IDEMIA StarChip

SCE900U version A

Public Security Target

Abstract

Public Security Target of the Product SCE900U.

Revision:

Rev	When
1.1	13/02/2024
2.0	23/07/2025
2.1	02/09/2025

Table of contents

List of Figures

List of Tables

1 Introduction

1.1 ST Reference

This document is the SCE900U public security target referenced **SEC242** version **2.1**.

1.2 TOE Reference

The Target Of Evaluation (TOE) is the secure IC, SCE900U version **A.**
The TOE is identified by each component defined in next chapter.

1.3 TOE identification:

1.3.1 Hardware component (IC)

- Chip name: SCE900U
- HW version ➔ A

1.3.2 Software component

- Bootloader version: **IDSLD SCE900U FLD 1.11.0**.
- Secure BootROM version 4.

1.3.3 Guidance documentation:

Operational user guidance:

- **[TEP124]** “SCE900U Technical Datasheet” v2.2
- **[TEP129]** “ SCE900U Erratasheet” v2.0
- **[TEP130]** “SCE900U Security Guidance” v1.2
- **[TEP131]** “IDSLD Secure Bootloader Guidance and functional specification” v1.1
- **[Ref1] “**Cortus APS3CD Programmers’ Reference Manual”

Preparative procedure guidance:

- **[TEP133]** “Preparative Procedure for SCE900U” v1.0

The guidance is delivered by IDEMIA StarChip according to IDEMIA StarChip Security policy. The documents are sent in PDF format, PGP encrypted using a secure channel (like a Secure FTP). Only authorized contacts under NDA are allowed to receive the guidance.

1.4 TOE Overview

1.4.1 TOE Type

Hardware secure Chip:
The SCE900U is a low-power, full Flash 32-bit microcontroller.
SCE900U embeds the state-of-the-art security peripherals and global architecture, StarChip® technology.

Dedicated software bootloader:

The TOE includes a software bootloader.
The IDEMIA Secure Bootloader is an embedded application designed to run on a secure smartcard. Its purpose is to program the non-volatile memory of the chip with a client application.

1.4.2 TOE Usage

SCE900U is designed to target SIM and M2M market.

1.4.3 TOE Major Security Features

Hardware secure Chip:

The SCE900U embeds the state-of-the-art security peripherals:

- AES
- PKI Accelerator
- Secured Memories
- True Random Number Generator
- Environmental Protection System
  - Frequency and Power Supply monitors
  - Active Shield
- Memory Protected Area
- Code Signature Mechanism
- Random Process Interrupt
- Unpredictable Index Generator
- Memory Protection Unit

Dedicated software bootloader:

The software bootloader implements a mutual authentication between the programming terminal and the TOE The software bootloader offers cryptographic features to secure the authentication mechanism.

The IDSLD is only meant to be used during the composite product integration phase. It is erased after software loading and before the composite product is issued to the end-user.

1.5 Non-TOE hardware/software/firmware required by the TOE.

None.

1.6 TOE Description

The TOE, is composed of the secure IC, SCE900U, with the dedicated software bootloader, IDSLD.

Guidance for the TOE is described in chapter 1.3.3.

NB: The TOE is intended to be used for a Security IC composite product. This Security IC composite product will comprises:

- The TOE (IC)
- The Security IC Embedded (Soft-coded Security IC Embedded Software stored in Flash Memory) and
- User Data (especially personalization data and other data generated and used by the Security IC Embedded Software).

1.6.1 TOE Hardware description

Hardware secure Chip:

General
- CORTUS 32 bits core
- Advanced Low power modes
- Internal Clock oscillator (VFO)
- ESD Protection
- Class A, B and C supported

Memory
- Flash Non volatile Memory
- RAM Memory
- 20 years data retention
- Flash Size configurable by User Embedded Software

Security
- AES 128/192/256
- GF(p) PKI Accelerator (with Montgomery support method)
    - Allows to calculate RSA up to 4096 bits
    - Allows to calculate ECC over GF(p), up to 521 bits
    - DMA access to RAM for fast PKI operations
- Secured Memories
    - Data Encryption
    - Error Detection Code
- True Random Number Generator ([ANSSI-PG-83] compliant)
- Environmental Protection System
    - Frequency and Power Supply monitors
    - Active Shield
- Memory Protected Area defined by software
- Unique Serial Number and Identifier per chip
- Code Signature Mechanism
- Random Process Interrupt
- Unpredictable Index Generator
- Memory Protection Unit

Peripherals
- Smart Card ISO7816 Controller
- GPIO interface
    - SPI
    - I2C
    - DMA
- Random Number Generator
- CRC-16/32 Engine
- 32 bits Counter

Conditions
- Operating Temperature:
    - SIM applications: -25°C to +85°C
    - M2M applications: -40°C to +105°C

The following figure summarizes TOE logical scope for HW:

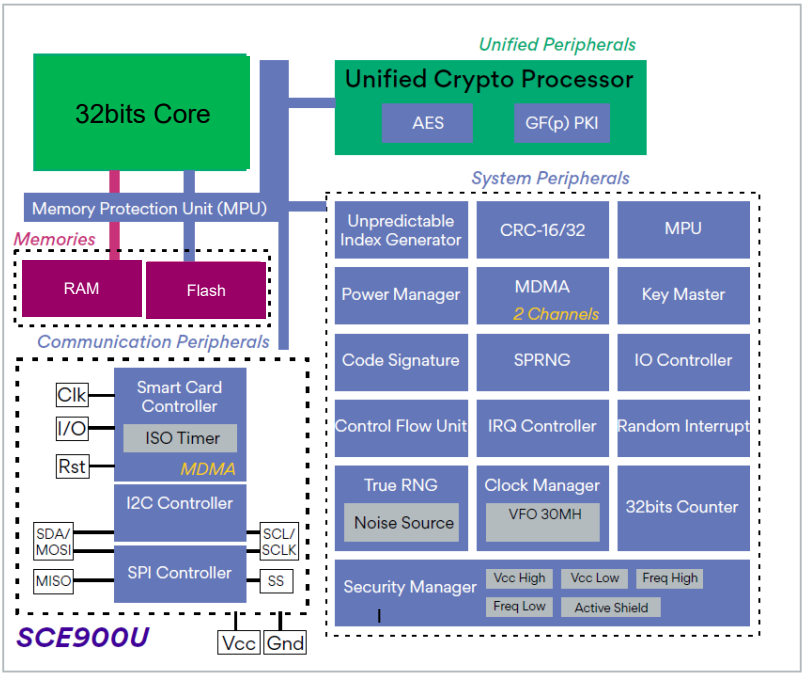


Figure 1: Block Diagram

1.6.2 TOE software bootloader description:

The software bootloaders (IDSLD) is an embedded application designed to upload a client application into the SCE900U NVM and execute it.

IDSLD uses typically three main scenarios:

- Programming a client application into the NVM via ISO7816 communication with a mutual authentication stage.
- Booting into a programmed client application.
- Giving back control to IDSLD for a client application upgrade/erase via a “restore” command.

1.6.3 Development Life Cycle

The following figure details development life cycle

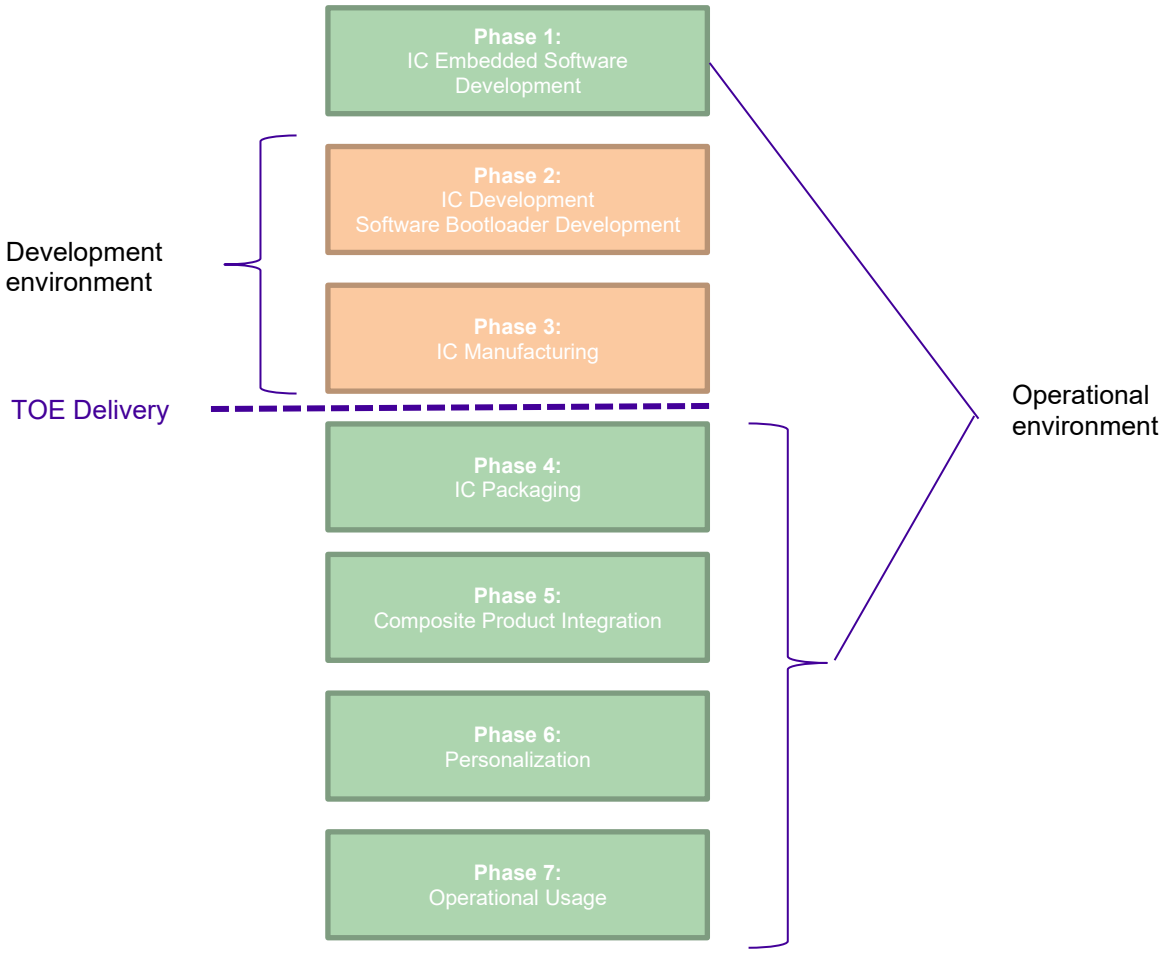


Figure 2: Development Life Cycle

The Embedded Software development (Phase 1) is done by another party, this represents an OS development.
The TOE is developed in Phase 2 and manufactured in Phase 3.

The TOE is delivered after “Test & NVM Loading”, in form of wafer.
“Test & NVM Loading” is done by UTAC USG1 or UMC Fab 12I (Phase 3).
After this phase, the product is self-protected and thus the TOE can be delivered to IDEMIA sites or other entities with a standard delivery.

The following table details how phase 2 & 3 are implemented for this Security Target:

Phase	Process	Company	Site
Phase 2	RTL & SCH design	IDEMIA StarChip	Meyreuil (France)
	External IP integration	IDEMIA StarChip	Meyreuil (France)
	Synthesis	IDEMIA StarChip	Meyreuil (France)
	Place & Route	IDEMIA StarChip	Meyreuil (France)
	Support	IDEMIA	Pessac/Courbevoie (France)
	Software Bootloader development	IDEMIA StarChip	Meyreuil (France)
Phase 3	Mask Preparation	UMC	HsinChu city R.O.C (Taiwan)

Phase	Process	Company	Site
	Generate Photo Mask	PDMC Photronics	HsinChu city R.O.C (Taiwan)
	Wafer Manufacturing	UMC	Singapore
	Prototype Assembly	CMP George Charpak	Gardanne (France)
	Test & NVM Loading	UTAC UMC	Singapore Singapore

Table 1: Phase 2 & 3 implementation

NB: External IPs (from third parties) are integrated in the TOE described in this security target. This is done through the acceptance plan evaluated in the frame of ALC_CMC activities.
NB: Characterization tests on prototypes are performed at PRESTO Engineering HVM).

2 Conformance claims

2.1 CC conformance

This Security Target claims to be compliant with Common Criteria version 2022 revision 1.

This Security Target claims conformance to [CCPart1], [CCPart2], [CCPart3], [CCPart4], [CCPart5] and [CEM]. The following Errata is used [CCErrata]

This Security Target is CC Part 2 [CCPart2], CC Part 3 [CCPart3] and CC Part 5 [CCPart5] conformant of Common Criteria version 2022, Rev 1.

Furthermore, it claims to be CC Part 2 extended with SFRs defined in chapter 5 and CC Part 3 compliant.

2.2 Package conformance

The conformance to the Common Criteria is claimed as follows:

CC	Conformance rationale
Part 5	Conformance to EAL 5, augmented with AVA_VAN.5: “Advanced methodical vulnerability analysis” ALC_DVS.2: “Sufficiency of security measures” ALC_FLR.3 “Systematic flaw remediation”

Table 2: CC Conformance

2.3 PP conformance

This Security Target claims strict conformance to [BSI-PP-0084] protection profile with Packages, Package 1 for loader ”Loader dedicated for usage in secure environment only” and Packages for Cryptographic Services (Package “AES”).

The PP0084 is applied with CC:2022, for this, the following updates are integrated:
The SFRs are adapted to CC:2022 by deprecating FCS_CKM.4 (replaced by FCS_CKM.6). On the same way FAU_SAS.1 is still extended SFR whereas FCS_RNG.1, ,FMT_LIM.1, FMT_LIM.2 and FDP_SDC.2 are no more considered as extended SFRs, as they are integrated in CC:2022. Dependencies are by consequence adapted to CC:2022.

The following section explains impacts of addition on assumptions (“A.Key-Function“ is added):

This new assumption does not mitigate any threat meant to be addressed by security objectives for the TOE. Indeed, this assumption is related to routines which may compromise keys when being executed as part of the Smartcard Embedded Software. In contrast to this, the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE and (ii) the processing of User Data including cryptographic keys.

To cover this new assumption, the following clarifications are made on objective on the operational environment OE.Resp-Appl

Clarification of “Treatment of User Data (OE.Resp-Appl)”
By definition, cipher or plain text data and cryptographic keys are User Data. The Smartcard Embedded Software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the TOE and use keys and functions appropriately in order to ensure the

strength of cryptographic operation. This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong.
For example, it must be ensured that it is beyond practicality to derive the private key from a public key if asymmetric algorithms are used. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realized in the environment.

The TOE also integrates a Memory protection unit (MPU) and the dedicated memory access control leads to the additional threat for access violation: T.Mem-Access. This threat does not mitigate any threat meant to be addressed by security objectives for the TOE.

All the additions are represented in corresponding chapter: chapter 3 for Security Problem definition, chapter 4 for security Objectives and chapter 6 for security requirements.

The TOE embeds the package “Authentication of the security IC” extract from [BSI-PP-0084] protection profile but claims the use only until Phase 6 for Personalization. In Phase 7 the embedded OS may ensure the unique identification of the TOE, with respect to authentication by external entities if needed. This package is considered as an additional package.

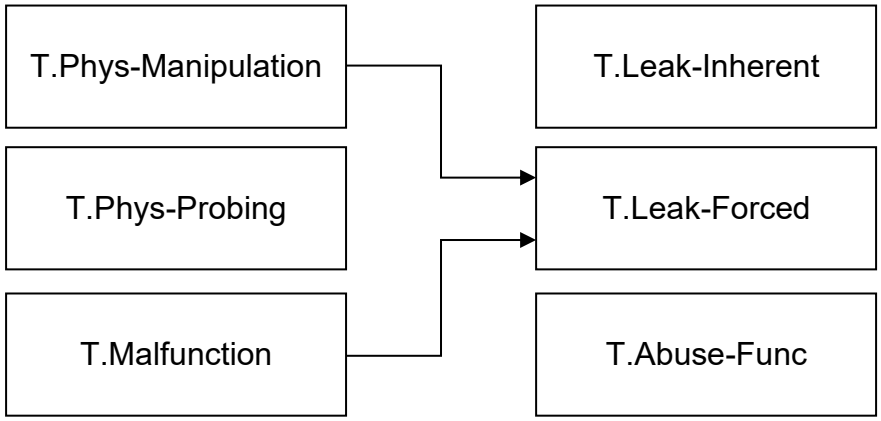
3 Security Problem Definition

3.1 Assets

Assets are defined in chapter 3.1 of [BSI-PP-0084]

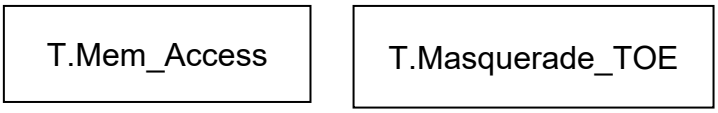
3.2 Threats

Standard threats are defined in section 3.2 of [BSI-PP-0084]:



The high-level security concern related to security service is refined below by defining threats as required by the Common Criteria :

In addition to threats defined above the following additional threats are identified:



Additional Package « Authentication of the Security IC » until Phase 6 included

T.Masquerade_TOE Masquerade the TOE

An attacker may threaten the property being a genuine TOE by producing a chip which is not a genuine TOE but wrongly identifying itself as genuine TOE sample, until personalization phase.

Additional threat

T.Mem-Access Memory Access Violation

Parts of the Smartcard Embedded Software may accidentally cause security violations. Restrictions are defined by the security policy of the specific application context and must be implemented by the Smartcard Embedded Software.

Clarification: This threat addresses the reliability of the abstract machine targeted by the software implementation. To avert the threat, the set of access rules provided by this TOE should be undefeated if operated according to the provided guidance. The threat is not realized if the Security IC Embedded Software is designed or implemented to grant access to restricted information. It is realized if an implemented access denial is granted under unexpected conditions or if the execution machinery does not effectively control a controlled access.
Here the attacker is expected to (i) take advantage of flaws in the design and/or the implementation of the TOE memory access rules (refer to T.Abuse-Func but for functions available after TOE delivery), (ii) introduce flaws by forcing operational conditions (refer to T.Malfunction) and/or by physical manipulation (refer to T.Phys-Manipulation). This attacker is expected to have a high attack potential.

3.3 Organizational security policies

Organizational security policies (OSPs) are defined in section 3.3 of [BSI-PP-0084].

P.Process-TOE

In addition to OSPs defined above the following additional OSPs are identified:

Addition from Packages for Cryptographic Services

P.Crypto-Service

P.Crypto-Service Cryptographic services of the TOE

The TOE shall provide secure hardware based cryptographic services for the IC Embedded Software

Package 1: Loader dedicated for usage in secured environment only

P.Lim_Block_Loader

P.Lim_Block_Loader Limiting and Blocking the Loader Functionality

The composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. He limits the capability and blocks the availability of the Loader in order to protect stored data from disclosure and manipulation.

3.4 Assumptions

Assumptions are defined in section 3.4 of [BSI-PP-0084]:

A.Process-Sec-IC

A.Resp-Appl

In addition to assumptions defined above the following additional assumption are identified:

A.Key-Function

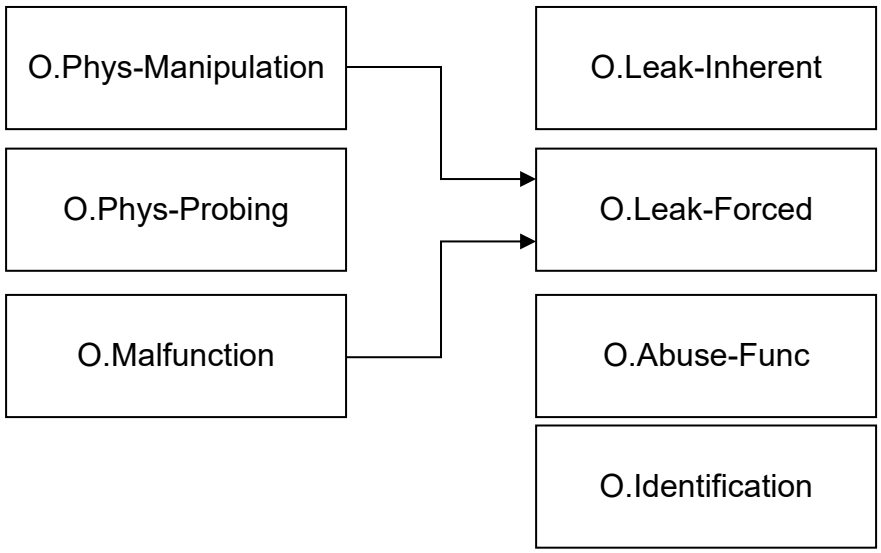
A.Key-Function	Usage of Key-dependent Functions

Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced). Note that here the routines which may compromise keys when being executed are part of the Smartcard Embedded Software.
In contrast to this, the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE and (ii) the processing of User Data including cryptographic keys.

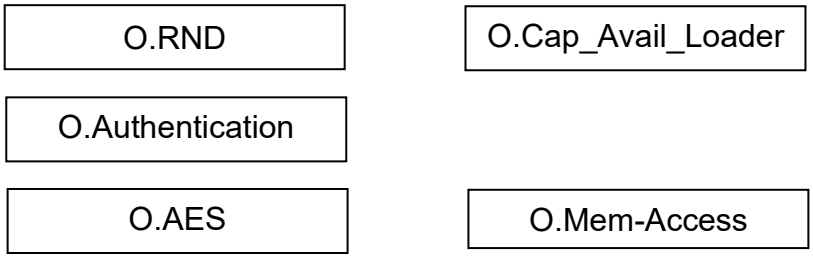
4 Security Objectives

4.1 Security Objectives for the TOE

Standard security objectives for the TOE are defined in section 4.1 of [BSI-PP-0084]:



In addition to security objective for the TOE defined above, the following additional security objective for the TOE are identified:



Addition from Package "AES"

The TOE shall provide "Cryptographic service AES (O.AES)" as specified below:

O.AES Cryptographic service AES

The TOE provides secure hardware based cryptographic services implementing the AES for encryption and decryption.

Addition from Package 1: Loader dedicated for usage in secured environment only

The TOE shall provide "Capability and availability of the Loader (O.Cap_Avail_Loader)" as specified below:

O.Cap_Avail_Loader The TSF provides limited capability of the Loader functionality and irreversible termination of the Loader in order to protect stored user data from disclosure and manipulation

Additional Package « Authentication of the Security IC » until Phase 6 included

O.Authentication Authentication to external entities

The TOE shall be able to authenticate itself to external entities. The initialization Data (or part of them) are used for TOE authentication verification data, until personalization phase included.

Addition:
The TOE shall provide “Area based Memory Access Control (O.Mem-Access)” as specified below.

O.Mem-Access Area based Memory Access Control

The TOE must provide the Smartcard Embedded Software with the capability to define restricted access memory areas. The TOE must then enforce the partitioning of such memory areas so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

4.2 Security Objectives for the Operational Environment

Security objectives for the Operational Environment are defined in section 4.2 & 4.3 of [BSI-PP-0084].

OE.Process-Sec-IC	OE.Resp-Appl

In addition to security objective for the Operational Environment defined above, the following additional security objective for the Operational Environment are identified

OE.TOE_Auth	OE.Lim_Block_Loader

Additional Package “Authentication of the Security IC” until Phase 6 included

The operational environment of the TOE shall provide “External entities authenticating of the TOE (OE.TOE_Auth” as specified below.

OE.TOE_Auth External entities authenticating of the TOE

The operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE, until personalization phase included.

Package 1: Loader dedicated for usage in secured environment only

The operational environment of the TOE shall provide “limitation of capability and blocking the Loader (OE.Lim_Block_Loader)” as specified below.

OE.Lim_Block_Loader Limitation of capability and Blocking the Loader

The composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversible the Loader after intended usage of the Loader

4.3 Security Objectives rationale

Security objective rationale is given in chapter 4.4 of [BSI-PP-0084].

Rationale from Packages for Cryptographic Services is given in the following table and detailed justifications in following subsection:

Assumption, Threat or Organizational Security Policy Security Objective Note	Security Objective	Note
P.Crypto-Service	O.AES	
A.Key-Function	OE.Resp-Appl	Related to Phase 1

Table 3: Rationale from Packages for Cryptographic Services

The justification related to the security objective O.AES is as follows: Since O.AES requires the TOE to implement exactly the same specific security functionality as required by P.Crypto-Service, the organizational security policy is covered by the objective. Nevertheless, the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality required by P.Crypto-Service. (Note that these objectives support that the specific security functionality is provided in a secure way as expected from P.Crypto-Service.) Especially O.Leak-Inherent and O.Leak-Forced refer to the protection of confidential data (User Data or TSF data) in general. User Data are also processed by the specific security functionality required by P.Crypto-Service.

OE.Resp-Appl actually upholds A.Key-Function. The Smartcard Embedded Software must implement functions which perform operations on keys (if any) in such a manner that they do not disclose information about confidential data.
Moreover, the Smartcard Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realized in the environment. These measures make sure that the assumption A.Resp-Appl is still covered by the security objective OE.Resp-Appl although additional functions are being supported according to P.Crypto-Service. The justification of the additional policy and the additional assumption show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there.

Rationale for “Area based Memory Access Control” is given in the following table and detailed justifications in following subsection:

Assumption, Threat or Organisational Security Policy Security Objective Note	Security Objective	Note
T.Mem-Access	O.Mem-Access	

Table 4: Rationale for “Area based Memory Access Control”

According to O.Mem-Access the TOE must enforce the partitioning of memory areas so that access of software to memory areas is controlled. Restrictions are defined by the Smartcard Embedded Software. Thereby security violations caused by accidental access to restricted data can be prevented (refer to T.Mem-Access). The threat T.Mem-Access is therefore removed if the objective is met.

It is up to the Smartcard Embedded Software to implement the memory management scheme by appropriately administrating the TSF. This is also expressed both in T.Mem-Access and O.Mem-Access. The TOE shall provide access control functions as a means to be used by the Smartcard Embedded Software. This is further emphasised by the clarification of “Treatment of User Data (OE.Resp-Appl)” which reminds that the Smartcard Embedded Software must not undermine the restrictions it defines. Therefore, the clarifications contribute to the coverage of the threat T.Mem-Access.

Rationale for “Package 1 : Loader dedicated for usage in security environment only” is given in the following table and detailed justifications in following subsection:

Assumption, Threat or Organizational Security Policy Security Objective Note	Security Objective	Note
P.Lim_Block_Loader	O.Cap_Avail_Loader OE.Lim_Block_Loader	

Table 5: Rationale for "Package 1 : Loader dedicated for usage in security environment only"

According to O.Cap_Avail_Loader, the TSF must provide limited capability of the Loader functionality and irreversible termination of the Loader to protect stored user data from disclosure and manipulation. In addition, the OE.Lim_Block_Loader request that the Composite Product Manufacturer protect the Loader functionality again misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.
Therefore, these 2 objectives allows the implementation of the organizational security policy Limitation of capability and blocking the Loader (P.Lim_Block_Loader)

The TOE security objective O.Cap_Avail_Loader mitigate also the threat "Abuse of Functionality" (T.Abuse-Func) if attacker tries to misuse the Loader functionality in order to manipulate security services of the TOE provided or depending on IC Dedicated Support Software or user data of the TOE as IC Embedded Software, TSF data or user data of the smartcard product.

Rationale for the additional package "Authentication of the Security IC" is given in the following table and detailed justifications in following subsection:

Assumption, Threat or Organizational Security Policy Security Objective Note	Security Objective	Note
T.Masquerade_TOE	O.Authentication OE.TOE_Auth	

Table 6: Rationale for the package "Authentication of the Security IC"

The treat T.Masquerade_TOE is directly covered by the TOE security objective O.Authentication describing the proving part of the authentication and the security objective for the operational environment of the TOE OE.TOE_Auth the verifying part of the authentication.

5 Extended Component Definition

The only extended component is the definition of the Family FAU_SAS made in chapter 5.3 of [BSI-PP-0084].

Indeed FCS_RNG, FMT_LIM, FDP_SDC, FIA_API families defined in [BSI-PP-0084] are now integrated in [CCPart2] of CC 2022.

6 IT Security requirements

6.1 Security Functional Requirements

Note: The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections made by the [BSI-PP-0084] author are denoted as underlined text. Selections filled by the ST author appear in bold and are italicized text.

6.1.1 Security Functional Requirements from BSI-PP-0084

The following chapters details Security functional requirements taken from [BSI-PP-0084]. Application notes are not copied in this document, please refer to [BSI-PP-0084] for details.

FRU_FLT.2 Limited fault tolerance

Hierarchical to: FRU_FLT.1

FRU_FLT.2.1 The TSF shall ensure the operation of **all the TOE's capabilities** when the following failures occur: exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1).

Dependencies: FPT_FLS.1

Refinement: ***The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.***

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur.

Dependencies: No dependencies.

Refinement: ***The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.***

Application note: The term "secure state" means the functional mode of the TOE. That is to say, the Embbeded software is running and all TSF are activated.
TOE detectors described in ASE_TSS chapter 7 allow the TSF to manage failure events with an interruption and thus preserve a secure state.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall limit its capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced: Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.

Dependencies: FMT_LIM.2

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits its availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced: Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.

Dependencies: FMT_LIM.1

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide the test process before TOE Delivery with the capability to store ***Initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software*** in the ***NVM (non-volatile Flash memory)***.

Dependencies: No dependencies.

FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.

FDP_SDC.1.1 The TSF shall ensure the confidentiality of ***all user data*** while it is stored in the ***temporary memory, persistent memory.***

Application note: persistent memory is Non Volatile Memory (Flash memory) and temporary memory is the Random Access Memory (RAM).

Dependencies: No dependencies.

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF *for* ***integrity errors detectable by EDC*** on all objects, based on the following attributes: ***EDC value corresponding to the protected user data.***

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall ***raise a flag. The Smartcard Embedded Software shall configure the TOE in order to take the appropriate action once this flag is raised (Example: Reset, Dead Lock or NMI)***

Dependencies: No dependencies.

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

FPT_PHP.3.1 The TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.

Refinement: ***The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.***

Dependencies: No dependencies.

Application note: The countermeasures are provided in chapter 7.3 and the violation detected at any time, answered automatically by Secure Manager whose role is indicated in chapter 7.1.

FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the Data Processing Policy to prevent the disclosure of user data when it is transmitted between physically-separated parts of the TOE.

Dependencies: FDP_ACC.1/MPU OR FDP_IFC.1

Refinement: ***The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.***

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies.

Refinement: ***The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.***

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the Data Processing Policy on all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software.

Dependencies: FDP_IFF.1

Data processing policy is defined in §176 of [BSI-PP-0084].

FCS_RNG.1 Cryptographic operation

Hierarchical to: No other components.

FCS_RNG.1.1 The TSF shall provide a ***physical*** random number generator that implements ***the rule RègleArchiGVA of [ANSSI-PG-083], the recommendation RecomArchiGVA of [ANSSI-PG-083], total failure tests and online tests.***

FCS_RNG.1.2 The TSF shall provide ***numbers in 16-bit words*** that meet: ***the rule RègleArchiGVA of [ANSSI-PG-083].***

Dependencies: No dependencies.

Application Note: To comply with [ANSSI-PG-083], a cryptographic post-processing must be implemented by the composite developer. This is described in the SCE900U Security Guidance [TEP130].

6.1.2 Security functional requirements from Packages “AES”

The following chapters details Security functional requirements taken from Packages “AES”. These SFRs are related AES crypto services. Operations are performed by the TSF, keys are imported from the ES and managed by the ES using TSF interfaces.

NB: PKI accelerator is present in the TOE but not formalized trough SFRs. Security, related to services provided by the TOE for PKI acceleration are described in ADV_ARC documentation.

FCS_COP.1/AES Cryptographic operation - AES

Hierarchical to: No other components.

FCS_COP.1.1/AES The TSF shall perform encryption & decryption in accordance with a specified cryptographic algorithm AES ***in ECB or CBC mode*** and cryptographic key sizes ***of 128, 192, and 256 bits*** that meet the following: [FIPS197], [NIST SP800-38A].

Dependencies: [FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1 OR FCS_CKM.5] FCS_CKM.6/1AES

Refinement: The hardware does not provide directly mode ECB or CBC but supports it from the Embedded software. The size of key is also determined by the ES.

FCS_CKM.6/AES Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.6.1/AES The TSF shall destroy **AES keys build with Embedded software** when **no longer needed, trigged by ES, no other circumstances**.

FCS_CKM.6.1/AES The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method **: The cryptographic key destruction is provided by overwriting the internal stored key when a new key value is provided through the key interface or a key zeroize initiated by a special signal.** that meets the following: ***NONE***.

Note: *The Secure ES is in charge of trigging the key destroying. See dependencies for discussion on FCS_CKM.1.*

Dependencies: [FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1 OR FCS_CKM.5]

6.1.3 Security functional requirements from “Area based Memory Access Control”

The following chapters details Security functional requirements taken from “Area based Memory Access Control”. These SFRs are related to TOE MPU features and configuration.

FDP_ACC.1/MPU Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1/MPU The TSF shall enforce the ***Memory access control policy*** on

Subjects:
- ***(CPU)***
- ***(MDMA)***
- ***(UCP)-PKI***
- ***(STI)***

Objects:
- ***(NVM) regions***
- ***(RAM) regions***
- ***Other memory regions***

Operations:
- ***Read operation.***
- ***Write operation.***
- ***Execution operation.***

Dependencies: FDP_ACF.1/MPU

FDP_ACF.1/MPU Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1/MPU The TSF shall enforce the ***Memory access control policy*** to objects based on the following:

Subjects security attributes (Permission control information)
- ***(CPU) “run” mode***
- ***(CPU) “runperso” mode***
- ***(CPU) “bootrun” mode***
- ***(STI) “testmode” mode***
- ***(STI) “testmode secure” mode***

Object security attributes (Permission control information)
- ***(NVM)/(RAM)/Peripherals region selection (MPUREGID)***
- ***(NVM)/(RAM)/Peripherals region base (MPUREGBASE)***
- ***(NVM)/(RAM)/Peripherals region limit (MPUREGLMT)***
- ***(NVM) limit address (MPUNVMLMT)***
- ***Access memory regions:***
  - ***(NVM)/(RAM)/Peripherals Read access to regions (MPUREGRUL.READ) identified by (MPUREGID)***
  - ***(NVM)/(RAM)/Peripherals Write access to regions (MPUREGRUL.WRITE) identified by (MPUREGID)***
  - ***(NVM) Code execution regions (MPUREGRUL.EXEC) identified by (MPUREGID)***
  - ***(NVM) Freeze area limit address (MPUFREEZELMT)***

FDP_ACF.1.2/MPU The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- ***The TSF shall allow (NVM)/ (RAM)/ Peripherals memory read on regions if MPUREGRUL.READ is cleared to 0.***
- ***The TSF shall allow (NVM)/ (RAM)/ Peripherals memory write on regions if MPUREGRUL.WRITE is cleared to 0.***
- ***The TSF shall allow (NVM) execution on regions if MPUREGRUL.EXEC is cleared to 0.***

Permission control information checks are achieved before the operation

FDP_ACF.1.3/MPU The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

- ***The TSF shall allow memory write of (NVM) Freeze area in (CPU) "runperso" mode, "test mode" mode and "test mode secure" mode.***
- ***The TSF shall allow (RAM) memory read and write to the (MDMA) and (UCP)-PKI.***

FDP_ACF.1.4/MPU The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- ***Execution is forbidden for all Peripherals windows, (RAM) area.***
- ***Once (NVM) Freeze area limit address is set (MPUFREEZELMT), the Freeze area cannot be modified anymore in "runmode" mode and "bootrun" mode, even after reset.***
- ***Once (NVM) Freeze area limit address is set (MPUFREEZELMT), this limit cannot be modified anymore in "runmode" mode and "runpersomode" mode, even after reset.***
- ***Once (NVM) limit address is set (MPUNVMLMT), this limit cannot be modified anymore in "runmode" mode and "runpersomode" mode, even after reset.***

Dependencies: FDP_ACC.1/MPU, FMT_MSA.3

FMT_MSA.3/MPU Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1/MPU The TSF shall enforce the ***Memory access control policy*** to provide **permissive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/MPU The TSF shall allow the ***any subject (provided that the Memory Access Control Policy is enforced and the necessary access is therefore allowed)*** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1/MPU, FMT_SMR.1

FMT_MSA.1/MPU Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1/MPU The TSF shall enforce the ***Memory access control policy*** to restrict the ability to **modify** the security attributes ***permission control information*** to ***CPU.***

Dependencies: [FDP_ACC.1/MPU OR FDP_IFC.1], FMT_SMR.1, FMT_SMF.1

6.1.4 Security Functional requirement for Authentication of the TOE

The following chapters details Security functional requirements taken from the additional Package «Authentication of the Security IC». These SFRs are related to TOE bootloader features and authentication.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

FIA_API.1.1 The TSF shall provide a ***mutual authentication*** **mechanism based on [GPC_SPE_014] and [GPC_SPE_034]** to prove the identity of ***the TOE*** by including the following properties **identification data inside OTP as defined in AGD** to an external entity.

Dependencies: No dependencies.

Refinement: The identification is provided until personalization Phase included.

Application Note: In Phase 7, the mutual authentication is no more available as bootloader has been deleted.

6.1.5 Security Functional requirement for the Loader dedicated for usage in secure environment only (Package 1)

The following chapters details Security functional requirements taken from “Package 1: Loader dedicated for usage in secured environment only”. These SFRs are related to TOE bootloader features and authentication.

FMT_LIM.1/Loader **Limited capabilities**

Hierarchical to: No other components.

FMT_LIM.1.1/Loader The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: Deploying Loader functionality after **TOE delivery** does not allow stored user data to be disclosed or manipulated by unauthorized user.

Dependencies: FMT_LIM.2

FMT_LIM.2/Loader **Limited availability - Loader**

Hierarchical to: No other components.

FMT_LIM.2.1/Loader The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capability (FMT_LIM.1)” the following policy is enforced: The TSF prevents deploying the Loader functionality after ***full loading of Embedded Software***.

Dependencies: FMT_LIM.1

Application Note: Regarding FMT_LIM.1/Loader and FMT_LIM.2/Loader, the Security Guidance requires erasing the bootloader after Embedded Software loading.

6.1.6 Security Functional Requirements summary

The following table summarize the Security Functional Requirements selected for this security target

SFR	Origin
FRU_FLT.2	BSI-PP-0084
FPT_FLS.1	
FMT_LIM.1	

SFR	Origin
FMT_LIM.2	
FAU_SAS.1	
FDP_SDC.1	
FDP_SDI.2	
FPT_PHP.3	
FDP_ITT.1	
FPT_ITT.1	
FDP_IFC.1	
FCS_RNG.1	
FCS_COP.1/AES	PP Package “AES”, FCS_CKM.4 (CC3.1) replaced by FCS_CKM.6 (CC:2022)
FCS_CKM.6/AES	
FDP_ACC.1/MPU	ST: “Area based Memory Access Control”
FDP_ACF.1/MPU	
FMT_MSA.3 /MPU	
FMT_MSA.1 /MPU	
FIA_API.1	PP Package « Authentication of the Security IC »
FMT_LIM.1/Loader	PP Package 1: “Loader dedicated for usage in secured environment only”
FMT_LIM.2/Loader	

Table 7: Security Functional Requirements

6.2 Security Assurance Requirements

The following table details assurance requirements for this security target regarding those defined in the protection profile [BSI-PP-0084].

Assurance components in [BSI-PP-0084]: EAL 4 augmented with: ALC_DVS.2 & AVA_VAN.5	**Assurance components in this ST EAL 5 augmented with: ALC_FLR.3, AVA_VAN.5 & ALC_DVS.2**	**Refined in [BSI-PP-0084]**	**Impact of ST level on PP refinement**
ADV_ARC.1 Security architecture description	ADV_ARC.1 Security architecture description	Yes	None
ADV_FSP.4 Complete functional specification	**ADV_FSP.5 Complete semi-formal functional**	Yes	None. Refinement is still valid
ADV_IMP.1 Implementation representation of the TSF	ADV_IMP.1 implementation representation of the TSF	Yes	None. Refinement is still valid
	ADV_INT.2 Minimally complex internals	No	
ADV_TDS.3 Basic modular design	**ADV_TDS.4 Semiformal modular design**	No	
AGD_OPE.1 Operational user guidance	AGD_OPE.1 Operational user guidance	Yes	None
AGD_PRE.1 Preparative procedures	AGD_PRE.1 Preparative procedures	Yes	None
ALC_CMC.4 Production support, acceptance procedures and automation	ALC_CMC.4 Production support, acceptance procedure and automation	Yes	None. Refinement is still valid
ALC_CMS.4 Problem tracking CM coverage	**ALC_CMS.5 Development tools CM coverage**	Yes	None. Refinement is still valid
ALC_DEL.1 Delivery procedures	ALC_DEL.1 Delivery procedures	Yes	None.

Assurance components in [BSI-PP-0084]: EAL 4 augmented with: ALC_DVS.2 & AVA_VAN.5	**Assurance components in this ST EAL 5 augmented with: ALC_FLR.3, AVA_VAN.5 & ALC_DVS.2**	**Refined in [BSI-PP-0084]**	**Impact of ST level on PP refinement**
ALC_DVS.2 Sufficiency of security measures	ALC_DVS.2 Sufficiency of security measures	Yes	None.
ALC_LCD.1 Developer defined life-cycle model	ALC_LCD.1 Developer defined life-cycle model	No	
ALC_TAT.1 Well-defined development tools	**ALC_TAT.2 Compliance with implementation standards**	No	
	ALC_FLR.3 Flaw remediation	No	
ASE_CCL.1 Conformance claims	ASE_CCL.1 Conformance claims	No	
ASE_ECD.1 Extended components definition	ASE_ECD.1 Extended components definition	No	
ASE_INT.1 ST introduction	ASE_INT.1 ST introduction	No	
ASE_OBJ.2 Security objectives	ASE_OBJ.2 Security objectives	No	
ASE_REQ.2 Derived security requirements	ASE_REQ.2 Derived security requirements	No	
ASE_SPD.1 Security problem definition	ASE_SPD.1 Security problem definition	No	
ASE_TSS.1 TOE summary specification	ASE_TSS.1 TOE summary specification	No	
ATE_COV.2 Analysis of coverage	ATE_COV.2 Analysis of coverage	Yes	None. Refinement is still valid
ATE_DPT.1 Testing: basic design	**ATE_DPT.3 Testing: modular design**	No	
ATE_FUN.1 Functional testing	ATE_FUN.1 Functional testing	No	
ATE_IND.2 Independent testing - sample	ATE_IND.2 Independent testing - sample	No	
AVA_VAN.5 Advanced methodical vulnerability analysis	AVA_VAN.5 Advanced methodical vulnerability analysis	Yes	None

Table 8: Security Assurance Requirements

NB: Refinements on Assurance Requirements are detailed in chapter 6.2.1 of [BSI-PP-0084]. They are also applicable to all augmented components in this ST

6.3 Security Requirements Rationale

6.3.1 Rationale for BSI-PP-0084 Security Functional Requirements

Rationale for security functional requirements is given in chapter 6.3.1 of [BSI-PP-0084].
Dependencies analysis is given in chapter 6.3.2 of [BSI-PP-0084] with the followings choices:

Security Functional Requirement	Dependencies	Fulfilled by security requirements or justification
FDP_ITT.1	[FDP_ACC.1 or [FDP_IFC.1]	Yes, by FDP_IFC.1

Table 9: Security Requirements Rationale for BSI-PP-0084

6.3.2 Rationale for Packages for Cryptographic Services Security Functional Requirements

Security Objective	Security Functional Requirement
O.AES	- FCS_COP.1/AES Cryptographic Operation – AES FCS_CKM.6/AES Cryptographic key destruction - AES

Table 10: Security Requirements Rationale for Packages for Cryptographic

The justification related to the security objective O.AES is as follows:
The security functional requirement(s) “Cryptographic operation (FCS_COP.1)” exactly requires this function to be implemented, which are demanded by O.AES. Therefore, FCS_COP.1 is suitable to meet the security objective. Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context.

Dependencies:

Security Functional Requirement	Dependencies	Fulfilled by security requirements or justification
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6	No: fulfilled by the ES and evaluated during composite TOE evaluation. These requirements are also considered as being related to OE.Resp-Appl. They are covered by guidance documentation evaluation. Dependence to FCS_CKM.6/AES ensured.
FCS_CKM.6/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	No: fulfilled by the ES. These requirements are also considered as being related to OE.Resp-Appl. They are covered by guidance documentation evaluation.

Table 11: Security Requirements Dependencies for Packages for Cryptographic Services

6.3.3 Rationale for O.Mem-Access Security Functional Requirements

Security Objective	Security Functional Requirement
O.Mem-Access	- FDP_ACC.1/MPU “Subset access control” - FDP_ACF.1/MPU “Security attribute based access control” - FMT_MSA.3/MPU “Static attribute initialization” - FMT_MSA.1/MPU “Management of security attributes”

Table 12: Security Requirements Rationale for O.Mem-Access

The justification related to the security objective “Area based Memory Access Control (O.Mem-Access)” is as follows:

The security functional requirements “Subset access control (FDP_ACC.1/MPU)” and “Security attribute based access control (FDP_ACF.1/MPU)” with the related Security Function Policy (SFP) “Memory Access Control Policy” exactly require to implement an area based memory access control as demanded by O.Mem-Access. Therefore, FDP_ACC.1/MPU with its SFP is suitable to meet the security objective. Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context.
The security functional requirement “Static attribute initialization (FMT_MSA.3/MPU)” requires that the TOE provides default values for security attributes. These default values can be overwritten by any subject (software) provided that the necessary access is allowed what is further detailed in the security functional requirement “Management of security attributes (FMT_MSA.1/MPU)”: The ability to update the security attributes is restricted to privileged subject(s). These management functions ensure that the required access control can be realized using the functions provided by the TOE.

Dependencies:

Security Functional Requirement	Dependencies	Fulfilled by security requirements or justification
FDP_ACC.1/MPU	FDP_ACF.1/MPU	yes
FDP_ACF.1/MPU	FDP_ACC.1/MPU	yes
FMT_MSA.3/MPU	FMT_MSA.1/MPU, FMT_SMR.1.	Yes, except for FMT_SMR.1: the access control specified for the intended TOE is not role-based but enforced for subjects. Therefore, there is no need to identify roles in form of a security functional requirement FMT_SMR.1.
FMT_MSA.1/MPU	FDP_ACC.1/MPU or FDP_IFC.1, FMT_SMR.1, FMT_SMF.1	Yes, by FDP_ACC.1/MPU, except for FMT_SMR.1 & FMT_SMF.1: the access control specified for the intended TOE is not role-based but enforced for subjects. Therefore, there is no need to identify roles in form of a security functional requirement FMT_SMR.1. Because actions related to the policies are already defined in FDP_ACC.1/MPU / FDP_ACF.1/MPU and because these functions are not-role based, there is no need to identify these functions in form of a security functional requirement FMT_SMF.1.

Table 13: Security Requirements Dependencies for O.Mem-Access

6.3.4 Rationale for **O.Authentication** from Package “Authentication of security IC”

Security Objective	Security Functional Requirement
O.Authentication	- FIA_API.1 Authentication Proof of Identity

Table 14: Security Requirements Rationale for O.Authentication

The justification related to the security objective “Authentication to external entities (O.Authentication)” is as follows:

The security functional requirement(s) “Authentication Proof of Identity (FIA_API.1)” require providing proof of the identity of the TOE to an external entity. Therefore, FIA_API.1 meets the security objective.

Dependencies:

Security Functional Requirement	Dependencies	Fulfilled by security requirements or justification
FIA_API.1	No dependencies	No dependencies

Table 15: Security Requirements Dependencies for O.Authentication

6.3.5 Rationale for **O.Cap_Avail_Loader** from “Package 1: Loader dedicated for usage in secured environment only “

Security Objective	Security Functional Requirement
O.Cap_Avail_Loader	- FMT_LIM.1/Loader Limited capabilities - FMT_LIM.2/Loader Limited availability - Loader

Table 16: Security Requirements Rationale for O.Cap_Avail_Loader

The justification related to the security objective “Capability and availability of the Loader (O.Cap_Avail_Loader)” is as follows:
The security functional requirements “Limited capability (FMT_LIM.1)” and “Limited availability – Loader (FMT_LIM.2)” require that deploying Loader functionality after full loading of Embedded Software does not allow stored user data to be disclosed or manipulated by unauthorized user and prevent deploying the Loader functionality after full loading of Embedded Software Therefore, FMT_LIM.1 and FMT_LIM.2 meet the security objective.

Dependencies:

Security Functional Requirement	Dependencies	Fulfilled by security requirements or justification
FMT_LIM.1/Loader	FMT_LIM.2	Yes: the Security Guidance recommends to erase the bootloader after Software loading.
FMT_LIM.2/Loader	FMT_LIM.1	Yes: the Security Guidance recommends to erase the bootloader after Software loading.

Table 17: Security Requirements Dependencies for O.Cap_Avail_Loader

6.3.6 Rationale for the Security Assurance Requirements

This security target claims an EAL5 with the augmentations AVA_VAN.5, ALC_DVS.2 and ALC_FLR.3 to permit the developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defense against such attacks, the evaluators must have access to the design and source code.

ALC_FLR.3 Systematic flaw remediation:
This component provides assurance that the TOE will be maintained and supported in the future, requiring the TOE developer to track and correct flaws in the TOE.

This assurance component has no dependencies

ALC_DVS.2 Sufficiency of security measures:
This component provides assurance that the TOE and its parts are protected in the development environment by physical, procedural personnel and other security measures.

This assurance component has no dependencies.

AVA_VAN.5 Advanced methodical vulnerability analysis:
This component provides assurance that the potential vulnerabilities cannot be exploited in the operational environment for the TOE.

This assurance component has dependencies to ADV_ARC.1 “Security architecture description”, ADV_FSP.5 “Complete semi-formal functional”, ADV_TDS.4 “Semiformal modular design”, ADV_IMP.1 “implementation representation of the TSF”, AGD_OPE.1 “Operational user guidance” and AGD_PRE.1 “Preparative procedures”.

7 TOE Summary Specification

7.1 Resistance to Faults:

Related SFRs:
FRU_FLT.2 Limited fault tolerance
FPT_FLS.1 Failure with preservation of secure state

Noise filters are embedded on SCE900U pads. This increases the resistance to transmission with noise.

SCE900U embeds environmental detectors to protect the code execution from an unexpected behavior due to high variation of running context.
Thus, several monitors are embedded to detect low/high voltages on Vcc, low and high frequencies on Clk.

Additional digital fault detectors are embedded in the product to cover light, EM injection and abnormal temperature operating.

Scrambling key diversification per chip increases difficulties of reproducing an attack from chip to chip.

UIG mechanism unpredictable index generator is embedded in the product. This tool can be used by the software to generate pseudo-random index in a given RANGE. It is useful to secure data block copy.

RPI (Random Process Interupt) mechanism can be used by the software to add randomness during code execution.

Hardware Code Signature Unit (CSU) and Control Flow Unit (CFU) peripherals are designed to let sensitive software ensure the algorithms it runs are executed as expected. It provides the embedded application with tool to resist Fault Injection attacks.

All these monitors generate security alarms for the Security Manager.

The role of the Security Manager is to collect all the security alarms from the whole system and reacts according to global security policy partially configured by the software.
The security alerts and system behavior are described in chapter 13 of the datasheet [TEP124].

7.2 Test mode & Personalization security:

Related SFR(s):
FMT_LIM.1 Limited capabilities
FMT_LIM.2 Limited availability
FAU_SAS.1 Audit storage

SCE900U embeds a full test mode (FTM) before the TOE release. This full test mode is protected by strong authentication mechanisms (128 bit password). It is also a dedicated protocol with a proprietary set of commands.

After TOE is released, the FTM is not accessible anymore, a reduced test mode is nevertheless present (RTM). This test mode permits to analyze field returns but without any sensitive action possible. This reduced test mode is protected by strong authentication mechanisms (128 bit password). It is also a dedicated protocol with a proprietary set of commands.

Traceability data (unique identifier) is written in the NVM during test mode.
Any other personalization or initialization data can be written in the NVM depending on customer needs.

7.3 Resistance to physical attack:

Related SFR(s):
FPT_PHP.3 Resistance to physical attack
FDP_SDC.1 Stored data confidentiality
FDP_SDI.2 Stored data integrity monitoring and action

SCE900U embeds an active shield. The active shield is a network of wires that uses dynamic values which are progressing on it.

Sensitive wire reverse is made difficult by a fully managed synthesis of the core. Data busses are encrypted.

The Flash memory uses a 17-bit word including 1-bit reserved for an EDC function. This allows error detection for security reasons. If an odd number of bits of the memory array have been physically modified, they will be detected.

The RAM uses a 40-bit word including 8-bit reserved for an EDC function. This allows error detection for security reasons. If one or few bits of the memory array have been physically modified, they will be detected.

TOE is designed in a manner to be resistant to physical attacks including probing.

7.4 Information leakage:

Related SFRs:
FDP_ITT.1 Basic internal transfer protection
FPT_ITT.1 Basic internal TSF data transfer protection
FDP_IFC.1 Subset information flow control

SCE900U embeds several mechanisms that guarantee that information leakage during transfers & processing is limited. SCE900U is also build in a way that stored information is protected.

Secured Memories & busses
- Data and code Scrambling
- Digital power consumption & electromagnetic masking

Secured Core
- Digital power consumption & electromagnetic masking

7.5 Cryptographic features

Related SFRs:
FCS_RNG.1 Cryptographic operation
FCS_COP.1/AES Cryptographic operation (AES)

SCE900U embeds a true random number generator: In this mode, the Analog Noise Source is the only source of entropy (randomness). Due to the noise source baud rate, interrupts permit to get the complete 16-bit word as soon as it is generated. Moreover, Failure detector (chi2 test) verifies if the Analog block works correctly.

SCE900U embeds Advanced Encryption Standard (AES) and cryptographic key sizes of 128, 192, and 256 bits with state of the art side channel protection (Digital power consumption & electromagnetic masking, fault protection).

7.6 Memory protection unit

Related SFRs:
FDP_ACC.1/MPU Subset access control

FDP_ACF.1/MPU	Security attribute based access control
FMT_MSA.3/MPU	Static attribute initialization
FMT_MSA.1/MPU	Management of security attributes

The Memory Protection Unit Secure (MPU) is a security module, which checks that the memory accesses are granted or not according to some restriction rules defined by the hardware or the software. In addition, the MPU checks that software memory accesses and code execution are not done outside regions or inside regions with restrictive rules defined by the software itself.

7.7 Software bootloader security features

Related SFRs:

FIA_API.1	Authentication Proof of Identity
FMT_LIM.1/Loader	Limited capabilities
FMT_LIM.1/Loader	Limited availability - Loader

The software bootloader implements a mutual authentication between the programming terminal and the TOE. The mutual authentication mechanism is based on [GPC_SPE_014] and [GPC_SPE_034] with AES-128 CMAC.

The software bootloader shall be removed from the memory after a successful Embedded Software loading and before final delivery from the Common Criteria certified personalization site.

8 Referenced documents

Reference	Description
[ANSSI-PG-083]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. ANSSI, Version 2.04, 2020-01-01
[BSI-PP-0084]	Security IC Platform Protection Profile Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014.
[CCpart1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version CC:2022, Revision 1, November 2022.
[CCpart2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version CC:2022, Revision 1, November 2022.
[CCpart3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, version CC:2022, Revision 1, November 2022.
[CCpart4]	Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities November 2022, CC:2022 Revision 1.
[CCpart5]	Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements November 2022, CC:2022 Revision 1.
[CEM]	Common Criteria for Information Technology Security Evaluation, Evaluation methodology, CEM:2022, Revision 1, November 2022
[CCErrata]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) Version 1.1.
[FIPS197]	FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001
[GPC_SPE_014]	Secure Channel Protocol '03' Card Specification v2.2 - Amendment D Version 1.1.1
[GPC_SPE_034]	GlobalPlatform Card Specification Version 2.2.1
[NIST SP800-38A]	NIST SP 800-38A Recommendation for Block Cipher Modes of Operation, 2001, with Addendum Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, October 2010
[Ref1](1)	Cortus APS3cd Programmers' Reference Manual"
[TEP131] (1)	IDSLD Gridr Secure Bootloader Specification
[TEP124] (1)	SCE900U Technical Datasheet
[TEP130] (1)	SCE900U Security Guidance
[TEP129] (1)	SCE900U Erratasheet
[TEP133] (1)	Preparative Procedure for SCE900U

Table 18: Referenced documents

(1) *The version of this document can be found in the Public Security Target*

9 Glossary & Abbreviations

Abbreviation	Definition
AES	Advanced Encryption Standard
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DEMA	Differential Electro Magnetic Analysis
DPA	Differential Power Analysis
DRNG	Deterministic Random Number Generator
DS	Dedicated Software
ECC	Elliptic Curves Cryptography
EDC	Error Detection Code
EMA	Electro Magnetic Analysis
ES	Embedded Software
IC	Integrated Circuit
IDSLD	IDEMIA Secure Bootloader
MDMA	Multi-Channel Direct Memory Access
MPU	Memory Protection Unit
NVM	Non-Volatile Memory
RAM	Random Access Memory
ROM	Read Only Memory
RSA	Ron Rivest, Adi Shamir, and Leonard Adleman algorithm for public-key cryptography
RTL	Register Transfer Language
SCH	Schematic
SPA	Simple Power Analysis
ST	Security Target
STI	Test Controller
TOE	Target Of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Security Specification
UCP	Unified Crypto Processor
UCP - PKI	PKI accelerator sub module of UCP

Table 19: Glossary & Abbreviations

10 Disclaimer

ALL PRODUCTS, PRODUCT SPECIFICATIONS, DATA AND INFORMATION ARE SUBJECT TO CHANGE WITHOUT NOTICE TO IMPROVE RELIABILITY, FUNCTION OR DESIGN OR OTHERWISE.

The Products described in this document are subject to continuous development and improvement.

All intellectual property rights referred to herein, whether registered or not in specific countries, are the properties of their respective owners. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document or by any conduct of IDEMIA STARCHIP S.A.S.

This Products has been prepared and is fully owned by IDEMIA STARCHIP S.A.S. The information in this document is provided in connection with IDEMIA STARCHIP S.A.S. Products and shall not be regarded as a guarantee of conditions or characteristics. IDEMIA STARCHIP S.A.S. reserves the right to make changes to the Products at any time without notice.

Implementation of certain elements of this Products may require licenses under third party intellectual property rights, including without limitation, patent rights and copyright. IDEMIA STARCHIP S.A.S. is not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

IDEMIA STARCHIP S.A.S. makes no representation or warranty whatsoever regarding the Product and its information which is provided on an “as-is” basis.

IDEMIA STARCHIP S.A.S. hereby disclaims any and all warranties, express or implied, including, without limitation, the continuing production of any Product, warranties of fitness for particular purpose, non-infringement and merchantability.

IDEMIA STARCHIP S.A.S. its affiliates, agents, and employees, and all persons acting on its or their behalf hereby disclaim any and all liability for any errors, inaccuracies or incompleteness contained in any datasheet or in any other disclosure relating to any Product.

To the extent permitted by applicable law, IDEMIA STARCHIP S.A.S. shall not be liable to any user of the Products for any damages under any theory of law, including, without limitation, any special, consequential, incidental, or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, nor any damages arising out of third party claims (including claims of intellectual property infringement) arising out of the use of or inability to use the Products, even if advised of the possibility of such damages. Customers are responsible for their product and applications using IDEMIA STARCHIP S.A.S. Product.

All Products are sold subject to IDEMIA STARCHIP S.A.S.’ terms and conditions of sale applicable at the time of order acknowledgment.

The Products and its information, including technical data, may be subject to export or import regulations in different countries. Any user of the Products agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import the Products.