PUFsecurity

PUFcc Security Target using SESIP Profile for PSA Certified™ RoT Component Level 3

psacertified™
level three

Document number:	PUFcc
Version:	1.2 REL
Release Number:	07
Author:	PUFsecurity PSA JSA Members: Applus+ Laboratories Arm Limited CAICT ECSEC Laboratory Inc Prove & Run S.A.S. Riscure B.V. Serma Safety & Security S.A.S. SGS Brightsight B.V. TrustCB B.V. UL TS B.V.
Authorized by:	PSA JSA Members
Date of Issue:	07/05/2024

Abstract

PSA Certified is the independent security evaluation scheme for Platform Security Architecture (PSA) based IoT systems. It establishes trust through a multi-level assurance program for chips containing a security component called a Root of Trust (PSA-RoT) that provides trusted functionality to the platform. The multi-level scheme has been designed to help device makers and businesses get the level of security they need for their use case.

PSA Certified Level 3 is a fixed time, test laboratory based, evaluation of the PSA-RoT. It is aimed at IoT devices that need to protect against substantial physical and software attacks. The Level 3 documents include: a SESIP Profile that describes the Target of Evaluation, its assets, the security objectives and security functions that will be evaluated and an Attack Methods (AM) document describing the attacks in scope.

Developers submit their PSA-RoT to an approved test laboratory, listed on **www.psacertified.org**, for Level 3 evaluation and receive an Evaluation Technical Report. If the PSA-RoT is assessed as passing and approved by the independent Certification Body, a digital certificate will be issued on the PSA Certified website.

Keywords

PSA Certified Level 3, SESIP, Certification, IoT, Platform Security Architecture, Questionnaire, PSA, Security

Non-Confidential Proprietary Notice

This document is protected by copyright and other related rights and the practice or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm. No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether implementations infringe any third-party patents.

THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document consists solely of commercial items. You shall be responsible for ensuring that any use, duplication or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word "partner" in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

If any of the provisions contained in these terms conflict with any of the provisions of any click through or signed written agreement covering this document with Arm, then the click through or signed written agreement prevails over and supersedes the conflicting provisions of these terms. This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of the Agreement shall prevail.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. Please follow Arm's trademark usage guidelines at http://www.arm.com/company/policies/trademarks.

Arm Limited. Company 02557590 registered in England.
110 Fulbourn Road, Cambridge, England CB1 9NJ.

Contents

1 About this document

1.1 Current Status and Anticipated Changes

Current Status: Published, version 1.2 REL 07.

1.2 Release Information

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

Date	Version	Confidentiality	Change
2024-05-07	1.2 REL 07	Non-confidential	Update hard-macro version.
2024-04-18	1.2 REL 06	Non-confidential	Update document version numbers.
2024-04-01	1.2 REL 05	Non-confidential	Update document version numbers.
2024-02-27	1.2 REL 04	Non-confidential	Revision.
2024-02-15	1.2 REL 03	Non-confidential	Revision.
2024-01-17	1.2 REL 02	Non-confidential	Update document version numbers.
2024-01-11	1.2 REL 01	Non-confidential	Update version numbers.
2023-12-31	1.1 REL 04	Non-confidential	Revision.
2023-12-21	1.1 REL 03	Non-confidential	Revision.
2023-12-20	1.1 REL 02	Non-confidential	Revision.
2023-11-28	1.1 REL 01	Non-confidential	Scope clarification and SFR revision.
2023-11-10	1.0 REL 03	Non-confidential	Revision.
2023-10-26	1.0 REL 02	Non-confidential	Add firmware version, ADV_IMP.3, and some minor changes
2023-08-23	1.0 REL 01	Non-confidential	PUFsecurity PUFcc PSA RoT Component Level 3 derived from [PSA-L3-Comp]

1.3 References

This document refers to the following documents.

1.3.1 Normative references

Ref	Doc No	Author(s)	Title
[PSA-L1]	JSADEN001	JSA	PSA Certified Level 1 Questionnaire
[PSA-EM-L2]	JSADEN003	JSA	PSA Certified: Evaluation Methodology for PSA L2
[PSA-EM-L3]	JSADEN010	JSA	PSA Certified: Evaluation Methodology for PSA L3
[PSA-AM]	JSADEN004	JSA	PSA Certified Attack Method
[PSA-PP-L2]	JSADEN002	JSA	PSA Certified Level 2 Lightweight Protection Profile
[PSA-PP-L3]	JSADEN009	JSA	PSA Certified Level 3 Lightweight Protection Profile
[SESIP-PP-L2]	JSADEN012	JSA	SESIP Profile for PSA Certified™ Level 2
[SESIP-PP-L3]	JSADEN011	JSA	SESIP Profile for PSA Certified™ Level 3
[PSA-L2-Comp]	JSADEN017	JSA	SESIP Profile for PSA Certified™ RoT Component Level 2
[PSA-L3-Comp]	JSADEN018	JSA	SESIP Profile for PSA Certified^{TM} RoT Component Level 3
[SESIP]	GP_FST_070	GlobalPlatform	Security Evaluation Standard for IoT Platforms (SESIP) v1.1
[CEM]	CCMB-2017-04-004	Common Criteria	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, revision 5, April 2017.

1.3.2 Informative references

Ref	Doc No	Author(s)	Title
[GP-ROT]	GP_REQ_025	GlobalPlatform	Root of Trust Definitions and Requirements, Version 1.1, Public Release, June 2018
[PSA-SM]	ARM DEN 0128	Arm	Platform Security Model 1.1

1.4 Terms and Abbreviations

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

Term	Meaning
API	Application Programming Interface
Application	Used in this SESIP Profile to refer to the components which are out of the scope of the evaluation.
Application Root of Trust Service(s)	Application specific security service(s) that are not defined by PSA. Such services execute in the Secure Processing Environment and are required to be in Secure Partitions.
Application Specific Software	Software that provides the functionality required of the specific device. This software runs in the Non-Secure Processing Environment, making use of the System Software, Application RoT Services and PSA-RoT Services.
Critical Security Parameter	Secret information, with integrity and confidentiality requirements, used to maintain device security, such as authentication data (passwords, PIN, certificates), secret cryptographic keys, etc..
Evaluation Laboratory	Laboratory or facility that performs the 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
HRoT	Hardware Root of Trust
Hardware Unique Key (HUK)	Secret and unique to the device symmetric key that must not be accessible outside the PSA Root of Trust. It is a Critical Security Parameter.
Host Platform	Used in this SESIP Profile to refer to the entity which when used in composition with the platform form a PSA Level 2 certifiable PSA-RoT (including any PSA-RoT Services).
Initial Attestation Key (IAK)	A PSA-RoT secret private key from an asymmetric key-pair used to sign attestation reports, thus ensuring that the report is bound to a unique PSA-RoT (and so device) instance.
KDK	Key-derivation key
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.
OTP	One-time programmable memory
Partition	The logical boundary of a software entity with intended interaction only via defined interfaces, but not necessarily isolated from software in other partitions. Note that both the NSPE and SPE may host partitions.
Platform	Used in this SESIP Profile to refer to the components which are in the scope of the evaluation.
PRoT	Platform Root-of-Trust
PSA	Platform Security Architecture

Term	Meaning
PSA Certification Body	The entity that receives applications for PSA security certification, issues the certificates, maintains the security certification scheme, and ensures consistency across all the evaluation laboratories.
PSA Functional APIs	PSA defined Application Programming Interfaces on which security services can be built. APIs defined so far include Crypto, Secure Storage and Attestation.
PSA Functional API Certification	Functional certification confirms that the device implements the PSA Functional APIs correctly by passing the PSA Functional certification test suites.
PSA Root of Trust (PSA-RoT)	The PSA defined combination of the Immutable Platform Root of Trust and the Updateable Platform Root of Trust and is considered to be the most trusted security component on the device. See [PSA-SM].
PUF	Physically unclonable function
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.
ROTPK	Root-of-trust public key
SESIP Profile	Document providing a common set of functionalities for similar products
Secure Partition	A Partition in the Secure Processing Environment.
Secure Processing Environment Partition Management	Management of the execution of software in Secure Partitions. Typical implementations will provide scheduling and inter partition communication mechanisms. Implementations may also enforce isolation between the managed Secure Partitions.
Secure Processing Environment (SPE)	The processing environment that hosts the PSA-RoT, and any Application RoT Service(s).
Secure Boot	The process of verifying and validating the integrity and authenticity of updateable firmware and software components as a pre-requisite to their execution. This must apply to all the firmware and software in the SPE. It should also apply to the first NSPE image loaded, which may extend the NSPE secure boot chain further.
Security Target (ST)	Document providing an implementation-dependant statement of security of a specific identified platform.
System Software	NSPE software that may comprise an Operating System or some run-time executive, together with any middleware, standard stacks and libraries, chip specific device drivers, etc., but not the application specific software.

Term	Meaning
TRNG	True random number generator
TOE	Target of Evaluation. In this SESIP Profile it is a synonym for Platform.
Trusted subsystem	A security subsystem that the PSA-RoT relies on for protection of its assets, or that implement some of its services.

1.5 PSA Certified Level 3

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

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

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

Two evaluation paths are currently possible for a PSA Certified Level 3 product, either through the PSA Certified Level 3 Protection Profile [PSA-PP-L3] and associated evaluation methodology [PSA-EM-L3], or through a SESIP evaluation using the SESIP Profile for PSA Certified Level 3 [SESIP-PP-L3].

1.5.1 PSA Certified Level 3 Root of Trust Component Certification

The PSA Certified scheme allows for certification of components that address a subset of the security functions required by an implementation for a Level 2 or Level 3 certifiable PSA Root-of-Trust (RoT). A typical example is an IP block that will be used in a chip. The IP could address a few security functions, with the rest of the chip covering all other requirements. Another example is an external chip that addresses a subset of the security functions, which when connected to another chip form a complete Level 2 or Level 3 certifiable PSA-RoT.

In PSA-SM such parts of a Level 2 or Level 3 certifiable chip are referred to as a Trusted Subsystem, which can be subject a Root-of-Trust Component (or RoT Component) certification. The intermediate step of certifying a RoT Component allows composite certification. This is especially beneficial as the RoT Component can be used in many chip products needing a Level 2 or Level 3 certified PSA-Root-of-Trust.

This component profile is based on the existing [SESIP-PP-L3]. The difference is that, where in [SESIP-PP-L3] all the SFRs that are required to meet PSA Certified requirements are mandatory, in this profile they are all optional. However, the SESIP process mandates that all Security Targets must include the “Verification of Platform Identity” SFR, and all must either include the “Secure Update of Platform” SFR or argue under ALC_FLR.2 why updates are not applicable [SESIP].

2 Introduction

This SESIP profile covers the platform types which implement a subset of the SFRs (Security Functional Requirements) described in [SESIP-PP-L3], with the goal of being re-used in a platform which targets conformance with [SESIP-PP-L3].

Due to the heterogeneity of the types of platforms that can claim conformance to this SESIP profile, no effort guideline is included for the AVA_VAN.2 activities as there is in [SESIP-PP-L3].

In this SESIP Profile the term Platform should be read as the PSA-RoT Component that implements the specific subset of SFRs described in any Security Target prepared against this profile. The Platform is intended to be used in composition with a Host Platform, which, in this SESIP Profile is referred to as the Application. Together, the Platform and the Application should form a PSA-RoT suitable for certification against [SESIP-PP-L2] or [SESIP-PP-L3].

For consistency, in the remainder of this document the term Platform refers to the PSA-RoT Component and the term Application refers to Host Platform.

2.1 SESIP Profile Reference

Reference	**Value**
PP Name	SESIP Profile for PSA Certified RoT Component Level 3
PP Version	See title page.
Assurance Claim	SESIP Assurance Level 3 (SESIP 3)
Optional and additional SFRs	- Verification of platform instance identity - Attestation of platform genuineness - Cryptographic operation - Cryptographic random number generation - Cryptographic key generation

Table 1: SESIP Profile Reference

2.2 Platform Reference

The platform is uniquely identified by its hardware and/or software references, depending on the platform type.

Reference	Value	
Platform Name	PUFcc – A PUF-based crypto coprocessor	
Platform Version	v1.0.1, see also Table 4 for the versions of the platform components	
Platform Identification	Hardware project code	PIF0P3, PSCC_SESIP_vM.m.b*
	Firmware version	v3.5.1
Platform type	A PUF-based hardware crypto coprocessor with included firmware and API. The exported API functions are expected to be integrated into the PRoT software running in SPE to provide the UID, HUK, OTP, TRNG, and cryptographic operations.	

*The version is represented as vM.m.b, where M, m, and b are the major version number, the minor version number, and the bug fix revision respectively.

Table 2: Platform Reference

2.3 Included Guidance Documents

The following documents are included with the platform:

Reference	Name	Version
[PUFcc-RN]	PUFcc Release Note	v1.0.1.a
[PUFcc-DS]	PUFcc Datasheet	v1.1
[PUFcc-IN]	PUFcc Integration Note	v1.2
[PUFcc-AN]	PUFcc Application Note (Memory Mapped Register)	v1.3
[PUFcc-ADG]	PUFcc API Development Guide	v1.0
[PUFcc-AUG]	PUFcc API User Guide	v3.5.1.a
[PUFcc-TM]	PUFcc Test Methodology	v1.0
[PUFcc-DAG]	PUFcc Device Attestation Guide	v1.1
[PUFcc-KSG]	PUFcc Key Security Guide	v1.0

Table 3: Guidance Documents

2.4 Platform Functional Overview and Description

2.4.1 Platform Type

The platform is a secure coprocessor composed of a PUF-based HRoT, a cryptographic coprocessor, and the firmware which exports API functions. The platform is expected to be integrated in the PRoT software as described in Figure 10 in [PSA-SM], providing the UID and HUKs derived from a built-in PUF, the OTP secure storage, the TRNG, and standard cryptographic operations. The hardware part of the PUFcc platform, including a sequencer, is securely updatable, and the firmware is updatable.

To perform the evaluation, Arm AN552, the Corstone-300 subsystem with Cortex-M55 CPU, is used as the host platform, the firmware and API are ported to Trusted Firmware-M (TF-M), and the whole system runs on MPS3

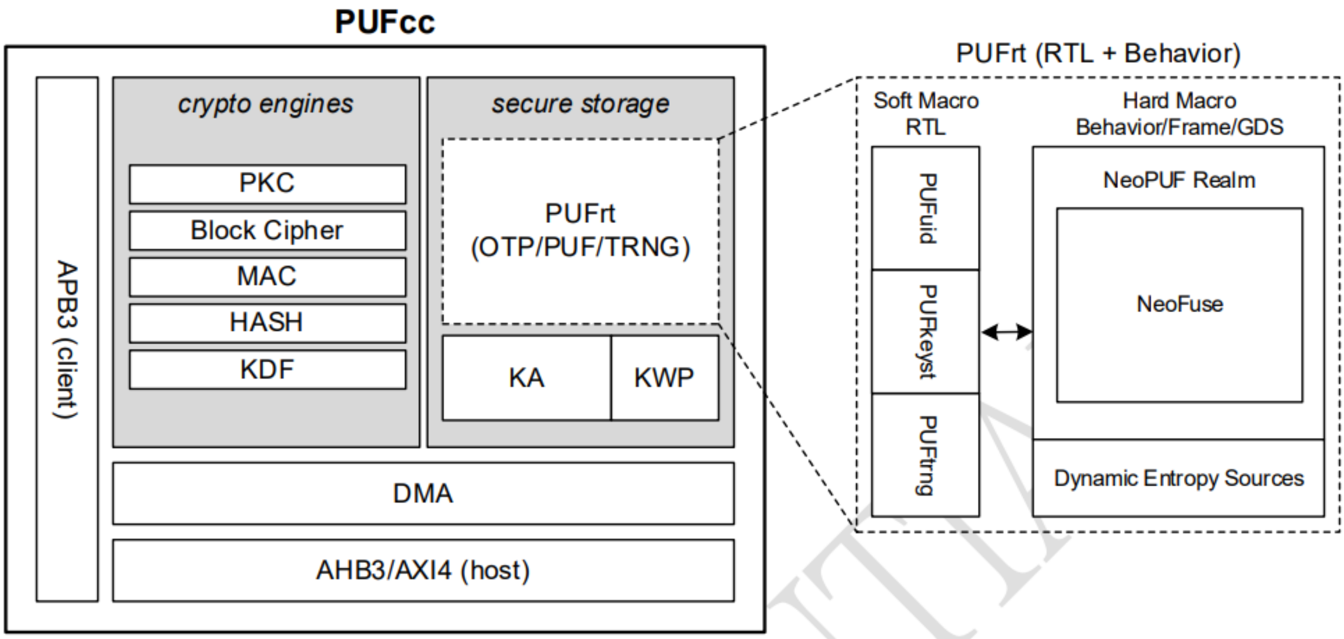
FPGA prototyping board. Note that the reference host platform AN552 and the TF-M itself are not part of the certification.

2.4.2 Physical Scope

The platform, from bottom to top, consists of the hard-macro, the Verilog RTL design, and the firmware. The guidance documents listed in Table 3 are also provided.

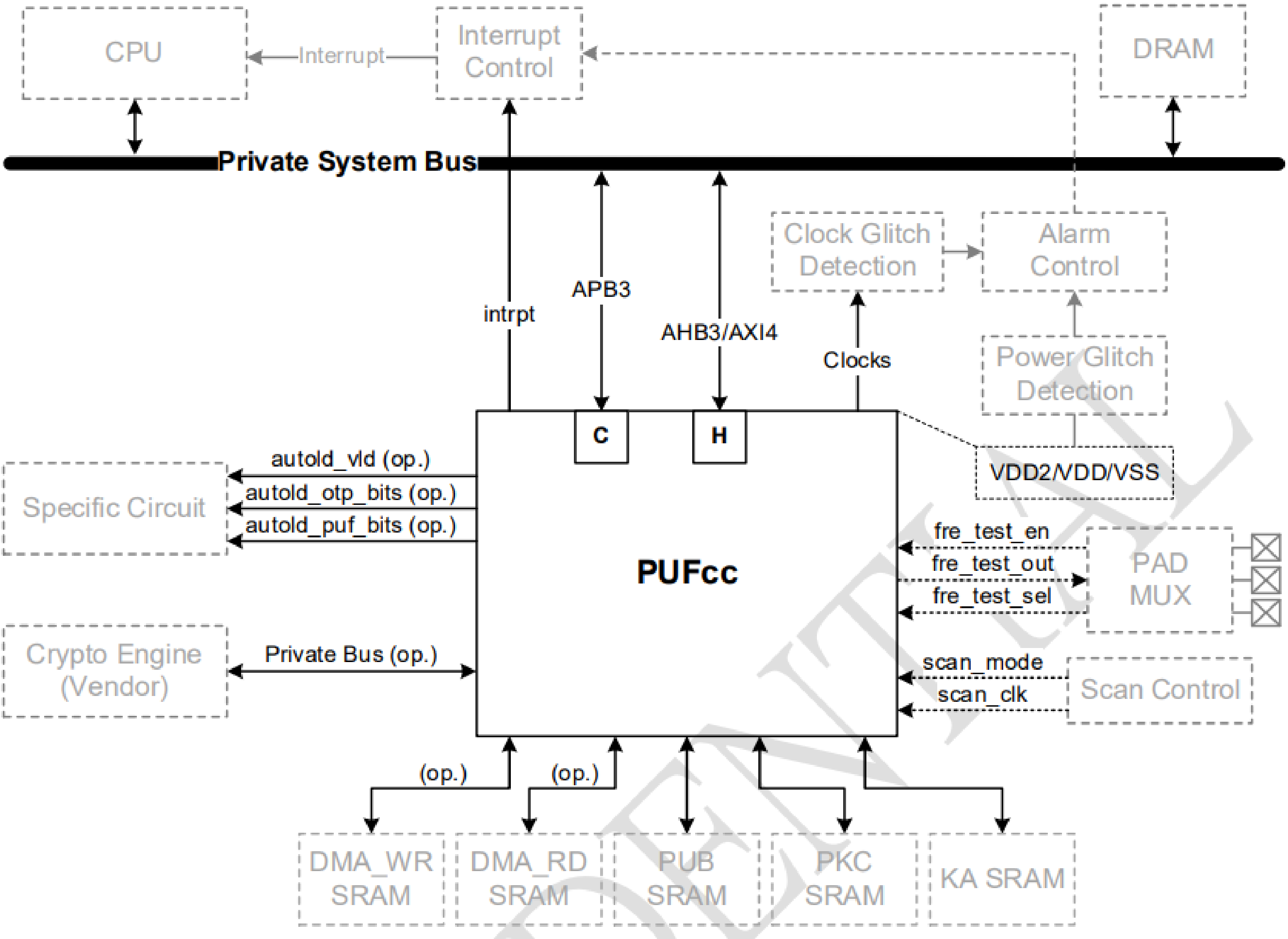
The hard-macro includes the analog circuit design of the PUF cells, the OTP cells, and several physical entropy sources. The hard-macro supports the operations of PUF enrollment, UID read, HUK read, OTP programming, OTP read, entropy retrieval, etc.

The Verilog RTL design includes the functions described in this paragraph. To initiate the hard-macro operations, the RTL is used to create the waveforms to interact with the hard-macro. Thus, it allows the integrated system to use the register interface to access the hard-macro functions. The access control to the data resident in the hard-macro is also handled by the RTL (via the register interface). This is designed to protect the confidentiality of the HUKs and the data stored in the OTP. Besides access control, there are additional mechanisms designed for other security purposes. For example, data zeroization is designed to support lifecycle management; data shuffle and data scramble are designed to prevent data leakage caused by physical attacks. The TRNG is built using the entropy sources of the hard-macro. To avoid key leakage, the standard cryptographic algorithms are implemented in PUFcc, eliminating the need to export the cryptographic keys stored or generated in PUFcc. Examples of such keys include the HUKs, the keys derived from said HUKs, and any keys provisioned and stored in the OTP. The DMA host, supporting either AHB3 or AXI4 protocol, is designed to handle the data flow between outside memory and the cryptographic engines of PUFcc. The register interface of the cryptographic operations is also designed in RTL. A full list of the supported cryptographic operations can be found in Section 2.4.4 below.



The hardware modules of PUFcc, including the Verilog RTL design and the hard-macro, are shown in the figure above. Note that the TOE hardware includes the Verilog RTL design and the behavioral model of the hard-macro on the FPGA board. That is, the behavioral model emulates the hard-macro by FPGA. Hence, only source code reviews of the hard-macro design will be performed, and any penetration testing on the protection provided by the hard-macro will be out of scope of this certification program.

The following figure shows an example system integration of PUFcc. The elements in the dotted boxes are external to PUFcc. Therefore, these elements are assumed to function properly, and are also out of scope of this evaluation.



The firmware controls the functions of the Verilog RTL design by interacting with its register interface. It also provides the API functions for the software to utilize the functionalities provided by the hardware. The API functions can be used to read UID, to read and program the OTP, to generate random bits from the TRNG, to set the access permissions of the data stored in the hard-macro, to zeroize the data resident in the hard-macro, and to perform the cryptographic operations. The API functions are expected to be integrated into the PRoT software of a host platform to provide the HRoT and cryptographic operations.

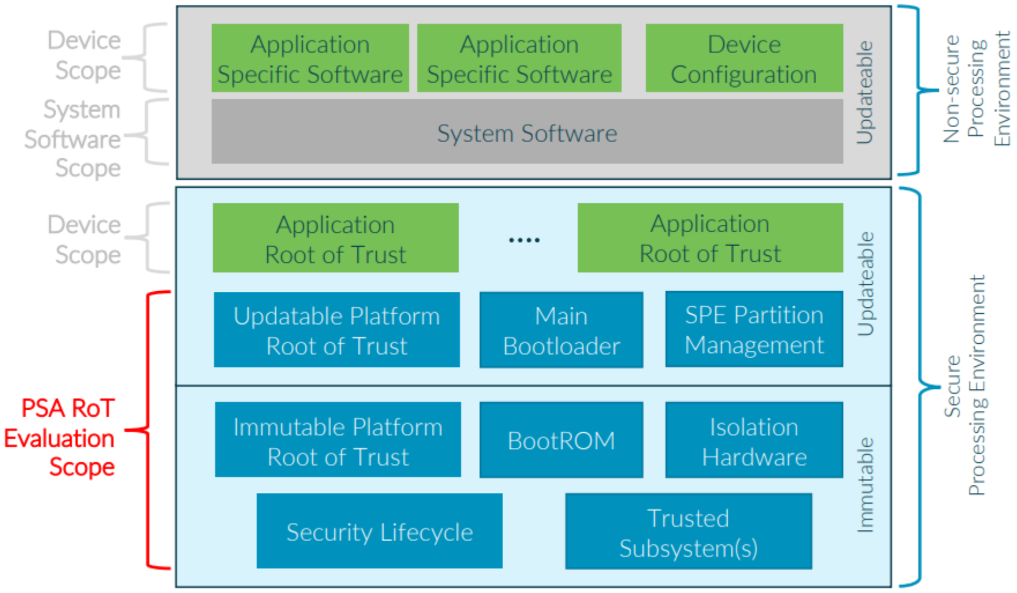
The delivery method for each piece of the platform and their corresponding versions are listed in Table 4.

Deliverables	Submodules	Version	Form of delivery
Hard-macro		EGP128X32UA028CW07	Hard-macro netlist, GDS, and timing liberty files by authorized download
Verilog RTL design	DMA	0x505000A3	Verilog and encrypted Verilog files by authorized download
	CRYPTO	0x50465003	
	SP38A	0x33384101	
	SP38B	0x33384200	
	SP38C	0x33384302	
	SP38D	0x33384402	
	SP38E	0x33384501	
	SP38F	0x33384600	
	HMAC/HASH	0x31393801	
	KDF	0x35364301	
	ABUF	0x414C4200	
	DRBG	0x39304100	
	A90A	0x39304120	
	KA	0x505001A2	
	PKC	0xECF79305	
	RNG	0x39304200	
	CFG	0x30D70005	
Firmware		See Table 2.	C source files by authorized download
Guidance documents		See Table 3.	PDF files by authorized download

Table 4: Platform Deliverables and Versions

2.4.3 Logical Scope

The scope of an implementation for a PSA Certified Level 2 or Level 3 PSA RoT is shown in the following figure. By the correct and secure integration, the PUFcc hardware will form a trusted subsystem, and the firmware will be integrated into the PRoT software, providing Level 2 or Level 3 certifiable chip its security functions, including PUF, OTP, TRNG, and cryptographic operations.



2.4.4 Usage and Major Security Features

The platform supports the following major security features:

To form a secure IoT device, PUFcc is responsible for establishing the HRoT of the host platform by providing the HUKs and by securely storing the root-of-trust information such as the ROTPK. PUFcc also offers standardized cryptographic operations to prevent key leakage to the system or to software that is external to the platform. The following security features provided by PUFcc to the host platform are listed below.

- Secure OTP storage
  - Anti-fuse OTP (divided into two sections)
    - OTP section 1 of size 8Kbits
      - First 7Kbits of this section can be planned by the host platform.
      - The last 1K bits OTP is used to store the CRC-32 for OTP and PUF.
    - OTP section 2 of size based on the capacity of the hard-macro.
      - It can be planned by the host platform.
      - Stored key data is followed by its corresponding CRC-32.
  - Permanent access control, determined by the system
    - Each segment of the OTP storage can be set to read-write (RW) access, read-only (RO) access, or non-accessible (NA) access. Note that OTP data with NA access can still be read by the Verilog RTL design.
  - Slot-based, temporary access restriction
    - Access to each slot can be individually restricted so that the system and even the Verilog RTL design cannot access the slot.
    - This access restriction is temporary, released after any system reset.
  - Slot-based erasure of OTP section 1
    - The command to erase the data of each slot can be individually issued.

- PUF
  - 1K bits of read-only values, derived from PUF
    - One 256-bit UID
    - Three 256-bit HUKs
      - These HUKs are restricted to be used for the key derivation functions in the Verilog design. They cannot be used by other cryptographic operations and cannot be read out by the system.
      - The derived keys are restricted to be used in the the Verilog design instance. Hence, these HUKs can be used to derive the device-specific keys for security services such as secure storage.
  - Temporary access restriction by 256-bit slots
    - Access to each slot can be individually restricted so that the system and even the Verilog RTL design cannot access the slot.
    - This access restriction is temporary, released after any system reset.
  - Permanent erasure by 256-bit slots
    - The command to erase the data of each slot can be individually issued.
- Hardware security mechanisms for hard-macro mass production
  - OTP secure repair to mitigate a limited number of broken OTP cells by redundant cells.
  - PUF quality check to ensure the PUF stability in variant voltages and temperatures.
  - PUF health check to ensure the equal distributions of 0’s and 1’s in the values derived from the PUF.
- Random number generation
  - True random number generation (TRNG) that meets the requirements defined in the NIST SP800-90B and AIS31.
  - Pseudo random number generation (PRNG)
    - Certified NIST SP800-90A counter-mode deterministic random bit generator (CTR-DRBG)
- Cryptographic operations
  - Cryptographic hash functions
    - SHA2 variants: SHA2-256, SHA2-384, SHA2-512, and SHA2-512/256
  - Block cipher algorithms
    - AES with 128-bit, 192-bit, and 256-bit key sizes
  - Message authentication code
    - Hash-based message authentication code (HMAC) with max key size 512 bits
      - HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, and HMAC-SHA2-512/256
    - Cipher-based message authentication code (CMAC)
      - AES-CMAC
  - Block cipher modes of operation
    - Electronic codebook mode (ECB)
    - Cipher feedback mode (CFB)
    - Output feedback mode (OFB)

  - Cipher block chaining mode (CBC)
  - CBC mode with ciphertext stealing variant 1 (CBC-CS1)
  - CBC mode with ciphertext stealing variant 2 (CBC-CS2)
  - CBC mode with ciphertext stealing variant 3 (CBC-CS3)
  - Counter mode (CTR)
  - Counter mode with CBC-MAC (CCM)
  - Galois/Counter mode (GCM)
  - XEX-based tweaked-codebook mode with ciphertext stealing (XTS)
  - Key wrap mode (KW)
  - Key wrap with padding mode (KWP)
- Key derivation functions (KDF)
  - Key-based KDF (KBKDF) functions
  - Password-based KDF (PBKDF) version 2
  - HMAC-based KDF (HKDF)
  - Internet Key Exchange (IKE) version 1 KDF functions
  - IKEv2 KDF functions
  - X9.63-2001 KDF
  - TPM KDF
  - TLS v1.2 KDF
  - SSH KDF
- Public key cryptosystems
  - Rivest-Shamir-Adleman (RSA) cryptosystems
    - Modular exponentiation operation
      - Supported key sizes
        - 3072-bit and 4096-bit key sizes
    - RSA signature schemes
      - X9.31 RSA signature scheme
      - PKCS#1 v1.5 signature scheme
      - Probabilistic signature scheme (RSA-PSS)
  - Elliptic curve cryptosystems (ECC)
    - Supported elliptic curves
      - 9 NIST suggested elliptic curves
        - B283, B409, B571, K283, K409, K571, P256, P384, and P521
      - Public key derivation from the private key
      - Public key validation
      - Elliptic curve Diffie-Hellman (ECDH) key exchange
      - Elliptic curve digital signature algorithm (ECDSA) signing and verification

  - Cryptographic key generation
    - Key sources
      - Ephemeral key generation from RNG and other controllable inputs
      - Static key generation from only controllable inputs
        - Device-specific key generation from the HUK and other controllable inputs
    - Key usages
      - Symmetric key generation for all the symmetric key cryptosystems with arbitrary key sizes supported by PUFcc
      - Asymmetric key generation for ECC cryptosystems for all the elliptic curves supported by PUFcc
- Cryptographic key store
  - The integrity of the keys stored in PUFcc are protected by CRC-32.
  - Non-volatile key storage
    - Three 256-bit HUKs derived from PUF
      - Inborn keys of the device which cannot be modified except through erasure.
    - Keys stored in OTP
      - Keys of arbitrary length may be stored in the OTP.
      - The keys can be protected by using either permanent access control mechanisms or temporary access restriction settings.
  - Volatile key storage
    - Key array (KA)
      - Components
        - 1Kbits space for symmetric keys partitioned into eight 128-bit slots, where at most 4 slots can be combined to store a 512-bit key
        - Three spaces for private keys of at most 576 bits long
        - 2Kbits of temporary space for shared secret
      - The key array in PUFcc aims to temporarily hold the symmetric or asymmetric keys that will be used by its cryptographic operations.
      - The keys in the key array can only be read out in encrypted form by KW or KWP with the device-specific key-encryption key (KEK). In this way, no other device can successfully import and use an exported key.
      - The integrating platform's key management system can adopt the PUFcc mechanisms to build their own secure key storage.
- Secure update mechanism for the PKC sequencer
  - The sequencer itself cannot be updated, but the microprograms executed on it can.
  - Before execution, the microprogram must be CMAC verified against the supported microprogram version and the hard-coded hardware key. One OTP word (32 bits) is used to store that version as the anti-rollback mechanism so that the older versions of microprograms cannot be executed.
- Countermeasures for physical attacks
  - See Section 4.2.3.

2.4.5 Required Hardware/Software/Firmware

For proper functionality, PUFcc requires 3 SRAM, PUB SRAM, PKC SRAM, and KA SRAM, as described in "suggested integration example" section in [PUFcc-IN]. For security consideration, the clock glitch detector and the power glitch detector are also needed for physical attack detection.

3 Security Objectives for the operational environment

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

ID	Description	Reference
PUF_ENROLLMENT	The PUF of this platform is expected to be enrolled so that the device-specific PUF can be used to derive an intrinsically random 256-bit UID and the HUKs.	[PUFcc-TM] *Production Flow;* [PUFcc-AN] *Section 31.18.*
UNIQUE_ID	After PUF enrollment, the platform provides 256-bit UID. (See PUF_ENROLLMENT) Although the probability is negligible to have the same UID created from different PUFs, the actors in charge of the application management shall ensure that no UIDs will conflict.	[PUFcc-ADG] *Section 3.4.*
SECURE_INTEGRATION	The “Security Consideration for Integration and Package” section in [PUFcc-IN] must be followed when performing the hardware integration. In addition, the host platform is expected to connect to the PUFcc via a private system bus so that only the PRoT software can access the platform register interface. In addition, the the access control mechanism is expected to be built in this service to ensure the applications use PUFcc functions in a secure and correct way.	[PUFcc-IN]*;* [PUFcc-ADG].
PLATFORM_GENUINENESS	The provided firmware is expected to be used by the PRoT software to verify the versions of all PUFcc submodules and to attest the platform genuineness as described in [PUFcc-DAG].	[PUFcc-ADG] *Section 2.2*; [PUFcc-DAG].
TRUSTED_USERS	Actors in charge of host platform management are trusted. That is, they will not sign a vulnerable boot image for update nor attempt to bypass the host platform security functionalities.	[PUFcc-IN]; [DEN 0128]
KEY_MANAGEMENT	The HUKs of the platform are restricted to be used as KDKs to derive the keys for applications using KDF functions. The PRoT software is expected to manage the access of the keys stored in the PUFcc OTP to prevent one application from accessing the keys of others. Cryptographic keys and certificates outside of the platform are subject to secure key management procedures.	[DEN 0128]; [PUFcc-KSG]
CRYPTO	The applications are expected to select cryptographic algorithms with appropriate key lengths to fulfill their security requirements.	*Table 6*; *Table 7.*
SECURE_INITIALIZATION	The host platform is expected to use a secure boot flow to ensure the genuineness of the software.	[DEN 0128]
SECURE_UPDATE	The sequencer is designed with secure update mechanism with the anti-rollback feature. The host platform is expected to apply the secure update, including secure communication for download, the integrity and authenticity check for the update image, and the anti-rollback feature for the PRoT software update.	*Section 2.4.4.*
LIFECYCLE_MANAGEMENT	The host platform is expected to configure the lifecycle state according to the stages of the product development and deployment. In particular, the PUFcc test mode shall be locked before deployment, and the HUKs and keys stored in the OTP shall be zeroized before being decommissioned.	[PUFcc-TM] *Production Flow;* [PUFcc-ADG] *Section 4.9, 4.10.*
ACCESS_CONTROL	The access to PUFcc register interface must be restricted to the PRoT software which runs in SPE. Moreover, the PRoT binding must be implemented to protect misuse of cryptographic keys.	[PUFcc-IN]; [DEN 0128]; [PUFcc-KSG]

Table 5: Security Objectives for the Operational Environment

4 Security Requirements and Implementation

4.1 Security Assurance Requirements

The claimed assurance requirements package is SESIP3 as described in Section 5.1.

4.1.1 Flaw Reporting Procedure (ALC_FLR.2)

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

PUFsecurity has *defined* a product security incident response process (PSIRP) to deal with the hardware and software vulnerabilities. This process includes the following four major steps using a publicly available website for reporting flaws.

1. Reporting.

The support center (**https://pufsecurity.atlassian.net/servicedesk/customer/portals**) is used for customers to report a found flaw to the dedicated team for mitigation. A “ticket” will be created on the support center to track and record any communications or follow-ups regarding the vulnerability. The reporter will receive an acknowledgement and all updates in the flaw handling process. The reporter can further interact with the dedicated team if necessary.

2. Evaluation.

The dedicated team will first confirm the potential vulnerabilities that have been reported. If the vulnerabilities are confirmed, the risk and impact will be assessed by the dedicated team and the product team. An assessment report will be created documenting the following information.

- Reporter and Discovery Date
- Assigned owner in the product team
- Description, symptoms, and the root cause of the vulnerability
- List of affected customers
- Required design changes and mitigative workaround with estimated schedule of completion

The assessment report will be filed and registered in an internal database.

3. Solution.

The platform is a combination of hard-macro, Verilog RTL design, and the firmware. Each of the affected customers will be assigned one or more members from the dedicated team. For other customers also affected by the same vulnerability, the notification up till resolution will also be recorded independently on the support center website. A solution will be provided in general; however, in some cases the design cannot be updated such as the chip is fabricated or the firmware is fixed in ROM code, a workaround can be provided as an additional security guidance, a updated driver, or a recommendation on the operating environment. In short, the dedicated team will also propose to implement a design change or workaround according to the stage of development (e.g. RTL integration stage, or after chip fabrication) a customer is currently under. The bug fix revision or the minor version is bumped for the workaround or the solution respectively.

4. Communication.

Upon completion of aforementioned design change and workaround, it will be delivered to every affected customer by the secure communication channel established previously. The channel will either be the customer's preferred method or default secure channel. The default secure channel will be established by:

- Customers are required to provide fixed IP address(es)
- An account of customer will be created and used to access PUFsecurity FTP/SFTP site
- Only designated account owner using a whitelisted IP address can access sensitive deliverables
- The deliverables will be removed from the FTP/SFTP site after a certain period of time (e.g. 7 days)

4.2 Base PP Security Functional Requirements

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

4.2.1 Verification of Platform Identity

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

Conformance rationale:

The versions of submodules in the Verilog RTL design are accessible by reading the version registers of the submodules. The reference values of these versions are shown in Table 4. The firmware also provides the initialization API to check all the versions of submodules as described in [PUFcc-ADG] Section 2.2.

The firmware version is readable by using the firmware version API as described in [PUFcc-ADG] Section 2.1. The reference value of the firmware version is also shown in Table 4.

4.2.2 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 platform includes the hardware, including the hard-macro design and the Verilog RTL design, and the firmware. The hardware portion is generally immutable, except for the sequencer which executes CMAC-verified microprograms. The sequencer itself cannot be updated, but the microprograms executed on it can. Before the microprogram is executed, the augmented CMAC value must be verified against the microprogram itself, the supported microprogram version, and the immutable hard-coded hardware key. To securely update the microprogram with the anti-rollback property, the supported microprogram version is stored in OTP. Then, once the supported microprogram version is bumped, the old CMAC values are invalid so that the old microprograms cannot be executed anymore. In other words, the sequencer only permits the execution of microprograms of the updated version. Therefore, the hardware part can be securely updated. On the other hand, though the firmware is updatable, the secure update cannot be achievable by the platform itself due to the lack of processor. As a result, the secure update of firmware part is considered out of scope of the evaluation.

In the composing platform that the firmware is expected to be integrated into the PRoT software, the secure update mechanisms of the host platform shall be used for secure firmware update of this platform.

4.2.3 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 following physical attack protections are developed on the hard-macro portion of the platform.

- Intrinsic physical security
- Countermeasures for voltage contrast attack
- Top metal shielding
- Security-oriented IP layout
- Active sense-amplifier read protection
- Hidden and obfuscated data interface
- Unified program power to prevent electrical analysis
- Power detection of VDD/VDDIO floating

The countermeasures adopted in Verilog RTL design to resist physical attacks are shown as follows.

- Device specific data address scrambler and I/O shuffler for the OTP and PUF using its PUF
- PUF and OTP output data fault detection
- Random dummy insertion read for the PUF and OTP
- Entropy source health check
- Fault injection prevention on mode, address, and post-masking mechanism for the PUF and OTP
- Control protection with redundancy for PUFrt, public key operations (RSA/ECC), and key wrapping operations (KWP)
- Key check by cyclic redundancy check (CRC) for RSA/ECC, key bus (KB), and KWP.
- Elliptic curve point validation for public key operations (ECC)
- Exponent blinding and message blinding for modular exponentiation operations (RSA)
- Scalar blinding and projective coordinates blinding for elliptic curve operations (ECC)
- Boolean masking for block cipher operations (AES) and SHA-2 operations
- Dual core lock step for block cipher operations (AES) and hash operations (SHA2)
- Error detection code (EDC) for SRAM interfaces

4.3 SFRs for PSA-RoT Component

4.3.1 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 platform provides a 256-bit UID derived from its PUF as the platform instance identity. The 256-bit UID is readable by using the read PUF API as described in [PUFcc-ADG] Section 3.4.

4.3.2 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 platform provides the device attestation key to the host platform so that the host platform can obtain and store the device attestation public key of this platform. Then, after the verification of the platform identity and the platform instance identity, the host platform can issue a random message as a challenge to the platform to get the digital signature of the random message signed by the device attestation key. With the stored public key of the device attestation key, the host platform can verify the digital signature against the public key to attest the platform genuineness. Please refer to the [PUFcc-DAG] document for the attestation procedure.

4.3.3 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.

Algorithm	Operations	Specification	Key lengths	Modes
AES	Encryption/decryption	NIST FIPS 197 NIST SP800-38A	128-bit 192-bit 256-bit	ECB
SHA-2	Secure hash	NIST FIPS 180-4	N/A	SHA2-256, SHA2-384, SHA2-512, SHA2-512/256
RSA	Digital signature	ANSI X9.31 PKCS#1 v1.5 PKCS#1 v2.1	3072-bit, 4096-bit	ANSI X9.31 RSA signature, PKCS#1 v1.5 RSA signature, RSA-PSS signature
ECC	Digital signature	FIPS 186-5	NIST curves: B283, B409, B571, K283, K409, K571, P256, P384, P521	ECDSA
	Key exchange	NIST SP800-56Ar3		ECC CDH
	Public key validation			Public key validation

Table 6: Cryptographic Operations

Conformance rationale:

The AES engine, the SHA-2 engine, and the public key coprocessor are designed to resist physical attacks such as side channel attacks and fault injection attacks. The firmware provides the cryptographic operation API functions as described in [PUFcc-ADG] Section 7 to Section 17. The PRoT software is expected to build the access control management mechanisms as described in ACCESS_CONTROL to prevent the key materials of an secure partition from being used by other partitions.

4.3.4 Cryptographic Random Number Generation

The platform provides the application with a way based on several oscillator rings to generate random numbers to as specified in NIST SP800-90B.

Conformance rationale:

The entropy sources are provided by the hard-macro, and the post-processing algorithm for random number generation is implemented in Verilog RTL design. The generated random bitstream passes the NIST SP800-22, NIST SP800-90B, and AIS31 statistical test suites.

4.3.5 Cryptographic Key Generation

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

ID	**Algorithm**	**Specification**	**Key lengths (bits)**
AES-128	AES-128	N/A	128
AES-192	AES-192	N/A	192
AES-256	AES-256	N/A	256
HMAC	HMAC	N/A	Up to 512
ECC B283	ECC	FIPS 186-5	283
ECC B409	ECC	FIPS 186-5	409
ECC B571	ECC	FIPS 186-5	571
ECC K283	ECC	FIPS 186-5	283
ECC K409	ECC	FIPS 186-5	409
ECC K571	ECC	FIPS 186-5	571
ECC P256	ECC	FIPS 186-5	256
ECC P384	ECC	FIPS 186-5	384
ECC P521	ECC	FIPS 186-5	521
KDF	KDF	N/A	Up to 512

Table 7: Cryptographic Key Generation

Conformance rationale:

The firmware provides the cryptographic key generation API as described in [PUFcc-ADG] Section 16, Section 17.1, and Section 17.5. The PRoT software is expected to build the access control management mechanisms as described in ACCESS_CONTROL to prevent the key materials of an secure partition from being used by other partitions.

4.4 Additional Security Functional Requirements

<complete this section with the additional SFRs defined in [SESIP].>

4.4.1 Secure Communication Support – PUFcc Control Register Interface

The platform provides the application with one or more secure communication channel(s).

Conformance rationale:

By the proper hardware integration of the platform as defined in SECURE_INTEGRATION, the host platform connects to the PUFcc control register interface through a private system bus. The access to the control register interface of the platform is dedicated to the PRoT software so that the dedicated communication channel cannot be accessed or modified from the external.

4.4.2 Secure Communication Support – PUFcc DMA Host Interface

The platform provides the application with one or more secure communication channel(s).

Conformance rationale:

By the proper hardware integration of the platform as defined in SECURE_INTEGRATION, the host platform connects to the PUFcc DMA host interface through a private system bus. Furthermore, the DMA host interface is managed by the platform itself. Thus, the security of the communication between the platform and the host platform is ensured.

4.4.3 Secure Communication Enforcement

The platform ensures that the application can only communicate with **trusted subsystems** over the secure communication channel(s) supported by the platform using the dedicated communication channel.

Conformance rationale:

The PUFcc hardware is a trusted subsystem with two interfaces: a host interface, connecting to the system bus, is managed by the platform itself for cryptographically operational data transmission, and a client interface for control register access. By the proper hardware integration of the platform as defined in SECURE_INTEGRATION, the host platform connects to the PUFcc through a private system bus, and the access to the control register interface of the platform is dedicated to the PRoT software. That is, the private system bus is the only way to access the platform, and thus the security of the communication between the platform and the host platform is enforced.

In addition, by the proper access control mechanism as defined in SECURE_INTEGRATION built in the PRoT software, the secure communication between the platform and other PRoT or other applications in either SPE or NSPE is also enforced.

4.5 Optional Security Functional Requirements

5 Mapping and Sufficiency Rationales

5.1 Assurance

The assurance activities defined in [PSA-EM-L3] fulfil the SESIP3 activities. In particular, the required source code review, vulnerability analysis and testing of the [PSA-EM-L3] is applicable.

Assurance Class	Assurance Family	Covered by
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section 2 and the title page of the Security Target
	Rationale: The ST reference is in the Title, the platform reference is in Section 2.2, and the platform functional overview and description is in Section 2.4.	
	ASE_OBJ.1 Security requirements for the operational environment	Section 3.
	Rationale: The objectives for the operational environment in Section 3 refer to the sections of this ST and the guidance documents.	
	ASE_REQ.3 Listed Security requirements	Section 4.
	Rationale: All SFRs in this ST are taken from SESIP. “Verification of Platform Identity” is included. “Secure Update of Platform” is included.	
	ASE_TSS.1 TOE Summary Specification	Section 4.
	Rationale: All SFRs are listed per definition, and for each of the selected SFRs the implementation and verification are defined in Sections 4.2, 4.3, 4.4, and 4.5.	
ADV: Development	ADV_FSP.4 Complete functional specification	Functional specification as specified in Section 2.3.
	Rationale: The interfaces provided by the platform are documented in the functional specification.	
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	The implementation representation of the security features is introduced in Section 2.4.4, and the mappings to the SFRs are described in Section 4.2, 4.3, 4.4, and 4.5.
	Rationale: The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.	
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	Documents listed in Section 2.3; Section 2.4.5.
	Rationale: The operational user guidance describes secure usage of the user accessible functions.	
	AGD_PRE.1 Preparative procedures	Documents listed in Section 2.3 and Section 2.4.5.
	Rationale: The preparative procedures describe how the platform is configured into a secure state.	

ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	Section 2.2.
	Rationale: The platform is clearly identified as stated in this ST.	
	ALC_CMS.1 TOE CM Coverage	Section 2.2, and documents listed in Section 2.3.
	Rationale: Configuration items are properly identified.	
	ALC_FLR.2 Flaw reporting procedures	Section 4.1.1.
	Rationale: The flaw reporting and remediation procedure is described.	
ATE: Tests	ATE_IND.1 Independent testing: conformance	Materials provided to the platform evaluator.
	Rationale: The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.	
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis	Vulnerability and testing carried out by the laboratory
	Rationale: The platform evaluator performs penetration testing, to confirm that potential vulnerabilities cannot be exploited in the operational environment for the platform. Penetration testing is performed by the platform evaluator assuming an attack potential of Enhanced-Basic.	

Table 8 : Assurance Mapping and Sufficiency Rationales

5.2 PSA Security Functions Mapping

PSA Security Function	Covered by SESIP SFR
F.FIRMWARE_ UPDATE	Secure Update of Platform
F.CRYPTO	Cryptographic Operation
	Cryptographic Random Number Generation
	Cryptographic Key Generation
F.ATTESTATION	Verification of Platform Identity
	Verification of Platform Instance Identity
	Attestation of Platform Genuineness
F.PHYSICAL	Physical Attacker Resistance
Additional security functionality	5.2.1 Secure Communication Support – PUFcc Control Register Interface The platform provides the application with one or more secure communication channel(s). **Conformance rationale:** By the proper hardware integration of the platform as defined in SECURE_INTEGRATION, the host platform connects to the PUFcc control register interface through a private system bus. The access to the control register interface of the platform is dedicated to the PRoT software so that the dedicated communication channel cannot be accessed or modified from the external. Secure Communication Support
	Secure Communication Enforcement

Table 9 Functionality Mapping and Sufficiency Rationales