration to protect itself against nonsecure ROM code used during platform secure initialization (refer to Figure 4).
- The platform secure ROM code manages RNG peripheral configuration.

The ROM code jumps to the authenticated image in Secure World (privileged), leaving the RIF with its default reset configuration (all memories reserved to secure privileged CPU access). The firmware is responsible for implementing isolation between secure and nonsecure domains.

3.6 Package “Hardware Protections” Security Functional Requirements

The platform fulfills the following Security Functional Requirements:

3.6.1 Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other functional requirements.

Conformance rationale:

The platform provides the following hardware countermeasures against physical attacks:

- ROM code execution hardening using redundancy checks and time jittering.
- Detection of transient perturbation attacks in crypto functions (SAES, PKA private operations).
- Detection of unauthorized modification of sensitive data stored in fuses.
- Prevention of leakage of information through electromagnetic emissions and power consumption when using AES algorithm (in SAES) or private key cryptography (in PKA).

Although not activated by default, the integrator can activate the tamper detection and response hardware present in the platform. Doing so does not impact the "Secure Initialization of Platform" SFR described in Section 3.3.2.

Refer to the security guidance [SG] Section 4.2.1 for details on antitamper optional features available in the platform.

4 Mapping and Sufficiency Rationales

4.1 SESIP3 Sufficiency

Table 11. SESIP3 Sufficiency

Assurance class	Assurance families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in the title, the TOE reference in the “Platform Reference”, the TOE overview and description in “Platform Functional Overview and Description”.
	ASE_OBJ.1 security requirements for the operational environment	Section 0	For the objectives for the operational environment in "Security Objectives for the Operational Environment", refer to the guidance documents.
	ASE_REQ.3 listed security requirements	Section 3.3 to Section 3.6	All SFRs in this ST are taken from [SESIP]. “Verification of Platform Identity” is included. “Secure Update of Platform” is not included (justification in ALC_FLR.2).
	ASE_TSS.1 TOE summary specification	Section 0	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in “Security Functional Requirements”.
ADV: Development	ADV_FSP.4 complete functional specification	Section 1.3 and material provided to the evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirements.
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	Material provided to the evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirements.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Section 1.3	The platform evaluator will determine whether the provided evidence is suitable to meet the requirements.
	AGD_PRE.1 Preparative procedures	Section 1.3	The platform evaluator will determine whether the provided evidence is suitable to meet the requirements.
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	Section 1.3	The platform evaluator will determine whether the provided evidence is suitable to meet the requirements.
	ALC_CMS.1 TOE CM Coverage	Section 4.2	The platform evaluator will determine whether the provided evidence is suitable to meet the requirements.
	ALC_FLR.2 Flaw reporting procedures	Section 3.2	The flaw reporting and remediation procedure is described.
ATE: Tests	ATE_IND.1 Independent testing: conformance	Material provided to the evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirements.
AVA_VAN.3	AVA_VAN.3 Focused Vulnerability analysis	NA A vulnerability analysis is performed by the platform evaluator to ascertain the presence of potential vulnerabilities.	The platform 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 platform evaluator assuming a potential attack of Enhanced-Basic.

4.2 PSA Security Function Mapping

This table refers to the *SESIP Profile for PSA Certified RoT Component Level 3* [SP2]. This section refers to the claims and activities which this SESIP evaluation scope to demonstrate sufficiency by SESIP methodology.

Table 12. PSA Security Function Mapping

PSA Security Function	Covered by SESIP SFR	This platform
F.INITIALIZATION	Secure Initialization	Yes
F.SOFTWARE_ISOLATION	Software Attacker Resistance: Isolation of Platform	Yes
	Software Attacker Resistance: Isolation of Application Parts	No
F.SECURE_STORAGE	Secure Encrypted Storage	No
	Secure Trusted Storage	No
	Secure Data Serialization	No
F.FIRMWARE_UPDATE	Secure Update of Platform	No
F.SECURE_STATE	Software Attacker Resistance: Isolation of Platform	Yes
	Secure Initialization	Yes
	Secure Update of Platform	No
F.CRYPTO	Cryptographic Operation	Yes
	Cryptographic KeyStore	Yes
	Cryptographic Random Number	Yes
	Cryptographic Key Generation	No
F.ATTESTATION	Verification of Platform Identity	Yes
	Verification of Platform Instance Identity	No
	Attestation of Platform Genuineness	No
	Attestation of Platform State	No
F.AUDIT	Audit Log Generation and Storage	No
F.DEBUG	Secure Debugging	No
F.PHYSICAL	Physical Attacker Resistance	Yes
Additional security functionality	Secure Communication Support	No
	Secure Communication Enforcement	No

5 Reference documents

Table 13. Reference documents

Reference	Definition
Evaluation documents	
[SESIP]	*Security Evaluation Standard for IoT Platforms (SESIP), version 1.2 (July 2023), GlobalPlatform®, GP_FST_070*
[SP1]	*SESIP Profile for Secure MCUs and MPUs, version 1.0 (Oct 2021), GlobalPlatform®, GPT_SPE_15*
[SP2]	*SESIP Profile for PSA Certified RoT Component Level 3, version 1.0 REL 02 (24/11/2022), Arm®, JSADEN018*
Development documents	
[SG]	*STM32N65x security guidance for SESIP level 3 certification (UM3451), revision 2*
[RM]	*STM32N6xx Arm®-based 32-bit MCUs (RM0486), revision 3*
[ES]	*STM32N6xxxx device errata (ES0620), revision 1*
Standards	
[SP 800-90B]	*NIST, Special Publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018, https://doi.org/10.6028/NIST.SP.800-90B*

6 Glossary

Table 14. **Glossary**

Term	Definition
Application	Used in SESIP to refer to the components that are out of the scope of the evaluation
Nonsecure processing environment (NSPE)	The Arm® Cortex® processing environment that hosts the nonsecure system software and application-specific software
Platform	Used in SESIP to refer to the components that are in the scope of the evaluation. It is a synonym for connected platform.
Product	Used by SESIP as a synonym for a connected product
Secure processing environment (SPE)	The Arm® Cortex® processing environment that usually hosts the RoT, and any application RoT services

7 Abbreviations

Table 15. **Abbreviations**

Term	Definition
DHUK	Derived hardware unique key
NSPE	Nonsecure processing environment
RoT	Root of Trust
SP	SESIP profile
SPE	Secure processing environment

Revision history

Table 16. **Document revision history**

Date	Revision	Changes
25-Feb-2025	1	Initial release.
25-Mar-2025	2	Updated title, Table 3 with additional note, Table 7 with additional device part number line, and Table 13 with revised document titles.

Contents

List of tables

List of figures