Public

Common Criteria Information Technology Security Evaluation

S3SSE2A

Version 1.1

28th July 2025

ST(Security Target) Lite

Important Notice

Samsung Electronics Co. Ltd. (“Samsung”) reserves the right to make changes to the information in this publication at any time without prior notice. All information provided is for reference purpose only. Samsung assumes no responsibility for possible errors or omissions, or for any consequences resulting from the use of the information contained herein.

This publication on its own does not convey any license, either express or implied, relating to any Samsung and/or third-party products, under the intellectual property rights of Samsung and/or any third parties.

Samsung makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does Samsung assume any liability arising out of the application or use of any product or circuit and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

Customers are responsible for their own products and applications. "Typical" parameters can and do vary in different applications. All operating parameters, including "Typicals" must be validated for each customer application by the customer's technical experts.

Samsung products are not designed, intended, or authorized for use in applications intended to support or sustain life, or for any other application in which the failure of the Samsung product could reasonably be expected to create a situation where personal injury or death may occur. Customers acknowledge and agree that they are solely responsible to meet all other legal and regulatory requirements regarding their applications using Samsung products notwithstanding any information provided in this publication. Customer shall indemnify and hold Samsung and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim (including but not limited to personal injury or death) that may be associated with such unintended, unauthorized and/or illegal use.

Samsung Electronics Co., Ltd.
San #24 Nongseo-Dong, Giheung-Gu
Yongin-City, Gyeonggi-Do, Korea 446-711

Contact Us: *junghyun.kim@samsung.com*

Home Page: *http://www.samsungsemi.com*

Chip Handling Guide

Precaution against Electrostatic Discharge

When using semiconductor devices, ensure that the environment is protected against static electricity:

1. Wear antistatic clothes and use earth band.
2. All objects that are in direct contact with devices must be made up of materials that do not produce static electricity.
3. Ensure that the equipment and work table are earthed.
4. Use ionizer to remove electron charge.

Contamination

Do not use semiconductor products in an environment exposed to dust or dirt adhesion.

Temperature/Humidity

Semiconductor devices are sensitive to:

- Environment
- Temperature
- Humidity

High temperature or humidity deteriorates the characteristics of semiconductor devices. Therefore, do not store or use semiconductor devices in such conditions.

Mechanical Shock

Do not to apply excessive mechanical shock or force on semiconductor devices.

Chemical

Do not expose semiconductor devices to chemicals because exposure to chemicals leads to reactions that deteriorate the characteristics of the devices.

Light Protection

In non- Epoxy Molding Compound (EMC) package, do not expose semiconductor IC to bright light. Exposure to bright light causes malfunctioning of the devices. However, a few special products that utilize light or with security functions are exempted from this guide.

Radioactive, Cosmic and X-ray

Radioactive substances, cosmic ray, or X-ray may influence semiconductor devices. These substances or rays may cause a soft error during a device operation. Therefore, ensure to shield the semiconductor devices under environment that may be exposed to radioactive substances, cosmic ray, or X-ray.

EMS (Electromagnetic Susceptibility)

Strong electromagnetic wave or magnetic field may affect the characteristic of semiconductor devices during the operation under insufficient PCB circuit design for Electromagnetic Susceptibility (EMS).

Revision History

Revision No.	Date	Description
0.0	24th April 2024	Creation
0.1	30th April 2024	The chapter 1.2.2,6.3.3.1 and 8 are updated
1.0	14th June 2025	The chapter 1,2,3,4,5,6 and 8 are updated
1.1	28th July 2025	Table 1 TOE Configuration is updated

Table of Contents

List of Figures

List of Tables

List of Conventions

Register RW Access Type Conventions

Type	Definition	Description
R	Read Only	The application has permission to read the Register field. Writes to read-only fields have no effect.
W	Write Only	The application has permission to write in the Register field.
RW	Read & Write	The application has permission to read and writes in the Register field. The application sets this field by writing 1'b1 and clears it by writing 1'b0.

Register Value Conventions

Expression	Description
x	Undefined bit
X	Undefined multiple bits
?	Undefined, but depends on the device or pin status
Device dependent	The value depends on the device
Pin value	The value depends on the pin status

Reset Value Conventions

Expression	Description
0	Clears the register field
1	Sets the register field
x	Don't care condition

Warning: Some bits of control registers are driven by hardware or write operation only. As a result the indicated reset value and the read value after reset might be different.

List of Terms

Terms	Descriptions
Application Data	All data managed by the Security IC Embedded Software in the application context. Application data comprise all data in the final Security IC.
Composite Product Integrator	Role installing or finalising the IC Embedded Software and the applications on platform transforming the TOE into the unpersonalised Composite Product after TOE delivery. The TOE Manufacturer may implement IC Embedded Software delivered by the Security IC Embedded Software Developer before TOE delivery (e.g. if the IC Embedded Software is implemented in ROM or is stored in the non-volatile memory as service provided by the IC Manufacturer or IC Packaging Manufacturer)
Composite Product Manufacturer	The Composite Product Manufacturer has the following roles (i) the Security IC Embedded Software Developer (Phase 1), (ii) the Composite Product Integrator (Phase 5) and (iii) the Personaliser (Phase 6). If the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice) he has the role of the IC Packaging Manufacturer (Phase 4) in addition.
End-consumer	User of the Composite Product in Phase 7.
IC Dedicated Software	IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
Initialisation Data	Initialisation Data defined by the TOE Manufacturer to identify the TOE and to keep track of the Security IC's production and further life-cycle phases are considered as belonging to the TSF data. These data are for instance used for traceability and for TOE identification (identification data).
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
Pre-personalisation Data	Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases.
Security IC	Composition of the TOE, the Security IC Embedded Software, User Data and the package (the Security IC carrier).
Security IC Embedded Software	Software embedded in a Security IC and normally not being developed by the IC Designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3 or in later phases of the Security IC product life-cycle. Some part of that software may actually implement a Security IC application others may provide standard services. Nevertheless, this distinction doesn't matter here so that the Security IC Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.

Security IC Product	Composite product which includes the Security Integrated Circuit (i.e. the TOE) and the Embedded Software and is evaluated as composite target of evaluation in the sense of the Supporting Document
TOE Delivery	The period when the TOE is delivered which is either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.
TOE Manufacturer	The TOE Manufacturer must ensure that all requirements for the TOE and its development and production environment are fulfilled. The TOE Manufacturer has the following roles: (i) IC Developer (Phase 2) and (ii) IC Manufacturer (Phase 3). If the TOE is delivered after Phase 4 in form of packaged products, he has the role of the (iii) IC Packaging Manufacturer (Phase 4) in addition.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE. This includes information about the TOE's configuration, if any is coded in non-volatile non-programmable memories (ROM), in specific circuitry, in non-volatile programmable memories (for instance E2PROM) or a combination thereof.
User data	All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.

List of Acronyms

Acronyms	Descriptions
CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Feature
TSFI	TSF Interface
TSP	TOE Security Policy

1 ST INTRODUCTION

1 This introductory chapter contains the following sections:

1.1 Security Target and TOE Reference

1.2 TOE Overview and TOE Description

1.3 Interfaces of the TOE

1.4 TOE Intended Usage

1.1 Security Target and TOE Reference

2 The Security Target Lite version is 1.1 and dated 28th July 2025
The Security Target Lite is strictly compliant to

3 [9] Eurosmart Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084-2014.

4 The Protection Profile and the Security Target are built on *Common Criteria CC:2022 Revision 1.*

Title: Security Target Lite of S3SSE2A

- Target of Evaluation: S3SSE2A
- TOE reference**:** S3SSE2A_20250522
- Provided by: Samsung Electronics Co., Ltd.
- Common Criteria version : refer to the chapter 2.1 CC Conformance Claim

1.2 TOE Overview and TOE Description

1.2.1 Introduction

5 The Target of Evaluation (TOE), the S3SSE2A microcontroller featuring the TORNADO™-E cryptographic coprocessor, is a smartcard integrated circuit which is composed of a processing unit, security components, contact based I/O ports, hardware circuit for testing purpose during the manufacturing process and volatile and non-volatile memories (hardware). The TOE also includes any IC Designer/Manufacturer proprietary IC Dedicated Software as long as it physically exists in the smartcard integrated circuit after being delivered by the IC Manufacturer. Such software (also known as IC firmware) is used for testing purpose during the manufacturing process but also provides additional services to facilitate the usage of the hardware and/or to provide additional services, a random number generation library and a random number generator. PQC engine (CRYSTALS) is a hardware coprocessor for high-speed Lattice operations. ACT1 Secure ML-DSA library is a software library that is built on the PQC coprocessor that provides high-level interface for ML-DSA.

The TOE consists of five sub-TSFs

- Main sub-TSF: this sub-TSF is defined as whole TSF except the sub-TSFs listed below.
- Memory access control policy sub-TSF
- Bootloader access control policy sub-TSF
- Security detector policy sub-TSF (only the detector's reaction to security incidents)
- Non-reversibility of TEST mode policy sub-TSF

1.2.2 TOE Definition

6 The S3SSE2A single-chip CMOS micro-controller is designed and packaged specifically for "Smart Card" applications.

7 The SC300 CPU architecture of the S3SSE2A microcontroller follows the Harvard style, that is, it has separate program memory and data memory. Both instruction and data can be fetched simultaneously without causing a stall, using separate paths for memory access.

8 The main security features of the S3SSE2A integrated circuit are:

- Environmental & Life time detector & filters
- Active shield
- Dedicated tamper-resistant design based on synthesizable glue logic and secure topology
- Dedicated hardware mechanisms against side-channel attacks
- Secure DES and AES Symmetric Cryptography support
- PQC(Post-Quantum Cryptography) engine(CRYSTALS)
- Secure TORNADO™-E Prime coprocessor for the support of RSA and ECC cryptographic operations
- PARITY/ CRC-32 calculators
- SHA-3

NOTE 1:

No security functionality is claimed for the SHA-3 hardware block.

SHA-3 is used internally by the ML-DSA library and the ML-DSA library is designed to use the SHA-3 in a secure way.

- Hardware Digital True Random Number Generator (DTRNG FRO M) that meet PTG.2 class of BSI AIS31 (German scheme) and some of ANSSI RGS requirements (French Scheme).
- The IC Dedicated Software includes:
  - One DTRNG FRO M library built around Hardware DTRNG FRO M together with corresponding DTRNG FRO M application notes. This library meets some of ANSSI RGS requirements (French scheme) as well as PTG.2 class of BSI-AIS31 (German scheme).
  - ACT1 Secure ML-DSA library (PQC library) for the support ML-DSA cryptographic operations. (optional)

9 The main hardware blocks of the S3SSE2A Integrated Circuit are described in **Figure 1** below:

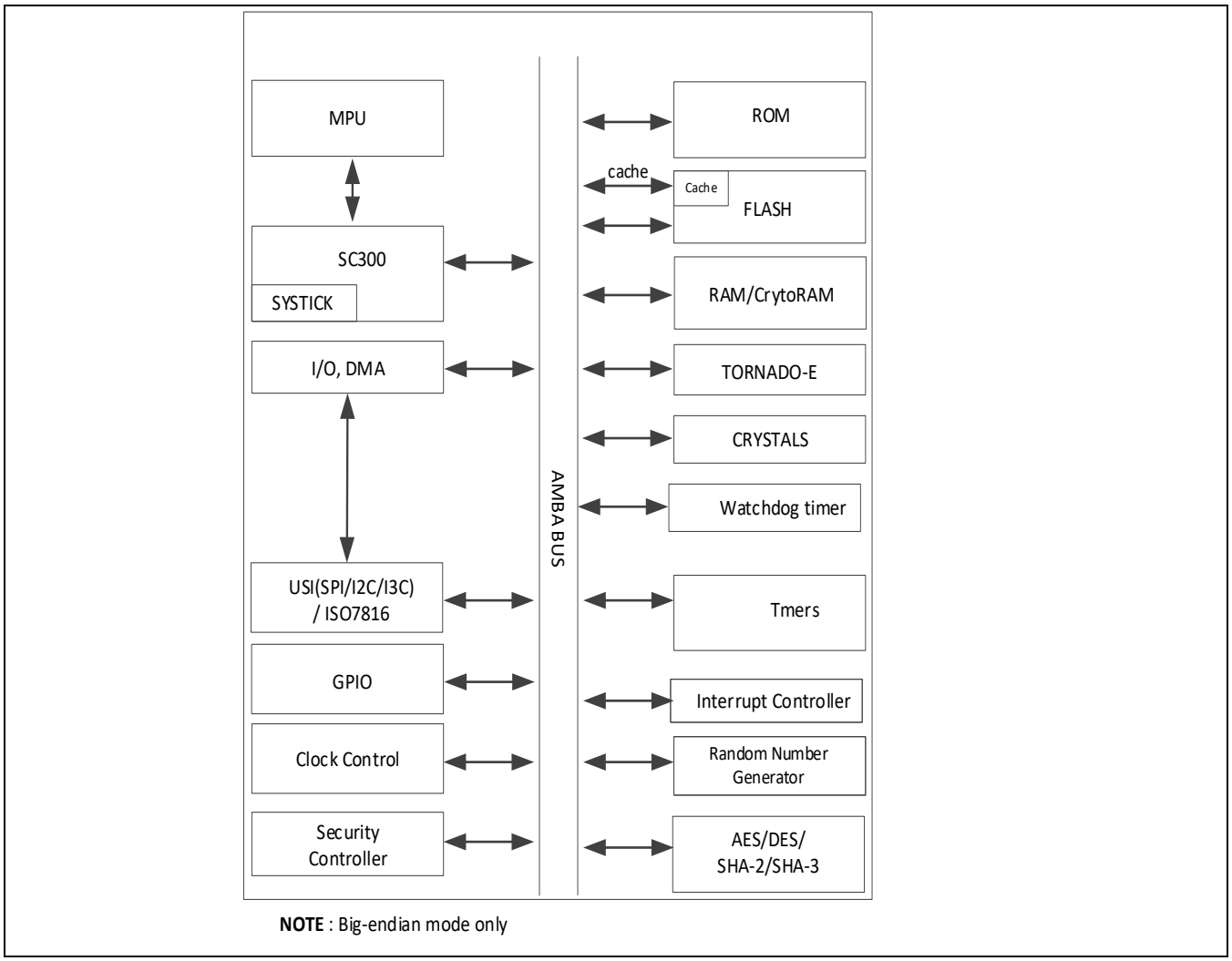


Figure 1 S3SSE2A Block Diagram

NOTE: That only the Triple DES algorithm belongs to the TOE, not the Single DES.

NOTE: 256/384/512 SHA-2 is not part of the TOE.

NOTE: CACHE is controlled by hardware of Flash. There is no address and then User software can't control CACHE.

The TOE consists of the following Hardware and Software:

TOE Hardware

- FLASH/SRAM for general purpose/ Cache RAM/Crypto RAM/ROM/ FLASH special area
- SC300 32-bit core
- Memory Protection Unit (MPU)
- Internal Voltage Regulator (IVR)
- Reset and Power down mode

  -Power-on reset and external reset
- External Clock : 1 MHz–10 MHz and Internal Clock
- Active shield, Environmental & Life time detector & filters
- Bilateral Pseudo Random Number Generator (BPRNG)
  - A Bilateral Pseudo Random Number Generator (BPRNG): no compliance to any specific metric, but BPRNG is used by the chip for internal use
- Digital True random number generator (DTRNG FRO M)
  - A Digital True random number generator (DTRNG FRO M): PTG.2 class compliant (German Scheme) and meeting some of ANSSI RGS requirements (French scheme)
- SHA-3 hardware engine
- Triple DES cryptographic coprocessor with 112 or 168 bits key size
  - Built-in hardware Triple DES accelerator
  - Circuit for resistance against SPA, DPA and safe error attacks
- AES cryptographic coprocessor with 128 bits, 192bits and 256bits key size
  - Built-in hardware AES accelerator
  - Circuit for resistance against SPA, DPA and safe error attacks
  - ECB mode
- TORNADO™-E coprocessor supports modular multiplications for the operand size up to 4128-bit and modular additions/subtractions for the operand size up to 544-bit.
  - Built-in hardware accelerator for big number calculation
- PQC(Post-Quantum Cryptography) engine(CRYSTALS)

- Memory Integrity checkers (ECC, Parity, CRC)

- Programmable interval Timers/ Idle Timer/ Watchdog Timer

- DMA controller for data transfer from UART and SPI to RAM
- Memory Encryption and Bus Scrambling
- FLASH encryption with User-defined value

- Interfaces
  - I2C,I3C interface for Serial communication
  - SPI interface for One hardware slave interface and Supporting class B, C
  - Serial I/O Interface

    . T=0 and 1 (ISO 7816-3)
    .Hardware UART (ISO7816) supports T=0 and T=1 protocols
    .Fast switching from transmission to reception
    .CRC-CCITT

1.2.2.1 Additional Hardware TOE Features

- FLASH Write Operations
- Interrupts
  -Nested Vector Interrupt Controller: 32ea
  -SYSTICK
- Operating Voltage Range
  1.62 V - 3.3 V
- Operating Temperature
  -30°C to 85°C
- Package
  - Wafer
  - 8/6-pin COB (compliant with ISO 7816)
  - WLP

TOE Software

10 The TOE software comprises the following components:

- One Digital True Random Number Generator (DTRNG FRO M) library that fulfills the requirements of Class PTG.2 (German Scheme) as well as meets some of ANSSI RGS requirements (French scheme)
- Secure Boot Loader is a loader for downloading in Flash and can download the encrypted user code with AES
- System API is an Application Programming Interface which controls Non-Volatile Memory (NOR Flash), receives and transmits data from a host and utilities supported. It is used in Bootloader and can be also used for the Security IC Embedded Software. No security relevant policy, mechanism or function is supported
- ACT1 Secure ML-DSA library(optional)

  PQC (CRYSTALs) is a hardware coprocessor for high-speed Lattice operations. ACT1 Secure ML-DSA library is a software library that is built on the PQC coprocessor that provides high-level interface for ML-DSA
  The ML-DSA functions of the library included in the TOE are
  - Dilithium_library_version_info (Print version information)
  - key_destruction_mldsa_sec (Secure Key destruction)
  - crypto_sign (Internal Function of Signature Generation in ML-DSA)
  - crypto_sign_open (Internal Function of signature verification in ML-DSA)
  - crypto_sign_keypair (Internal Function of Key generation in ML-DSA)
  - secure_get_parity_from_secret_key_packed_key (Parity check for verifying the integrity of a secret key)

11 **The TOE configuration is summarized in table 1 below:**

Item type	Item	Version	Date	Form of delivery
Hardware	S3SSE2A 32-bit RISC Microcontroller for Smart Card	0	-	Wafer or Module
Software	Test ROM Code	1.0	-	- Included in S3SSE2A Test ROM - Test ROM code is not part of the TOE.
Software	Secure Boot loader & System API Code (s3sse2a_se_rom_release_v1_1.hex)	1.1	2023.06.01	Included in S3SSE2A in ROM
Software	DTRNG FRO M library (S3SSE2A_PTG2_DTRNG_library_v1.2.lib)	1.2	2024.03.07	Software Library. This library is delivered as object file and is optionally integrated into user NVM code.
Software	ACT1 ML-DSA Library v1.15	1.15	2025.05.26	Software Library. This library

Item type	Item	Version	Date	Form of delivery
	(ACT1_MLDSA_V1.15.lib)			is delivered as object file and is optionally integrated into user NVM code.
Document	S3SSE2A HW DTRNG FRO M and DTRNG FRO M Library Application Note (S3SSE2A_DTRNG_FRO_M_AN_v1.0.pdf)	1.0	2023.12.07	Softcopy
Document	CRYSTALS ML-DSA (Module Lattice based Digital signature algorithm) Library v1.15 API Manual (ACT1 MLDSA Library API Manual v1.10.pdf)	1.10	2025.06.02	Softcopy
Document	S3SSE2A User's Manual (S3SSE2A_UM_v1.0.pdf)	1.0	2025.04.08	Softcopy
Document	Security Application Note For S3SSE2A (SAN_S3SSE2A_v0.3.pdf)	0.3	2025.05.09	Softcopy
Document	S3SSE2A Chip Delivery Specification (DeliverySpec_S3SSE2A_Rev1.01.pdf)	1.01	May,2025	Softcopy
Document	S3SSE2A Boot Loader Specification (S3SSE2A_TN01_Bootloader_Specification_v0.5.pdf)	0.5	2025.05.10	Softcopy
Document	S3SSE2A System API Application Note (S3SSE2A_AN01_SystemAPI_v1.0.pdf)	1.0	2023.03.22	Softcopy
Document	SC300 Reference Manual (SC300_Reference_Manual v0.0.pdf)	0.0	2014.05.12	Softcopy
Document	Cryptographic Mechanisms For S3SSE2A (Cryptographic_Mechanisms_S3SSE2A_v0.2.pdf)	0.2	2025.03.26	Softcopy

Item	Method of delivery
Hardware	Secure carrier
Software	Libraries are encrypted by PGP encryption and then delivered by email.
Documents	Documents are encrypted by PGP encryption and then delivered by email.

Table 1 TOE Configuration

12 TEST mode and NORMAL mode

In NORMAL mode of the TOE, TOE can no longer go back to TEST mode domain again

13 PRIVILEGE mode and USER mode

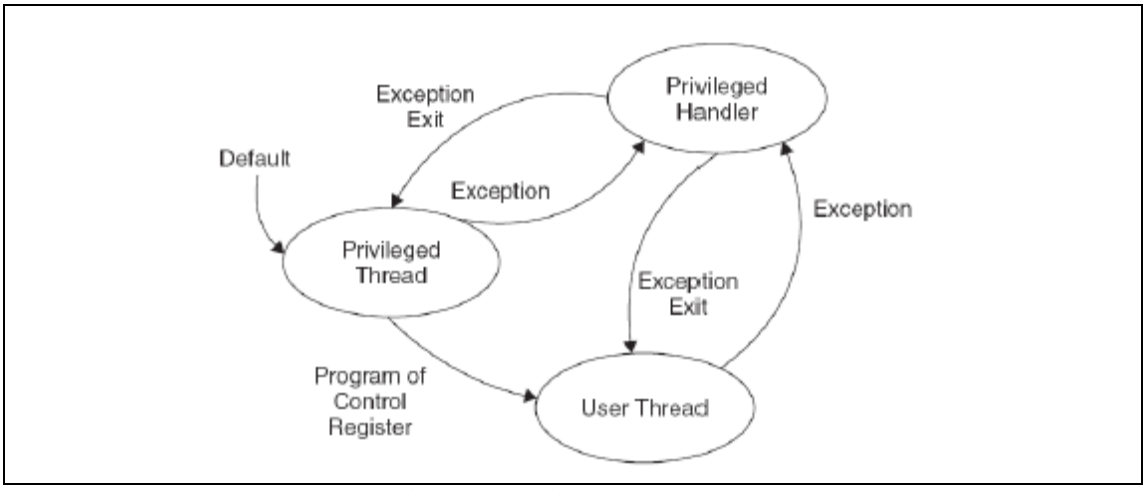


Figure 1-2 Privilege and User Modes

Code can execute as privileged or unprivileged.

Software in the privileged access level can switch the program into the user access level using the control register. When an exception takes place, the processor will always switch back to the privileged state and return to the previous state when exiting the exception handler.

1.2.3 TOE Life cycle

14 The complex development and manufacturing processes of a Composite Product can be separated into seven distinct phases. The phases 2 and 3 of the Composite Product life cycle cover the IC development and production:

Company	**phase**
Hwasung Plant/DSR building	(2)
Giheung Plant/ SR3 building	(2)
Giheung Plant/ SR1 building	(2)
Giheung Plant/ Line S1	(3)
Giheung Plant/ Line 2	(3)
Giheung Plant/ Line 1	(3)
Onyang Plant/Warehouse	(4)
Onyang Plant/ Line 2	(4)
Onyang Plant/ Line 4	(4)
Photronics Plant	(3)
TOPPAN Plant	(3)
HANAMICRON Plant	(4)
Inesa Plant	(4)

Doosan TESNA Plant	(3)
ASE Korea	(4)
SFA Plant	(4)

Table 2 Sites of the TOE life cycle

- IC Development (Phase 2):
  - IC design,
  - IC Dedicated Software development,
- the IC Manufacturing (Phase 3):
  - integration and photomask fabrication,
  - IC production,
  - IC testing,
  - preparation and
  - Pre-personalisation if necessary

15 The Composite Product life cycle phase 4 can be included in the evaluation of the IC as an option:

- the IC Packaging (Phase 4):
  - Security IC packaging (and testing),
  - Pre-personalisation if necessary(if not done in phase 3).

16 In addition, three important stages have to be considered in the Composite Product life cycle:

- Security IC Embedded Software Development (Phase 1),
- the Composite Product finishing process, preparation and shipping to the personalisation line for the Composite Product (Composite Product Integration Phase 5),

Package in Phase 5	Description
Package 1 (Static Mutual Authentication)	Loader dedicated for usage in Secured Environment only
Package 2 (Dynamic Mutual Authentication)	Loader dedicated for usage by authorized users only

- the Composite Product personalisation and testing stage where the User Data is loaded into the Security IC's memory (Personalisation Phase 6),

- the Composite Product usage by its issuers and consumers (Operational Usage Phase 7) which may include loading and other management of applications in the field.

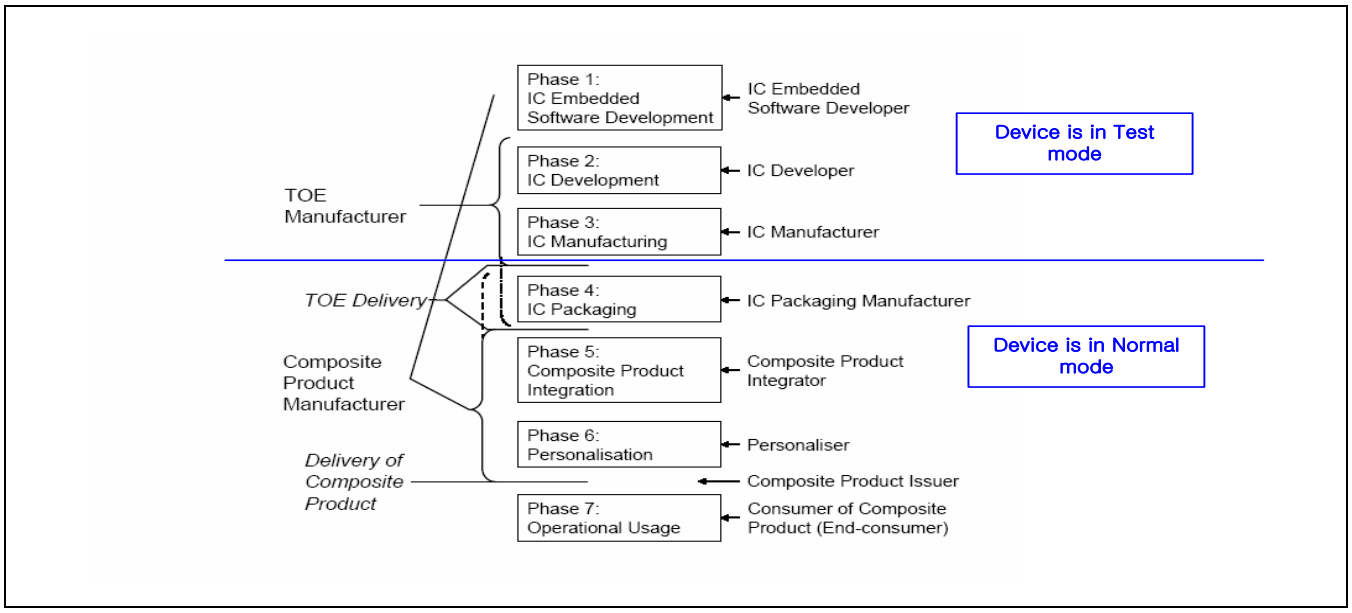


Figure 2 Definition of "TOE Delivery" and responsible Parties

17 The Security IC Embedded Software is developed outside the TOE development in Phase 1. The TOE is developed in Phase 2 and produced in Phase 3. Then the TOE is delivered in form of wafers. The TOE can also be delivered in form of packaged products. In this case, the development and production of the TOE not only pertain to Phase 2 and 3 but to Phase 4 in addition.

1.3 Interfaces of the TOE

- The physical interface of the TOE with the external environment is the entire surface of the IC
- The electrical interface of the TOE with the external environment is made of the chip's pads including the VDD, XRSTB, XCLK, GND, SIO, SPI ,I2C, I3C as well as GPIO interface
- The data interface of the TOE is made of the Contact I/O, SPI, I2C and I3C interfaces.
- The software interface of the TOE with the hardware consists of Special Function Registers (SFR) and CPU instructions.
- The TRNG interface of the TOE is defined by the DTRNG FRO M libraries interface.
- The Bootloader interface and the System API interface
- The PQC interface of the TOE is defined by the CRYSTALS ML-DSA library interface (optional).

1.4 TOE Intended Usage

18 The TOE is dedicated to applications such as:

- Banking and finance applications for credit or debit cards, electronic purse (stored value cards) and electronic commerce.
- Network based transaction processing such a mobile phones (GSM SIM cards), pay TV (subscriber and pay-per-view cards), communication highways (Internet access and transaction processing).

- Transport and ticketing applications (access control cards).
- Governmental cards (ID cards, health cards, driving licenses).
- Multimedia applications and Digital Right Management protection.

2 CONFORMANCE CLAIMS

19 This chapter 2 contains the following sections:

2.1 CC Conformance Claim

20 This Security target claims to be conformant to the Common Criteria CC:2022 Revision 1.

21 Furthermore, it claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in chapter 5.

22 This Security Target has been built with the Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, which comprises:

[1] Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022 - Part 1: Introduction and General Model, CCMB-2022-11-001

[2] Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022 - Part 2: Security functional components, CCMB-2022-11-002

[3] Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022 - Part 3: Security assurance components, CCMB-2022-11-003

[4] Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022 — Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004

[5] Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022 — Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005

[6] Common Criteria for Information Technology Security Evaluation, CEM:2022, Revision 1, November 2022 - Evaluation methodology, CCMB-2022-11-006

[7] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, 2024-07-22, CCMB-2024-002

2.2 PP Claim

23 This Security Target is strictly compliant to the Security IC Platform Protection Profile [9]. The Security IC Platform Protection Profile is registered and certified by the Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084, Version 1.0, dated 01.2014

24 This ST does not claim conformance to any other PP.

2.3 Package Claim

25 The Security Target is modularized as a multi-assurance Security Target as detailed in section 2.4.

26 This Security Target is strictly compliant to the Security IC Platform Protection Profile [9] with additional packages:

- Packages “Authentication of the Security IC”, “TDES” and “AES” and “Hash functions”, conformant
- Package 1 : Loader dedicated for usage in secured environment , conformant
- Package 2 : Loader dedicated for usage by authorized users only, conformant

27 The Security IC Platform Protection Profile is registered and certified by the Bundesamt für Sicherheit in

der Informationstechnik (BSI) under the reference BSI-CC-PP-0084, Version 1.0, dated 01.2014.

28 This ST does not claim conformance to any other PP.

2.4 Conformance Claim Rationale

29 This security target claims strict conformance only to one PP, the Security IC Platform Protection Profile [9].

30 The Evaluation Assurance Level (EAL) of the PP [9] is EAL 4 augmented with the assurance components ALC_DVS.2 and AVA_VAN.5.

The Security Target is modularized as a multi-assurance Security Target.

The Security Target claims a global conformance to EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5 and ASE_TSS.2.

This Security Target claims conformance to assurance package EAL6 augmented with ASE_TSS.2 for the following sub-TSFs:

- memory access control policy,
- bootloader access control policy,
- security detector policy (only the detector's reaction to security incidents),
- non-reversibility of TEST mode policy

31 The Target of Evaluation (TOE) is a complete solution implementing a security integrated circuit (security IC) as defined in the PP [9] section 1.3.1, so the TOE is consistent with the TOE type in the PP [9].

32 The security problem definition of this security target is consistent with the statement of the security problem definition in the PP [9], as the security target claimed strict conformance to the PP [9]. Additional threats, organizational security policies and assumptions are introduced in chapter 3 of this ST, a rationale is given in chapter 4.4.

33 The security objectives of this security target are consistent with the statement of the security objectives in the PP [9], as the security target claimed strict conformance to the PP [9]. Additional security objectives are added in chapter 4.1 of this ST, a rationale is given in chapter 4.4.

34 The security requirements of this security target are consistent with the statement of the security requirements in the PP [9], as the security target claimed strict conformance to the PP [9]. Additional security requirements are added in chapter 6.1 of this ST, a rationale is given in chapter 6.3. All assignments and selections of the security functional requirements are done in the PP [9] and in this security target section 6.

3 SECURITY PROBLEM DEFINITION

35 This chapter 3 contains the following sections:

3.1 Description of Assets

3.2 Threats

3.3 Organizational Security Policies

3.4 Assumptions

3.1 Description of Assets

Assets regarding the Threats

36 The assets (related to standard functionality) to be protected are

- the User Data of the Composite TOE,
- the Security IC Embedded Software stored and in operation,,
- the Security services provided by the TOE for the Security IC Embedded Software.

37 The user (consumer) of the TOE places value upon the assets related to high-level security concerns:

SC1 integrity of user data of the Composite TOE,

SC2 confidentiality of user data of the Composite TOE being stored in the TOE's protected memory areas,

SC3 correct operation of the security services provided by the TOE for the Security IC Embedded Software.

Note the Security IC Embedded Software is user data and shall be protected while being executed/processed and while being stored in the TOE's protected memories.

38 The Security IC may not distinguish between user data which is public knowledge or kept confidential. Therefore the security IC shall protect the user data of the Composite TOE in integrity and in confidentiality if stored in protected memory areas, unless the Security IC Embedded Software chooses to disclose or modify it.

39 In particular integrity of the Security IC Embedded Software means that it is correctly being executed which includes the correct operation of the TOE's functionality. Parts of the Security IC Embedded Software which do not contain secret data or security critical source code, may not require protection from being disclosed. Other parts of the Security IC Embedded Software may need to be kept confidential since specific implementation details may assist an attacker.

40 The Protection Profile[9] requires the TOE to provide at least one security service: the generation of random numbers by means of a physical Random Number Generator. The Security Target may require additional security services as described in the annexe 7 of the protection profile or define TOE specific security services. It is essential that the TOE ensures the correct operation of all security services provided by the TOE for the Security IC Embedded Software.

41 According to the Protection Profile there is the following high-level security concern related to security service:

SC4 deficiency of random numbers.

42 To be able to protect these assets (SC1 to SC4) the TOE shall self-protect its TSF. Critical information about the TSF shall be protected by the development environment and the operational environment. Critical information may include:

- logical design data, physical design data, IC Dedicated Software, and configuration data,
- Initialisation Data and Pre-personalisation Data, specific development aids, test and characterisation related data, material for software development support, and photomasks.

43 Such information and the ability to perform manipulations assist in threatening the above assets.

44 Note that there are many ways to manipulate or disclose the user data of the Composite TOE: (i) An attacker may manipulate the Security IC Embedded Software or the TOE. (ii) An attacker may cause malfunctions of the TOE or abuse Test Features provided by the TOE. Such attacks usually require design information of the TOE to be obtained. They pertain to all information about (i) the circuitry of the IC (hardware including the physical memories), (ii) the IC Dedicated Software with the parts IC Dedicated Test Software (if any) and IC Dedicated Support Software (if any), and (iii) the configuration data for the TSF. The knowledge of this information may enable or support attacks on the assets. Therefore the TOE Manufacturer must ensure that the development and production of the TOE (refer to Section 1.2.3) is secure so that no restricted, sensitive, critical or very critical information is unintentionally made available for attacks in the operational phase of the TOE (cf. [15] for details on assessment of knowledge of the TOE in the vulnerability analysis).

45 The TOE Manufacturer must apply protection to support the security of the TOE. This not only pertains to the TOE but also to all information and material exchanged with the developer of the Security IC Embedded Software. This covers the Security IC Embedded Software itself if provided by the developer of the Security IC Embedded Software or any authentication data required to enable the download of software. This includes the delivery (exchange) procedures for Phase 1 and the Phases after TOE Delivery as far as they can be controlled by the TOE Manufacturer. These aspects enforce the usage of the supporting documents and the refinements of SAR defined in the protection profile.

46 The information and material produced and/or processed by the TOE Manufacturer in the TOE development and production environment (Phases 2 up to TOE Delivery) can be grouped as follows:

- logical design data,
- physical design data,
- IC Dedicated Software, Initialisation Data and Pre-personalisation Data,
- Security IC Embedded Software, provided by the Security IC Embedded Software developer and implemented by the IC manufacturer,
- specific development aids,
- test and characterisation related data,

- material for software development support, and
- photomasks and products in any form

as long as they are generated, stored, or processed by the TOE Manufacturer.

3.2 Threats

47 The following explanations help to understand the focus of the threats and objectives defined below. For example, certain attacks are only one step towards a disclosure of assets, others may directly lead to a compromise of the application security.

- Manipulation of user data (which includes user data and code of the Composite TOE, stored in or processed by the Security IC) means that an attacker is able to alter a meaningful block of data. This should be considered for the threats T.Malfunction, T.Phys-Manipulation and T.Abuse-Func
- Disclosure of user data (which may include user data and code of the Composite TOE, stored in protected memory areas or processed by the Security IC) or TSF data means that an attacker is realistically3F2 able to determine a meaningful block of data. This should be considered for the threats T.Leak-Inherent, T.Phys-Probing, T.Leak-Forced and T.Abuse-Func.
- Manipulation of the TSF or TSF data means that an attacker is able to deliberately deactivate or otherwise change the behaviour of a specific security functionality in a manner which enables exploitation. This should be considered for the threat T.Malfunction, T.Phys-Manipulation and T.Abuse-Func.

48 The cloning of the functional behaviour of the Security IC on its physical and command interface is the highest level security concern in the application context. This should be considered for the threat T.Masquerade_TOE.

49 The cloning of that functional behaviour requires to (i) develop a functional equivalent of the Security IC Embedded Software, (ii) disclose, interpret and employ the user data of the Composite TOE stored in the TOE, and (iii) develop and build a functional equivalent of the Security IC using the input from the previous steps.

50 The Security IC is a platform for the Security IC Embedded Software which ensures that especially the critical user data of the Composite TOE are stored and processed in a secure way (refer to below). The Security IC Embedded Software must also ensure that critical user data of the Composite TOE are treated as required in the application context. In addition, the personalisation process supported by the Security IC Embedded Software (and perhaps by the Security IC in addition) must be secure. This last step is beyond the scope of this security target. As a result the threat "cloning of the functional behaviour of the Security IC on its physical and command interface" is averted by the combination of mechanisms which split into those being evaluated according to this security target (Security IC) and those being subject to the evaluation of the Security IC Embedded Software or Security IC and the corresponding personalisation process. Therefore, functional cloning is indirectly covered by the security concerns and threats described below.

The following threats from the Security IC Platform Protection Profile BSI-PP-0084 [9] are applicable for this Security Target:

Threat	**Description**	**Origin**
T.Phys-Manipulation	Physical Manipulation	BSI-PP-0084 - Standard threat
T.Phys-Probing	Physical Probing	BSI-PP-0084 - Standard threat
T.Malfunction	Malfunction due to Environmental Stress	BSI-PP-0084 - Standard threat

T.Leak-Inherent	Inherent Information Leakage	BSI-PP-0084 - Standard threat
T.Leak-Forced	Forced Information Leakage	BSI-PP-0084 - Standard threat
T.Abuse-Func	Abuse of Functionality	BSI-PP-0084 - Standard threat
T.RND	Deficiency of Random Numbers	BSI-PP-0084 - Threat related to security service
T.Masquerade_TOE	Masquerade the TOE	BSI-PP-0084 – Package "Authentication of the Security IC"

Table 4 Threats from BSI-PP-0084 [9]

The Security Target defines the following additional threats:

Threat	**Description**	**Origin**
T.Mem-Access	Memory Access Violation	Additional threat defined by the ST
T.Open_Samples_Diffusion	Diffusion of open samples	Additional threat defined by the ST (PP0084 – Interpretations [21])

Table 5 Additional threats defined in this Security Target

51 The high-level security concerns are refined below by defining threats as required by the Common Criteria (refer to Figure 3). Note that manipulation of the TOE is only a means to threaten user data and is not a success for the attacker in itself.

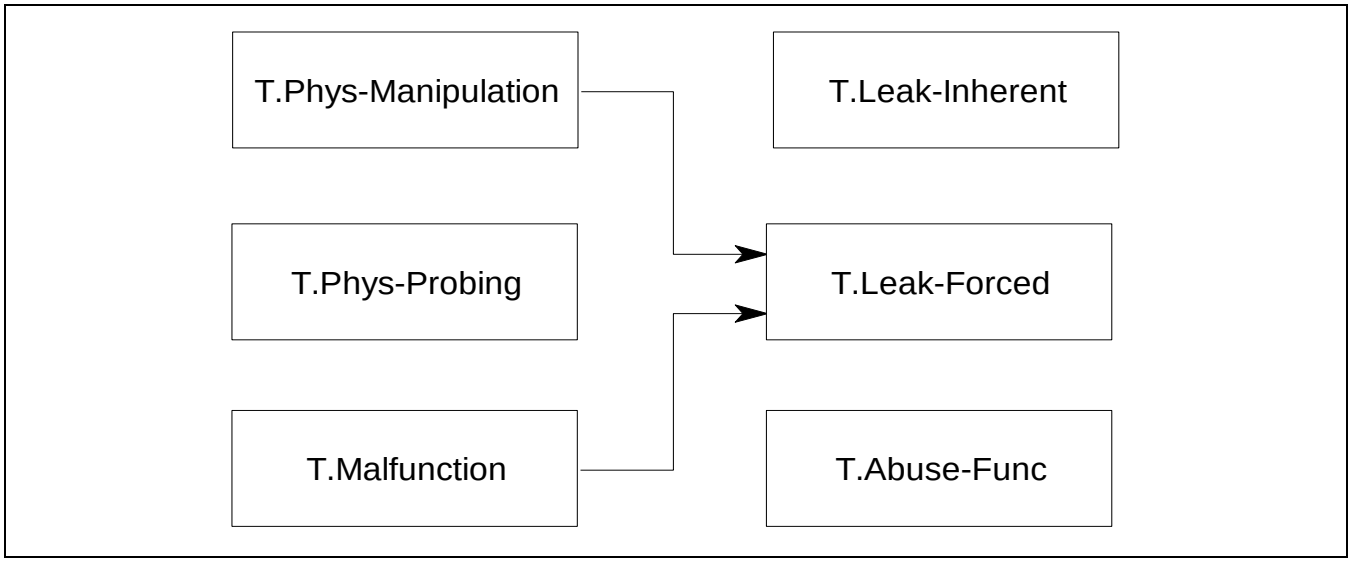


Figure 3 Standard Threats

52 The high-level security concern related to security service is refined below by defining threats as required by the Common Criteria (refer to Figure 4).

Figure 4 Threats related to security service

53 The Security IC Embedded Software must contribute to averting the threats: At least it must not undermine the security provided by the TOE.

54 The above security concerns are derived from considering the end-usage phase (Phase 7) since

- Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by assumptions and
- the development and production environment starting with Phase 2 up to TOE Delivery are covered by an organisational security policy.

55 The TOE's countermeasures are designed to avert the threats described below. Nevertheless, they may be effective in earlier phases (Phases 4 to 6).

56 The TOE is exposed to different types of influences or interactions with its outer world. Some of them may result from using the TOE only but others may also indicate an attack. The different types of influences or interactions are visualised in Figure 5. Due to the intended usage of the TOE all interactions are considered as possible.

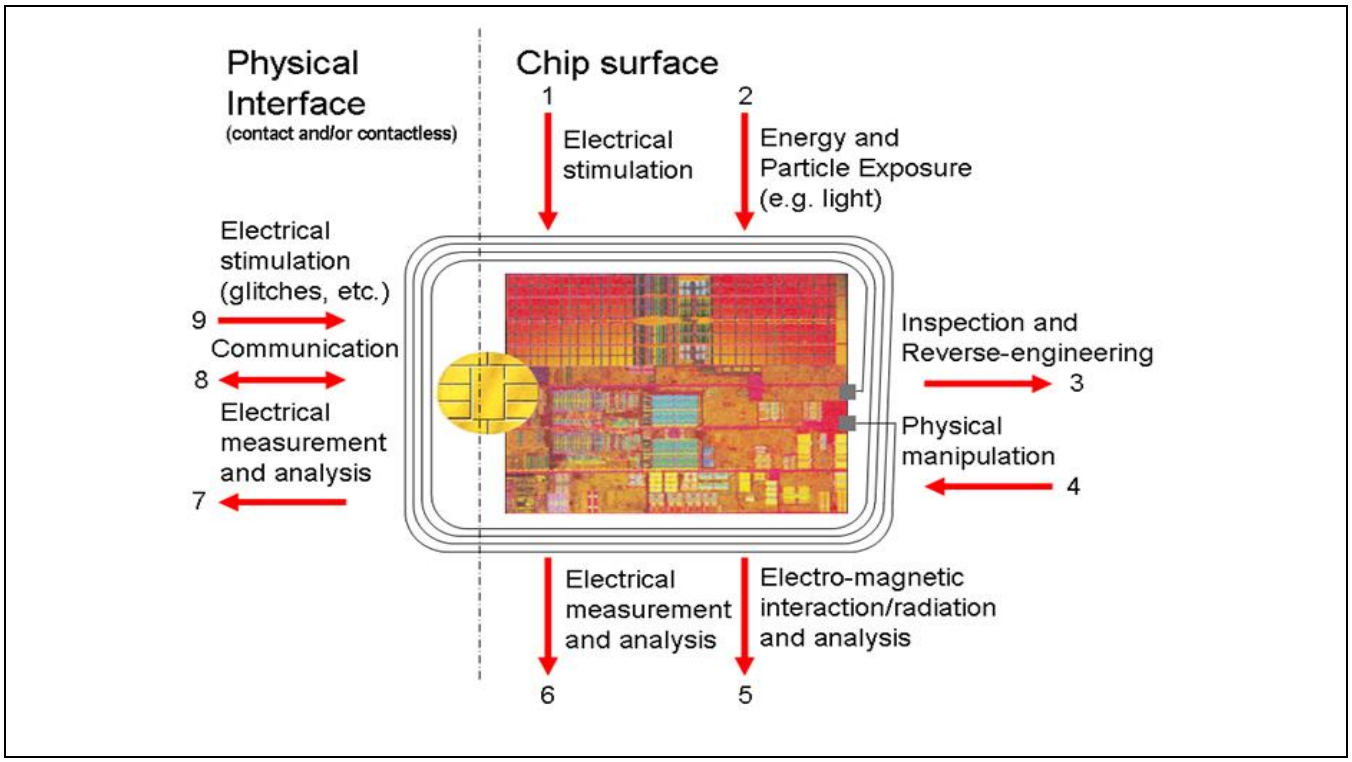


Figure 5 Interactions between the TOE and its outer world

57 An interaction with the TOE can be done through the physical interfaces (Number 7 – 9 in Figure 5) which are realised using contacts and/or a contactless interface. Influences or interactions with the TOE also occur through the chip surface (Number 1 – 6 in Figure 5). In Number 1 and 6 galvanic contacts are used. In

Number 2 and 5 the influence (arrow directed to the chip) or the measurement (arrow starts from the chip) does not require a contact. Number 3 and 4 refer to specific situations where the TOE and its functional behaviour is not only influenced but definite changes are made by applying mechanical, chemical and other methods (such as 1, 2). Many attacks require a prior inspection and some reverse-engineering (Number 3). This demonstrates the basic building blocks of attacks. A practical attack will use a combination of these elements.

3.2.1 Standard Threats

58 The TOE shall avert the threat "Inherent Information Leakage (T.Leak-Inherent)" as specified below.

T.Leak-Inherent	Inherent Information Leakage An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data as part of the assets.

59 No direct contact with the Security IC internals is required here. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. One example is the Differential Power Analysis (DPA). This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from direct (contact) measurements (Numbers 6 and 7 in Figure 5) or measurement of emanations (Number 5 in Figure 5) and can then be related to the specific operation being performed.

60 The TOE shall avert the threat "Physical Probing (T.Phys-Probing)" as specified below.

T.Phys-Probing	Physical Probing An attacker may perform physical probing of the TOE in order (i) to disclose user data while stored in protected memory areas, (ii) to disclose/reconstruct the user data while processed or (iii) to disclose other critical information about the operation of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.

61 Physical probing requires direct interaction with the Security IC internals (Numbers 5 and 6 in Figure 5). Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that hardware security mechanisms and layout characteristics need to be identified (Number 3 in Figure 5). Determination of software design including treatment of user data of the Composite TOE may also be a pre-requisite.

62 This pertains to "measurements" using galvanic contacts or any type of charge interaction whereas manipulations are considered under the threat "Physical Manipulation (T.Phys-Manipulation)". The threats "Inherent Information Leakage (T.Leak-Inherent)" and "Forced Information Leakage (T.Leak-Forced)" may use physical probing but require complex signal processing in addition.

63 The TOE shall avert the threat "Malfunction due to Environmental Stress (T.Malfunction)" as specified below.

T.Malfunction	Malfunction due to Environmental Stress An attacker may cause a malfunction of TSF or of the Security IC Embedded Software by applying environmental stress in order to (i) modify security services of the TOE or (ii) modify functions of the Security IC Embedded Software (iii) deactivate or affect security mechanisms of the TOE to enable attacks disclosing

or manipulating the user data of the Composite TOE or the Security IC Embedded Software. This may be achieved by operating the Security IC outside the normal operating conditions (Numbers 1, 2 and 9 in Figure 5).

64 The modification of security services of the TOE may e.g. affect the quality of random numbers provided by the random number generator up to undetected deactivation when the random number generator does not produce random numbers and the Security IC Embedded Software gets constant values. In another case errors are introduced in executing the Security IC Embedded Software. To exploit this an attacker needs information about the functional operation, e.g. to introduce a temporary failure within a register used by the Security IC Embedded Software with light or a power glitch.

65 The TOE shall avert the threat "Physical Manipulation (T.Phys-Manipulation)" as specified below.

T.Phys-Manipulation	Physical Manipulation An attacker may physically modify the Security IC in order to (i) modify user data of the Composite TOE, (ii) modify the Security IC Embedded Software, (iii) modify or deactivate security services of the TOE, or (iv) modify security mechanisms of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.

66 The modification may be achieved through techniques commonly employed in IC failure analysis (Numbers 1, 2 and 4 in Figure 5) and IC reverse engineering efforts (Number 3 in Figure 5). The modification may result in the deactivation of a security feature. Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of user data of the Composite TOE may also be a pre-requisite. Changes of circuitry or data can be permanent or temporary.

67 In contrast to malfunctions (refer to T.Malfunction) the attacker requires gathering significant knowledge about the TOE's internal construction here (Number 3 in Figure 5).

68 The TOE shall avert the threat "Forced Information Leakage (T.Leak-Forced)" as specified below:

T.Leak-Forced	Forced Information Leakage An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data of the Composite TOE as part of the assets even if the information leakage is not inherent but caused by the attacker.

69 This threat pertains to attacks where methods described in "Malfunction due to Environmental Stress" (refer to T.Malfunction) and/or "Physical Manipulation" (refer to T.Phys-Manipulation) are used to cause leakage from signals (Numbers 5, 6, 7 and 8 in Figure 5) which normally do not contain significant information about secrets.

70 The TOE shall avert the threat "Abuse of Functionality (T.Abuse-Func)" as specified below.

T.Abuse-Func	Abuse of Functionality An attacker may use functions of the TOE which may not be used after TOE Delivery in order to (i) disclose or manipulate user data of the Composite TOE, (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE or (iii) manipulate (explore, bypass, deactivate or change) functions of the

Security IC Embedded Software or (iv) enable an attack disclosing or manipulating the the user data of the Composite TOE or the Security IC Embedded Software.

3.2.2 Threats related to security services

71 The TOE shall avert the threat "Deficiency of Random Numbers (T.RND)" as specified below.

T.RND	Deficiency of Random Numbers An attacker may predict or obtain information about random numbers generated by the TOE security service for instance because of a lack of entropy of the random numbers provided.

An attacker may gather information about the random numbers produced by the TOE security service. Because unpredictability is the main property of random numbers this may be a problem in case they are used to generate cryptographic keys. The entropy provided by the random numbers must be appropriate for the strength of the cryptographic algorithm, the key or the cryptographic variable is used for. Here the attacker is expected to take advantage of statistical properties of the random numbers generated by the TOE. Malfunctions or premature ageing are also considered which may assist in getting information about random numbers.

3.2.3 Threats related to additional TOE Specific Functionality

72 The TOE shall avert the additional threat "Memory Access Violation (T.Mem-Access)" as specified below.

T.Mem-Access	Memory Access Violation Parts of the IC Smartcard Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). Any restrictions are defined by the security policy of the specific application context and must be implemented by the Smartcard IC Embedded Software.

Clarification: This threat does not address the proper definition and management of the security rules implemented by the Security IC Embedded Software, this being software design and correctness issue.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 level potential of attack.

3.2.4 Threats related to Authentication of the Security IC

The TOE shall avert the threat "Masquerade the TOE (T. Masquerade_TOE)" as specified below.

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.

The threat T.Masquerade_TOE may threaten the unique identity of the TOE as described in the P.Process-TOE or the property as being a genuine TOE without unique identity. Mitigation of masquerade requires tightening up the identification by authentication.

3.2.5 Threats related to Diffusion of open samples

The TOE shall avert the threat "Diffusion of open samples(T.Open_Samples_Diffusion)" as specified below.

T.Open_Samples_Diffusion Diffusion of open samples

An attacker may get access to open samples of the TOE and use them to gain information about the TSF (loader, memory management unit, ROM code, …). He may also use the open samples to characterize the behavior of the IC and its security functionalities (for example: characterization of side channel profiles, perturbation cartography, …). The execution of a dedicated security features (for example: execution of a DES computation without countermeasures or by de-activating countermeasures) through the loading of an adequate code would allow this kind of characterization and the execution of enhanced attacks on the IC.

3.3 Organizational Security Policies

The following policies from the Security IC Platform Protection Profile BSI-PP-0084 [9] are applicable for this Security Target:

Policy	Description	Origin
P.Process-TOE	Identification during TOE Development and Production	BSI-PP-0084 – Standard OSP
P.Crypto-Service	Cryptographic services of the TOE	BSI-PP-0084 - Packages for Cryptographic Services
P.Lim_Block_Loader	Limiting and Blocking the Loader Functionality	BSI-PP-0084 - Package 1 for loader
P.Ctlr_Loader	Controlled usage to Loader Functionality	BSI-PP-0084 – Package 2 for loader

Table 6 Policies from BSI-PP-0084 [9]

73 The following Figure 6 shows the policies applied in this Security Target.

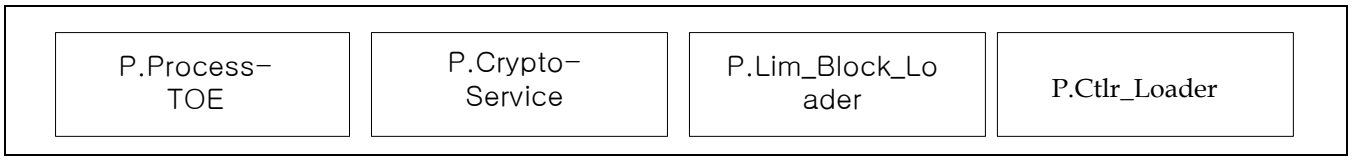


Figure 6 Policies

74 The IC Developer / Manufacturer must apply the policy "Identification during TOE Development and Production (P.Process-TOE)" as specified below.

P.Process-TOE Identification during TOE Development and Production

An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

75 The accurate identification is introduced at the end of the production test in phase 3. Therefore the production environment must support this unique identification.

76 The information and material produced and/or processed by the TOE Manufacturer in the TOE development and production environment (Phases 2 up to TOE Delivery) can be grouped as follows:

- logical design data,
- physical design data,
- IC Dedicated Software, Security IC Embedded Software, Initialisation Data and Pre-personalisation Data,
- specific development aids,
- test and characterisation related data,
- material for software development support, and
- photomasks and products in any form

as long as they are generated, stored, or processed by the TOE Manufacturer.

77 The TOE provides specific cryptographic services which can be used by the Smartcard Embedded Software. In the following specific cryptographic services are listed which is not derived from threats identified for the TOE's environment because it can only be decided in the context of the smartcard applications, against which threats the Smartcard Embedded Software will use the specific cryptographic service.

The IC Developer / Manufacturer must apply the policy "Cryptographic Service (P.Crypto-Service)" as specified below.

P.Crypto-Service Cryptographic Services provided by the TOE

The TOE shall provide the following cryptographic services to the IC Embedded Software:

- Triple Data Encryption Standard (TDES)
- Advanced Encryption Standard (AES)

- Module-Lattice Digital Signature Standard (ML-DSA) (optional)

The IC Developer / Manufacturer must apply the organisational security policy "Limiting and Blocking the Loader Functionality (P.Lim_Block_Loader)" applies to Loader dedicated for usage in secured environment specified below.

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.

The organizational security policy "Controlled usage to Loader Functionality (P.Ctlr_Loader)" applies to Loader dedicated for usage by authorized users only.

P.Ctlr_Loader Controlled usage to Loader Functionality

Authorized user controls the usage of the Loader functionality in order to protect stored and loaded user data from disclosure and manipulation.

3.4 Assumptions

The following assumptions are applicable for this Security Target:

Assumption	Description	Origin
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation	BSI-PP-0084
A.Resp-Appl	Treatment of user data of the Composite TOE	BSI-PP-0084
A.Key-Function	Usage of Key-dependent Functions	Additional assumption defined in the Security Target

Table 7 Assumptions

78 The following Figure 7 shows the assumptions applied in this Security Target.

Figure 7 Assumptions

79 The intended usage of the TOE is twofold, depending on the Life Cycle Phase: (i) The Security IC Embedded Software developer use it as a platform for the Security IC software being developed. The Composite Product Manufacturer (and the consumer) uses it as a part of the Security IC. The Composite Product is used in a terminal which supplies the Security IC (with power and clock) and (at least) mediates the communication with the Security IC Embedded Software.

80 Before being delivered to the consumer the TOE is packaged. Many attacks require the TOE to be removed from the carrier. Though this extra step adds difficulties for the attacker no specific assumptions are made here regarding the package.

81 Appropriate "Protection during Packaging, Finishing and Personalisation (A.Process-Sec-IC)" must be ensured after TOE Delivery up to the end of Phase 6, as well as during the delivery to Phase 7 as specified below.

A.Process-Sec-IC Protection during Packaging, Finishing and Personalisation

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

This means that the Phases after TOE Delivery are assumed to be protected appropriately.

82 The information and material produced and/or processed by the Security IC Embedded Software Developer in Phase 1 and by the Composite Product Manufacturer can be grouped as follows:

- the Security IC Embedded Software including specifications, implementation and related documentation,
- Pre-personalisation Data and Personalisation Data including specifications of formats and memory areas, test related data,
- the user data of the Composite TOE and related documentation, and
- material for software development support

83 as long as they are not under the control of the TOE Manufacturer. Details must be defined in the Protection Profile or Security Target for the evaluation of the Security IC Embedded Software and/or Security IC.

84 The developer of the Security IC Embedded Software must ensure the appropriate usage of Security IC while developing this software in Phase 1 as described in the (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.

85 Note that particular requirements for the Security IC Embedded Software are often not clear before considering a specific attack scenario during vulnerability analysis of the Security IC (AVA_VAN). A summary of such results is provided in the document "ETR for composite evaluation" (ETR-COMP). This document will be provided for the evaluation of the composite product. The ETR-COMP may also include guidance for additional tests being required for the combination of hardware and software. The TOE evaluation must be completed before evaluation of the Security IC Embedded Software can be completed. The TOE evaluation can be conducted before and independently from the evaluation of the Security IC Embedded Software.

86 The Security IC Embedded Software must ensure the appropriate “Treatment of user data of the Composite TOE (A.Resp-Appl)” as specified below.

A.Resp-Appl	Treatment of user data of the Composite TOE All user data of the Composite TOE are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant user data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.

87 The application context specifies how the user data of the Composite TOE shall be handled and protected. The evaluation of the Security IC according to this Security Target is conducted on generalized application context. The concrete requirements for the Security IC Embedded Software shall be defined in the Protection Profile respective Security Target for the Security IC Embedded Software. The Security IC cannot prevent any compromise or modification of user data of the Composite TOE by malicious Security IC Embedded Software.

88 The developer of the Smartcard Embedded Software must ensure the appropriate “Usage of Key-dependent Functions (A.Key-Function)” while developing this software in Phase 1 as specified below.

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).

89 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

90 This chapter Security Objectives contains the following sections:

4.1 *Security Objectives for the TOE*

4.2 *Security Objectives for the Security IC* Embedded Software

4.3 *Security Objectives for the* operational Environment

4.4 *Security Objectives Rationale*

4.1 Security Objectives for the TOE

The Security Objectives for the TOE are summarized in the following table:

Objective	Description	Origin
O.Leak-Inherent	O.Leak-Inherent	BSI-PP-0084 - Standard Security Objective
O.Phys-Probing	Protection against Physical Probing	BSI-PP-0084 - Standard Security Objective
O.Malfunction	Protection against Malfunctions	BSI-PP-0084 - Standard Security Objective
O.Phys-Manipulation	Protection against Physical Manipulation	BSI-PP-0084 - Standard Security Objective
O.Leak-Forced	Protection against Forced Information Leakage	BSI-PP-0084 - Standard Security Objective
O.Abuse-Func	Protection against Abuse of Functionality	BSI-PP-0084 - Standard Security Objective
O.Identification	TOE Identification	BSI-PP-0084 - Standard Security Objective
O.RND	Random Numbers	BSI-PP-0084 - Security Objective related to Specific Functionality
O.Mem-Access	Area based Memory Access Control	Security Objective defined by the ST
O.Cap_Avail_Loader	Capability and availability of the Loader	BSI-PP-0084 - Package 1 for loader
O.Ctrl_Auth_Loader	Access control and authenticity for the Loader	BSI-PP-0084 – Package 2 for loader
O.TDES	Cryptographic service Triple-DES	BSI-PP-0084 - Package "TDES"
O.AES	Cryptographic service AES	BSI-PP-0084 - Package "AES"
O.ML-DSA	Cryptographic service ML-DSA	Security Objective defined by the ST
O. Authentication	Authentication to external entities	BSI-PP-0084 – Package "Authentication of the Security IC"
O.Prot_TSF_Confidentiality	Protection of the confidentiality of the TSF	Security Objective defined by the ST (PP0084 – Interpretations [21])

Table 8 Security Objectives for the TOE

91 The user have the following standard high-level security goals related to the assets:

SG1 maintain the integrity user data (when being executed/processed and when being stored in the TOE's memories) as well as

SG2 maintain the confidentiality of user data (when being processed and when being stored in the TOE's protected memories).

SG3 maintain the correct operation of the security services provided by the TOE for the Security IC Embedded Software.

92 Note, the Security IC may not distinguish between user data which are public known or kept confidential. Therefore the security IC shall protect the user data in integrity and in confidentiality if stored in protected memory areas, unless the Security IC Embedded Software chooses to disclose or modify it. Parts of the Security IC Embedded Software which do not contain secret data or security critical source code, may not require protection from being disclosed. Other parts of the Security IC Embedded Software may need kept confidential since specific implementation details may assist an attacker.

93 These standard high-level security goals in the context of the security problem definition build the starting point for the definition of security objectives as required by the Common Criteria (refer to Figure 8). Note that the integrity of the TOE is a means to reach these objectives.

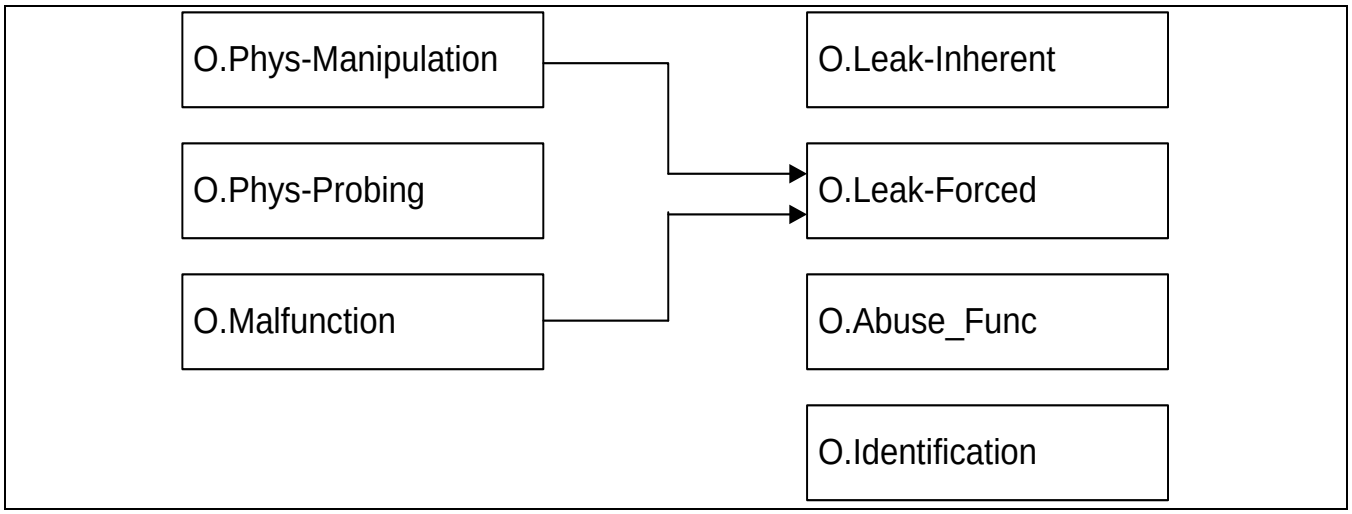


Figure 8 Standard Security Objectives

94 According to the Protection Profile there is the following high-level security goal related to specific functionality:

95 SG4 provide random numbers.

96 The additional high-level security considerations are refined below by defining security objectives as required by the Common Criteria (refer to Figure 9).

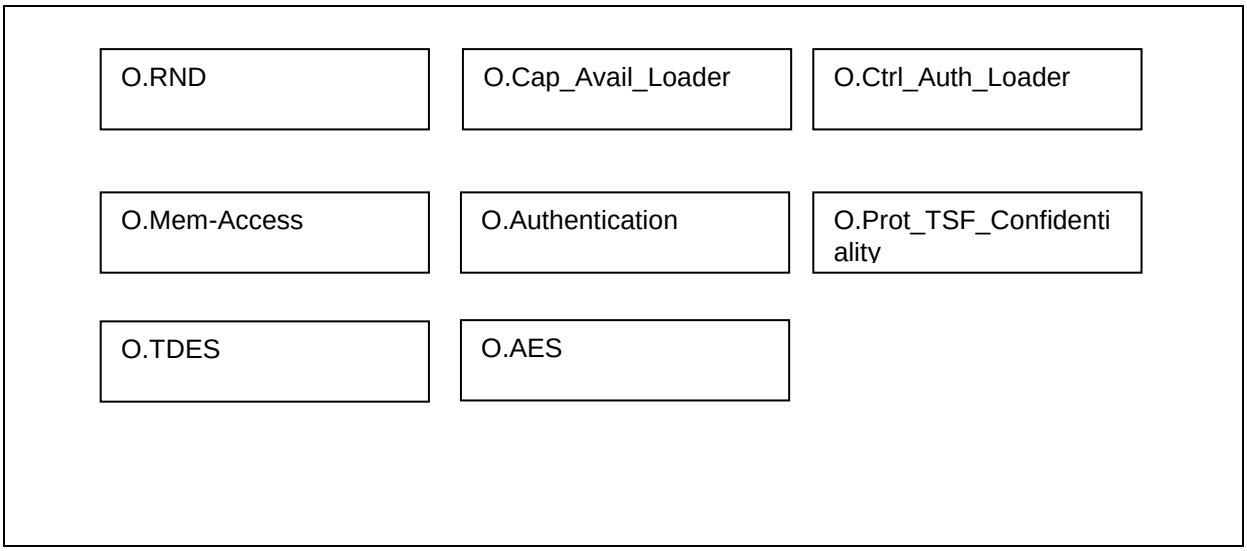


Figure 9 Security Objectives related to Specific Functionality

4.1.1 Standard Security Objectives

97 The TOE shall provide "Protection against Inherent Information Leakage (O.Leak-Inherent)" as specified below.

O.Leak-Inherent Protection against Inherent Information Leakage

The TOE must provide protection against disclosure of confidential data (User Data or TSF data) stored and/or processed in the Smartcard IC

- by measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and
- by measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or I/O lines).

This objective pertains to measurements with subsequent complex signal processing whereas O.Phys-Probing is about direct measurements on elements on the chip surface. Details correspond to an analysis of attack scenarios which is not given here.

98 The TOE shall provide "Protection against Physical Probing (O.Phys-Probing)" as specified below.

O.Phys-Probing Protection against Physical Probing

The TOE must provide protection against disclosure/reconstruction of user data while stored in protected memory areas and processed or against the disclosure of other critical information about the operation of the TOE.

This includes protection against

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)

with a prior reverse-engineering to understand the design and its properties and functions.

The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

99 The TOE shall provide "Protection against Malfunctions (O.Malfunction)" as specified below.

O.Malfunction Protection against Malfunctions

The TOE must ensure its correct operation.

The TOE must indicate or prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent malfunctions. Examples of environmental conditions are voltage, clock frequency, temperature, or external energy fields.

Remark: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective O.Phys-Manipulation) provided that detailed knowledge about the TOE´s internal construction is required and the attack is performed in a controlled manner.

100 The TOE shall provide "Protection against Physical Manipulation (O.Phys-Manipulation)" as specified below.

O.Phys-Manipulation Protection against Physical Manipulation

The TOE must provide protection against manipulation of the TOE (including its software and TSF data), the Smartcard Embedded Software and the user data of the Composite TOE. This includes protection against

- reverse-engineering (understanding the design and its properties and functions),
- manipulation of the hardware and any data, as well as
- undetected manipulation of memory contents.

The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

101 The TOE shall provide "Protection against Forced Information Leakage (O.Leak-Forced)" as specified

below:

O.Leak-Forced Protection against Forced Information Leakage

The Security IC must be protected against disclosure of confidential data processed in the Security IC (using methods as described under O.Leak-Inherent) even if the information leakage is not inherent but caused by the attacker

- by forcing a malfunction (refer to "Protection against Malfunction due to Environmental Stress (O.Malfunction)" and/or
- by a physical manipulation (refer to "Protection against Physical Manipulation (O.Phys-Manipulation)".

If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.

102 The TOE shall provide "Protection against Abuse of Functionality (O.Abuse-Func)" as specified below.

O.Abuse-Func Protection against Abuse of Functionality

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical user data of the Composite TOE, (ii) manipulate critical user data of the Composite TOE, (iii) manipulate Security IC Embedded Software or (iv) bypass, deactivate, change or explore security features or security services of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

103 The TOE shall provide "TOE Identification (O.Identification)" as specified below:

O.Identification TOE Identification

The TOE must provide means to store Initialisation Data and Pre-personalisation Data in its non-volatile memory. The Initialisation Data (or parts of them) are used for TOE identification.

4.1.2 Security Objectives related to Specific Functionality (referring to SG4)

104 The TOE shall provide "Random Numbers (O.RND)" as specified below.

O.RND Random Numbers

The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have sufficient entropy.

The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.

4.1.3 Security Objectives for Added Function

105 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.

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

O.Cap_Avail_Loader Capability and availability of the 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.

107 The TOE shall provide "Access control and authenticity for the Loader (O.Ctrl_Auth_Loader)" as specified below.

O.Ctrl_Auth_Loader Access control and authenticity for the Loader

The TSF provides trusted communication channel with authorized user, supports confidentiality protection and authentication of the user data to be loaded and access control for usage of the Loader functionality.

108 The TOE shall provide "Cryptographic service Triple-DES (O.TDES)" as specified below.

O.TDES Cryptographic service Triple-DES

The TOE provides secure hardware based cryptographic services implementing the Triple-DES for encryption and decryption.

109 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 for the AES for encryption and decryption.

110 The Security IC Embedded Software shall provide "Authentication to external entities (O.Authentication)" as specified below.

O. Authentication	Authentication to external entities
	The TOE shall be able to authenticate itself to external entities. The Initialisation Data (or parts of them) are used for TOE authentication verification data.

111 The TOE shall provide "Protection of the confidentiality of the TSF (O.Prot_TSF_Confidentiality)" as specified below.

O.Prot_TSF_Confidentiality	Protection of the confidentiality of the TSF
	The TOE must provide protection against disclosure of confidential operations of the Security IC (loader, memory management unit, …) through the use of a dedicated code loaded on open samples.

4.2 Security Objectives for the Security IC Embedded Software

The Security Objectives for the Security IC Embedded Software and for the operational environment are summarized in the following table:

Objective	Description	Origin
OE.Resp-Appl	Treatment of user data of the Composite TOE	BSI-PP-0084
OE.Process-Sec-IC	Protection during composite product manufacturing	BSI-PP-0084
OE.Lim_Block_Loader	Limitation of capability and blocking the Loader	BSI-PP-0084 - Package 1 for loader
OE.Loader_Usage	Secure communication and usage of the Loader	BSI-PP-0084 – Package 2 for loader
OE.TOE_Auth	External entities authenticating of the TOE	BSI-PP-0084 – Package "Authentication of the Security IC"

Table 9 Security Objectives for the Security IC Embedded Software and the operational environment

112 The development of the Security IC Embedded Software is outside the development and manufacturing of the TOE. The Security IC Embedded Software defines the operational use of the TOE. This section describes the security objective for the Security IC Embedded Software.

Note, in order to ensure that the TOE is used in a secure manner the Security IC Embedded Software shall be designed so that the requirements from the following documents are met: (i) hardware data sheet for the TOE, (ii) data sheet of the IC Dedicated Software of the TOE, (iii) TOE application notes, other guidance documents, and (iv) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as referenced in the certification report.

113 The Security IC Embedded Software shall provide "Treatment of user data of the Composite TOE (OE.Resp-Appl)" as specified below.

OE.Resp-Appl Treatment of user data of the Composite TOE

Security relevant user data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context.

For example the Security IC Embedded Software will not disclose security relevant user data of the Composite TOE to unauthorised users or processes when communicating with a terminal.

4.2.1 Clarification of "Treatment of User Data of the Composite TOE(OE.Resp-Appl)"

114 Regarding the cryptographic services this objective of the environment has to be clarified. 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.

115 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. 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 realised in the environment.

116 Regarding the area based access control this objective of the environment has to be clarified. The treatment of User Data of the Composite TOE is also required when a multi-application operating system is implemented as part of the Smartcard Embedded Software on the TOE. In this case the multi-application operating system should not disclose security relevant user data of one application to another application when it is processed or stored on the TOE.

4.3 Security Objectives for the Operational Environment

TOE Delivery up to the End of Phase 6

117 Appropriate "Protection during Packaging, Finishing and Personalisation (OE.Process-Sec-IC)" must be ensured after TOE Delivery up to the end of Phases 6, as well as during the delivery to Phase 7 as specified below.

OE.Process-Sec-IC	Protection during composite product manufacturing Security procedures shall be used after TOE Delivery up to delivery to the "end-consumer" to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that Phases after TOE Delivery up to the end of Phase 6 must be protected appropriately.

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 irreversibly the Loader after intended usage of the Loader and before the end of phase 5. Note: To maintain the confidentiality of the data of the composite TOE, the intended usage of the Loader is limited to the phase 5 of the life cycle.

The operational environment of the TOE shall provide "Secure communication and usage of the Loader (OE.Loader_Usage)" as specified below.

OE.Loader_Usage	Secure communication and usage of the Loader The authorized user must support the trusted communication channel with the TOE by confidentiality protection and authenticity proof of the data to be loaded and fulfilling the access conditions required by the Loader

The operational environment shall provide "External entities authenticating of the TOE (OE.TOE_Auth)".

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.

4.3.1 Clarification of "Protection during Composite Product Manufacturing (OE.Process-Sec-IC)"

118 The protection during packaging, finishing and personalization includes also the personalization process and the personalization data during Phase 4, Phase 5 and Phase 6.

119 Since OE.Process-Sec-IC requires the Composite Product Manufacturer to implement those measures assumed in A.Process-Sec-IC, the assumption is covered by this objective.

4.4 Security Objectives Rationale

120 The Table below gives an overview, how the assumptions, threats, and organisational security policies are addressed by the objectives. The text following after the table justifies this in detail.

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
A.Resp-Appl	OE.Resp-Appl	Phase 1
P.Process-TOE	O.Identification	Phase 2 – 3 optional Phase 4
A.Process-Sec-IC	OE.Process-Sec-IC	Phase 5 – 6 optional Phase 4
T.Leak-Inherent	O.Leak-Inherent	
T.Phys-Probing	O.Phys-Probing	
T.Malfunction	O.Malfunction	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Forced	O.Leak-Forced	
T.Abuse-Func	O.Abuse-Func	
T.RND	O.RND	
T.Mem-Access	O.Mem-Access	
P.Crypto-Service	O.TDES O.AES O.ML-DSA	
A.Key-Function	OE.Resp-Appl	
P.Lim_Block_Loader	O.Cap_Avail_Loader OE.Lim_Block_Loader	Phase 5
P.Ctlr_Loader	O.Ctrl_Auth_Loader OE.Loader_Usage	Phase 5
T.Masquerade_TOE	O.Authentication OE.TOE_Auth	
T.Open_Samples_Diffusion	O.Prot_TSF_Confidentiality O.Leak-Inherent O.Leak-Forced	Phase 4, 5

Table 10 Security Objectives versus Assumptions, Threats or Policies

121 The justification related to the assumption “Treatment of user data of the Composite TOE (A.Resp-Appl)” is as follows:

122 Since OE.Resp-Appl requires the Security IC Embedded Software to implement measures as assumed in A.Resp-Appl, the assumption is covered by the objective.

123 The justification related to the organisational security policy “Protection during TOE Development and

Production (P.Process-TOE)" is as follows:

124 O.Identification requires that the TOE has to support the possibility of a unique identification. The unique identification can be stored on the TOE. Since the unique identification is generated by the production environment the production environment must support the integrity of the generated unique identification. The technical and organisational security measures that ensure the security of the development environment and production environment are evaluated based on the assurance measures that are part of the evaluation. For a list of material produced and processed by the TOE Manufacturer refer to paragraph 44. All listed items and the associated development and production environments are subject of the evaluation. Therefore, the organisational security policy P.Process-TOE is covered by this objective, as far as organisational measures are concerned.

125 The justification related to the assumption "Protection during Packaging, Finishing and Personalisation (A.Process-Sec-IC)" is as follows:

126 Since OE.Process-Sec-IC requires the Composite Product Manufacturer to implement those measures assumed in A.Process-Sec-IC, the assumption is covered by this objective.

127 The justification related to the threats "Inherent Information Leakage (T.Leak-Inherent)", "Physical Probing (T.Phys-Probing)", "Malfunction due to Environmental Stress (T.Malfunction)", "Physical Manipulation (T.Phys-Manipulation)", "Forced Information Leakage (T.Leak-Forced)", "Abuse of Functionality (T.Abuse-Func)" and "Deficiency of Random Numbers (T.RND)" is as follows:

128 For all threats the corresponding objectives are stated in a way, which directly corresponds to the description of the threat. It is clear from the description of each objective, that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds.

129 The justification related to the threat "Memory Access Violation (T.Mem-Access)" is as follows:

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

131 The clarification of O.Mem-Access makes clear that it is up to the Smartcard Embedded Software to implement the memory management scheme by appropriately administrating the TSF. 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 of the Composite TOE(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. .

132 Compared to Smartcard IC Platform Protection Profile a clarification has been made for the security objective "Treatment of User Data of the Composite TOE(OE.Resp-Appl)": By definition cipher or plain text data and cryptographic keys are User Data. So, 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 realised in the environment. That is expressed by the assumption A.Key—Function which is covered from OE.Resp–Appl. These measures make sure that the assumption A.Resp-Appl is still covered by the security objective OE.Resp-Appl.

133 The organisational security policy Limitation of capability and blocking the Loader (P.Lim_Block_Loader)

is directly implemented by the security objective for the TOE "Capability and availability of the Loader (O.Cap_Avail_Loader)" and the security objective for the TOE environment "Limitation of capability and blocking the Loader (OE.Lim_Block_Loader)". The TOE security objective "Capability and availability of the Loader" (O.Cap_Avail_Loader)" mitigates 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.

134 The organisational security policy "Controlled usage to Loader Functionality (P.Ctlr_Loader) is directly implemented by the security objective for the TOE "Access control and authenticity for the Loader (O.Ctrl_Auth_Loader)" and the security objective for the TOE environment "Secure communication and usage of the Loader (OE.Loader_Usage)".

135 The threat "Masquerade the TOE (T.Masquerade_TOE)" is directly covered by the TOE security objective "Authentication to external entities (O.Authentication)" describing the proving part of the authentication and the security objective for the operational environment of the TOE "External entities authenticating of the TOE (OE.TOE_Auth)" the verifying part of the authentication.

136 The justification related to the security objectives O.TDES, O.ML-DSA and O.AES are followings: Since these objectives require the TOE to implement the same specific security functionality as required by P.Crypto-Service, the organization security policy is covered by the objective.

137 The threat "Diffusion of open samples" (T.Open_Samples_Diffusion) is directly covered by the TOE security objective "Protection of the confidentiality of the TSF" (O.Prot_TSF_Confidentiality) based on the self-protection of the TOE and the authentication mechanism of the Loader. Additionally to O.Prot_TSF_Confidentiality (Protection of the confidentiality of the TSF), T.Open_Samples_Diffusion threat is countered by O.Leak-Inherent (Protection against Inherent Information Leakage) and O.Leak-Forced (Protection against Forced Information Leakage) from the PP.

5 EXTENDED COMPONENTS DEFINITION

138 This chapter 5 Extended Components Definition contains the following sections:

5.1 Definition of the Family FAU_SAS

5.1 Definition of the Family FAU_SAS

139 To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

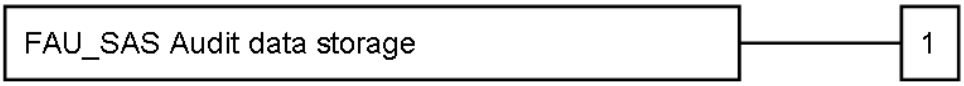
140 The family "Audit data storage (FAU_SAS)" is specified as follows.

FAU_SAS Audit data storage

Family behaviour

This family defines functional requirements for the storage of audit data.

Component levelling



FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide [assignment: *list of subjects*] with the capability to store [assignment: *list of audit information*] in the [assignment: *type of persistent memory*].

Dependencies: No dependencies.

6 IT security requirements

141 This chapter 6 IT Security Requirements contains the following sections:

6.1 Security Functional Requirements for the TOE

6.2 Security Assurance Requirements for the TOE

6.3 Security Requirements Rationale

6.1 Security Functional Requirements for the TOE

142 In order to define the Security Functional Requirements the Part 2 of the Common Criteria was used. However, some Security Functional Requirements have been refined. The refinements are described below the associated SFR. The operations completed in the ST are marked in italic font.

6.1.1 Malfunctions

143 The TOE shall meet the requirement "Limited fault tolerance (FRU_FLT.2)" as specified below.

FRU_FLT.2	Limited fault tolerance
Hierarchical to:	FRU_FLT.1 Degraded fault tolerance
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 Failure with preservation of secure state
Refinement:	The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.
Application Note 13:	Environmental conditions include but are not limited to power supply, clock, and other external signals (e.g. reset signal) necessary for the TOE operation.

144 The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below.

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 also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.
Application note:	The secure state is maintained by TOE's detectors. The TOE's detectors are monitoring the failure occurs. The failures are abnormal frequency, abnormal voltage, abnormal temperature, and power glitch detectors that detect out of the specified range (refer to table 14). If the failures are happen, the TOE goes into RESET state. This satisfies the FPT_FLS.1 "Failure with preservation of secure state."

6.1.2 Abuse of Functionality

145 The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below.

FMT_LIM.1	Limited capabilities
Hierarchical to:	No other components.
FMT_LIM.1.1	The TSF shall limits 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 Limited availability.

146 The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below.

FMT_LIM.2	Limited availability
Hierarchical to:	No other components.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their 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 Limited capabilities.

147 The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 extended).

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 *the Initialisation Data and/or Prepersonalisation Data and/or supplements of the Smartcard Embedded Software* in the *Test ROM area*.
Dependencies:	No dependencies.
Application Note:	The integrity and uniqueness of the unique identification of the TOE must be supported by the development, production and test environment.

6.1.3 Physical Manipulation and Probing

148 The TOE shall meet the requirement "Stored data confidentiality (FDP_SDC.1)" as specified below.

FDP_SDC.1	Stored data confidentiality
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SDC.1.1	The TSF shall ensure the confidentiality of *all user data* while it is stored in the *FLASH, RAM or ROM.*

149 The TOE shall meet the requirement "Stored data integrity monitoring and action (FDP_SDI.2)" as specified below.

FDP_SDI.2	Stored data integrity monitoring and action
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for *ECC error or Parity error* on all objects, based on the following attributes*: FLASH, RAM or ROM read operation*.
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall *enforce a device RESET or an interrupt (IRQ).*
Application Note:	This requirement is achieved by security features such as memory encryption, bus scrambling, security detectors and memory access control.

150 The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below.

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.
Dependencies:	No dependencies.
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.
Application Note:	This requirement is achieved by security feature as the Active shield must be removed and bypassed in order to perform physical intrusive attacks. The TOE makes a reset or IRQ occurs to stops operation if a physical manipulation or

physical probing attack is detected. And also Static Address/Data scrambling for bus and memory & Synthesizable processor core make the reverse-engineering of the TOE layout unpractical. So these functionalities meet the security functional requirement of FPT_PHP.3: Resistance to physical attack.

6.1.4 Leakage

151 The TOE shall meet the requirement "Basic internal transfer protection (FDP_ITT.1)" as specified below.

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 Subset access control, or FDP_IFC.1 Subset information flow control]
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.

152 The TOE shall meet the requirement "Basic internal TSF data transfer protection (FPT_ITT.1)" as specified below.

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 separated parts of the TOE.

This requirement is equivalent to FDP_ITT.1 above but refers to TSF data instead of user data. Therefore, it should be understood as to refer to the same *Data Processing Policy* defined under FDP_IFC.1 below.

153 The TOE shall meet the requirement "Subset information flow control (FDP_IFC.1)"as specified below:

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 Simple security attributes

154 The following Security Function Policy (SFP) Data Processing Policy is defined for the requirement " Subset information flow control (FDP_IFC.1)":

User data of the Composite TOE and TSF data shall not be accessible from the TOE except when the

Security IC Embedded Software decides to communicate the user data of the Composite TOE via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security IC Embedded Software.

6.1.5 Random Numbers (DTRNG FRO M)

155 The TOE shall meet the requirement "Quality metric for random numbers (FCS_RNG.1)" as specified below.

FCS_RNG.1/PTG.2 Random number generation - PTG.2

Hierarchical to: No other components.

FCS_RNG.1.1/PTG.2 The TSF shall provide a *physical* true random number generator that implements:

(PTG.2.1) *A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.*

(PTG.2.2) *If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source*

(PTG.2.3) *The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.*

(PTG.2.4) *The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.*

(PTG.2.5) *The online test procedure checks the quality of the raw random number sequence. It is triggered, externally applied upon specified internal events (i.e., crypto key generation). The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time*

FCS_RNG.1.2/PTG.2 The TSF shall provide *numbers, 16-bit per number* that meet:

(PTG.2.6) *Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.*

(PTG.2.7) *The average Shannon entropy per internal random bit exceeds 0.997.*

Application Note: The DTRNG FRO M library comprises some functions that perform statistical tests on the DTRNG FRO M output in order to execute so-called total-failure test and online test. The online test function triggers a set of statistical tests embedded in a logic block connecting to DTRNG FRO M hardware directly, Upon completing the statistical tests, the logic block shall notify embedded software of the test result. The total-failure test is implemented in pure software. If either test fails, the function returns an error value and the DTRNG FRO M is shut down. Those functions are described in DTRNG FRO M Application note in detail and are available to embedded software.

Dependencies: No dependencies

FCS_RNG.1/RGS-IC Random number generation – RGS-IC

Hierarchical to: No other components.

FCS_RNG.1.1/RGS-IC The TSF shall provide a *physical* random number generator that implements:

- the rules RègleArchiGVA-1 and the recommendation RecomArchiGVA-1 of [16] ;

- total failure tests and online tests.

FCS_RNG.1.2/RGS-IC The TSF shall provide *random numbers* that meet *the rule RègleArchiGVA-2 of [16].*

Dependencies: No dependencies.

Warning: The TSF fulfils some but not all the necessary rules to comply with [16] regarding random numbers generators (RNG). The composite product's RNG will comply with [16] only when all the rules of §2.4 "Génération d'aléa cryptographique" of [16] are addressed. In particular, a cryptographic post-processing must be implemented by the composite developer.

6.1.6 Memory Access Control

156 Usage of multiple applications in one Smartcard often requires separating code and data in order to prevent that one application can access code and/or data of another application. To support the TOE provides Area based Memory Access Control.

157 The security service being provided is described in the Security Function Policy (SFP) Memory Access Control Policy. The security functional requirement “Subset access control (FDP_ACC.1)” requires that this policy is in place and defines the scope were it applies. The security functional requirement “Security attribute based access control (FDP_ACF.1)” defines addresses security attribute usage and characteristics of policies. It describes the rules for the function that implements the Security Function Policy (SFP) as identified in FDP_ACC.1. The decision whether an access is permitted or not is taken based upon attributes allocated to the software. The user software defines the attributes and memory areas. The corresponding permission control information is evaluated “on-the-fly” by the hardware so that access is granted/effective or denied/inoperable.

158 The security functional requirement “Static attribute initialization (FMT_MSA.3)” ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. Alternative values can be specified by any subject provided that the Memory Access Control Policy allows that. This is described by the security functional requirement “Management of security attributes (FMT_MSA.1)”. The attributes are determined during TOE manufacturing (FMT_MSA.3) or set at run-time (FMT_MSA.1).

159 From TOE´s point of view the different roles in the user software can be distinguished according to the memory based access control. However the definition of the roles belongs to the user software.

160 The following Security Function Policy (SFP) Memory Access Control Policy is defined for the requirement

"Security attribute based access control (FDP_ACF.1)":

Memory Access Control Policy

The TOE shall control read, write, delete, and execute accesses of software running at between two different modes (privilege and user mode) on data including code stored in memory areas.

The TOE shall restrict the ability to define, to change or at least to finally accept the applied rules (as mentioned in FDP_ACF.1) to software with privilege mode).

161 The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below.

FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the *Memory Access Control Policy* on *all subjects (software with privilege mode and user mode), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy.* *Subjects are software codes in Privilege and User mode.* *Objects are data stored in ROM, RAM and FLASH memories.*
Dependencies:	FDP_ACF.1 Security attribute based access control

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below.

FDP_ACF.1	Security attribute based access control The attributes are all the operations related to the data stored in memories, which are *the read, write* and *execute* operations.
Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the *Memory Access Control Policy* to objects based on the following: *memory area where the software is executed from and/or the memory area where the read is performed to and/or the memory area where the write is performed to and/or the operation to be performed*.
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *evaluate the corresponding permission control information before the access so that accesses to be denied cannot be utilised by the subject attempting to perform the operation*.
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules*: none*.

Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

The TOE shall meet the requirement "Static attribute initialisation (FMT_MSA.3)" as specified below.

FMT_MSA.3	Static attribute initialisation
Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the *Memory Access Control Policy* to provide *well defined* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow 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 Management of security attributes FMT_SMR.1 Security roles

162 The TOE shall meet the requirement "Management of security attributes (FMT_MSA.1)" as specified below:

FMT_MSA.1	Management of security attributes
Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the *Memory Access Control Policy* to restrict the ability to *change default, modify or delete* the security attributes *permission control information* to *running at privilege mode.*
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

163 The TOE shall meet the requirement "Specification of management functions (FMT_SMF.1)" as specified below:

FMT_SMF.1	Specification of management functions
Hierarchical to:	No other components
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: *access the control registers of the MPU*.
Dependencies:	No dependencies

6.1.7 Cryptographic Support

164 FCS_COP.1 Cryptographic operation requires, a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

165 The following additional specific security functionality is implemented in the TOE:

- Triple Data Encryption Standard (TDES) with 112bit or 168bit key size

- Advanced Encryption Standard (AES) with 128 bit, 192bit and 256bit key size

6.1.8 Triple-DES Operation

166 The Triple DES (TDES) operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/TDES	Cryptographic operation – TDES
Hierarchical to:	No other components.
FCS_COP.1.1/TDES	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *TDES in ECB mode* and cryptographic key sizes *112 bit, 168 bit* that meet the following: *[NIST SP 800-67] chapter 2 and 3, [NIST SP 800-38A].*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
Application Note:	The TOE implements TDES with key option 1 and 2 with ECB mode.

167 The TOE shall meet the requirement "Timing and event of cryptographic key destruction – TDES (FCS_CKM.6/TDES)" as specified below.

FCS_CKM.6/TDES	Timing and event of cryptographic key destruction - TDES
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6.1/TDES	The TSF shall destroy *cryptographic keys* when *no longer needed.*
FCS_CKM.6.2/TDES	The TSF shall destroy *cryptographic keys* and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method *overwriting* that meets the following: *none.*
Application Note	The cryptographic key destruction can be done by overwriting the internal stored key when a new key value is provided through the key interface or by TOE reset, which provides randomization of the internal stored key.

6.1.9 AES Operation

168 The AES operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/AES	Cryptographic operation – AES
Hierarchical to:	No other components.
FCS_COP.1.1/AES	The TSF shall perform *decryption and encryption* in accordance with a specified cryptographic algorithm *AES in ECB mode* and cryptographic key sizes *128 bit, 192 bit, 256 bit* that meet the following: *[FIPS197] chapter 5, [NIST SP 800-38A].*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation], or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction

169 The TOE shall meet the requirement "Timing and event of cryptographic key destruction – AES (FCS_CKM.6/AES)" as specified below.

FCS_CKM.6/AES	Timing and event of cryptographic key destruction - AES
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6.1/AES	The TSF shall destroy *cryptographic keys* when *no longer needed.*
FCS_CKM.6.2/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 *overwriting* that meets the following: *none.*
Application Note	The cryptographic key destruction can be done by overwriting the internal stored key when a new key value is provided through the key interface or by TOE reset, which provides randomization of the internal stored key.

6.1.10 ML-DSA Operations

170 The ACT1 Secure ML-DSA library of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/ML-DSA	Cryptographic operation – ML-DSA

Hierarchical to:	No other components.
FCS_COP.1.1/ML-DSA	The TSF shall perform *Lattice Operations of ML-DSA signature generation and verification* in accordance with a specified cryptographic algorithm *ML-DSA (ML-DSS: standard ML-DSA)* and cryptographic key sizes *corresponding to* ML-DSA-44, ML-DSA-65 that meet the following: *[FIPS 204] section 4 (parameters), section 3 (ML-DSA Signature Scheme).*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction

171 The ACT1 Secure ML-DSA library shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below.

FCS_CKM.1/ML-DSA	Cryptographic key generation – ML-DSA
Hierarchical to:	No other components.
FCS_CKM.1.1/ML-DSA	The TSF shall generate cryptographic keys in accordance with the specified cryptographic key generation algorithm *ML-DSA* and with the specified cryptographic key sizes *corresponding to ML-DSA-44, ML-DSA-65* that meet the following: *[FIPS 204] section 4 (parameters)*
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction

172 The TOE shall meet the requirement "Timing and event of cryptographic key destruction – ML-DSA (FCS_CKM.6/ML-DSA)" as specified below.

FCS_CKM.6/ML-DSA	Timing and event of cryptographic key destruction – ML-DSA
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6.1/ML-DSA	The TSF shall destroy *cryptographic keys* when *no longer needed.*

FCS_CKM.6.2/ML-DSA	The TSF shall destroy *cryptographic keys* and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method *overwriting or zeroing* that meets the following: *none*.
Application Note	The key destruction FCS_CKM.6/ML-DSA applies only for the keys stored by the ACT1 Secure ML-DSA library in crypto RAM and/or RAM. This internal key storage can be cleared by hardware resetting.

6.1.11 Reserved

6.1.12 Reserved

6.1.13 Bootloader

The TOE Functional Requirement "Limited capabilities – Loader(FMT_LIM.1/Loader)" is specified as follows.

FMT_LIM.1/Loader	Limited capabilities
Hierarchical to:	No other components.
FMT_LIM.1.1/Loader	The TSF shall limit its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced*: Deploying Loader functionality after locking the chip to FLASH booting mode does not allow stored user data to be disclosed or manipulated by unauthorized user.*
Dependencies:	FMT_LIM.2 Limited availability.

The TOE Functional Requirement "Limited availability – Loader (FMT_LIM.2/Loader)" is specified as follows.

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 capabilities (FMT_LIM.1)" the following policy is enforced: *The TSF prevents deploying the Loader functionality after locking the chip to FLASH booting mode*.
Dependencies:	FMT_LIM.1 Limited capabilities.

The TOE Functional Requirement "Inter-TSF trusted channel (FTP_ITC.1)" is specified as follows.

FTP_ITC.1	Inter-TSF trusted channel
Hierarchical to:	No other components.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and *the authorized user for using the Bootloader* that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit *another trusted IT product* to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for *deploying Loader mutual Authentication and establishment of session keys*.
Dependencies:	No dependencies.

The TOE Functional Requirement "Basic data exchange confidentiality (FDP_UCT.1)" is specified as follows.

FDP_UCT.1	Basic data exchange confidentiality
Hierarchical to:	No other components.
FDP_UCT.1.1	The TSF shall enforce the *Loader SFP* to *receive* user data in a manner protected from unauthorised disclosure.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

The TOE Functional Requirement "Data exchange integrity (FDP_UIT.1)" is specified as follows.

FDP_UIT.1	Data exchange integrity
Hierarchical to:	No other components.
FDP_UIT.1.1	The TSF shall enforce the *Loader SFP* to *receive* user data in a manner protected from *modification, deletion, insertion* errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion* has occurred.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

The TOE Functional Requirement "Subset access control - Loader (FDP_ACC.1/Loader)" is specified as follows.

FDP_ACC.1/ Loader	Subset access control - Loader
Hierarchical to:	No other components.
FDP_ACC.1.1/ Loader	The TSF shall enforce the *Loader SFP* on *(1) Loader authorized users,* *(2) the objects user data in FLASH or ROM* *(3) the operation deployment of Loader*
Dependencies:	FDP_ACF.1 Security attribute based access control.

Application Note : The TOE enforces the Loader SFP by FTP_ITC.1, FDP_UCT.1 and FDP_UIT.1 and FDP_ACF.1 to describe additional access control rules.

The TOE Functional Requirement "Security attribute based access control - Loader (FDP_ACF.1/Loader)" is specified as follows.

FDP_ACF.1/ Loader	Security attribute based access control - Loader
Hierarchical to:	No other components.
FDP_ACF.1.1/ Loader	The TSF shall enforce the *Loader SFP* to *objects* based on the following: *(1) the subjects Loader authorized users with security attributes FLASH write.* *(2) the objects user data in FLASH with security attributes FLASH write.*
FDP_ACF.1.2/ Loader	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *Bootloader can do write operation in FLASH after a successful Authentication*.
FDP_ACF.1.3/ Loader	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *FLASH can be controlled based on security attributes, which can be limited by Bootloader APDU command*.
FDP_ACF.1.4/ Loader	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *Bootloader can't access the FLASH without successful Authentication*..
Dependencies:	FMT_MSA.3 Static attribute initialisation.
Application Note:	Bootloader is only allowed in ROM Booting mode. To access all Bootloader APDU command except public APDU command, the mutual authentication sequence must be passed. In Flash booting mode, all APDU commands cannot be accessed.

6.1.14 Authentication Proof of Identity

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as specified below.

FIA_API.1	Authentication Proof of Identity
Hierarchical to:	No other components
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a *mutual authentication of Bootloader* to prove the identity of the *TOE* to an external entity

6.1.15 Summary of Security Functional Requirements

Security Functional Requirement	Origin
FRU_FLT.2	BSI-PP-0084
FPT_FLS.1	BSI-PP-0084
FAU_SAS.1	BSI-PP-0084
FDP_SDC.1	BSI-PP-0084, updated in CC:2022
FDP_SDI.2	BSI-PP-0084
FMT_LIM.1	BSI-PP-0084, updated in CC:2022
FMT_LIM.2	BSI-PP-0084, updated in CC:2022
FPT_PHP.3	BSI-PP-0084
FDP_ITT.1	BSI-PP-0084
FPT_ITT.1	BSI-PP-0084
FDP_IFC.1	BSI-PP-0084
FIA_API.1	BSI-PP-0084, updated in CC:2022
FMT_LIM.1/Loader	BSI-PP-0084 - Package 1 for loader, updated in CC:2022
FMT_LIM.2/Loader	BSI-PP-0084 - Package 1 for loader, updated in CC:2022
FTP_ITC.1	BSI-PP-0084 - Package 2 for loader
FDP_UCT.1	BSI-PP-0084 - Package 2 for loader
FDP_UIT.1	BSI-PP-0084 - Package 2 for loader

FDP_ACC.1/Loader	BSI-PP-0084 - Package 2 for loader
FDP_ACF.1/Loader	BSI-PP-0084 - Package 2 for loader
FCS_RNG.1/RGS-IC	BSI-PP-0084
FCS_RNG.1/PTG.2	BSI-PP-0084
FCS_RNG.1/EHP	BSI-PP-0084
FDP_ACC.1	CC:2022
FDP_ACF.1	CC:2022
FMT_MSA.3	CC:2022
FMT_MSA.1	CC:2022
FMT_SMF.1	CC:2022
FCS_COP.1/TDES	BSI-PP-0084 – package "TDES", updated in CC:2022
FCS_COP.1/AES	BSI-PP-0084 – package "AES", updated in CC:2022
FCS_COP.1/ML-DSA (optional)	CC:2022
FCS_CKM.1/ML-DSA (optional)	CC:2022
FCS_CKM.6/TDES	BSI-PP-0084 – package "TDES" FCS_CKM.4 replaced by FCS_CKM.6 in CC:2022
FCS_CKM.6/AES	BSI-PP-0084 – package "AES" FCS_CKM.4 replaced by FCS_CKM.6 in CC:2022
FCS_CKM.6/ML-DSA	CC:2022, FCS_CKM.4 replaced by FCS_CKM.6

Table 11 Security Functional Requirements for the TOE

6.2 TOE Assurance Requirements

The Security Target will be evaluated according to

Security Target evaluation (Class ASE)

This Security Target is modularized as a multi-assurance ST with a global compliance (EAL5+) and four sub-TSFs (EAL6+) for the memory access control policy, the bootloader access control policy, the security detector policy (only the detector's reaction to security incidents) and the non-reversibility of the TEST mode policy.

The following table lists the global security assurance requirements for the TOE. These security functional requirements are either copied from the Protection Profile BSI-PP-0084 [9] without modifications, or augmented from there, or newly added in this Security Target as indicated in column four of the table. This partly addresses the Protection Profile BSI-PP-0084 [9] Application Note 22.

Class	Family	Title	Compared to PP
ADV: Development	ADV_ARC.1	Architectural design	As in PP
	ADV_FSP.5	Functional Specification	Augmented from PP to EAL6
	ADV_IMP.2	Implementation Representation	Augmented from PP to EAL6
	ADV_INT.3	TSF Internals	Added at EAL6 level
	ADV_TDS.5	TOE Design	Augmented from PP to EAL6
AGD: Guidance documents	AGD_OPE.1	Operational User Guidance	As in PP
	AGD_PRE.1	Preparative procedures	As in PP
ALC: Life-cycle support	ALC_CMC.5	CM Capabilities	Augmented from PP to EAL6
	ALC_CMS.5	CM Scope	Augmented from PP to EAL6
	ALC_DEL.1	Delivery	As in PP
	ALC_DVS.2	Development Security	As in PP
	ALC_LCD.1	Life Cycle Definition	As in PP
	ALC_TAT.3	Tools and Techniques	Augmented from PP to EAL6
ASE: Security Target	ASE_CCL.1	Conformance claims	As in PP

Class	Family	Title	Compared to PP
evaluation	ASE_ECD.1	Extended components definition	As in PP
	ASE_INT.1	ST introduction	As in PP
	ASE_OBJ.2	Security objectives	As in PP
	ASE_REQ.2	Derived security requirements	As in PP
	ASE_SPD.1	Security problem definition	As in PP
	ASE_TSS.2	TOE summary specification	Augmented from PP
ATE: Tests	ATE_COV.3	Coverage	Augmented from PP to EAL6
	ATE_DPT.3	Depth	Augmented from PP to EAL6
	ATE_FUN.2	Functional Tests	Augmented from PP to EAL6
	ATE_IND.2	Independent Testing	As in PP
AVA: Vulnerability assessment	AVA_VAN.5	Vulnerability Analysis	As in PP

Table 12 Global Security assurance requirements for the TOE

Note: According to section 2 “Conformance Claims“, the global claimed SAR is EAL5 with all augmentation towards EAL6 except for ADV_SPM.

6.3 Security Requirements Rationale

6.3.1 Rationale for the Security Functional Requirements

173 The Table below gives an overview, how the security functional requirements are combined to meet the security objectives. The detailed justification follows after the table.

Objective	TOE Security Functional and Assurance Requirements
O.Leak-Inherent	- FDP_ITT.1 "Basic internal transfer protection" - FPT_ITT.1 "Basic internal TSF data transfer protection" - FDP_IFC.1 "Subset information flow control" - AVA_VAN.5 "Advanced methodical vulnerability analysis"
O.Phys-Probing	- FDP_SDC.1 "Stored data confidentiality" - FPT_PHP.3 "Resistance to physical attack"
O.Malfunction	- FRU_FLT.2 "Limited fault tolerance - FPT_FLS.1 "Failure with preservation of secure state" - ADV_ARC.1 "Architectural Design with domain separation and non-bypassability"
O.Phys-Manipulation	- FDP_SDI.2 "Stored data integrity monitoring and action" - FPT_PHP.3 "Resistance to physical attack"
O.Leak-Forced	All requirements listed for O.Leak-Inherent - FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, AVA_VAN.5 plus those listed for O.Malfunction and O.Phys-Manipulation - FRU_FLT.2, FPT_FLS.1, FPT_PHP.3, ADV_ARC.1
O.Abuse-Func	- FMT_LIM.1 "Limited capabilities" - FMT_LIM.2 "Limited availability" plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced - FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1, ADV_ARC.1
O.Identification	- FAU_SAS.1 "Audit storage"
O.RND	- FCS_RNG.1/PTG.2 "Quality metric for random numbers" and FCS_RNG.1/RGS-IC "Quality metric for random numbers" plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced - FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1, AVA_VAN.5, ADV_ARC.1
OE.Resp-Appl	not applicable

Objective	TOE Security Functional and Assurance Requirements
OE.Process-Sec-IC	not applicable
O.Mem-Access	- FDP_ACC.1 "Subset access control" - FDP_ACF.1 "Security attribute based access control" - FMT_MSA.3 "Static attribute initialisation" - FMT_MSA.1 "Management of security attributes" - FMT_SMF.1 "Specification of Management Functions"
O.TDES	- FCS_COP.1/TDES "Cryptographic operation" - FCS_CKM.6/TDES "Timing and event of cryptographic key destruction"
O.AES	- FCS_COP.1/AES "Cryptographic operation" - FCS_CKM.6/AES "Timing and event of cryptographic key destruction"
O.ML-DSA	- FCS_COP.1/ML-DSA "Cryptographic operation" - FCS_CKM.1/ML-DSA "Cryptographic key generation" - FCS_CKM.6/ML-DSA "Timing and event of cryptographic key destruction"
O.Authentication	- FIA_API.1 " Authentication Proof of Identity"
OE.TOE_Auth	not applicable
O.Cap_Avail_Loader	- FMT_LIM.1/Loader "Limited capabilities" - FMT_LIM.2/Loader "Limited availability – Loader"
OE.Lim_Block_Loader	not applicable
O.Ctrl_Auth_Loader	- FTP_ITC.1 "Inter-TSF trusted channel" - FDP_UCT.1 "Basic data exchange confidentiality" - FDP_UIT.1 "Data exchange integrity" - FDP_ACC.1/Loader "Subset access control - Loader" - FDP_ACF.1/Loader "Security attribute based access control - Loader"
OE.Loader_Usage	not applicable
O.Prot_TSF_Confidentiality	- FDP_ACC.1/Loader "Subset access control - Loader" - FDP_ACF.1/Loader "Security attribute based access control - Loader"

Table 13: Security Requirements versus Security Objectives

174 The justification related to the security objective "Protection against Inherent Information Leakage (O.Leak-Inherent)" is as follows:

175 The refinements of the security functional requirements FPT_ITT.1 and FDP_ITT.1 together with the policy statement in FDP_IFC.1 explicitly require the prevention of disclosure of secret data (TSF data as well as user data) when transmitted between separate parts of the TOE or while being processed. This includes that attackers cannot reveal such data by measurements of emanations, power consumption or other behavior of

the TOE while data are transmitted between or processed by TOE parts.

176 It is possible that the TOE needs additional support by the Security IC Embedded Software (e.g. timing attacks are possible if the processing time of algorithms implemented in the software depends on the content of secret). This support must be addressed in the Guidance Documentation. Together with this FPT_ITT.1, FDP_ITT.1 and FDP_IFC.1 are suitable to meet the objective.

177 The justification related to the security objective "Protection against Physical Probing (O.Phys-Probing)" is as follows:

178 The SFR FDP_SDC.1 requires the TSF to protect the confidentiality of the information of the user data stored in specified memory areas and prevent its compromise by physical attacks bypassing the specified interfaces for memory access. The scenario of physical probing as described for this objective is explicitly included in the assignment chosen for the physical tampering scenarios in FPT_PHP.3. Therefore, it is clear that this security functional requirement supports the objective.

179 It is possible that the TOE needs additional support by the Security IC Embedded Software (e. g. to send data over certain buses only with appropriate precautions). This support must be addressed in the Guidance Documentation. Together with this FPT_PHP.3 is suitable to meet the objective.

180 The justification related to the security objective "Protection against Malfunctions (O.Malfunction)" is as follows:

181 The definition of this objective shows that it covers a situation, where malfunction of the TOE might be caused by the operating conditions of the TOE (while direct manipulation of the TOE is covered O.Phys-Manipulation). There are two possibilities in this situation: Either the operating conditions are inside the tolerated range or at least one of them is outside of this range. The second case is covered by FPT_FLS.1, because it states that a secure state is preserved in this case. The first case is covered by FRU_FLT.2 because it states that the TOE operates correctly under normal (tolerated) conditions. The functions implementing FRU_FLT.2 and FPT_FLS.1 must work independently so that their operation cannot affected by the Security IC Embedded Software (refer to the refinement). Therefore, there is no possible instance of conditions under O.Malfunction, which is not covered.

182 The justification related to the security objective "Protection against Physical Manipulation (O.Phys-Manipulation)" is as follows:

183 The SFR FDP_SDI.2 requires the TSF to detect the integrity errors of the stored user data and react in case of detected errors. The scenario of physical manipulation as described for this objective is explicitly included in the assignment chosen for the physical tampering scenarios in FPT_PHP.3. Therefore, it is clear that this security functional requirement supports the objective.

184 It is possible that the TOE needs additional support by the Embedded Software (for instance by implementing FDP_SDI.1 to check data integrity with the help of appropriate checksums, refer to Section 6.1). This support must be addressed in the Guidance Documentation. Together with this FPT_PHP.3 is suitable to meet the objective.

185 The justification related to the security objective "Protection against Forced Information Leakage (O.Leak-Forced)" is as follows:

186 This objective is directed against attacks, where an attacker wants to force an information leakage, which would not occur under normal conditions. In order to achieve this the attacker has to combine a first attack step, which modifies the behaviour of the TOE (either by exposing it to extreme operating conditions or by directly manipulating it) with a second attack step measuring and analysing some output produced by the

TOE. The first step is prevented by the same measures which support O.Malfunction and O.Phys-Manipulation, respectively. The requirements covering O.Leak-Inherent also support O.Leak-Forced because they prevent the attacker from being successful if he tries the second step directly.

187 The justification related to the security objective "Protection against Abuse of Functionality (O.Abuse-Func)" is as follows:

188 This objective states that abuse of functions (especially provided by the IC Dedicated Test Software, for instance in order to read secret data) must not be possible in Phase 7 of the life-cycle. There are two possibilities to achieve this: (i) They cannot be used by an attacker (i. e. its availability is limited) or (ii) using them would not be of relevant use for an attacker (i. e. its capabilities are limited) since the functions are designed in a specific way. The first possibility is specified by FMT_LIM.2 and the second one by FMT_LIM.1. Since these requirements are combined to support the policy, which is suitable to fulfil O.Abuse-Func, both security functional requirements together are suitable to meet the objective.

189 Other security functional requirements which prevent attackers from circumventing the functions implementing these two security functional requirements (for instance by manipulating the hardware) also support the objective. The relevant objectives are also listed in Table 13.

190 It was chosen to define FMT_LIM.1 and FMT_LIM.2 explicitly (not using Part 2 of the Common Criteria) for the following reason: Though taking components from the Common Criteria catalogue makes it easier to recognise functions, any selection from Part 2 of the Common Criteria would have made it harder for the reader to understand the special situation meant here. As a consequence, the statement of explicit security functional requirements was chosen to provide more clarity.

191 The justification related to the security objective "TOE Identification (O.Identification)" is as follows:

192 Obviously the operations for FAU_SAS.1 are chosen in a way that they require the TOE to provide the functionality needed for O.Identification. The Initialisation Data (or parts of them) are used for TOE identification. The technical capability of the TOE to store Initialisation Data and/or Pre-personalisation Data is provided according to FAU_SAS.1.

193 It was chosen to define FAU_SAS.1 explicitly (not using a given security functional requirement from Part 2 of the Common Criteria) for the following reason: The security functional requirement FAU_GEN.1 in Part 2 of the CC requires the TOE to generate the audit data and gives details on the content of the audit records (for instance data and time). The possibility to use the functions in order to store security relevant data which are generated outside of the TOE, is not covered by the family FAU_GEN or by other families in Part 2. Moreover, the TOE cannot add time information to the records, because it has no real time clock. Therefore, the new family FAU_SAS was defined for this situation.

194 The objective must be supported by organisational and other measures, which the TOE Manufacturer has to implement. These measures are a subset of those measures, which are examined during the evaluation of the assurance requirements of the classes AGD and ALC.

195 The justification related to the security objective "Random Numbers (O.RND)" is as follows:

196 FCS_RNG.1 requires the TOE to provide random numbers of good quality. The metrics associated to the DTRNG FRO M are given by the SFRs FCS_RNG.1/PTG.2, FCS_RNG.1/RGS-IC.

197 Other security functional requirements, which prevent physical manipulation and malfunction of the TOE (see the corresponding objectives listed in the table), support this objective because they prevent attackers from manipulating or otherwise affecting the random number generator.

198 Random numbers are often used by the Security IC Embedded Software to generate cryptographic keys for internal use. Therefore, the TOE must prevent the unauthorised disclosure of random numbers. Other security functional requirements which prevent inherent leakage attacks, probing and forced leakage attacks ensure the confidentiality of the random numbers provided by the TOE.

199 Depending on the functionality of specific TOEs the Security IC Embedded Software will have to support the objective by providing runtime-tests of the random number generator. Together, these requirements allow the TOE to provide cryptographically good random numbers and to ensure that no information about the produced random numbers is available to an attacker.

200 It was chosen to define FCS_RNG.1 explicitly, because Part 2 of the Common Criteria does not contain generic security functional requirements for Random Number generation. (Note, that there are security functional requirements in Part 2 of the Common Criteria, which refer to random numbers. However, they define requirements only for the authentication context, which is only one of the possible applications of random numbers.)

201 The security objective “Capability and availability of the Loader (O.Cap_Avail_Loader) is directly covered by the SFR FMT_LIM.1/Loader and FMT_LIM.2/Loader.

202 The security objective Access control and authenticity for the Loader (O.Ctrl_Auth_Loader) is covered by the SFR as follows:

203 The SFR FDP_ACC.1/Loader defines the subjects, objects and operations of the Loader SFP enforced by the SFR FTP_ITC.1, FDP_UCT.1, FDP_UIT.1 and FDP_ACF.1/Loader.

204 The SFR FTP_ITC.1 requires the TSF to establish a trusted channel with assured identification of its end points and protection of the channel data from modification or disclosure.

205 The SFR FDP_UCT.1 requires the TSF to receive data protected from unauthorised disclosure.

206 The SFR FDP_UIT.1 requires the TSF to verify the integrity of the received user data.

207 The SFR FDP_ACF.1/Loader requires the TSF to implement access control for the Loader functionality.

208 The FCS_COP.1/TDES and FCS_CKM.6/TDES meets the security objective “Cryptographic service Triple-DES (O.TDES)”.

209 The FCS_COP.1/AES and FCS_CKM.6/AES meets the security objective “Cryptographic service AES (O.AES)”.

210 The security functional requirement(s) “Cryptographic operation (FCS_COP.1/ML-DSA)” exactly requires those functions to be implemented which are demanded by O.ML-DSA. FCS_CKM.1 supports the generation of keys needed for this cryptographic operation(optional). Therefore, FCS_COP.1/ML-DSA and FCS_CKM.1/ML-DSA, FCS_CKM.6/ML-DSA are suitable to meet the security objective

211 The security objective “Authentication to external entities (O.Authentication) is directly covered by the SFR FIA_API.1.

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

213 The security functional requirement “Subset access control (FDP_ACC.1)” with the related Security Function Policy (SFP) “Memory Access Control Policy” exactly require the implementation of an area based memory access control, which is a requirement from O.Mem-Access. Therefore, FDP_ACC.1 with its SFP is

suitable to meet the security objective.

214 The security functional requirement "Static attribute initialisation (FMT_MSA.3)" requires that the TOE provides default values for the security attributes. Since the TOE is a hardware platform these default values are generated by the reset procedure. Therefore FMT_MSA.3 is suitable to meet the security objective O.Mem-Access.

215 The security functional requirement "Management of security attributes (FMT_MSA.1)" requires that the ability to change the security attributes is restricted to privileged subject(s). It ensures that the access control required by O.Mem-Access can be realised using the functions provided by the TOE. Therefore FMT_MSA.1 is suitable to meet the security objective O.Mem_Access.

216 Finally, the security functional requirement "Specification of Management Functions (FMT_SMF.1)" is used for the specification of the management functions to be provided by the TOE as required by O.MEM_ACCESS. Therefore, FMT_SMF.1 is suitable to meet the security objective O.Mem_Access.

217 The justification related to the security objective "Protection during Packaging, Finishing and Personalisation (OE.Process-Sec-IC)" is as follows:

218 The Composite Product Manufacturer has to use adequate measures to fulfil OE.Process-Sec-IC. Depending on the security needs of the application, the Security IC Embedded Software may have to support this for instance by using appropriate authentication mechanisms for personalisation functions.

219 The security objective Protection of the confidentiality of the TSF (O.Prot_TSF_Confidentiality) is covered by the SFR as follows:

220 The SFR FDP_ACC.1/Loader defines the subjects, objects and operations of the Loader SFP enforced by the FDP_ACF.1/Loader.

221 The SFR FDP_ACF.1/Loader requires the TSF to implement authentication mechanism for the Protection of the confidentiality of the TSF

6.3.2 Dependencies of Security Functional Requirements

222 The Table below lists the security functional requirements defined in this Security Target, their dependencies and whether they are satisfied by other security requirements defined in this Security Target. The text following the table discusses the remaining cases.

Security Functional Requirement	**Dependencies**	**Fulfilled by security requirements**
FCS_COP.1/TDES	FCS_CKM.6	Yes
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1 or FCS_CKM.5) or FCS_CKM.1 or FCS_CKM.6	Yes (by environment, see discussion below)
FCS_CKM.6/TDES	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1 or FCS_CKM.5	Yes (by environment, see discussion below)

FCS_COP.1/AES	FCS_CKM.6	Yes (by environment, see discussion below)
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)
FCS_CKM.6/AES	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1 or FCS_CKM.5	Yes (by environment, see discussion below)
FCS_COP.1/ML-DSA (optional)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes
	FCS_CKM.6	Yes, fulfilled by FCS_CKM.6/ML-DSA
FCS_CKM.1/ML-DSA (optional)	FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1	Yes, fulfilled by FCS_COP.1/ML-DSA
	FCS_RBG.1 or FCS_RNG.1	Yes (see discussion below)
	FCS_CKM.6	Yes (by environment, see discussion below)
FCS_CKM.6/ML-DSA (optional)	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1 or FCS_CKM.5	Yes (by environment, see discussion below)

Table 14 Dependencies of the Security Functional Requirements

223 Part 2 of the Common Criteria defines the dependency of FDP_IFC.1 (information flow control policy statement) on FDP_IFF.1 (Simple security attributes). The specification of FDP_IFF.1 would not capture the nature of the security functional requirement nor add any detail. As stated in the Data Processing Policy referred to in FDP_IFC.1 there are no attributes necessary. The security functional requirement for the TOE is sufficiently described using FDP_ITT.1 and its Data Processing Policy (FDP_IFC.1). Therefore the dependency is considered satisfied.

224 In particular the security functional requirements providing resistance of the hardware against manipulations (e. g. FPT_PHP.3) support all other more specific security functional requirements (e. g. FCS_RNG.1) because they prevent an attacker from disabling or circumventing the latter. Together with the discussion of the dependencies above this shows that the security functional requirements build a mutually supportive whole.

225 The functional requirements FCS_CKM.1 which is dependent to FCS_COP.1/TDES and FCS_COP.1/AES are not included in this Security Target since the TOE only provides an engine for encryption and decryption. But the Security IC Embedded Software may fulfill these requirements related to the needs of the implemented application. The dependent requirements of FCS_COP.1/TDES and FCS_COP.1/AES concerning these functions shall be fulfilled by the environment (Security IC Embedded Software).

226 The functional requirements FDP_ITC.1, FDP_ITC.2, FCS_CKM.1 and FCS_CKM.5 which are dependent to FCS_CKM.6/TDES and FCS_ CKM.6/AES are not included in this Security Target since the TOE only provides an engine for encryption and decryption. However, the Security IC Embedded Software may fulfill these requirements related to the needs of the implemented application. The dependent requirements of FCS_CKM.6/TDES and FCS_ CKM.6/AES concerning these functions shall be fulfilled by the environment (the cryptographic key destruction can be done by overwriting the key register interfaces or by TOE reset which provides randomization of the key registers).

227 The TOE provides the cryptographic key generation for PQC by the TOE (FCS_CKM.1/ML-DSA), but it is up to the Smart Card Embedded Software's security policy to adopt the cryptographic key generation by the TOE or use the cryptographic key generation by the Smart Card Embedded Software. The dependent requirements of FCS_COP.1/ML-DSA shall be fulfilled by the environment (Security IC Embedded Software).

228 The dependency FMT_SMR.1 introduced by the two components FMT_MSA.1 and FMT_MSA.3 is considered to be satisfied because the access control specified for the intended TOE is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of a security functional requirement FMT_SMR.1.

229 The dependency FMT_MSA.3 of FDP_ACF.1/Loader is not be necessary. The security attributes of ROM and Flash used to enforce the Loader SFP are fixed by the IC manufacturer. The access attribute of ROM and Flash memory have DEFAULT value.

230 The dependencies of FCS_CKM.1/ML-DSA to FCS_RNG.1 are fulfilled by the TOE since random numbers are used to generate cryptographic keys.

6.3.3 Rationale for the Assurance Requirements

231 The assurance level EAL6 and the augmentation with the requirement ASE_TSS.2 were chosen to demonstrate that the TOE fulfils the high-level Common Criteria requirements. An assurance level of EAL6 is required for this type of TOE since it is intended to defend against sophisticated attacks. This evaluation assurance level was selected since it is designed to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defence against such attacks, the evaluators should have access to the low level design and all the source code.

232 In addition, the TOE security policy is formally described and its security objective i.e. the complete memory access control is formally proved. The ASE_TSS.2 was chosen to demonstrate further assurance extensions provided by the TOE.

6.3.3.1 ADV_SPM.1 Formal TOE Security Policy Model

233 The formally modelled security policy consists of the complete TSF access control, in particular:

- The access control to the security registers, the Flash, ROM regions and Booting memory area are correctly enforced.
- The access control with respect to the MPU memory areas is correctly enforced, in particular:
  - A data is accessible if and only if its address is included in one of the Data Memory areas and this area has the access right (i.e. Read-only or Writing);
  - A data is writable if and only if

- its address is included in one of the Data Memory areas and this area has the Writing right, and
- its address is not included in any Data Memory area that has the Read-only right;

  - A code element is executable if and only if its address is included in one of the Program Memory areas and this area has the Execute right;
  - Any other access is a violation and is detected by the TSF;

- The consistency of the memory areas is correctly enforced i.e.
  - All memory areas and access rights are correctly initialized at the IC reset
  - Each fixed data area and program area is completely contained in the physical memory space of its memory type
- The consistency of the bootloader is correctly enforced.

- ADV_SPM.1 Formal TOE security policy model

ADV_SPM.1	Formal TOE Security Policy Model as defined in Section 13.5 of [3]
Dependencies:	ADV_FSP.4 Complete functional specification
Developer action elements:	
ADV_SPM.1.1D	The developer shall provide a formal security policy model for the *following policies*: • *Memory access control policy* • *Loader access control policy* • *Non-reversibility of TEST mode*
ADV_SPM.1.2D	For each policy covered by the formal security policy model, the model shall identify the relevant portions of the statement of SFRs that make up that policy.
ADV_SPM.1.3D	The developer shall provide a formal proof of correspondence between the model and any formal specification.
ADV_SPM.1.4D	The developer shall provide a demonstration of correspondence between the model and the functional specification.

6.3.3.2 ASE_TSS.2 TOE Summary specification with architectural design summary

234 The augmentation ASE_TSS.2 is required in order to provide the potential users (e.g. the embedded software developers) with a succinct but comprehensive explanation on the TOE security functions that protect it against interference, logical tampering and bypass. This description is also necessary to establish the component ASE_TSS.2 for any composed TOE.

235 This assurance component is a higher hierarchical component to EAL6. ASE_TSS.2 has two dependencies (ASE_INT.1 and ASE_REQ.1) that both are satisfied by this TOE.

6.3.4 Security Requirements are Internally Consistent

236 The discussion of security functional requirements and assurance components in the preceding sections has shown that mutual support and consistency are given for both groups of requirements. The arguments given for the fact that the assurance components are adequate for the functionality of the TOE also shows that the security functional requirements and assurance requirements support each other and that there are no inconsistencies between these groups.

237 The security functional requirements FDP_SDC.1 and FDP_SDI.2 address the protection of user data in the specified memory areas against compromise and manipulation. The security functional requirement FPT_PHP.3 makes it harder to manipulate data. This protects the primary assets identified in Section 3.1 and other security features or functionality which use these data.

238 Though a manipulation of the TOE (refer to FPT_PHP.3) is not of great value for an attacker in itself, it can be an important step in order to threaten the primary assets. Therefore, the security functional requirement FPT_PHP.3 is not only required to meet the security objective O.Phys-Manipulation. Instead it protects other security features or functions of both the TOE and the Security IC Embedded Software from being bypassed, deactivated or changed. In particular this may pertain to the security features or functions being specified using FDP_ITT.1, FPT_ITT.1, FPT_FLS.1, FMT_LIM.2, FCS_RNG.1, and those implemented in the Security IC Embedded Software.

239 A malfunction of TSF (refer to FRU_FLT.2 and FPT_FLS.1) can be an important step in order to threaten the primary assets. Therefore, the security functional requirements FRU_FLT.2 and FPT_FLS.1 are not only required to meet the security objective O.Malfunction. Instead they protect other security features or functions of both the TOE and the Security IC Embedded Software from being bypassed, deactivated or changed. In particular this pertains to the security features or functions being specified using FDP_ITT.1, FPT_ITT.1, FMT_LIM.1, FMT_LIM.2, FCS_RNG.1, and those implemented in the Security IC Embedded Software.

240 In a forced leakage attack the methods described in “Malfunction due to Environmental Stress” (refer to T.Malfunction) and/or “Physical Manipulation” (refer to T.Phys-Manipulation) are used to cause leakage from signals which normally do not contain significant information about secrets. Therefore, in order to avert the disclosure of primary assets it is important that the security functional requirements averting leakage (FDP_ITT.1, FPT_ITT.1) and those against malfunction (FRU_FLT.2 and FPT_FLS.1) and physical manipulation (FPT_PHP.3) are effective and bind well. The security features and functions against malfunction ensure correct operation of other security functions (refer to above) and help to avert forced leakage themselves in other attack scenarios. The security features and functions against physical manipulation make it harder to manipulate the other security functions (refer to above).

241 Physical probing (refer to FPT_PHP.3) shall directly avert the disclosure of primary assets. In addition, physical probing can be an important step in other attack scenarios if the corresponding security features or functions use secret data. For instance the security functional requirement FMT_LIM.2 may use passwords. Therefore, the security functional requirement FPT_PHP.3 (against probing) help to protect other security features or functions including those being implemented in the Security IC Embedded Software. Details depend on the implementation.

242 Leakage (refer to FDP_ITT.1, FPT_ITT.1) shall directly avert the disclosure of primary assets. In addition, inherent leakage and forced leakage (refer to above) can be an important step in other attack scenarios if the corresponding security features or functions use secret data. For instance the security functional requirement FMT_LIM.2 may use passwords. Therefore, the security functional requirements FDP_ITT.1 and FPT_ITT.1 help to protect other security features or functions implemented in the Security IC Embedded Software (FDP_ITT.1) or provided by the TOE (FPT_ITT.1). Details depend on the

implementation.

243 The user data of the Composite TOE are treated as required to meet the requirements defined for the specific application context (refer to Treatment of user data of the Composite TOE (A.Resp-Appl)). However, the TOE may implement additional functions. This can be a risk if their interface cannot completely be controlled by the Security IC Embedded Software. Therefore, the security functional requirements FMT_LIM.1 and FMT_LIM.2 are very important. They ensure that appropriate control is applied to the interface of these functions (limited availability) and that these functions, if being usable, provide limited capabilities only.

244 The combination of the security functional requirements FMT_LIM.1 and FMT_LIM.2 ensures that (especially after TOE Delivery) these additional functions cannot be abused by an attacker to (i) disclose or manipulate user data of the Composite TOE, (ii) to manipulate (explore, bypass, deactivate or change) security features or services of the TOE or of the Security IC Embedded Software or (iii) to enable other attacks on the assets. Hereby the binding between these two security functional requirements is very important:

245 The security functional requirement Limited Capabilities (FMT_LIM.1) must close gaps which could be left by the control being applied to the function's interface (Limited Availability (FMT_LIM.2)). Note that the security feature or services which limits the availability can be bypassed, deactivated or changed by physical manipulation or a malfunction caused by an attacker. Therefore, if Limited Availability (FMT_LIM.2) is vulnerable, it is important to limit the capabilities of the functions in order to limit the possible benefit for an attacker.

246 The security functional requirement Limited Availability (FMT_LIM.2) must close gaps which could result from the fact that the function's kernel in principle would allow to perform attacks. The TOE must limit the availability of functions which potentially provide the capability to disclose or manipulate user data of the Composite TOE, to manipulate security features or services of the TOE or of the Security IC Embedded Software or to enable other attacks on the assets. Therefore, if an attacker could benefit from using such functions, it is important to limit their availability so that an attacker is not able to use them..

247 No perfect solution to limit the capabilities (FMT_LIM.1) is required if the limited availability (FMT_LIM.2) alone can prevent the abuse of functions. No perfect solution to limit the availability (FMT_LIM.2) is required if the limited capabilities (FMT_LIM.1) alone can prevent the abuse of functions. Therefore, it is correct that both requirements are defined in a way that they together provide sufficient security.

248 It is important to avert malfunctions of TSF and of security functions implemented in the Security IC Embedded Software (refer to above). There are two security functional requirements which ensure that malfunctions cannot be caused by exposing the TOE to environmental stress. First it must be ensured that the TOE operates correctly within some limits (Limited fault tolerance (FRU_FLT.2)). Second the TOE must prevent its operation outside these limits (Failure with preservation of secure state (FPT_FLS.1)). Both security functional requirements together prevent malfunctions. The two functional requirements must define the "limits". Otherwise there could be some range of operating conditions which is not covered so that malfunctions may occur. Consequently, the security functional requirements Limited fault tolerance (FRU_FLT.2) and Failure with preservation of secure state (FPT_FLS.1) are defined in a way that they together provide sufficient security.

249 The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms implemented according to the security functional requirement FCS_COP.1. Therefore, these security functional requirements support the secure implementation and operation of FCS_COP.1.

250 Parts of the Smartcard IC Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). In order to avert the memory access violation it is important to the security functional requirement defining the scope where the Memory Access Policy is applied (FDP_ACC.1) and the security functional requirement defining the Memory Access Policy(FDP_ACF.1), and the security functional requirement ensuring the default value of security attribute(FMT_MSA.3) and the security functional requirement managing security attribute (FMT_MSA.1) and the security functional requirement performing security management function(FMT_SMF.1) are effective and bind well.

251 Two refinements from the PP [5] have to be discussed here in the ST as the assurance level is increased. The refinement for ALC_CMS from the PP [5] can even be applied at the assurance level EAL6 augmented with ALC_CMS.5. The assurance component ALC_CMS.4 is augmented to ALC_CMS.5 with aspects regarding the configuration control system for the TOE. The refinement is not touched. The refinement for ADV_FSP from the PP [5] can even be applied at the assurance level EAL6 augmented with ADV_FSP.5. The assurance component ADV_FSP.4 is extended to ADV_FSP.5 with aspects regarding the description level. The level is increased from informal to semi-formal with informal description. The refinement is not touched by this measure.

7 TOE SUMMARY SPECIFICATION

252 This chapter 7 TOE Summary Specification contains the following sections:

7.1 List of Security Functional Requirements

7.1 List of Security Functional Requirements

SFR1: FPT_FLS.1: Failure with preservation of secure state

253 The detection thresholds of TOE's detectors are inside the operating range of the TOE. Therefore abnormal events/failures are detected before the secure state is compromised. This allows to take User's defined appropriate actions by software or to immediately RESET the TOE.

254 The secure state is maintained by TOE's detectors. The TOE's detectors are monitoring the failure occurs. If the failures are happen, the TOE goes into RESET state.

TOE's Detectors

255 These functions records in register the events notified by the detectors (refer to list below). The software configures the reaction in case of detection:

- The TOE is immediately reset when an event is detected.
- Or, a special function register bit is set.

TOE's detectors are implemented by the hardware. The detection cannot be affected or bypassed by Smartcard Embedded Software. The reaction to the detection can be configured by the software. The influence on security and the way how to configure it is described in details in the S3SSE2A User's Manual. Therefore, FPT_FLS.1 is implemented by TOE.

256 Security domains are maintained since accesses to the access-prohibited area are trapped by this access control function.

SFR2: FRU_FLT.2: Limited fault tolerance

257 All operating signals are filtered/regulated in order to prevent malfunction.

TOE's Filters

258 These filters are used for preventing abnormal environment conditions from causing undefined or unpredictable behavior of the chip.

Integrity Checkers

259 These Integrity Checkers are used for preventing noise and laser from causing undefined or unpredictable behavior of the chip.

260 TOE's filters and integrity checkers are implemented by the hardware. The filtering cannot be affected or bypassed by Smartcard Embedded Software. The reaction to the detection can be configured by the software. The influence on security and the way how to configure it is described in details in the S3SSE2A User's Manual. Therefore, FRU_FLT.2 is implemented by TOE. Refer to the table 9 for the filters specification.

SFR3: FPT_PHP.3: Resistance to physical attacks

261 This requirement is achieved by security feature as the shield must be removed and bypassed in order to perform physical intrusive attacks. The TOE makes appropriate secure reaction to stops operation if a physical manipulation or physical probing attack is detected. Scrambling and encryption mechanisms make the reverse-engineering of the TOE layout unpractical and protect from probing attack and signal identification of the TOE layout unpractical. So these functionalities meet the security functional requirement of FPT_PHP.3: Resistance to physical attack.

SFR4: FDP_ACC.1: Subset access control

262 This requirement is achieved by security register access control, invalid address access and so on.

1) Security registers access control: This security function manages access to the security control registers through access control security attributes.

2) Invalid address access: This function detects invalid address access occurrence, allowing to take dedicated and appropriate actions.

3) Access rights for the code executed in FLASH: This function detects invalid access allowing to take dedicated and appropriate actions.

4) Access control for Operating state: This security function selects booting memory area. User can select ROM-BOOT or FLASH-BOOT.

5) Flash protection about Write operation: This function provides protection about flash write operation.

SFR5: FDP_ACF.1: Security attributes based access control.

263 This is covered by the Privilege and User modes of the TOE. The more information on chapter 1.2 Figure 1-2. Privilege and User Modes basic description

SFR6: FMT_MSA.3: Static attribute initialization.

264 All Special Function Registers including MPU have DEFAULT values after Power on Reset.

The access attribute of ROM and Flash memory have DEFAULT values.

SFR7: FMT_MSA.1: Management of security attributes.

265 This is achieved with the following feature.

The Memory Protection Unit (MPU) enables user to partition memory and set individual protection attributes for each partition. This allows the operating system to control the memory regions accessible by a User mode application process.

The OPRSEL enables user to ROM protection attributes. This allows the operating system to control the ROM regions accessible by a User mode application process.

The OPRSEL enables user to FLASH and set individual protection attributes.

SFR8: FMT_SMF.1: Specification of management functions.

266 This is achieved via access to Special Function Registers of Memory Protection Unit(MPU). MPU provides Special Function Registers which defines the base address and the limit address for a partition. The Registers exist for Flash, and RAM. Additional Registers exist for defining the protection attribute for each partition.

SFR9: FAU_SAS.1: Audit Storage

267 This is fulfilled by the traceability/identification data written once and for all during the TEST mode of the manufacturing process.

1) Non-reversibility of TEST mode and NORMAL mode: This function disables the TEST mode and enables the NORMAL mode of the TOE. This function ensures the non-reversibility of the NORMAL mode. This function is used once during the manufacturing process.

2) TEST mode communication protocol and data commands: This function is the proprietary protocol used to operate the chip in TEST mode. This function enforces the identification and authentication of the TEST administrator during the test phase of the manufacturing process.

3) Functional Tests: During the manufacturing process, the operation of the TOE and the embedded software checksum are verified. This security function ensures the correct operation of the TOE security functions and the integrity of the embedded software.

4) Identification: During the TEST mode of manufacturing process, traceability data are written in the non-volatile memory of the TOE. Once the TOE is switched from TEST to NORMAL mode, those traceability data are READ ONLY and cannot be modified anymore. In particular, user can identify the silicon chip version and the version of the device Dedicated SW parts (Test ROM code, Bootloader). The DTRNG FRO M library is identified by the version function in the library.

SFR10: FMT_LIM.1: Limited capabilities

268 TEST mode can be accessed only by the TEST administrator by supplying an authentication password through a proprietary protocol. Once the TOE is changed to NORMAL mode, TEST mode functions are no more available for NORMAL mode.

SFR11: FMT_LIM.2: Limited availabilities

269 TEST mode can be accessed only by the TEST administrator by supplying an authentication password through a proprietary protocol. Once the TOE is changed to NORMAL mode, TEST mode commands are no more available for NORMAL mode. Functional test during manufacturing process is only available for TEST mode only.

SFR12: FDP_IFC.1: Subset information flow control

270 Memory Encryption: This is achieved by the function protects the memory contents of the TOE from data analysis on the stored data as well as on internally transmitted data.

Shield: This requirement is achieved by security feature as the shield must be removed and bypassed

in order to perform physical intrusive attacks.

Life time detector: Life time detector detects if detector signals are modified or not.

SFR13: FDP_ITT.1: Basic internal transfer protection

271 This requirement is achieved by the combination of the TOE security features TOE features 1) to 5) as it is unpractical to get access to internal signals and interpret them.

1) Static Address/Data scrambling for bus and memory: This function protects memory and address/data bus from probing attacks.

2) Data encryption for bus: This function protects data bus from probing attacks.

3) Memory encryption: This security function protects the memory contents of the TOE from data analysis on the stored data as well as on internally transmitted data.

4) Synthesizable processor core: The Central Processing Unit (CPU) of the TOE is synthesizable with glue logic, which makes reverse engineering and signal identification more difficult.

5) De-synchronization and signal-to-noise ratio reduction mechanisms: The TOE operations can be made asynchronous. They make a full range of intrusive (e.g. probing attacks) and non intrusive attacks (e.g. side-channel attacks) more complex and difficult.

SFR14: FPT_ITT.1: Basic internal TSF data transfer protection

272 This requirement is achieved by the combination of the TOE security features TOE features 1) to 5) as it is unpractical to get access to internal signals and interpret them.

1) Static Address/Data scrambling for bus and memory: This function protects memory and address/data bus from probing attacks.

2) Data encryption for bus: This function protects data bus from probing attacks.

3) Memory encryption: This security function protects the memory contents of the TOE from data analysis on the stored data as well as on internally transmitted data.

4) Synthesizable processor core: The Central Processing Unit (CPU) of the TOE is synthesizable with glue logic, which makes reverse engineering and signal identification more difficult.

5) De-synchronization and signal-to-noise ratio reduction mechanisms: The TOE operations can be made asynchronous. They make a full range of intrusive (e.g. probing attacks) and non intrusive attacks (e.g. side-channel attacks) more complex and difficult.

SFR15: Random number generation

FCS_RNG.1/PTG.2

273 This requirement is ensured by the design of the random number generation algorithm that makes use of Digital True Random Number Generator (DTRNG FRO M) and the associated DTRNG FRO M library conforming to *BSI-AIS31 Class PTG.2* requirements (German scheme).

FCS_RNG.1/RGS-IC

274 This requirement is ensured by the design of the random number generation algorithm that makes use of Digital True Random Number Generator (DTRNG FRO M) and the associated DTRNG FRO M library conforming to some of *ANSSI RGS* requirements (French scheme).

SFR16: FCS_COP.1: Cryptographic operation

275 This requirement is covered by the TOE.

Triple Data Encryption Standard Engine

276 This function is used for encrypting and decrypting data using the Triple DES symmetric algorithm with 112bit or 168bit key size. (FCS_COP.1/TDES)

AES (Advanced Encryption Standard)

277 This function supports the AES operation with 128 bit, 192bit and 256bit key size. (FCS_COP.1/AES)

SFR17: FCS_CKM.6 Timing and event of cryptographic key destruction

278 This requirement is covered by the TOE.

Timing and event of cryptographic key destruction – Triple Data Encryption Standard Engine

279 This requirement is achieved by overwriting the TDES key registers or by TOE reset.

Timing and event of cryptographic key destruction – AES (Advanced Encryption Standard)

280 This requirement is achieved by overwriting the AES key registers or by TOE reset.

Timing and event of cryptographic key destruction – ML-DSA (Module Lattice Based Digital Signature Algorithm)

281 This requirement is achieved by key destruction function of ACT1 Secure ML-DSA Algorithm.

SFR18: Limited capabilities - Loader(FMT_LIM.1/Loader)

This requirement is achieved by changing the Operating Mode Selection from ROM Booting mode to Flash Booting mode and then locking the Operating Mode. If the chip is locked in FLASH Booting mode, the Bootloader cannot be deployed any more. It is then not possible to use the FLASH read and write commands of the Bootloader to read, download or modify any data or code in FLASH.

SFR19: Limited availability – Loader (FMT_LIM.2/Loader)

This requirement is achieved by changing the Operating Mode Selection from ROM Booting mode to Flash Booting mode and then locking the Operating Mode. If the chip is locked in FLASH booting mode, the TSF prevents deploying the Loader functionality. The Bootloader is then disabled and user cannot change the TOE Booting mode any more after the locking.

SFR20: Inter-TSF trusted channel (FTP_ITC.1)

This requirement is achieved by processing the mutual Authentication sequence. This channel is only distinct from other communication channels and provides assured identification for its end points and

protection of the channel data from modification or disclose.

SFR21: Basic data exchange confidentiality (FDP_UCT.1)

This requirement is achieved by secure writing. User data which is encrypted data.

SFR22: Data exchange integrity (FDP_UIT.1)

This requirement is achieved by appropriate code integrity mechanism.

SFR23: Subset access control - Loader (FDP_ACC.1/ Loader)

This requirement is achieved by following functions.

ROM hiding function: The attribute of ROM is changed from Accessible ROM to Inaccessible ROM.

Flash memory attribute as Read only.

.

SFR24: Security attribute based access control - Loader (FDP_ACF.1/Loader)

This is covered by the ROM Booting(ROM Reset) and Flash Booting(Flash Reset) mode of the TOE. TOE can be set to ROM Booting(ROM Reset) and FLASH Booting(FLASH Reset) mode domains exclusively. All Bootloader APDU commands are accessible only in Rom Booting mode. The Flash Booting mode can not access all Bootloader APDU commands.

SFR25: Stored data confidentiality (FDP_SDC.1)

This requirement is achieved by the combination of the TOE security features TOE features 1) to 9) as it is unpractical to get access to internal signals and interpret them.

1) Static Address/Data scrambling for bus and memory: This function protects memory and address/data bus from probing attacks.

2) Data encryption for bus: This function protects data bus from probing attacks.

3) Memory encryption: This security function protects the memory contents of the TOE from data analysis on the stored data as well as on internally transmitted data.

4) Invalid address access: This function detects invalid address access occurrence.

5) Shield: This requirement is achieved by security feature as the shield must be removed and bypassed in order to perform physical intrusive attacks.

6) Life time detector: Life time detector detects modifications.

7) Filters: These filters are used for preventing noise, glitches and extremely high frequency in the external reset or clock pad from causing undefined or unpredictable behavior of the chip.

8) Non-reversibility of TEST and NORMAL modes: This function disables the TEST mode and enables the NORMAL mode of the TOE. This function ensures the non-reversibility of the NORMAL mode. This function is used once during the manufacturing process

9) Control of Booting mode: This requirement is achieved by changing the Operating Mode Selection.

SFR26: Stored data integrity monitoring and action (FDP_SDI.2)

This requirement is achieved by following functions.

Flash/RAM: Error manage features.

SFR27: Authentication Proof of Identity (FIA_API.1)

This requirement is achieved by processing the mutual Authentication sequence.

SFR28: Cryptographic key generation

282 This requirement is achieved by the TOE by the ML-DSA key generation function (optional):

ML_DSA_keygen - FCS_CKM.1/ML-DSA.

This function generates ML-DSA public/private key pair.

7.2 Architectural Design Summary

283 The TOE claims the assurance requirement ASE_TSS.2, the security architectural information on a very high level is included in the TSS to inform the embedded software developers on how the TOE protects itself against interference, logical tampering and bypass.

284 Interference

285 Interference consists in interfering in the TSF in order to get access to assets.

286 Logical tampering

287 Logical tampering consists in get access to the assets by a logical means (in contrast with physical tampering). For this TOE, logical tampering may be used on

- the access control
- the information flow control

288 The access control is enforced by the following security functions: "Security registers access control", "Invalid address access", "Access rights for the code executed in FLASH", "Access control for Operating state", "Flash protection about Write operation".

289 The information flow control is enforced by the following security function "Memory Encryption".

290 Bypass

291 Non-bypassability is a property that the security functionality of the TSF is always invoked. For this TOE, bypassing a security function may be caused by

292 A physical perturbation on the IC: protection against this bypass if ensured by the security functions "Static Address/Data scrambling for bus and memory", "Synthesizable processor core", "Detectors", "Filters"

293 Switching back from Normal mode to Test mode in order to get more privilege: protection against this bypass if ensured by the security functions "Non-reversibility of TEST mode and NORMAL mode"

294 Masking the security errors: protection against this bypass if ensured by the security function "Security registers access control"

8 Annex

8.1 References

[1] Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022 - Part 1: Introduction and General Model, CCMB-2022-11-001

[2] Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022 - Part 2: Security functional components, CCMB-2022-11-002

[3] Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022 - Part 3: Security assurance components, CCMB-2022-11-003

[4] Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022 — Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004

[5] Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022 — Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005

[6] Common Criteria for Information Technology Security Evaluation, CEM:2022, Revision 1, November 2022 - Evaluation methodology, CCMB-2022-11-006

[7] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, 2024-07-22, CCMB-2024-002

[8] Transition Policy to CC:2022 and CEM:2022, April 20th 2023, CCMC-2023-04-001

[9] Eurosmart Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084-2014.

[10] AIS31: Functionality classes and evaluation methodology for true (physical) random number generators, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

[11] A proposal for: Functionality classes for random number generators, Version 2.0, 18.09.2011, Bundesamt für Sicherheit in der Informationstechnik

[12] ALGO: Federal Gazette No 19, Notification in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance (overview of suitable algorithms), Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway, 2008-11-17

[13] [NIST SP 800-67] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised January 2012, National Institute of Standards and Technology

[14] [FIPS 197]Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

[15] CC Supporting Document, Mandatory Technical Document, "Application of Attack Potential to Smartcards": version 3.2.1 (February 2024).

[16] Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. Version 2.04, 01/01/2020, ANSSI. http://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf

[17] [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

[18] [FIPS PUB 202] Federal Information Processing Standards Publication FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions; U.S. department of Commerce / National Institute of Standards and Technology (NIST), August 2015

[19] [FIPS 204] Federal Information Processing Standards Publication FIPS 204, Module-Lattice-Based Digital Signature Standard; U.S. department of Commerce / National Institute of Standards and Technology (NIST), August 13, 2024

[20] ADV_SPM.1 interpretation for [CC:2022] transition, Joint Interpretation Library, Version 1.0 , May 2024

[21] PP0084 – Interpretations – v3, 01/06/2016, ANSSI