Security Target for Series 3 Secure Vault™

Version: 1.3
Date: 3 July 2025

Silicon Labs, Inc.

Based on [SESIP] methodology, version “Public Release v1.2”

Contents

1 Introduction 5

1.1 ST Reference 5

1.2 SESIP Profile Reference 5

1.3 Platform Reference 5

1.4 Included Guidance Documents 5

1.5 Platform Functional Overview and Description 6

1.5.1 Platform Type 6

1.5.2 Physical Scope 6

1.5.3 Usage and Major Security Features 8

1.5.4 Required Hardware/software/firmware 8

2 Security Objectives for the operational environment 9

2.1 Platform Objectives for the Operational Environment 9

3 Security requirements and implementation 10

3.1 Security Assurance Requirements 10

3.1.1 Flaw Reporting Procedure (ALC_FLR.2) 10

3.2 Base PP Security Functional Requirements 10

3.2.1 Verification of Platform Identity 10

3.2.2 Verification of Platform Instance Identity 11

3.2.3 Attestation of Platform Genuineness 11

3.2.4 Secure Initialization of Platform 11

3.2.5 Attestation of Platform State 12

3.2.6 Secure Update of Platform 12

3.2.7 Physical Attacker Resistance 12

3.2.8 Software Attacker Resistance: Isolation of Platform (between SPE and NSPE) 13

3.2.9 Cryptographic Operation 13

3.2.10 Cryptographic Random Number Generation 13

3.2.11 Cryptographic Key Generation 14

3.2.12 Cryptographic KeyStore 14

3.3 Additional Security Functional Requirements 14

3.3.1 Secure Communication Support 14

3.4 Optional Security Functional Requirements 15

3.4.1 Secure Debugging 15

3.4.2 Secure Confidential Storage 15

3.4.3 Secure Data Serialization 15
4 Mapping and sufficiency rationales 16
4.1 SESIP3 sufficiency 16
5 References 19
6 Abbreviations 20
7 Revision history 21

1 Introduction

This Security Target describes the security features provided by the Series 3 Secure Vault™ embedded on SixG301 System-on-Chip (SoC), which are evaluated against the requirements of SESIP Assurance Level 3. The security claims are only maintained when the security objectives for its environment, detailed later in this ST, are fulfilled.

1.1 ST Reference

Security Target for Series 3 Secure Vault™, Version 1.3, dated 2025-07-03.

1.2 SESIP Profile Reference

Table 1 SESIP Profile Reference

Reference	Value
PP Name	SESIP Profile for PSA Certified Level 4 iSE/SE
PP Version	2.0 BETA
Assurance Claim	SESIP Assurance Level 3 (SESIP3)
SESIP Standard	[SESIP]
Optional and additional SFRs	• Secure Communication Support • Secure Debugging • Secure Confidential Storage • Secure Data Serialization

1.3 Platform Reference

Table 2 Platform reference

Reference	Value
Platform name	Series 3 Secure Vault™
Platform version	Hardware version: B0 ROM version: 5, Patch version: 3 SE Firmware version: 3.3.2
Platform identification	Series 3 Secure Vault™ on SixG301
Platform type	Integrated hardware secure engine

1.4 Included Guidance Documents

The following documents are included with the platform:

Table 3 Guidance documents

Name	Version
Security Target for Series 3 Secure Vault™	Ver. 1.3
SiMG301 Wireless SoC Family Datasheet	Rev. 0.5
SiSDK Platform Documentation	Ver. 5.2.0
SiXG301 Wireless SoC Reference Manual Reference Manual	Rev. 0.4
CRISIS006 - Product Security Incident Response plan (PSIRP)	Rev. J
AN1504: Series 3 Security Overview	Rev 0.1
AN1268: Authenticating Silicon Labs Devices Using Device Certificates	Rev. 0.4
Simplicity Commander User Guide	Ver. 1.17.4

1.5 Platform Functional Overview and Description

1.5.1 Platform Type

TOE is the pre-integrated Series 3 Secure Vault ™ (hereinafter referred to as “S3 HSE” or “HSE”) of SixG301 System-on-Chip (SoC). This dedicated HSE contains its own CPU and isolates cryptographic functions and data from the host Cortex-M33 core and provides several additional security features. Usage and security features of the HSE is further described in section 1.5.3.

1.5.2 Physical Scope

The scope of this evaluation is the HSE that is pre-integrated in SixG301 SoC. Additionally, due to the complex security measurements and design layout, the TOE physical boundary extends beyond the secure element. Three main parts that comprises the TOE are:

1. **Secure Element Subsystem**
   - comprised of dedicated RISC-V CPU (CV32E40S processor), Boot ROM, PUF, OTP, RNG, DMA, RAM, mailbox, crypto engines (AES, ECC, SHA), clocking, tamper response unit.
2. **External Memory Subsystem (EXTMEM)**
   - consists of QSPI controller and L2ICACHE.
   - provides AXiP/EXiP memory protection.
3. **Key Slot Unit (KSU)**
   - facilitates in storing and transferring of symmetric keys in a secure way to the cryptographic engines in the host subsystem.

The scope also includes the firmware running on the SE. The SE firmware can either be pre-integrated in the chip or it can be downloaded from Silicon Labs website in an encrypted update binary form.

The physical scope is highlighted in red in Figure 1 of the SoC architecture diagram. TOE hardware can be purchased by end-users via select distributors.

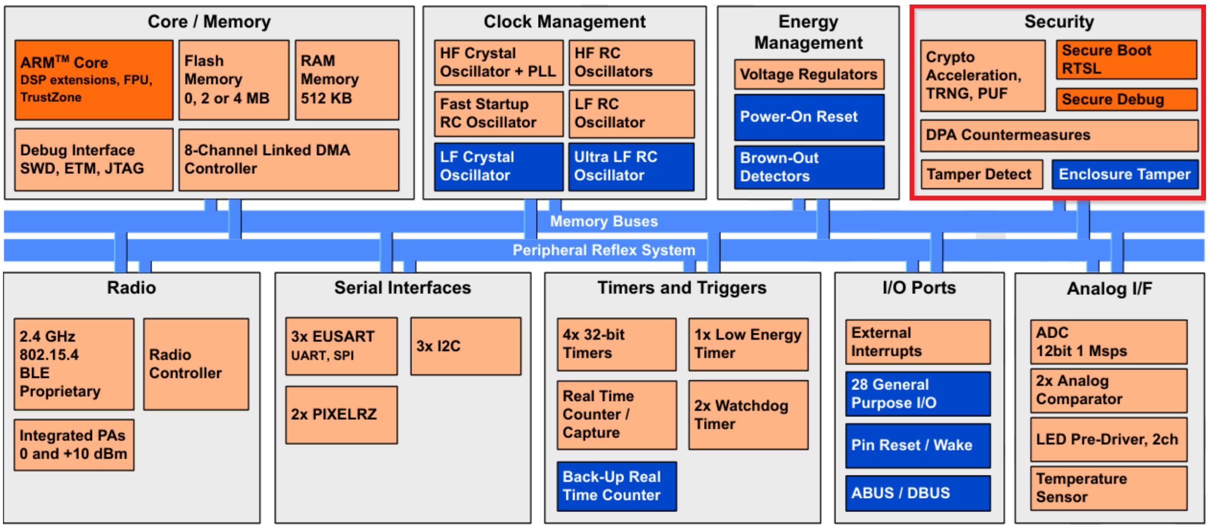

Figure 2: TOE scope

EXTMEM is intended to provide a seamless interface for the system to access an external Flash via QSPI controller and the L2ICACHE. This subsystem provides AXiP/EXiP that allows the device to execute instructions from NVM securely via encryption/decryption and integrity-checking on-the-fly. This provides confidence that the content of the external NVM does not change between secure boot verification and subsequent runtime read-outs of the same memory. The L2ICACHE is intended to cache instructions for the Host CPU and SE CPU. Instructions that are not cached will be fetched from the external NVM via the QSPI controller.

The Key Slot Unit (KSU) is a hardware block that allows the system to use securely stored keys in the high-performance host AES and SHA engines without exposing them. The KSU also separates the process of key unwrapping from key usage, allowing faster access to keys. Either the host or radio processor can request a specific key to be unwrapped by the SE and stored in a certain key slot. The processor can then tell encryption hardware to use the key in that slot to perform an operation. The key material itself is protected and never accessible to the processor.

Logical Scope:

The scope for a PSA Certified Level 4 Security evaluation is the combination of the trusted hardware and firmware components implementing a secure element environment with the Security Functional Requirements stated in this document. The logical scope includes:

Table 4 Logical scope

Component	Version
ROM	ROM version: 5, Patch version: 3
SE Firmware	Version: 3.3.2

1.5.3 Usage and Major Security Features

TOE is a secure element solution that is integrated in SixG301 SoC which is to be further used in Internet of Things (IoT) endpoint. The aim is to provide enhanced security, small form factor, and low power consumption.

TOE provides the following features for the purpose of PSA Level 4 security evaluation:

- Security Functions.
    - Cryptographic key generation/derivation
    - Data encryption/decryption
    - Digital signature generation/verification
    - Random number generation
    - Secure Boot with Root of Trust and Secure Loader
    - Secure booting of firmware code, e.g. SE firmware and host firmware in Flash.
    - Secure OTP storage
- Host Control Functions.
    - Host system lockdown
    - Tamper protection
    - Feature configuration
    - Chip configuration
- Isolation between host subsystem and security assets on the chip. Security assets include cryptographic keys, non-volatile secure counters, non-volatile manufacturing data such as device calibration and feature configuration.

1.5.4 Required Hardware/software/firmware

Remaining parts of SixG301 SoC outside of the red boxes in Figure 3 are considered as required non-TOE hardware. The TOE is delivered pre-integrated inside a SoC.

SoC includes a co-packaged external Flash NVM up to 4MB which is partitioned to include an SE region that stores the encrypted SE Firmware. The SE region has a separate address range that is inaccessible by the host. SoC reserves 192 KB of the attached flash to store the upgradeable portion of SE firmware. SE firmware is always stored using AXiP. Flash memory contents are managed by the SE and the external memory hardware to provide robust security for program memory.

Besides being co-packaged and delivered with the SoC, end-users also have the option to purchase the external flash separately. Silicon Labs provides a list of supported external flash and allows end-users to configure the flash parameters themselves. The supported flashes are: GT25Q32B-L, MX25U1632FW8K, MX25U3232FW8K, XM25LU32, GT25Q16C-L.

No additional non-TOE software or firmware is required.

2 Security Objectives for the operational environment

2.1 Platform Objectives for the Operational Environment

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

Table 5 Security Objectives for the operational environment

Title	Description	Reference
KEY_MANAGEMENT	Cryptographic keys and certificates outside of the Platform are subject to secure key management procedures.	[8], this document
TRUSTED_USERS	Actors in charge of platform management are trusted.	This document
UNIQUE_ID	The integrity and uniqueness of the unique identification of the platform must be provided by the platform user during the personalization stage.	[2] Section 3.10.11
PLATFORM_ACCEPTANCE	When receiving the platform, the user is expected to verify the correct version of all platform components that it depends on.	This document, Section 1.3
SECURE_USE	Users shall ensure secure and correct use of the platform according to guidance listed in Section 1.4.	This document, Section 1.4
SECURE_UPDATE	Actors in charge of executing update of the platform firmware or applications are expected to securely initiate the update process. The update image is expected to be properly signed and distributed in secure manner to ensure its confidentiality and authenticity.	[8]

3 Security requirements and implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP3** as defined in [SESIP].

3.1.1 Flaw Reporting Procedure (ALC_FLR.2)

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

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 documents [4] and [5].

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 PSIRT 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 whether 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

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. ROM and patch version, along with SE firmware version (identified in section 1.3) are exposed over a status command that is available over DCI and mailbox.

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.

Conformance rationale:

For verification, the device attestation service creates an Entity Attestation Token (EAT) in IETF EAT format that contains a fixed set of device-specific data (including Instance ID) when requested [7]. The device uses the private device key to sign the token, and the caller uses the public device key to verify the token's authenticity. This private/public key pair is described in Section 3.2.3 “Attestation of Platform Genuineness”.

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 ensures that the platform 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.

During production, TOE is generated with its own NIST P-256 device key pair and securely stores the wrapped private key into immutable OTP memory and this key never leaves the device. The corresponding public key is extracted from the device and inserted into a binary DER-encoded X.509 device certificate, which is signed into a Silicon Labs CA chain and then programmed back into immutable OTP memory.

The unique device public key is bound to the device certificate in the certification chain which can be requested remotely from the product is used to verify that the TOE was authentically produced by Silicon Labs. A challenge can be sent to the chip at any point in time to be signed by the device private key. The public key in the device certificate can then be used to verify the challenge response, proving that the device has access to the securely stored private key, which prevents counterfeit products or impersonation attacks.

This implementation is conformant to the Arm PSA Initial Attestation Token standard [6]. It is accessible from the “Attestation” API, described in section “SE Manager” of the guidance documentation [3].

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 a state where no other operation except optionally Secure Update of Platform (section 3.2.6) can be performed.

Conformance rationale:

The secure element runs from ROM out of reset and that ROM image verifies the SE firmware using ECDSA over the P-256 NIST curve (with SHA-512 as the hash operation) against a Silicon Labs public key stored in ROM.

Additionally, when loading ROM patches, the patches are verified using the same algorithmic combination: SHA-512 hash and ECDSA over P-256.

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:

In order to determine that the platform is in a known state, TOE uses Entity Attestation Tokens which include the lifecycle state of the TOE. This process is described in Section 3.2.2 “Attestation of Platform Instance Identity”.

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 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. SE version information is stored in the upgrade manifest, signed by Silicon Labs Root key.

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.

Conformance rationale:

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

- Electromagnetic pulse Glitch Detection
- Supply Glitch Detection
- DPA countermeasure
- RC trigger glitch detector
- Clock jittering
- Redundant/hardened code

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.

3.2.9 Cryptographic Operation

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

Table 6 Cryptographic operations

Algorithm	*Operation*	*Specification*	*Key length (bits)*	*Modes*
AES	*Encrypt, Decrypt, Sign/MAC, Verify*	*NIST FIPS 197* *NIST SP800-38*	*128, 192, 256*	*CTR, CCM, GCM/GMAC*
SHA-256	*Hash*	*NIST FIPS 180-3*	-	-
SHA-512	*Hash*	*NIST FIPS 180-3*	-	-
ECC	*ECDSA, ECDH, EdDSA*	*ANSI X9.62* *FIPS 186-3* *RFC 7748*	*Up to 256-bits*	-

Conformance rationale:

The secure element provide means to generate cryptographic operation according to Table 6.

3.2.10 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 True Random Number Generator module is a non-deterministic random number generator that harvests entropy from a ring oscillator based (thermal) noise source. It includes start-up health tests for the entropy source as required by NIST SP800-90B and AIS-31 as well as online health tests required for NIST SP800-90C. The TRNG is suitable for periodically generating entropy to seed an approved pseudo random nrumber generator.

3.2.11 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in Table 7 as specified in Table 7 for key lengths in Table 7.

Table 7 Cryptographic key generation

ID	Algorithm	Key length (bits)
RAW	AES	128, 192, 256
ECC	Weierstrass curves	192, 256
ECC	Montgomery curves	256
ECC	EdDSA	256

Conformance rationale:

The secure element provide means to generate cryptographic keys according to Table 7. For specifications, refer to Table 6.

3.2.12 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:

Key material in TOE products is protected by "key wrapping" with a standardized symmetric encryption mechanism. The Secure Vault Key Management system uses a Physically Unclonable Function (PUF) to generate a persistent device-unique seed key on power up to dynamically generate this critical wrapping/unwrapping key which is only visible to the AES encryption engine and is not retained when the device loses power.

In addition, KSU contains a Key Slot RAM which is used to store keys that has been unwrapped by SE. KSU has a root-only accessible SLAXI slave bus interface which allows SE to directly access the memory-mapped KSURAM. User bus masters like the Host CPU will not have direct access to the contents in the Key Slot RAM. The idea is to disallow direct access of cryptographic keys except from SE.

3.3 Additional Security Functional Requirements

3.3.1 Secure Communication Support

The secure communication channel authenticates Host Platform and protects against disclosure, modification, replay, erasure of messages between the endpoints.

Conformance rationale:

The mailbox interface is a hardware component that facilitates internal command-and-response communication exclusively between the host and the SE. These connections are internal logical links within the die, with no external access via the physical die or pins.

Communication between the host and the SE is a 1:1 communication, strictly limited to the mailbox interface.

3.4 Optional Security Functional Requirements

3.4.1 Secure Debugging

The platform only provides debug access port authenticated as specified in Section 3.10.4 of [2] with debug functionality.

The platform ensures that all data stored by the application, with the exception of *none*, is made unavailable.

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.

3.4.2 Secure Confidential Storage

The platform ensures that all data stored, except for certificates, calibration data, patch code and any user data, is protected to ensure its confidentiality, integrity, authenticity, and binding to the platform instance.

Conformance Rationale:

The data stored in the OTP is both encrypted and authenticated using AES-GCM, with a PUF-derived key. While the PUF key has a size of 256 bits, the derived key used for encryption is 128 bits. Certificates stored in the OTP are neither encrypted nor authenticated; however, their validity can be confirmed through the signature chain. Calibration data, although not encrypted, undergoes integrity validation using checksums. Patch code stored in OTP is kept in plaintext but is validated via signature verification (ECDSA-P256-SHA512) using the public key stored in ROM.

3.4.3 Secure Data Serialization

The platform ensures that all data stored outside the direct control of the platform, except for user code and user data, is protected such that the authenticity, integrity, confidentiality is ensured.

Conformance Rationale:

The platform interfaces to an external flash memory through a high speed QSPI with dedicated encryption, decryption and authentication hardware. Flash memory contents are managed by the SE and the external memory hardware to provide robust security for program memory.

Flash layout is partitioned into three regions: SE region (MTP area and SE FW), user code and user data. By default, SE region is always encrypted and authenticated. AXiP operates with 256-bit keys in AES-GCM mode.

4 Mapping and sufficiency rationales

This ST and associated TOE provide exact conformance to [SESIP] and [PSA].

4.1 SESIP3 sufficiency

Assurance Class	Assurance Families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introductions	Section "Introduction"	The ST reference is in the "ST Reference", the TOE reference in the "Platform Reference", the TOE overview and description in "Platform Functional Overview and Description".
	ASE_OBJ.1 Security requirements for the operational environment	Section "Security Objectives for the operational environment"	The objectives for the operational environment in "Security Objectives for the operational environment" refers to the guidance documents.
	ASE_REQ.3 Listed Security requirements	Section "Base PP Security Functional Requirements"	All SFRs in this ST are taken from [SESIP].
	ASE_TSS.1 TOE Summary Specification	Section "Security requirements and implementation"	All SFRs are listed per definition, and for each SFR the implementation and verification is defined in Base PP Security Functional Requirements.
ADV: Development	ADV_FSP.4 Complete functional specification	Functional specification is provided in [3].	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	Full source code provided to the evaluators.	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.

Assurance Class	Assurance Families	Covered by	Rationale
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 platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	All the guidance documents are listed in the “Included Guidance Documents” section of the ST.	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	The list of configuration items is available in [9].	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ALC_CMS.1 TOE CM Coverage	The list of configuration items is available in [9].	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	ALC_FLR.2 Flaw reporting procedures	“Flaw Reporting Procedure (ALC_FLR.2)” section in the Security Target and description of which developer evidence is used to meet this requirement.	The flaw reporting and remediation procedure is described.
ATE: Tests	ATE_IND.1 Independent testing: conformance	Vulnerability and testing carried out by the laboratory.	The platform evaluator will determine devise an independent functional test campaign.
AVA: Vulnerability Assessment	AVA_VAN.4 Methodical Vulnerability Analysis	Vulnerability and testing carried out by the laboratory.	The platform evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the platform.

Assurance Class	Assurance Families	Covered by	Rationale
			Penetration testing is performed by the platform evaluator assuming an attack potential of Enhanced-Basic.

5 References

[1] Security Target for Series 3 Secure Vault™, Version 1.3

[2] Silicon Labs, Inc, "SixG301 Wireless SoC Family Datasheet", Rev. 0.5

[3] Silicon Labs, Inc, "SiSDK Platform Documentation", v5.2.0, https://docs.silabs.com/gecko-platform/5.2.0/platform-overview,

[4] Silicon Labs, Inc, "Security Vulnerability Disclosure Policy", https://www.silabs.com/security/security-vulnerability-disclosure-policy

[5] Silicon Labs, Inc, "CRISIS006 - Product Security Incident Response plan (PSIRP), Revision J," March 2023.

[6] 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 19 08 2024].

[7] Silicon Labs, Inc, "AN1268: Authenticating Silicon Labs Devices Using Device Certificates", Rev. 0.4

[8] Silicon Labs, Inc, "AN1504: Series 3 Security Overview", rev 0.1

[9] Silicon Labs, Inc, "Series 3 Secure Vault™ on SixG301 SESIP Configuration Item List", Version 0.5

[10] Silicon Labs, Inc, "Simplicity Commander User Guide", v1.17.4, https://docs.silabs.com/simplicity-commander/latest/simplicity-commander-start/

[SESIP] GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP) Methodology, version 1.2, GP_FST_070.

[PSA] SESIP Profile for PSA Certified Level 4 iSE/SE or RoT Component, Version 2.0 BETA.

6 Abbreviations

Term	Definition
AXiP	Authenticated Execute-in-Place
BLE	Bluetooth Low Energy
DCI	Debug Challenge Interface
DMA	Direct Memory Access
DPA	Differential Power Analysis
EXiP	Encrypted Execute-in-Place
HSE	Hardware Secure Engine
KSU	Key Slot Unit
NSPE	Non-secure Processing Environment
NVM	Non-Volatile Memory
OTP	One-Time Programmable
PSA	Platform Security Architecture
PUF	Physically Unclonable Function
QSPI	Quad Serial Peripheral Interface
RNG	Random Number Generator
RoT	Root of Trust
SE	Secure Element
SRK	Storage Root Key
SPE	Secure Processing Environment
SoC	System-on-a-Chip
ULP	Ultra-Low Power
XiP	Execute-in-Place

7 Revision history

v1.0	Updated
v1.1	Added DCI acronym to the list of acronyms. Removed references to documentation that was not needed. Updated ROM and SE FW version numbers. Updated product name.
v1.2	Updated product name.
v1.3	Updated reference in section 1.1, Table 3 and References