EFR32FG23 Wireless SoC Family SESIP Security Target for PSA Certified™ Level 3

Based on [SESIP] methodology, version “Public Release v1.1”

Document number:	-
Version:	0.4
Release Number:	01
Author	Silicon Labs, Inc
Date of Issue:	02/12/2021

Table of Contents

1 Introduction

The Security Target contains the platform and its security properties evaluated against SESIP Assurance Level 3. Potential customer can rely on the security functionality of the platform as long as the requirement in the security objectives for the environment are fulfilled.

1.1 ST Reference

Please refer to the title page

1.2 SESIP Profile Reference

Reference	Value
PP Name	SESIP Profile for PSA Certified Level 3
PP Version	V1.0BET01
Assurance Claim	SESIP Assurance Level 3 (SESIP 3)
Optional and additional SFRs	• Secure Encrypted Storage (internal storage) • Secure Storage (internal storage) • Secure External Storage • Residual information purging • Secure debugging

Table 1: SESIP Profile Reference

1.3 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	
TOE Name	EFR32FG23	
TOE Version	Revision B	
TOE Identification	Chip name and version	EFR32FG23B…-B (Revision B)
	PSA-RoT name and version	SE Firmware V2.1.6
TOE type	Secure element subsystem of a SoC	

Table 2: Platform Reference

1.4 Included Guidance Documents

The following documents are included with the platform:

Reference	Name	Version
[1]	EFR32xG23 Wireless Gecko Reference Manual	Revision 0.5, August 2021
[2]	EFR32FG23 Wireless SoC Family Data Sheet	Revision 0.5, August 2021
[3]	AN1218: Series 2 Secure Boot with RTSL	Revision 0.3, July 2020
[4]	AN1190: Series 2 Secure Debug	Revision 0.4, September 2021
[5]	EFR32 Wireless Gecko EFR32FG23 Errata	Revision 0.4, September 2021
[6]	AN1222: Production Programming of Series 2 Devices	rev 0.5, September 2021
[7]	UG162: Simplicity Commander Reference Guide	Rev. 2.1
[8]	EFR32FG23 Wireless SoC Family SESIP Configuration Item List	v0.3, 2 December 2021
[9]	PS1012 – Security Vulnerability Disclosure Policy	Rev C
[10]	CRISIS006 - Product Security Incident Response plan (PSIRP)	Rev H

Table 3: Guidance Documents

1.5 Platform Functional Overview and Description

1.5.1 TOE Type

The TOE is a secure element inside an SoC with its own internal eFuse, ROM, SRAM, PUF, Crypto accelerator, etc. The SE is isolated from the rest of the system using a mailbox interface. The application processor can request service from the SE using API provided by Gecko SDK Suite.

1.5.2 TOE Physical Scope

The scope of this evaluation is the secure element subsystem of the xG23 MCU. This is implemented by a dedicated Arm M0+ CPU with its corresponding hardware such as TRNG, Crypto Accelerator, Mailbox, and Memory Protection Unit. The scope also includes the firmware running on the secure subsystem. The TOE is pre-integrated in a SoC. It is delivered as a subsystem within a chip. The SE firmware can either be pre-integrated in the chip or it can be downloaded from Silicon Labs, Inc website in an encrypted update binary form.

1.5.3 TOE Logical Scope

The scope for a PSA Certified Level 3 Security evaluation, or Target of Evaluation (TOE), is the combination of the trusted hardware and firmware components implementing a PSA-RoT with the Security Functional Requirements stated in this document. PSA Certified Level 3 scope is identical to PSA Certified Level 2.

The Chip security evaluation scope includes the following components as described in [PSA-SM]:

- Immutable Platform Root of Trust, in this case, the Boot ROM, the isolation hardware, and hardware based security lifecycle management and enforcement, and the root parameters stored in the eFuse.
- Updateable Platform Root of Trust, for example, can include the Main Bootloader code, the code that implements the SPE Partition Management function, and the code that implements the PSA defined services such as attestation, secure storage, and cryptography. In this TOE, this is called SE Firmware

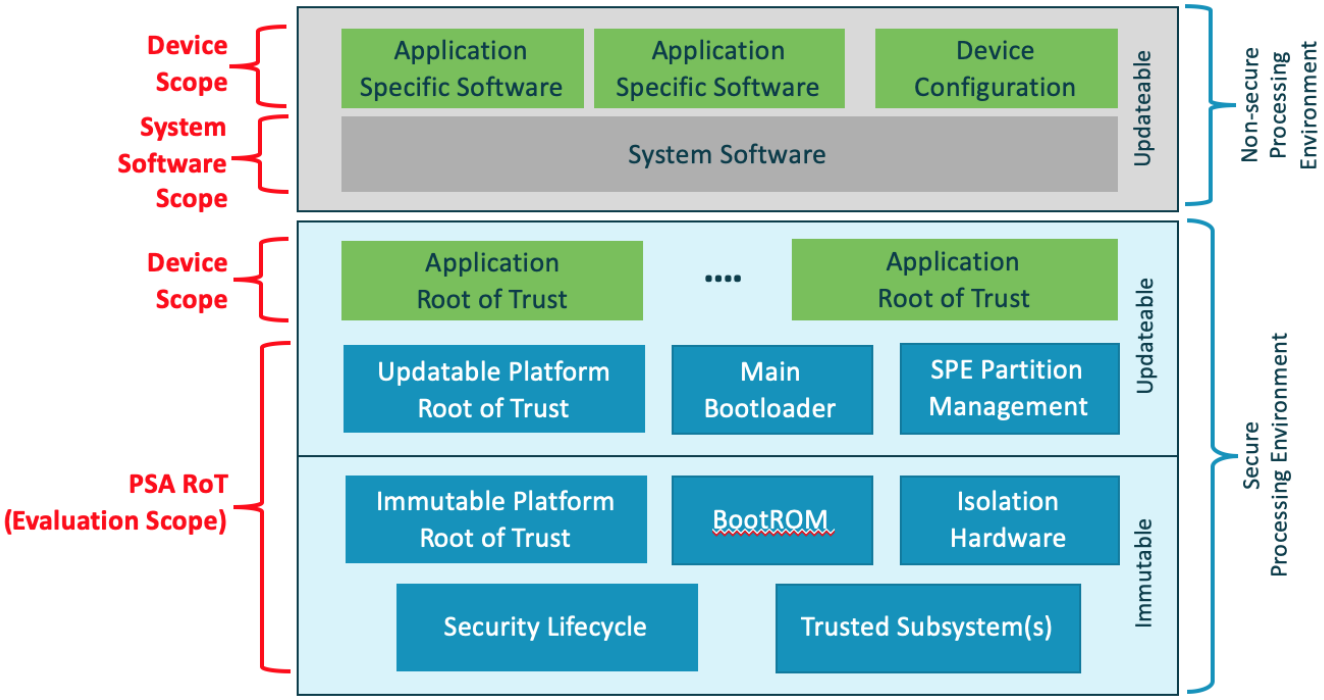
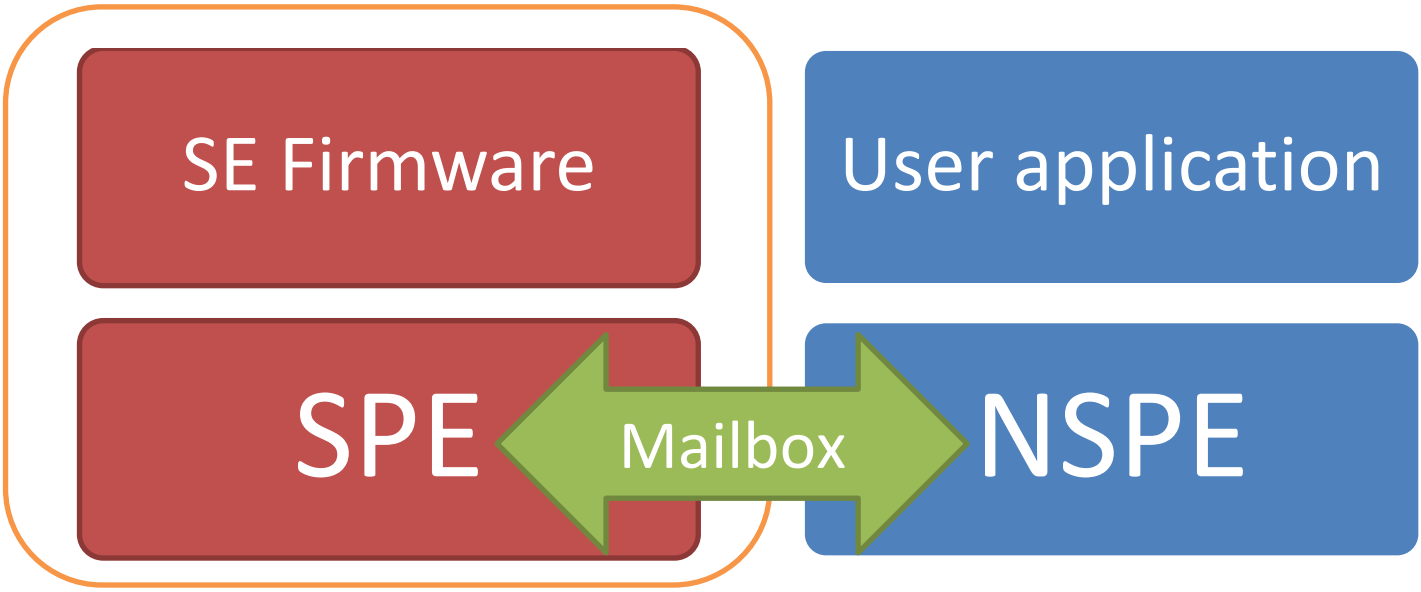


Figure 1: Scope of PSA Certified Level 3



1.5.4 Usage and Major Security Features

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

- A Secure Processing Environment (SPE) isolated by hardware mechanisms to protect critical services and related assets from the Non-Secure Processing Environment. This is implemented by the separate M0+ processor.
- 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. This is implemented by the combination of ROM code and eFuse.
- 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 Attestation key.
- A Security Lifecycle for the SPE, to protect the lifecycle state for the device and enforce the transition rules between states, implemented in the eFuse.
- Cryptographic functions services for SPE and NSPE applications.
- Support for an attestation method, for example Entity Attestation Token (according to IETF specification).
- SPE debug is completely locked after production
- Tamper protection to protect against voltage and EM fault injection
- PUF-derived key to provide a chip-unique secure storage key

1.5.5 Non-TOE Hardware/Software/Firmware

No other components are supplied within the TOE scope.

2 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.	[3] Section 1.3
TRUSTED_USERS	Actors in charge of TOE management, for instance for signature of firmware update, are trusted.	[6] Section 5
UNIQUE_ID	The integrity and uniqueness of the unique identification of the TOE must be provided by the TOE user during the personalization stage.	[2] Section 3.8.8

Table 4: Security Objectives for the Operational Environment

3 Security Requirements and Implementation

3.1 Security Assurance Requirements

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

3.1.1 Flaw Reporting Procedure (ALC_FLR.2)

Silicon Labs has a Product Security Incident Response Process to intake hardware and software vulnerabilities, triage such issues, remediate them where possible, and communicate the vulnerabilities and recommendations to security researchers and product stakeholders. This plan is described in internal documents [9] and [10].

Instructions for researchers to disclose vulnerabilities to Silicon Labs are located at the following URL: https://www.silabs.com/security/product-security

The method described recommends the researcher or other party encrypt the email using the Silicon Labs-supplied PSRIT PGP Key, and to address the encrypted email to productsecurity@silabs.com.

The email will be received by a member of the Product Security Incidence Response Team, who will create a case in an internal ticket tracking system. The ticket will be assigned to a PSIRT team member who is responsible for triaging the issue and working with internal R&D teams to prioritize mitigation and communication efforts.

The case owner is also responsible for direct communication and coordination with the researcher/discloser. If the PSIRT team determines the issue should be shared publicly, a Security Advisory will be drafted and published on our security portal.

Security researchers and other stakeholders can subscribe to receive security advisories via the security portal. Instructions can be found here: https://www.silabs.com/security

If the vulnerability is located in stack code or another software component, the patch will be delivered via an SDK update that is published via Simplicity Studio.

3.2 Base PP Security Functional Requirements

As a base, the platform fulfils the following security functional requirements:

3.2.1 Verification of Platform Identity

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

Conformance rationale:

Identification of the TOE can be performed by inspecting the package of the TOE. The Package Marking in the datasheet described how to identify the TOE physically. The identity of the firmware can be verified using Simplicity Studio, or via the mailbox interface.

3.2.2 Verification of Platform Instance Identity

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

Conformance rationale:

The TOE supports a cryptographic identity that is formed from a NIST P-256 key pair that is generated at the time the chip is produced. The device randomly generates its private key using the on-chip TRNG and securely stores this key in OTP. The public portion of the key is exported to the production infrastructure which wraps the public key in an X.509 certificate and signs the certificate into a Silicon Labs certificate chain. The signed device certificate is reinjected into the device and stored in SE OTP, along with its associated production batch certificate.

3.2.3 Attestation of Platform Genuineness

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

Conformance rationale:

The genuineness of the platform can be verified by verifying the signed device certificate injected to the device. This implementation is conformant to the Arm PSA Initial Attestation Token standard [11]. It is accessible from the "Attest PSA Initial" API. The back-end provided a nonce to the SE. It is then signed with the attestation key stored in the OTP.

3.2.4 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 an infinite loop with Physical attacker resistance.

Conformance Rationale:

During boot, the Secure Element subsystem verifies the authenticity and integrity of the SPE runtime images. The Secure Element runs from ROM out of reset and that ROM image verifies the SE SPE firmware using ECDSA over Curve25519 against a Silicon Labs public key stored in ROM.

3.2.5 Attestation of Platform State

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

Conformance Rationale:

The private key in the SE is used to sign the initial attestation tokens in IETF EAT format containing measurements of the firmware. This data includes the state of the TOE that can be verified by the back end.

3.2.6 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 SE has a mailbox command that is capable of upgrading SPE SE firmware or NSPE firmware on the Cortex M33. SE firmware upgrades are versioned, encrypted, and signed with a Silicon Labs private key. SE firmware upgrades are checked for authenticity and integrity against a Silicon Labs public key stored in ROM prior to the upgrade being applied. SE firmware upgrades are versioned and rollback protected.

3.2.7 Physical Attacker Resistance

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

Conformance Rationale:

The TOE implemented the following tamper protection mechanisms to resist against physical attacker:

- Electromagnetic pulse Glitch Detection
- Supply Glitch Detection
- DPA countermeasure

3.2.8 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 SPE is implemented by a Secure Element subsystem that contains its own CPU, RAM, ROM, OTP, and peripherals. This subsystem is isolated from the Host CPU Cortex-M33 at the bus level. Communication between the Cortex-M33 and the SPE is via a shared mailbox interface. The Host CPU does not have direct access to any peripherals or memories of the SPE other than the mailbox interface. All PSA RoT functionality is implemented inside the SPE.

3.2.9 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 TOE does not allow for the user to install their own Application Root of Trust. This is due to the fact that the TOE architecture that locks everything in the SPE to Silicon Labs. Therefore, the requirement has been fulfilled.

3.2.10 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**.

Algorithm	**Operations**	**Specification**	**Key lengths**	**Modes**
AES	Encrypt, Decrypt, Sign/MAC, Verify	NIST FIPS 197 NIST SP800-38	128-bit, 192-bit, 256-bit	CTR, CCM, GCM/GMAC

ChaCha20	Encrypt, Decrypt, Sign/MAC, Verify	RFC7539	256-bit	CTR, CCM, GCM/GMAC
ChaCha20_Poly1305	Encrypt, Decrypt, Sign/MAC, Verify	RFC7539	256-bit	CTR, CCM, GCM/GMAC
SHA_256	Hash	FIPS 180-3		
SHA_512	Hash	FIPS 180-3		
ECC	ECDSA, ECDH, EdDDSA	ANSI X9.62 FIPS 186-3 REFC 7748	Up to 521-bits	

Table 5: Cryptographic Operations

3.2.11 Cryptographic Random Number Generation

The platform provides the application with a way based on oscillator rings to generate random numbers to as specified in NIST-800-90B.

Conformance Rationale:

The functionality is implemented inside the SE Firmware that is accessible to the NSPE via the mailbox interface. The RNG implemented in the TOE passes the NIST 800-22 and AIS31 test suites.

3.2.12 Cryptographic Key Generation

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

ID	Algorithm	Specification	Key lengths(bits)
RAW	Symmetric algorithms: AES, ChaCha20	N/A	128, 192, 256(AES) 256(ChaCha20) Any value up to 512 bytes
ECC	Weierstrass Prime	N/A	192
ECC	Montgomery	N/A	255, 448
ECC	EDDSA	N/A	255

Table 6 Cryptographic Key Generation

3.2.13 Cryptographic KeyStore

The platform provides the application with a way to store cryptographic keys and passwords such that not even the application can compromise the authenticity, integrity, and confidentiality of this data. This data can be used for the cryptographic operations: encrypt, decrypt, sign/MAC, and verify

Conformance Rationale:

The cryptographic key store is implemented by a PUF-derived Hardware Encryption Key that is used to protect the authenticity, integrity, and confidentiality of the other keys in the system using AES-GCM.

3.3 Optional Security Functional Requirements

3.3.1 Secure Encrypted Storage (internal storage)

The platform ensures that all data stored by the application is encrypted as specified in NIST Special Publication 800-38D (AES-GCM) with a platform instance unique key of key length 256-bit from the PUF key.

Conformance Rationale:

The cryptographic key store is implemented by a PUF-derived Hardware Encryption Key that is used to protect the authenticity, integrity, and confidentiality of the other keys in the system using AES-GCM.

3.3.2 Secure Storage (internal storage)

The platform ensures that all data stored by the application is protected to ensure its authenticity and integrity as specified in NIST Special Publication 800-38D (AES-GCM) with a platform instance unique key of key length 256-bit from the PUF key.

Conformance Rationale:

The cryptographic key store is implemented by a PUF-derived Hardware Encryption Key that is used to protect the authenticity, integrity, and confidentiality of the other keys in the system using AES-GCM.

3.3.3 Secure External Storage

The platform ensures that all data stored outside the direct control of the platform is protected such that the **authenticity, integrity, confidentiality** binding to the platform instance is ensured. It follows the specification of NIST Special Publication 800-38D (AES-GCM) with a platform instance unique key of key length 256-bit from the PUF key.

Conformance Rationale:

The cryptographic key store is implemented by a PUF-derived Hardware Encryption Key that is used to protect the authenticity, integrity, and confidentiality of the other keys in the system using AES-GCM.

3.3.4 Residual Information Purging

The platform ensures that main flash and RAM, with the exception of SE Firmware is erased using the method specified in [12] before the memory is (re)used by the platform or application again and before an attacker can access it.

Conformance Rationale:

The TOE provided an API to erase the main flash and RAM, unlock flash locks, reset debug settings, as well as release the bus lock. It is accessible via the “Device erase” SE command.

3.3.5 Secure Debugging

The platform locked the debug mechanism of the SE during manufacturing. SE debug are allowed only with authentication.

Conformance Rationale:

The SE on the TOE has a debug interface that is securely locked during device manufacturing and can only be unlocked via a cryptographic token that is signed by a Silicon Labs private key.

4 Mapping and Sufficiency Rationales

4.1 Assurance

The assurance activities defined in [PSA-EM-L3] are fulfilled by SESIP3 level. In particular, the required source code review, vulnerability analysis and vulnerability analysis to an equivalent of 35 man days of the [PSA-EM-L3] is applicable.

Assurance Class	Assurance Family	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section “Introduction” and title page of the Security Target	The section contains the ST reference, Platform reference, and the functional overview and description
	ASE_OBJ.1 Security requirements for the operational environment	Section “Security Objectives for the Operational Environment” of the Security Target	The requirements are all indicated in the guidance document
	ASE_REQ.3 Listed Security requirements	Section “Security Requirements and Implementation” of the Security Target	The SFRs in this ST are taken from [13]. Mandatory SFR “Verification of Platform Identity” and “Secure Update of Platform” is included.
	ASE_TSS.1 TOE Summary Specification	Section “Security Requirements and Implementation” of the Security Target	The conformance rationale on each SFR describes how the SFR is implemented.
ADV: Development	ADV_FSP.4 Complete functional specification	Functional specification is provided in [12].	[12] list all the interfaces that is provided by the TOE.
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	Full source code provided to the evaluators.	The evaluator will validate the suitability of the provided evidence.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	All the guidance documents are listed in the “Included Guidance Documents” section of the ST.	The evaluator shall validate the suitability of the evidence.

	AGD_PRE.1 Preparative procedures	All the guidance documents are listed in the “Included Guidance Documents” section of the ST.	The TOE is preconfigured in the factory. No user preparation is needed.
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	The list of configuration items are available in [8]	The evaluator shall validate the suitability of the evidence.
	ALC_CMS.1 TOE CM Coverage	The list of configuration items are available in [8]	The evaluator shall validate the suitability of the evidence.
	ALC_FLR.2 Flaw reporting procedures	ALC_FLR section in the Security Target and description of which developer evidence is used to meet this requirement	The flaw remediation procedures are described.
ATE: Tests	ATE_IND.1 Independent testing: conformance	Vulnerability and testing carried out by the laboratory	The evaluator will perform independent testing.
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis	Vulnerability and testing carried out by the laboratory	The evaluator will perform penetration testing.

Table 7: Assurance Mapping and Sufficiency Rationales

4.2 Functionality

Table 8 Functionality Mapping and Sufficiency Rationales

PSA Security Function	**(detail)**	**Covered by SESIP SFR**	**Rationale**
F.INITIALIZATION	Boot sequence in scope: Chip PSA Root of Trust Application Root of Trust Services	Secure initialization of platform	Full coverage
F.SOFTWARE_ ISOLATION	Level 1: Isolation between SPE and NSPE	Software Attacker Resistance: Isolation of Platform (Level 1)	Full coverage
	Level 2: Isolation between PSA-RoT and Application RoT	Software Attacker Resistance: Isolation of Platform (Level 2)	Full coverage

	Level 3: Isolation between Application RoT	Software Attacker Resistance: Isolation of Application Parts	Full coverage
F.SECURE_ STORAGE	Integrity and Confidentiality	Secure Encrypted Storage (internal storage)	Full coverage with AES-GCM with hardware unique key
	Authenticity and integrity	Secure Storage (internal storage)	Full coverage with AES-GCM with hardware unique key
	Binding to the RoT	Software Attacker Resistance: Isolation of Platform	Stored data is isolated from the NSPE and Application Root of Trust Services by using a HUK for each platform.
	Basic rollback – atomicity	Not covered by any SESIP SFR. Note added in “Secure Encrypted Storage”.	Full coverage with rollback protection
	External storage (optional)	Secure External Storage	Full coverage with AES-GCM with hardware unique key
F.FIRMWARE_ UPDATE	Integrity and authenticity of the update.	Secure Update of Platform	Full coverage
F.SECURE_STATE	Protects itself against abnormal situations caused by programmer errors or violation of good practices from code executed outside of the TOE, either from SPE or NSPE.	Software Attacker Resistance: Isolation of Platform	Full coverage
	Controls the access to its services by Applications and checks the validity of parameters of any operation requested from Applications	Software Attacker Resistance: Isolation of Platform	Full coverage
	Enters a secure state upon platform initialization error or software failure detection, without exposure of any sensitive data.	Partially covered by the SFR “Secure initialization of platform”, “Secure update of platform” and also for the TF-M implementation covering the software failure detection.	Full coverage

F.CRYPTO	Minimum cryptographic operations supported: Attestation Secure Storage	Cryptographic Operation	Full coverage with both symmetric and asymmetric cryptography
	Minimum cryptographic keys for secure storage: Attestation Secure Storage	Cryptographic KeyStore	Full coverage with AES-GCM with hardware unique key
	PSA SM requires that all devices implement at least the following trusted cryptographic services: True random number generator Global nonce counter	Cryptographic Random Number	Full coverage with oscillator rings compliant to NIST-800-90B.
		Cryptographic Key Generation	Full coverage with both symmetric and asymmetric cryptography
F.ATTESTATION		Verification of Platform Identity	Unique identification of the platform
	Unique platform number	Verification of Platform Instance Identity	Unique identification of the platform instance
	Proof of origin	Attestation of Platform Genuineness	“Verification of Platform Instance” and “Verification of Platform Instance Identity” are included in the attestation token.
	Lifecycle state	Attestation of Platform State	Full coverage
F.AUDIT	(Optional) Protect the stored audit records from unauthorized deletion	Audit Log Generation and Storage	N/A
	(Optional) Prevent unauthorized modifications	Audit Log Generation and Storage	N/A
F.DEBUG		Secure Debugging	Full coverage

		Physical attacker Resistance	Full coverage
F.PHYSICAL		Physical Attacker Resistance	Full coverage

5 About this document

5.1 Current Status and Anticipated Changes

Current Status: Beta

5.2 Release Information

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

Date	Version	Confidentiality	Change
2020-08-28	1.0ALP01	Non-confidential	Initial version to be discussed with JSA members
2020-10-26	1.0ALP02	Non-confidential	Updates discussed with JSA members
2020-12-11	1.0BET01	Non-confidential	Feedback from vendors and JSA members

5.3 References

This document refers to the following documents.

5.3.1 Normative references

Ref	Doc No	Author(s)	Title
[PSA-EM-L2]	JSADEN003	JSA	PSA Certified: Evaluation Methodology for PSA L2 v1.1
[PSA-EM-L3]	JSADEN010	JSA	PSA Certified: Evaluation Methodology for PSA L3 v1.0-ALP01
[PSA-AM-L2]	JSADEN004	JSA	PSA Certified Attack Method for PSA L2 v1.1
[PSA-AM-L3]	JSADEN008	JSA	PSA Certified Attack Method for PSA L3 v1.0-ALP01
[PSA-PP-L2]	JSADEN002	JSA	PSA Certified Level 2 Lightweight Protection Profile v1.1
[PSA-PP-L3]	JSADEN009	JSA	PSA Certified Level 3 Lightweight Protection Profile v1.0-ALP01
[SESIP]	GP_FST_070	GlobalPlatform	Security Evaluation Standard for IoT Platforms (SESIP) v1.1
[CEM]	CCMB-2017-04-004		Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, revision 5, April 2017.

5.3.2 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

[JIL-APSC]	-	JHAS	Joint Interpretation Library – Application of Attack Potential to Smartcards v3.1 June 2020
[PSA-SM]	ARM DEN 0079	ARM	Platform Security Architecture Security Model v1.0

5.4 Terms and Abbreviations

This document uses the following terms and abbreviations (see PSA-SM and PSA Cert L1 V2.1 or newer questionnaire).

Term	Meaning
Application	Used in SESIP to refer to the components which are out of the scope of the evaluation. It is a synonym for Connected Application.
Application Root of Trust Service(s)	Application specific security service(s), and so not defined by PSA. Such services execute in the Secure Processing Environment 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.
Connected Application	Software developed by an IoT vendor, implementing IoT end-user use case based on the underlying Connected Platform. May be referred to as "Application" when there is no ambiguity.
Connected Platform	Combination of hardware and software that provides a runtime environment for a Connected Application. A Connected Platform implements security features and makes security services available to the Connected Application. May be referred to as "platform" when there is no ambiguity.
Connected product	Combination of a Connected Platform and a Connected Application that a product vendor puts on the market.May be referred as "product" when there is no ambiguity.
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 technical review of questionnaires submitted for Level 1 PSA certification. 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.
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. In SESIP terms, the NSPE is the "application".

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 SESIP to refer to the components which are in the scope of the evaluation. It is a synonym for Connected platform.
Product	Used by SESIP as a synonym for Connected product
PSA	Platform Security Architecture
PSA Certification Body	The entity that receives applications for PSA security certification, issues 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 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.
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, and any Application RoT Service(s). In SESIP terms, the SPE is the “platform”.
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.
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.
Trusted subsystem	A security subsystem that the PSA-RoT relies on for protection of its assets, or that implement some of its services.

6 Bibliography

[1] Silicon Labs, Inc, “EFR32xG23 Wireless Gecko Reference Manual Rev. 0.5 *WIP*,” August, 2021.

[2] Silicon Labs, Inc, “EFR32FG23 Wireless SoC Family Data Sheet Preliminary Rev. 0.5*WIP*,” Aug, 2021.

[3] Silicon Labs, Inc, “AN1218: Series 2 Secure Boot with RTSL,” July 2020.

[4] Silicon Labs, Inc, “AN1190: Series 2 Secure Debug Revision 0.4,” September 2021.

[5] Silicon Labs, Inc, “EFR32 Wireless Gecko EFR32FG23 Errata,” September, 2021.

[6] Silicon Labs, Inc, “AN1222: Production Programming of Series 2 Devices Rev. 0.5,” Sep, 2021.

[7] Silicon Labs, Inc, “UG162: Simplicity Commander Reference Guide,” Rev. 2.1.

[8] Silicon Labs, Inc, “EFR32FG23 Wireless SoC Family SESIP Configuration Item List,” 1 December 2021.

[9] Silicon Labs, Inc, “PS1012 – Security Vulnerability Disclosure Policy Rev. C,” 12/17/2020.

[10] SIlicon Labs, Inc, “CRISIS006 - Product Security Incident Response plan (PSIRP) Revision H,” September 2021.

[11] Arm Limited, “Arm's Platform Security Architecture (PSA) Attestation Token,” 24 03 2021. [Online]. Available: https://tools.ietf.org/id/draft-tschofenig-rats-psa-token-08.html. [Accessed 22 11 2021].

[12] Silicon Labs, Inc, “Gecko Platform,” 2021. [Online]. Available: https://docs.silabs.com/gecko-platform/3.2/index. [Accessed 1 December 2021].

[13] GlobalPlatform Technology, “Security Evaluation Standard for IoT Platforms (SESIP) Version 1.1,” June 2021.