EFR32FG23 Wireless SoC Family
SESIP Security Target

Version: 0.3

Date: 1 December 2021

Silicon Labs, Inc

1. Version history

Version	Date	Description	Author
0.1	20 September 2021	Initial draft	Silicon Labs, Inc
0.2	8 November 2021	Updated content	Silicon Labs, Inc
0.3	1 December 2021	Updated content	Silicon Labs, Inc

1. Table of Contents

2. Identification

2.1 Identification of the ST

The ST is identified as EFR32FG23 Wireless SoC Family SESIP Security Target Version 0.3 issued on 1 December 2021.

SESIP version is identified as Version 1.1 [1].

2.2 SESIP Profile Reference

Reference	Value
SP Name	SESIP Profile for Secure MCUs and MPUs
SP Version	V1.0
TOE Type	Secure Processing Unit for IoT devices
Assurance Claim	SESIP Assurance Level 3 (SESIP3)
Package Claim	Base SP, Package Security Services. Package Software Isolation, Package Hardware Protections

2.3 Identification of the platform

Reference	Value	Verification method
Commercial name	EFR32FG23	[2] Section 2
HW reference	EFR32FG23B…-B	[2] Section 2
HW version	Revision B	[2] Section 2
FW reference	SE_firmware	[3] Section 5.2.2
FW version	V2.1.6	[3] Section 5.2.2

2.4 Identification of the guidance

2.4.1 Manuals

Title	Version	Date
EFR32xG23 Wireless Gecko Reference Manual	Revision 0.5	August, 2021
EFR32FG23 Wireless SoC Family Data Sheet	Revision 0.5	August, 2021
AN1218: Series 2 Secure Boot with RTSL	Revision 0.3	July 2020
AN1190: EFR32xG21 Secure Debug	Revision 0.4	September 2021
EFR32 Wireless Gecko EFR32FG23 Errata	Revision 0.4	September 2021
AN1222: Production Programming of Series 2 Devices	Revision 0.5	September 2021
UG162: Simplicity Commander Reference Guide	Rev. 2.1	
EFR32FG23 Wireless SoC Family SESIP Configuration Item List	v0.3	2 December 2021
PS1012 – Security Vulnerability Disclosure Policy	Rev C	17-Dec-2020
CRISIS006 - Product Security Incident Response plan (PSIRP)	Rev H	2021-09-16

2.5 Life Cycle

The TOE is delivered in a pre-configured state, meaning that Silicon Labs key is already provisioned to authenticate the SE firmware.

2.6 Configurations

The security services provided by the TOE intended to be used by the higher software layers to implement a full-fledged Root of Trust and operating system. A Secure Enclave is used to fulfil all of the security features. The hardware interface to the secure enclave is a mailbox mechanism and a DMA from the secure enclave to the rest of the system. The SFRs are accessible for application developer using Gecko SDK suite [4].

2.7 Use Case

The TOE is intended to be used as a secure platform to develop IoT application such as smart home, security, lighting, building automation, and metering.

[any user]

The product may be physically accessed by an unknown or untrusted user, in an environment where access to the product cannot be sufficiently controlled or even in a more hostile environment.

[any code]

It cannot be excluded that the product will execute code that is unknown to the product developer. This is due to the fact that the Arm Cortex M33 core is completely open to the application developer. Therefore, this ST assumes that the application core can run any attacker controlled code trying to compromise TOE assets.

3. Platform Security Features and Scope

The EFR32FG23B is an SoC designed to be used as a secure microcontroller to support Internet of Things application. The TOE supports secure boot, secure update, secure debug authentication, random number generation, and cryptographic acceleration.

The TOE consists of a secure element inside the SoC, as well as the firmware running in the secure element. The communication of the secure element to the rest of the SoC is provided via a mailbox. This mailbox interface is accessible through APIs provided by the developer.

The hardware scope of the evaluation is available in Figure 3-1 inside the red box. Additionally, the software scope of the evaluation is available in Figure 3-2 inside the red box.

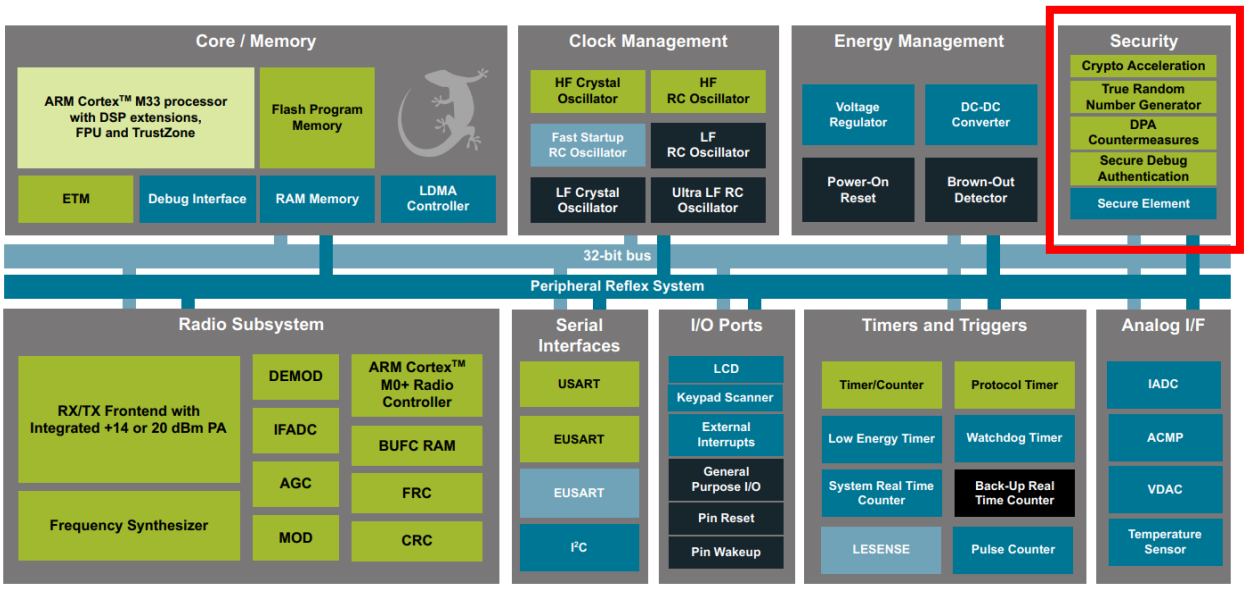

Figure 3-1 TOE Scope

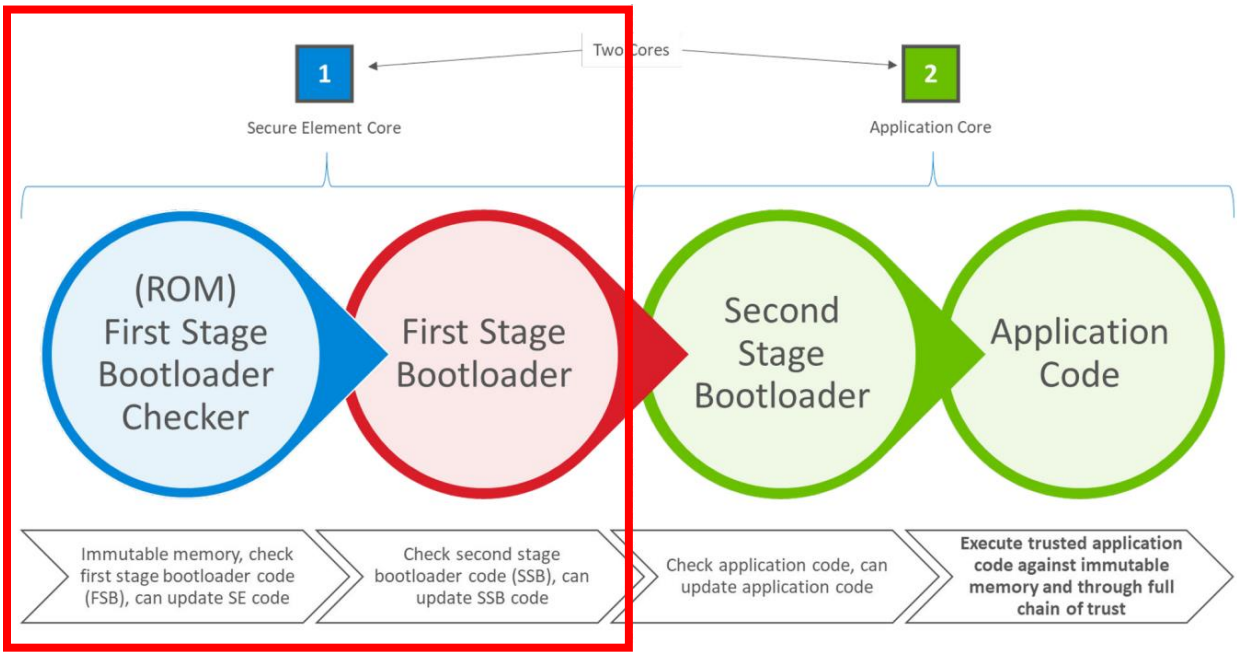

Figure 3-2 TOE Firmware Scope

The TOE is intended to be used as a platform to develop secure IoT device. The OEM will develop an application that is running on the application core as well as develop the circuit board with the additional components needed for the TOE to be operational. The TOE supports the following security features:

- 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

3.1 Physical Scope

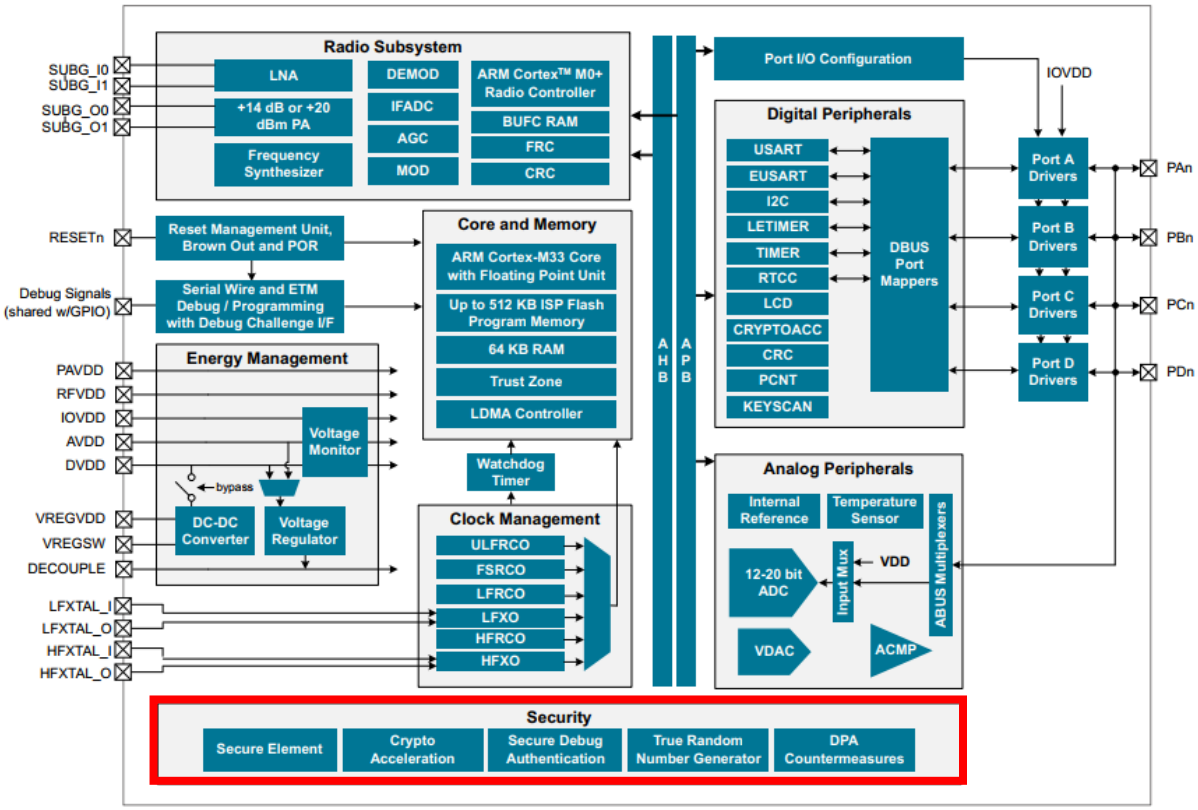

Figure 3-3 Detailed EFR32FG23 Block Diagram taken from [2].

The physical scope includes the hardware identified in 2.2 and the guidance identified in 2.4. The bus diagram on Figure 3-3 marked the TOE scope within the red box. The TOE hardware as well as the ROM code is delivered as a pre-integrated subsystem inside a SoC. The TOE software is downloadable as an encrypted binary from Silicon Labs, Inc website.

3.2 Logical Scope

The logical scope comprises the secure functions defined in section 3 above. It is implemented by the SE Firmware.

3.3 Non-TOE Hardware/Software/Firmware

The subsystems outside of the red box in Figure 3-3 is considered Non-TOE hardware. The TOE is delivered as a pre-integrated secure element inside a SoC. No additional Non-TOE software or firmware is required.

4. Security objectives for the operational environment

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

ID	Description	Reference
KEY_MANAGEMENT	Cryptographic keys and certificates outside of the TOE are subject to secure key management procedures.	[5] Section 1.3
TRUSTED_USERS	Actors in charge of TOE management, for instance for signature of firmware update, are trusted.	[3] 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

5. Security Requirements and Implementation

5.1 Security Assurance Requirements

The claimed assurance package is SESIP3 as defined in [1] section 4.3.

5.1.1 Flaw remediation process (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 [6] and [7].

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.

5.2 Security Functional Requirements

5.2.1 Base SP Security Functional Requirements

5.2.1.1 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.

5.2.1.2 Secure Initialization of Platform

The platform ensures its authenticity and integrity during the platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will 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.

5.2.1.3 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.

5.2.1.4 Residual Information Purging

The platform ensures that main flash and RAM, with the exception of SE Firmware is erased using the method specified in [4] 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.

5.2.1.5 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.

5.2.2 Package ‘Security Services’ Security Functional Requirements

5.2.2.1 Cryptographic Operation

The platform provides the application with Operations in Table 1 functionality with algorithms in Table 1 as specified in specifications in Table 1 for key lengths described in Table 1 and modes described in Table 1.

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 1: Cryptographic Operations

5.2.2.2 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in cryptographic operations in Table 2 for key lengths described in Table 2.

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 2: Cryptographic Key Generation

5.2.2.3 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.

5.2.2.4 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.

5.2.3 Package 'Software Isolation' Security Functional Requirements

5.2.3.1 Software Attacker Resistance: Isolation of Platform

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 the SFRs are implemented inside the SPE.

5.2.4 Package 'Hardware Protections' Security Functional Requirements

5.2.4.1 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

5.2.5 Additional Security Functional Requirements

5.2.5.1 Software Attacker Resistance: Isolation of Platform Parts

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.

5.2.5.2 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.

5.2.5.3 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.

5.2.5.4 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 [8]. 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.

5.2.5.5 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.

5.2.5.6 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.

5.2.5.7 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.

6. Mapping and Sufficiency rationales

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 [1]. 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 [4].	[4] 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 [9]	The evaluator shall validate the suitability of the evidence.

	ALC_CMS.1 TOE CM Coverage	The list of configuration items are available in [9]	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.

7. References

[1] GlobalPlatform Technology, "Security Evaluation Standard for IoT Platforms (SESIP) Version 1.1," June 2021.

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

[3] Silicon Labs, Inc, "AN1222: Production Programming of Series 2 Devices Rev. 0.5," Sep, 2021.

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

[5] Silicon Labs, Inc, "AN1218: Series 2 Secure Boot with RTSL," July 2020.

[6] Silicon Labs, Inc, "PS1012 – Security Vulnerability Disclosure Policy Rev. C," 12/17/2020.

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

[8] 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].

[9] Silicon Labs, Inc, "EFR32FG23 Wireless SoC Family SESIP Configuration Item List," November 2021.