# RW61x

## SESIP Security Target

Rev. 1.0 — 6 February 2024 Evaluation document

**Document information**

| Information | Content |
|---|---|
| Keywords | SESIP, PSA, Security Target, RW61x, RW610, RW612 |
| Abstract | Security target for evaluation of the RW61x developed and provided by NXP Semiconductors, according to SESIP Assurance Level 3 (SESIP3) based on SESIP methodology, version 1.1, and PSA Certified Level 3 |

## Revision History

| Rev. | Date | Description |
|---|---|---|
| 1.0 | 6 February 2024 | First released version |

# 1 Introduction

This Security Target describes the RW61x platform and the exact security properties of the platform that are evaluated against  GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.1, SESIP Assurance Level 3 (SESIP3) [1].

## 1.1 ST Reference

RW61x, SESIP Security Target, Revision 1.0, NXP Semiconductors, 6 February 2024.

## 1.2 SESIP Profile Reference and Conformance Claims

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

| Reference | Value |
|---|---|
| SP Name | GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs [2] |
| SP Version | Version 1.0 |
| Assurance Claim | SESIP Assurance Level 3 (SESIP3) |
| Package Claim | Base SP, Package Secure Services, Package Software Isolation, Package Hardware Protection, Package Secure Enclave |

Table 2. SESIP Profile for PSA Certified Level 3 Conformance Claims

| Reference | Value |
|---|---|
| SP Name | SESIP Profile for PSA Certified Level 3 [3] |
| SP Version | V1.0 REL 01 |
| Assurance Claim | SESIP Assurance Level 3 (SESIP3) |
| Optional and Additional SFRs | See Section 4.3 |

## 1.3 Platform Reference

RW61x

Table 3. Platform Reference

| Reference | Value | |
|---|---|---|
| Platform Name and Version | See Table 5 | |
| Platform Identification | Chip name and version | See IC hardware in Table 5 |
| | PSA-RoT name and version | See updatable platform RoT in Table 5 |
| Platform Type | Microcontroller platform for IoT applications | |
| Trusted Subsystem Identification | See security enclave and its software in Table 5 | |

## 1.4 Included Guidance Documents

The following documents are included with the platform:

Table 4. Guidance Documents

| Document | Reference |
|---|---|
| User Manual | UM11865, RW61x User Manual [4] |
| User Manual | UM11864, RW61x Crypto Subsystem [5] |
| Reference Manual | RM00278, RW610/RW612 Registers[6] |
| Datasheet | RW610, Wireless MCU with Integrated Wi-Fi 6 and Bluetooth Low Energy 5.3 Data Sheet [7] |
| Datasheet | RW612, Wireless MCU with Integrated Wi-Fi 6 and Bluetooth Low Energy 5.3 / 802.15.4Data Sheet [8] |
| SESIP Security Target | RW61x, SESIP Security Target, Revision 1.0, NXP Semiconductors, 6 February 2024. |
| API Reference Manual | User Manual of Crypto Library Normal Secure (CLNS) [9] |
| Application Note | AN13813 Secure boot on RW61x [10] |
| Application Note | AN13814 Debug authentication on RW61x [11] |
| Application Note | AN6259, Common Trust Provisioning Conceptional Overview [15] |
| Application Note | AN13023, Selecting and using cryptographic algorithms and protocols [14] |
| Software Development Kit | RW61x SDK with TF-M v1.7 ported [12] |
| Tool User Guidance | Secure Provisioning SDK (SPSDK) Application User Guides [13] |
| Reference Manual | ARM Platform Security Architecture Firmware Framework 1.0 [19] |
| Reference Manual | ARM Firmware Framework for M 1.1 Extensions [20] |
| API Reference Manual | PSA Attestation API 1.0 [21] |
| API Reference Manual | PSA Cryptography API 1.1 [22] |
| API Reference Manual | PSA Storage API 1.0 [23] |

## 1.5 Platform Overview and Description

The RW61x family is a highly integrated, low-power tri-radio Wireless MCU with an integrated MCU and Wi-Fi 6 + Bluetooth Low Energy (LE) 5.3 / 802.15.4[1] radios designed for a broad array of applications. Applications include connected smart home devices, gaming controllers, enterprise and industrial automation, smart accessories, and smart energy.

The RW61x MCU subsystem includes a 260 MHz Arm® Cortex®-M33 core with TrustZone™-M, 1.2 MB on-chip SRAM. The RW61x also includes a Quad SPI interface with high bandwidth, and an on-the-fly decryption engine for securely accessing off-chip XIP flash.

[1] Superset feature, availability depends on product part number ordered

The RW61x includes a full-featured 1x1 dual-band (2.4 GHz / 5 GHz) 20 MHz Wi-Fi 6 (802.11ax) subsystem bringing higher throughput, better network efficiency, lower latency, and improved range over previous generation Wi-Fi standards. The Bluetooth LE radio supports 2 Mbit/s high-speed data rate, long range and extended advertising as well as LE Audio for a better overall audio experience. The on-chip 802.15.4 radio can support Thread mesh networking protocol.[1]

The RW61x is an ideal device for Matter applications running over Wi-Fi, Ethernet and/or Thread. The RW61x can operate as a Matter Controller as well as Thread Border Router.[1] This capability enables full Matter functionality for local and cloud-based control, and for monitoring of IoT products seamlessly across major ecosystems.

EdgeLock™ security technology of NXP is incorporated, offering secure boot, secure debug, secure firmware updates, and secure life cycle management as well as hardware cryptography and Physically Unclonable Function (PUF) for secure key management.

The advanced design of the RW61x delivers tight integration, low power, and highly secure operation in a space- and cost-efficient wireless MCU requiring only a single 3.3 V power supply.

### 1.5.1 Platform Security Features

RW61x employs a security subsystem, EdgeLock System S50 (ELS S50), which together with platform firmware provides the following security features:

- NXP EdgeLock™ Assurance
- NXP EdgeLock 2GO Trust Provisioning
- Trusted execution environment (TEE) based on Arm TrustZone-M
- Hardware root of trust
- Hardware cryptography accelerators (symmetric, asymmetric, secure hash, KDF, etc.)
- True Random Number Generator (TRNG)
- Physically Unclonable Function (PUF)
- OTP-based device configuration and life cycle management
- Secure boot, software update and debug
- On-chip tamper detection for voltage level and glitch, temperature and reset

### 1.5.2 Platform Type

Processor with internal hardware isolation with Arm TrustZone technology, secure memory, and a secure subsystem.

### 1.5.3 Platform Physical Scope

The physical scope is the part of RW61x microcontroller silicon chip as shown in Figure 1.

The hardware components and interfaces are listed in Chapter 1 of [7] and [8].

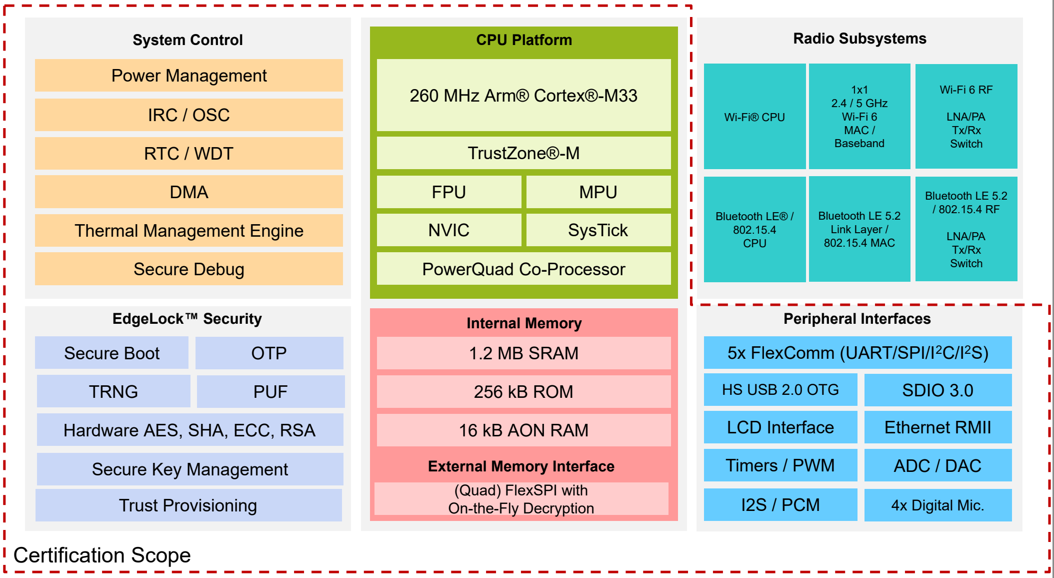

**Figure 1. RW61x Family Superset Block Diagram**

### 1.5.4 Platform Logical Scope

The logical scope includes the ROM firmware, and the optional flash loadable updatable platform root of trust (RoT) as illustrated in Figure 2 and listed in Table 5. Any additional firmware, OS or application software stored on the platform is not in scope of this evaluation.

**Table 5. Platform Deliverables**

| Type | Name | Release | Form of delivery |
|---|---|---|---|
| IC Hardware and ROM Firmware | RW61x | A1, A2 | Silicon Chip and Onchip ROM Firmware |
| ROM Firmware Patch | RW61x ROM Patch | A1: 00120208<br>A2: 00210010 | Onchip Firmware |
| Security Enclave | EdgeLock System S50 (ELS S50) | 2.16.1 | Onchip Hardware Subsystem |
| Security Enclave Software | ELS S50 software (microcode) | 1.02.1 | Onchip ROM Firmware |
| Updatable Platform RoT | RW61x SDK with TF-M v1.7 ported | 2.13.0 EAR4 TF-M Secure Hardened | Software Package |
| Crypto Library | Crypto Library Normal Secure (CLNS) SDK | 1.3.0 | Included in Software Package |

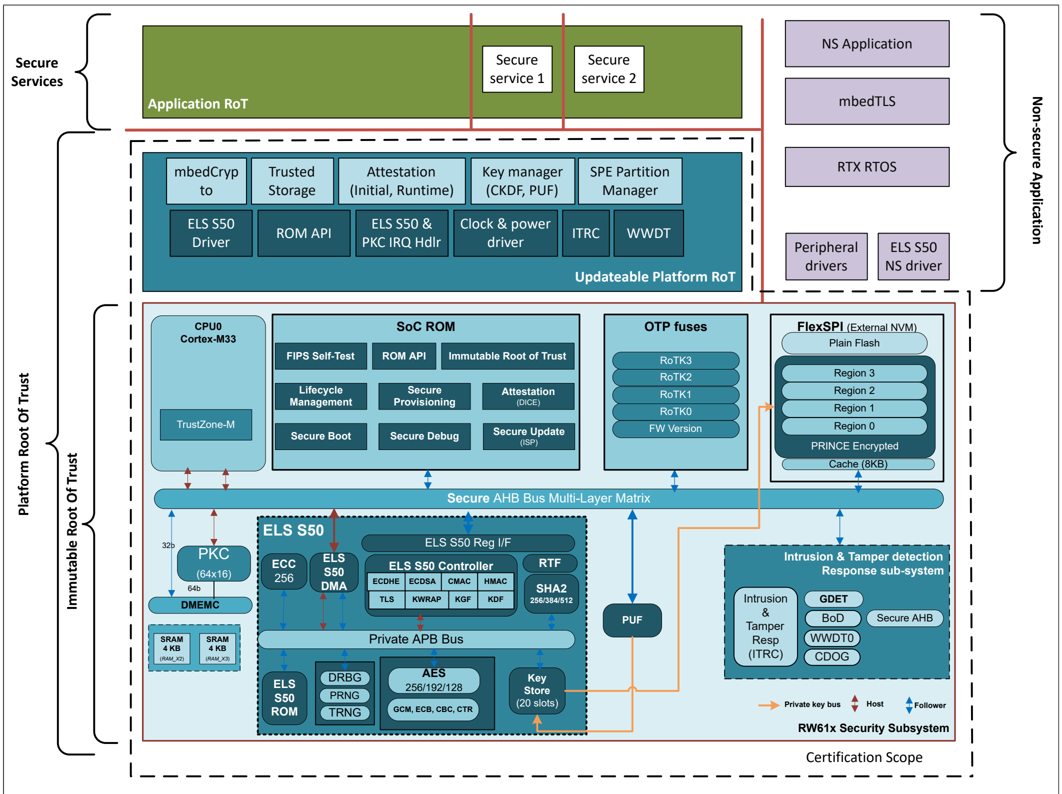

Figure 2. RW61x Logical Architecture and Certification Scope

### 1.5.5 Required Non-Platform Hardware/Software/Firmware

RW61x has no internal flash, hence compatible external non-volatile memory shall be deployed via FlexSPI for image storage with sufficient size. See Chapters 4 of [4] for compatible external flash.

### 1.5.6 Life Cycle

This device supports a security Life-Cycle state model. The current Life-Cycle state determines the device functionality, debug and test port availability, and asset accessibility. The LC_STATE fuse value controls the Life-Cycle state. The state values are selected so that additional fuse bits are burned to advance the state. Because fuses control the Life-Cycle state, moving to a more advanced state is an irreversible and permanent process. The Life-Cycle can only be advanced and cannot return to a previous state.

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

See more in Chapter 12 of [4].

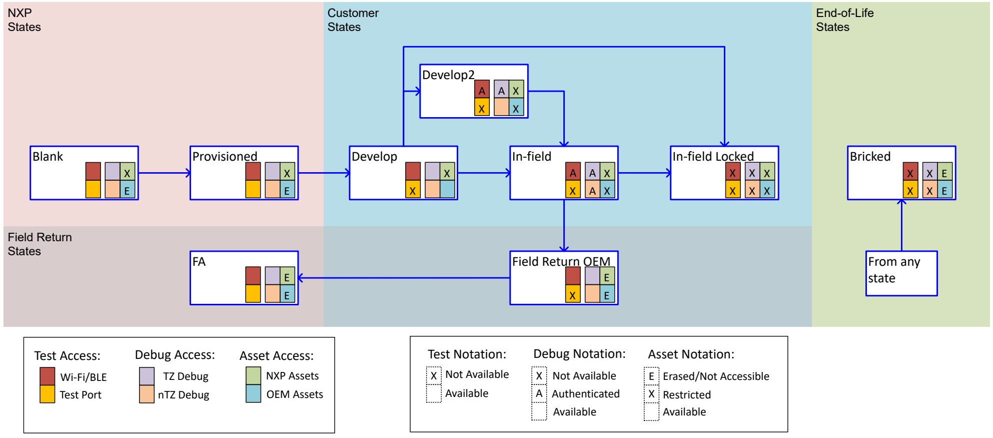

Figure 3. RW61x security Life-Cycle states

## 1.5.7 Configurations

The MCU/MPU ensures the execution of platform trusted code, particularly the functions related to secure boot, updatability, and code isolation.

The security features discussed above are complemented by security services intended to be used by the higher software layers to implement a full-fledged Root of Trust and operating system

A Secure Enclave is used to fulfil the following security features as described in Section 3.2.

## 1.5.8 Use Case

**[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:

Table 6. Platform Objectives for the Operational Environment

| Title | Description | Reference |
|---|---|---|
| Platform Verification | The operating system or application code are expected to verify the correct version of all platform components it depends on, as described in Section 3.4.1.1 of this document. | Section 3.4.1.1 |
| Secure Boot | The operating system or application code are expected to make use of the Secure Boot feature as described in Chapter 10 of [4]. | [10] and Chapter 10 of [4] |
| Secure Debug | The integrating environment is expected to configure the debug functionality as described in Chapter 13.7 of [4]. and [11] to meet the extra physical attacker resistance. | [11] and Chapter 13.7 of [4] |
| Key Management | Cryptographic keys and certificates outside of the Platform are subject to secure key management procedures. | This document |
| Trusted Users | Actors in charge of platform management, for instance for signature of firmware update, are trusted. | This document |
| SW Integration | The operating system or application code are expected to ensure the correct version of the crypto library and SDK drivers are integrated and configured. | This document |
| Secure Update and Key Revoke | The operating system or application code are expected to update an image with proper remedy solution and version increased and/or revoke key in case of security incidence occurrence of the image and/or the key. | Chapter 10 of [4] |
| Lifecycle Management | RW61x provides 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 In-field or in-field locked state. | Chapter 12 of [4] |
| Software Isolation | RW61x provides majorly two different isolation mechanisms: S50 vs rest of SoC, and TF-M SPE vs NSPE based on Trust Zone technology. The operating system or application code are expected to configure and utilize these mechanisms for isolation between platform and application. | Chapters 14 and 16 of [5], [19] |
| Memory Encryption | RW61x supports both CTR and GCM modes for PRINCE external memory encryption. If memory integrity, authenticity, and/or physical attacker resistance are in demand for the use cases, the operating system or application code are expected to configure the PRINCE to GCM mode. | Chapters 4.2.11 of of [4], and Chapter 12 of [5] |
| Physical Attacker Resistance Configurations | If local physical attack is applicable for the use cases, the following configurations shall be kept after boot by the operating system or application code:<br>• ITRC settings<br>• FIH and CDOG configurations in TF-M | Chapter 13 of [5], [12] |

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

### 3.1.1 Flaw Reporting Procedures (ALC_FLR.2)

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

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

- **Reporting**. The process begins when the PSIRT becomes aware of a potential security vulnerability in an NXP product. The reporter receives an acknowledgment and updates throughout the handling process.
- **Evaluation**. The PSIRT confirms the potential vulnerability, assesses the risk, determines the impact and assigns a processing priority. If the vulnerability is confirmed, the priority determines how the issue is handled throughout the remaining steps in the process.
- **Solution**. Working with PSIRT, the product team develops a solution that mitigates the reported security vulnerability. Solutions will take different forms based on the vulnerability. Because of the nature of NXP products – mostly silicon products where the firmware is in ROM -, very often the solution can only be provided in a next version of the chips and the short-term solution will consist of recommending security measures to be applied in systems using the NXP product.
- **Communication**. As said above, because of the nature of the NXP products, the solution to systems using the affected products often needs to be found in additional countermeasures in those systems. The communication on the vulnerability and solutions will in most cases be done directly towards the affected customers. For previously unknown or unreported issues, NXP will acknowledge the reporter of the issues (unless the reporter requests otherwise).

The platform's Secure Boot feature is able to verify the authenticity of customer code during the initial boot and outside of the boot sequence, providing an appropriate mechanism for supporting the update of this code. The update mechanism is also supported in the loadable firmware of TF-M. See Section 3.4.2.1 for further information.

## 3.2 Security Process Packages (SPPs)

This package is extended from SESIP draft version to the CEN Enquiry (prEN 17927:2022) by CEN/JTC 13.

### 3.2.1 Trust provisioning

A trust provisioning process ensures the secure management in a trusted environment of *assets in Table 7* and its/their loading into the platform for the following use cases *in Table 7* as specified in *reference in Table 7*.

Both the trusted environment and the platform protect the *access, confidentiality, integrity* of provisioned data.

**Table 7. Trust provisioning**

| Assets | Use Case | Reference |
|---|---|---|
| Cryptographic Keys | OEM Secure Provisioning | [15] |
| Cryptographic Keys | EdgeLock 2GO | [15] |
| Customer Data | Customer Customized Provisioning by NXP | [15] |

**Conformance rationale:**

Trust Provisioning (TP) describes the process of establishing a trust anchor in NXP devices that can be used by customers. This trust anchor could be a cryptographic key (or a set of keys), a unique identifier, or customer specific content. See more in [15], Section 3.4.2.1 and Section 3.4.4.2.

## 3.3 Security Functional Requirements for Security Enclave

RW61x employ a security enclave: EdgeLock System S50 (ELS S50), which fulfills the following security functional requirements:

### 3.3.1 Identification and Attestation of Platforms and Applications

#### 3.3.1.1 Verification of Platform Identity

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

**Conformance rationale:**

The ELS S50 version is available from `ELS_VERSION`. The values shall match the versions indicated in Table 5. See more in Chapter 16.5.19 of [5].

### 3.3.2 Extra Attacker Resistance

#### 3.3.2.1 Software Attacker Resistance: Isolation of Platform Parts

The platform provides isolation between platform parts, such that an attacker able to run code *in the platform parts outside of the Secure Enclave* can compromise neither the integrity and confidentiality of *the Secure Enclave* nor the provision of any other Security Functional Requirements.

**Conformance rationale:**

The ELS S50 module is a security subsystem supporting a wide range of cryptographic algorithms and providing strong key isolation from the rest of the system. When embedded in an SoC, ELS S50 serves as the main building block of the SoC's immutable Root of Trust. It is used as part of the trust anchor during secure boot, secure debug access, life-cycle management, and trust provisioning.

ELS S50 has its own controller and exclusive system resources with enforced access control, hence it is isolated from the rest of platform. See more in Chapter 16 of [5].

### 3.3.3 Cryptographic Functionality

#### 3.3.3.1 Cryptographic Operation

The platform provides the application with *operations in Table 8* functionality with *algorithms in Table 8* as specified in *specifications in Table 8* for key lengths *described in Table 8* and modes *described in Table 8*.

**Table 8. Cryptographic Operations by ELS S50**

| Operation | Algorithm | Specification | Key Lengths | Modes |
|---|---|---|---|---|
| Encryption and decryption | AES | NIST FIPS 197 | 128, 192, 256 [1][2] | ECB, CBC, CTR |
| Authenticated encryption, authenticated decryption | AES | NIST SP 800-38d | 128, 192, 256 [1][2] | GCM |
| Hashing | SHA2 | NIST FIPS 180-4 | 224, 256, 384, 512 | - |
| MAC generation and verification | HMAC | RFC2104 | Up to 512 [1][3] | SHA-256 |
| MAC generation and verification | CMAC | RFC4493 | 128, 256 [1][2] | AES |
| Signature generation and verification | ECDSA | NIST FIPS 186-5 | 256 | secp256r1 |

[1] All key lengths supported by key stored in memory outside of ELS S50.
[2] ELS S50 keystore available for 128- and 256-bit keys.
[3] ELS S50 keystore available for 256-bit keys.

**Conformance rationale:**

The crypto coprocessors are located in ELS S50. ELS S50 provides the symmetric, hashing, and more functions. See more in Chapter 16 of [5]..

#### 3.3.3.2 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in *algorithms in Table 9* as specified in *specifications in Table 9* for key lengths *described in Table 9*

**Table 9. Cryptographic Key Generation**

| ID | Algorithm | Specification | Key Lengths |
|---|---|---|---|
| ECC | ECC | ANSI X9.62 | 256 |
| HKDF | HKDF | RFC5869 | 128, 256 |
| CKDF | CKDF | NIST 800-108 | 128, 256 |
| TLS KDF | TLS Master Key Derivation | TLS1.2 | - |
| TLS KDF | TLS Session Key Derivation | TLS1.2 | - |
| ECDH | ECDH | NIST SP 800-56A | 256 |

**Conformance rationale:**

The ELS S50 also provides key generation service. See more in Chapter 16.5.2 of [5].

#### 3.3.3.3 Cryptographic KeyStore

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

**Conformance rationale:**

ELS S50 provides key store function. Keys can be stored in ELS in a bank of internal 128-bit registers (each register is called a "key slot"). Specifically, their values (the key material) cannot be accessed by the system. Keys in KeyStore can be created by key exchange and key derivation functions in Section 3.3.3.1, key generation function in Section 3.3.3.2, unwrapping external RFC3394 wrapped key, or imported from unique key derivated from PUF. Each Keystore Key has associated properties and ELS S50 enforces usage rules based on the properties of keys. See more in Chapter 16.5.16 of [5].

#### 3.3.3.4 Cryptographic Random Number Generation

The platform provides the application with a way based on *physical noise and DRBG* to generate random numbers to as specified in *NIST.SP.800-90B and NIST.SP.800-90A CTR-DRBG with AES-128*.

**Conformance rationale:**

ELS S50 has physical true random number generator and internal DRBG module as defined in NIST SP 800-90A. The TRNG archives NIST SP 800-90B compliance.

Furthermore:

- TRNG is capable to pass AIS 31 statistical tests T0-T8

See more in Chapters 16.5.6 of [5].

### 3.3.4 Compliance Functionality

#### 3.3.4.1 Residual Information Purging

The platform ensures that *key store areas*, with the exception of *none*, is erased using the method specified in *Chapter 16.5.2.9 of [5]* before the memory is (re)used by the platform or application again and before an attacker can access it.

**Conformance rationale:**

ELS S50 provide KDELETE command which removes the key and zeroize the register. See more in Chapter 16.5.2.9 of [5].

## 3.4 Security Functional Requirements for SoC

In the following Security Functional Requirements, the term **platform** covers the **RW61x physical and logical scope**, and the term **application** refer to any additional firmware, OS or application software which is out of evaluation scope. It represents a part of the final connected device.

RW61x fulfils the following security functional requirements:

## 3.4.1 Identification and Attestation of Platforms and Applications

### 3.4.1.1 Verification of Platform Identity

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

**Conformance rationale:**

Besides reading out ELS S50 HW and driver version as introduced in Section 3.3.1.1, SoC Hardware and ROM identifier and revision number can be read from `CHIP_INFO` register and one way to do so is to use `GetProperty` command in ISP mode as specified in Section 8.5.2 and 8.5.16 of [4] with tag `10h`. The return value shall match to the value in Chapter 71.1.30 of [6] and the version shall match the value indicated in Section 1.5.4.

The ROM patch revision is stored in OTP fuse index `359`, which can be read via ISP mode or ROM API, and the return value shall be the same as Section 1.5.4. See more in Sections 8.5.12 and 9.2.4 of [4].

The Updatable Platform RoT Firmware including TF-M ported are delivered in logical format as a software library. One can identified the version in readme file and verify the commit hash as defined in Section 1.5.4.

### 3.4.1.2 Verification of Platform Instance Identity

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

**Conformance rationale:**

The platform stores a 128-bit IETF RFC4122 compliant non-sequential Universally Unique Identifier (UUID). It can be read from the fuseword `46` onwards. Refer to Chapter 10.2.4.1 of [4].. One way to read out UUID is to use `GetProperty` command in ISP mode with tag `12h` as specified in Chapter 8.5.2 and 8.5.16 of [4]..

### 3.4.1.3 Attestation of Platform Genuineness

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

**Conformance rationale:**

RW61x with TF-M Ported also supports the PSA attestation API to produce an initial attestation token in IETF EAT format containing measurements of the firmware, which provides an attestation service which reports on the device identity, firmware measurements and runtime state of the device. The attestation can be verified by remote entities. The tokens are signed using attestation keys stored in the internal flash. See more in [19] and [21].

### 3.4.1.4 Attestation of Platform State

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

**Conformance rationale:**

See Section 3.4.1.3.

#### 3.4.1.5 Secure Initialization of Platform

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

**Conformance rationale:**

The secure part of the ROM bootloader of RW61x provides secure boot operation.

Secure boot prevents unauthorized code from being executed on a given product. To ensure this level of security, secure boot always leaves the device ROM in an executing mode when coming out of a reset. The ROM can then assess the first user executable image resident in the external flash memory and determine the authenticity of that code. The control is transferred to authentic code only. A chain of trusted code from the ROM to the user boot code is established. And the chain can be further extended through the verification of digital signatures associated with additional code layers.

The Elliptic Curve Digital Signature Algorithm (ECDSA) is used in this architecture to verify the authenticity of the boot code. The boot code is always signed with ECDSA private keys, either based on P-256 or P-384. The corresponding ECDSA public keys used for signature verification (Root of Trust Keys) are contained in the certificate block included in the signed image. Support is provided for up to four Root of Trust keys.

The operating system or application code have the option to further enable built-in self-tests in Secure Boot ROM to ease the certification of NIST CMVP.

See more in Chapter 10 of [4]..

### 3.4.2 Product Lifecycle: Factory Reset / Install / Update / Decommission

#### 3.4.2.1 Secure Update of Platform

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

**Conformance rationale:**

The secure part of the ROM bootloader of RW61x provides secure firmware update operation.

Secure firmware updates perform an authentication of the new firmware prior to committing it to the memory. In this case, the chain of trust is extended from the old, currently executing code, to the new code.

Another use case for secure firmware update is to hide the application binary code during transit over public media such as the web. For this use case, the firmware update image is encrypted. As the new firmware is written into the device memory, it is decrypted.

In this architecture, both cases of secure firmware update are supported. The SB file format is encrypted and digitally signed. The SB file can be loaded via interfaces such as USB, and UART. Or the SB file can be provided to the ROM API as a complete binary file.

The anti-rollback is achieved by OTP fuseword. The OTP fusemap contains monotonic counters or ROTKH revocation fields that can be updated as these are implemented as redundant 16-bit fusewords. See more in Chapter 10 of [4]..

Furthermore, trust provisioned private key, together with other pre-installed key material, is then used for authentication and secure connection to the device, enabling secure provisioning of OEM assets even in the manufacturing environment OEM may not fully trust. See more in Sections 3.8.3, 4.1 and 4.2.2 of [15], and Section 3.2.1.

NXP further offers services to securely provision customer's data, keys and/or firmware in NXP trust provision process during product manufacture, and advance device life cycle state if needed. The customer data is unknown for this evaluation, hence it is out of scope. See more in Section 3.8.1 of [15], and Section 3.2.1.

#### 3.4.2.2 Field Return of Platform

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

**Conformance rationale:**

The ROM on this device has an FA mode command (`SET_FA_MODE`). The command disables sensitive information (for example, rekeying of keys) before giving the device to OEM factory for fault analysis. The ROM allows the `SET_FA_MODE` command only when a corresponding flag in Debug_State is set. Upon receiving the command ROM will program OTP fuseword (45) to set LifeCycle to Field Return OEM (`0x1F`) and triggers a sw reset.

The FA_MODE sequence when activated by the boot ROM is:

1. Put PUF and ELS modules in FA mode.

2. Rekeys all the application usage keys including the memory encryption IPED keys.

3. Open all debug ports.

4. Enter while(1) loop.

This mechanism protects leakage of any residue data left during life-cycle state transition. It can further move to FA life cycle state if the device is being returned to NXP for testing and failure analysis, and further sensitive information is erased, and that is equivalent that all information protected by the application usage key is purged. See more in Chapters 12.6 and 13.7.6 of [4]..

#### 3.4.2.3 Decommission of Platform

The platform can be decommissioned.

**Conformance rationale:**

RW61x provides Bricked End-of-Life security life-cycle state. Customers or NXP can use this state to remove a device from regular use, and erase or block the access to secret information inside the device.

The Bricked state is the end-of-life state for the device, when a part is removed permanently from service. In this mode, the ROM locks up the device immediately on any reset. The debug and test mode ports are also disabled.

Bricked is the final life-cycle state. The device cannot be advanced to any other state from Bricked. Also all the keys stored in ELS S50, PUF derived data including die unique keys and the memory encryption IPED keys are permanently destroyed, hence the PUF derived data and IPED protected memory is equivalent to be purged. See more in Chapter 12.7 in [4]..

### 3.4.3 Extra Attacker Resistance

#### 3.4.3.1 Physical Attack Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the functional requirements, ensuring that the functional requirements are not compromised.

**Conformance rationale:**

RW61x is equipped with Intrusion and Tamper Response Controller (ITRC). ITRC provides mechanism to configure the response action for an intrusion event detected by on-chip security sensors. Intrusion Response is the action a device performs in order to prevent misuse of the device or disclosure of critical assets (cryptographic keys, personal data) that are generated or stored within the device. The response mechanism is typically triggered by either a signal from an on-chip sensor designed to detect that the device is in a threat condition or by an explicit command provided by the software. See more in Chapter 13 of [5].

Also, the software components including ROM and TF-M ported leverage the code watchdog. For code watchdog, see more in Chapter 15 of [5]. The crypto coprocessor and the library are secure hardened against potential physical attacks. The TF-M ported further enables Fault Injection Hardening (FIH) library in the HIGH profile.

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

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

**Conformance rationale:**

There are multiple isolation features presented in the platform.

The ELS S50 isolation has been introduced in Section 3.3.

PRINCE-based memory encryption also ensures Secure Isolation between multiple IP vendors. Initial Vector (IV) is derived by secure-privilege and a different value is used for every independent memory region, ensuring the isolation between each other. See more in Chapters 7.3 and 7.4 of [4].

ARM TrustZone enables Secure Isolation during run-time by providing four distinct levels of privilege: secure-privilege, secure-user, non-secure-privilege, non-secure-user. Every peripheral is equipped with Peripheral Protection Checker (PPC) that can be programmed to control access to that peripheral, following the ARM TrustZone philosophy. Every memory is equipped with Memory Protection Checker (MPC) that can also be programmed in the same way as the PPC. Secure AHB Controller is in charge of programming all PPC and MPC blocks and only the highest level of privilege, which is secure-privilege, is allowed to do that. See more in Chapter 14 of [5]. PSA Level 2 Isolation supported by TF-M SPM using TrustZone and Secure MPU on v8-M cores [19].

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

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

**Conformance rationale:**

The isolation between PSA-RoT and Application Root of Trust Services is included in Section 3.4.3.2.

Also see more in Section 3.4.4.4 about key isolation.

#### 3.4.3.4 Software Attacker Resistance: Isolation of Platform Parts

See Section 3.3.2.1.

### 3.4.4 Cryptographic Functionality

#### 3.4.4.1 Cryptographic Operation

The platform provides the application with *operations in Table 8 and Table 10* functionality with *algorithms in Table 8 and Table 10* as specified in *specifications in Table 8 and Table 10* for key lengths *described in Table 8 and Table 10* and modes *described in Table 8 and Table 10*.

Table 10. Cryptographic Operations provided outside of ELS S50

| Operation | Algorithm | Specification | Key Lengths | Modes |
|---|---|---|---|---|
| Signature generation and verification | EdDSA | NIST FIPS 186-5 | 255 | Ed25519 |
| Signature generation and verification | ECDSA | NIST FIPS 186-5 | 192, 224, 256, 384, 521 | secpXXXr1, XXX = key length |
| | | | 192, 224, 256 | secpYYYk1, YYY = key length |
| | | | 160[1], 192, 224, 256, 320, 384, 512 | brainpoolPZZZr1, ZZZ = key length |
| Signature generation and verification | RSA | PKCS v1.15 and RSA PSS | 2048, 3072, 4096 | - |

[1] Refer to [14] for considerations on algorithm and key lengths.

**Conformance rationale:**

On top of ELS S50 security coprocessor introduced in Section 3.3.3.3, RW61x also deploys Public-Key Crypto Coprocessor (PKC, Chapter 18 of [5]). Crypto Library has been developed leveraging ELS S50 and PKC [9]. Part of supported algorithms are further enabled in the TF-M ported [22].

#### 3.4.4.2 Cryptographic Operation (with provisioned key)

The platform provides the application with *operations in Table 11* functionality with *algorithms in Table 11* as specified in *specifications in Table 11* for key lengths *described in Table 11* and modes *described in Table 11*.

Table 11. Cryptographic Operations

| Operation | Algorithm | Specification | Key Lengths | Modes |
|---|---|---|---|---|
| Signature Generation | ECDSA | ANSI X9.62 | 256 | NIST P-256 |

Table 11. Cryptographic Operations*...continued*

| Operation | Algorithm | Specification | Key Lengths | Modes |
|---|---|---|---|---|
| Key unwrapping | AES | RFC3394 | 256 | - |

**Conformance rationale:**

The trust provisioning service also provide provision for EdgeLock 2GO root-of-trust keys, hence their cryptographic operations are available to the platform which can enable secure communication establishment with EdgeLock 2GO infrastructure and hence EdgeLock 2GO Services. See more in Section 4.6 of [15] and Section 3.2.1.

### 3.4.4.3 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in *algorithms in Table 9 and Table 12* as specified in *specifications in Table 9 and Table 12* for key lengths *described in Table 9 and Table 12*.

Table 12. Cryptographic Key Generation

| ID | Algorithm | Specification | Key Lengths |
|---|---|---|---|
| AES | AES | NIST SP800-133 | 128, 192, 256 |
| ECC | ECC | ANSI X9.62 | 160, 192, 224, 255, 256, 320, 384, 512, 521 |
| RSA | RSA | PKCS#1 | 2048, 3072, 4096 |
| ECDH | ECDH | NIST SP 800-56A | 255 (Curve25519), 448 (Curve448) |
| | | | 192, 224, 256, 384, 521 (secpXXXr1, XXX = key length) |
| | | | 192, 224, 256 (secpYYYk1, YYY = key length) |
| | | | 160[1], 192, 224, 256, 320, 384, 512 (brainpoolPZZZr1, ZZZ = key length) |

[1] Refer to [14] for considerations on algorithm and key lengths.

**Conformance rationale:**

The crypto library also provides key generation service leveraging the coprocessors. On top of the crypto library, the TF-M ported further provides APIs for key generation.

### 3.4.4.4 Cryptographic KeyStore

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

**Conformance rationale:**

ELS S50 keystore is introduced in Section 3.3.3.3. Also, PSA Crypto API including Key Handling is supported in TF-M ported.

#### 3.4.4.5 Cryptographic Random Number Generation

The platform provides the application with a way based on *physical noise and DRBG* to generate random numbers to as specified in *NIST.SP.800-90B and NIST.SP.800-90A CTR-DRBG with AES-128*.

The platform provides the application with a way based on *physical noise and DRBG* to generate random numbers to as specified in *NIST.SP.800-90B and NIST.SP.800-90A CTR-DRBG with AES-256*.

**Conformance rationale:**

There are two RNG instances in RW61x. One locates inside ELS S50 as stated in Section 3.3.3.4. The other RNG together with Crypto Library further provides random numbers at 256-bit security level.

### 3.4.5 Compliance Functionality

#### 3.4.5.1 Secure External Storage

The platform ensures that all data stored outside the direct control of the platform, except for *data not stored in the configured address area,* is protected such that the *authenticity, integrity, confidentiality and binding to platform instance* is ensured.

**Conformance rationale:**

External flash storage can also be encrypted by PRINCE algorithm GCM mode using IPED engine to achieve authenticity and confidentiality (see more in Chapter 12 in [5], and Chapters 7.3 and 7.4 of [4].. The key is stored in ELS S50 and derived from PUF which also provides binding to platform instance. See more in Chapter 10.9.3 of [4].. Also PSA storage API is supported by TF-M ported [23].

#### 3.4.5.2 Secure Debugging

The platform only provides *Arm's Serial Wire Debug (SWD) interface* authenticated as specified in *Chapter 13.7 of [4].* with debug functionality.

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

**Conformance rationale:**

The fundamental principles of debugging, which require access to the system state and system information, conflict with the principles of security, which require the restriction of access to assets. Thus, many products disable debug access completely before deploying the product. This causes challenges for product design teams to do proper Return Material Analysis (RMA). To address these challenges, the chip offers a debug authentication protocol as a mechanism to authenticate the debugger (an external entity) has the credentials approved by the product manufacturer before granting debug access to the device.

The debug authentication is a challenge-response scheme and assures that only the debugger in possession of the required debug credentials can successfully authenticate over the debug interface and access restricted parts of the device. Furthermore, the debug subsystem is sub-divided into multiple debug domains to allow finer access control.

See more in Chapter 13.7 of [4]. and [11].

#### 3.4.5.3 Residual Information Purging

The platform ensures that *key store areas*, with the exception of *none*, is erased using the method specified in *Chapter 16.5.2.9 of [5]* before the memory is (re)used by the platform or application again and before an attacker can access it.

The platform ensures that *PUF derived data, ELS stored keys and IPED protected memory*, with the exception of *none*, is erased using the method specified in *Section 12.6 and 12.7 of [4]* before the memory is (re)used by the platform or application again and before an attacker can access it.

**Conformance rationale:**

The keystore erase in ELS S50 is introduced in Section 3.3.4.1.

Entering the FA Mode or Bulk Erase Flash purges sensitive data. See more in Section 3.4.2.2 and Section 3.4.2.3.

#### 3.4.5.4 Reliable Index

The platform implements a strictly increasing function.

**Conformance rationale:**

RW61x provides fuses for customer definition and usage which can be used as reliable index due to the irreversible nature. The fuse programming and readout is achieved by ROM API. See more in Section 9.2.4 of [4].

# 4 Mapping and Sufficiency Rationales

## 4.1 SESIP3 Sufficiency

| Assurance Class | Assurance Family | Covered By | Rationale |
|---|---|---|---|
| ASE: Security target evaluation | ASE_INT.1 ST Introduction | Section 1 | The ST reference is in Section 1.1, the TOE reference in Section 1.3, the TOE overview and description in Section 1.5. |
| | 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 | Security Requirements and Implementation | All SFRs in this ST are taken from [1]. SFR "Identification of Platform Type" is included. SFR "Secure Update of Platform" is mentioned but refers to ALC_FLR.2. |
| | ASE_TSS.1 TOE Summary Specification | Security Requirements and Implementation | 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 specifications | Material provided to evaluator. | The evaluator will determine whether the provided evidence 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. | The evaluator will determine whether the provided evidence is suitable to meet the requirement. |
| AGD: Guidance documents | AGD_OPE.1 Operational user guidance | Section 1.4 | The evaluator will determine whether the provided evidence is suitable to meet the requirement. |
| | AGD_PRE.1 Preparative procedures | Section 1.4 | The evaluator will determine whether the provided evidence is suitable to meet the requirement. |
| ALC: Life-cycle support | ALC_CMC.1 Labelling of the TOE | Material provided to evaluator. | The evaluator will determine whether the provided evidence is suitable to meet the requirement. |
| | ALC_CMS.1 TOE CM Coverage | Material provided to evaluator. | The evaluator will determine whether the provided evidence is suitable to meet the requirement. |

| Assurance Class | Assurance Family | Covered By | Rationale |
|---|---|---|---|
| | ALC_FLR.2 Flaw reporting procedures | Section 3.1.1 | The flaw reporting and remediation procedure is described. |
| ATE: Test | ATE_IND.1 Independent testing: conformance | Material provided to evaluator. | The evaluator will determine whether the provided evidence is suitable to meet the requirement. |
| AVA: Vulnerability assessment | AVA_VAN.3 Focused vulnerability analysis | N.A.<br>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 Enhanced-Basic. |

## 4.2 Conformance Mapping for SESIP Profile for Secure MCUs and MPUs

This section provides rationales of conformance claimed in Section 1.2

Table 13. SESIP Profile for Secure MCUs and MPUs Sufficiency

| Package Claimed | Security Functional Requirements | Covered By |
|---|---|---|
| Base | Verification of Platform Identity | Section 3.4.1.1 |
| | Secure Initialization of Platform | Section 3.4.1.5 |
| | Secure Updated of Platform | Section 3.4.2.1 |
| | Residual Information Purging | Section 3.4.5.3 |
| | Secure Debugging | Section 3.4.5.2 |
| Security Services | Cryptographic Operation | Section 3.4.4.1 |
| | Cryptographic Key Generation | Section 3.4.4.3 |
| | Cryptographic KeyStore | Section 3.4.4.4 |
| | Cryptographic Random Number Generation | Section 3.4.4.5 |
| Software Isolation | Software Attacker Resistance: Isolation of Platform | Section 3.4.3.2,<br>Section 3.4.3.3 |
| Hardware Protections | Physical Attacker Resistance | Section 3.4.3.1 |
| Secure Enclave | Software Attacker Resistance: Isolation of Platform Parts, and<br>SFRs per Section 3.3 | Section 3.3.2.1,<br>Section 3.3 |
| Additional Security Functional Requirements (Optional) | Verification of Platform Instance Identity<br>Attestation of Platform Genuineness<br>Attestation of Platform State<br>Decommission of Platform<br>Field Return of Platform<br>Secure External Storage | Section 3.4.1.2<br>Section 3.4.1.3<br>Section 3.4.1.4<br>Section 3.4.2.3<br>Section 3.4.2.2<br>Section 3.4.5.1 |

## 4.3 Conformance Mapping for SESIP Profile for PSA Certified Level 3

This section provides rationales of conformance claimed in Section 1.2

Table 14. SESIP Profile for PSA Certified Level 3 Sufficiency

| Package Claimed | Security Functional Requirements | Covered By |
|---|---|---|
| Base | Verification of Platform Identity | Section 3.4.1.1 |
| | Verification of Platform Instance Identity | Section 3.4.1.2 |
| | Attestation of Platform Genuineness | Section 3.4.1.3 |
| | Secure Initialization of Platform | Section 3.4.1.5 |
| | Attestation of Platform State | Section 3.4.1.4 |
| | Secure Updated of Platform | Section 3.4.2.1 |
| | Physical Attacker Resistance | Section 3.4.3.1 |
| | Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) | Section 3.4.3.2 |
| | Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) | Section 3.4.3.3 |
| | Cryptographic Operation | Section 3.4.4.1 |
| | Cryptographic Key Generation | Section 3.4.4.3 |
| | Cryptographic KeyStore | Section 3.4.4.4 |
| | Cryptographic Random Number Generation | Section 3.4.4.5 |
| Optional SFR | Secure Debugging | Section 3.4.5.2 |
| | Secure External Storage | Section 3.4.5.1 |

# 5 Appendix

## 5.1 ETSI EN 303 645 Mapping and Sufficiency

ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements [16] is released by European Telecommunications Standard Institute (ETSI), and as its title suggests, it intends to prepare consumer IoT devices with a set of baseline requirements to address common cybersecurity threats. SESIP methodology is acknowledged as one of the schemes that aligning with EN 303 645.[2] GlobalPlatform also released a white paper on SESIP Applicability for EN 303 645 [17]. Yet at the time of writing, there is no recognized SESIP mapping to EN 303 645 released, hence NXP provides the following informative mapping and self-assessment towards EN 303 645 sufficiency rational from this evaluation. The mapping and rational is provided under each EN 303 645 provision entry, and for complete requirements by EN 303 645 provision, please refer to original text of [16].

This section refers to the claims and activities within this SESIP evaluation scope to demonstrate the sufficiency by SESIP methodology. Note EN 303 645 is targeting for consumer IoT device with full software stack mounted and physically designed, and connection to network-based services. The full software stack includes the operating system, communication stack and protocol, and/or application code, which is designed and owned by NXP (direct and indirect) customers, i.e. OEMs and the network service providers. So not all requirements are directly applicable to NXP product scope but more to OEMs and the network service providers. Thus, rationale on how RW61x can support customers to meet EN 303 645 requirements are provided.

**Table 15. EN 303 645 Mapping and Sufficiency**

| EN 303 645 Provisions | Covered/ Supported by | Rationale |
|---|---|---|
| 5.1-1 Unique device password | ADV: Development;<br>AVA: Vulnerability assessment | Password feature shall be implemented by the operating system or application code.<br>Yet, a default or other easy to manipulate password at hardware and firmware level can render security of operating system or application. This evaluation provides full software source code access to evaluator for vulnerability assessment, and it assures there is no such attack path identified within the evaluation scope and attack potential |
| 5.1-2 Password diversification | Verification of Platform Instance Identity | Password feature shall be implemented by the operating system or application code.<br>The OEM can leverage platform instance identity for unique per device password diversification. |
| 5.1-3 Cryptography for user authentication | Cryptographic Functionality | User authentication feature shall be implemented by the operating system or application code.<br>RW61x provides cryptographic operations and secure storage which can be leveraged to fulfil this requirement. |
| 5.1-4 Change of authentication value | - | User authentication feature shall be implemented by the operating system or application code. |

[2] See more in https://www.etsi.org/technologies/consumer-iot-security

Table 15. EN 303 645 Mapping and Sufficiency*...continued*

| EN 303 645 Provisions | Covered/ Supported by | Rationale |
|---|---|---|
| 5.1-5 Authentication mechanism attack resilience | | |
| 5.2-1 Vulnerability disclosure policy | Flaw Reporting Procedures | Final product vulnerability disclosure policy shall be owned by OEMs.<br>For NXP product, the NXP Product Security Incident Response Team (PSIRT) is committed to rapidly address security vulnerabilities in NXP products by responding and documenting reported vulnerabilities and by providing customers with clear guidance on the impact, severity and mitigation. |
| 5.2-2 Timely response | | |
| 5.2-3 Vulnerability monitoring | | |
| 5.3-1 Secure Updatability | Secure Update of Platform | RW61x provides secure update capabilities. |
| 5.3-2 Secure installation of updates | | |
| 5.3-3 Ease for update | AGD: Guidance document | Guidance document for secure update of platform is part of SESIP evaluation. |
| 5.3-4 Automatic update | Secure Update of Platform;<br>AGD: Guidance document | Final product update mechanism shall be implemented by the operating system or application code.<br>RW61x provides guidance document and corresponding tool chain for ease of use for OEM. |
| 5.3-5 Check for update | - | Final product update mechanism shall be implemented by the operating system or application code. |
| 5.3-6 Configurability for update | | |
| 5.3-7 Cryptography for update | Secure Update of Platform;<br>Cryptographic Functionality | RW61x secure update feature employs best practice cryptography.<br>RW61x provides cryptographic operations and secure storage for operating system or application code to implement other secure update mechanisms. |
| 5.3-8 Timely update | Flaw Reporting Procedures | Final product security update shall be owned by OEMs.<br>For NXP product, the NXP Product Security Incident Response Team (PSIRT) is committed to rapidly address security vulnerabilities in NXP products by responding and documenting reported vulnerabilities and by providing customers with clear guidance on the impact, severity and mitigation. |
| 5.3-9 Authenticity and Integrity of software update | Secure Update of Platform;<br>Cryptographic Functionality | RW61x secure update feature ensures authenticity and integrity.<br>RW61x provides cryptographic operations and secure storage for operating system or application code to implement other secure update mechanisms.<br>Final product update mechanism shall be implemented by the operating system or application code. |
| 5.3-10 Trust relationship for updates | | |

Table 15. EN 303 645 Mapping and Sufficiency*...continued*

| EN 303 645 Provisions | Covered/ Supported by | Rationale |
|---|---|---|
| 5.3-11 Security update communication | Flaw Reporting Procedures | Final product security update shall be owned by OEMs.<br>For NXP product, the NXP Product Security Incident Response Team (PSIRT) is committed to rapidly address security vulnerabilities in NXP products by responding and documenting reported vulnerabilities and by providing customers with clear guidance on the impact, severity and mitigation. |
| 5.3-12 Update notification | - | Final product update mechanism shall be implemented by the operating system or application code. |
| 5.3-13 Defined support period | - | Support period of final product shall be defined by OEM.<br>For RW61x, this requirement is not covered by SESIP evaluation, yet NXP provides Product Longevity program where RW61x will be included. |
| 5.3-14 Communication for constrained device | - | Final device updatability, end user communication and mitigation shall be defined by OEM |
| 5.3-15 Isolatability and replaceability for constrained device | | |
| 5.3-16 Model recognizability | Verification of Platform Identity | Final product model designation shall be defined by OEM.<br>SESIP methodology mandates unique identification of the platform under evaluation, RW61x conformance rational is provided. |
| 5.4-1 Security parameter storage | Isolation of Platform Parts; Isolation of Platform (between SPE and NSPE); Secure External Storage | RW61x provides multiple security mechanism including TEE, secure enclave and secure external storage to support operating system or application code to fulfil this provision requirement. |
| 5.4-2 Tamper resistance of hard-coded identity | Verification of Platform Instance Identity ; Extra Attacker Resistance | Platform instance identity is unique per device and OTP based which can be used for security purposes.<br>SESIP includes remote attack surface by default and RW61x provides extra attacker resistance including physical attacker resistance. |
| 5.4-3 No hard-coded security parameters in software | ADV: Development; AVA: Vulnerability assessment | This evaluation provides full software source code access to evaluator for vulnerability assessment, and it assures that there is no hard-coded security parameter which leads to attack path within the attack potential. |

Table 15. EN 303 645 Mapping and Sufficiency*...continued*

| EN 303 645 Provisions | Covered/ Supported by | Rationale |
|---|---|---|
| 5.4-4 Device unique and diversified critical security parameters | Verification of Platform Instance Identity; Secure Update of Platform | Final product update and communication mechanism shall be implemented by the operating system or application code.<br>RW61x provides platform instance identity and secure update feature which support the operating system or application code to fulfil this requirement. |
| 5.5-1 Best practice cryptography for communication | Cryptographic Functionality | Final product communication shall be designed by OEM.<br>RW61x provides cryptography supports to implement secure communication protocol. Reference designs (e.g. mbedTLS) are also available yet it is not part of this evaluation. |
| 5.5-2 Implementation review and evaluation | SESIP methodology and certification | This SESIP evaluation is performed by 3rd party independent laboratory and certifier who are specialized in security including cryptography. |
| 5.5-3 Cryptoagility | Secure Update of Platform, Cryptographic Functionality | RW61x provides update capability where software based cryptography can be updated. Supported key sizes are clearly stated in cryptographic functionality sections. |
| 5.5-4 Initialization state device access after authentication via network interface | Secure Initialization of Platform; Secure Debugging | The operating system or application code will take over control after RW61x boot up, hence up to the design by OEM. RW61x ensures secure initialization of the device before handling over control to operating system or application code when secure boot is configured. RW61x also supports debug authentication. |
| 5.5-5 Security configuration after authentication via network interface | Cryptographic Functionality | Final product communication shall be designed by OEM. RW61x provides cryptography supports to implement secure communication protocol. |
| 5.5-6 Confidentiality for security parameter in transition | | |
| 5.5-7 Confidentiality for security parameter via network | | |
| 5.5-8 Secure management process | Trust Provisioning | The secure management or key management process for OEM provisioned security parameters is owned by OEM. NXP trust provision process ensures security of the provisioned data. |
| 5.6-1 Unused interface disablement | - | RW61x provides configurabilities and the enablement and disablement of interfaces is upon OEM's design. |
| 5.6-2 Minimize disclosure during in initialization | Secure Initialization of Platform | The operating system or application code will take over control after RW61x boot up, hence up to the design by OEM. RW61x ensures secure initialization of the device before handling over control to operating system or application code when secure boot is configured. |

Table 15. EN 303 645 Mapping and Sufficiency*...continued*

| EN 303 645 Provisions | Covered/ Supported by | Rationale |
|---|---|---|
| 5.6-3 No unnecessary physical interface exposure | - | The design of final product including the physical interface exposure and its usability is by OEM |
| 5.6-4 Debug disablement | - | Debug function of RW61x can be disabled. Note RW61x provides Secure Debugging, yet by provision requirement this feature shall be disabled if interface is physically accessible. |
| 5.6-5 Least functionality | - | Software services of final product is defined by the operating system or application code. |
| 5.6-6 Minimized code | ADV: Development;<br>AVA: Vulnerability assessment | This evaluation provides full software source code access to evaluator for vulnerability assessment, and it assures that there is no unused code in the immutable part which could lead to attack path within the attack potential. |
| 5.6-7 Least privilege | Isolation of Platform (between SPE and NSPE) | RW61x provides different hardware based privilege levels and isolation mechanism which can be used to fulfil these requirements. |
| 5.6-8 Hardware-level memory access control | | |
| 5.6-9 Secure development process | - | Final product development process shall be defined and applied by OEM. RW61x is part of NXP Edge Lock Assurance Program and secure development process is applied |
| 5.7-1 Secure boot for software verification | Secure Initialization of Platform | RW61x provides secure boot feature and hardware root of trust. |
| 5.7-2 Notification of unauthorized change. | - | This provision requirement shall be implemented by the operating system or application code. |
| 5.8-1 Confidentiality of personal data transition between device and service | Cryptographic Functionality | Final product communication shall be designed by OEM. RW61x provides cryptography supports to implement the provision requirements. |
| 5.8-2 Confidentiality of personal data transition between devices | | |
| 5.8-3 External sensing capability documented | - | Final product sensing capability and its document handling is up to OEM. |
| 5.9-1 Resilience to outages | Secure Initialization of Platform;<br>Attestation of Platform State | The resilience to outrages and recovery shall be designed by OEM and service provider. RW61x provides secure initialization and attestation features which can support to fulfil the provision requirements. |
| 5.9-2 Local function with loss of network | | |
| 5.9-3 Orderly reconnection | | |
| 5.10-1 Telemetry data examination | Secure Initialization of Platform;<br>Attestation of Platform State | The use case and feature shall be defined by OEM of the final product. RW61x provides secure initialization and attestation features which can support to fulfil the provision requirements. |

Table 15. EN 303 645 Mapping and Sufficiency*...continued*

| EN 303 645 Provisions | Covered/ Supported by | Rationale |
|---|---|---|
| 5.11-1 Ease for user data deletion | Residual Information Purging | The feature for user data management shall be defined by OEM of the final product. RW61x provide information purging mechanism which can support to fulfil the provision requirements. |
| 5.11-2 Ease for user data deletion from service | - | These requirements shall be fulfilled by OEM and/or service provider. |
| 5.11-3 Instruction for personal data deletion | | |
| 5.11-4 Deletion confirmation | | |
| 5.12-1 Ease of installation and maintenance | - | These requirements shall be fulfilled by OEM and/or service provider. |
| 5.12-2 Guidance on setup | | |
| 5.12-3 Check on secure setup | Secure Initialization of Platform; Attestation of Platform State | This requirement shall be fulfilled by OEM and/or service provider. RW61x provides secure initialization and attestation features which can support to fulfil the provision requirement. |
| 5.13-1 Input Validation | ADV: Development; AVA: Vulnerability assessment | The final product operating system or application code is responsible for their input validation. The SESIP evaluation ensures there is no attack path identified including input manipulation within the attack potential in RW61x scope. |
| 6-1 Clear personal data usage | - | These requirements shall be fulfilled by OEM and/or service provider. |
| 6-2 Consumer's consent | | |
| 6-3 Consent withdraw | | |
| 6-4 Minimum telemetry data collection | | |
| 6.5 Clear telemetry data collection and usage | | |

## 5.2 NIST IR 8425 Mapping and Sufficiency

NIST has developed Profile of the IoT Core Baseline for Consumer IoT Products as NIST IR 8425 [18], which identifies cybersecurity capabilities commonly needed for the consumer IoT sector.

This section refers to the claims and activities within this SESIP evaluation scope to demonstrate the sufficiency by SESIP methodology towards compliance of NIST IR 8425. Note NIST IR 8425 is targeting for consumer IoT products with full software stack mounted and physically designed, and connection to network-based services. The full software stack includes the operating system, communication stack and protocol, and/or application code, which is designed and owned by NXP (direct and indirect) customers, i.e. the consumer IoT product manufactures (aka OEMs), and the network service providers. So not all requirements are directly applicable to NXP product scope but more to OEMs and the network service providers. Thus, rationale on how RW61x can support customers to meet NIST IR 8425 requirements are provided.

The descriptions below are checked by the independent security laboratory as part of the SESIP evaluation and provide evidences reusable in the context of consumer IoT product towards compliance to NIST IR 8425 when the corresponding security features are leveraged.

Table 16. NIST IR 8425 Mapping and Sufficiency

| NIST IR 8425 | Covered/Supported by | Rationale |
|---|---|---|
| Asset Identification - 1 & 2 | Verification of Platform Identity; Verification of Platform Instance Identity ; Attestation of Platform Genuineness | RW61x provides identifications for its internal parts and their versions, and unique instance identification, which OEM can leverage for IoT Device identification.<br>Attestation APIs further support to get the identitiy information in a secure manner. |
| Product Configuration - 1 | Cryptographic Functionality; Secure Update of Platform | The authorization and configuration of the IoT device shall be implemented by the operating system or application code.<br>RW61x 's cryptographic functionalities provide the IoT products capablity to implement the authorization and access control mechanisms. Based on such mechanisms, the IoT product configuration settings can be changed by authorized individuals, services or other IoT product components.<br>Cryptographic KeyStore additionally supports the protection of the cryptographic secrets involved in the authorization mechanism described above.<br>Secure Update of Platform allows the IoT devices to update to a newer version in the field in secure manner if this is needed for a configuration update. |
| Product Configuration - 2 | Residual Information Purging | The authorization and configuration of the IoT device shall be implemented by the operating system or application code.<br>RW61x provides Residual Information Purging functions, which can erase corresponding data when the IoT product is returned to a secure default configuration. |
| Product Configuration - 3 | Secure Update of Platform | The way the IoT product applies configuration to IoT components depends on the IoT product architecture, and the IoT device operating system or application shall be implemented accordingly.<br>RW61x's Secure Update of Platform function allows the IoT Device to update to a newer version in the field in secure manner if this is needed for a configuration update. |

Table 16. NIST IR 8425 Mapping and Sufficiency*...continued*

| NIST IR 8425 | Covered/Supported by | Rationale |
|---|---|---|
| Data Protection - 1 | Secure External Storage; Cryptographic Key Store; Physical Attack Resistance; Isolation of Platform Parts; Secure Debugging; Verification of Platform Identity; Verification of Platform Instance Identity | RW61x provides various mechanisms to protect date it stores.<br>The IoT device can leverage the secure external storage function.<br>The Cryptographic KeyStore function protects the storage of the cryptographic data.<br>Physical Attacker Resistance and Software Attacker Resistance: Isolation of Platform support the secure data storage by implementing protections against physical and logical, remote and local attacks.<br>Secure Debugging supports the secure data storage by not protecting unauthorized access to those data via debug features.<br>The platform identity and instance identity are also stored securely. |
| Data Protection - 2 | Residual Information Purging; Field Return of Platform; Decommission of Platform | RW61x's Residual Information Purging function supports the ability to delete or render inaccessible user data stored in RW61x.<br>Field Return of Platform and Decommission of Platform can be levearged by IoT devices to delete or render inaccessible inaccessible stored data when changing life-cycle state. |
| Data Protection - 3 | Cryptographic Functionality | The communication function of the IoT device shall be fully facilitated by the operating system or application code.<br>RW61x provides cryptographic functionalities by which the IoT device can implement protection of data transmission.<br>Cryptographic KeyStore additionally supports the protection of the cryptographic secrets involved in the data transmission protection mechanism. |

Table 16. NIST IR 8425 Mapping and Sufficiency*...continued*

| NIST IR 8425 | Covered/Supported by | Rationale |
|---|---|---|
| Interface Access Control - 1 & 2 | Cryptographic Functionality; Extra Attacker Resistance; Secure Debugging; VA: Vulnerability Assessment; ADV: Development; ATE: Test | The design of final device including the physical interface exposure and its usability is by OEM. The access control, authentication, and communcation mechanism shall also be implemented by the operating system or application code of the IoT device.<br>RW61x provides cryptographic functionalities by which the IoT devices can implement access control and authentication mechanism.<br>Cryptographic KeyStore additionally supports the protection of the cryptographic secrets involved in the authentication mechanism described above.<br>Software Attacker Resistance: Isolation of Platform and Software Attacker Resistance: Isolation of Platform Part implement protections against illegal access to resources (physically isolated by design), by restricting the access between Secure and Non Secure domain of trust zone, and between the security enclave and the rest of system.<br>Secure Debugging supports the access control to RW61x debug interfaces only for authorized party.<br>Also, the AVA (vulnerability assessment), ADV (development) and ATE (Test) activities in SESIP evaluation verify that the interfaces provided at RW61x platform level are restricted to only the necessary functions and privileges, and there is no unnecessary privilege, interface and/or code remained. |
| Software Update - 1 & 2 | Secure Update of Platform | Secure Update of Platform implements the secure update ensuring integrity and authentication verification.<br>The software update development, distribution and customer notification are expected to be managed by OEMs and/or the network service providers. |
| Cybersecurity State Awareness - 1 | Attestation of Platform Genuineness; Attestation of Platform State; Secure External Storage; Physical Attack Resistance; Isolation of Platform Parts | The cybersecurity state awareness of the IoT device shall be designed and implemented by the operating system or application code.<br>RW61x provides various services that can facilitate such mechanism:<br>The attesetation function can attest the identity and platform state.<br>Secure External Storage can be leveraged for secure storage of audit records.<br>Software Attacker Resistance: Isolation of Platform can provide secure handling of audit records as well as capture of attempts of privilage violation.<br>Physical Attacker Resistance also provide protections on secure audit record handling. |

Table 16. NIST IR 8425 Mapping and Sufficiency*...continued*

| NIST IR 8425 | Covered/Supported by | Rationale |
|---|---|---|
| Documentation | ASE: Security Target; AGD: Guidance document; SESIP Methodology [1]; SESIP Profile for Secure MCUs and MPUs [2];<br>SESIP Profile for PSA Certified Level 3 [3]; Flaw Reporting Procedures | NXP provides RW61x documents related to cybersecurity. The ASE (Security Target) and AGD (user guidance) activities in SESIP evaluation (see [1]) evaluates the documents to ensure information is provided related to security including security scope, functions, assurance level, secure use of the platform, etc.<br>Flaw Reporting Procedure (ALC_FLR.2) in SESIP evlaution ensures that it is clear that how a customer get informed |
| Information and Query Reception | Flaw Reporting Procedures | This is a requirement to OEMs and/or the network service providers.<br>At NXP level, we have Flaw Reporting Procedure defined, and as part of SESIP evaluation (see also [1]), such procedure is verified that flaw reporting process is in place and allows the efficient tracking of flaws, and users get notifications on a flaw and how to handle it |
| Information Dissemination | ASE: Security Target; AGD: Guidance document; Flaw Reporting Procedures | This is a requirement to OEMs and/or the network service providers.<br>NXP provides RW61x documents related to cybersecurity. See more in rational in Documentation and Information and Query Reception entry. |
| Product Education and Awareness | ASE: Security Target; AGD: Guidance document; | This is a requirement to OEMs and/or the network service providers.<br>NXP provides RW61x documents related to cybersecurity. The ASE (Security Target) and AGD (user guidance) activities in SESIP evaluation (see [1]) evaluates the documents to ensure information is provided related to security including security scope, functions, assurance level, secure use of the platform, etc. |

# 6 Bibliography

## 6 . 1 Evaluation Documents

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

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

[3] SESIP Profile for PSA Certified Level 3, V1.0 REL 01, PSA JSA, Oct 2022.

## 6 . 2 Developer Documents

[4] UM11865, RW61x User Manual, Rev. 1, May 2023, NXP Semiconductors

[5] UM11864, RW61x Crypto Subsystem, Rev. 1, May 2023, NXP Semiconductors

[6] RM00278, RW610/RW612 Registers, Rev. 3, November 2022, NXP Semiconductors

[7] RW610, Wireless MCU with Integrated Wi-Fi 6 and Bluetooth Low Energy 5.3 Data Sheet, Rev. 2, December 2022, NXP Semiconductors

[8] RW612, Wireless MCU with Integrated Wi-Fi 6 and Bluetooth Low Energy 5.3 / 802.15.4Data Sheet, Rev. 2, December 2022, NXP Semiconductors

[9] User Manual of Crypto Library Normal Secure (CLNS), CLNS SDK 1.3.0, NXP Semiconductors

[10] AN13813 Secure boot on RW61x, Rev. 0.1, May 2023, NXP Semiconductors

[11] AN13814 Debug authentication on RW61x, Rev. 0.1, May 2023, NXP Semiconductors

[12] RW61x SDK with TF-M v1.7 ported, 2.13.0 EAR4 TF-M Secure Hardened

[13] Secure Provisioning SDK (SPSDK) Application User Guides, Rev. 2facbebd, NXP Semiconductors, https://spsdk.readthedocs.io/

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

[15] AN6259, Common Trust Provisioning Conceptional Overview, Rev 1.1, NXP Semiconductors, March 2021.

## 6 . 3 Standards

[16] ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI, v2.1.1, June 2020

[17] SESIP Applicability for EN 303 645, White Paper, GlobalPlatform, January 2022

[18] NIST IR 8425 Profile of the IoT Core Baseline for Consumer IoT Products, National Institute of Standards and Technology, Sepptember 2022, https://csrc.nist.gov/pubs/ir/8425/final

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

[20] ARM Firmware Framework for M 1.1 Extensions, ARM Limited, AES 0039. Issue number 0, ALPHA release, Dec 2020

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

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

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

# 7 Legal information

## 7.1 Definitions

**Draft** — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

## 7.2 Disclaimers

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

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

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

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

**Applications** — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

**Terms and conditions of commercial sale** — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

**Suitability for use in automotive applications** — This NXP product has been qualified for use in automotive applications. If this product is used by customer in the development of, or for incorporation into, products or services (a) used in safety critical applications or (b) in which failure could lead to death, personal injury, or severe physical or environmental damage (such products and services hereinafter referred to as "Critical Applications"), then customer makes the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. As such, customer assumes all risk related to use of any products in Critical Applications and NXP and its suppliers shall not be liable for any such use by customer. Accordingly, customer will indemnify and hold NXP harmless from any claims, liabilities, damages and associated costs and expenses (including attorneys' fees) that NXP may incur related to customer's incorporation of any product in a Critical Application.

**Export control** — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

**Translations** — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

**Security** — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

## 7.3 Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

**NXP** — wordmark and logo are trademarks of NXP B.V.

# Tables

Tab. 1. SESIP Profile for Secure MCUs and MPUs Conformance Claims ........................................3
Tab. 2. SESIP Profile for PSA Certified Level 3 Conformance Claims ........................................3
Tab. 3. Platform Reference .......................................... 3
Tab. 4. Guidance Documents ........................................4
Tab. 5. Platform Deliverables ........................................ 6
Tab. 6. Platform Objectives for the Operational Environment ...................................................... 9
Tab. 7. Trust provisioning ............................................ 11
Tab. 8. Cryptographic Operations by ELS S50 ............12
Tab. 9. Cryptographic Key Generation ........................ 12
Tab. 10. Cryptographic Operations provided outside of ELS S50 ......................................................18
Tab. 11. Cryptographic Operations ............................... 18
Tab. 12. Cryptographic Key Generation ........................ 19
Tab. 13. SESIP Profile for Secure MCUs and MPUs Sufficiency ....................................................... 23
Tab. 14. SESIP Profile for PSA Certified Level 3 Sufficiency ....................................................... 24
Tab. 15. EN 303 645 Mapping and Sufficiency ............. 25
Tab. 16. NIST IR 8425 Mapping and Sufficiency ...........31

## Figures

Fig. 1. RW61x Family Superset Block Diagram ........... 6
Fig. 2. RW61x Logical Architecture and Certification Scope ............................................ 7
Fig. 3. RW61x security Life-Cycle states ......................8

## Contents

**1 Introduction .......... 3**
1.1 ST Reference .......... 3
1.2 SESIP Profile Reference and Conformance Claims .......... 3
1.3 Platform Reference .......... 3
1.4 Included Guidance Documents .......... 4
1.5 Platform Overview and Description .......... 4
1.5.1 Platform Security Features .......... 5
1.5.2 Platform Type .......... 5
1.5.3 Platform Physical Scope .......... 5
1.5.4 Platform Logical Scope .......... 6
1.5.5 Required Non-Platform Hardware/Software/ Firmware .......... 7
1.5.6 Life Cycle .......... 7
1.5.7 Configurations .......... 8
1.5.8 Use Case .......... 8
**2 Security Objectives for the Operational Environment .......... 9**
2.1 Platform Objectives for the Operational Environment .......... 9
**3 Security Requirements and Implementation .......... 10**
3.1 Security Assurance Requirements .......... 10
3.1.1 Flaw Reporting Procedures (ALC_FLR.2) .......... 10
3.2 Security Process Packages (SPPs) .......... 10
3.2.1 Trust provisioning .......... 10
3.3 Security Functional Requirements for Security Enclave .......... 11
3.3.1 Identification and Attestation of Platforms and Applications .......... 11
3.3.1.1 Verification of Platform Identity .......... 11
3.3.2 Extra Attacker Resistance .......... 11
3.3.2.1 Software Attacker Resistance: Isolation of Platform Parts .......... 11
3.3.3 Cryptographic Functionality .......... 12
3.3.3.1 Cryptographic Operation .......... 12
3.3.3.2 Cryptographic Key Generation .......... 12
3.3.3.3 Cryptographic KeyStore .......... 13
3.3.3.4 Cryptographic Random Number Generation .......... 13
3.3.4 Compliance Functionality .......... 13
3.3.4.1 Residual Information Purging .......... 13
3.4 Security Functional Requirements for SoC .......... 13
3.4.1 Identification and Attestation of Platforms and Applications .......... 14
3.4.1.1 Verification of Platform Identity .......... 14
3.4.1.2 Verification of Platform Instance Identity .......... 14
3.4.1.3 Attestation of Platform Genuineness .......... 14
3.4.1.4 Attestation of Platform State .......... 14
3.4.1.5 Secure Initialization of Platform .......... 15
3.4.2 Product Lifecycle: Factory Reset / Install / Update / Decommission .......... 15
3.4.2.1 Secure Update of Platform .......... 15
3.4.2.2 Field Return of Platform .......... 16
3.4.2.3 Decommission of Platform .......... 16
3.4.3 Extra Attacker Resistance .......... 17
3.4.3.1 Physical Attack Resistance .......... 17
3.4.3.2 Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) .......... 17
3.4.3.3 Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services .......... 17
3.4.3.4 Software Attacker Resistance: Isolation of Platform Parts .......... 18
3.4.4 Cryptographic Functionality .......... 18
3.4.4.1 Cryptographic Operation .......... 18
3.4.4.2 Cryptographic Operation (with provisioned key) .......... 18
3.4.4.3 Cryptographic Key Generation .......... 19
3.4.4.4 Cryptographic KeyStore .......... 19
3.4.4.5 Cryptographic Random Number Generation .......... 20
3.4.5 Compliance Functionality .......... 20
3.4.5.1 Secure External Storage .......... 20
3.4.5.2 Secure Debugging .......... 20
3.4.5.3 Residual Information Purging .......... 21
3.4.5.4 Reliable Index .......... 21
**4 Mapping and Sufficiency Rationales .......... 22**
4.1 SESIP3 Sufficiency .......... 22
4.2 Conformance Mapping for SESIP Profile for Secure MCUs and MPUs .......... 23
4.3 Conformance Mapping for SESIP Profile for PSA Certified Level 3 .......... 24
**5 Appendix .......... 25**
5.1 ETSI EN 303 645 Mapping and Sufficiency .......... 25
5.2 NIST IR 8425 Mapping and Sufficiency .......... 30
**6 Bibliography .......... 35**
6.1 Evaluation Documents .......... 35
6.2 Developer Documents .......... 35
6.3 Standards .......... 35
**7 Legal information .......... 36**

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

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

**Date of release: 6 February 2024**