Security Target for Hi3322V100

Version 1.9, dated *2025-11-25*

Hisilicon

Based on [2] methodology, version “Public Release v1.2, July 2023”

1 Introduction

The Security Target describes the Hi3322V100 platform and the exact security properties of the Platform that are evaluated against GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.2, SESIP Assurance Level 2 (SESIP2) [2].

1.1 ST reference

See title page.

1.2 SESIP Profile Reference and Conformance Claims

Table 1. SESIP Profile Reference and Conformance Claims

Reference	Value
PP Name	SESIP Profile for PSA Certified Level 2 [1]
PP Version	2.0 REL 01
Assurance Claim	SESIP Assurance Level 2 (SESIP L2)

1.3 Platform reference

Table 2. Platform Reference

Reference	Value
Platform Name and Version	See section 3.2.1
Platform Identification	Chip Name: Hi3322V100
Platform Type	Microcontroller platform for IoT applications

1.4 Included guidance documents

The following documents are included with the platform:

Document	Reference
Hi3322V100 system security design	[4]
Hi3322V100 Secure Boot Design	[5]
Hi3322V100 Secure Upgrade Design	[6]
Hi3322V100 SELiteOS Secure Design	[7]
Hi3322V100 Data Sheet	[8]
Hi3322V100 Software Development Kit Guidance	[9]
Hi3322V100 Secure Provisioning Guidance	[10]
Hi3322V100 lifecycle	[3]

Management	

1.5 Platform functional overview and description

Hi3322V100 is a low-power and highly secure IoT chipset which targets market of consumer smart wearable device. It integrates state-of-the-art security components including TEE RISC-V core, system memory security isolation technology, cryptographic algorithm hardware accelerator, true random generator, key management and secure debug etc. It provides a trusted execution environment for running applications that require high security. External NOR Flash as an extended executable memory supports configurable on-the-fly decryption and Flash Access Permission Control(FAPC) to enhance the security.

The main security features of TOE are as follows:

- Secure boot and Secure upgrade.
- Cryptographic algorithm accelerator

  - AES 128 with ECB, CBC, CTR and GCM modes.

  - ECDSA and ECDH with brainpoolP256 curve

  - SHA2-256

  - HMAC-SHA2-256
- True random number.
- Key derivation function based on efuse root key.
- Trusted executed environment, consist of TEE RISC-V MCU, APC(Access Permission Check) for I/D TCM memory, FAPC(Flash Access Permission Check) for external NOR-Flash, and inbuild hardware isolation mechanisms in eFuse Controller, KM, PKE, TRNG, SPAcc and SFC modules. You can find more details in [4].
- On-the-fly decryption of SELiteOS Firmware stored in external NOR Flash. It uses AES 128 CTR mode with hardware key derived by KM module.
- Trusted service embeded in SELiteOS Firmware running in TEE, such as secure encrypted storage, attestation of platform genuineness, cryptographic key generation etc.
- Secure debugging of SWD and SSI, binding with lifecycle states.

1.5.1 Platform Physical Scope

The physical scope is the Hi3322V100 chip as shown in Figure 1.

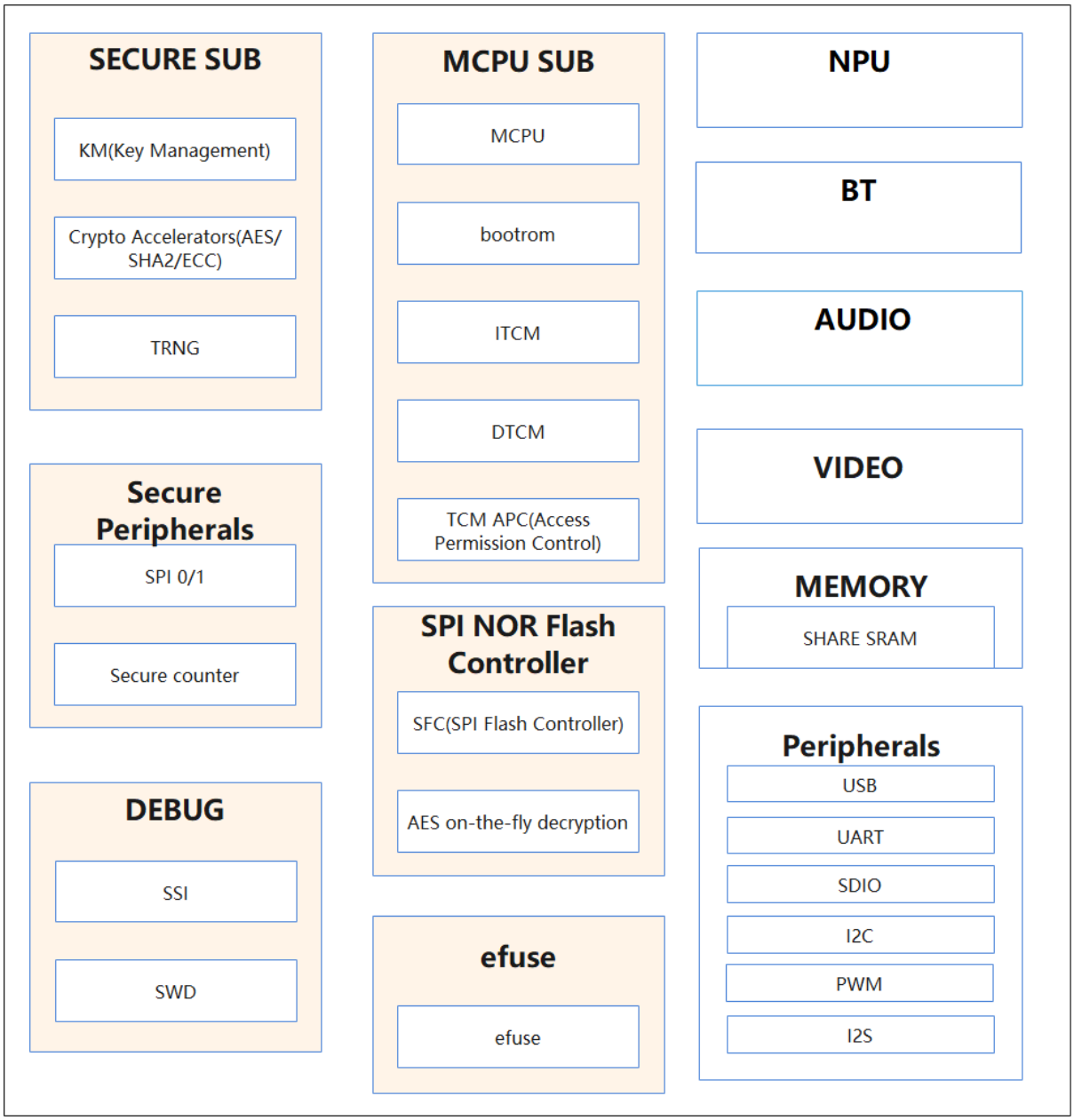

Figure 1 Platform Physical Scope

1.5.2 Platform Logical Scope

The logical scope includes immutable part and updatable part, as shown in Figure 2. Table 3 shows the list of immutable components and Table 4 shows the list of updatable components.

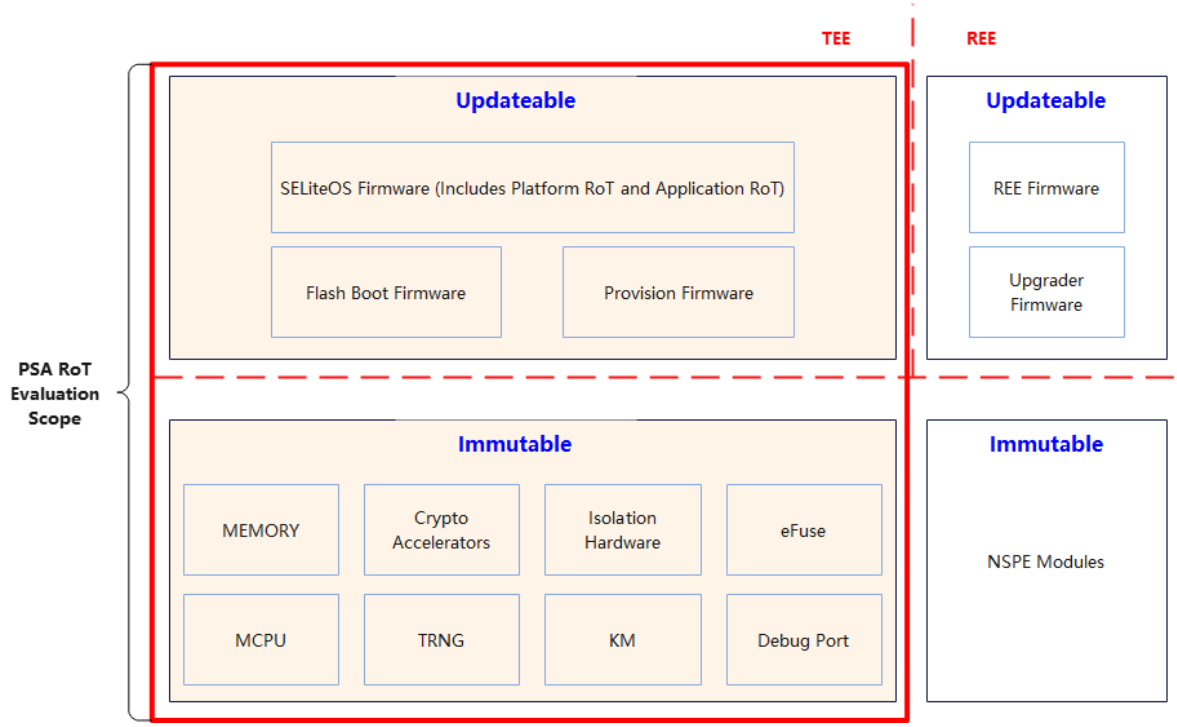

Figure 2: Scope of PSA Certified Level 2

Table 3. List of immutable components in TOE

Components	Description
MCPU	Trusted Execution State CPU is Hisilicon's proprietary RISC-V IP. The microarchitecture of TES CPU supports in-built hardware isolation between trusted executed state(TEE) and rich executed state(REE).
MEMORY	Includes ITCM, DTCM, bootrom and SPI Nor Flash.
eFuse	One of one-time programmable non-volatile memory technology. It stores the platform identity and platform instance identity, root key of product, the hash value of the root public key of RoT, the version of upgradable firmware and the security control bits of the system.
Debug Port	Includes SWD, SSI and JTAG.
KM	Key Management component, to derive various effective keys from efuse root key.
TRNG	True Random Number Generator.
Crypto Accelerators	Includes AES/ECC/SHA2 hardware accelerators.
Isolation Hardware	Hardware modules which are responsible for TEE/REE isolation.

Table 4. List of updatable components in TOE

Components	Description
Provision Firmware	A firmware which is used for programming flash and efuse in provision stage. It is loaded via UART or USB and verified by bootrom code.
Flash Boot Firmware	Mutable Root of Trust firmware which loaded and verified by bootrom.

Components	Description
SELiteOS Firmware	Firmware running in Trusted executable environment, performs the functions which meet some of SFRs. SELiteOS includes the function of Platform RoT and Application RoT.

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 5. Platform Objectives for the Operational Environment

Secure Objectives	Description	Reference
Trusted provisioning environment	Both chip vendor provision and OEM provision are required to be deployed in environment where there is no physical attack possible. The OEM provision is expected to be done correctly, including the efuse program and flash image program, fully following the guidance provided by chip vendor.	[10] section 2.1
Trusted Users	Actors in charge of platform management, for instance for signature of firmware update, are trusted.	[10] section 2.4.2
Secure Boot	Secure boot feature is expected to be enabled by OEM during OEM vendor provision stage.	[10] section 2.4.2 [3] section 3 [5]
Secure Debug	Secure Debug feature is expected to be enabled by OEM during OEM vendor provision stage. Secure Debug state is enabled by changing lifecycle status to 'End User state'.	[10] section 2.4.3 [3] section 3
SW Integration	The operating system or application code are expected to ensure the correct version of the firmware are integrated and configured.	[10] section 2.4.1
Secure Update	The operating system or application code are expected to update an image with proper remedy solution and version increased.	[5] section 2.2.1 and section 2.2.2 [6]
Key management	Cryptographic keys and certificates outside of the platform are managed securely by OEM vendor.	[10] section 2.4.2
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 End-User state.	[10] section 2.4.3 [3] section 3

3 Security requirements and implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP2** as defined in [2].

3.1.1 Flaw Reporting Procedure (ALC_FLR.2)

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to give generate any needed update and distribute it, the developer has defined the following procedure:
The Product Security Incident Response Team (PSIRT) of HiSilicon (Shanghai) receives, investigates, and discloses security vulnerabilities of HiSilicon (Shanghai) products and solutions. PSIRT provides a public available interface(https://www.hisilicon.com/en/PSIRT), to publish the comprehensive vulnerability handling process based on ISO 29147/30111 standard. This process includes 6 steps:

- **Report.** Any vulnerability finders can report potential vulnerabilities to HiSilicon (Shanghai) PSIRT at hi_psirt@hisilicon.com in an encrypted manner, with PSIRT public PGP key encryption.
- **Vulnerability Awareness.** After receiving a vulnerability report, HiSilicon (Shanghai) PSIRT acknowledges the receipt and asks the product team to analyze the reported vulnerability.
- **Vulnerability Verification.** HiSilicon (Shanghai) confirms potential vulnerabilities and uses the CVSSv3.1 scoring system (https://www.first.org/cvss/) to assess the risk level and determine the response priority.
- **Remediation Development.** HiSilicon (Shanghai) develops patches and versions to remediate vulnerabilities and tests them to ensure their quality.
- **Publish.** HiSilicon (Shanghai) generally releases remediation solutions to customers in the form of guides, patches, or software versions, and notifies customers through an SA or release notes so that customers can make risk-related decisions accordingly.
- **Post-Remediation Activity.** HiSilicon (Shanghai) collects feedback from customers and updates remediation solutions if necessary. HiSilicon (Shanghai) TAC provides patch download, update, and Q&A services.

3.2 Security Functional Requirements

The platform fulfills the following security functional requirements:

3.2.1 Verification of Platform Identity

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

Conformance rationale:

IC hardware version & Bootrom version: compose of 16 bit register ‘glb_ctl_chip_name’ and 2 bit efuse ‘chip_version’. Value of platform Identity can be get by calling API uapi_efuse_get_chip_version(const uint8_t *buffer, uint16_t length), the expected value is

"332200" in ASCII encoded. Bootrom version is always same as IC hardware version. IC hardware version can also be retrieved by API psa_initial_attest_get_token, for more details please refer to [9].

NSPE firmware version: All NSPE firmware share one unified version: B220. It is upgradable when NSPE firmware updates in future. It can be retrieved by AT command 'AT+ GETWSTPVER'. It can also be retrieved by API psa_initial_attest_get_token, for more details please refer to [9].

SPE firmware version: All SPE firmware share one unified version: S200. It is upgradable when SPE firmware updates in future. It can be retrieved by AT command 'AT+ GETWSTPVER'. It can also be retrieved by API psa_initial_attest_get_token, for more details please refer to [9].

3.2.2 Verification of Platform Instance Identity

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

Conformance rationale:

The platform stores a 128-bit non-sequential Universally Unique Identifier (UUID) defines by Hisilicon, also known as DieID. This UUID is generated in wafer sort, compose of time, die location, wafer lot id and wafer id etc., to ensure the uniqueness of this UUID. The lock bit of UUID is programmed together with UUID, to make UUID non-writable. This is for ensuring the integrity of this UUID. Both UUID and its lock bit are programmed in on-chip efuse memory.

3.2.3 Attestation of Platform Genuineness

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

Conformance rationale:

The platform can generate attestation token based on information such as Client ID, Instance ID, lifecycle state and run-time state of the device etc. This attestation token is signed by device-unique Attestation Private key which is generated and stored at OEM provision stage. The attestation token can be verified by attestation verification entity. Please see [7] to get more details of attestation generation.

3.2.4 Secure Initialization of Platform

The platform ensures its integrity and authenticity during platform initialization. If the platform integrity or authenticity cannot be ensured, the platform will go to a state where no other operation except optionally Secure Update of Platform can be performed.
Conformance rationale:

Secure boot prevents unauthorized code from being executed on a given product. The product always boots from on-chip immutable ROM code and ROM code verifies the integrity and authenticity of code resident in external NOR Flash. If the code resident in external memory is authentic, then control is transferred to it. This establishes a chain of trusted code from the ROM to the other code. This chain can be further extended, through the verification of digital signatures associated with additional code layers. If either authenticity or integrity of the code cannot be ensured, the platform never boot up normally, print the failure information, and reboot.
Please see [5] for more details.

3.2.5 Attestation of Platform State

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

See section 3.2.3.

3.2.6 Secure Update of Platform

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

Conformance rationale:

Secure Update is the process used to securely update the firmware to a newer version.

The firmware to be updated is downloaded by application, and signed with ECDSA brainpoolP256r1 algorithm, to ensure both the authenticity and integrity. Furthermore, SELiteOS Firmware is in encrypted form, to ensure confidentiality. After that application programs an upgrade flag to dedicated location of external NOR Flash, to indicate the system need to enter upgrade mode.

Then application triggers a system reset to reboot the system. When boot up again flash boot checks the upgrade flag and starts secure upgrade of platform. Secure upgrade function will check the authenticity and integrity of all newer version of all firmware to be updated, and check SELiteOS firmware is in encrypted form, not in clear form. Only check is pass, the corresponding firmware can be programmed to flash. Please refer to [5] and [6] for details.

3.2.7 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 the other functional requirements.
Conformance rationale:

There are multiple isolation designs in the platform.

Hisilicon's TES extension RISC-V core supports secure isolation by providing 2 distinct levels of privilege: secure mode(TEE) and normal mode(REE), and PMP(Physical Memory Protection) for each mode.
The TCM Access Permission Control(TCM APC) block implements access control for on-chip memories.
The Flash Access Permission Control(FAPC) block in SFC implements access control for external NOR Flash.
The hardware secure/nonsecure isolation is also embedded in system modules which are relevant to security features, such as cryptographic accelerators.
Please refer to [4] and [7] for further details.

3.2.8 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 the other functional requirements.
Conformance rationale:

This is implemented by enhanced PMP configuration, enhanced PMP also belongs to RISC-V PMP standard which supports user mode and machine mode isolation feature based on original RISC-V PMP standard. For detailed introduction of enhanced PMP, please refer to https://github.com/riscvarchive/riscv-tee/blob/main/Smepmp/Smepmp.pdf.
A new CSR register named mseccfg is imported to support isolation between user mode and machine mode, when mseccfg.MML is set, enhanced PMP configuration is activated.
SELiteOS code use enhanced PMP to achieve user/machine mode isolation for whole SOC address space, please refer to [7] section 4.2 for more details.

3.2.9 Cryptographic Operation

The platform provides the application with list of cryptographic operations/algorithms/specifications/ken lengths/modes specified in Table 6.

Table 6. Cryptographic Random Number GenerationOperation	**Algorithm**	**Specification**	**Key Lengths (bits)**	**Modes**
Encryption and decryption	AES	NIST FIPS 197	128	ECB, CBC, CTR
Authenticated Encryption, Authenticated Decryption	AES	NIST SP800-38d	128	GCM
Hash	SHA2	NIST FIPS 180-4	256	-
MAC generation and verification	HMAC	RFC 2104	256	SHA2
Key Exchange	ECDH	RFC 5639	256	BrainpoolP256r1

Table 6. Cryptographic Random Number GenerationOperation	Algorithm	Specification	Key Lengths (bits)	Modes
Signature generation and verification	ECDSA	RFC 5639	256	BrainpoolP256r1

Conformance rationale:

The cryptographic accelerators are supported in Hi3322V100. SELiteOS implements above algorithm with hardware acceleration.

3.2.10 Cryptographic Random Number Generation

The platform provides the application with a way based on methods in Table 7 to generate random numbers.

Table 7. Cryptographic Random Number Generation

Methods	Specification
Physical Noise	8 physical Galois Ring Oscillators
DRBG	NIST SP800-90A CTR-DRBG with AES-128

Conformance rationale:

The platform provides a physical true random number generator with inbuilt online test and DRBG. The TRNG can pass AIS 31 statistical tests T0-T8.

3.2.11 Cryptographic Key Generation

The platform provides a way to generate cryptographic keys for use in Table 8.

Table 8. Cryptographic Key Generation

ID	Algorithm	Specification	Key Lengths (bits)
ECC	ECC	ANSI X9.62	256 bits
Symmetric	Symmetric	None	128 bits

Conformance rationale:

The ECC key and Symmetric key generation function are provided by SELiteOS firmware. Please see more in [7].

3.2.12 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 dedicated efuse key slots for rootkey storage. Rootkey is obfuscated with RTL harden key, using AES algorithm, to ensure the key storage in efuse protects against physical tampering attack. Rootkeys are invisible to any software and debug port, they are routed to hardware KM module for key derivation only. KM module derive the effective key from rootkey, and route effective key to cryptographic accelerators, none of intermediate keys and final keys are invisible to software.
The KeyStore of asymmetric key like attestation private key are under protection of Secure Encrypted Storage service. It is encrypted with AES-GCM and stored in external NOR Flash.

3.2.13 Secure Debugging

The platform provides two debug interfaces: Serial Wire Debug (SWD) interface and Synchronized Serial Interface(SSI).
Conformance rationale:

The availability of debug functionality depends on the life-cycle state of the platform, as specified in [4].

3.2.14 Secure Encrypted Storage

The platform provides that all user data stored, except for data not stored by calling secure storage API, is encrypted with AES-128-GCM algorithm, with a platform instance unique key.
Conformance rationale:

The platform provides secure storage service in TEE domain and provide API to both TEE domain and REE domain. The secure storage service has inbuilt TEE/REE isolation mechanism. It performs data encryption/decryption with platform instance unique key, derived from hardware KM module. Please see [7] for more details.

3.2.15 Secure Data Serialization

The platform ensures that all data stored outside the direct control of the platform, except for NSPE user data, is protected such that the authenticity, integrity, confidentiality and binding to the platform instance identity is ensured.
Conformance rationale:

Same as section 3.2.14.

Confidentiality, integrity and authenticity are ensured by AES-128-GCM algorithm. Confidentiality(encryption) and integrity(GCM tag calculation) are easy for understanding, authenticity is ensured by platform instance unique key derived from efuse Rootkey and Platform Instance identity(also known as DieID) via hardware KM module. Please see [7] for more details.

4 Mapping and sufficiency rationales

This ST and associated TOE provide exact conformance to [1].

4.1 SESIP2 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 is in section 1.3, the TOE overview and description is in section 1.5.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in section 2 refers to the guidance documents.
	ASE_REQ.3 Listed Security requirements	Section 3.2	All SFRs in this ST are taken from [1] and [2].
	ASE_TSS.1 TOE Summary Specification	Section 3	All SFRs are listed per definition, and for each SFR the implementation and verification is defined in section 3.2.
ADV: Development	ADV_FSP.4 Complete functional specification	Materials provided to evaluator	The evaluator will determine whether the provided evidence meets the requirement.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	section 1.4	The evaluator will determine whether the provided evidence meets the requirement.
	AGD_PRE.1 Preparative procedures	section 1.4	The evaluator will determine whether the provided evidence meets 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: Tests	ATE_IND.1 Independent testing: conformance	Materials provided to evaluator	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA_VAN.2	AVA_VAN.2 Vulnerability survey	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.

5 References

[1] SESIP Profile for PSA Certified Level 2, JSADEN012, 2.0 REL
[2] GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP) Methodology, GP_FST_070, Public Release v1.2, July 2023
[3] Hi3322V100 lifecycle Management
[4] Hi3322V100 system security design
[5] Hi3322V100 Secure Boot Design
[6] Hi3322V100 Secure Upgrade Design
[7] Hi3322V100 SELiteOS Secure Design
[8] Hi3322V100 Data Sheet
[9] Hi3322V100 Software Development Kit Guidance
[10] Hi3322V100 Secure Provisioning Guidance