Security Target for SiWG917X1X Single Chip Wi-Fi® and Bluetooth® LE Wireless Secure MCU Version 0.4

27/11/2025
Silicon Labs
Based on [PSA-SESIP-L2] methodology, Version 0.1 REL 02

CHANGE HISTORY

Version	Date	Author	Comment
0.1	04/06/2025	Silicon Labs	First Release
0.2	13/08/2025	Silicon Labs	Fixes
0.3	30/09/2025	Silicon Labs	Fixes
0.4	27/11/2025	Silicon Labs	TOE Rename

Abstract

PSA Certified is the independent security evaluation scheme for Platform Security Architecture (PSA) based IoT systems. It establishes trust through a multi-level assurance program for chips containing a security component called a Root of Trust (PSA-RoT) that provides trusted functionality to the platform. The multi-level scheme has been designed to help device makers and businesses get the level of security they need for their use case. An overview of SESIP Profiles important to the PSA Certified scheme is given in Figure 1 that shows how this document relates to others for the chip's Root of Trust.

PSA Certified Level 2 is a fixed time, test laboratory based, evaluation of the PSA-RoT. It is aimed at IoT devices that need to protect against basic software attacks. The Level 2 documents include: a SESIP Profile that describes the Target of Evaluation, its assets, the security objectives and security functions that will be evaluated and an Attack Methods (AM) document describing the attacks in scope.

Developers submit their PSA-RoT to an approved test laboratory, listed on www.psacertified.org, for Level 2 evaluation and receive an Evaluation Technical Report. If the PSA-RoT is assessed as passing and approved by the independent Certification Body, a digital certificate will be issued on the PSA Certified website.

Keywords

PSA Certified Level 2, SESIP, Certification, IoT, Platform Security Architecture, Questionnaire, PSA, Security

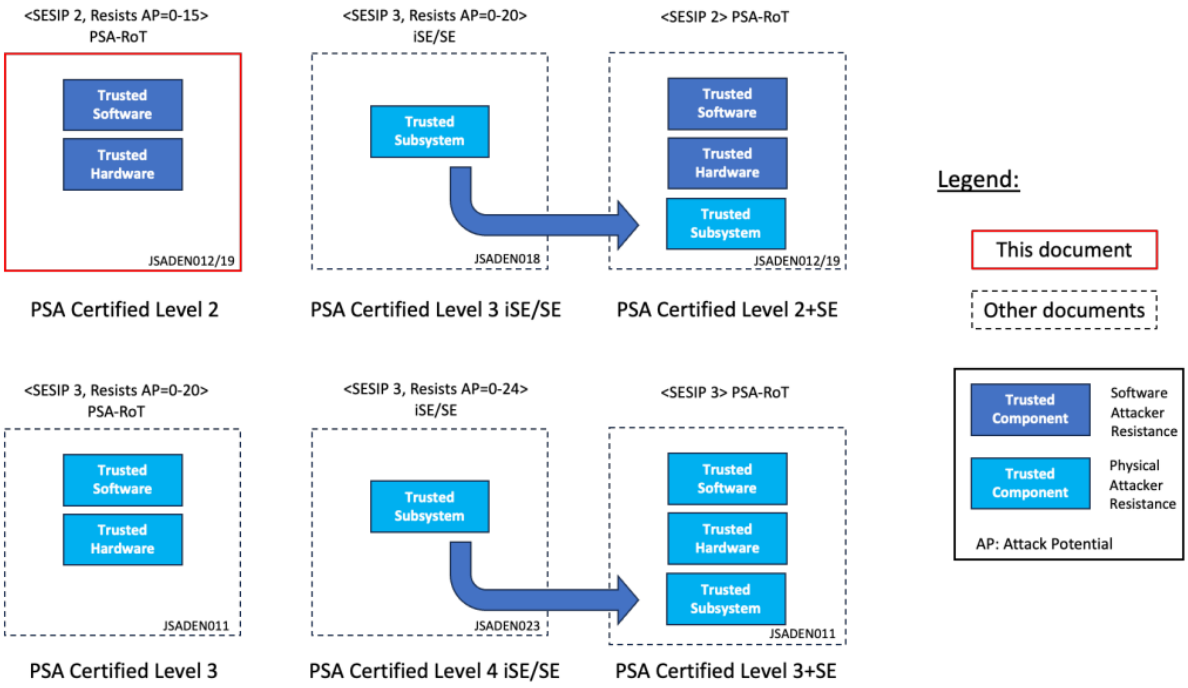

Figure 1: PSA Certified SESIP Profiles for the chip's RoT

Non-Confidential Proprietary Notice

Contents

Abstract 4
Contents 6
1 About this document 8
1.1 Current Status and Anticipated Changes 8
1.2 Release Information 8
1.3 References 9
1.3.1 Normative references 9
1.3.2 Informative references 9
1.4 Terms and Abbreviations 10
1.5 PSA Certified Level 2 12
1.5.1 PSA Certified Level 2 Ready Evaluation 13
1.5.2 PSA Certified Level 2+SE Certification 13
1.5.3 PSA Certified RoT Component Certification 13
2 Introduction 14
2.1 SESIP Profile Reference 14
2.2 Platform reference 14
2.3 Included guidance documents 15
2.4 Platform functional overview and description 15
2.4.1 Platform Type 15
2.4.2 Physical Scope 18
2.4.3 Logical Scope 18
2.4.4 Usage and Major Security Features 19
2.4.5 Required Hardware/Software/Firmware 20
3 Security Objectives for the Operational Environment 21
4 Security Requirements and Implementation of the Security Target 22
4.1 Security Assurance Requirements 22
4.1.1 Flaw Reporting Procedure of the Security Target (ALC_FLR.2) 22
4.2 Base PP Security Functional Requirements 23
4.2.1 Verification of Platform Identity 23
4.2.2 Verification of Platform Instance Identity 25
4.2.3 Attestation of Platform Genuineness 25
4.2.4 Secure Initialization of Platform 26
4.2.5 Attestation of Platform State. 27
4.2.6 Secure Update of Platform. 27
4.2.7 Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) 29
4.2.8 Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) 30
4.2.9 Cryptographic Operation 30
4.2.10 Cryptographic Random Number Generation 31
4.2.11 Cryptographic Key Generation 31
4.2.12 Cryptographic KeyStore 33
4.2.13 Secure Confidential Storage 33
5 Mapping and sufficiency rationales 37
5.1 Assurance 37
5.2 Functionality 39

6 References 42
7 Appendix: SFRs by PSA Certified Levels 43

1 About this document

1.1 Current Status and Anticipated Changes

Current Status: Released, Version 0.4

1.2 Release Information

The change history table lists the changes that have been made to this document.

Date	Version	Change
2025-06-04	0.1	First Release
2025-08-13	0.2	Fixes
2025-09-30	0.3	Fixes
2025-11-27	0.4	TOE Rename

1.3 References

This document refers to the following documents.

1.3.1 Normative references

Ref	Dos No	Author(s)	Title
[PSA-L1]	JSADEN001	JSA	PSA Certified Level 1 Questionnaire
[PSA-EM-L2]	JSADEN003	JSA	PSA Certified: Evaluation Methodology for PSA L2
[PSA-EM-L3]	JSADEN010	JSA	PSA Certified: Evaluation Methodology for PSA L3
[PSA-AM]	JSADEN004	JSA	PSA Certified Attack Methods
[PSA-PP-L2]	JSADEN002	JSA	PSA Certified Level 2 Lightweight Protection Profile
[PSA-PP-L3]	JSADEN009	JSA	PSA Certified Level 3 Lightweight Protection Profile
[SESIP-PP-L3]	JSADEN011	JSA	SESIP Profile for PSA Certified™ Level 3
[PSA-L2-COMP]	JSADEN017	JSA	SESIP Profile for PSA Certified™ RoT Component Level 2
[PSA-L3-COMP]	JSADEN018	JSA	SESIP Profile for PSA Certified™ RoT Component Level 3
[PSA-L4-iSE-SE]	JSADEN023	JSA	SESIP Profile for PSA Certified™ Level 4 iSE/SE and RoT Component
[SESIP]	GP_FST_070	GlobalPlatform	Security Evaluation Standard for IoT Platforms (SESIP) v1.2
[CEN-SESIP]	EN 17927	CEN/CENELEC	Security Evaluation Standard for IoT Platforms (SESIP) 2023
[CEM]	CCMB-2017-04-004	Common Criteria	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, revision 5, April 2017.

1.3.2 Informative references

Ref	Doc No	Author(s)	Title
[GP-ROT]	GP_REQ_025	GlobalPlatform	Root of Trust Definitions and Requirements, Version 1.1, Public Release, June 2018
[PSA-SM]	JSADEN014	ARM	Platform Security Model
[PSA-SS]	IHI 0087	ARM	PSA Certified Secure Storage API, Version 1.0 or later

[SP-800-57]	SP 800-57 Part 1	NIST	Recommendation for Key Management: Part 1 – General, Rev. 5

1.4 Terms and Abbreviations

This document uses the following terms and abbreviations (see PSA-SM and PSA-L1)-

Term	Meaning
Application	Used in this SESIP profile to refer to the components which are out of the scope of the evaluation.
Application Root of Trust Service(s)	Application specific security service(s) that are not defined by PSA. Such services execute in the Secure Processing Environment and are required to be in Secure Partitions.
Application Specific Software	Software that provides the functionality required of the specific device. This software runs in the Non-Secure Processing Environment, making use of the System Software, Application RoT Services and PSA-RoT Services.
Critical Security Parameter	Secret information, with integrity and confidentiality requirements, used to maintain device security, such as authentication data (passwords, PIN, certificates), secret cryptographic keys, etc..
Evaluation Laboratory	Laboratory or facility that performs the assessment of products submitted for PSA Certified. The list of evaluation laboratories participating to PSA Certified can be found on www.psacertified.org
Hardware Unique Key (HUK)	Secret and unique to the device symmetric key that must not be accessible outside the PSA Root of Trust. It is a Critical Security Parameter.
Host Platform	The entity which when used in composition with a certified PSA Level 2 RoT Component [PSA-L2-COMP], a certified PSA Level 3 RoT Component [PSA-L3- COMP] or a certified PSA Level 4 RoT Component [PSA-L4-iSE-SE] form the scope of the certification covered in this profile.
Initial Attestation Key (IAK)	A PSA-RoT secret private key from an asymmetric key-pair used to sign attestation reports, thus ensuring that the report is bound to a unique PSA- RoT (and so device) instance.
Non-secure Processing Environment (NSPE)	The processing environment that hosts the non-secure System Software and Application Specific Software. PSA requires the NSPE to be isolated from the SPE. Isolation between partitions within the NSPE is not required by PSA though is encouraged where supported.
Partition	The logical boundary of a software entity with intended interaction only via defined interfaces, but not necessarily isolated from software in other partitions. Note that both the NSPE and SPE may host partitions.
Platform	Used in this SESIP Profile to refer to the components which are in the scope of the evaluation.
PSA	Platform Security Architecture
PSA Certification Body	The entity that receives applications for PSA security certification, issues the certificates, maintains the security certification scheme, and ensures consistency across all the evaluation laboratories.

PSA Functional APIs	PSA defined Application Programming Interfaces on which security services can be built. APIs defined so far include Crypto, Secure Storage and Attestation.
PSA Functional API Certification	Functional certification confirms that the device implements the PSA Functional APIs correctly by passing the PSA Functional certification test suites.
PSA Root of Trust (PSA-RoT)	The PSA defined combination of the Immutable Platform Root of Trust and the Updateable Platform Root of Trust and is considered to be the most trusted security component on the device. See [PSA-SM].
Immutable Platform Root of Trust	The minimal set of hardware, firmware and data of the PSA-RoT, which is inherently trusted because it cannot be modified following manufacture. There is no software at a deeper level that can verify that it as authentic and unmodified.
Updateable Platform Root of Trust	The firmware, software and data of the PSA-RoT that can be securely updated following manufacture.
Platform Root of Trust Service(s)	PSA defined security services for use by PSA-RoT, Application RoT Service(s) and by the NSPE. Executes in the Secure Processing Environment and may use Trusted Subsystems. This includes the services offered by the PSA Functional APIs.
SESIP Profile	Document providing a common set of functionalities for similar products
Secure Partition	A Partition in the Secure Processing Environment.
Secure Processing Environment Partition Management	Management of the execution of software in Secure Partitions. Typical implementations will provide scheduling and inter partition communication mechanisms. Implementations may also enforce isolation between the managed Secure Partitions.
Secure Processing Environment (SPE)	The processing environment that hosts the PSA-RoT, the PSA-RoT Services, and any Application RoT Service(s).
Secure Boot	The process of verifying and validating the integrity and authenticity of updateable firmware and software components as a pre-requisite to their execution. This must apply to all the firmware and software in the SPE. It should also apply to the first NSPE image loaded, which may extend the NSPE secure boot chain further.
Security Target (ST)	Document providing an implementation-dependent statement of security of a specific identified platform.
System Software	NSPE software that may comprise an Operating System or some run-time executive, together with any middleware, standard stacks and libraries, chip specific device drivers, etc., but not the application specific software.
TOE	Target of Evaluation. In this SESIP Profile it is a synonym for Platform.
Trusted subsystem	A security subsystem that the PSA-RoT relies on for protection of its assets, or that implement some of its services.

Abbreviation	Meaning
AEM	Advance Energy Monitoring
APB	Advance Peripheral Bus
DUT	Device Under Test

GPIO	General Purpose Input Outputs
I2S	Inter-IC Sound Bus
ISP	In System Programming
LE	Low Energy
MBR	Master Boot Record
MCU	Micro-Controller Unit
MIC	Message Integrity Check
MVP	Matrix vector Processor
OTA	Over the Air
PUF	Physically Unclonable Function
PWM	Pulse Width Modulation
QEI	Quadrature Encoder Interface
RTC	Real Time Counter
SDIO	Secure Digital Input Output
SDR	Single Data Rate
SIO	Serial Input Output
SOC	System On Chip
SPI	Serial Peripheral Interface
SWD	Serial Wire Debug comprehensive debug functionality.
TA	ThreadArch
TCM	Tightly Coupled Interfaces
UART	Universal Asynchronous Receiver Transmitter
USART	Universal Synchronous/Asynchronous Receiver Transmitter
WDT	Watchdog Timer
WFI	Wait for interruption
XIP	eXecute In Place

1.5 PSA Certified Level 2

PSA defines a common hardware and software security platform, providing a generic security foundation and allowing secure products and features to be developed on top of this platform.

The PSA Certified scheme involves the evaluation by a laboratory of a device against a set of security requirements and, in case of a successful evaluation, the certification by the PSA Certified certification body of this Platform. The evaluation laboratory examines measures and processes to ensure that a functional Platform is not vulnerable to the identified threats to the levels defined in this document.

The PSA programme recognises that there will be different security requirements and different cost/security trade-offs for different applications and eco-systems. This is reflected in specifications by introducing a range of assurance levels.

Two evaluation paths are currently possible for a PSA Certified Level 2 product, either through the PSA Certified Level 2 Protection Profile [PSA-PP-L2] and associated evaluation methodology [PSA-EM-L2], or through a SESIP evaluation using the SESIP Profile defined in this document. The SESIP standard associated with this document is defined either by GlobalPlatform [GP-SESIP] or by CEN/CENELEC [CEN-SESIP].

1.5.1 PSA Certified Level 2 Ready Evaluation

The PSA Certified scheme allows for pre-certification evaluation of FPGA or development-based systems, which provide reference designs for ASIC or custom chip, but which may not be able to meet all security functions of this profile. In this case, only the claimed security functions are tested by the Evaluation Laboratory who issues the Evaluation Technical Report. No PSA Certified Level 2 certificate is generated for a Level 2 Ready evaluation, but the Developer can obtain the rights to use a specific "PSA Certified Level 2 Ready" logo and showcase its solution on www.psacertified.org.

Such a logo could be used to demonstrate, for example, the benefit of software security assurance offered from an evaluated FPGA based system for development of secure AROTs, RTOS or device while maximizing chances of passing PSA Certified Level 2 certification for future ASIC or custom chips based on the FPGA reference design.

1.5.2 PSA Certified Level 2+SE Certification

The PSA Certified scheme also considers a PSA Certified Level 2 certification where the product architecture, as illustrated in Figure 2, includes a trusted subsystem, typically an external Secure Element or an on-chip integrated Secure Element.

The Developer can obtain the rights to use the specific "PSA Certified Level 2+SE" logo and showcase the solution on www.psacertified.org, when the trusted subsystem has been certified for the security functions listed below for protection against physical attacks to at least PSA Certified Level 3 RoT Component [PSA-L3- COMP], or SESIP3, or AVA_VAN.3 (with Common Criteria).

The L2+SE logo could be used to demonstrate, for example, the benefit of protection against hardware attacks for the most sensitive assets of the product.

1.5.3 PSA Certified RoT Component Certification

The PSA Certified scheme allows for certification of RoT Components that address a subset of the security functions required by an implementation for a Level 2 certifiable PSA Root-of-Trust (RoT) in accordance with this protection profile.

In the PSA Security Model [PSA-SM] such parts of a root-of-trust are referred to as a Trusted Subsystem. A typical example is an IP block that will be used in a chip. The IP could address a few security functions, with the Document Number: JSADEN012 Version: 2.0 REL 01 Non-Confidential 11 rest of the chip covering all other requirements. Another example is an external chip that addresses a subset of the security functions, which when connected to another chip (Host Platform) form a complete Level 2 certifiable PSA-Root-of-Trust.

A PSA L2 RoT Component [PSA-L2-COMP] may be used to aid the evaluation of an L2 PSA-RoT certification.

2 Introduction

This SESIP profile proposes a mapping between the security functionality defined in the PSA L2 Protection Profile [PSA-PP-L2] and the SFRs (Security Functional Requirements) listed in the SESIP catalogue [SESIP]. This profile also includes some optional SFRs aiming to cover most of the platform use cases.

The effort for performing the AVA_VAN.2 activities of a standard implementation of a PSA-RoT is **25 person-days**. It is assumed for this workload that:

- the source code for the components in scope of the platform (see Sections 2.4.2 and 2.4.3, hardware design is not required). This shall include drivers for Trusted Subsystems if used;
- no additional SFRs are added in the Profile;
- evaluation activities are not re-used;
- the SFRs "Cryptographic Operation" and "Cryptographic Key Generation" include one cryptographic algorithm;
- the platform does not rely on a certified trusted subsystem or certified PSA Certified RoT Component (see Sections 1.5.2 and 1.5.3)

2.1 SESIP Profile Reference

Reference	**Value**
PP Name	*SESIP Profile for PSA Certified Level 2*
PP Version	V1.0 REL 02
Assurance Claim	*SESIP Assurance Level 2 (SESIP2)*
SESIP Standard	*GP-SESIP*
Optional and additional SFRs	*None*

Table 1: SESIP Profile Reference

2.2 Platform reference

The platform is uniquely identified by its chip (hardware) reference and its PSA defined Root of Trust (software) reference as described below. The developer declares that only the evaluated and successfully certified products identify in this way.

Reference	**Value**	
Platform Name	SiWG917X1X	
Platform Version	*Version 1.0*	
Platform Identification	Chip name and version	*SiWG917X1X version 1.0*
	PSA-RoT name and version	*Firmware version 1711.2.11.0:0.6*
Platform Type	*Single Chip Wi-Fi and Bluetooth LE Wireless Secure MCU.*	
Trusted Subsystem Identification	*None*	
Trusted Sub-system Certification	*None*	

Table 2: Platform Reference

2.3 Included guidance documents

The following documents are included with the platform:

Reference	Name	Version
[AGD_PRE]	AGD_PRE for SiWG917X1X SoC Single Chip Wi-Fi® and Bluetooth® LE Wireless Secure MCU Version 1.1	*Version 1.2*
[AGD_OPE]	AGD_OPE for SiWG917X1X SoC Single Chip Wi-Fi® and Bluetooth® LE Wireless Secure MCU Version 1.1	*Version 1.2*
[Datasheet]	SiWG917 SoC Single Chip Wi-Fi® and Bluetooth® LE Wireless Secure MCU Solutions.	*Preliminary Rev. 0.51*
[UG562]	UG562: SiWG917 Single-band Wi-Fi and BLE with 8 MB Flash Radio Board User's Guide. Revision 1.2, December 2023.	*Revision 1.2*
[UG574]	UG574: SiWx917 SoC Manufacturing Utility User Guide.	*Version 1.1*
[UG519]	UG519: Custom Part Manufacturing Service User's Guide.	*Revision 0.1*
[WC_SDK_v3]	Developing with WiSeConnect SDK v3.x with the SiWx91x Host. Version 3.1.3	*Version 3.1.3*
[API]	API reference guide v3.3.0.	*Version 3.3.0*
[AN1416]	SiWG917 SoC Memory Map Application Note.	*Version 1.0*
[AN1429]	SiWx917 SoC Throughput.	*Revision 1.2*
[AN1430]	SiWG917 Low-Power Application Note.	*Revision 1.0*
[AN1431]	SiWx917 SoC Firmware Update Application Note.	*Revision 1.0*
[AN1335]	RS9116 and SiWx917 Crystal Selection Guide, version 1.2, 20/12/2023	*Version 1.2*
[AN1423]	SiWx917 RF Matching and Layout Design Guide.	*Revision 0.1*
[AN1428]	SiWx917 Secure Debug.	*Revision 0.1*
[AN1436]	SiWx917 QMS Crystal Calibration Application Note.	*Revision 1.0*
[AN1437]	SiWx917 RF Regulatory Testing.	*Revision 0.1*
[AN1439]	SiWx917 Hardware Debugging Guidelines.	*Revision 1.0*
[AN1440]	SiWx917 Gain Offset Calibration.	*Revision 0.1*
[AN1448]	SiWx917 Power Supply Architecture and Configurations.	*Revision 1.0*
[AN1491]	SiWx917 RF Transmit & Receive Measurements, version 0.1, 03/07/2024.	*Version 0.1*
[NIST_197]	NIST FIPS 197 Specification for the ADVANCED ENCRYPTION STANDARD (AES), Nov 2001.	*November 2001*
[NIST_186-3]	NIST FIPS PUB 186-3 Digital Signature Standard (DSS), June 2009.	*June 2009*

Table 3. Guidance documents.

2.4 Platform functional overview and description

2.4.1 Platform Type

Silicon Labs SiWG917X1X is a low power Wi-Fi 6 plus Bluetooth LE 5.4 SoC, ideal for ultra-low power IoT wireless devices using Wi-Fi®, Bluetooth, Matter, and IP networking for secure cloud connectivity. It is optimal for developing battery operated devices that need long battery life.

The TOE is intended to be used by manufacturers as a fully integrated solution in a wide range of embedded wireless IoT application, such as: smart home devices, security cameras, HVAC, smart sensors, smart appliances, health and fitness devices, pet trackers, smart cities, smart meters…

The TOE consists of:

- Wi-Fi 6 Single Band 2.4 GHz 20 MHz 1x1 stream IEEE 802.11 b/g/n/ax, with TWT for improved efficiency and longer battery life, MUMIMO/OFDMA for Higher Throughput and network capacity and low latency. The transmit power is up to +20 dBm with integrated PA and the receive sensitivity as low as -97.5 dBm. The Operating Frequency Range is 2412 MHz – 2484 MHz. The Wi-Fi Standby Associated mode current is 55 µA at 1-second listen interval.
- Bluetooth LE with Transmit power up to +20 dBm with integrated PA and receive sensitivity of LE: -95 dBm, LR 125 Kbps: -106 dBm. The Operating Frequency Range is 2.402 GHz - 2.480 GHz.
- ARM® Cortex® M4 Processor with FPU, MPU and NVIC subsystems. The M4 microcontroller runs up to 180 MHz with rich set of Digital and Analog Peripherals.
- Silicon Labs' ThreadArch® (TA) 4-Threaded processor running up to 160 MHz. The Cortex-M4 is dedicated for peripheral and application related processing, whereas all the networking and wireless stacks run on independent threads of the ThreadArch®. In addition, in adherence to the Secure Execution Environment architecture, the ThreadArch® subsystem also acts as the secure processing domain and takes care of secure boot, secure firmware update, and provides access to security accelerators and secure peripherals through pre-defined APIs. The device provides a PUF to generate a unique hardware-based Root of Trust, providing both Platform and Application RoT through the secure cryptographic modules.
- Hardware Accelerators: Advanced Encryption Standard (AES) 128/256/192, Secure Hash Algorithm (SHA) 256/384/512, Hash Message Authentication Code (HMAC), Random Number Generator (RNG), Cyclic Redundancy Check (CRC), SHA3, AES-Galois Counter Mode (GCM)/ Cipher based Message Authentication Code (CMAC), ChaCha-poly, True Random Number Generator (TRNG).
- Security Features:
    - Secure Boot: Ensures your device runs authentic code in the boot and OTA update to eliminate malware insertion threats, Secure Immutable Bootloader in ROM, authenticates signatures of all other SW using public keys and Protocol and Application flash images can be encrypted with separate keys.
    - Secure OTA Firmware update.
    - TRNG: Generates high-entropy random numbers based on RF noise, increasing the effort/time needed to expose secret keys.
    - Secure Zone: Barrier between the Security/Protocol core and Application core and No access to the security processor, memory, and HW registers from external peripherals, including the Cortex-M4.
    - Secure Key storage: HW device identity and key storage with PUF.
    - Secure Debug: Debug ports are disabled in HW by default, it can be enabled in SW using cryptographically secure host interface commands validated by immutable bootloader and it allows the device's JTAG ports to be locked and unlocked.
    - Anti-Rollback: Firmware downgrade to a lower version is prohibited through OTP to prevent the use of older, potentially vulnerable FW version.
    - Secure XIP from flash with XTS/CTR mode.
    - Secure Attestation: Allows a device to authenticate its identity using a cryptographically signed token and exchange of secret keys.
    - Hardware Accelerators: AES128/256/192, SHA256/384/512, HMAC, RNG, CRC, SHA3, AES-GCM/ CMAC, ChaCha-poly.
    - Software Accelerators: RSA and ECC.
    - Programmable Secure Hardware Write protect for Flash sectors.

    - Support for secure firmware upgrade using PUF based Roots-of-Trust (RoT).
- Embedded Flash option up to 8 MB/ optional external Flash up to 16 MB
- Embedded PSRAM option up to 8 MB/ optional external PSRAM option up to 16 MB
- Embedded SRAM up to 672 kB total for Application and Wireless Processor.
- On-chip SRAM of 192 K/256 K/320 Kbytes for M4 Application Processor based on the memory configuration.
- Three software-configurable MCU application memory options for sharing the RAM between the wireless, system, and application (192/256/320 kB).
- Digital peripherals, including; SDIO 2.0 Secondary, Universal Synchronous/Asynchronous Receiver Transmitter (USART), 2X Universal Asynchronous Receiver Transmitter (UART), 4x Serial Peripheral Interface (SPI), 2x Inter-IC Sound Bus (I2S), Serial Input Output (SIO), Pulse Width Modulation (PWM), Quadrature Encoder Interface (QEI), Timers: 4x 16/32-bit, 1x 24-bit, Watchdog Timer (WDT), Real Time Counter (RTC) and up to 45 General Purpose Input Outputs (GPIOs) with GPIO multiplexer.
- Analogue Peripherals, including 12-bit 16-ch, 5 Mbps Analog to Digital Converter (ADC), 10-bit Digital to Analog Converter (DAC), 3x Op-amps, 2x Comparators, InfraRed (IR) detector and Temperature Sensor and 8 capacitive touch sensor inputs.
- Ultra-Low Power (ULP) Peripherals, such as; RTC, BOD, ULP I2C, ULP I2S, ULP UART, ULP GPIO, ULP Timers.
- Integrated baseband processor with calibration memory.
- Integrated RF transceiver, high-power amplifier, balun and T/R switch.

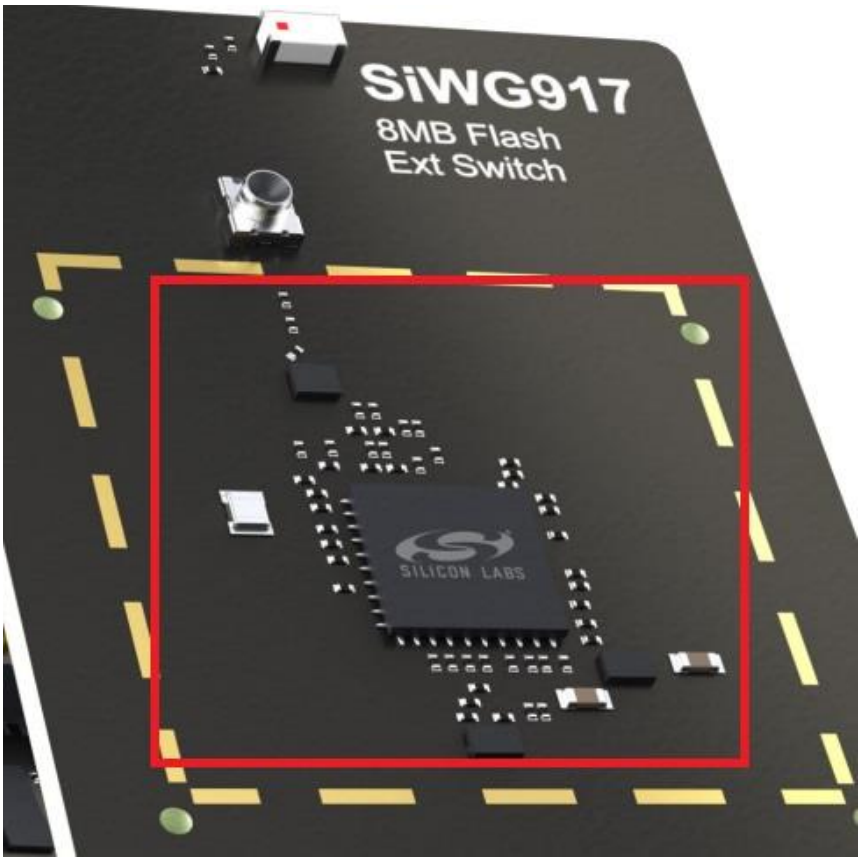

Figure 2. TOE Overview

2.4.2 Physical Scope

The hardware is a System on Chip. SiWG917X1X includes an ultra-low power Wi-Fi 6 plus Bluetooth Low Energy (LE) 5.4 wireless CPU subsystem, and an integrated micro-controller (MCU) application subsystem, security, peripherals and power management subsystem all in a single 7x7 mm QFN package. The wireless subsystem consists of a multi-threaded processor (ThreadArch®) running up to 160 MHz, baseband digital signal processing, analog front end, 2.4 GHz RF transceiver and integrated power amplifier. The application subsystem consists of an ARM® Cortex®-M4 running up to 180 MHz, embedded SRAM, FLASH, ultra-low power sensor hub and AI/ML accelerator. The ARM® Cortex®- M4 is dedicated for peripheral and application-related processing, while the ThreadArch® runs the wireless and networking stacks on independent threads.

Hardware is considered in the evaluation because it provides key security measures, such as immutable storage or protection of JTAG, which are essential for ensuring the security of the implementation. The physical scope refers to the aspects of hardware that ensure these protections and is defined by the following elements: only the described peripherals, the M4 MCU, TA MCU, the buses which connects both MCUs and the memory for the MCU (SRAM, PSRAM and flash).

2.4.3 Logical Scope

The scope for a SESIP Security evaluation, or Target of Evaluation (TOE), according to this profile is the combination of the trusted hardware and firmware components implementing a PSA-RoT with the Security Functional Requirements stated in this document, see Figure 3.

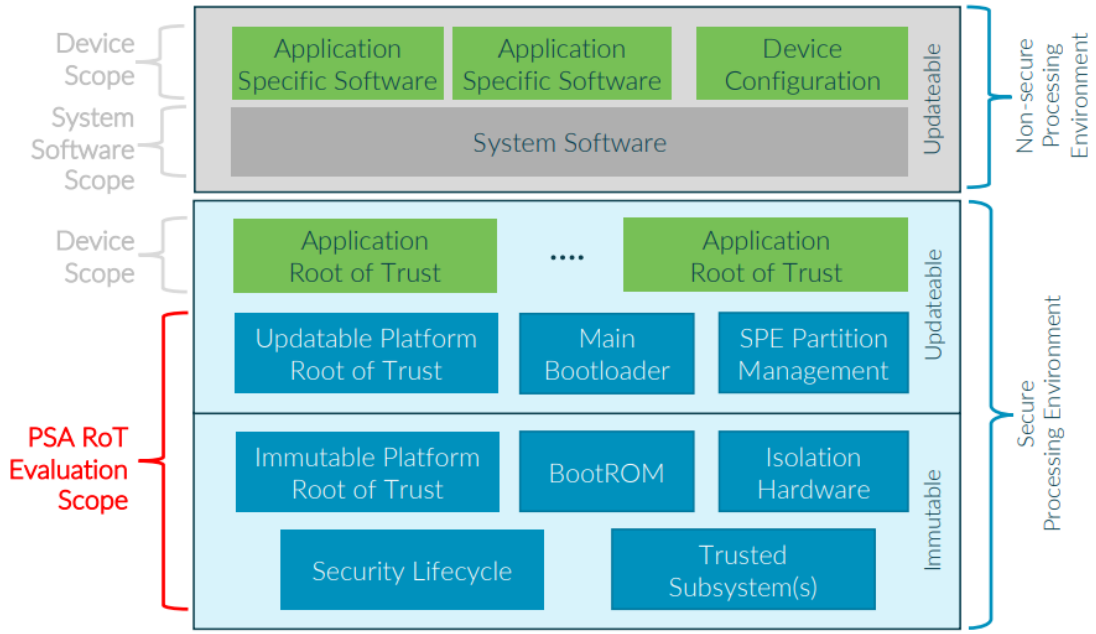

Figure 3: Scope of PSA Certified Level 2

The Chip security evaluation scope includes the following Secure Processing Environment PSA-RoT elements, as described in [PSA-SM]:

- Immutable Platform Root of Trust, for example, the Boot ROM, any root parameters, the NSPE/SPE isolation hardware, and any hardware-based security lifecycle management and enforcement.
- Updateable Platform Root of Trust, for example, a main bootloader, the code that implements the SPE Partition Management function, the code that implements the PSA defined services such as attestation, secure storage, and cryptography.
- Any Trusted subsystems that the host processor relies on for protection of its assets, or that implement some of its services.

The logical scope includes The Trusted Application (TA) running on the thread-architecture core, it hosts the network stack and wireless software, and the API, used by both, the M4 and the TA

processors to communicate. Consequently, the TA is responsible for secure boot, for establishing the secure processing domain, and for performing secure firmware updates. It also mediates access to security accelerators and peripheral services, enforcing access control and exposing those capabilities via well-defined APIs. In addition, the Wise Connect Wi-Fi integration, which forwards TA commands over the network through an API and also supports OTA updates, is included in the logical scope. By contrast, the Bluetooth interface and its stack were determined to have no security implications for this evaluation and were therefore excluded. The TA includes a coexistence manager that coordinates and alternates between protocols, see Figure 4.

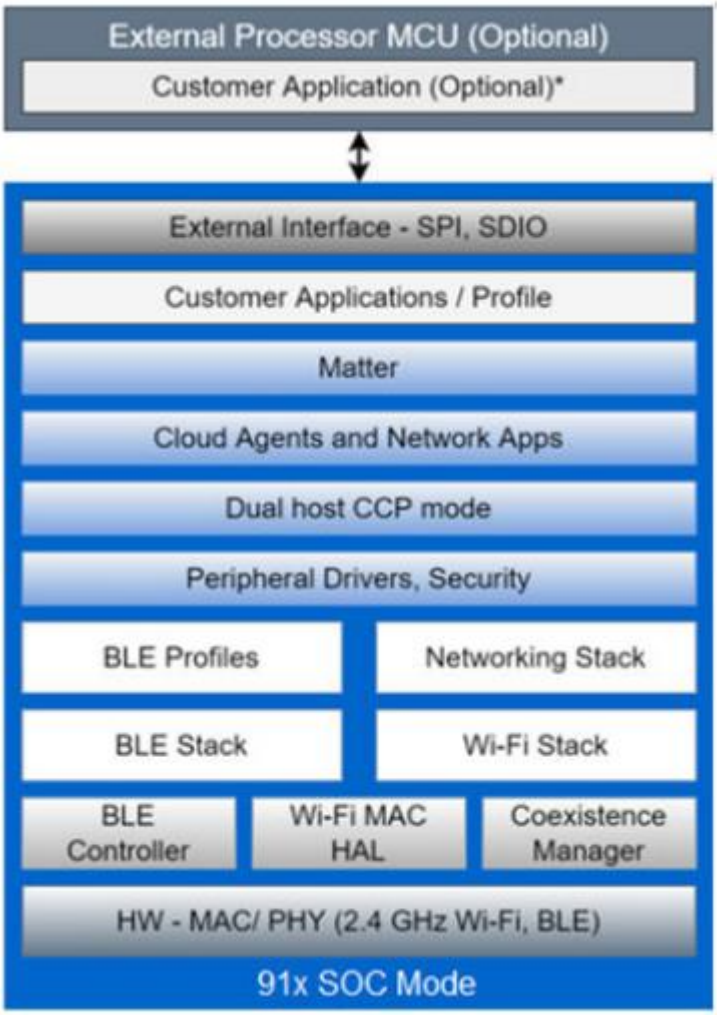

Figure 4 TOE scope

2.4.4 Usage and Major Security Features

This profile considers the following features for the purpose of PSA Level 2 security evaluation:

- A Secure Processing Environment (SPE) isolated by hardware mechanisms to protect critical services and related assets from the Non-Secure Processing Environment.
- A Secure Boot process to verify integrity and authenticity of executable code in a chain of trust starting from the Boot ROM. Related certificates are protected in integrity by hardware mechanisms.
- Support for Secure Storage, to protect in integrity and confidentiality sensitive assets for the SPE and related applications. These assets include at least the Hardware Unique Key (HUK), the PSA-RoT Public Key (ROTPK), the Initial Attestation Key (IAK), and the unique instance ID.

- A Security Lifecycle for the SPE, to protect the lifecycle state for the device and enforce the transition rules between states.
- Cryptographic functions services for SPE and SPE applications.
- Support for an attestation method, for example Entity Attestation Token (according to IETF specification)

As stated before, the TOE is intended to be used by manufacturers as a fully integrated solution in a wide range of embedded wireless IoT application, such as: smart home devices, security cameras, HVAC, smart sensors, smart appliances, health and fitness devices, pet trackers, smart cities, smart meters…

The main security features of the TOE are as follows:

- Secure Boot
- Secure firmware upgrade through boot-loader, Secure OTA.
- Secure Key storage and HW device identity with PUF
- Secure Zone
- Secure XIP (Execution in place) from flash/ PSRAM
- Secure Attestation
- Hardware Accelerators: Advanced Encryption Standard (AES) 128/256/192, Secure Hash Algorithm (SHA) 256/384/512, Hash Message Authentication Code (HMAC), Random Number Generator (RNG), Cyclic Redundancy Check (CRC), SHA3, AES-Galois Counter Mode (GCM)/ Cipher based Message Authentication Code (CMAC), ChaCha-poly, True Random Number Generator (TRNG)
- Software Accelerators: RSA, ECC
- Programmable Secure Hardware Write protect for Flash sectors
- Anti-Rollback
- Secure Debug

2.4.5 Required Hardware/Software/Firmware

The platform is supplied with the firmware and no apps. To develop applications (which are outside the scope of the evaluation), the client shall use the simplicity command studio, where examples of applications and functionality can be found

3 Security Objectives for the Operational Environment

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

ID	Description	Reference
KEY_MANAGEMENT	Cryptographic keys and certificates outside of the TOE are subject to secure key management procedures.	Section 3.4 from [AGD_PRE]
TOE_INTERACTING	Device security is the main consideration for the TOE. But the TOE, when deployed may be interfacing with some other associated services over various communication channels, e.g., mobile application, cloud base services, OTA server or other remote relying servers and firmware signing infrastructure. These associated services are considered to be secure and configurated correctly to avoid any secure consideration that may affect the TOE.	Section 3 from [AGD_PRE], Section 4 from [AGD_OPE]
ASSOCIATED_SERVICES	Device security pays attention to the interfaces which connect with these external services, and it is assumed that these associated services are trusted and follow the best security practices.	Section 3 from [AGD_PRE], Section 4 from [AGD_OPE]
TRUSTED_USERS	The platform is expected to be used by trusted users only, thus all the code/firmware running in M4 MCU is expected to be secure.	Section 3 from [AGD_OPE]
PHYSICAL_ATTACKS	Side channel attacks and fault injection attacks are outside the scope of security considerations here.	N/A
UNIQUE_ID	The integrity and uniqueness of the unique identification of the platform must be provided by the platform user during the personalization stage.	Section 2 from [AGD_PRE]

Table 4. Security Objectives for the Operational Environment.

4 Security Requirements and Implementation of the Security Target

4.1 Security Assurance Requirements

The claimed assurance requirements package is **SESIP2,** as defined in Section 5.1.

4.1.1 Flaw Reporting Procedure of the Security Target (ALC_FLR.2)

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to report a flaw and generate any needed update and distribute it, the developer has defined the following procedure:

SLB has defined a Product Security Incident Response Team (PSIRT), formed by multidisciplinary members, including the CSO, product security apps team, software quality, security systems, security governance, security PdM and software security engineers. PSIRT team is the responsible of the flaw remediation and reporting procedure for SLB. This process can be divided into 4 different phases:

- **Reporting:** There is a public web page (https://www.silabs.com/security/report-security-vulnerability) with a form to report all the details regarding the found bug or flaw: Asset(s) affected, weaknesses, severity, PoC… The report is received by the PSIRT team. There is another way of contacting the PSIRT team, sending an email to **product-security@silabs.com**.

- **Evaluation:** After the report has been received, the PSIRT team with the stakeholders determine the security incident priority. If the vulnerability is confirmed, and the PoC successful, the priority determines what are the timers to solve the issue and how it is handled throughout the complete process. Any Software bug associated with PSIRT team are automatically assigned as "critical", so they are on the top of the bugfix list.

- **Solution:** Working with PSIRT, the product team develops a remediation or fix to the flaw or bug. The fixes for the TA or SDF are released as a package on github.

- **Communication:** PSIRT team publishes an advisory for security vulnerabilities that the customers can subscribe to. The time taken to publish advisory will depend on the PSIRT priority and workload. The goal of the communication is to get an accurate fix to the customer as soon as possible, after verifying the information received. Silicon Labs is a CNA (CVE Numbering Authority) thus, all the CVEs found will be published.

To be aware of the communications or advisories, the customer must be registered on https://www.silabs.com and subscribed to the change notification.

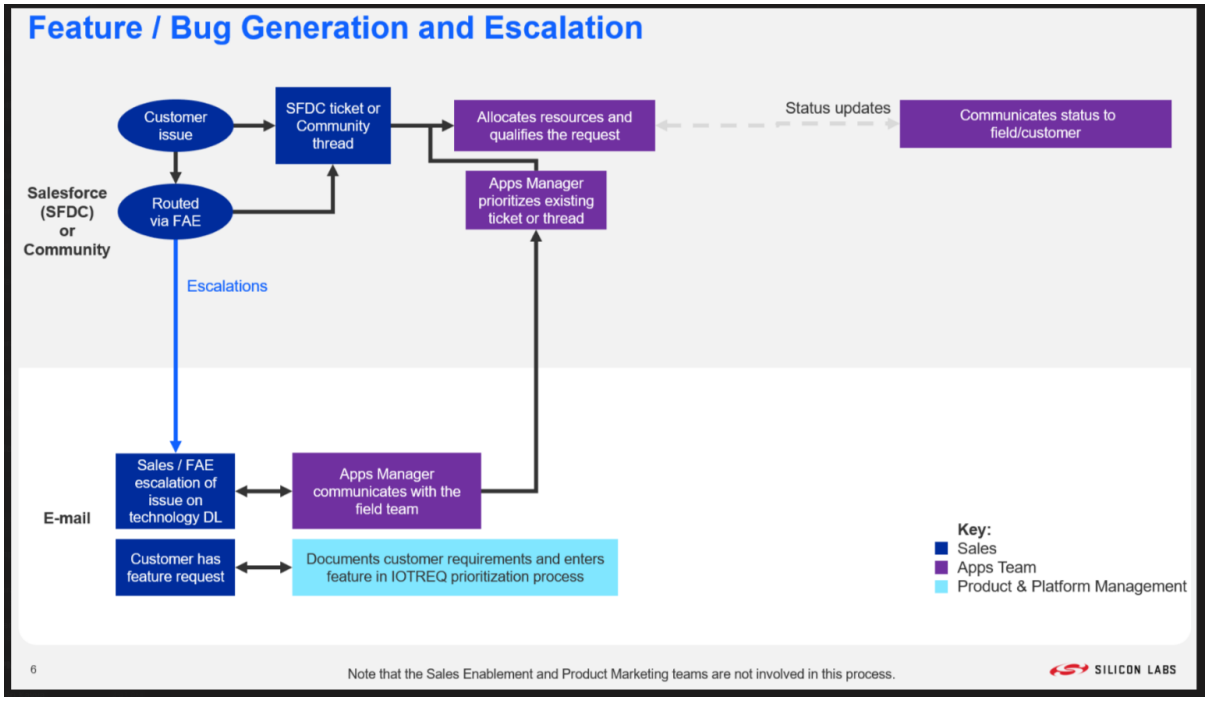

Figure 5. Feature/Bug report and escalation

4.2 Base PP Security Functional Requirements

The platform fulfills the following security functional requirements:

4.2.1 Verification of Platform Identity

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

Conformance rationale:

The platform identity can be obtained with the OPN info. To retrieve the OPN info, it is required to be connected with the TOE through UART interface. Once the connection through UART interface is established, the user can obtain the OPN information sending the command 'o'. After that, the 16 bytes of OPN information will be printed on the terminal, verifying the identity of the platform.

The OPN data is structured as follows:

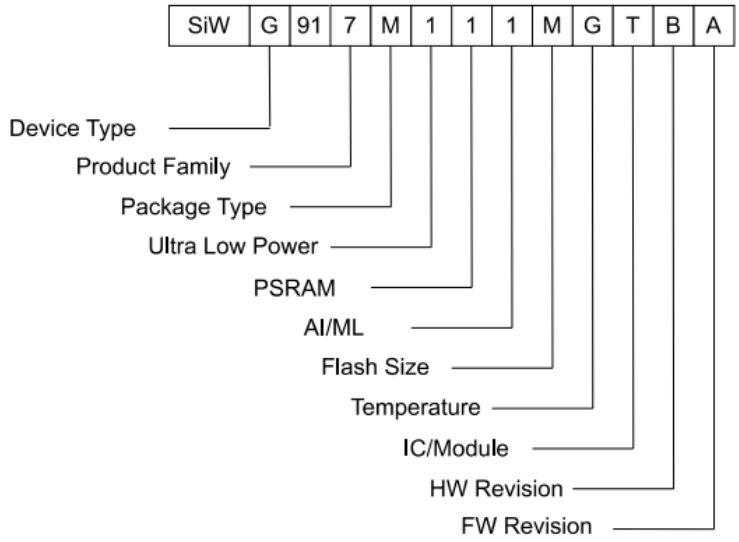

Figure 2.1. Ordering Guide

Figure 6. Ordering guide.

The fields of the OPN and their possible values are defined in the following table:

Field	Options
Device Type	**T**: RCP (Transceiver) **N**: NCP **G**: SoC
Product Family	**7**: Ultra-low power
Package Type	**M**: QFN
Ultra Low Power	**0**: ULP features disabled **1**: ULP Features enabled
PSRAM	**0**: No PSRAM Support **1**: External PSRAM **2**: 2 MB In-package PSRAM **4**: 8 MB In-package PSRAM
AI/ML	**0**: AI/ML features disabled **1**: AI/ML Features enabled

Field	Options
Flash Size	**X**: No Flash **L**: 4 MB In-package Flash **M**: 8 MB In-package Flash
Temperature	**G**: -40°C to 85°C **N**: -40°C to 105°C
IC/Module	**T**: IC Package
HW Revision	**B**: Revision B
FW Revision	**A**: Revision A

Figure 7. OPN decoder.

4.2.2 Verification of Platform Instance Identity

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

Conformance rationale:

The TOE is defined as a SoC, embedded into a SiWG917 board. These 2 components are attached as Figure 2 shows. To identify a specific instantiation of the TOE, the serial number is required. The serial number can be obtained looking at the top of the TOE, where the serial number is printed. The last row with alphanumeric characters is built as YYWWTTTTTT where YY refers to the last two digits of the assembly year, WW refers to the workweek when the device was assembly and TTTTTT corresponds to the manufacturing code. The first letter is the device revision.

Figure 8. Serial number of the TOE.

4.2.3 Attestation of Platform Genuineness

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

Conformance rationale:

A PUF is a unique fingerprint of a chip based on tiny physical variations that occur during manufacturing. These variations generate a raw pattern of bits that, after error correction and processing, produce a stable identifier called the PUF ID. This acts as a secure, unique number for the chip and can be used to derive cryptographic keys.

As all the user keys are encrypted and verified using PUF keys (Master or Unwrap keys), cloning a device will fail in generating the same keys using the PUF on another device, because of the PUF would not be able to generate the same key with the key codes which are specific to the device on which they were generated. The flash can be copied but the firmware in that flash would not run.

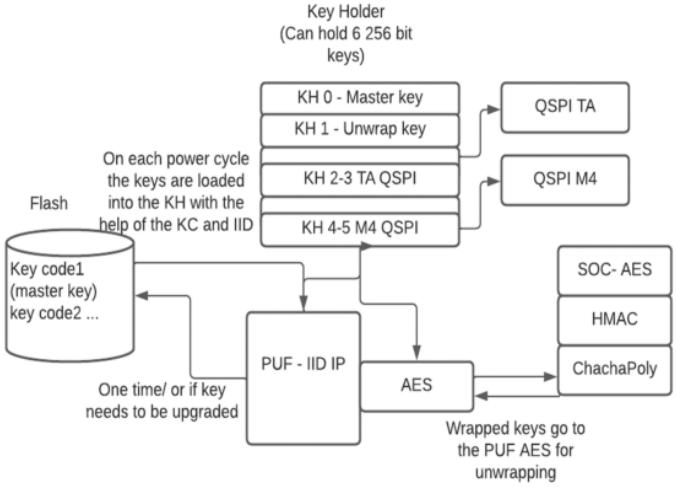

Figure 9. PUF Key Derivation.

For the activation of the PUF, a unique activation code is created and saved to flash. After rebooting the device, the PUF initializes and derives intrinsic keys. Static keys are then generated externally using Simplicity Commander and securely provisioned into flash, wrapped using the PUF-derived keys.

4.2.4 Secure Initialization of Platform

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

Conformance rationale:

On reset, the Security Bootloader configures the module hardware based on the configuration present in the eFuse. It also passes the required information from the eFuse to the Application Bootloader.

The Security Bootloader validates the integrity and authenticity of the firmware in the Flash and invokes the Application Bootloader. It detects and prevents execution of unauthorized software during the boot sequence.

The Bootloader uses public & private key based digital signatures to recognize authentic software. The Security Bootloader provides provision for inline execution (XIP) of encrypted firmware from Flash.

The Bootloader provides 3 flash protection levels which can used to secure different sections of the Flash for different purposes:

- Protection level 1: Stored at manufacturing, not allowed to modify by the Security Bootloader
- Protection level 2: Allowed to modify by the Bootloader only, usually used to maintain secure information used/consumed by Bootloader
- Protection level 3: Allowed to modify by the Bootloader only, usually used to maintain protected firmware images.

The protection levels are written to Flash during the manufacturing process. The write-protection feature prevents the application program from changing the Flash protection levels. The Security configurations can be enabled or disabled during the manufacturing process.

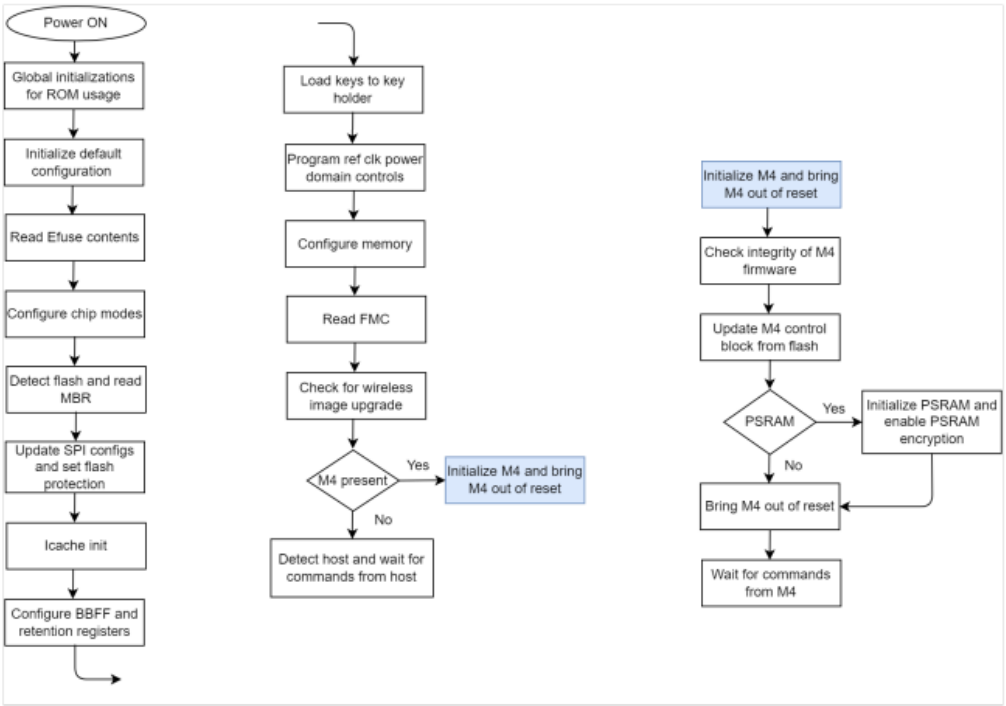

Figure 10. Explanation of TA bootloader flow.

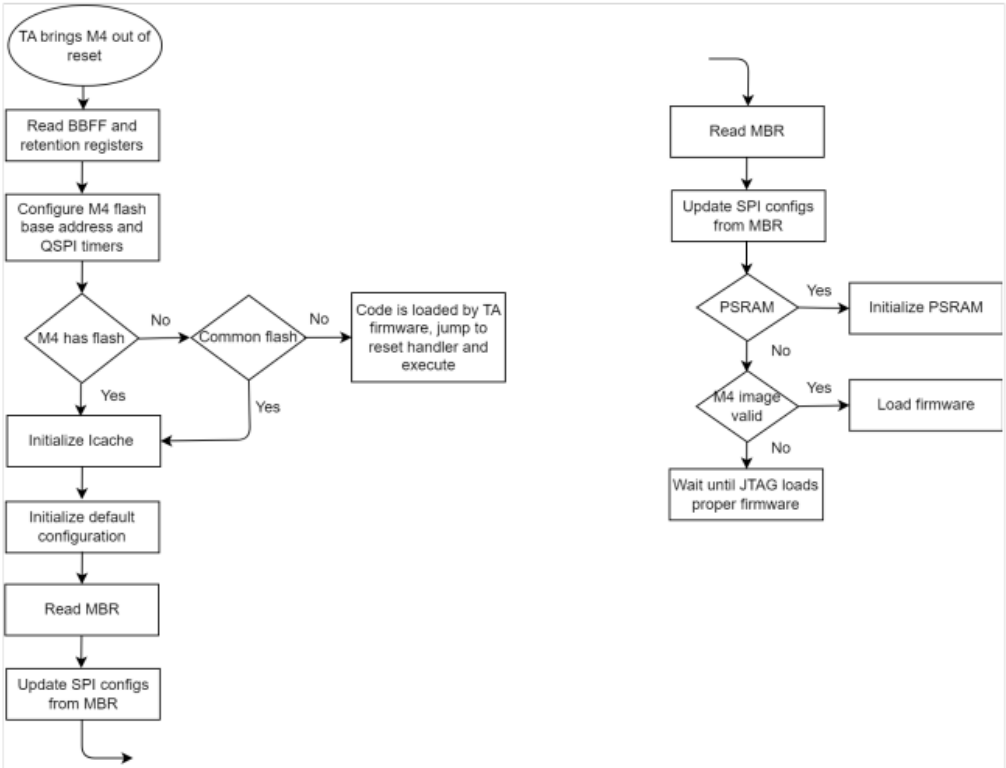

Figure 11. Explanation of M4 bootloader flow.

4.2.5 Attestation of Platform State.

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

Conformance rationale:

The TOE has only 2 modes; the ISP mode and the normal execution mode. The ISP mode runs in the bootloader, and it is possible to check this state with the host boot options, which are available through UART interface. If the TOE is not in ISP mode, then it is in normal execution mode.

The TOE can be initialized in ISP mode using the ISP button. This mode is only used to programming or reprogramming the flash through boot loader, using UART, SPI, and SDIO interfaces. Boot loader can be requested to boot in ISP mode by pulling down a specific GPIO pin and this pin has to be left unconnected during reset for the boot loader to bypass ISP and execute the code that is present in flash.

Normal execution mode is the mode where the TOE will be operating when on use and the flash is not being upgraded/modified.

4.2.6 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 way the TOE has for updating to a newer version is using a different version of the firmware. This mechanism can be used by the application to initiate an update.

For this process to begin, an authenticity check is mandatory. The new firmware image is checked, verifying its integrity. The bootloader updates the firmware image after successfully validating the authenticity and integrity of the image.

The Bootloader also supports transparent migration to a wirelessly updated image and protection against failures by providing recovery mechanisms.

This mechanism has 3 different security models: Message Integrity Check (MIC) + encryption, MIC + encryption + signature and only signature. Furthermore, a fourth model is available, the no security model, where the default CRC of the image it's within the RPS header.

Besides the bootloader mechanism to update the firmware, thus the version, of the software, another mechanism is contemplated, the update via OTA (Over the Air). Within this mechanism, update via HTTP/S and update via M4 as a Host is possible.

For the firmware update, the following steps are executed:

1. The device boots into the bootloader.
2. An RPS file containing an application image is transmitted from the host to the device. The device saves the image data received into the download location of the flash.
3. After the complete image is transmitted, the received image's integrity and authenticity is verified using CRC, MIC or Signature based check, depending on the control flags of the RPS and the MBR configuration.
    a. First the image's version number is verified to be equal to or greater than current FW version. If the version is less than current version, the update is ignored. The version number is 32bits. The whole 32 bits is compared with the current version.
    b. The image's size is verified to be within the range of the maximum allocated image size depending on the type of image -TA or M4.
    c. If MIC check is enabled then the key for the OTA key is loaded based on the image type - TA or M4. MIC is calculated for the entire image including header using the OTA key using the AES CBC mode. If the image is encrypted, then MIC is calculated by first decrypting the encrypted image with the OTA key. The decryption mode to be used is part of the flags which can be CTR or XTS mode.
    d. If the CRC check is enabled instead of MIC, then CRC is calculated and verified.
    e. Signature is calculated using the public key based on the FW type - TA or M4. The algorithm is ECDSA-P256. If signature check is enabled, then:
        i. If MIC check is also enabled for the RPS, then signature is calculated only for the header of the RPS.
        ii. If MIC is not enabled, then signature is calculated for the entire image including the header.
4. After the image is verified, the Bootloader transfers the image from download location to the execution/ target location. If the image encryption is enabled (security configuration from MBR) and the image is encrypted (control flag bit of RPS), decryption is performed during the process of transferring and parsing the RPS file.
5. Finally, the Bootloader updates FMC data which contains the new image's details such as its execution location, size, the CRC, MIC or Signature values (depending on the MBR configuration) and the version number of the image.

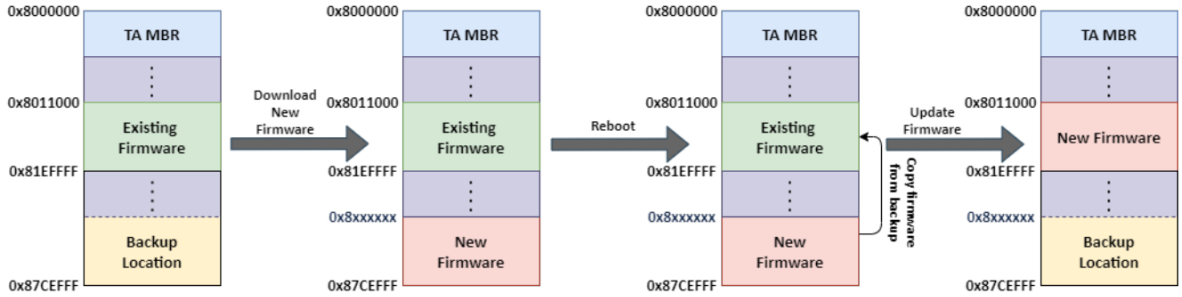

Figure 12. TA firmware update process.

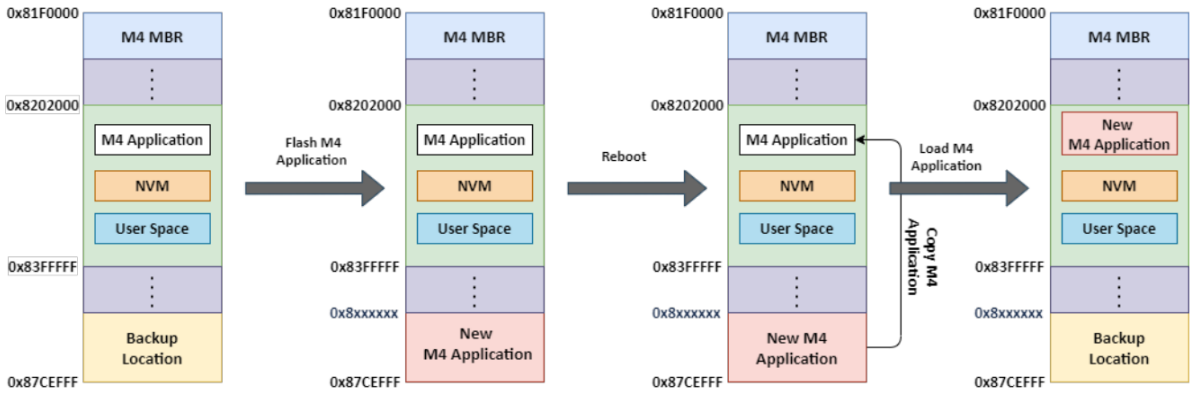

Figure 13. M4 Application update process.

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

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

Conformance rationale:

The Secure Zone is hardware enforced isolation between the trusted and non-trusted modules in the system. Secure zone protects the secure assets residing in secure execution environment by restricting direct access. It also provides a secure execution environment to store confidential data and to run secure applications. The Bootloader configures Secure Zone, secure firmware upgrade and secure bootup in "Secure Zone enabled" mode. This mode is programmed during the manufacturing process. All of TASS is secure execution environment and secure zone is enabled using an EFUSE config bit **disable_m4_access_frm_tass_sec.**

Network Processor (NWP) subsystem is the secure zone. The secure zone is enabled by programming the disable_m4_access_frm_tass_sec in CHIP_CONFIG_MCU register. When secure zone is enabled, all the accesses to NWP subsystem from MCU is disabled. This is achieved in Hardware by transferring all the Advanced High-performance Bus (AHB) transactions from MCU via MCU-NWP AHB bridge to NWP miscellaneous config registers. So MCU will not be able to configure or access anything in NWP subsystem other than NWP miscellaneous config registers as all the transactions are bypassed.

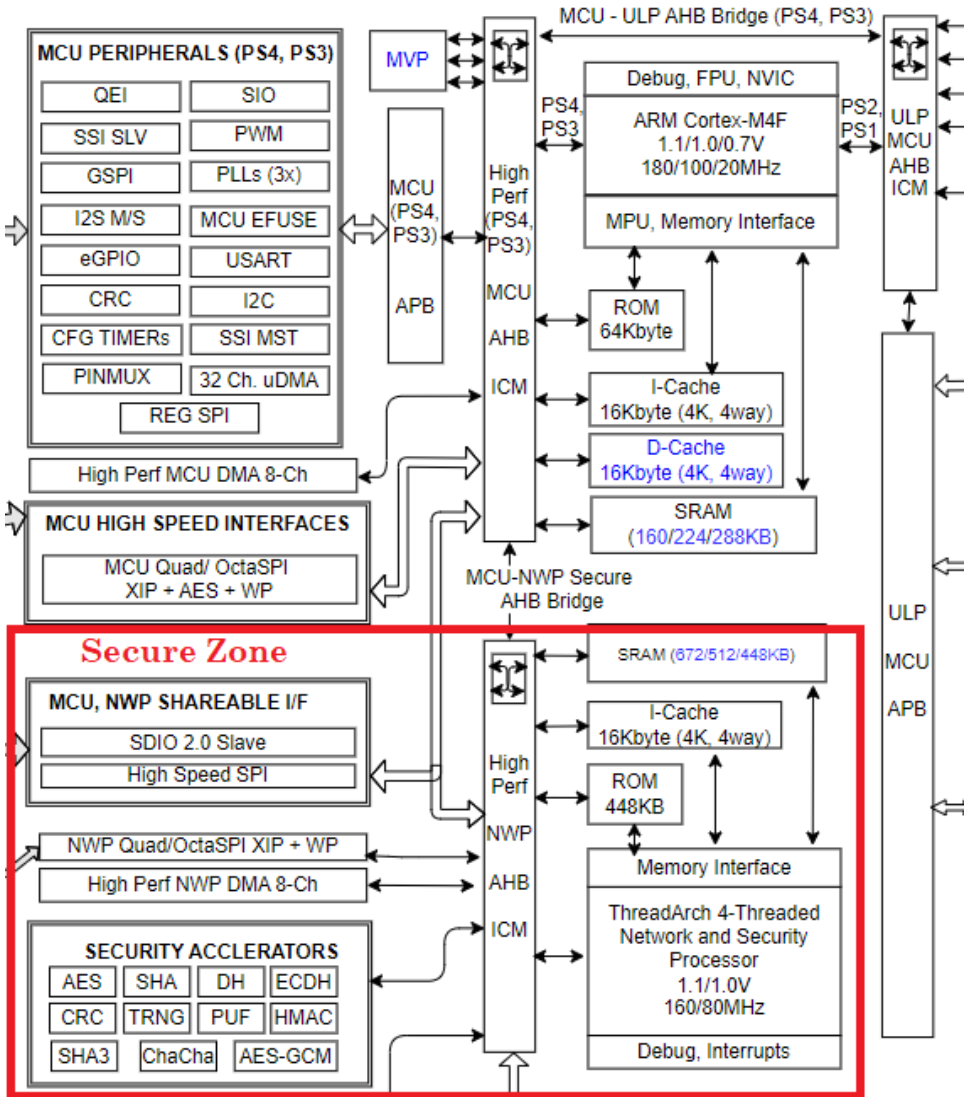

Figure 14. SPE and NSPE scheme.

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

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

Conformance rationale:

The firmware of the platform is controlled by SLB and an API is used by the M4 processor to communicate with the TA, to avoid direct access to the secure functionality. From the M4 processor, the wireless subsystem is only accessible through the API and those functions are executed in an environment controlled by the developer. Because of the existence of this API, the access to the RoT is not direct and it is isolated from the application root of trust services.

4.2.9 Cryptographic Operation

The platform provides the application with **Operations in Table 5** functionality with **algorithms in Table 5** as specified in **specifications** in **Table 5** for **key lengths** described in **Table 5** and **modes** described in **Table 5.** For detailed information about key lengths refer to document [UG574].

Algorithm	Operations	Specification	Key Lengths	Modes
AES	Encryption	NIST FIPS 197 [NIST_197]	16 bytes 32 bytes	CTR, XTS
AES	MIC Calculation	NIST FIPS 197 [NIST_197]	16 bytes 32 bytes	CMAC
ECDSA	Sign Verification	NIST FIPS 186-3 [NIST_186-3]	96 bytes	P-256
ECDSA	Secure Attestation Sign	NIST FIPS 186-3 [NIST_186-3]	240 bytes (PEM format)	P-256

Table 5. Cryptographic operations

4.2.10 Cryptographic Random Number Generation

The platform provides the application with a way based on R distinct oscillator rings and each ring is composed of I inverters to generate random numbers to as specified in NIST-800-90B and AIS31.

Conformance rationale:

The user can use PSA Crypto APIs that Silicon Labs provide as part of the SDK to request TRNG values. These requests are routed to TA Sub system which actually returns the random data. The TRNG is NIST-800-22, AIS31 and NIST-800-90B compliant.

TRNG entropy source is based on the use of R distinct oscillator rings, each ring is composed of I inverters. Each inverter introduces its own propagation delay, and the oscillation period of the ring is determined by the sum of those delays across all inverter stages. The analog signal going out of the binary XOR-tree is converted into a digital signal by sampling it at a regular clock frequency.

The TOE includes two oscillators that can operate either synchronously for simulation purpose (Pseudo-Random generator) or asynchronously free running for NDRNG, depending on the configured settings. In For more information, refer to [BA431].

4.2.11 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in **cryptographic algorithms in** Table 6 as specified in specifications in Table 6 for key lengths described in **Table 6.**

ID	Algorithm	Specification	Key Lengths	Generation	Storage
Master KEY	AES-256	NIST FIPS 197 [NIST_197]	32 bytes	Generated at runtime using PUF and a 52-byte key code stored in flash	52 bytes key code used to initialize key in Key Holder (Permanent)
Unwrap KEY	AES-256	NIST FIPS 197 [NIST_197]	32 bytes	Generated at runtime using PUF and a 52-byte key code stored in flash	52 bytes key code used to initialize key in Key Holder (Permanent)
TA FW key 1	AES-128/256 CTR or XTS mode	NIST FIPS 197 [NIST_197]	16/32 bytes	Generated using PUF and a 52-byte key code stored in flash	Flash (Updatable)

				and wrapped with Master Key	
TA FW key 2	AES-128/256 CTR or XTS mode	NIST FIPS 197 [NIST_197]	16/32 bytes	Generated at runtime using PUF and a 52-byte key code stored in flash and wrapped with Master Key	Flash (Updatable)
M4 FW key 1	AES-128/256 CTR or XTS mode	NIST FIPS 197 [NIST_197]	16/32 bytes	Generated using PUF and a 52-byte key code stored in flash and wrapped with Unwrap Key	Flash (Updatable)
M4 FW key 2	AES-128/256 CTR or XTS mode	NIST FIPS 197 [NIST_197]	16/32 bytes	Generated using PUF and a 52-byte key code stored in flash and wrapped with Unwrap Key	Flash (Updatable)
M4-OTA key	AES-256	NIST FIPS 197 [NIST_197]	32 bytes	Generated externally with Simplicity Commander and wrapped with Unwrap Key	Flash (Permanent)
M4-public key	ECDSA	NIST FIPS 186-3 [NIST_186-3]	91 bytes + 5 bytes padding added to make key size multiple of 16 for AES encryption.	Generated externally with Simplicity Commander and wrapped with Unwrap Key	Flash
Attestation private	ECDSA	NIST FIPS 186-3 [NIST_186-3]	240 bytes	Generated externally with Simplicity Commander and wrapped PUF derived intrinsic keys	Flash
OTP Symmetric key	AES-128	NIST FIPS 197 [NIST_197]	16 bytes	Generated externally with Simplicity Commander	OTP (Immutable)
OTP Public key	ECDSA	NIST FIPS 186-3 [NIST_186-3]	91 bytes	Generated externally with Simplicity Commander	OTP (Immutable)
TA public key	ECDSA	NIST FIPS 186-3 [NIST_186-3]	91 bytes + 5 bytes padding added to make key size multiple of 16 for AES encryption.	Generated externally with Simplicity Commander and wrapped with Master Key	Flash

TA OTA key	AES-256	NIST FIPS 197 [NIST_197]	32 bytes	Generated externally with Simplicity Commander and wrapped with Master Key	Flash (Permanent)

Table 6. Cyptographic key generations

4.2.12 Cryptographic KeyStore

The platform provides the application with a way to store the 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, wrapping/unwrapping keys and MIC calculation and verification

Conformance rationale:

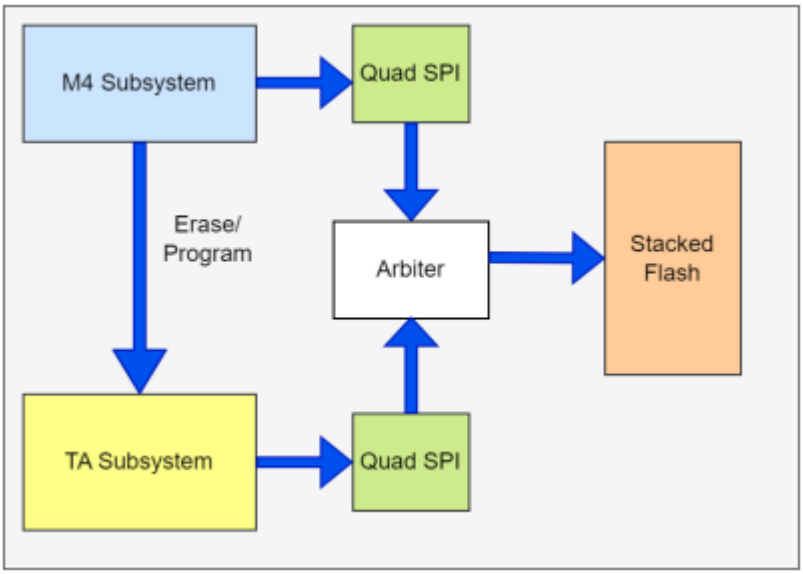

Figure 15. Common flash usage scheme of the TOE.

In the TOE, Flash is shared between both TA and M4 processors. Flash Initialization, configuration, program and erase can be done only by TA processor. M4 processor can do only instruction fetching in direct access mode. Flash memory is divided into two regions, one each for the processor. M4 can only read M4 assigned memory region. TA has no restriction and it can access to the complete Flash memory.

The keys are stored in flash and only accessible by TA. Even if M4 Application needs to cipher data using one of the M4 keys, Silicon Labs provides PSA Crypto APIs which can be used with Key ID where TA SS will use the appropriate key to perform the cipher operation. M4 will never get the location of the key nor the plain key in its space.

In addition, all keys stored in flash are encrypted using their corresponding PUF-derived intrinsic keys, Master Key for TA and Unwrap Key for M4, and are appended with a MIC to ensure authenticity and integrity.

4.2.13 Secure Confidential Storage

The platform ensures that all data stored, is protected to ensure its confidentiality, integrity, authenticity, and binding to the platform instance.

Conformance rationale:

As previously described, the TOE can establish a secure zone, which enables secure storage of data within a controlled environment, in such a way that not even the application can compromise the authenticity, integrity, confidentiality of this data. This region is composed of the following components: ROM, Cache and SRAM.

Access to these memory areas is managed through the memory interface, which is protected by the MPU, which defines memory attributes for different memory regions.

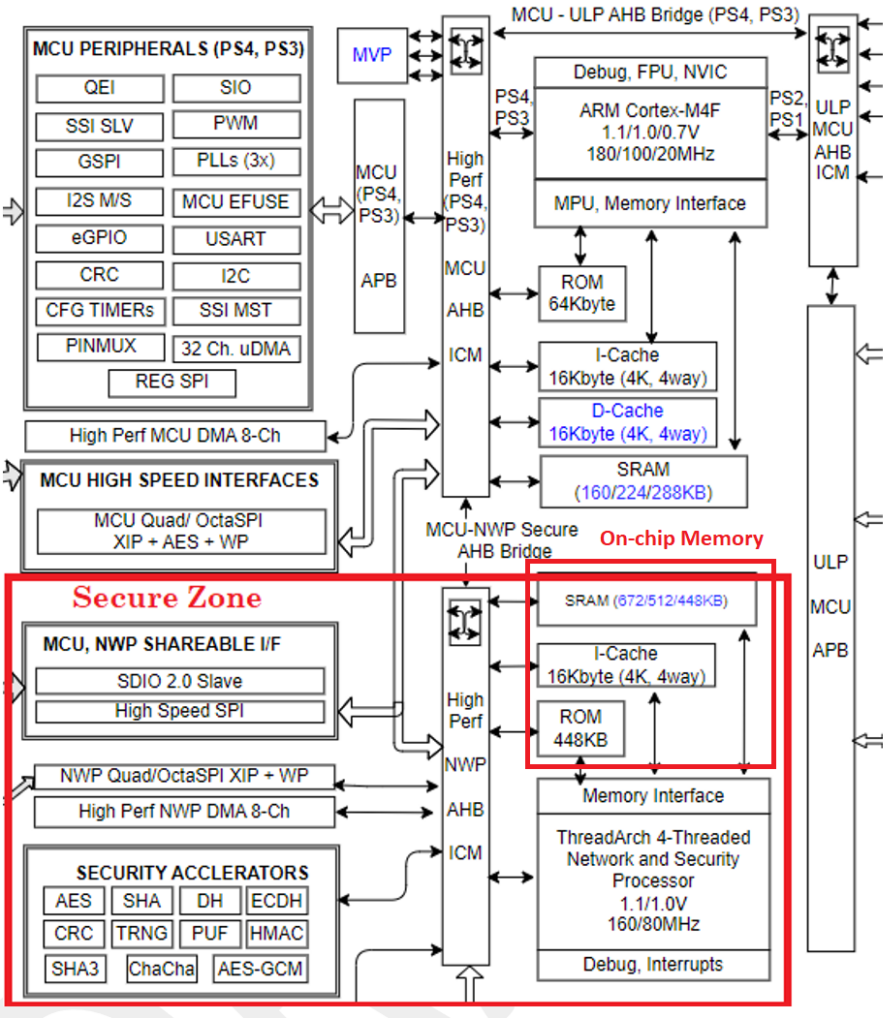

Figure 16. On-chip memory of the TOE.

Access to the SRAM is logically partitioned between the M4 core and the Trusted Area. The TA has full access to the entire SRAM, whereas the M4 is restricted to a controlled region. Communication between the M4 and the TA is managed through a secure API, preventing unauthorized access to sensitive data. The memory partitioning is configurable, allowing flexible allocation based on the specific needs of each domain, while maintaining strong isolation and security.

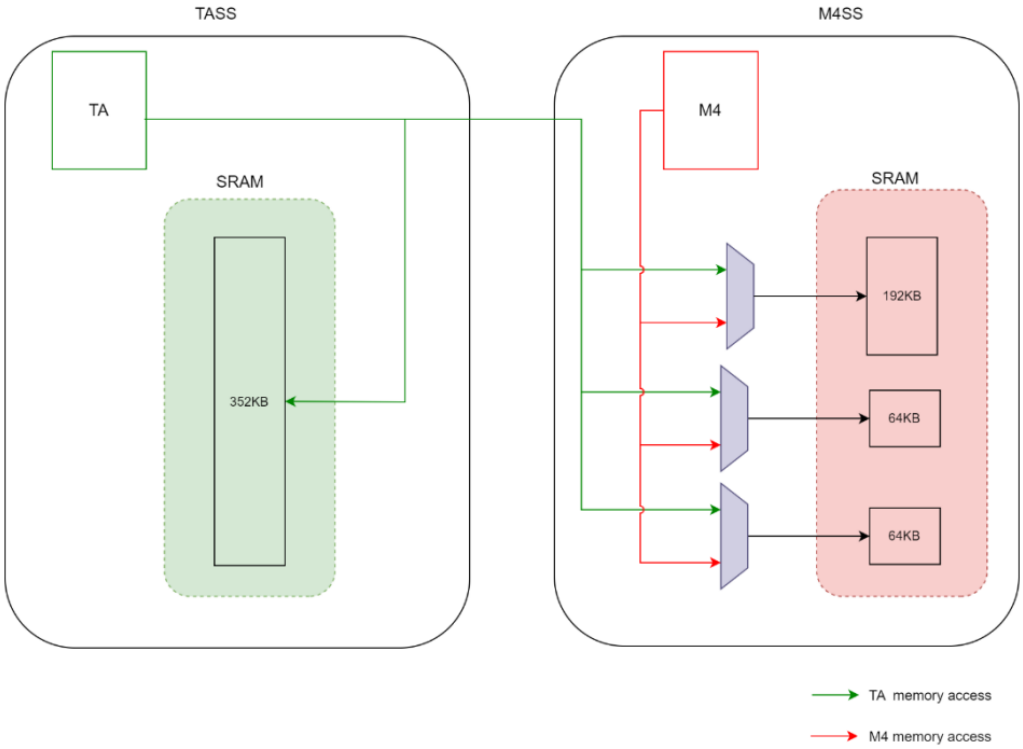

Figure 17. SRAM usage scheme of the TOE.

For software execution directly from Flash instead of copying it into RAM Images are saved in encrypted format and decrypted using device-specific PUF intrinsic keys while executing. In-line decryption based on-the-fly AES engine (based on PUF keys). Multiple protection levels can be set for flash, including unmodifiable.

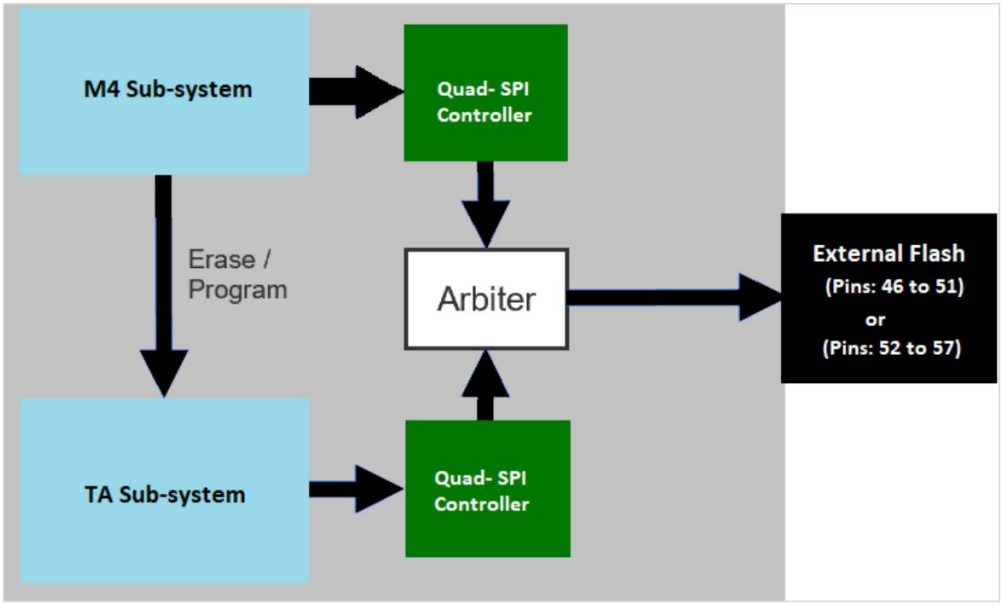

Figure 18. Common Flash usage scheme of the TOE.

For Flash storage, the two processors access flash memory over dedicated Quad-SPI (QSPI) with an arbiter in between that helps in arbitration for flash accesses. Though the flash memory is shared between M4 and TA, TA performs only low-level operations while M4 supports only flash read operation on the flash memory. As with the SRAM, for operations such as erasing and writing, M4

requests TA through a command and sends the data for the write operation. The M4 uses QSPI interface access and communicates with TA.

5 Mapping and sufficiency rationales

This ST and associated TOE provide exact conformance to [PSA-EM-L2].

5.1 Assurance

The assurance activities defined in [PSA-EM-L2] fulfil the SESIP2 activities. In particular, the required source code review, vulnerability analysis and testing to an equivalent of 25 person-days of the [PSA-EM-L2] is applicable.

<table>
<tr><th>Assurance Class</th><th>Assurance Family</th><th>Covered by</th></tr>
<tr><td rowspan="8">ASE: Security Target evaluation</td><td>ASE_INT.1 ST Introduction</td><td>Title and Section 2. Introduction and 2.2 Platform reference.</td></tr>
<tr><td colspan="2"><u>Rationale:</u>
The ST reference is in the Title, the TOE reference in subsection 2.2 Platform reference, the TOE overview and description in subsection 2.4 Platform functional overview and description.</td></tr>
<tr><td>ASE_OBJ.1 Security requirements for the operational environment</td><td>Section 3. Security Objectives for the Operational Environment</td></tr>
<tr><td colspan="2"><u>Rationale:</u>
The objectives for the operational environment in section 3 Security Objectives for the Operational Environment refers to the guidance documents.</td></tr>
<tr><td>ASE_REQ.3 Listed Security requirements</td><td>Section 4.2 Base PP Security Functional Requirements.</td></tr>
<tr><td colspan="2"><u>Rationale:</u>
All SFRs in this ST are taken from [SESIP].
Verification of Platform Identity is included in subsection 4.2.1
Verification of Platform Instance Identity is included in subsection 4.2.2
Attestation of Platform Genuineness is included in subsection 4.2.3
Secure Initialization of Platform is included in subsection 4.2.4
Attestation of Platform State is included in subsection 4.2.5
Secure Update of Platform is included in subsection 4.2.6
Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) is included in subsection 4.2.7
Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services) is included in subsection 4.2.8
Cryptographic Operation is included in subsection 4.2.9</td></tr>
</table>

	• Cryptographic Random Number Generation is included in subsection **4.2.10** • Cryptographic Key Generation is included in subsection **4.2.11** • Cryptographic KeyStore is included in subsection **4.2.12** • Secure Confidential Storage in subsection **4.2.13**	
	ASE_TSS.1 TOE Summary Specification	Section **4.2 Base PP Security Functional Requirements.**
	Rationale: All SFRs are listed per definition, and for each SFR the implementation and verification are defined in its correspondent subsection.	
ADV: Development	ADV_FSP.4 Complete functional specification	Met in [ADV_FSP]
	Rationale: [ADV_FSP] provides the list of TSFIs that are present in the TOE, alongside the non-TSFIs. Moreover, it also includes a list of errors associated to the UART TSFI, and the mapping between interfaces and SFRs.	
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Met in [AGD_OPE] document
	Rationale: [AGD_OPE] provides the features of the platform, its operational modes, external interfaces and available commands over each interface, providing enough guidance on how to securely operate the platform.	
	AGD_PRE.1 Preparative procedures	Met in [AGD_PRE] document
	Rationale: [AGD_PRE] provides guidance on the secure acceptance of the TOE, a list of all guidance documentation, preparation of operational environment, and possible error codes. Therefore, [AGD_PRE] is considered to provide enough guidance on the procedures and steps that must be followed for the secure preparation of the TOE.	
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section **4.1.1 Flaw Reporting Procedure of the Security Target**
	Rationale: Section **4.1.1 Flaw Reporting Procedure of the Security Target** describes all the procedures used to report, track security flaws and generate any needed update and distribute it.	
ATE: Tests	ATE_IND.1 Independent testing: conformance	Performed by evaluation Laboratory
	Rationale: The evaluation laboratory will determine whether the TOE meets or not the requirements by performing independent testing.	

AVA: Vulnerability Assessment	AVA_VAN.2 Focused vulnerability analysis	Performed by evaluation Laboratory
	Rationale: The evaluation laboratory will perform the vulnerability analysis.	

Table 7: Assurance Mapping and Sufficiency Rationales

5.2 Functionality

PSA security Function	Covered by SESIP SFR
F.INITIALIZATION	Secure Initialization of Platform
F.SOFTWARE_ISOLATION	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)
	(Optional) Software Attacker Resistance: Isolation of Application Parts (between each of the Application Root of Trust services)
F.SECURE_STORAGE	Secure Encrypted Storage (internal storage)
	Secure Storage (internal storage)
	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)
	Not covered by any SESIP SFR. Note added in “Secure Encrypted Storage”.
	Secure External Storage
F.FIRMWARE_ UPDATE	Secure Update of Platform

F.SECURE_STATE	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services
	Partially covered by the SFR “Secure initialization of platform” and “Secure update of platform”.
	Limited Physical Attacker Resistance
F.CRYPTO	Cryptographic Operation
	Cryptographic KeyStore
	Cryptographic Random Number
	Cryptographic Key Generation
F.ATTESTATION	Verification of Platform Identity
	Verification of Platform Instance Identity
	Attestation of Platform Genuineness
	Attestation of Platform State
F.AUDIT	Audit Log Generation and Storage

F.DEBUG	Secure Debugging

6 References

[PSA] SESIP Profile for PSA certified level 2. version 2.0 REL, release number 01 28/03/20242

[SESIP] GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.2, July 2023

[PSA-SESIP-L2] SESIP Profile for PSA Certified Level 2, version 1.0 REL 02, November 2022.

[BA431] BA431 - Non Deterministic Random Number Generator Datasheet Version: 4.11 14/09/2018

[DATASHEET] SiWG917 SoC Single Chip Wi-Fi® and Bluetooth® LE Wireless Secure MCU Solutions. Version 0.51, 20/12/2023.

[UG562] UG562: SiWG917 Single-band Wi-Fi and BLE with 8 MB Flash Radio Board User's Guide. Version 1.2, 20/12/2023.

[UG574] UG574: SiWx917 SoC Manufacturing Utility User Guide. Version 1.1 30/01/2024.

[UG519] UG519: Custom Part Manufacturing Service User's Guide. Version 0.1, 24/11/2021.

[WC_SDK_v3] Developing with WiSeConnect SDK v3.x with the SiWx91x Host(https://docs.silabs.com/wiseconnect/3.1.3/wiseconnect-developers-guide-developing-for-silabs-hosts/)

[API] API reference guide v3.3.0. (https://docs.silabs.com/wiseconnect/3.3.0/wiseconnect-api-reference-guide-summary/).

[AN1416] SiWx917 SoC memory map, version 1.0, 11/2024.

[AN1429] SiWx917 SoC throughput, version 1.2, 26/12/2023.

[AN1430] SiWx917 SoC low power Application Note, version 1.0 , 11/01/2024.

[AN1431] SiWx917 SoC firmware update Application Note, version 1.0, 22/01/2024.

[AN1335] RS9116 and SiWx917 Crystal Selection Guide, version 1.2, 20/12/2023.

[AN1423] SiWx917 RF Matching and Layout Design Guide, version 0.1, 20/12/2023.

[AN1428] SiWx917 Secure Debug, version 0.1, 16/02/2024.

[AN1436] SiWx917 QMS Crystal Calibration, version 1.0, 20/12/2023.

[AN1437] SiWx917 RF Regulatory Testing, version 0.1, 20/12/2023.

[AN1439] SiWx917 Hardware Debugging Guidelines, version 1.0, 17/01/2024.

[AN1440] SiWx917 Gain Offset calibration, version 0.1, 20/12/2023.

[AN1448] SiWx917 Power Supply Architecture and Configurations, version 1.0, 03/05/2024.

[AN1491] SiWx917 RF Transmit & Receive Measurements, version 0.1, 03/07/2024.

[NIST_197] NIST FIPS 197 Specification for the ADVANCED ENCRYPTION STANDARD (AES), Nov 2001.

[NIST_186-3] NIST FIPS PUB 186-3 Digital Signature Standard (DSS), June 2009.

[AGD_PRE] AGD_PRE for SiWG917X1X SoC Single Chip Wi-Fi® and Bluetooth® LE Wireless Secure MCU Version 1.2

[AGD_OPE] AGD_OPE for SiWG917X1X SoC Single Chip Wi-Fi® and Bluetooth® LE Wireless Secure MCU Version 1.2

[ADV_FSP] ADV_FSP for SiWG917X1X SoC Single Chip Wi-Fi® and Bluetooth® LE Wireless Secure MCU Version 0.3

7 Appendix: SFRs by PSA Certified Levels

The following table summarizes the required SFRs according to PSA Certified Levels. In this table, Y stands for mandatory SFR, O for optional SFR and N/A for not applicable for this level.

PSA Certified Level	Level 2	Level 3	Level 3 iSE/SE or Level 4 iSE/SE
Scope	PSA-RoT	PSA-RoT	Trusted Sybsystem
Evaluation Methodology	SESIP Level 2	SESIP Level 3	SESIP Level 3
Attack Resistance	0-15	0-20	0-20 (Level 3) 0-24 (Level 4)
Mandatory SFRs			
Verification of Platform Identity	Y	Y	Y
Verification of Platform Instance Identity	Y	Y	O
Attestation of Platform Genuineness	Y	Y	O
Secure Initialization of Platform	Y	Y	Y
Attestation of Platform State	Y	Y	O
Secure Update of Platform	Y	Y	Y
Physical Attacker Resistance	N/A	Y	Y
Software Attacker Resistance: Isolation between SPE and NSPE	Y	Y	Y
Software Attacker Resistance: Isolation between PSA-RoT and Application RoT	Y	Y	Y
Cryptographic Operation	Y	Y	Y
Cryptographic Random Number Generator	Y	Y	Y
Cryptographic Key Generation	Y	Y	Y
Cryptographic KeyStore	Y	Y	Y
Secure Storage (At least one of Secure Encrypted Storage, Secure Confidential Storage or Secure Trusted Storage)	Y	Y	O

Additional SFRs			
Secure Communication Support	N/A	N/A	(1)
Optional SFRs			
Audit Log Generation and Storage	O	O	O
Software Attacker Resistance: Isolation of Application parts (between each of the ARoTs)	O	O	

Table 8 SFRs by PSA Certified Levels

For iSE/SE, the Secure Communication Support SFR marked with (1) must be included into the security target if protection of the link between the Host Platform and the iSE/SE relies on cryptographic means (as opposed to access control means).