

**Security Target for  
SQ713x Series Secure Element  
Version 1.7,  
Dated 2026-04-10**

**iMQ Technology Inc.**

## Table of Contents

|          |                                                                  |           |
|----------|------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Introduction.....</b>                                         | <b>3</b>  |
| 1.1      | ST Reference.....                                                | 3         |
| 1.2      | SESIP Profile Reference .....                                    | 3         |
| 1.3      | Platform Reference .....                                         | 3         |
| 1.4      | Included Guidance Documents .....                                | 3         |
| 1.5      | Platform Functional Overview and Description .....               | 3         |
| 1.5.1    | Platform Type .....                                              | 4         |
| 1.5.2    | Physical Scope .....                                             | 4         |
| 1.5.3    | Logical Scope of the Platform .....                              | 4         |
| 1.5.4    | Usage and Major Security Features .....                          | 5         |
| 1.5.5    | Required Hardware/Software/Firmware .....                        | 5         |
| <b>2</b> | <b>Security Objectives for the Operational Environment .....</b> | <b>6</b>  |
| <b>3</b> | <b>Security Requirements and Implementation.....</b>             | <b>7</b>  |
| 3.1      | Security Assurance Requirements.....                             | 7         |
| 3.2      | Flaw Reporting Procedure (ALC_FLR.2) .....                       | 7         |
| 3.3      | Security Functional Requirements.....                            | 7         |
| 3.3.1    | Verification of Platform Identity .....                          | 7         |
| 3.3.2    | Secure Initialization of Platform .....                          | 7         |
| 3.3.3    | Secure Update of Platform.....                                   | 8         |
| 3.3.4    | Physical Attacker Resistance .....                               | 8         |
| 3.3.5    | Cryptographic Operation.....                                     | 9         |
| 3.3.6    | Physical Scope of the Platform.....                              | 9         |
| 3.3.7    | Cryptographic Random Number Generation .....                     | 10        |
| 3.3.8    | Cryptographic Key Generation.....                                | 11        |
| 3.3.9    | Cryptographic KeyStore .....                                     | 11        |
| 3.4      | Additional Security Functional Requirements .....                | 11        |
| 3.4.1    | Secure Communication Support.....                                | 12        |
| 3.5      | Optional Security Functional Requirements.....                   | 12        |
| <b>4</b> | <b>Mapping and Sufficiency Rationales.....</b>                   | <b>13</b> |
| 4.1      | Assurance.....                                                   | 13        |
| 4.2      | PSA Security Functions Mapping.....                              | 14        |
| <b>5</b> | <b>Glossary .....</b>                                            | <b>15</b> |
| <b>6</b> | <b>References .....</b>                                          | <b>16</b> |
| <b>7</b> | <b>Revision History.....</b>                                     | <b>17</b> |

# 1 Introduction

## 1.1 ST Reference

This ST's title is "SQ713x Series Secure Element" version 1.7 dated 2026-04-10.

## 1.2 SESIP Profile Reference

| Reference                    | Value                                                                    |
|------------------------------|--------------------------------------------------------------------------|
| PP Name                      | SESIP Profile for PSA Certified™ Level 3 iSE/SE and RoT Component [SP-1] |
| PP Version                   | V2.0 BETA 01                                                             |
| Assurance Claim              | SESIP Assurance Level 3 (SESIP 3)                                        |
| SESIP Standard               | GP-SESIP [SESIP]                                                         |
| Optional and Additional SFRs | Secure Communication Support                                             |

**Table 1 SESIP Profile Reference and Conformance Claims**

## 1.3 Platform Reference

| Reference               | Value                                                                                                |                        |
|-------------------------|------------------------------------------------------------------------------------------------------|------------------------|
| Platform Name           | SQ713x Series Secure Element                                                                         |                        |
| Platform Version        | Hardware and ROM: V1.06 – detailed in section 3.3.1<br>Firmware: V2.1.00 – detailed in section 3.3.1 |                        |
| Platform Identification | Hardware reference                                                                                   | SQ7131, SQ7133, SQ7135 |
|                         | Software Reference                                                                                   | iMQ_FW_2_1_00          |
| Platform type           | Secure Element                                                                                       |                        |

**Table 2 Platform Reference**

## 1.4 Included Guidance Documents

| Reference             | Name                                                                  | Version          |
|-----------------------|-----------------------------------------------------------------------|------------------|
| [AGD_PRE_OPE]         | Preparative and Operative Procedures for SQ713x Series Secure Element | V1.7, 2026-04-10 |
| [Datasheet]           | SQ7131 7133 7135 Datasheet V1.8                                       | V1.8, 2026-03-27 |
| [UserManual_StartKit] | Secure StarterKit User Manual                                         | V2.3, 2025-11-26 |

**Table 3 Guidance Documents**

All these guidance documents are available to authorized users via secure request.

## 1.5 Platform Functional Overview and Description

### 1.5.1 Platform Type

The TOE is a **Secure Element** which can be used as a Trustable System-on-Chip (TSoC) for providing cryptographic services to a secure connected IOT device. The iMQ SQ713x series platform IC is built on iMQ's proprietary 16-bit CPU core, the 870E, derived from Toshiba's 8-bit TLCS-870/C1 core. The 870E core retains the same instruction set architecture (ISA) as the 870C1. However, its internal general-purpose registers, as well as the address, instruction, and data buses, have been upgraded from 8-bit to 16-bit. The usage and security features of the SE is further described in section 1.5.3.

### 1.5.2 Physical Scope

The proposed TOE is composed of hardware design, embedded firmware, and guidance documents:

- **Hardware:** iMQ SQ713x series IC is the secure element dedicated for network security and authentication. iMQ proprietary Trust Computing Engine, hereinafter will be referred to as "iMQ\_TCE," is a physical hardware implemented design with high security strength compliant with NIST standard FIPS 140-3 level 3. iMQ\_TCE\_V1\_06 hardware design includes hash, symmetric and asymmetric cryptographic algorithms, secure boot loader as well as anti-tamper physical layer protection. The relevant security function claimed in [Datasheet] section 3.3.
- **Embedded firmware:** iMQ specific firmware stack and crypto library are tailored for encryption/decryption application. iMQ\_FW\_2\_1\_00 software design includes iMQ proprietary secure boot, command handler and self-test on health as well as exception and zeroization procedure.
- **Guidance documents:** refer to Section 1.4.

### 1.5.3 Logical Scope of the Platform

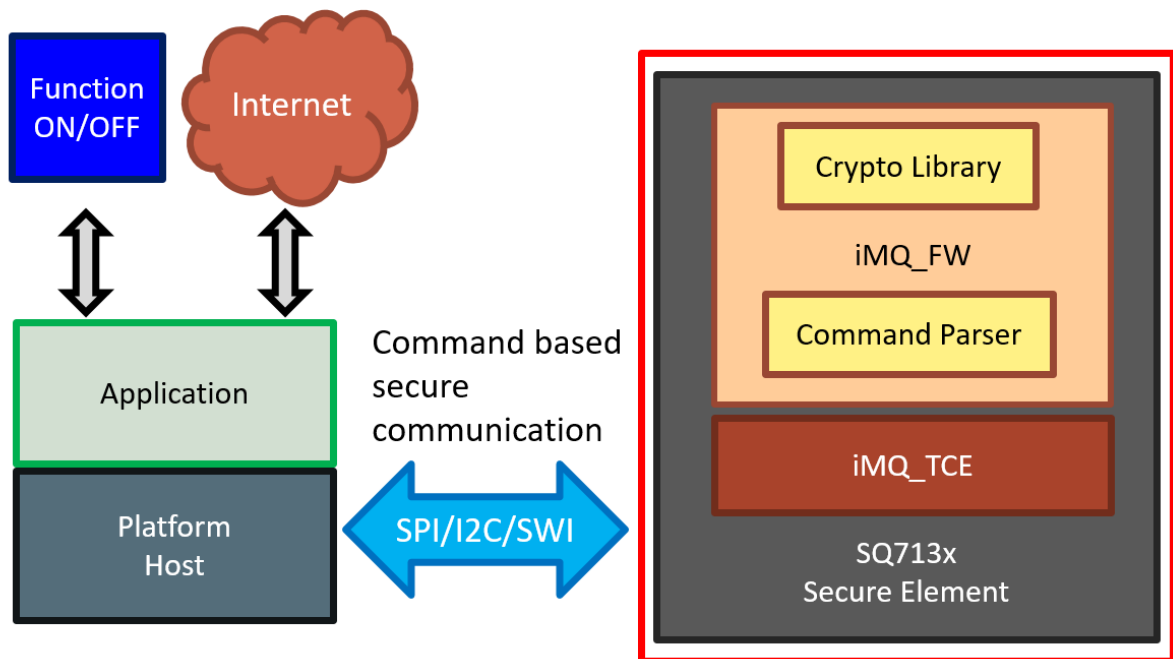


Figure 2 Logical Scope of TOE

The logical scope of the platform is illustrated within the red box of Figure 2. The logical scope includes: SE Hardware (V1.06) and Firmware (V2.1.00). The scope for the Security evaluation is the combination of the trusted hardware and firmware components implementing a secure element environment with the Security Functional Requirements stated in this document. The SQ713x secure element includes the embedded firmware "iMQ\_FW" and the circuit implemented cryptographic accelerator "iMQ\_TCE." The secure boot loader is bundled in the iMQ\_TCE design to check the digest from firmware image. Within iMQ\_FW, the major two portions are a compact "Crypto Library" which is based on the supported cryptographic algorithms in iMQ\_TCE and a proprietary "Command Parser" used to handle the command request from platform host. The security functions built inside iMQ\_FW are only accessible if the data of firmware passes the integrity validation by boot loader during startup. If the validation fails during the boot stage, subsequent command requests from

platform host will be rejected by iMQ\_FW, which instead returns an error status.

The “Crypto Library” is primarily designed to bridge the computing efforts between software-based cryptographic procedures and the hardware-implemented trusted computing engine, iMQ\_TCE. iMQ\_TCE consists of the comprehensive cryptographic accelerators that assist with the computation of cryptographic operations—such as hashing, symmetric, and asymmetric algorithms—all of which are software-programmable.

The only means of communication between the platform host and the proposed TOE is through the command interface. The platform host can request the activation of relevant security functions by adhering to the iMQ proprietary command set protocol. Common serial interfaces such as I2C, SPI, and SWI are supported.

Applications built on top of the platform host are well-suited for network communication equipment due to the implementation of cryptographic features, such as compliance with Internet protocols TLS 1.2 and 1.3 and X.509 certificate, and support for signing and verification operations. Additionally, the proposed TOE is an ideal fit for specific applications like accessory authentication and industrial-grade function switches that require secure control.

### **1.5.4 Usage and Major Security Features**

The TOE is a Secure Element implemented as a discrete hardware component in an SOP8 or 8-Lead DFN package. The TOE operates as an independent security component that interfaces with a Trustable System-on-Chip (TSoC), which is to be further used in Internet of Things (IoT) endpoint. The aim is to provide enhanced security, fast, and low power consumption.

TOE provides the following features for the purpose of PSA Level 3 security evaluation:

- I2C, SPI, and SWI interface with integrity protection
- Cryptographic store for keys and data with confidentiality protection
- Each key and data slot has its own access and usage permissions
- Cryptographic support:
  - ECDH, ECDSA, ECC signature generation/verification, key generation; supported curves:
    - NIST P-256/384
  - RNG:
    - NIST SP800-90B/NIST SP800-90A
  - AES 128/256 encryption/decryption/MAC generation/verification: ECB, GCM
  - HMAC generation/verification based on SHA-256
  - Key Derivation Function (KDF) derives one or more secret keys: KDF-PRF, KDF-HKDF

### **1.5.5 Required Hardware/Software/Firmware**

No additional hardware, software, or firmware are required to utilize the platform.

## 2 Security Objectives for the Operational Environment

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

| ID                    | Description                                                                                                                                                                                                                                                                                                                                  | Reference                                                                                                                                                                         |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KEY_MANAGEMENT        | The operational environment must ensure secure storage and confidentiality of cryptographic keys provisioned into the Secure Element. Keys stored outside the TOE must be protected from unauthorized access and use.                                                                                                                        | [AGD_PRE_OPE] section 4.3.2 "Operational Environment Security and Tools"                                                                                                          |
| SECURE_KEY_PROVISION  | Keys such as Secret Key and IO Protection Key must be provisioned during manufacturing in a secure, trusted facility. No in-field key generation or injection is allowed.                                                                                                                                                                    | [AGD_PRE_OPE] section 4.3.2 "Operational Environment Security and Tools"                                                                                                          |
| SECURE_COMMUNICATION  | The host device must initialize/ establish and end a secure communication channel with the Secure Element, protecting confidentiality, integrity, and authenticity of transmitted data.<br>The host platform application must setup data objects accordingly to enforce shielded connection with pre-shared secret upon these objects.       | [AGD_PRE_OPE] section 4.1 "User Roles and Functionality"<br>[Datasheet] section 11.0 "Authentication and Secure Communication"<br>[Datasheet] section 11.2 "Secure Communication" |
| SECURE_INITIALIZATION | The host platform must ensure that the Secure Element is initialized securely, with verified firmware and boot mechanisms to prevent execution of unauthorized code.                                                                                                                                                                         | [AGD_PRE_OPE] section 4.3.2 "Operational Environment Security and Tools"                                                                                                          |
| PLATFORM_ACCEPTANCE   | When receiving the platform, the user is expected to verify the correct version of all platform components that it depends on, as described in Section 3.3.1 of this document.                                                                                                                                                               | [AGD_PRE_OPE] section 2.1 "Physical TOE"                                                                                                                                          |
| TRUSTED_USERS         | Users shall ensure secure and correct use of the platform according to guidance listed in Section 1.4.<br>Note that there is only one user role allowing to access all the interfaces of the platform with the same privilege and in a unique mode of operation; also all features are accessible in only one configuration of the platform. | [AGD_PRE_OPE] section 4 "Security Guidance"                                                                                                                                       |
| PRESHARED_SECRET      | The pre-shared secret needs to be kept in a confidential way by the application                                                                                                                                                                                                                                                              | [Datasheet] section 11.2 "Secure Communication"                                                                                                                                   |

Table 4 Platform Objectives for the Operational Environment

Note:

- UNIQUE\_ID is not a security objective for this platform, because identification data is already added before customer delivery by the developer of this TOE.

## 3 Security Requirements and Implementation

### 3.1 Security Assurance Requirements

The claimed assurance requirements package is SESIP3, as described in Section 4.1.

### 3.2 Flaw Reporting Procedure (ALC\_FLR.2)

As the TOE consists of MCU hardware with immutable firmware (firmware storage is permanently locked), the platform's SFR secure update is not applicable, since post-deployment updates are not technically feasible.

In accordance with 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 following procedure.

iMQ has defined a Software and Hardware Security Incident Response Procedure (SHSIRP), implemented by a dedicated team (Technical Support). This process provides a publicly available interface (<https://www.imqtech.com/en/tools/pss>) and includes 4 steps:

- Reporting. The process begins when Technical Support becomes aware of a potential security vulnerability in an iMQ product. Upon receiving a report, Technical Support provides an acknowledgment to the reporter and ensures timely updates throughout the investigation and resolution process.
- Evaluation. Technical Support evaluates the reported issue to confirm its validity, assesses associated risks, determines potential impacts, and assigns an appropriate processing priority. This step is critical to ensure that the response is proportionate to the threat level and product context.
- Solution. Once the issue is confirmed, Technical Support collaborates with the relevant product teams to develop an appropriate mitigation strategy. The nature of the solution may vary depending on the type and severity of the vulnerability.
- Communication. The communication on the vulnerability and solutions will in most cases be done directly towards the affected customers.

### 3.3 Security Functional Requirements

#### 3.3.1 Verification of Platform Identity

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

##### Conformance rationale:

The platform referenced in Section 1.3 provides the identifiers listed in Table 5. And the platform implements "Info – Revision" command which can read back the FW revision, device name and silicon revision of the device as described in [Datasheet] section 8.2.1 "Info – Revision."

| Field              | Value                                      | Interpretation             |
|--------------------|--------------------------------------------|----------------------------|
| HW and ROM version | 0x00 0xA6                                  | iMQ_TCE_V1_06              |
| FW version         | 0x02 0x01 0x00 0x00<br>0x00 0x00 0x00 0x00 | iMQ_FW_2_1_00              |
| Device Name        | "SQ7131", "SQ7133" or "SQ7135"             | Device name in ASCII value |

Table 5 Platform identifiers

#### 3.3.2 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 enter a state where it cannot perform any other commands except responding to Info Command and providing information such as revision and error status.

**Conformance rationale:**

The platform implements a robust secure initialization mechanism to ensure the authenticity and integrity of the execution environment during the boot phase. If firmware verification fails or the platform enters an abnormal state, a default security failure response is triggered—such as system reset, halt, or firmware erasure—to prevent execution of unauthorized or potentially malicious code.

The Secure Boot process is fulfilled by the BootROM and executes the corresponding verification process according to the BootOPT mode locked by the NVR and prevents subsequent rewriting through NVR locking mechanism. Depending on the selected mode, the platform applies SHA256 hash or CRC16 algorithms, optionally combined with a 32-byte Boot Key and a device Unique Identifier (UID), to achieve the following functions:

- Utilize SHA256 to generate a digest for the specified firmware segment to verify its integrity.
- Incorporate the BootKey and UID into the SHA256 calculation to strengthen device binding and authorization verification.

All key parameters involved in authentication (such as BootOPT, ACTION, Digest, BootKey) are stored in a Flash security area with hardware access control and are prevented from being rewritten through an NVR locking mechanism. Verification operations are all performed in SRAM, and sensitive data is cleared to prevent data remanence after verification is completed.

If verification fails, the system will take one of the following security actions based on the ACTION field setting:

- Reset: Restart the system immediately
- Erase: Clear the firmware image to prevent improper use
- Hold: The system is stopped and waiting for external processing

Once Secure Boot is set and locked, it forms a fixed and unique root of trust that cannot be modified. If verification fails or the system is abnormal, the platform will enter a security protection state, such as pausing execution, restarting, or forcibly erasing the firmware image, and record the failure information in DIGEST\_LOG to prevent circumventing the platform initialization security line through brute force.

### **3.3.3 Secure Update of Platform**

The platform does not support this update.

**Non-conformance rationale:**

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

### **3.3.4 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 TOE implemented the following protection mechanisms to resist against both side channel and fault

injection physical attacks:

- Exceed High Voltage Detection and Top Metal Shielding
  - ◆ Either high voltage detection or top metal shielding is enabled by user configurable. User shall follow secure use guidance as described in [Datasheet] section 8.15 "Tamper Command (0x92)" to correctly configure the TOE in a secure state so that these mechanisms would take effect.
- DPA Countermeasure
- Redundant/hardened code against Fault Injection

### 3.3.5 Cryptographic Operation

The platform provides Operations in Table 6 functionality with algorithms in Table 6 as specified in specifications in Table 6 for key lengths described in Table 6 and modes described in Table 6.

| Algorithm | Operations               | Specification                   | Key lengths       | Modes                |
|-----------|--------------------------|---------------------------------|-------------------|----------------------|
| AES       | Encryption/decryption    | NIST FIPS 197<br>NIST SP800-38A | 128-bit, 256-bit  | ECB                  |
| SHA-2     | Secure hash              | NIST FIPS 180-4                 | N/A               | SHA-256              |
| ECC       | Digital signature(ECDSA) | FIPS 186-5                      | NIST curves: P256 | ECDSA<br>SecureBoot  |
|           | Key exchange(ECDH)       | NIST SP800-56Ar3                |                   | ECC CDH              |
|           | Key generation           |                                 |                   | Key<br>generation    |
| HMAC      | Generate, Verify         | [N198-1]                        | 256-bit           | SHA-256              |
|           | Key generation           | NIST SP800-135r1                | Up to 512-bit     | KDF-PRF,<br>KDF-HKDF |

Table 6 Cryptographic Operations

#### Conformance rationale:

These cryptographic claims are partly implemented by the cryptographic libraries of the hardware and partly by the firmware. The firmware uses the cryptographic libraries for provisioning cryptographic commands in a harmonized interface to the application. The application then uses these cryptographic commands to implement cryptographic protocols like the Shielded connection with pre-shared secret, or provides APIs to use the cryptographic commands directly. In total, these were designed to meet the requirements mentioned in specification column in Table 6.

### 3.3.6 Physical Scope of the Platform

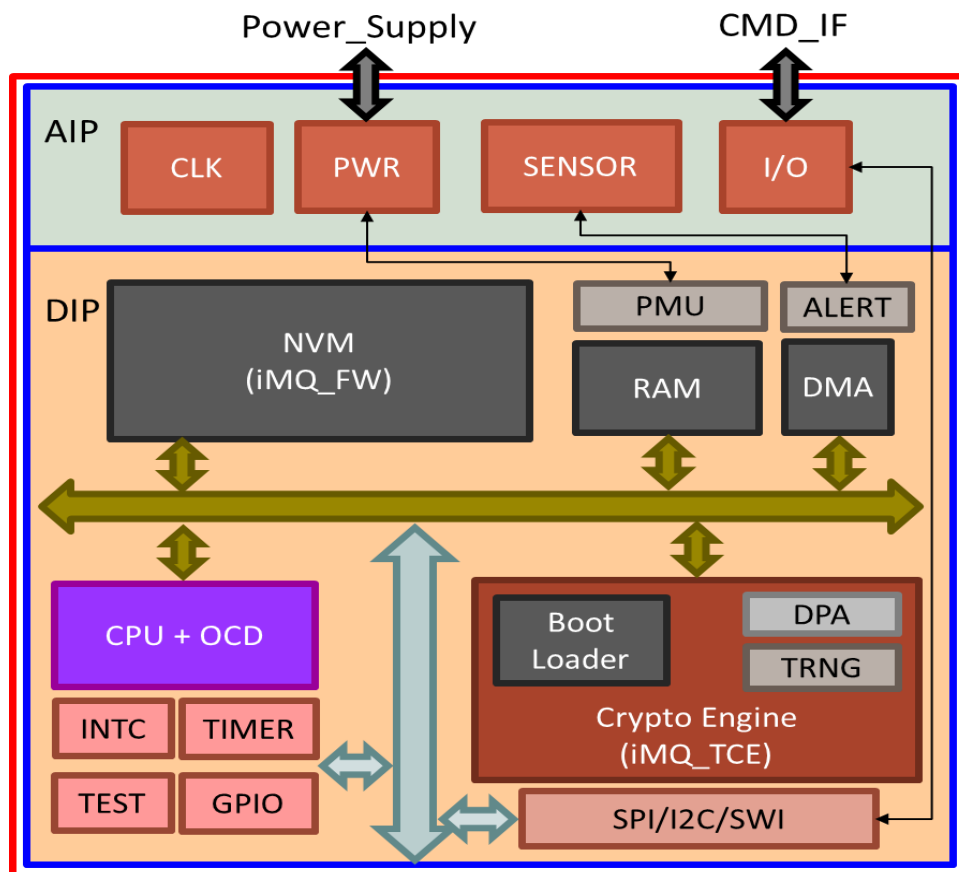


Figure 1 Physical Scope of TOE

The physical scope of the platform is defined by the red box shown in Figure 1.

Within the boundary, two major functional blocks—Analog Intellectual Property (AIP) and Digital Intellectual Property (DIP)—are separated and classified based on their circuit design characteristics.

AIP customized all the analog circuitry required in the TOE, including multiple clock sources (CLK), an internal low-dropout regulator (LDO) as the power supply (PWR), input/output circuits (I/O) for communication with the host via the command interface (CMD\_IF) and environmental sensors (SENSOR) to protect key information from tampering.

DIP designed the required digital circuitry for the TOE, including cryptographic hardware accelerators such as the Trusted Computing Engine (TCE) and the embedded True Random Number Generator (TRNG), as well as essential system-on-chip (SoC) components. These include the processor core (CPU), on-chip debug port (OCD), boot ROM, data memory (RAM), non-volatile program memory (NVM), interrupt controller (INTC), timers, interface peripherals (SPI/I2C/SWI), and a Direct Memory Access (DMA) module to accelerate data movement tasks within the chip.

The proposed TOE is a secure element IC with built-in key protection and management capabilities. It integrates proprietary firmware running on the processor, cryptographic algorithms implemented in digital circuitry, and analog sensors designed to detect and resist tampering attempts. The scope also includes the firmware running on the SE. The SE firmware is pre-installed in the chip.

### 3.3.7 Cryptographic Random Number Generation

The platform provides a way based on several oscillator rings to generate random numbers as specified in NIST SP800-90A [N800-90A] and NIST SP800-90B [N800-90B].

**Conformance rationale:**

The entropy sources are provided by the hard-macro, and the post-processing algorithm for random number generation is implemented by firmware and cryptographic operation. The platform implements random number generation by utilizing the True Random Number Generation capability of the security engine. The TRNG implementation consists of an SP800-90A compliant DRBG that is fed by an SP800-90B compliant seed, which is generated from an entropy source. Each TRNG request generates a 128-bit random number.

### 3.3.8 Cryptographic Key Generation

The platform provides a way to generate cryptographic keys for use in cryptographic algorithms in Table 7 as specified in specifications in Table 7 for key lengths described in Table 7.

| ID       | Algorithm | Specification    | Key lengths |
|----------|-----------|------------------|-------------|
| ECC P256 | ECC       | NIST SP800-56Ar3 | 256         |
| ECC P384 | ECC       | NIST SP800-56Ar3 | 384         |
| KDF      | KDF       | NIST SP800-135r1 | Up to 512   |

Table 7 Cryptographic Key Generation

#### Conformance rationale:

The firmware provides the cryptographic key generation commands as described in [Datasheet] section 5.2 "Data Slot and Access Policies" and section 10.4 "KDF Command (0x56)"

### 3.3.9 Cryptographic KeyStore

The platform provides a way to store cryptographic keys and other protected data objects such that not even the application can compromise the confidentiality of this data. This data can be used for the cryptographic operations: ECDSA, AES, HMAC.

#### Conformance rationale:

TOE provides a complete key storage and usage protection mechanism to ensure that even if the key is stored within the platform, sensitive information will not be leaked due to access by applications or unauthorized entities.

TOE supports AES-128, AES-256, ECC-P256, and ECC-P384 encryption keys. The method of generating and importing keys depends on the type and usage scenario. For example, the ECC private key is randomly generated internally by the TOE based on the GenKey command sent by the Host and stored in a controlled secure area; while the AES key can be imported by the Host in plain text, encrypted format, or generated through the ECDH algorithm or KDF key derivation mechanism.

All keys are stored in TOE's dedicated EEPROM or SRAM space, which has access restrictions and hardware isolation design. The host cannot read the key plaintext in any way and that can only be used in a controlled manner through an authorization mechanism.

To ensure the confidentiality and resistance against analysis of keys during storage, the TOE applies a scrambling process to the key content. The scrambling uses a random seed uniquely stored in NVR, ensuring that even when identical keys are stored on different chips, the actual data representation in memory differs. This further enhances security against physical attacks.

In addition, if the internal CPU needs to perform key import operations, this must be processed through a dedicated hardware encryption engine to ensure that the generation, input, storage and use of keys throughout their entire life cycle are completed within a trusted boundary, thereby achieving the goal of protecting the confidentiality and integrity of the keys.

## 3.4 Additional Security Functional Requirements

### **3.4.1 Secure Communication Support**

The platform provides one secure communication channel.

The secure communication channel authenticates Host Platform and protects against disclosure, modification, replay, erasure of messages between the endpoints, using self-defined protocols and measures.

#### **Conformance rationale:**

The TOE and the host application exchange session public keys, random nonce, and signatures. Based on these parameters and their respective private keys, a shared session key is generated. This key is used to protect the confidentiality (AES-256 CBC) and integrity (MAC) of data during secure communication. For more information, please refer to Section 11.1 "Authentication" and Section 11.2 "Secure Communication" in the [Datasheet].

### **3.5 Optional Security Functional Requirements**

The TOE does not implement any of the optional security functional requirements.

## 4 Mapping and Sufficiency Rationales

### 4.1 Assurance

The assurance activities defined in [PSA-EM-L3] fulfil the SESIP3 activities. In particular, the required source code review, vulnerability analysis and testing of the [PSA-EM-L3] is applicable.

| Assurance Class                 | Assurance Family                                                                       | Covered by                      | Rationale                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ASE: Security Target Evaluation | ASE_INT.1 ST Introduction                                                              | Section 1                       | The ST reference is in Section 1.1, the TOE reference in Section 1.3, the TOE overview and description in Section 1.5.                                                               |
|                                 | ASE_OBJ.1 Security requirements for the operational environment                        | Section 2                       | The objectives for the operational environment in Section 2 refer to the guidance documents.                                                                                         |
|                                 | ASE_REQ.3 Listed Security requirements                                                 | Section 3                       | All SFRs in this ST are taken from [SP-1]. SFR "Identification of Platform Type" is included. SFR "Secure Update of Platform" is mentioned but refers to ALC_FLR.2.                  |
|                                 | ASE_TSS.1 TOE Summary Specification                                                    | Section 3                       | All SFRs are listed per definition, and for each SFR the implementation and verification is defined in the SFR.                                                                      |
| ADV: Development                | ADV_FSP.4 Complete functional specification                                            | Material provided to evaluator. | There is a dedicated mapping table between interface and user guidance reference.<br>The evaluator will determine whether the evidence provided is suitable to meet the requirement. |
|                                 | ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs | Material provided to evaluator. | There is a dedicated mapping table between source code and TSF.<br>The platform evaluator will determine whether the evidence provided is suitable to meet the requirement.          |
| AGD: Guidance Documents         | AGD_OPE.1 Operational user guidance                                                    | Section 1.4                     | These guidelines provide sufficient guidance to operate the TOE in a secure way. It is one of the evaluation tasks to assure this.                                                   |
|                                 | AGD_PRE.1 Preparative procedures                                                       | Section 1.4                     | These guidelines provide sufficient guidance to receive, accept and prepare the TOE in a correct way. It is one of the evaluation tasks to assure this.                              |
| ALC: Life-cycle Support         | ALC_CMC.1 Labelling of the TOE                                                         | Material provided to evaluator. | The evaluator will determine whether the evidence provided is suitable to meet the requirement.                                                                                      |
|                                 | ALC_CMS.1 TOE CM Coverage                                                              | Material provided to evaluator. | The evaluator will determine whether the evidence provided is suitable to meet the requirement.                                                                                      |
|                                 | 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 evaluator. | The evaluator will determine whether the provided evidence and joint execution of testcases is suitable to meet the requirement.                                                     |

|                               |                                          |                                                         |                                                                                                                                                           |
|-------------------------------|------------------------------------------|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| AVA: Vulnerability Assessment | AVA_VAN.3 Focused vulnerability analysis | Vulnerability and testing carried out by the laboratory | The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. |
|-------------------------------|------------------------------------------|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|

**Table 8 Assurance – Evidence Mapping**

## 4.2 PSA Security Functions Mapping

This section shows the platform mapping to the PSA Security Functions.

| PSA Security Function             | Covered by SESIP SFR                                         | This Platform |
|-----------------------------------|--------------------------------------------------------------|---------------|
| F.INITIALIZATION                  | Secure Initialization                                        | Yes           |
| F.SOFTWARE_ISOLATION              | Software Attacker Resistance: Isolation of Platform          | No            |
|                                   | Software Attacker Resistance: Isolation of Application Parts | No            |
| F.SECURE_STORAGE                  | Secure Trusted Storage                                       | No            |
|                                   | Secure Confidential Storage                                  | No            |
|                                   | Secure Encrypted Storage                                     | No            |
|                                   | Secure Data Serialization                                    | No            |
| F.FIRMWARE_UPDATE                 | Secure Update of Platform                                    | No            |
| F.SECURE_STATE                    | Software Attacker Resistance: Isolation of Platform          | No            |
|                                   | Software Attacker Resistance: Isolation of Platform          | No            |
|                                   | Secure Initialization                                        | Yes           |
|                                   | Secure Update of Platform                                    | No            |
| F.CRYPTO                          | Cryptographic Operation                                      | Yes           |
|                                   | Cryptographic KeyStore                                       | Yes           |
|                                   | Cryptographic Random Number                                  | Yes           |
|                                   | Cryptographic Key Generation                                 | Yes           |
| 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                                 | Yes           |

**Table 9 Functionality Mapping and Sufficiency Rationales**

## 5 Glossary

| Term        | Definition                                                                                                                |
|-------------|---------------------------------------------------------------------------------------------------------------------------|
| Application | Used in SESIP to refer to the components that are out of the scope of the evaluation                                      |
| 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                                                                        |
| ECC         | Elliptic Curve Cryptography                                                                                               |
| PSA-RoT     | PSA Root of Trust                                                                                                         |
| SHSIRP      | Software and Hardware Security Incident Response Procedure                                                                |
| SFR         | Security Functional Requirement                                                                                           |
| ST          | Security Target                                                                                                           |
| TOE         | Target of Evaluation, equivalent to “Platform” in current document.                                                       |

## 6 References

| Reference Name | Standard Description                                                                                                                         |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| [N800-135]     | NIST SP 800-135 Rev. 1: Recommendation for Existing Application-Specific Key Derivation Functions, December 2011                             |
| [RFC 5869]     | HMAC-based Extract-and-Expand Key Derivation Function (HKDF)                                                                                 |
| [N180-4]       | NIST: FIPS publication 180-4: Secure Hash Standard (SHS), August 2015                                                                        |
| [N186-5]       | NIST: FIPS publication 186-5: Digital Signature Standard (DSS), July 2013                                                                    |
| [N197]         | NIST: FIPS publication 197: Advanced Encryption Standard (AES), May 2023                                                                     |
| [N198-1]       | NIST: FIPS publication 198-1: The Keyed Hash Message Authentication Code (HMAC), July 2008                                                   |
| [N800-38A]     | NIST SP 800-38B: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001                                   |
| [N800-90B]     | NIST SP 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018                                         |
| [N800-90A]     | NIST Special Publication 800-90A Revision 1 Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015 |
| [N800-56A]     | NIST SP 800-56A Rev. 3: Recommendation for Pair-Wise Key- Establishment Schemes Using Discrete Logarithm Cryptography, April 2018            |
| [SESIP]        | Security Evaluation Standard for IoT Platforms (SESIP) Methodology, GlobalPlatform GP_FST_070, version 1.2, July 2023                        |
| [SP-1]         | SESIP Profile for PSA Certified™ Level 3 iSE/SE and RoT Component, Arm® JSADEN018, version 2.0 BETA 01, 09/07/2024                           |
| [PSA-SM]       | Platform Security Model, Arm, ARM DEN 0079.                                                                                                  |

## 7 Revision History

| Document version | Date of release | Description of changes                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0.7              | 2025-05-09      | First release                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 0.8              | 2025-05-30      | Updated section 3.2 by modifying the flaw reporting procedure; updated section 1.3 by rewriting the platform type; updated section 1.5.4 by modifying the figure; updated section 2 by adding the reference contents of PLATFORM_ACCEPTANCE and SECURE_USE; updated section 3.3.1 by modifying the content of verification of platform identity; updated section 3.3.3 by modifying the content of physical attacker resistance |
| 0.9              | 2025-06-27      | Updated section 1.5.3 and 1.5.4 by modifying both figures and rewording both descriptions; updated section 3.3.5 by adding SecureBoot; updated section 3.3.4 by modifying the content of secure initialization of platform                                                                                                                                                                                                      |
| 1.0              | 2025-07-18      | Updated section 1.4 by adding other guidance documents; updated section 2 by adding the contents of KEY_MANAGEMENT and SECURE_KEY_PROVISION; updated section 2 by modifying SECURE_COMMUNICATION                                                                                                                                                                                                                                |
| 1.1              | 2025-09-08      | Updated section 1.2 to refer to “SESIP Profile for PSA Certified™ Level 3” Protection Profile.                                                                                                                                                                                                                                                                                                                                  |
| 1.2              | 2025-09-10      | Updated section 1.2 to refer to “SESIP Profile for PSA Certified™ Level 3 iSE/SE and RoT Component” Protection Profile. And make alignment with this PP on terminologies, the table format, chapter structure, etc. Additional justification is added to section 3.4.                                                                                                                                                           |
| 1.3              | 2025-10-17      | Add section 3.4.1 Secure Communication and 3.4.2 Secure Communication Enforcement. A minor-modified logical scope is updated. In section 2 Secure Objectives for the Operational Environment, update secure communication, PRESHARED_SECRET, and SHIELDED_CONNECTION.                                                                                                                                                           |
| 1.4              | 2026-02-05      | Remove 3.4.2 Communication Enforcement and PRESHARED_SECRET, and SHIELDED_CONNECTION in section 2 Secure Objectives for the Operational Environment                                                                                                                                                                                                                                                                             |
| 1.5              | 2026-02-26      | Update ST to V 1.5 in Section 1.1; update [AGD_PRE_OPE] to V 1.0 in Section 1.4; remove the wordings of “The function is enabled by default” in “Redundant/hardened code... The function is enabled by default” in Section 3.3.4; modify descriptions of Sections 3.3.5, 3.3.7, and 3.3.8.                                                                                                                                      |
| 1.6              | 2026-04-09      | Update [AGD_PRE_OPE] to V 1.6 and remove [UserManual_Secure Writer] in Section 1.4                                                                                                                                                                                                                                                                                                                                              |
| 1.7              | 2026-04-10      | Update FW version from 2.0 to 2.1 in sections 1.3 and 3.3.1; update [AGD_PRE_OPE] to V 1.7                                                                                                                                                                                                                                                                                                                                      |