Infineon Edge Protect Secure Enclave

SESIP Security Target

Table of contents

1 Introduction

1.1 ST reference

This ST's title is "Infineon Edge Protect Secure Enclave" version 1.2 dated 2025-09-29.

1.2 SESIP Profile Reference

Reference	Value
PP name	SESIP Profile for PSA Certified Level 4 iSE/SE or RoT Component
PP version	2.0 BETA REL 03
Assurance Claim	SESIP Assurance Level 3 (SESIP3)
SESIP standard	[GP-SESIP][GP-SESIP]
Optional and additional SFRs	none

1.3 Platform Reference

Table 1 Subsystem Reference

Reference	Value	
Platform name	Infineon Edge Protect Secure Enclave	
Platform version	No overall version identifier available	
Platform Identification	hardware	Silicon: 0xED91 Family: 0x0115 Revision: 0x22 (B1)
	PSA-RoT name and version	BASE_SE_RT_SERVICES: 1.0.0.2361 SE_RT_SERVICES (including Crypto functions): 1.1.0.2735 SROM Boot: 2.0.0.6022 RRAM Boot: 2.0.0.7127
Platform type	Integrated Secure Enclave	

1.4 Included Guidance Documents

Table 2 Guidance Documents

Reference	Name	Version
[PSOC84_HRM]	PSoC™ Edge E84 MCU architecture, Preliminary Reference manual	2023-11-09
[SetupMan]	Early Access Pack for Modus Tool Box (Secure Services Utility)	V3.2.0

Reference	Name	Version
[SE_RT_Services]	SE RT Services Utilities Library (doxygen documentation)	V1.1.0
[GettingStarted]	Getting started with PSOC™ Edge security	2025-04-28
[Provisioning]	PSOC™ Edge provisioning specification	2025-04-28
[ST]	See section 6	See section 6

Note: part of the secure acceptance procedure is to check platform identification, which has to match the versions from Table 1. The version information can be extracted from the IDE tool Modus Toolbox, when connecting to the debugger. Among others this information is read from the device and output to the console.

Note: in case security services of the TOE are used, integrity and/or confidentiality of provided input data have to be ensured by the environment, up to the point, where the TOE receives these data in context of the application. Further integrity and/or confidentiality of received output data, from the point, where these leave the TOE also have to be ensured depending on the context of the application. E.g. if input data to a cryptographic decryption service of the TOE are not protected by the environment, the plain output data may be incorrect. Performing decryption twice can be a measure to detect manipulation of input data during transfer.

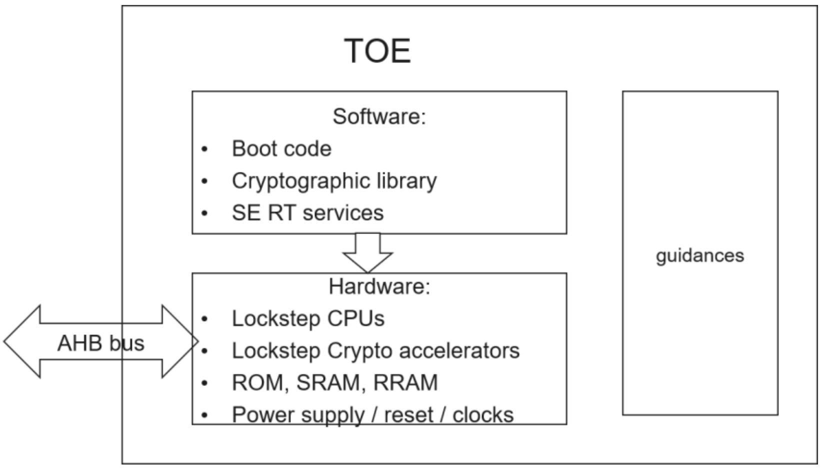
1.5 Platform Functional Overview and Description

1.5.1 Platform type

The platform type is an integrated secure enclave within a SOC.

1.5.2 TOE Physical Scope

Figure 1 TOE physical scope



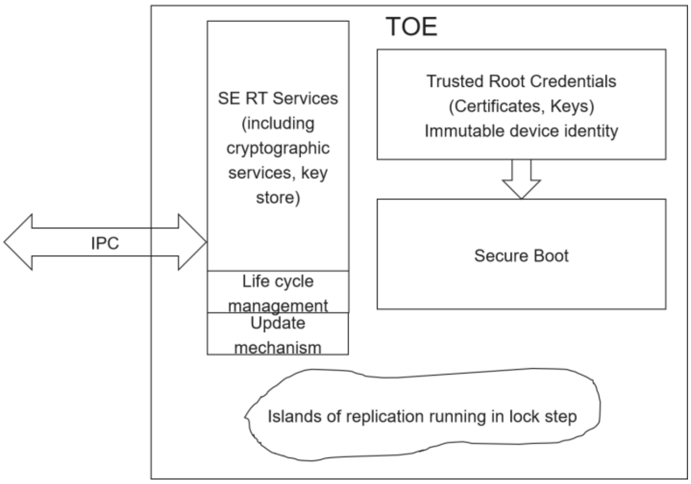
The platform consists of a combination of software, hardware and guidance documents. The hardware is an integrated secure enclave. It is a semicustom part of an SoC. The software is stored in a dedicated RRAM. Guidance documents and software code remain with the developer, i.e. user guidance is kept within the developer's premises, as there is no intention to provide the TOE to external users. In fact the TOE hardware can only be provided as semicustom logic embedded into a SoC. The SoC is PSoC™ Edge E84 MCU. PSoC™ Edge E84 interfaces to the TOE hardware via AHB. A user of PSoC™ Edge E84 does not have direct access to the TOE. It can only use dedicated services of the TOE, which are available via an IPC.

1.5.3 Usage and Major Security Features

The platform is integrated into Infineon specific microcontrollers, which are built for a variety of consumer and industrial applications including HMI, smart home, wearables, robotics, and other smart connected IoT products.

The draft as follows summarizes the most important security features:

Figure 2 TOE major security features



The platform features:

- Immutable RoT Anchor
- Update mechanism for mutable SE RT services
- Lockstep CPU and temperature sensor against fault attacks, sidechannel resistant cryptographic library
- Cryptographic support
    - AES: CMAC, ECB, CBC, CTR, CCM
    - ECDSA
    - ECDH
    - DRBG based on AES CTR
- Cryptographic Key Store, which stores e.g. HUK and ECDSA private and public keys.
- Management of secure life cycle states
- Access to the TOE restricted to IPC interface in operation mode.

1.5.4 Required Hardware/Software/Firmware

The hardware of the TOE is part of an integrated SOC and depends on other silicon parts to function correctly, which are power supply, clocks, external RRAM (NVM memory) and AHB interfaces. However, any malfunction or unavailability of these external entities do not impact security of the TOE. The TOE software does not depend on other software. It is the first component to boot up the system.

2 Security Objectives

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

Table 3

ID	Description	Reference
KEY_MANAGEMENT	Cryptographic keys and certificates outside of the platform are subject to secure key management procedures.	[Provisioning] section 1.1 "Provisioning overview"
TRUSTED_USERS	Actors in charge of platform management, for instance for signature of firmware update, are trusted.	[Provisioning] section 1.1 "Provisioning overview"
ACCEPTANCE	Platform users shall verify that the platform version is consistent with the evaluated version.	Follow the method defined in section 3.3.1 of [ST] and verify that the versions obtained are consistent with Table 1 of this ST.
DATA_TRANSFER	The level of protection by the environment may be lower than the protection provided by the TOE. In this case the user has to be aware, that data transferred to and from the TOE needs additional protection to achieve the same security level of the TOE	See section 1.4

Note: Uniqueness of the unique identification of the platform is provided by the platform and is therefore not an objective to the environment.

3 Security Requirements and Implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is SESIP3.

3.2 Flaw Reporting Procedure (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:

Flaws can be reported following the procedures as described in https://www.infineon.com/cms/en/about-infineon/company/cybersecurity/

3.3 Security Functional Requirements from Base PP

3.3.1 Verification of Platform Identity

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

Conformance rationale: The version information can be extracted from the IDE tool Modus Toolbox, when connecting to the debugger. Among others this information is read from the device and output to the console.

3.3.2 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 a state where no other operation except optionally Secure Update of Platform can be performed.

Conformance rationale: ROM boot is the first code that is executed after any type of Reset. This boot code verifies the next stage immutable boot code in RRAM via a mechanism called hash locking (for further information see [PSM]), which then verifies SE RT services, also via hash locking. The hashes are integrity protected. In case of SE RT services the hash is updated and authenticity is checked as part of a FW update.

3.3.3 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: for the secure update SE RT services an application in RAM is used. The image is copied to SRAM by the application and hash is calculated. Finally signature and hash is verified before image update. For signature generation and verification ECDSA-256 is used.

3.3.4 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: Lockstep CPU and Crypto processor to prevent fault attacks, sidechannel hardened cryptographic library, Temperature sensor to prevent extreme temperatures from triggering faults, semicustom logic to harden against easy reverse engineering.

3.3.5 Cryptographic Operation

The platform provides the application with Operations in functionality with algorithms in Table 4 as specified in specifications in Table 4 for key lengths described in Table 4 and modes described in Table 4.

Table 4 Cryptographic Operations

Algorithm	Operations	Specification	Key lengths	Modes
AES	AEAD	[FIPS197] [NIST800-38C]	128	CCM
ECDSA	Signature generation	[FIPS186-5] section 6.4 Hashing the message is not implemented. Pre-hashed input is required. The only supported curve is P-256 according to [NIST800-186]	256	
AES	Block cipher	[FIPS197] [NIST800-38A] sections 6.2, 6.5	128, 256	ECB, CBC, CTR,
ECDH	Raw Key agreement (scalar multiplication)	[NIST800-56A] Section 5.7.1.2 Step 1 The only supported curve is P-256 according to Appendix D Table 24.	256	
AES	Key derivation	[FIPS197] [NIST800-38B] [NIST800-108r1_upd1] section 4.1	128, 256	CMAC
AES	Message authentication	[FIPS197] [NIST800-38B]	128,	CMAC

Conformance Rational: The cryptographic operations utilize a hardware Crypto accelerator, which supports AES and EC cryptographic calculations.

Note: For AES cipher only non-volatile keys are claimed.

3.3.6 Cryptographic Random Number Generation

The platform provides a way based on *AES CTR DRBG* to generate random numbers to as specified in [NIST800-90A] section 10.2.

Conformance Rational: A hardware TRNG of the TOE is used to seed the DRBG. In order to achieve prediction resistance the DRBC uses AES-128 from the Crypto accelerator.

3.3.7 Cryptographic Key Generation

The platform provides a way to generate cryptographic keys for use in cryptographic algorithms in Table 5 as specified in specifications in Table 5 for key lengths described in Table 5.

Table 5 Cryptographic Key Generation

ID	Algorithm	Specification	Key lengths
ECDSA	ECDSA	[FIPS186-5] section 6.2.1 with A.2.1	256
AES	AES	DRBG according to section 3.3.6	128, 256

Conformance Rationale: The TOE utilizes the AES CTR DRBG from section 3.3.6 to generate these keys.

3.3.8 Cryptographic Key Store

The platform provides a way to store assets as specified in Table 6 such that not even the application can compromise the attributes as specified in Table 6 of this data. This data can be used for the cryptographic operations as specified in Table 6.

Table 6 Cryptographic Assets

Asset	Attributes	Cryptographic operation
HUK (Hardware Unique Key),	Integrity & confidentiality	AES key derivation
OEM RoT public key	Integrity	ECDSA signature verification
IFX SE RT SERVICES public key	Integrity	ECDSA signature verification
IFX RoT public key	Integrity	ECDSA signature verification
Device Key: DICE generated (or provisioned) device unique asymmetric private key	Integrity & confidentiality	ECDSA signature generation
Attestation private key	Integrity & confidentiality	ECDSA signature generation
Attestation public key	Integrity	ECDSA signature verification

Protected FW RoT Public Key	Integrity	ECDSA signature verification
Protected FW Key	Integrity & confidentiality	AES key derivation
Custom keys (can be provisioned by OEM)	Integrity & confidentiality	
IFX Keys (can be provisioned by IGFX only)	Integrity & confidentiality	

Conformance rational: Cryptographic keystorage is implemented in secured non volatile RRAM. The keys are generated/imported during provisioning.

3.3.9 Secure Communication Support

The SFR “secure Communication Support” is not claimed. Protection is provided by means of access control. Only instances of the host with dedicated security level can utilize the IPC channel. Additionally TOE’s semicustom logic harden it against easy reverse engineering and successful probing/forcing attacks.

4 Mapping and Sufficiency Rationales

4.1 Assurance

The assurance activities defined in this Profile fulfil the SESIP3 activities and extend the Vulnerability Assessment assurance to AVA_VAN.4.

Table 7 assurance to AVA_VAN.4.Assurance – Evidence Mapping

Assurance Class	Assurance Family	Covered by
ASE: Security Target Evaluation	ASE_INT.1 ST Introduction	This document chapter 1
	Rationale: this chapter is dedicated and reviewed to meet these requirements	
	ASE_OBJ.1 Security requirements for the operational environment	This document chapter 2
	Rationale: this chapter is dedicated and reviewed to meet these requirements	
	ASE_REQ.3 Listed Security requirements	This document chapter 3
	Rationale: this chapter is dedicated and reviewed to meet these requirements	
	ASE_TSS.1 TOE Summary Specification	From this document the rationales from chapter 3
	Rationale: TSS is merged with the security requirements, as it also described, how these are implemented	
ADV: Development	ADV_FSP.4 Complete functional specification	This document chapter 1.4, especially [PSOC84_HRM] and
	Rationale: the guidance documents describe all interfaces and user functionality of the TOE.	
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	This task was carried out by the evaluator during joint code review.
	Rationale: there is a dedicated mapping table between source code and TSF	
AGD: Guidance Documents	AGD_OPE.1 Operational user guidance	See [SE_RT_Services]
	Rationale: These guidelines provide sufficient guidance to operate the TOE in a secure way. It is one of the evaluation tasks to assure this.	
	AGD_PRE.1 Preparative procedures	[GettingStarted]
	Rationale: These guidelines provide sufficient guidance to receive, accept and prepare the TOE in a correct wy. It is one of the evaluation tasks to assure this.	
ALC: Life-cycle Support	ALC_CMC.1 Labelling of the TOE	ALC.xlsx, v1.1, 2025-09-29
	Rationale	
	ALC_CMS.1 TOE CM Coverage	ALC.xlsx, v1.1, 2025-09-29
	Rationale:	
	ALC_FLR.2 Flaw reporting procedures	This document chapter 3.2
	Rationale: the link provided allows externals to report flaws of the TOE to Infineon Technologies AG.	

Assurance Class	Assurance Family	Covered by
ATE: Tests	ATE_IND.1 Independent testing: conformance	Witnessing session performed at 11th of September 2025 and logfiles provided on 15th of September 2025: ■ bootfw_logs.zip ■ rt_services_logs.zip ■ WitnessingSession_20250911.xlsx
	Rationale:	
AVA: Vulnerability Assessment	AVA_VAN.4 Methodical vulnerability analysis	Vulnerability and testing carried out by the laboratory
	Rationale:	

5 Abbreviations

HMI	Human-Machine Interface
IOT	Internet of Things
IPC	Inter Process Communication
iSE	integrated Secure Enclave
SE RT	Secured Enclave Runtime
SE RoT	Secured Enclave Root of Trust

6 References

[FIPS186-5] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (Supersedes FIPS 186-4) Digital Signature Standard (DSS), February 3, 2023

[FIPS197] FIPS, Advance Encryption Standard (AES), November 26, 2001; Updated May 9, 2023

[GP-SESIP] Security Evaluation Standard for IoT Platforms (SESIP) v1.2

[NIST800-108r1_upd1] NIST Special Publication 800 NIST SP 800-108r1-upd1 Recommendation for Key Derivation Using Pseudorandom Functions, August 2022

[NIST800-186] NIST Special Publication NIST SP 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters, February 2023

[NIST800-38A] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation Methods and Techniques, December 2001

[NIST800-38B] NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005

[NIST800-38C] NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004

[NIST800-56A] NIST Special Publication 800-56A Revision 3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, April 2018

[NIST800-90A] NIST Special Publication 800-90A Revision 1 Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015

[PP] SESIP Profile for PSA Certified Level 4 iSE/SE or RoT Component, 2.0 BETA REL 03

[GettingStarted] Getting started with PSOC™ Edge security, 2025-04-28

[Provisioning] PSOC™ Edge provisioning specification, 2025-04-28

[PSM] Platform Security Model, JSADEN14, v1.1, 2021-12-01

[PSOC84_HRM] PSoC™ Edge E84 MCU architecture, Preliminary Reference Manual, 2023-11-09

[SE_RT_Services] SE RT Services Utilities Library (doxygen documentation), V1.1.0

[SetupMan] Early Access Pack for Modus Tool Box (Secure Services Utility), V3.2.0

[ST] Infineon Edge Protect Secure Enclave, SESIP Security Target, v1.2, 2025-09-29

7 Revision history

Document version	Date of release	Description of changes
0.1	2024-11-13	Initial beta version
0.2	2024-11-19	Some adaptations to SE only component
1.0	2025-06-11	Initial stable version
1.1	2025-09-26	Change design step -> B1; updated se rt services version; added environmental objective; changed method of identification
1.2	2025-09-29	Editorial changes; correction of “Mapping and Sufficiency Rationales”

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2025-09-29

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email: erratum@infineon.com

Document reference