TIEMPO S.A.S., 110 Rue Blaise Pascal,
Bâtiment Viseo - Inovallée
38330 Montbonnot St-Martin
France

# ASE – Security Target Lite

**Security Target Lite of the Security Enclave in SEQUANS communication SoC Monarch 2/N-SQN3401**

TESIC-04001R20

D-SPD-1113-1311-1.0

Security Level 1: Public

Revision: 1.0

Date: 30/07/2021

# Tiempo Trademarks and Copyright Information

# Contents

# Figures and Tables

# Version

| Version | Date | Description |
|---|---|---|
| **1.0** | 30/07/2021 | Initial release |

# 1 Security Target Introduction

## This chapter Version

| Version | Date | Description |
|---|---|---|
| **1.0** | 30/07/2021 | Initial release |

1 Security Target Introduction contains the following sections:

*Security Target and Target of* Evaluation Reference *(1.1)*

*TOE Overview and TOE Description (1.2)*

*Interfaces of the TOE (1.3)*

*TOE intended Usage (1.4)*

## 1.1 Security Target and Target of Evaluation Reference

2 This document is entitled “Security Target Lite of the Security Enclave in SEQUANS communication SoC Monarch 2/N-SQN3401”, is in its version 1.0 and is dated 30/07/2021. The Target of Evaluation (TOE) is the Tiempo Security IP TESIC-04001R20 with an optional specific IC-dedicated firmware and an optional cryptographic library. It constitutes the security enclave of the Sequans Communication SoC Monarch 2/N – SQN3401. The Target of Evaluation (TOE) TESIC-04001R20 is described in the following sections.

3 The Security Target is strictly compliant to Eurosmart Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 2014, BSI-CC-PP-0084 [1] and built on *Common criteria* version 3.1 [2-5].

4 The targeted Evaluation Assurance Level for the TOE is EAL5 augmented with AVA_VAN.5 and ALC_DVS.2.

| | |
|---|---|
| Title: | Security Target Lite of the Security Enclave in SEQUANS communication SoC Monarch 2/N-SQN3401 |
| Target of Evaluation | Tiempo Security IP TESIC-04001R20 |
| TOE reference: | TESIC-04001R20-BL2.0-AL28-CL3.0.F |
| Provided by: | TIEMPO-IC |
| Evaluation schema: | France (ANSSI) |
| Evaluator: | LETI ITSEF (France) |
| Common Criteria version: | [2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; April 2017, Version 3.1, Revision 5, CCMB-2017-04-001.<br>[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; April 2017, Version 3.1, Revision 5, CCMB-2017-04-002.<br>[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; April 2017, Version 3.1, Revision 5, CCMB-2017-04-003.<br>[5] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; April 2017, Version 3.1, Revision 5, CCMB-2017-04-004. |

## 1.2 TOE Overview and TOE Description

### 1.2.1 Introduction

5 The Target of Evaluation (TOE) is the security enclave TESIC-04001R20 of the communication chip Monarch 2/N - SQN3401. The security enclave includes a ROM (64Kbytes), a RAM (32Kbytes), a CACHERAM (16Kbytes), a CRYPTORAM (4Kbytes), an OTP (128 Kbits), accelerators for symmetric/asymmetric cryptography and random number/keys generation. The security enclave is able to securely manage an external non-volatile memory. A Crypto-library is provided which includes symmetric and asymmetric cryptography as well as keys and random number generation. An ADMIN loader and services is also provided to manage the external memory.

### 1.2.2 TOE Definition

6 TESIC-04001R20 is the security enclave of SQN3401 and is a hardware IP provided by Tiempo, based on Tiempo TESIC asynchronous platform, built around an 8/16/32-bit asynchronous CPU with coprocessors for hardware acceleration of standard cryptographic operations, peripherals, communication interfaces, embedded memories and security features.

7 The main security features associated to security services integrated in TESIC-04001R20 are listed below:

- Security sensors.
- Shield.
- Security mechanisms for memory protection.
- Dedicated hardware techniques against side-channel attacks
- Dedicated hardware techniques against fault injection attacks
- Secure DES/Triple DES cryptographic coprocessor
- Secure AES cryptographic coprocessor
- Secure accelerator for RSA and ECC against side channel and fault injection attacks.
- True Random Number Generator (TRNG) that meets some of ANSSI requirements (RGS_B1).
- Pseudo Random Number Generator (PRNG)
  - No compliance to any specific metric but PRNG is used by the chip for internal use.
- Proprietary secure asynchronous CPU.
- Secure CRC coprocessor for integrity check.
- Memory protection unit (MPU) for secure access memory.
- Deterministic Random Bit Generator (DRBG) that meets some of ANSSI requirements (RGS_B1).
- Secure software AES.
- Secure software DES.
- Secure software RSA.
- Secure software ECC.
- Secure software SHA2 (SHA2-224/ SHA2-256/SHA2-384/SHA2-512).
- Secure software AEAD algorithm.

- Secure external memory management.

Note: the DRBG from the IC Dedicated Support Software combined with the TRNG from the IC together meet some of the ANSSI requirements (RGS_B1).

8 The operating temperature range is defined as:

- -40°C to +125°C

9 The operating voltage range is defined as:

- 0.99 V – 1.1 V

10 The overview of the architecture of the Monarch 2/N-SQN3401 SoC is presented in Figure 1-1.

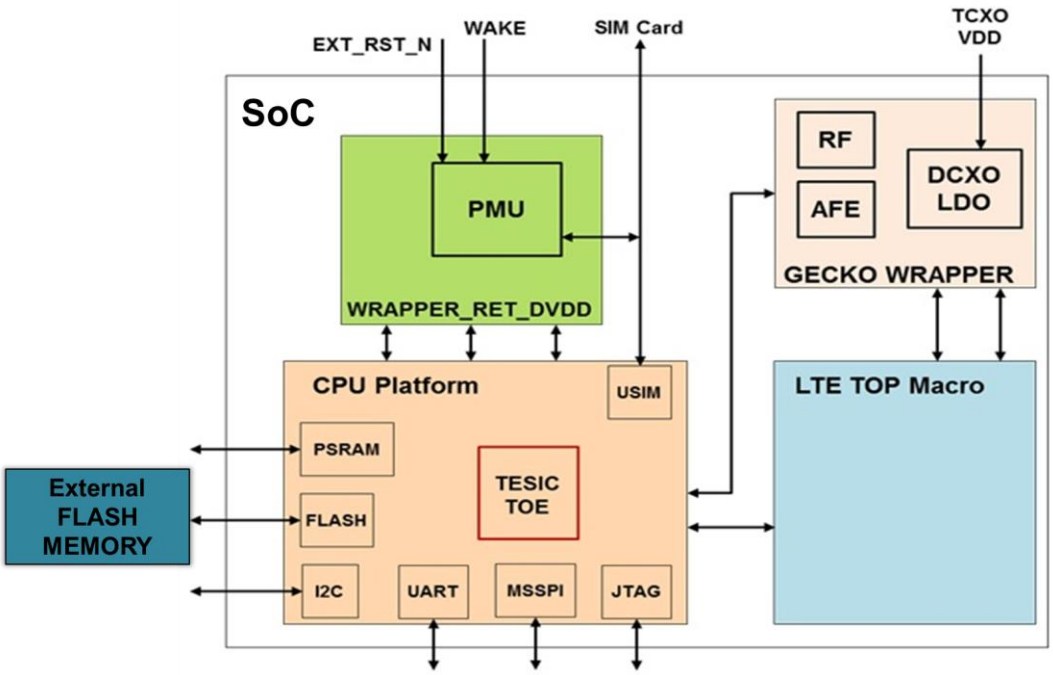


*Figure 1-1: SoC simplified architecture*

11 The CPU platform macro includes the 3 CPUs and all additional functional blocks (timers, WDT, etc.) together with all interfaces (UARTs, SPI, I2C, etc.). Additionally, 10 DMAs, QSPI, PSRAM controllers are included in the platform as well as a PCM/I2S block for audio support. The CPU platform also includes a Flash controller which communicates with the external NVM. The TESIC-04001R20 security enclave is one of the featured subsystems of the CPU platform.

12 The power supply for the TOE and the global reset are handled by the PMU in a separate wrapper.

13 The architecture described in Figure 1-1 uses a passive external NVM (Flash memory) that does not implement any security functionality.

14 The TOE fetches the IC dedicated software from the external NVM.

15 The external NVM comprises an area dedicated for the TOE in which the data is encrypted using diversified keys that are specific to each chip.

16 The IC dedicated software is optionally loaded in external NVM in phase 5 secured by the Tiempo keys loaded in phase 4. It includes a full featured Admin loader with the services needed to store TSF and user data in external memory (providing confidentiality, authenticity and anti-roll-back protection). Then the composite application software is loaded into the external NVM in phase 5.

17 The software stored in the external memory is decrypted, authenticated and loaded in the internal CACHE RAM memory before being executed.

### 1.2.3 TOE Hardware

18 The overview of the hardware architecture is presented in Figure 1-2.

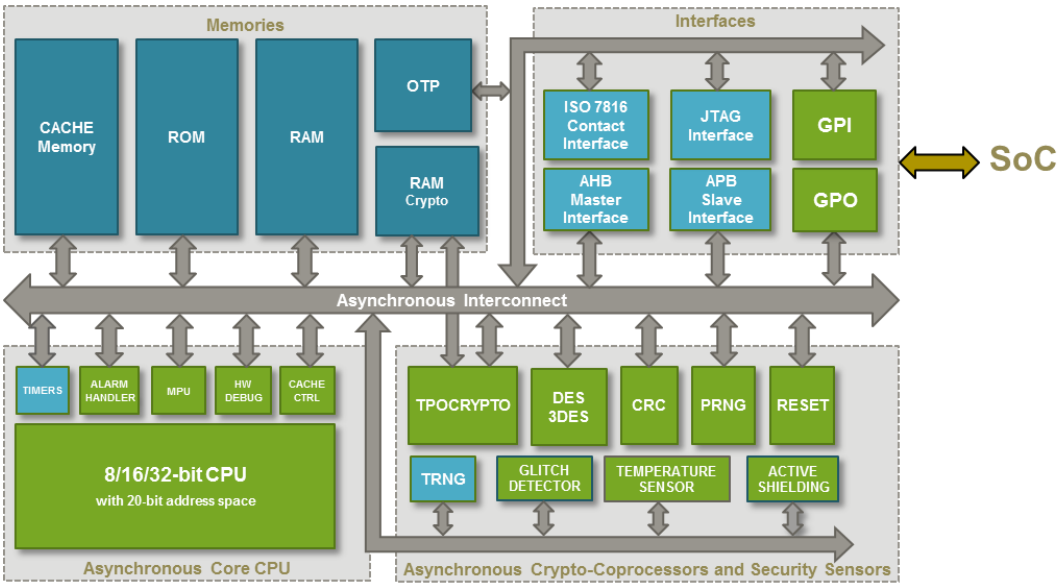


*Figure 1-2: Block diagram of the TOE*

19 The hardware blocks integrated in the TOE are listed below:

- Low power 8/16-bit microcontroller which provides 32-bit operations.
- Timers: 3 timers providing periodic timestamp, watchdog, application timeout, profiling function, and CPU power saving mode features.
- Interrupt controller with 2 types of interrupts: Maskable interrupts (MI) and non-maskable interrupts (NMI).
- Hardware contact interface compliant with ISO7816-3 [6].
- AMBA AHB-Lite master interface as a suitable interface for high-performance designs.
- AMBA APB slave interface.
- Hardware AES cryptographic coprocessor compliant with the AES-128, AES-192 and AES-256 standards [7] as a part of the TPOCRYPTO subsystem which regroups the AES and PKA cryptographic modules.
- Hardware DES/Triple DES cryptographic coprocessor with 56 bits, 112 bits and 168 bits of key sizes [8].
- Hardware asymmetric cryptographic accelerator (PKA) implementing RSA and ECC over GF(p) with operand sizes up to 4096 bits. It integrates modular multiplication function, addition and subtraction functions, shift functions and logical operation functions [11]. It is a part of the TPOCRYPTO subsystem which regroups the AES and PKA cryptographic modules.
- CRC-16 block compliant with ISO/IEC 13239 with additional recommendation in CCITTv41 [12].
- Security sensors.
- True Random Number Generator (TRNG) that meets some of ANSSI requirements (RGS_B1).
- Pseudo Random Number Generator (PRNG)
  - No compliance to any specific metric but PRNG is used by the chip for internal use.

- Shield.
- OTP (One-Time programmable) memory of 128 Kbits.
- RAM of 52 Kbytes.
- Read-Only Memory of 64 Kbytes.
- Reset block.
- Memory controller block (BUS).
- General Purpose Inputs and Outputs (GPI, GPO).
- Memory protection unit (MPU).

20 The TOE directly reads the external memories content, but communicates with the SoC software in order to write and erase.

### 1.2.4 TOE Software

21 The software TOE components are described in the Figure 1-3.

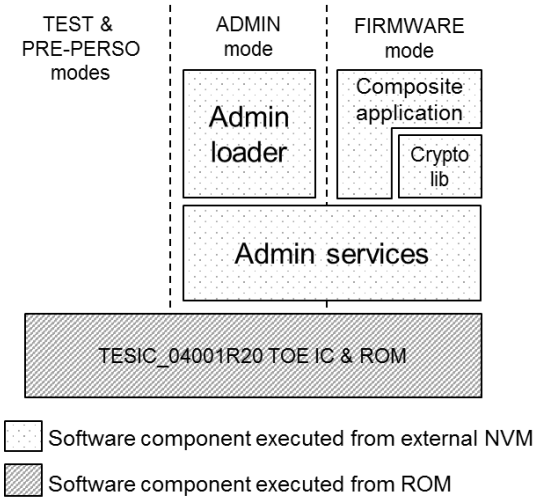


*Figure 1-3 : Software TOE components*

22 The software components contained in the TOE is listed below:

- The IC Dedicated Test software which provides the self-test capabilities and allows to pre-personalize the IC in OTP before the external NVM is available. This software is not available after TOE delivery.
- The IC Dedicated Support Software is part of the TOE. It provides services after TOE delivery and is composed of:
  - The Secure Bootloader used to initialize the product and located in ROM.
  - The RMA domain used as a special diagnostic mode which can be run at every steps of the life cycle to provide failure analysis without modifying the TOE state. The advanced debug capabilities are locked before TOE delivery.
  - The PRE-PERSO loader used to load data and code to RAM, OTP or external memory and switch to the ADMIN mode. The PRE-PERSO software is located in the ROM memory.
  - The Write interface installer is a software loaded by the PRE-PERSO-loader and executed during the load process. It installs the eNVM driver which is used by the loader to write and erase in external flash.

- The AEAD service dedicated to encryption and authentication of data/code which are initially accessed from the external memory. The AEAD service is part IC Dedicated Software written in the ROM memory.
- The ADMIN loader and services (optional) are loaded into the external NVM. The ADMIN loader is used load the composite application in external memory. The ADMIN services are used by both the ADMIN loader and the composite application to protect the external memory against modification, disclosure or roll-back.
- The crypto library (optional). The crypto library is loaded into the external NVM. The software components of the Crypto Library are:
  - The optional secure DRBG library built on top of the TESIC-04001R20 cryptographic coprocessors and TRNG. The DRBG library meets some of the ANSSI requirements (RGS_B1). It provides high level interface functions to perform Random Number Generation:
    - Generation of the internal DRBG seed matching the specified entropy strength.
    - Secure instantiation of a DRBG engine.
    - Secure reseed of a DRBG instance.
    - Secure generation of a pseudo random bit stream from an instantiated DRBG.
    - Release of the resources of a DRBG instance.
  - The optional secure DES library built on top of the TESIC-04001R20 TDES coprocessor and providing the following high-level interface to DES cryptographic algorithms:
    - Secure DES cryptographic encryption or decryption operation in ECB mode.
    - Secure TDEA (triple DES) cryptographic encryption or decryption operation in ECB mode.
    - Secure DES cryptographic encryption or decryption operation in CBC mode.
    - Secure TDEA (triple DES) cryptographic encryption or decryption operation in CBC mode.
  - The optional secure AES library built on top of the TESIC-04001R20 AES coprocessor and providing the following high-level interface to AES cryptographic algorithms:
    - Secure AES cryptographic encryption or decryption operation in ECB mode.
    - Secure AES cryptographic encryption or decryption operation in CBC mode.
    - Secure AES cryptographic encryption or decryption operation in CTR mode.
    - Secure AES cryptographic encryption or decryption operation in CMAC mode.
  - The optional secure RSA library built on top of the TESIC-04001R20 crypto processors and providing high-level interface to RSA cryptographic algorithms. The following RSA interfaces are provided:
    - Secure RSA public and private key pair generation.
    - Secure RSA signature generation using CRT or standard method.
    - Secure RSA signature verification.
    - Secure RSA encryption operation.
    - Secure RSA decryption operation.

- The optional secure ECC library built on top of the TESIC-04001R20 crypto processors and providing high-level interface to ECC cryptographic operations. The following ECC functions are provided:
  - Secure ECC point addition.
  - Secure ECC point scalar multiplication.
  - Secure ECC Diffie-Hellman Key agreement.
  - Secure ECC key pair generation.
  - Secure ECDSA signature generation.
  - Secure ECDSA signature verification.
- The optional secure hash calculation (SHA) library built on top of the TESIC-04001R20 and providing high-level interface to SHA hash algorithms. The following SHA functions are provided:
  - Secure hash calculation according to the SHA2-224.
  - Secure hash calculation according to the SHA2-256.
  - Secure hash calculation according to the SHA2-384.
  - Secure hash calculation according to the SHA2-512.Secure

### 1.2.5 TOE Configuration

23 The Table 1-1 summarizes the hardware, software and guidance documents of the TOE.

| Component | Version | Date |
|---|---|---|
| Hardware, delivered as encrypted GDSII to the manufacturer | | |
| Monarch 2/N – SQN3401 | A1 | 23/05/2020 |
| TESIC-04001R20 Hard Macro | 04001 | 23/05/2020 |
| Software, integrated in ROM memory and delivered in the hardware GDSII | | |
| TESIC-04001R20 Secure Bootloader | 2.0 | 23/05/2020 |
| Software, delivered as Embedded software | | |
| TESIC-04001R20 Admin Loader and services<br>TESIC-04001R20 Write interface installer | 28<br>1.0 | |
| Software, delivered as Embedded software | | |
| TESIC-04001R20 Cryptographic Library | 3.0.F | |
| Guidance, delivered as electronic document | | |
| TESIC-04001R20 - AGD_PRE - Preparative | 1.1 | 22/07/2021 |
| TESIC-04001R20 - AGD_OPE - Operational User Guidance | 1.2 | 16/07/2021 |
| TESIC-04001R20 Hardware User Manual | 1.11 | 08/07/2021 |

| | | |
|---|---|---|
| TESIC-04001R20 Crypto Library User Manual | 3.0.F Rev 1 | 30/07/2021 |
| TESIC-04001R20 Software Development Kit User Manual | 1.1 | 30/07/2020 |
| TESIC-04001R20 TESIC Host Loader User Manual | 1.5 | 06/04/2021 |
| TESIC-04001R20 - Admin Loader User Specification | 1.0 | 22/01/2021 |
| TESIC-04001R20 - AGD_OPE - Developer role | 2.4 | 16/07/2021 |
| TESIC_04001R20 - AGD_OPE - eNVM loader role | 1.4 | 01/07/2021 |
| TESIC_04001R20- AGD_OPE – Package generator role | 1.3 | 11/06/2021 |
| TESIC_04001R20- AGD_OPE – Flash Write interface specification | 1.6 | 28/11/2019 |
| TESIC-04001R20-CL AGD_OPE - Security Guidelines | 1.2 | 11/06/2021 |
| TESIC_04001R20- AGD_OPE ADMIN – Package generator role | 1.3 | 06/07/2021 |
| TESIC_04001R20 ADM - AGD_OPE - Developer role | 1.1 | 02/07/2021 |
| TESIC_04001R20 ADM - AGD_OPE - Loader role | 1.3 | 01/07/2021 |
| TESIC-04001R20 ADMIN services – User guide | 1.1 | 16/04/2021 |
| Monarch N Platform - SQN3410 Chipset - Datasheet | Rev. 2 | January 2020 |

*Table 1-1: Summary of TOE hardware, software and guidance documents*

24 The methods of delivery of the TOE components are the following:

- The crypto library files, composed of header files (.h) and static binary libraries (.a), are compressed (tar.gz), PGP encrypted using the recipient key and signed using the sender PGP key. The software package is then sent by email or pushed to a server.
- The ADMIN loader is packaged in a self-secure load package suitable for being loaded by the TOE in PRE-PERSO mode. It is signed using AES-CMAC and encrypted using AES-CBC, with a key set devoted to each production lot. The self-secure load package is made available using a HSM.
- All user guide and security guidance are delivered as a pdf format, PGP encrypted using the recipient key and signed using the Tiempo sender key. The signed and encrypted documents are then sent by email or pushed to a server.
- The hardware TOE is delivered using standard transportation at the end of phase 4.

25 The Table 1-2 gives the expected values of the TOE hardware identifiers for the TOE Reference TESIC-04001R20-BL2.0-AL28-CL3.0.F.

| Identifier | Expected Value |
|---|---|
| **PRODUCTID** | 0x0400 |
| **MASKID0** | 0x1110 |

| | |
|---|---|
| **MASKID1** | 0x0001 |
| **MASKID2** | 0x5000 |
| **MASKID3** | 0x0005 |
| **JTAGID** | 0x00400AAB |
| **ROM_VERSION** | 0x0002 |

*Table 1-2: TOE Hardware identification*

### 1.2.6 TOE Life Cycle

26 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. The table below details these different phases by giving the companies involved and their locations.

| Phase | Description | Company | Location |
|---|---|---|---|
| Phase 2 | IC Development<br>- IC Design<br>- IC Dedicated Software development.<br>- Integration of the Security enclave into the SoC GDSII | TIEMPO SAS | 110 rue Blaise Pascal<br>Bâtiment Viseo –Inovallée<br>38330 Montbonnot Saint Martin FRANCE<br>T : +33 4 76 61 10 00<br>F : +33 4 76 44 19 69 |
| Phase 3 | IC Manufacturing<br>- Mask preparation<br>- Integration and photo mask fabrication.<br>- IC production | TSMC Fab 14A<br>TSMC Fab 14A<br>TSMC Fab 14A | 1-1, Nan-ke North Road, Tainan Science Park, Shanhua District<br>741-44 Tainan City<br>TAIWAN<br>T : +886 6 505 6688<br>F : +886 6 505 1262 |
| Phase 3 | IC testing<br>- SoC testing | UTAC Singapore<br>SPIL TAIWAN | 5 Serangoon North Ave 5<br>Singapore 554916<br>T:+65 6481 0033<br>No. 19, Keya Rd., Daya, Taichung , Taiwan 428, R. O. C.<br>T: +886 4 2554 5527 |
| Phase 4 | IC Packaging<br>- Security IC packaging<br>- Security enclave testing & Pre personalization | SPIL TAIWAN<br>TIEMPO SAS | No. 19, Keya Rd., Daya, Taichung , Taiwan 428, R. O. C.<br>T: +886 4 2554 5527<br>110 rue Blaise Pascal Bâtiment Viseo –Inovallée 38330 Montbonnot Saint Martin FRANCE<br>T : +33 4 76 61 10 00<br>F : +33 4 76 44 19 69 |
| In addition, four important stages have to be considered in the Composite Product life cycle | | | |
| Phase 1 | Security IC Embedded Software Development. | | |
| Phase 5 | Composite Product Integration.<br>- The Composite Product finishing process, preparation and shipping to the personalization line for the Composite Product | | |

| | | | |
|---|---|---|---|
| Phase 6 | Personalization<br>- The Composite Product personalization and testing stage where the User Data is loaded into the Security IC's memory. | | |
| Phase 7 | Operational Usage<br>- The Composite Product usage by its issuers and consumers which may include loading and other management of applications in the field. | | |

*Table 1-3: TOE engineering Samples Life cycle phases & development location*

27 Figure 1-4 provides an overview of the TOE's engineering sample Life cycle and maps it onto the relevant PP0084 phases [1] as well as the corresponding IC operating modes.

28 This engineering samples life cycle is the temporary life cycle that is assessed in the current evaluation. It is limited to the TOE development and is meant to replace the standard production life-cycle in the short term. A revaluation process is to be expected once the site used for the production life cycle are determined and in place.

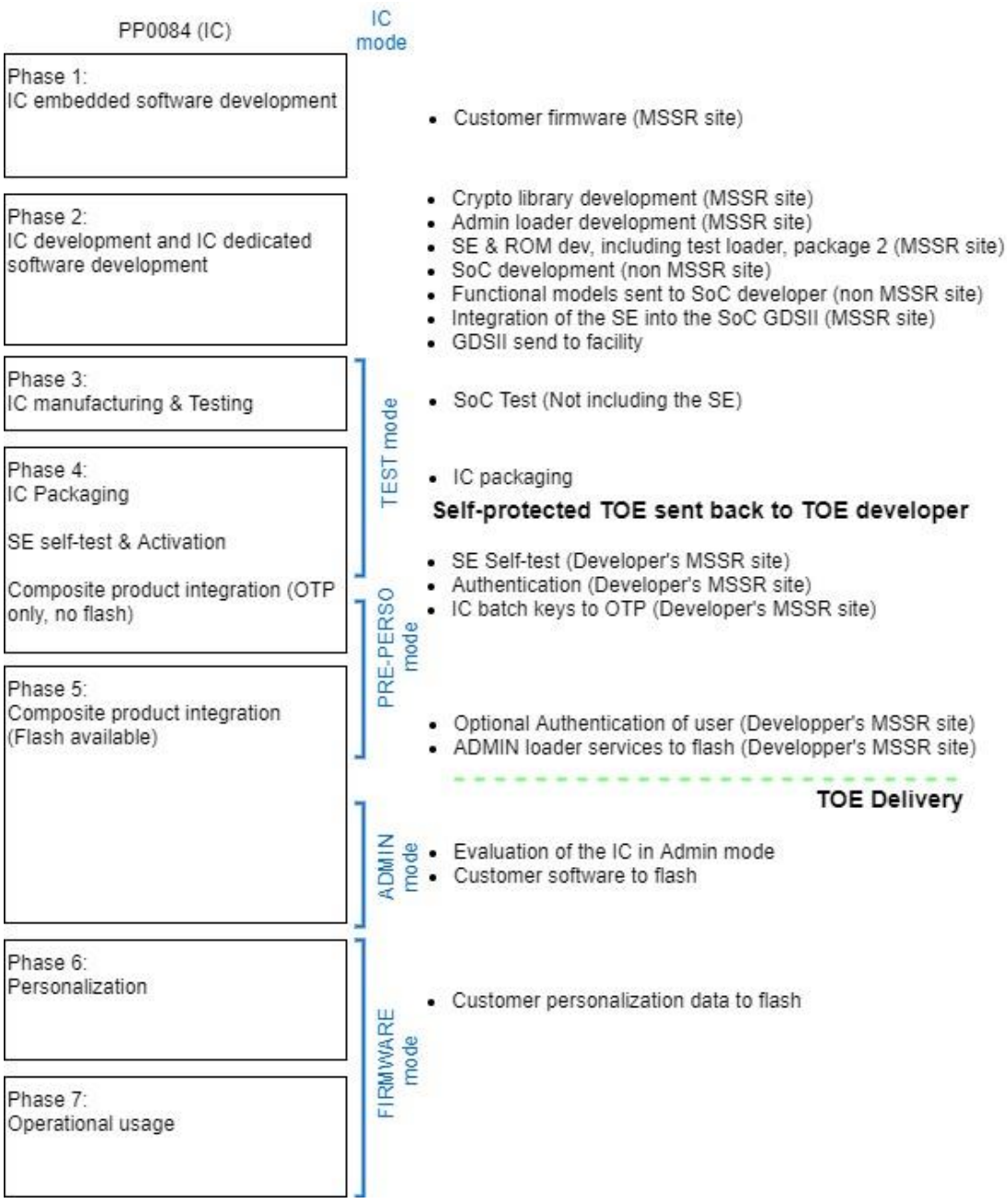


*Figure 1-4: TOE Engineering Samples life cycle*

29 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.

30 In the following the term “TOE Delivery” (refer to Figure 1-4) is uniquely used to indicate:

- during phase 5 when the TOE in Admin mode (as part of the SoC) is delivered in form of packaged products. Indeed, the pre-personalization is performed by the developer and the TOE is delivered in admin mode.

31 The Protection Profile uniquely uses the term “TOE Manufacturer” which includes the following roles:

- the IC Developer (Phase 2),
- the IC Manufacturer (Phase 3) and
- the IC Packaging Manufacturer (Phase 4)

32 Hence the “TOE Manufacturer” comprises all roles beginning with Phase 2 and before “TOE Delivery”. Starting with “TOE Delivery” another party takes over the control of the TOE.

33 The Protection Profile uniquely uses the term “Composite Product Manufacturer” which includes all roles (outside TOE development and manufacturing) except the End-consumer as user of the Composite Product (refer to Figure 1-3) which are the following:

- security IC Embedded Software development (Phase 1).

- the IC Packaging Manufacturer (Phase 4)

if the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice)

- the Composite Product Manufacturer (Phase 5) and the Personaliser (Phase 6).

### 1.2.7 TOE security domains

34 The TOE integrates two separated domains: the RMA domain and the NORMAL domain.

The RMA domain is a domain for test and debug purposes. It implements:

- A diagnostic mode which allows to run self-test procedures at any step of the life cycle. It does not change the internal state of the TOE.
- An advanced diagnostic mode which is only usable by Tiempo. This mode is locked before the TOE delivery.

The NORMAL domain is the default domain which contains several modes:

- TEST mode: this is the first operating mode after manufacturing which allows to test the circuit and run the self-test
- PRE-PERSO mode: this mode is dedicated to loading data and code to OTP or external memory (when available). It is used in phase 4 before TOE delivery for pre-personalization and key provisioning, and after TOE delivery in phase 5 to load the ADMIN loader and switch to ADMIN mode.
- ADMIN mode: this mode aims at loading the firmware to external memory using ADMIN services loaded in PRE-PERSO, and preparing the chip to enter in FIRMWARE mode. The ADMIN services include the secure external memory management which is used by the ADMIN loader to load the data, and then by the loaded firmware to access it.
- FIRMWARE mode: is entered once the ADMIN mode is locked. This mode is the privileged execution mode of the user firmware and is the default mode for the operational use of the composite product.

35 The selection of the operating domain and mode is done at each boot.

36 It is not possible to go back to a previous mode in NORMAL domain.

## 1.3 Interfaces of the TOE

### 1.3.1 Hardware Interfaces

37 The interfaces of the TOE are listed below:

- The electrical interface of the TOE with the external environment consists of the power supply input (Vdd, ground), the 2.3V OTP power supply OTP_HV_2Vx, the enable input of the OTP Macro HDR_EN_2Vx. These inputs are generated by the SoC.
- The data interface of the TOE is made of 4 General Purpose Inputs (GPI), 8 General Purpose Outputs, the AHB-Lite Master Interface, the APB slave interface, the JTAG interface and the ISO7816 contact interface.

### 1.3.2 Software Interfaces

38 The TOE software interfaces consist of interfaces between hardware and software, and interfaces providing high-level security or cryptographic features to the composite software. The Hardware/Software interface is made of interface registers. All TESIC-04001R20 blocks, particularly the crypto-processors, integrate such registers which enable together with software drivers to access into TESIC-04001R20 hardware functions.

39 The TOE software also includes the PRE-PERSO and ADMIN loader command interfaces, and ADMIN services and crypto library API.

40 The interface of the PRE-PERSO loader is made of interpreted commands. These commands are used to load the ADMIN loader and services to external NVM.

41 The interface of the ADMIN loader and services are the following:

- The command interpreter interface of the TOE used to receive user command during the load process
- The ADMIN services interface used secure the storage of the TSF and user data in external memory against disclosure, modification and roll-back attacks. This interface is used by both the ADMIN loader in ADMIN mode to store the ADMIN TSF data and the loaded user data. This services are also available to the user application.

42 The high-level cryptographic software interfaces with the TOE are defined as follows:

- The DRBG interface of the TOE is defined by the DRBG library interface (optional).
- The high-level DES interface of the TOE is defined by the DES library interface (optional).
- The high-level AES interface of the TOE is defined by the AES library interface (optional).
- The RSA interface of the TOE is defined by the RSA library interface (optional).
- The ECC interface of the TOE is defined by the ECC library interface (optional).
- The external memory interface of the TOE (optional).
- The ADMIN loader (optional).

## 1.4 TOE intended Usage

43 Monarch 2/N - SQN3401 is intended to be used for narrowband IoT applications, including sensors, wearables, and other low data, low power M2M and IoT devices.

44 The TOE TESIC-04001R20 is designed to provide security services to the SoC Monarch 2/N - SQN3401.

# 2 Conformance Claims

45 This chapter contains the following sections:

*CC Conformance Claim (2.1)*

*PP* Claim *(2.2)*

*PP Additions (2.3)*

*Package Claim (2.4)*

Conformance Claim Rationale *(2.5)*

46 The TOE has been designed to be compliant with the security requirements of the GSMA composite certification for integrated eUICC.

## 2.1 CC Conformance Claim

47 This Security Target claims to be conformant to the Common Criteria version 3.1 R5, [2], [3], [4] and [5].

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

49 This Security Target has been built with the Common Criteria for Information Technology Security Evaluation; Version 3.1

which comprises

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; April 2017, Version 3.1, Revision 5, CCMB-2017-04-001.

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; April 2017, Version 3.1, Revision 5, CCMB-2017-04-002.

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; April 2017, Version 3.1, Revision 5, CCMB-2017-04-003.

50 The following reference has been taken into account :

[5] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; April 2017, Version 3.1, Revision 5, CCMB-2017-04-004.

## 2.2 PP Claim

51 This Security Target is strictly conformant to the Protection Profile BSI-CC-PP-0084 “Security IC Platform Protection Profile with Augmentation Packages” [1].

52 All refinements described in the Protection Profile BSI-CC-PP-0084 [1] are taken into consideration. In particular the refinements of Security Assurance Requirements ADV_FSP.5 and ALC_CMS.5.

53 The conformance to the following additional packages from BSI-CC-PP-0084 [1] is also claimed:

- Package “Authentication of the Security IC”
- Packages for Loader
  - Package 1: Loader dedicated for usage in secured environment only
  - Package 2: Loader dedicated for usage by authorized users only

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

## 2.3 PP Additions

55 The following security problems, security objectives and security functional requirements have been added:

- T.Mem-Access
- T.Open_Samples_Diffusion
- T.External-Content-Abuse
- T.NVM-Command-Replay
- T.NVM-Unauthorized-Rollback
- T.NVM-Clone-Replace
- T.NVM-Shared-Content-Abuse
- A.Key-Function
- O.Mem-Access
- O.PKA
- O.RSA
- O.ECC
- O.Prot_TSF_Confidentiality
- T.External-Content-Abuse
- T.NVM-Command-Replay
- T.NVM-Unauthorized-Rollback
- T.NVM-Clone-Replace
- T.NVM-Shared-Content-Abuse
- FDP_ACC.1
- FDP_ACF.1
- FMT_MSA.1
- FMT_MSA.3
- FMT_SMF.1
- FDP_RIP.1
- FCS_COP.1/RSA
- FCS_COP.1/ECDSA
- FCS_COP.1/ECDH
- FCS_COP.1/SHA
- FCS_CKM.1/RSA
- FCS_CKM.1/ECDSA
- FDP_URC.1/PM
- FDP_IRA.1/PM
- FPT_RPL.1/PM
- FDP_DAU.2/PM
- FIA_UID.1/PM

## 2.4 Package Claim

56 The assurance level for this Security Target is EAL5+. It includes the assurance level EAL5 augmented with AVA_VAN.5 and ALC_DVS.2.

57 The Protection Profile [1] enables the TOE to be evaluated above the EAL4+, therefore the fact that this Security Target addresses the EAL5+ level still maintains the conformance claims to Protection Profile [1]. The rationale is given in section 4.4 and section 6.3.

## 2.5 Conformance Claim Rationale

58 This Security Target claims strict conformance to only one Protection Profile, the Security IC Platform Protection Profile BSI-CC-PP-0084 [1].

59 The Evaluation Assurance Level (EAL) of the Protection Profile [1] is EAL4 augmented with the assurance components ALC_DVS.2 and AVA_VAN.5. The Assurance Requirements of the TOE obtain the Evaluation Assurance Level 5 augmented with the assurance components ALC_DVS.2 and AVA_VAN.5.

60 The Target of Evaluation (TOE) is a complete solution implementing a security integrated circuit (security IC) as defined in the Protection Profile [1] section 1.3.1, so the TOE is consistent with the TOE type defined in [1].

61 The security problem definition of this Security Target is consistent with the statement of the security problem definition in the Protection Profile [1].

62 The security objectives of this Security Target are consistent with the statement of the security objectives in the Protection Profile [1].

63 The differences between this Security Target and the Protection Profile BSI-CC-PP0084 [1] that is the addition of:

- Threats
- Organizational Security Policy
- Assumption
- Security Objectives for the TOE
- Security Functional Requirements for the TOE

do not affect the conformance claims of this Security Target. The Rationale for these additions is given in section 5.1 of this Security Target.

# 3 Security Problem Definition

64 The chapter 3 contains the following sections:

*Description of Assets (3.1)*

*Threats (3.2)*

*Organizational Security Policies (3.3)*

*Assumptions (3.4)*

## 3.1 Description of Assets

**Assets regarding the Threats**

65 The assets (related to standard functionality) to be protected are:

- the user data of the composite TOE,
- TSF data including root keys and keys derived from root keys as well as the unique identification of the TOE instances,
- the Security IC Embedded Software, stored and in operation,
- the security services provided by the TOE for the Security IC Embedded Software.

66 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.

67 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.

68 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.

69 The Protection Profile requires the TOE to provide at least one security service: the generation of random numbers by means of a physical Random Number Generator. The annex 7 of Protection Profile BSI-CC-PP-0084 provides packages for typical additional security services. The Security Target may require additional security services as described in these packages 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.

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

SC4 deficiency of random numbers.

71 The TOE uses a passive external NVM for code and data storage, hence, the following security concerns are identified:

SC5 Integrity, Authenticity, Freshness of TOE code when loaded and stored in TOE environment (External Memory and/or Device) and then loaded for execution in TOE

SC6 Integrity, Authenticity, Freshness of TOE data when loaded, stored and updated in TOE environment (External Memory and/or Device) and loaded for execution in TOE

SC7 (o) Confidentiality of TOE code when loaded and stored in TOE environment (External Memory and/or Device) and then loaded for execution in TOE

SC8 (o) Confidentiality of TOE data when loaded, stored and updated in TOE environment (External Memory and/or Device) and loaded for execution in TOE

SC9 Confidentiality of TOE data during TOE usage observed at TOE environment level (by logical or physical observation using SoC)

72 Also, in the context of a System-On-Chip product, the following security concern is identified:

SC10 Isolation of TOE execution from perturbation induced in TOE environment and especially in SoC

73 To be able to protect these assets (SC1 to SC10) 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,
- Initialization Data and Pre-personalization Data, specific development aids, test and characterization related data, material for software development support, and photo masks.

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

75 Note that there are many ways to manipulate or disclose the User Data: (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 security functionality. The knowledge of this information enables or supports attacks on the assets. Therefore, the TOE Manufacturer must ensure that the development and production of the TOE is secure so that no restricted, sensitive, critical or very critical information is unintentionally made available for the operational phase of the TOE.

76 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.

77 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, Initialization Data and Pre-personalization Data,
- specific development aids,
- test and characterization related data,
- material for software development support,
- photo masks and products in any form,

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

## 3.2 Threats

78 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 realistically 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.

79 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.

80 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.

81 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 (refer to Section 3.4). In addition, the personalization process supported by the Security IC Embedded Software (and perhaps by the Security IC in addition) must be secure (refer to Section 3.4). This last step is beyond the scope of the Protection Profile. 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 the Protection Profile (Security IC) and those being subject to the evaluation of the Security IC Embedded Software or Security IC and the corresponding personalization process. Therefore, functional cloning is indirectly covered by the security concerns and threats described below.

82 The high-level security concerns are refined below by defining threats as required by the Common Criteria (refer to Figure 3-1). Note that manipulation of the TOE is only a means to threaten user data is not a success for the attacker in itself.

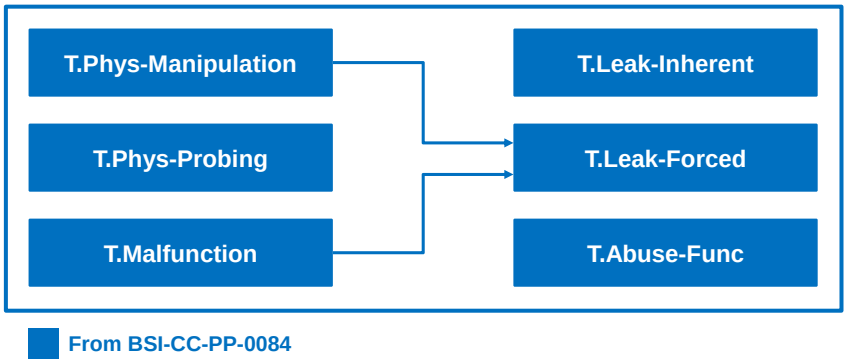


*Figure 3-1: Standard Threats*

83 The high-level security concern related to specific security service is refined below by defining threats as required by the Common Criteria (refer to Figure 3-2).

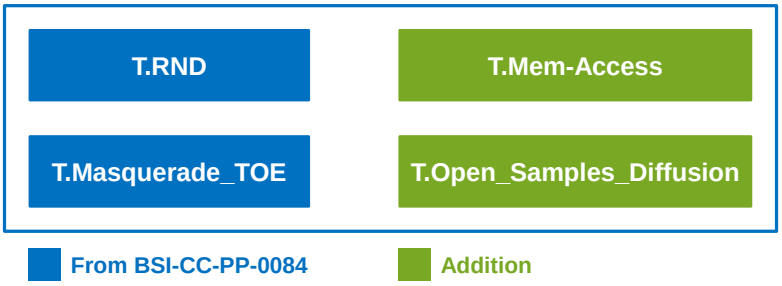


*Figure 3-2: Threats related to security service*

84 The Security IC Embedded Software may be required to contribute to averting the threats. At least it must not undermine the security provided by the TOE. For detail refer to the assumptions regarding the Security IC Embedded Software specified in Section 122.

85 The above security concerns are derived from considering the operational usage by the end-consumer (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 organizational security policy.

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

87 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 visualized in Figure 3-3. Due to the intended usage of the TOE all interactions are considered as possible.

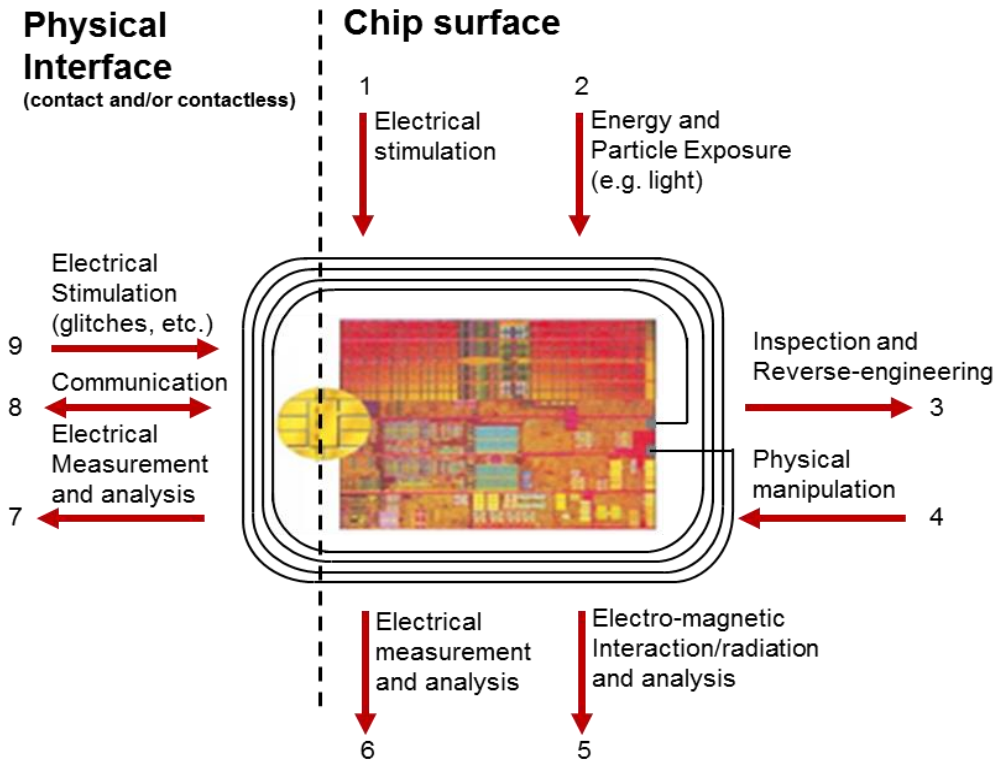


*Figure 3-3: Interactions between the TOE and its outer world*

88 An interaction with the TOE can be done through the physical interfaces (Number 7–9 in Figure 3-3) which are realized using the contact interface. Influences or interactions with the TOE also occur through the chip surface (Number 1–6 in Figure 3-3). 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

89 The TOE shall avert the threat “Inherent Information Leakage (T.Leak-Inherent)” as specified below.

| | |
|---|---|
| T.Leak-Inherent | Inherent Information Leakage<br><br>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. |

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 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 3-3) or measurement of emanations (Number 5 in Figure 3-3) and can then be related to the specific operation being performed.

90 The TOE shall avert the threat “Physical Probing (T.Phys-Probing)” as specified below.

| | |
|---|---|
| T.Phys-Probing | Physical Probing<br><br>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. |

Physical probing requires direct interaction with the Security IC internals (Numbers 5 and 6 in Figure 3-3). 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 3-3). Determination of software design including treatment of user data of the Composite TOE may also be a prerequisite.

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.

91 The TOE shall avert the threat “Malfunction due to Environmental Stress (T.Malfunction)” as specified below.

| | |
|---|---|
| T.Malfunction | Malfunction due to Environmental Stress<br><br>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 3-3). |

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.

92 The TOE shall avert the threat “Physical Manipulation (T.Phys-Manipulation)” as specified below.

| | |
|---|---|
| T.Phys-Manipulation | Physical Manipulation<br><br>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. |

The modification may be achieved through techniques commonly employed in IC failure analysis (Numbers 1, 2 and 4 in Figure 3-3) and IC reverse engineering efforts (Number 3 in Figure 3-3). 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.

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 3-3).

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

| | |
|---|---|
| T.Leak-Forced | Forced Information Leakage<br><br>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. |

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 3-3) which normally do not contain significant information about secrets.

94 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 user data of the Composite TOE or the Security IC Embedded Software.

### 3.2.2 Threats related to security services

95 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

96 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 Security IC 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 Security 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 th/e 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

97 The TOE shall avert the additional threat “Masquerade the TOE (T.Masquerade-TOE)” as specified below.

| | |
|---|---|
| T.Masquerade-TOE | Masquerade the TOE<br><br>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 flash ICs'

98 The TOE shall avert the additional threat “Diffusion of Open Samples (T.Open_Samples_Diffusion)” as specified below.

| | |
|---|---|
| T.Open_Samples_Diffusion | Diffusion of Open Samples<br><br>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 behaviour of the IC and its security functionalities (for example: characterization of side channel profiles, perturbation cartography…). The execution of 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. |

### 3.2.6 Threats related to architectures with passive external NVMs

99 As described in 1.2.2, the TOE uses a passive external NVM. Hence, The Security IC is entirely in charge of protecting the confidentiality and integrity of the contents stored in the passive external NVM or in transit through the interconnection bus, as well as protecting against replay attacks. This implies parrying several threats which will list in what follows.

100 The TOE shall avert the threat “Unauthorized abuse of NVM content (T.External-Content-Abuse)”, as specified below.

| | |
|---|---|
| T.External-Content-Abuse | Unauthorized access of NVM contents.<br><br>An attacker may attempt to access for disclosing or modifying the contents of the passive external NVM. |

101 An attacker may obtain direct access to the passive external NVM and attempt to access the contents stored to disclose or modify it. Consequently, the TOE must ensure that confidentiality of contents is guaranteed before contents (TSF code and TSF data) are serialized into the passive external NVM, and that integrity of contents (TSF code and TSF data) is verified when contents are deserialized from the passive external NVM.

102 The TOE shall avert the threat “Replay of commands between the host MCU and the passive external NVM (T.NVM-Command-Replay)” as specified below.

| | |
|---|---|
| T.NVM-Command-Replay | Replay of commands between the host MCU and the passive |

| | |
|---|---|
| | external NVM<br><br>An attacker may attempt to replay the write and erase commands or responses to the read commands between the host MCU and the passive external NVM, to affect the freshness of the contents read from or written to the external NVM. |

103 The read, write and erase commands issued by the TOE to exercise the storage functionality of the external memory, and their payloads, can be intercepted by an attacker (e.g. eavesdrop the commands on the link between the TOE and the external memory). Such attacker may use copies of these commands to try to misuse the TOE or compromise data. The command replay attack can take the following forms:

- The attacker reacts on a read command and replies a previously recorded answer e.g. to a previous read request. Thereby the TOE gets an old version of such content.
- The attacker issues a previous write command, trying to overwrite the external memory with the previous content, leading to the TOE obtaining old versions of such content in later read operations.
- The attacker issues a previous erase command, trying to overwrite status information or other data that may lead to misuse for the TOE.

104 The TOE shall avert the threat “Unauthorized rollback of NVM contents (T.NVM-Unauthorized-Rollback)”, as specified below.

| | |
|---|---|
| T.NVM-Unauthorized-Rollback | Unauthorized rollback of NVM contents to a previous version<br><br>An attacker may attempt to read the contents of the passive external NVM, record them, and later write them back to the passive external NVM after the original contents were updated by the host MCU. |

105 This threat takes advantage of the fact that the passive external NVM is not integrated into the host MCU chip. Hence, the physical protections for preventing the replacement of stored contents may not cover the passive external NVM. This situation enables an attacker to read and write the contents of the passive external NVM. Even when the NVM contents are protected in confidentiality and integrity, the replacement may be valid as well, since it is retrieved from the passive external NVM.

106 Since TSF code is stored in the passive external NVM, this threat may lead to an unauthorized rollback of the TSF code to an older version. Similarly, overwriting the NVM with an older version of TSF data (partially or fully) might affect the behaviour of the TSF.

107 The TOE shall avert the threat “Cloning or replacement of NVM (T.NVM-Clone-Replace)”, as specified below.

| | |
|---|---|
| T.NVM-Clone-Replace | Cloning or replacement of NVM<br><br>An attacker may attempt to clone the full contents of the passive external NVM of the TOE and write them to the passive external NVM of a different TOE unit; alternatively, an attacker may physically replace the NVM of a TOE with a different NVM that may come from a different TOE unit. |

108 This threat refers to the case where the full contents of the passive external NVM are cloned to a different device. It can also cover the replacement of the NVM of the TOE with the NVM of a different unit. The second case might not be viable on some architectures when the physical design or assembling procedures impede it.

109 The effect of this threat is in replacing the data or code of a TOE with a different one.

110 Unlike T.NVM-Unauthorized-Rollback, the threat of T.NVM-Clone-Replace involves using two different TOE units or instances. One TOE unit is used as a source for the passive external NVM contents. Those contents are used to replace the genuine contents of the external NVM of the second TOE unit.

111 Another possible scenario for this threat can be contemplated for passive external non-volatile memory: the external non-volatile memory is replaced with an empty or virgin non-volatile memory, removing the user and TSF data used by the TOE, and possibly forcing the TSF to generate new user and TSF data, potentially affecting the TSF behaviour.

112 The TOE shall avert the threat “Confidentiality of TSF content in shared NVM (T.NVM-Shared-Content-Abuse)”, as specified below.

| | |
|---|---|
| T.NVM-Shared-Content-Abuse | Confidentiality of TSF content in shared NVM<br><br>Other parts of the SoC may attempt to access or modify TSF content that is written in the external NVM |

113 Other parts of the SoC which have access to the shared external NVM may attempt to access TSF code, TSF data or application data that was written by the TOE in the external NVM. This threat covers the confidentiality and integrity requirements of the TSF content w.r.t to access/modification by other parts of the SoC which are allowed to use the external NVM.

## 3.3 Organizational Security Policies

114 The following Figure 3-4 shows the policies applied in this Security Target.

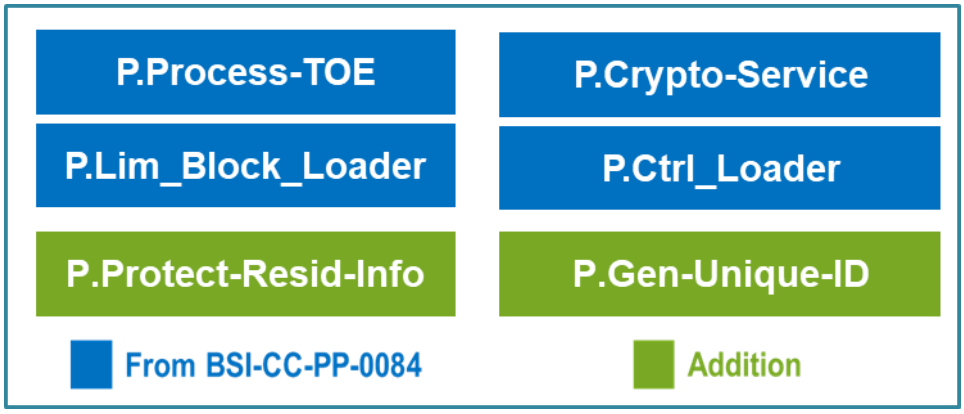


*Figure 3-4: Policies*

115 The IC Developer / Manufacturer must apply the policy “Protection during TOE Development and Production (P.Process-TOE)” as specified below.

| | |
|---|---|
| P.Process-TOE | Protection during TOE Development and Production<br><br>An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification. |

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

117 The groups of information and material processed and/or produced by the TOE manufacturer in the TOE development and production environment (Phase 2 to TOE Delivery) are listed below:

- logical design data,
- physical design data,
- IC Dedicated Software, Initialization Data and Pre-personalization Data,
- specific development aids,
- test and characterisation related data,
- material for software development support,
- photo masks and products in any form,

while they are processed by the TOE Manufacturer.

118 The IC Developer / Manufacturer must apply the organisational security policy “Protection of residual information (P.Protect-Resid-Info)” as specified below.

| | |
|---|---|
| P.Protect-Resid-Info | Protection of residual information<br><br>The TOE shall provide an additional security functionality to the Security IC Embedded Software to ensure the protection of residual information. |

119 The IC Developer / Manufacturer must apply the policy “Cryptographic services of the TOE (P.Crypto-Service)” as specified below.

| | |
|---|---|
| P.Crypto-Service | Cryptographic services of the TOE<br><br>The TOE provides secure hardware based cryptographic services for the IC Embedded Software. |

**Application note:** The TOE shall provide the following security functionality to the Security IC Embedded Software:

Triple Data Encryption Standard (TDES)

Advanced Encryption Standard (AES)

Public Key Accelerator (PKA) supporting Rivest-Shamir-Adleman (RSA) cryptography and Elliptic Curve Cryptography (ECC) in GF(p).

Cryptographic hash functions (SHA2-224, SHA2-256, SHA2-384, SHA2-512).

**Note:** The TOE can be delivered without the RSA/ECC cryptographic library. In this case the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman (RSA) Cryptography and Elliptic Curve Cryptography (ECC).

120 The IC Developer / Manufacturer must apply the policy “Limiting and Blocking the Loader Functionality (P.Lim_Block_Loader)” as specified below.

| | |
|---|---|
| P.Lim_Block_Loader | Limiting and Blocking the Loader Functionality<br><br>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. |

**Application note:** This policy applies to the admin loader.

121 The organisational security policy “Controlled usage to Loader Functionality (P.Ctlr_Loader)” applies to Loader dedicated for usage by authorized users only.

| | |
|---|---|
| P.Ctrl_Loader | Controlled usage to Loader Functionality<br><br>Authorized user controls the usage of the Loader functionality in order to protect stored and loaded user data from disclosure and manipulation. |

122 The organisational security policy “Identification of each TOE instance (P.Gen-Unique-ID)” applies to Loader dedicated for usage in testing and pre-personalization.

| | |
|---|---|
| P.Gen-Unique-ID | Identification of each TOE instance<br><br>An accurate identification must be established for the TOE. The policy requires that each instantiation of the TOE stores its own unique identification. |

## 3.4 Assumptions

123 The following Figure 3-5 shows the assumptions applied in this Security Target.

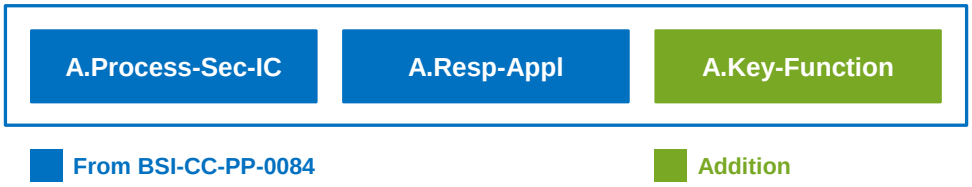


*Figure 3-5: Assumptions*

124 The intended usage of the TOE is twofold, depending on the Life Cycle Phase: (i) The Security IC Embedded Software developer uses it as a platform for the Security IC software being developed (ii) The Composite Product Manufacturer (and the consumer) uses it as a part of the Security IC.

125 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.

126 Appropriate “Protection during Packaging, Finishing and Personalization (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 Personalization<br><br>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 unauthorized use).<br><br>This means that the Phases after TOE Delivery are assumed to be protected appropriately. |

127 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-personalization Data and personalization 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

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

128 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.

129 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 can 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 independent from the evaluation of the Security IC Embedded Software.

130 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<br><br>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. |

131 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.

132 The developer of the Security IC 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<br><br>Key-dependent functions (if any) shall be implemented in the Security IC Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced). |

133 Note that here the routines which may compromise keys when being executed are part of the Security IC 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

134 This chapter Security Objectives contains the following sections:

*Security Objectives for the TOE (4.1)*

*Security Objectives for the Security IC Embedded Software (4.2)*

*Security Objectives for the operational Environment (4.3)*

*Security Objectives Rationale (4.4)*

## 4.1 Security Objectives for the TOE

135 The standard high-level security goals related to the assets are described as followed for the user:

SG1 Maintain the integrity of 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.

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.

136 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 4-1). Note that the integrity of the TOE is a means to reach these objectives.

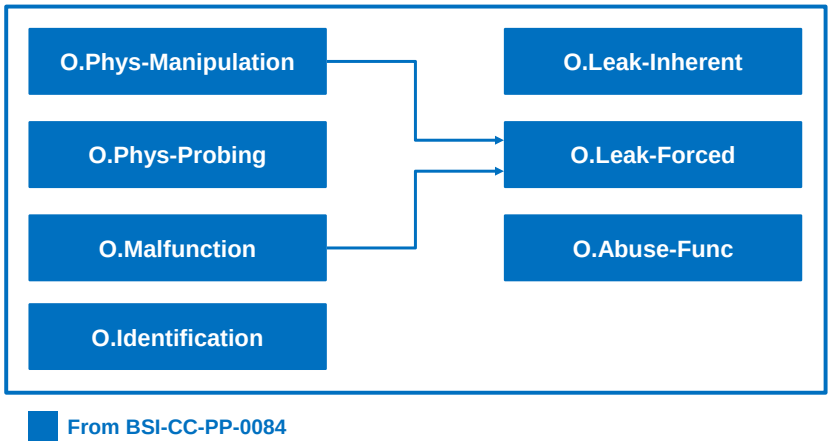


*Figure 4-1: Standard Security Objectives*

137 According to this Security Target there are the following security goals related to TOE architectures using passive external NVM:

SG4 Protect against disclosure and undetected modification of external NVM contents.

SG5 Ensure that the contents stored in the external NVM have not been replaced by a previous version of them.

SG6 Ensure that the contents of the NVM are genuine.

138 According to this Security Target there is the following high-level security goal related to specific functionality:

SG7 Provide true random numbers.

139 The additional high-level security considerations are refined below by defining security objectives as required by the Common Criteria (refer to Figure 4-2).

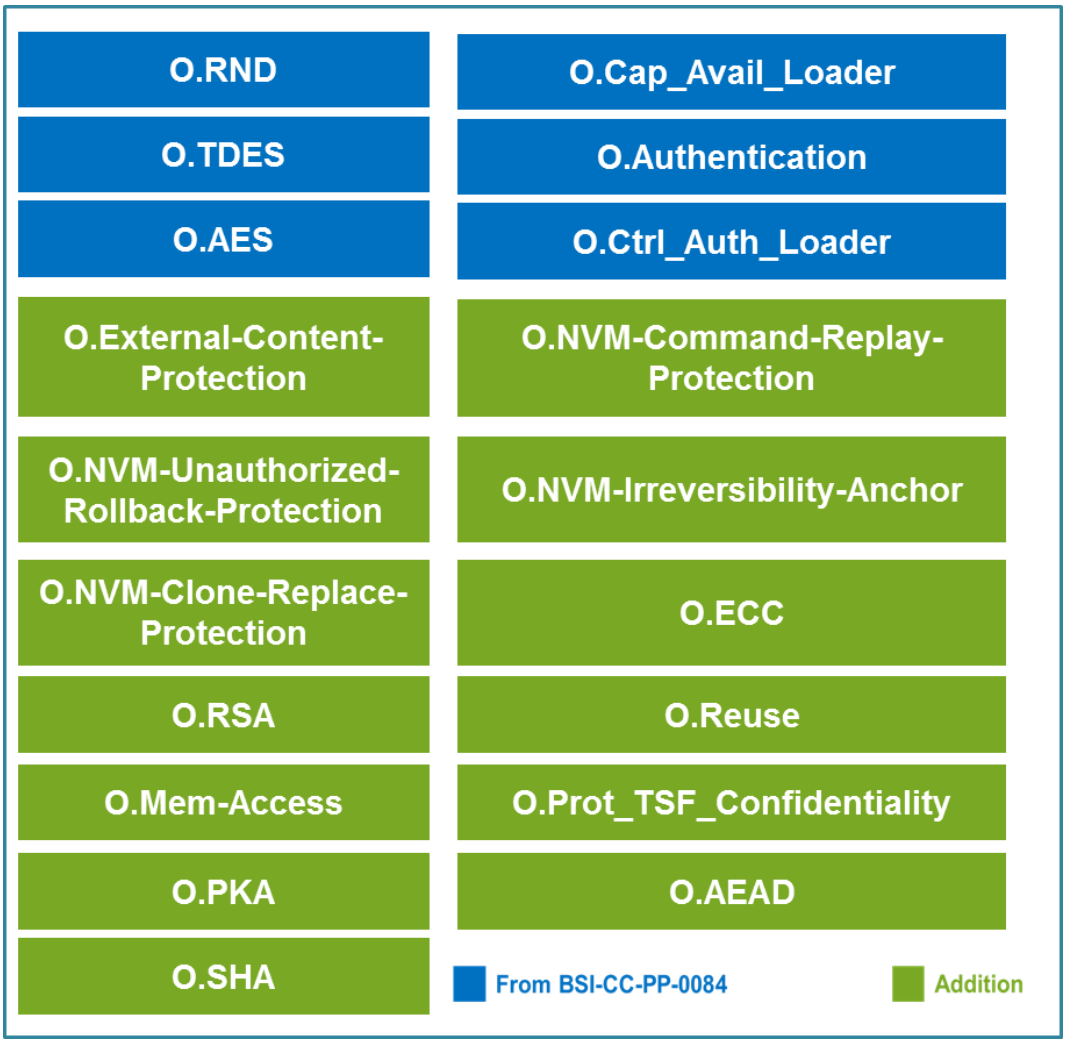


*Figure 4-2: Security Objectives related to Specific Functionality*

**Standard Security Objectives**

140 The TOE shall provide “Protection against Inherent Information Leakage (O.Leak-Inherent)” as specified below:

| | |
|---|---|
| O.Leak-Inherent | Protection against Inherent Information Leakage<br>The TOE must provide protection against disclosure of confidential data stored and/or processed in the Security IC<br>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.

141 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. |

142 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.

143 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 Security IC 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.

144 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<br>- by forcing a malfunction (refer to “Protection against Malfunction due to Environmental Stress (O.Malfunction)” and/or<br>- by a physical manipulation (refer to “Protection against Physical Manipulation (O.Phys-Manipulation)”.<br>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. |

145 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. |

146 The TOE shall provide “TOE Identification (O.Identification)” as specified below:

| | |
|---|---|
| O.Identification | TOE Identification |
| | The TOE must provide means to store Initialization Data and Pre-personalization Data in its non-volatile memory. The Initialization Data (or parts of them) are used for TOE identification. |

**Security Objectives Related to SG.External-Content-Protection (SG4)**

147 The TOE shall provide “Passive External NVM content protection (O.External-Content-Protection)” as specified below:

| | |
|---|---|
| O.External-Content- | Passive External NVM content protection |

| | |
|---|---|
| Protection | Protection against disclosure and undetected modification of external NVM contents. Since an attacker can get direct access to the external NVM, the contents stored in the external NVM must be protected against disclosure and undetected modification.<br><br>This security objective requires protection of the content stored in external memory by the TOE. The protection prevents disclosure and identifies modifications of stored code and data that is not performed by the TOE. |

**Security Objectives Related to SG.NVM-Updated-Contents (SG5)**

148 The TOE shall provide “Protection against replay of commands between host MCU and external NVM (O.NVM-Command-Replay-Protection)”, as specified below:

| | |
|---|---|
| O.NVM-Command-Replay-Protection | Protection against replay of commands between host MCU and external NVM<br><br>The TOE shall protect against replay of the read, write and erase commands issued by the TOE to the external NVM through the interconnection bus.<br><br>This security objective requires protection against replay of read, write and erase operations. This covers simple replay of previously recorded commands or memory content but also the replay of modified commands or memory content. The TOE shall be able to detect such attacks violating the TOE. |

149 The TOE shall provide “Protection against an unauthorized rollback of NVM contents (O.NVM-Unauthorized-Rollback-Protection)”, as specified below:

| | |
|---|---|
| O.NVM-Unauthorized-Rollback-Protection | Protection against an unauthorized rollback of NVM contents<br><br>The TOE shall protect against replacement of the external NVM contents with a previous version, even if it was valid in the past.<br><br>The security objective requires protection against the simulation of outdated memory content. Replacement of memory content with a previous version of the same content or the manipulations of write operations violate the freshness of the external memory content and shall be detected by the TOE |

150 The TOE shall provide “(O.NVM-Irreversibility-Anchor)”, as specified below:

| | |
|---|---|
| O.NVM-Irreversibility-Anchor | Passive External NVM Contents Irreversibility Anchor<br><br>The TOE shall implement a non-volatile mutable mechanism that goes through a predefined sequence of states (that are associated with increasing ‘values’) that can never be returned to a previous state. This value given by a sequence of states shall be used to determine whether the external NVM contents meet the data freshness property and to prevent replay attacks.<br><br>In order to manage data freshness, the TOE shall provide an irreversibility anchor, as described in the above security objective. Advancing the value of the irreversibility anchor through its defined sequence of states mechanism occurs when write/erase operations are issued by the Security IC. This mechanism shall allow detecting and protecting against violation of data freshness of the external NVM contents. |

**Application Note:** This mechanism can be vulnerable to fault injection attacks, e.g. voltage glitches. The attacker may try to prevent the Irreversibility Anchor from incrementing, or alter its perceived value, which would enable the attacker to replay old sessions of commands. These kinds of attack are covered by the T.Malfunction threat defined in [1].

**Security Objectives Related to SG.NVM-Genuine-Content (SG6)**

151 The TOE shall provide “Protection against external NVM cloning or replacement (O.NVM-Clone-Replace-Protection)”, as specified below.

| | |
|---|---|
| O.NVM-Clone-Replace-Protection | Protection against NVM cloning or replacement.<br>The TOE shall protect against cloning the memory contents of another unit into the TOE’s external NVM and against replacement of the external NVM with the one from a different unit.<br>By means of this objective, the TOE shall protect against the replacement of its external NVM contents with ones from a different unit. While those contents are valid for the TOE from where they were extracted, they shall be detected as non-belonging to the TOE unit where they were cloned to and, thus, non-valid. The TOE shall also protect against a similar scenario where, instead of cloning the contents of one NVM into another, the external NVM is physically replaced by the external NVM of a different TOE unit. |

**Security Objectives related to Specific Functionality (referring to SG7)**

152 The TOE shall provide “Random Numbers (O.RND)” as specified below:

| | |
|---|---|
| O.RND | Random Numbers<br>The TOE will ensure the cryptographic quality of random number generation. For instance, random numbers shall not be predictable and shall have sufficient entropy.<br>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. |

**Security Objectives for Cryptographic Services**

153 The TOE shall provide “Cryptographic service Triple-DES (O.TDES)” as specified below.

| | |
|---|---|
| O.TDES | Cryptographic service Triple-DES<br>The TOE provides secure hardware based cryptographic services implementing the Triple-DES for encryption and decryption. |

154 The security objective “Cryptographic service Triple-DES (O.TDES)” enforces the organizational security policy P.Crypto-Service.

155 The TOE shall provide “Cryptographic service AES (O.AES)” as specified below.

| | |
|---|---|
| O.AES | Cryptographic service AES<br>The TOE provides secure hardware based cryptographic services for the AES for encryption and decryption. |

156 The security objective “Cryptographic service AES (O.AES)” enforces the organizational security policy P.Crypto-Service.

157 The TOE shall provide “Cryptographic service PKA (O.PKA)” as specified below.

| | |
|---|---|
| O.PKA | Cryptographic service PKA<br>The TOE shall provide the following specific security functionality to |

the Security IC Embedded Software:

Public Key Accelerator (PKA) supporting Rivest-Shamir-Adleman (RSA) cryptography and Elliptic Curve Cryptography (ECC) in GF(p).

**Note:** The TOE can be delivered without the RSA/ECC cryptographic library. In this case the TOE does not provide the Additional Specific Security Functionalities Rivest-Shamir-Adleman (RSA) Cryptography and Elliptic Curve Cryptography (ECC).

158 The security objective “Cryptographic service PKA (O.PKA)” enforces the organizational security policy P.Crypto-Service.

159 The TOE shall provide “Cryptographic service RSA (O.RSA)” as specified below.

| | |
|---|---|
| O.RSA | Cryptographic service RSA<br>The TOE provides shall provide the following specific security functionality to the Security IC Embedded Software:<br>Rivest-Shamir-Adleman (RSA) public key asymmetric cryptography. |

**Note:** The TOE can be delivered without the RSA cryptographic library. In this case the TOE does not provide the specific security functionalities Rivest-Shamir-Adleman (RSA) Cryptography.

160 The security objective “Cryptographic service RSA (O.RSA)” enforces the organizational security policy P.Crypto-Service.

161 The TOE shall provide “Cryptographic service RSA (O.ECC)” as specified below.

| | |
|---|---|
| O.ECC | Cryptographic service ECC<br>The TOE provides shall provide the following specific security functionality to the Security IC Embedded Software:<br>Elliptic Curve Cryptography (ECC). |

**Note:** The TOE can be delivered without the ECC library. In this case the TOE does not provide the specific security functionalities Elliptic Curve Cryptography (ECC).

162 The security objective “Cryptographic service ECC (O.ECC)” enforces the organizational security policy P.Crypto-Service.

163 The TOE shall provide “Cryptographic service Hash function (O.SHA)” as specified below.

| | |
|---|---|
| O.SHA | Cryptographic service Hash function<br>The TOE provides secure software cryptographic services for secure hash calculation. |

164 The security objective “Cryptographic service Hash function (O.SHA)” enforces the organizational security policy P.Crypto-Service.

**Security Objectives for Added Function**

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

| | |
|---|---|
| O.Mem-Access | Area based Memory Access Control<br>The TOE must provide the Security IC 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.

166 The TOE shall provide "(O.Reuse)" as specified below.

| | |
|---|---|
| O.Reuse | Cryptographic reuse of memory<br>The TOE shall provide the measures to ensure that the memory resources being used by the TOE for the Crypto Library cannot be disclosed to subsequent users of the same memory resource. |

167 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<br>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. |

168 The TOE shall provide "Authentication to external entities (O.Authentication)" as specified below:

| | |
|---|---|
| O.Authentication | Authentication to external entities<br>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. |

169 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<br>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. |

170 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<br>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

171 The development of the Security IC Embedded Software is outside the development and manufacturing of the TOE (cf. section 1.2.6). The Security IC Embedded Software development defines the operational use of the TOE. This section describes the security objectives for the Security IC Embedded Software development.

172 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.

**Phase 1**


*Figure 4-3: Security Objectives for the Security IC Embedded Software development environment*

173 The Security IC Embedded Software shall provide “Treatment of User Data (OE.Resp-Appl)” as specified below.

| | |
|---|---|
| OE.Resp-Appl | Treatment of user data of the Composite TOE<br><br>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.<br><br>For example, the Security IC Embedded Software will not disclose security relevant user data of the Composite TOE to unauthorized users or processes when in operation. |

### 4.2.1 Clarification of “Treatment of User Data (OE.Resp-Appl)”

174 User Data are defined but not limited to cipher or plain text data and cryptographic keys. These data shall be manipulated appropriately by the Security IC Embedded Software. Secret keys used as input for the cryptographic function of the TOE shall be chosen carefully in order to ensure the strength of cryptographic operation.

175 Keys are defined and must be treated as confidential data which must be unique with high entropy. The environment shall integrate appropriate key management for manipulating keys (for example the importation of keys into TOE and/or the derivation from other keys).

176 If the Embedded Software of the TOE integrates multi-application operating systems, user data shall be treated carefully. The Multi-application operating system should not disclose security relevant user data of one application to another application.

## 4.3 Security Objectives for the operational Environment

**TOE Delivery up to the end of Phase 6**

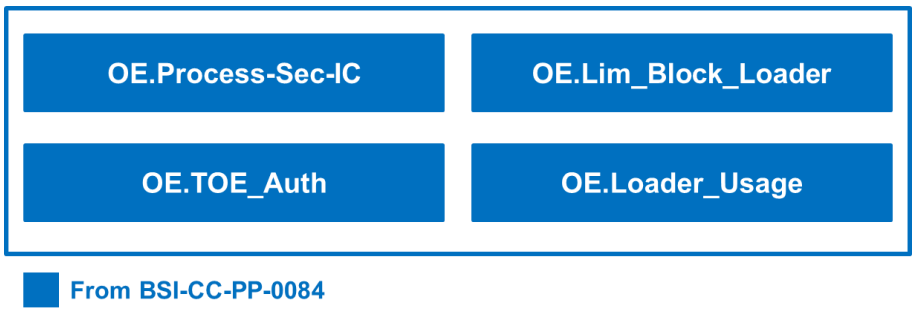


*Figure 4-4: Security Objectives for the operational Environment*

### 4.3.1 "Protection during Packaging, Finishing and Personalization (OE.Process-Sec-IC)"

177 Appropriate "Protection during Packaging, Finishing and Personalization (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<br><br>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 unauthorized use).<br><br>This means that Phases after TOE Delivery up to the end of Phase 6 (refer to section 1.2.6) must be protected appropriately. For a preliminary list of assets to be protected refer to Section 122. |

178 The pre-personalisation environment shall ensure "Uniqueness and authenticity of the device individual identifier" (OE.Secure-Initialisation).

| | |
|---|---|
| OE.Secure-Initialisation | Uniqueness and authenticity of the device individual identifier<br><br>Security procedures shall be applied during the initialisation of the TOE to ensure that each device is loaded with an individual identifier. The identifier shall allow the unique identification of each device in later life cycle phases. |

179 Phases after the initialisation can use the individual identify for tracking and further provisioning. Depending on the application context, the tracking may not be possible in the operational phase of the TOE.

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

180 The personalization process and the personalization of data happening during phase 4, 5 and 6 of life cycle, shall be protected as the packaging, finishing and personalization phases are protected.

181 Measures assumed in A.Process-Sec-IC should be implemented by the Composite Product Manufacturer according to requirement of OE.Process-Sec-IC. This objective covers this assumption.

### 4.3.3 "Limitation of capability and blocking the Loader (OE.Lim_Block_Loader)"

182 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<br><br>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. |

183 Note: The Loader is intended to be used from phase 3 to 5 of the life cycle.

#### 4.3.4 Clarification of "Limitation of capability and blocking the Loader (OE.Lim_Block_Loader)"

184 The Loader functionality during phases 3 to 5 shall be protected against misuse. Measures assumed in P.Lim_Block_Loader should be implemented by the Composite Product Manufacturer according to requirement of OE.Lim_Block_Loader and O.Cap-Avail-Loader.

185 Note: To maintain the confidentiality of the data of the Composite TOE, the intended usage of the Loader is limited to the phases 3 to 5 of the life cycle.

#### 4.3.5 "External entities authenticating of the TOE (OE.TOE_Auth)"

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

| | |
|---|---|
| OE.TOE_Auth | External entities authenticating of the TOE<br>The operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE. |

187 The justification of the additional policy and the additional assumption show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there.

#### 4.3.6 "Secure communication and usage of the Loader (OE.Loader_Usage)"

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

| | |
|---|---|
| OE.Loader_Usage | Secure communication and usage of the Loader<br>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. |

## 4.4 Security Objectives Rationale

189 Table 4-1 below gives an overview, how the assumptions, threats, and organizational security policies are addressed by the objectives. The text following after the table justifies this in details.

| Assumption, Threat or Organizational 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.Abuse-Func | O.Leak-Forced | |
| T.RND | O.RND | |
| T.Mem-Access | O.Mem-Access | |
| P.Protect-Resid-Info | O.Reuse | |
| P.Crypto-Service | O.TDES<br>O.AES<br>O.PKA<br>O.RSA<br>O.ECC<br>O.SHA | |
| A.Key-Function | OE.Resp-Appl | |
| P.Lim_Block_Loader | O.Cap_Avail_Loader<br>OE.Lim_Block_Loader | Phases 3 to 6 |
| T.Masquerade_TOE | O.Authentication<br>OE.TOE_Auth | |
| T.Open_Samples_Diffusion | O.Prot_TSF_Confidentiality<br>O.Leak-Inherent<br>O.Leak-Forced | |
| P.Ctrl_Loader | O.Ctrl_Auth_Loader<br>OE.Loader_Usage | Phases 3 to 5 |
| P.Gen-Unique-ID | OE.Secure-Initialisation | Phases 3 to 5 |
| T.External-Content-Abuse | O.External-Content-Protection | Phases 5 to 7 |
| T.NVM-Command-Replay | O.NVM-Command-Replay-Protection<br>O.NVM-Irreversibility-Anchor | Phases 5 to 7 |
| T.NVM-Unauthorized-Rollback | O.NVM-Unauthorized-Rollback-Protection<br>O.NVM-Irreversibility-Anchor | Phases 5 to 7 |
| T.NVM-Clone-Replace | O.NVM-Clone-Replace-Protection | Phases 5 to 7 |
| T.NVM-Shared-Content-Abuse | O.External-Content-Protection | Phases 5 to 7 |

*Table 4-1: Security Objectives versus Assumptions, Threats or Policies*

190 The justification related to the assumption “Treatment of User Data (A.Resp-Appl)” is as follows:

191 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.

192 The justification related to the organizational security policy “Protection during TOE Development and Production (P.Process-TOE)” is as follows:

193 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 organizational 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 Section 3.1. All listed items and the associated development and production environments are subject of the evaluation. Therefore, the organizational security policy P.Process-TOE is covered by this objective, as far as organizational measures are concerned.

194 The justification related to the assumption “Protection during Packaging, Finishing and Personalization (A.Process-Sec-IC)” is as follows:

195 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.

196 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:

197 For all threats the corresponding objectives (refer to Table 4-1) are stated in a way, which directly corresponds to the description of the threat (refer to Section 3.2). It is clear from the description of each objective (refer to Section 4.1), 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.

198 The threat “Memory Access Violation (T.Mem-Access)” is justified as follows: the TOE must enforce the partitioning of the memory areas and must control its accesses. The Security IC Embedded Software must define restrictions so that accidental or deliberate security violation access to restricted memory area shall be prevented (T.Mem-Access). Therefore, the threat T.Mem-Access is eliminated when the objective O.Mem-Access is achieved.

199 The Security IC Embedded Software should implement the memory management mechanism exploiting appropriately TSF. This assertion is clarified in T.Mem-Access and O.Mem-Access. The TOE makes available to Security IC Embedded Software access control functions. Clarification "Treatment of User Data (OE.Resp-Appl)” emphasizes this point by reminding that the Security IC Embedded Software must not bypass access memory restrictions. This clarification allows covering the threat T.Mem-Access.

200 The Security Objective O.Reuse covers the Organisational Security Policy P.Protect-Resid-Info because it requires the TOE to partially implement functionality to provide protection of residual information as required by the Security Policy.

201 The justification related to the security objectives “Cryptographic service TDES (O.TDES)”, “Cryptographic service AES (O.AES)”, “Cryptographic service PKA (O.PKA)”, “Cryptographic service RSA (O.RSA)” , “Cryptographic service ECC (O.ECC)” and “Cryptographic service Hash function (O.SHA)” is as follows:

202 Since the objectives O.TDES, O.AES, O.PKA, O.RSA, O.ECC and O.SHA require the TOE to implement exactly the same specific security functionality as required by P.Crypto-Service, the organizational security policy is covered by these objectives.

203 The implementation of the specific security functionality required by P.Crypto-Service is defined by the following security objectives: O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced. As expected from P.Crypto-Service and described in these objectives, the specific security functionality is provided in a secure way. In general, the protection of confidential data (User data or TSF data) is referred in O.Leak-Inherent and O.Leak-Forced. P.Crypto-Service require specific security functions which enable to process User data.

204 The clarification has been made for the security objective “Treatment of User Data (OE.Resp-Appl)”. The Security IC Embedded Software will protect User data such as cipher, plain text and cryptographic keys if required by using secured functions for ensuring the security of cryptographic operations. Secure mechanism in the environment must be used for the management of keys or derived keys. This is supported by the assumption A.Key-Function

covered by OE.Resp-Appl. Therefore, the assumption A.Key-Function is covered by the objective OE.Resp-Appl.

205 The organizational 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.

206 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.

207 The justification related to the threat "Diffusion of Open Samples (T.Open_Samples_Diffusion)" is as follows:

208 The authentication required before having access to the Loader ensures the TOE is self-protected at delivery point. The threat "Diffusion of Open Samples is then removed if the following objectives are valid: "Protection of the confidentiality of the TSF (O.Prot_TSF_Confidentiality)", "Protection against Inherent Information Leakage (O.Leak-Inherent)" and "Protection against Forced Information Leakage (O.Leak-Forced)".

209 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 usage of the Loader (OE.Loader_Usage)".

210 T.External-Content-Abuse is countered by O. External-Content-Protection, which requires the TOE to prevent disclosure and undetected modification of the contents stored in external NVM.

211 T.NVM-Command-Replay is countered by O.NVM-Command-Replay-Protection and O.NVM-Irreversibility-Anchor as follows:

- O.NVM-Command-Replay-Protection requires that the TOE implements protection against the replay of commands between the Security IC and the external NVM through the interconnection bus, mitigating T.NVM-Command-Replay.
- O.NVM-Irreversibility-Anchor requires that the TOE implements a mechanism that goes through a sequence of states associated with the changes issued by the Security IC on the NVM. This mechanism helps for the detection of older NVM commands, as contents of such commands would not meet the requirement of having a consistent value of the irreversibility anchor.

212 T.NVM-Unauthorized-Rollback is countered by O.NVM-Unauthorized-Rollback-Protection and O.NVM-Irreversibility-Anchor as follows:

- O.NVM-Unauthorized-Rollback-Protection requires that the TOE protects against replacement of external NVM contents with older contents of the same NVM, where the data freshness property is not met, thus, mitigating this threat.
- O.NVM-Irreversibility-Anchor requires that the TOE implements a mechanism that goes through a sequence of states associated with the changes issued by the Security IC on the external NVM. Unauthorized rollback of contents of the external NVM would result in a state that would fail the validation against the current value of the irreversibility anchor mechanism.

213 T.NVM-Clone-Replace is countered by O.NVM-Clone-Replace-Protection, which requires the TOE to detect the replacement of the external NVM contents with those of a different TOE's NVM, or physical replacement of the external NVM with the external NVM of a different TOE unit.

214 T.NVM-Shared-Content-Abuse is countered by O.External-Content-Protection which requires the TOE to protect the TSF content written in the external NVM through cryptographic security mechanisms which prevent other parts of the SoC from accessing (read) the TSF content and

prevent any security impact which be due to TSF data being overwritten by other parts of the SoC.

215 The organisational security policy “Identification of each TOE instance (P.Gen-Unique-ID)” is implemented in order to fulfil the security objective “Uniqueness and authenticity of the device individual identifier (OE.Secure-Initialisation)”. Indeed, a unique identification must be stored on each instance of the TOE. Phases after the initialisation can use the individual identify for tracking and further provisioning.

# 5 Extended Components Definition

216 This chapter presents the extended components definition. The extended components include the following components which are introduced in the PP0084 [1]:

- FCS_RNG.1
- FMT_LIM.1
- FMT_LIM.2
- FAU_SAS.1
- FDP_SDC.1
- FIA_API.1

217 The components listed in 216 are defined in the PP0084 [1].

218 Additionally, the following extended components are introduced:

- FDP_URC.1
- FDP_IRA.1

## 5.1 Definition of the Family FDP_URC

219 To define the security functional requirements of the TOE, an additional family (FDP_URC) of the Class FDP (User data protection) is defined here.

220 This family describes the functional requirements for the detection of unauthorized rollback of the contents stored in the external NVM. An unauthorized rollback situation occurs when the contents of the external NVM are replaced with other previous contents of the same NVM that were valid at a certain moment in the past. The unauthorized rollback is understood as a full replacement of external NVM contents with previous valid contents, or partial content replacement.

221 The family “Protection against an unauthorized rollback of stored contents (FDP_URC)” is specified as follows:

**FDP_URC: Protection against an unauthorized rollback of stored contents**

Family behaviour

This family defines functional requirements for the detection of an unauthorized rollback of contents stored in the external NVM.

Component levelling:

| | |
|---|---|
| FDP_URC.1 Protection against an unauthorized rollback of stored contents | 1 |

| | |
|---|---|
| FDP_URC.1 | Requires the TOE to protect against an unauthorized rollback of the contents stored in the external NVM. |
| Management: | FDP_URC.1<br>There are no management activities foreseen. |
| Audit: | FDP_URC.1 |

There are no actions defined to be auditable.

| | |
|---|---|
| **FDP_URC.1** | **Protection against an unauthorized rollback of stored contents** |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FDP_URC.1.1 | The TOE shall detect an unauthorized replacement of the contents stored in the external NVM before the contents are used. The detection shall take place even if the contents were previously stored in the same NVM and were valid and consistent at a given past time. |
| FDP_URC.1.2 | Upon detection of unauthorized rollback of external NVM contents, the TOE shall [selection: stop TOE operation, [assignment: other actions]]. |

## 5.2 Definition of the Family FDP_IRA

222 To define the security functional requirements of the TOE, an additional family (FDP_IRA) of the Class FDP (User Data Protection) is defined here.

223 This family describes the functional requirements for the implementation of an irreversibility anchor mechanism linked to the data freshness property for the contents of the external NVM. The external NVM irreversibility anchor mechanism consists of a non-volatile mutable mechanism that goes through a predefined sequence of states (that are associated with increasing values). These values are increasing and cannot revert to previous states. They serve to determine whether the contents of the NVM meet the property of data freshness, by verifying that they are those resulting from the latest write or erase operation issued by the Security IC on the external NVM. Otherwise, the data freshness property is not met, and this mechanism serves to prevent or detect it.

224 The family FDP_IRA aims to cover the requirements associated with the above problem, providing the ability to prevent or detect the scenario of external NVM contents not being fresh.

225 The family “Irreversibility Anchor of NVM contents (FDP_IRA)” is specified as follows:

**FDP_IRA: Irreversibility Anchor of NVM contents**

Family behaviour

This family defines functional requirements for the implementation of a non-volatile mutable irreversibility anchor that goes through a series of predefined states in an irreversible way, i.e., without the possibility of going back to previous states. The irreversibility anchor value resulting from its state is linked to the data freshness of the external NVM contents. Violating data freshness property of the external NVM contents would result in a non-concordance of the value of the irreversibility anchor with the contents retrieved from the external NVM. Therefore, this mechanism serves to maintain the data freshness of the external NVM contents.

Component levelling:

| | |
|---|---|
| FDP_IRA.1 Irreversibility Anchor of NVM Contents | 1 |

| | |
|---|---|
| Management: | FDP_IRA.1<br>There are no management activities foreseen. |
| Audit: | FDP_IRA.1<br>There are no actions defined to be auditable. |
| **FDP_IRA.1** | **Irreversibility Anchor of NVM contents** |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FDP_IRA.1.1 | The TOE shall implement a non-volatile irreversibility anchor mechanism that maintains a value that goes through a predefined sequence of states without the possibility of reversion to a previous state. The state of the Irreversibility Anchor is used to verify that NVM contents preserve data freshness as follows: [selection, choose one of:<br>- Its value is (1) associated to the state of the external NVM contents, (2) advanced to the next state before contents are updated by the host MCU, and (3) checked to determine if the external NVM contents are fresh before they are used;<br>- Its value is (1) associated to sequences of commands or individual commands sent by the host MCU to the external NVM, (2) advanced to the next state before each command or sequence of commands are issued by the host MCU to the external NVM and (3) checked to determine if command contents are fresh when a command is issued;<br>- [assignment: other option]].<br>[assignment: indication of in which way the irreversibility anchor serves to determine that external NVM contents meet data freshness]. |
| FDP_IRA.1.2 | Upon detection of unauthorized rollback of external NVM contents, the TOE shall [selection: stop TOE operation, [assignment: other actions]]. |
| ***Application Note:*** | *The TSF related to this mechanism can be implemented in multiple ways. Typical architectures include:*<br>*- A protected field in an internal memory of the Security IC, e.g., an effuse array, an EEPROM variable, etc.*<br>*- A mechanism in the external NVM (in case it implements any TSF), e.g., a dedicated Flash array programmed bit-by-bit, etc.*<br>*The above implementation mechanisms are illustrative, and the possible implementation options are not limited to them.* |

# 6 IT Security Requirements

226 The chapter IT Security Requirements describes the security functional requirements for the TOE (6.1), the TOE assurance requirements (6.2) and the security requirement rationale (6.3) as required in [1].

## 6.1 Security Functional Requirements for the TOE

227 A summary of the Security Functional Requirements for the TOE is given in Table 6-1.

| # | Security Functional Requirements | | Origin of the SFR | Threats or policies |
|---|---|---|---|---|
| **1** | **FRU_FLT.2** | Limited fault tolerance | BSI-CC-PP-0084 | T.Malfunction<br>T.Leak-Forced<br>T.Abuse-Func<br>T.RND |
| **2** | **FPT_FLS.1** | Failure with preservation of secure state | BSI-CC-PP-0084 | T.Malfunction<br>T.Leak-Forced<br>T.Abuse-Func<br>T.RND |
| **3** | **FMT_LIM.1** | Limited capabilities | BSI-CC-PP-0084 (extended component) | T.Abuse-Func |
| **4** | **FMT_LIM.2** | Limited availability | BSI-CC-PP-0084 (extended component) | T.Abuse-Func |
| **5** | **FAU_SAS.1** | Audit storage | BSI-CC-PP-0084 (extended component) | P.Process-TOE |
| **6.1** | **FDP_SDC.1/IM** | Stored data confidentiality for internal memories | BSI-CC-PP-0084 (extended component) | T.Phys-Probing<br>T.Phys-Manipulation |
| **6.2** | **FDP_SDC.1/PM** | Stored data confidentiality for passive external NVM | Extended Components due to external NVMs | T.External-Content-Abuse<br>T.NVM-Shared-Content-Abuse |
| **7.1** | **FDP_SDI.2/IM** | Stored data integrity monitoring and action for internal memories | BSI-CC-PP-0084 | T.Phys-Probing<br>T.Phys-Manipulation |
| **7.2** | **FDP_SDI.2/PM** | Stored data integrity monitoring and action for passive external NVM | Extended Components due to external NVMs | T.External-Content-Abuse<br>T.NVM-Shared-Content-Abuse |
| **8** | **FPT_PHP.3** | Resistance to physical attack | BSI-CC-PP-0084 | T.Phys-Probing<br>T.Phys-Manipulation<br>T.Leak-Forced<br>T.Abuse-Func<br>T.RND |
| **9** | **FDP_ITT.1** | Basic internal transfer protection | BSI-CC-PP-0084 | T.Leak-Inherent<br>T.Leak-Forced<br>T.Abuse-Func<br>T.RND |

| | | | | |
|---|---|---|---|---|
| **10** | **FPT_ITT.1** | Basic internal TSF data transfer protection | BSI-CC-PP-0084 | T.Leak-Inherent<br>T.Leak-Forced<br>T.Abuse-Func<br>T.RND |
| **11.1** | **FDP_IFC.1/IM** | Subset information flow control for internal memories | BSI-CC-PP-0084 | T.Leak-Inherent<br>T.Leak-Forced<br>T.Abuse-Func<br>T.RND |
| **11.2** | **FDP_IFC.1/PM** | Subset information flow control for passive external NVM | Extended Components due to external NVMs | T.Leak-Inherent<br>T.Leak-Forced<br>T.Abuse-Func<br>T.RND |
| **12.1** | **FCS_RNG.1/RGS-IC** | Random number generation – RGS-IC | BSI-CC-PP-0084 (extended component) | T.RND |
| **12.2** | **FCS_RNG.1/DRBG** | Random number generation – DRBG | BSI-CC-PP-0084 (extended component) | T.RND |
| **12.3** | **FCS_RNG.1/PRNG** | Pseudo-Random Generation - PRNG | BSI-CC-PP-0084 (extended component) | T.RND |
| **13** | **FDP_ACC.1** | Subset access control | CC 3.1 - Part 2 | T.Mem-Access |
| **14** | **FDP_ACF.1** | Security attribute based access control | CC 3.1 - Part 2 | T.Mem-Access |
| **15** | **FMT_MSA.3** | Static attribute initialization | CC 3.1 - Part 2 | T.Mem-Access |
| **16** | **FMT_MSA.1** | Management of security attributes | CC 3.1 - Part 2 | T.Mem-Access |
| **17** | **FMT_SMF.1** | Specification of management functions | CC 3.1 - Part 2 | T.Mem-Access |
| **18** | **FDP_RIP.1** | Subset residual information protection | CC 3.1 - Part 2 | P.Protect-Resid-Info |
| **19.1** | **FCS_COP.1/[HW]TDES** | Cryptographic operation - TDES (Hardware) | BSI-CC-PP-0084 (Packages for Cryptographic Services) | P.Crypto-Service |
| **19.2** | **FCS_COP.1/[SW]TDES** | Cryptographic operation - TDES (Software) | BSI-CC-PP-0084 (Packages for Cryptographic Services) | P.Crypto-Service |
| **19.3** | **FCS_COP.1/[HW]AES** | Cryptographic operation - AES (Hardware) | BSI-CC-PP-0084 (Packages for Cryptographic Services) | P.Crypto-Service |
| **19.4** | **FCS_COP.1/[SW]AES** | Cryptographic operation - AES (Software) | BSI-CC-PP-0084 (Packages for Cryptographic Services) | P.Crypto-Service |
| **19.4** | **FCS_COP.1/PKA** | Cryptographic Operation - PKA | CC 3.1 - Part 2 (derived from the component FCS_COP.1) | P.Crypto-Service |
| **19.5** | **FCS_COP.1/RSA** | Cryptographic Operation - RSA | CC 3.1 - Part 2 (derived from the component FCS_COP.1) | P.Crypto-Service |
| **19.6** | **FCS_COP.1/ECDSA** | Cryptographic operation - ECDSA | CC 3.1 - Part 2 (derived from the component FCS_COP.1) | P.Crypto-Service |

| | | | | |
|---|---|---|---|---|
| **19.7** | **FCS_COP.1/ECDH** | Cryptographic operation - ECDH | CC 3.1 - Part 2 (derived from the component FCS_COP.1) | P.Crypto-Service |
| **19.8** | **FCS_COP.1/SHA** | Cryptographic operation – SHA | BSI-CC-PP-0084 (Packages for Cryptographic Services) | P.Crypto-Service |
| **20.1** | **FCS_CKM.1/RSA** | Cryptographic key generation - RSA | CC 3.1 - Part 2 (derived from the component FCS_CKM.1) | P.Crypto-Service |
| **20.2** | **FCS_CKM.1/ECDSA** | Cryptographic key generation - ECDSA | CC 3.1 - Part 2 (derived from the component FCS_CKM.1) | P.Crypto-Service |
| **21** | **FMT_LIM.1/Loader** | Limited capabilities - Loader | BSI-CC-PP-0084 (Package 1: Loader dedicated for usage in secured environment only) | P.Lim_Block_Loader |
| **22** | **FMT_LIM.2/Loader** | Limited availability - Loader | BSI-CC-PP-0084 (Package 1: Loader dedicated for usage in secured environment only) | P.Lim_Block_Loader |
| **23** | **FIA_API.1** | Authentication Proof of Identity | BSI-CC-PP-0084 (Package “Authentication of the Security IC”) | T.Masquerade_TOE |
| **24** | **FTP_ITC.1** | Inter-TSF trusted channel | BSI-CC-PP-0084 (Package 2 for Loader) | P.Ctrl_Loader |
| **25** | **FDP_UCT.1** | Basic data exchange confidentiality | BSI-CC-PP-0084 (Package 2 for Loader) | P.Ctrl_Loader |
| **26** | **FDP_UIT.1** | Data exchange integrity | BSI-CC-PP-0084 (Package 2 for Loader) | P.Ctrl_Loader |
| **27** | **FDP_ACC.1/Loader** | Subset access control – Loader | BSI-CC-PP-0084 (Package 2 for Loader) | P.Ctrl_Loader |
| **28** | **FDP_ACF.1/Loader** | Security attribute based access control – Loader | BSI-CC-PP-0084 (Package 2 for Loader) | P.Ctrl_Loader |
| **29** | **FDP_URC.1/PM** | Protection against an unauthorized rollback of stored contents | Extended Components due to external NVMs | T.NVM-Unauthorized-Rollback |
| **30** | **FDP_IRA.1/PM** | Irreversibility Anchor of NVM contents | Extended Components due to external NVMs | T.NVM-Command-Replay<br>T.NVM-Unauthorized-Rollback |
| **31** | **FIA_UID.1/PM** | Stored data authenticity | Extended Components due to external NVMs | T.External-Content-Abuse<br>T.NVM-Shared-Content-Abuse |
| **33** | **FDP_DAU.2/PM** | Data Authentication with Identity of Guarantor | CC 3.1 - Part 2 | T.NVM-Clone-Replace |
| **34** | **FPT_RPL.1/PM** | Replay detection | CC 3.1 - Part 2 | T.NVM-Command-Replay |

*Table 6-1: Summary of the Security Functional Requirements for the TOE*

228 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. These refinements are described below along with the associated SFR. The refinements appear in bold font whereas the assignments and selections appear in italic bold font.

### 6.1.1 Malfunctions

229 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 |
| Dependencies: | FPT_FLS.1 Failure with preservation of secure state. |
| 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)***. |
| **Refinement:** | **The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.** |

230 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. |
| Dependencies: | No dependencies. |
| 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***. |
| **Refinement:** | **The term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.** |

### 6.1.2 Abuse of Functionality

231 The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

| | |
|---|---|
| **FMT_LIM.1** | **Limited capabilities** |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_LIM.2 Limited availability. |

| | |
|---|---|
| FMT_LIM.1.1 | The TSF shall be designed and implemented in a manner that limits their 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.*** |

232 The TOE shall meet the requirement "Limited capabilities – Loader (FMT_LIM.1/Loader)" as specified below.

| | |
|---|---|
| **FMT_LIM.1/Loader** | **Limited capabilities – Loader** |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_LIM.2 Limited availability. |
| FMT_LIM.1.1/Loader | The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: ***Deploying Loader functionality after the locking of the Loader does not allow stored user data to be disclosed or manipulated by unauthorized user*** |
| Application Note | FMT_LIM.1 supplements FMT_LIM.2 allowing for non-overlapping loading of user data and protecting the TSF against misuse of the Loader for attacks against the TSF. The TOE Loader may allow for correction of already loaded user data before the assigned action e.g. before blocking the TOE Loader for TOE Delivery to the end customer or any intermediate step in the life cycle of the Security IC or the smartcard. |

233 The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

| | |
|---|---|
| **FMT_LIM.2** | **Limited availability** |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_LIM.1 capabilities. |
| FMT_LIM.2.1 | The TSF shall be designed and implemented 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.*** |

234 The TOE shall meet the requirement "Limited availability – Loader (FMT_LIM.2/Loader)" as specified as follows.

| | |
|---|---|
| **FMT_LIM.2/Loader** | **Limited availability – Loader** |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_LIM.1 Limited capabilities. |

| | |
|---|---|
| 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 the locking of the Loader.*** |

235 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. |
| Dependencies: | No dependencies. |
| FAU_SAS.1.1 | The TSF shall provide<br>- The test process<br>- The pre-personalization process<br>- The admin loader<br>- The firmware<br>With the capability to store ***the initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software and/or firmware data in the Non-volatile Memory.*** |
| Application note: | The development, production and the testing phases require the TOE to support unique identification number. |

### 6.1.3 Physical Manipulation and Probing

236 The TOE shall meet the requirement "Stored data confidentiality for internal memories (FDP_SDC.1/IM)" as specified below.

| | |
|---|---|
| **FDP_SDC.1/IM** | **Stored data confidentiality for internal memories** |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FDP_SDC.1.1/IM | The TSF shall ensure the confidentiality of the information of the user data while it is stored in the ***memories within TOE Hardware boundary (ROM, CRAM, RAM and OTP).*** |

237 The TOE shall meet the requirement "Stored data confidentiality for passive external NVM (FDP_SDC.1/PM)" as specified below.

| | |
|---|---|
| **FDP_SDC.1/PM** | **Stored data confidentiality for passive external NVM** |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |

| | |
|---|---|
| FDP_SDC.1.1/PM | The TSF shall ensure the confidentiality of the information of the user data while it is stored in the ***memories outside the TOE Hardware boundary (passive external NVM).*** |

238 The TOE shall meet the requirement “Stored data integrity monitoring and action for internal memories (FDP_SDI.2/IM)” as specified below.

| | |
|---|---|
| **FDP_SDI.2/IM** | **Stored data integrity monitoring and action for internal memories** |
| Hierarchical to: | FDP_SDI.1/IM Stored data integrity monitoring for internal memories |
| Dependencies: | No dependencies. |
| FDP_SDI.2.1/IM | The TSF shall monitor user data stored in containers controlled by the TSF for ***integrity errors using the CRC coprocessor and the CRC modules integrated in both RAM and CRAM*** on all objects, based on ***the content of the OTP, RAM and CRAM memories within TOE Hardware boundary*** |
| FDP_SDI.2.2/IM | Upon detection of a data integrity error, the TSF shall ***reset the TOE or generate a non-maskable interrupt signal***. |
| **Refinement:** | **The TOE needs additional support by the Embedded Software to check data integrity on external memory with the help of CRC coprocessor.** |

239 The TOE shall meet the requirement “Stored data integrity monitoring and action for passive external NVM (FDP_SDI.2/PM)” as specified below.

| | |
|---|---|
| **FDP_SDI.2/PM** | **Stored data integrity monitoring and action for passive external NVM** |
| Hierarchical to: | FDP_SDI.1 Stored data integrity monitoring |
| Dependencies: | No dependencies. |
| FDP_SDI.2.1/PM | The TSF shall monitor user data stored in containers controlled by the TSF ***for integrity errors using the AEAD service*** on all objects, based on the ***content of the passive external NVM.*** |
| FDP_SDI.2.2/PM | Upon detection of a data integrity error, the TSF shall ***reset the TOE or generate a non-maskable interrupt signal***. |
| **Refinement:** | **The TOE needs additional support by the Embedded Software to check data integrity on external memory with the help of CRC coprocessor.** |

240 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. |
| Dependencies: | No dependencies. |

| | |
|---|---|
| FPT_PHP.3.1 | The TSF shall resist ***physical manipulation and physical probing*** to the ***TSF*** by responding automatically such that the SFRs are always enforced. |
| **Refinement:** | **The TSF implements 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: | Security features such as active shield, data and bus scrambling for memory and 1 to N encoding data style make the reverse-engineering of the TOE layout impracticable. When a physical probing attack is detected a Non-Maskable Interrupt is generated. These features enable to meet the security functional requirement of FPT_PHP.3. |

### 6.1.4 Leakage

241 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. |
| Dependencies: | [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]. |
| 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. |
| **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.** |

242 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. |
| Dependencies: | No dependencies. |
| FPT_ITT.1.1 | The TSF shall protect TSF data from ***disclosure*** when it is transmitted between separate parts of the TOE. |
| **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.** |

243 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.

244 The TOE shall meet the requirement “Subset information flow control for internal memories (FDP_IFC.1/IM)” as specified below:

| | |
|---|---|
| **FDP_IFC.1/IM** | **Subset information flow control for internal memories** |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_IFF.1 Simple security attributes. |
| FDP_IFC.1.1/IM | 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. |

245 The TOE shall meet the requirement “Subset information flow control for passive external NVM (FDP_IFC.1/PM)” as specified below:

| | |
|---|---|
| **FDP_IFC.1/PM** | **Subset information flow control for passive external NVM** |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_IFF.1 Simple security attributes. |
| FDP_IFC.1.1/PM | The TSF shall enforce the Data Processing Policy on all confidential data when they are transferred from passive external NVM to the TOE or by the TOE to the passive external NVM. |

246 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

247 The TOE shall meet the requirement “Quality metric for random numbers (FCS_RNG.1/RGS-IC)” as specified below (Common Criteria Part 2 extended).

| | |
|---|---|
| **FCS_RNG.1/RGS-IC** | **Random number generation – RGS-IC** |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FCS_RNG.1.1/RGS-IC | The TSF shall provide a ***physical*** random number generator that implements: ***the rule RègleArchiGVA-1 of [14] and the recommendation RecomArchiGVA-1 of [14], 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 [14].*** |
| **Warning** | **The TSF fulfils some but not all the necessary rules to comply with [14] regarding random numbers generators (RNG). The composite product's RNG will comply with [14] only when all** |

| | |
|---|---|
| | **the rules of §2.4 "Génération d'aléa cryptographique" of [14] are addressed. In particular, a cryptographic post-processing must be implemented by the composite developer.** |
| Application note: | The TRNG integrates a post-processing function with features that enable to perform online tests and statistical tests. |

248 In addition to FCS_RNG.1/RGS-IC the TOE shall optionally provide a DRBG cryptographic library to produce deterministic random bit generator as follows:

| | |
|---|---|
| **FCS_RNG.1/DRBG** | **Random number generation – DRBG** |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FCS_RNG.1.1/DRBG | The TSF shall provide a ***deterministic*** random number generator that implements **a software post-processing algorithm that meets:**<br>**(DRBG.1) the rule *RègleArchiGDA-4 of [14] and* the recommendation *RecomArchiGDA-1 of [14].***<br>**(DRBG.2) the rule *RègleAlgoGDA-1 of [14].*** |
| FCS_RNG.1.2/DRBG | The TSF shall provide ***random numbers*** that meet ***the rules RègleAlgoGDA-2 and RègleAlgoGDA-3 of [14].*** |
| Application note | The DRBG relies on a random seed provided by the TRNG. |

249 The TOE provides a hardware pseudo-random number generator that can be used for cryptographic support.

| | |
|---|---|
| **FCS_RNG.1/PRNG** | **Pseudo-Random number generation – PRNG** |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FCS_RNG.1.1/PRNG | The TSF shall provide a ***deterministic*** random number generator that meets:<br>***(PRNG.1.1) Generated random numbers shall pass AIS31 statistical tests (Test procedure A).*** |
| Application note | The PRNG relies on a random seed provided by the TRNG. |

### 6.1.6 Memory Access Control

250 The TOE shall support mechanism that enable to separate code and data in order to prevent one application to access code and/or data of another application. Several Security Functional Policies (SFP) are used for protecting data such as access control and information flow control.

251 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. |

| | |
|---|---|
| Dependencies: | FDP_ACF.1 Security attribute based access control. |
| FDP_ACC.1.1 | The TSF shall enforce the ***Memory Access Control Policy*** on ***all subjects (software with test mode, pre-personalization mode, administrator mode and firmware mode), all objects (data including code stored in memories within TOE Hardware boundary (ROM, CRAM, RAM and OTP) and in memories outside the TOE Hardware boundary (Flash) and all the operations among subjects and objects covered by the SFP.*** |

252 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.** |
| Hierarchical to: | No other components. |
| Dependencies: | FDP_ACC.1 Subset access control<br>FMT_MSA.3 Static attribute initialization |
| FDP_ACF.1.1 | The TSF shall enforce the ***Memory Access Control Policy*** to objects based on the following: ***memories within TOE Hardware boundary (ROM, CRAM, RAM and OTP) and in memories outside the TOE Hardware boundary (Flash).It includes access rights and the software executed from these memories.*** |
| 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 permission access rights before granting access to controlled subjects and objects.*** |
| FDP_ACF.1.3 | The TSF shall explicitly authorize 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***. |

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

| | |
|---|---|
| **FMT_MSA.3** | **Static attribute initialization** |
| Hierarchical to: | No other components. |
| Dependencies: | FMT_MSA.1 Management of security attributes<br>FMT_SMR.1 Security roles |
| FMT_MSA.3.1 | The TSF shall enforce the ***Memory Access Control Policy*** to provide ***initialization*** default values for security attributes that are used to enforce the SFP. |
| FMT_MSA.3.2 | The TSF shall allow any ***subjects*** to specify alternative initial values to override the default values when an object or information is created. |

254 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. |
| Dependencies: | FDP_ACC.1 Subset access control or<br>FDP_IFC.1 Subset information flow control<br>FMT_SMF.1 Specification of management functions<br>FMT_SMR.1 Security roles |
| FMT_MSA.1.1 | The TSF shall enforce the ***Memory Access Control Policy*** to restrict the ability to ***change initial values, modify or delete*** *the security* ***access rights of control information*** to ***running at privilege mode***. |

255 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. |
| Dependencies: | No dependencies |
| FMT_SMF.1.1 | The TSF shall make available the ***access of control registers of the MPU*** for allowing security management functions. |

### 6.1.7 Cryptographic reuse of memory

256 The TOE shall support mechanisms to prevent cryptographic resource stored in memory from being reused.

257 The TOE shall meet the requirement “Subset residual information protection (FDP_RIP.1)” as specified below.

| | |
|---|---|
| **FDP_RIP.1** | **Subset residual information protection** |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies |
| FDP_RIP.1.1 | The TSF shall ensure that any previous information content is made unavailable upon the ***deallocation of the resource*** from the following objects: ***all objects used by the cryptographic library as specified in the user guidance documentation***. |

### 6.1.8 Cryptographic Support

258 The Cryptographic Operation component FCS_COP.1 requires the cryptographic algorithm and key size used to perform specified cryptographic operations which can be based on assigned standard.

259 The following additional specific security functionality is implemented in the TOE as software libraries:

- Triple Data Encryption Standard (TDES) (optional)

- Advanced Encryption Standard (AES) (optional)
- Rivest-Shamir-Adleman (RSA) public key asymmetric cryptography, with key size 1280-bit up to 4096-bit with (optional)
- Elliptic Curve Cryptography (ECC) (optional)
- Cryptographic service Hash function (SHA) (optional)

260 The TOE shall meet the Cryptographic Operation (FCS_COP.1) requirements as specified below:

**Triple DES operation**

| **FCS_COP.1/[HW]TDES** | **Cryptographic Operation - TDES (Hardware)** |
|---|---|
| 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] FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/[HW]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 [9], NIST SP 800-38A [10]***. |

The optional DES cryptographic library of the TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below.

| **FCS_COP.1/[SW]TDES** | **Cryptographic Operation - TDES (Software)** |
|---|---|
| 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] FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/[SW]TDES | The TSF shall perform ***encryption and decryption*** in accordance with a specified cryptographic algorithm TDES in ***ECB and CBC modes*** and cryptographic key sizes: ***112 bit, 168 bit*** that meet the following: ***NIST SP 800-67 [9], NIST SP 800-38A [10]***. |

**AES Operation**

| **FCS_COP.1/[HW]AES** | **Cryptographic Operation - AES (Hardware)** |
|---|---|
| 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] FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/[HW]AES | The TSF shall perform ***decryption and encryption*** in accordance with a specified cryptographic algorithm AES in ***ECB , CBC, CTR and CMAC modes*** and cryptographic key sizes: ***128*** |

***bit, 192 bit and 256 bit*** that meet the following standard: ***FIPS 197 [7], NIST SP 800-38A [10], NIST SP 800-38B [17]***.

The optional AES cryptographic library of the TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below.

| **FCS_COP.1/[SW]AES** | **Cryptographic Operation - (Software)** |
|---|---|
| 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] FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/[SW]AES | The TSF shall perform ***decryption and encryption*** in accordance with a specified cryptographic algorithm: AES in ***ECB , CBC, CTR and CMAC modes*** and cryptographic key sizes: ***128 bit, 192 bit and 256 bit*** that meet the following standard: ***FIPS 197 [7], NIST SP 800-38A [10], NIST SP 800-38B [17]***. |

**Public Key Accelerator (PKA) Operation**

| **FCS_COP.1/PKA** | **Cryptographic Operation - PKA** |
|---|---|
| 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] FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/PKA | The TSF shall perform **modular exponentiation** in accordance with a specified cryptographic algorithm **none** and cryptographic key sizes **between 128 and 4096 bits** that meet the following standard: **none**. |

**Rivest-Shamir-Adleman (RSA) Operation**

| **FCS_COP.1/RSA** | **Cryptographic Operation - RSA** |
|---|---|
| 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] FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/RSA | The TSF shall perform ***encryption, decryption, signature generation and verification*** in accordance with a specified cryptographic algorithm ***RSA Cryptography Standard with Montgomery*** and cryptographic key sizes: ***between 128-bit and 4096-bit*** that meet the following: ***PKCS#1 v2.1 June, 14, 2002***. |

**Rivest-Shamir-Adleman (RSA) Key Generation**

The RSA key generation for the optional RSA cryptographic library shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below.

| | |
|---|---|
| **FCS_CKM.1/RSA** | **Cryptographic key generation - RSA** |
| Hierarchical to: | No other components. |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM.1.1/RSA | The TSF shall generate the RSA public/private key pair in accordance with the specified cryptographic key generation algorithm and with the specified cryptographic key sizes ***from 1280-bit up to 4096-bit with 32-bit granularity*** that meet the following standards: ***ETSI TS 102 176-1, section 6.2.2.1 Key and parameter generation algorithm rsagen1***. |

**Elliptic Curve DSA (ECDSA) Operation**

The ECC cryptographic library of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

| | |
|---|---|
| **FCS_COP.1/ECDSA** | **Cryptographic operation - ECDSA** |
| 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]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/ECDSA | The TSF shall perform ***signature generation and verification*** in accordance with the specified cryptographic algorithm ***ECDSA and cryptographic key sizes up to 640-bit*** that meet the following standard: ***ANS X9.62, section 7.3 Signing Process and section 7.4 Verifying Process***. |

**Cryptographic hash function (SHA) Operation**

The SHA cryptographic library of the TOE shall meet the requirement "Cryptographic operation – SHA (FCS_COP.1/SHA)" as specified below.

| | |
|---|---|
| **FCS_COP.1/SHA** | **Cryptographic operation - SHA** |
| 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]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/SHA | The TSF shall perform **hashing** in accordance with the specified cryptographic algorithms: **SHA2-224, SHA2-256, SHA2-384, SHA2-512** that meet the following standard: ***FIPS 180-4 [16].*** |

**Elliptic Curve DSA (ECDSA) Key Generation**

The key generation for the ECC cryptographic library shall meet the requirement "Cryptographic key generation (FCS_CKM.1/ECDSA)" as specified below.

| **FCS_CKM.1/ECDSA** | **Cryptographic key generation - ECDSA** |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_CKM.1.1/ECDSA | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***specified in ANS X9.62*** and with the cryptographic key sizes ***up to 640-bit*** that meet the following standard: ***ANS X9.62, section A.4.3 Elliptic Curve Key Generation***. |

**Elliptic Curve Diffie-Hellman (ECDH) Key Agreement**

The ECC cryptographic library of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

| **FCS_COP.1/ECDH** | **Cryptographic operation - ECDH** |
|---|---|
| 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]<br>FCS_CKM.4 Cryptographic key destruction |
| FCS_COP.1.1/ECDH | The TSF shall perform ***the key exchange*** in accordance with a specified cryptographic algorithm ***ECDH*** and cryptographic key sizes ***from 192-bit up to 640-bit*** that meet the following standard: ***ANS X9.63, section 5.4.1 Standard Diffie-Hellman primitive***. |

### 6.1.9 Authentication of the TOE

261 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 an ***authentication mechanism*** to prove the identity of the ***TOE*** to an external entity. |

### 6.1.10 Loader dedicated for usage by authorized users only

262 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. |
| Dependencies | No dependencies. |
| FTP_ITC.1.1 | The TSF shall provide a communication channel between itself and ***authorized users*** 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.*** |

263 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. |
| 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] |
| FDP_UCT.1.1 | The TSF shall enforce the Loader SFP to receive user data in a manner protected from unauthorized disclosure. |

264 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. |
| 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] |
| 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. |

265 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. |

| | |
|---|---|
| Dependencies | FDP_ACF.1 Security attribute based access control. |
| FDP_ACC.1.1/ Loader | The TSF shall enforce the ***Loader SFP*** on<br>(1) the subjects: ***Loader role***,<br>(2) the objects user data in ***Memory outside the TOE Hardware (Flash)***,<br>(3) the operation deployment of Loader |

266 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. |
| Dependencies | No dependencies. |
| FDP_ACF.1.1/ Loader | FDP_ACF.1.1 The TSF shall enforce the ***Loader SFP*** to objects based on the following:<br>(1) the subjects : ***Loader role*** with security attributes : ***writing access rights***.<br>(2) the objects user data in ***Memory outside the TOE Hardware (Flash)*** with security attributes : ***data are located in controlled sectors of the external memory devoted to TESIC***. |
| FDP_ACF.1.2/ Loader | 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 writing access rights before granting access to the controlled subjects or objects***. |
| FDP_ACF.1.3/ Loader | FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***the Loader role shall be authenticated before access is granted***. |
| FDP_ACF.1.4/ Loader | The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***the TSF prevents deploying the Loader functionality after the locking of the Loader, the TSF prevents deploying the Loader functionality if the Loader role has not been authenticated***. |
| **Note** | **The SFR FMT_MSA.3 as a dependency is not necessary as the security attributes used to enforce the Loader SFP are fixed by the IC manufacturer and no new objects under control of the Loader SFP are created.** |

### 6.1.11 Passive External NVM

#### 6.1.11.1 Protection of NVM content freshness

267 The TOE shall meet the requirement “Protection against an unauthorized rollback of stored contents in Passive external NVM (FDP_URC.1/PM)”, as specified below.

| | |
|---|---|
| **FDP_URC.1/PM** | **Protection against an unauthorized rollback of stored contents in Passive external NVM** |

| | |
|---|---|
| Hierarchical to: | No other components |
| Dependencies: | No dependencies |
| FDP_URC.1.1/PM | The TOE shall detect an unauthorized replacement of the contents stored in the **passive** external NVM before the contents are used. The detection shall take place even if the contents were previously stored in the same **passive** external NVM and were valid and consistent at a given past time. |
| FDP_URC.1.2/PM | Upon detection of unauthorized rollback of **passive** external NVM contents, the TOE shall ***throw an exception and the exception shall be handled accordingly by the application software***. |

268 The TOE shall meet the requirement “Irreversibility Anchor of passive external NVM contents (FDP_IRA.1/PM)”, as specified below.

| | |
|---|---|
| **FDP_IRA.1/PM** | **Irreversibility Anchor of passive external NVM contents** |
| Hierarchical to: | No other components |
| Dependencies: | No dependencies |
| FDP_IRA.1.1/PM | The TOE shall implement a non-volatile irreversibility anchor mechanism that maintains a value that goes **increasingly** through a predefined sequence of states without the possibility of reversion to a previous state. The state of the Irreversibility Anchor is used to verify that NVM contents preserve data freshness as follows:<br>***- Its value is (1) associated to the state of the passive external NVM contents, (2) advanced to the next state before contents are updated by the host MCU, and (3) checked to determine if the passive external NVM contents are fresh before they are used***.<br>***The irreversibility anchor keeps track of the state of the external NVM contents and its value is used to sign the associated image in the external NVM. Thus, this association allows to verify that the external NVM contents do meet data freshness.*** |
| FDP_IRA.1.2/PM | Upon detection of unauthorized rollback of external NVM contents, the TOE shall ***throw an exception and the exception shall be handled accordingly by the application software***. |

#### 6.1.11.2 Data transfer between host MCU and passive external NVM

269 The TOE shall meet the requirement “Replay detection in passive external NVM (FPT_RPL.1/PM)”, as specified below.

| | |
|---|---|
| **FPT_RPL.1/PM** | **Replay detection in passive external NVM** |
| Hierarchical to: | No other components |
| Dependencies: | No dependencies |
| FPT_RPL.1.1/PM | The TSF shall detect replay for the following entities: ***commands issued by the host MCU to the passive external NVM for the read, write and erase operations.*** |

| | |
|---|---|
| FPT_RPL.1.2/PM | The TSF shall ***throw an exception and the exception shall be handled accordingly by the application software*** when replay is detected. |

270 The TOE shall meet the requirement “Data Authentication with Identity of Guarantor (FDP_DAU.2/PM)”, as specified below.

| | |
|---|---|
| **FDP_DAU.2/PM** | **Data Authentication with Identity of Guarantor** |
| Hierarchical to: | FDP_DAU.1 Basic Data Authentication |
| Dependencies: | FIA_UID.1 Timing of Identification |
| FDP_DAU.2.1/PM | The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of ***data objects and containers stored in the external memory.*** |
| FDP_DAU.2.2/PM | The TSF shall provide the TOE with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence. |

271 The TOE shall meet the requirement “Timing of Identification (FIA_UID.1/PM)”, as specified below.

| | |
|---|---|
| **FIA_UID.1/PM** | **Timing of Identification** |
| Hierarchical to: | No other components |
| Dependencies: | No dependencies |
| FIA_UID.1.1/PM | The TSF shall allow **the secure start-up or wake-up without access to data objects and containers stored in the external memory** on behalf of the user to be performed before the user is identified. |
| FIA_UID.1.2/PM | The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. |

## 6.2 Security Assurance Requirements for the TOE

272 The Security Target will be evaluated according to

Security Target evaluation (Class ASE)

273 The Security Assurance Requirements for the evaluation of the TOE are those taken from the

Evaluation Assurance Level 5 (EAL5)

and augmented by taking the following components:

ALC_DVS.2 and AVA_VAN.5.

this corresponds to level “EAL5+”

274 The assurance requirements are (augmented components are highlighted):

| Title | Label | Origin |
|---|---|---|
| **Class ADV: Development** | | |
| Architectural design | (ADV_ARC.1) | CC & BSI-CC-PP-0084 |
| Functional specification | (ADV_FSP.5) | CC & BSI-CC-PP-0084 |
| Implementation representation | (ADV_IMP.1) | CC & BSI-CC-PP-0084 |
| Well-structured internals | (ADV_INT.2) | CC |
| TOE design | (ADV_TDS.4) | CC |
| **Class AGD: Guidance documents** | | |
| Operational user guidance | (AGD_OPE.1) | CC & BSI-CC-PP-0084 |
| Preparative user guidance | (AGD_PRE.1) | CC & BSI-CC-PP-0084 |
| **Class ALC: Life-cycle support** | | |
| CM capabilities | (ALC_CMC.4) | CC & BSI-CC-PP-0084 |
| CM scope | (ALC_CMS.5) | CC & BSI-CC-PP-0084 |
| Delivery | (ALC_DEL.1) | CC & BSI-CC-PP-0084 |
| Development security | (ALC_DVS.2) | CC & BSI-CC-PP-0084 |
| Life-cycle definition | (ALC_LCD.1) | CC |
| Tools and techniques | (ALC_TAT.2) | CC |
| **Class ASE: Security Target evaluation** | | |
| Conformance claims | (ASE_CCL.1) | CC |
| Extended components definition | (ASE_ECD.1) | CC |
| ST introduction | (ASE_INT.1) | CC |
| Security objectives | (ASE_OBJ.2) | CC |
| Derived security requirements | (ASE_REQ.2) | CC |
| Security problem definition | (ASE_SPD.1) | CC |
| TOE summary specification | (ASE_TSS.1) | CC |
| **Class ATE: Tests** | | |
| Coverage | (ATE_COV.2) | CC & BSI-CC-PP-0084 |
| Depth | (ATE_DPT.3) | CC |
| Functional tests | (ATE_FUN.1) | CC |
| Independent | (ATE_IND.2) | CC |
| **Class AVA: Vulnerability assessment** | | |
| Vulnerability analysis | (AVA_VAN.5) | CC & BSI-CC-PP-0084 |

275 All refinements of Security Assurances requirements (CC V3.1 Part 3) defined in the Protection Profile BSI-CC-PP-0084 are considered (claimed) in this Security Target. They also include refinement for the augmented components ALC_DVS.2 and AVA_VAN.5.

## 6.3 Security Requirements Rationale

### 6.3.1 Rationale for the Security Functional Requirements

276 Table 6-2 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”<br>- FPT_ITT.1 “Basic internal TSF data transfer protection”<br>- FDP_IFC.1 “Subset information flow control” |
| O.Phys-Probing | - FDP_SDC.1 “Stored data confidentiality”<br>- FPT_PHP.3 “Resistance to physical attack” |
| O.Malfunction | - FRU_FLT.2 “Limited fault tolerance”<br>- FPT_FLS.1 “Failure with preservation of secure state” |
| O.Phys-Manipulation | - FDP_SDI.2 “Stored data integrity monitoring and action”<br>- FPT_PHP.3 “Resistance to physical attack” |
| O.Leak-Forced | All requirements listed for O.Leak-Inherent<br>- FDP_ITT.1, FPT_ITT.1, FDP_IFC.1<br>plus those listed for O.Malfunction and O.Phys-Manipulation<br>- FRU_FLT.2, FPT_FLS.1, FPT_PHP.3 |
| O.Abuse-Func | - FMT_LIM.1 “Limited capabilities”<br>- FMT_LIM.2 “Limited availability”<br>plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced<br>- FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3,<br>FRU_FLT.2, FPT_FLS.1 |
| O.Identification | - FAU_SAS.1 “Audit storage” |
| O.RND | - FCS_RNG.1/RGS-IC “Quality metric for random numbers”<br>plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced<br>- FCS_RNG.1/DRBG<br>- FCS_RNG.1/PRNG<br>- FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3,<br>FRU_FLT.2, FPT_FLS.1 |
| O.Reuse | - FDP_RIP.1 “Subset residual information protection” |
| O.TDES | - FCS_COP.1/[HW]TDES "Cryptographic operation - TDES (Hardware)"<br>- FCS_COP.1/[SW]TDES "Cryptographic operation - TDES (Software)" |
| O.AES | - FCS_COP.1/[HW]AES "Cryptographic operation - AES (Hardware)"<br>- FCS_COP.1/[SW]AES "Cryptographic operation - AES (Software)" |
| O.PKA | - FCS_COP.1/PKA “Cryptographic operation - PKA” |
| O.RSA | - FCS_COP.1/RSA "Cryptographic operation - RSA"<br>- FCS_CKM.1/RSA “Cryptographic key generation - RSA” |
| O.ECC | - FCS_COP.1/ECDSA “Cryptographic operation - ECDSA”<br>- FCS_COP.1/ECDH “Cryptographic operation - ECDH”<br>- FCS_CKM.1/ECDSA “Cryptographic key generation - ECDSA” |

| | |
|---|---|
| O.SHA | - FCS_COP.1/SHA “Cryptographic operation - SHA” |
| OE.Resp-Appl | Not applicable |
| OE.Process-Sec-IC | Not applicable |
| O.Mem-Access | - FDP_ACC.1 “Subset access control”<br>- FDP_ACF.1 “Security attribute based access control”<br>- FMT_MSA.3 “Static attribute initialisation”<br>- FMT_MSA.1 “Management of security attributes”<br>- FMT_SMF.1 “Specification of Management Functions” |
| O.Cap_Avail_Loader | - FMT_LIM.1/Loader “Limited capabilities - loader”<br>- FMT_LIM.2/Loader “Limited availability - loader” |
| OE.Lim_Block_Loader | Not applicable |
| O.Authentication | - FIA_API.1 “Authentication Proof of Identity” |
| OE.TOE_Auth | - FIA_API.1 “Authentication Proof of Identity” |
| O.Prot_TSF_Confidentiality | - FTP_ITC.1 “Inter-TSF trusted channel”<br>- FDP_UCT.1 “Basic data exchange confidentiality”<br>- FDP_UIT.1 “Data exchange integrity”<br>- FDP_ACC.1/Loader “Subset access control - Loader”<br>- FDP_ACF.1/Loader “Security attribute based access control - Loader” |
| O.Ctrl_Auth_Loader | - FTP_ITC.1 “Inter-TSF trusted channel”<br>- FDP_UCT.1 “Basic data exchange confidentiality”<br>- FDP_UIT.1 “Data exchange integrity”<br>- FDP_ACC.1/Loader “Subset access control - Loader”<br>- FDP_ACF.1/Loader “Security attribute based access control - Loader” |
| OE.Loader_Usage | Not applicable |
| O.External-Content-Protection | - FDP_SDC.1/PM for confidentiality protection<br>- FDP_SDI.2/PM for integrity protection<br>- FDP_IFC.1/PM |
| O.NVM-Command-Replay-Protection | - FPT_RPL.1/PM “Replay detection” |
| O.NVM-Unauthorized-Rollback-Protection | - FDP_URC.1/PM “Protection against an unauthorized rollback of stored contents” |
| O.NVM-Irreversibility-Anchor | - FDP_IRA.1/PM “Irreversibility Anchor of NVM contents” |
| O.NVM-Clone-Replace-Protection | - FDP_DAU.2/PM “Data Authentication with Identity of Guarantor”<br>- FIA_UID.1/PM “Timing of identification” |

*Table 6-2: Security Requirements versus Security Objectives*

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

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

279 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.

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

281 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.

282 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.

283 The justification related to the security objective “Protection against Malfunctions (O.Malfunction)” is as follows:

284 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 be 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.

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

286 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.

287 It is possible that the TOE needs additional support by the Embedded Software (for instance by implementing FDP_SDI.2 to check data integrity with the help of appropriate checksums, refer to section 6.1). This support must be addressed in the Guidance Documentation. The combination of the Embedded Software together with this FPT_PHP.3 is suitable to meet the objective.

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

289 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 mechanisms 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.

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

291 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.

292 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 6-1.

293 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 recognize 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.

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

295 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.

296 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 date 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.

297 The Manufacturer has to support this objective which is examined during the evaluation of the assurance requirements of the classes AGD and ALC.

298 The justification related to the security objective “Random Numbers (O.RND)” is as follows:

299 FCS_RNG.1 requires the TOE to provide random numbers of good quality. The exact metric is defined in [14].

300 Other security functional requirements, which prevent physical manipulation and malfunction of the TOE (see the corresponding objectives listed in the Table 6-2) support this objective because they prevent attackers from manipulating or otherwise affecting the random number generator.

301 Random numbers are often used by the Security IC Embedded Software to generate cryptographic keys for internal use. Therefore, the TOE must prevent the unauthorized 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.

302 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.

303 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.).

304 The SFR FCS_COP.1/[HW]TDES and FCS_COP.1/[SW]TDES meet the security objective “Cryptographic service Triple-DES (O.TDES)”.

305 The SFR FCS_COP.1/[HW]AES and FCS_COP.1/[SW]AES meet the security objective “Cryptographic service AES (O.AES)”.

306 The security objective “Cryptographic service PKA (O.PKA)” is implemented by the security functional requirements FCS_COP.1/PKA.

307 The security objective “Cryptographic service RSA (O.RSA)” is implemented by the security functional requirements FCS_COP.1/RSA and FCS_CKM.1/RSA.

308 The security objective “Cryptographic service ECC (O.ECC)” is implemented by the security functional requirements FCS_COP.1/ECDSA, FCS_COP.1/ECDH and FCS_CKM.1/ECDSA.

309 The security objective “Cryptographic service hash function (O.SHA)” is implemented by the security functional requirements FCS_COP.1/SHA.

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

311 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.

312 The security functional requirement “Static attribute initialization (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.

313 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 realized using the functions provided by the TOE. Therefore FMT_MSA.1 is suitable to meet the security objective O.Mem-Access.

314 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.

315 The justification related to the security objective “Protection of residual information (O.Reuse)” is as follows:

316 O.Reuse requires the TOE to provide procedural measures to prevent disclosure of memory contents used by the TOE. This applies to the Crypto Library of TESIC-04001R20 and is met by the SFR “Subset residual information protection (FDP_RIP.1)” which requires the library to make unavailable all memory content that has been used by it. Note that the requirement for residual information protection applies to all functionality of the Cryptographic Library.

317 The justification related to the security objective “Protection during Packaging, Finishing and Personalization (OE.Process-Sec-IC)” is as follows:

318 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 personalization functions.

319 The justification related to the security objective “Capability and availability of the Loader (O.Cap_Avail_Loader)” is as follows:

320 The security functional requirement “Limited capabilities – loader (FMT_LIM.1/Loader)” with the security functional requirement “Limited availability - Loader (FMT_LIM.2/Loader)” require the implementation that enable to limit the availability and capabilities of Loader. Therefore, 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.

321 The justification related to the security objective “Limitation of capability and blocking the Loader (OE.Lim-Block-Loader)” is as follows:

322 The Composite Product Manufacturer has to use adequate measures to protect the Loader functionality against misuse in order to fulfil (OE.Lim_Block_Loader). The Security IC Embedded Software may have to support this for instance by limiting the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.

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

- 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.
- 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.
- The SFR FDP_UCT.1 requires the TSF to receive data protected from unauthorised disclosure.
- The SFR FDP_UIT.1 requires the TSF to verify the integrity of the received user data.
- The SFR FDP_ACF.1/Loader requires the TSF to implement access control for the Loader functionality.

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

- 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.
- 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.
- The SFR FDP_UCT.1 requires the TSF to receive data protected from unauthorised disclosure.
- The SFR FDP_UIT.1 requires the TSF to verify the integrity of the received user data.
- The SFR FDP_ACF.1/Loader requires the TSF to implement access control for the Loader functionality.

325 The SFR FDP_SDC.1/PM and FDP_SDI.2/PM support the objective O.External-Content-Protection.

326 The justification related to the security objective “Protection against unauthorized disclosure and undetected modification of passive external NVM contents (O.External-Content-Protection)” is as follows:

327 The SFR FDP_SDC.1/PM ensures protection of confidentiality of the contents stored in the passive external NVM, while the SFR FDP_SDI.2/PM ensures protection of the integrity of the contents stored in the NVM. Finally, FDP_DAU.2/PM ensures the authenticity of the user data while it is stored in the passive external NVM. Therefore, it is clear that these security functional requirements support the objective.

328 The justification related to the security objective “Protection against replay of commands between host MCU and passive external NVM (O.NVM-Command-Replay-Protection)” is as follows:

329 The SFR FPT_RPL.1/PM requires the TSF to detect replays in responses in the read commands to the NVM or replays of sequences of write/erase commands to the passive external NVM. This requirement is considered in the assignment of FPT_RPL.1.1/PM. Therefore, it is clear that this security functional requirement supports the objective.

330 The justification related to the security objective “Protection against contents (O.NVM-Unauthorized-Rollback-Protection)” is as follows:

331 The SFR FDP_URC.1/PM requires that the TSF detects the case when the contents of the passive external NVM have been replaced by previous versions of them. This way, this security functional requirement supports the objective.

332 The justification related to the security objective “Passive External NVM Contents Irreversibility Anchor (O.NVM-Irreversibility-Anchor)” is as follows:

333 The SFR FDP_IRA.1/PM requires the TOE to implement distinct transaction references for each write and erase operation that is unambiguously linked with the current content of the transaction with the external memory. Thereby, the data freshness can be verified during a read operation based on the data maintained by the irreversible anchor. If the external memory is a non-volatile memory, the Irreversibility-Anchor needs to be maintained in any operation mode. By providing the mechanism required by this SFR, the security objective O.Mem-Irreversibility-Anchor is directly supported.

334 The justification related to the security objective “Protection against NVM cloning or replacement (O.NVM-Clone-Replace-Protection)” is as follows:

335 The SFR FDP_DAU.2/PM requires the TOE to be able to generate evidence that guarantees the validity of data objects and containers stored in the external memory. With the refinement that the dedicated TOE instance is the user in case of user data the cloning or replacement of the external memory is detected. The SFR FIA_UID.1/PM requires the definition of actions that can be performed without user identification. The authenticity external memory content needs to be identified instead of a user. The authenticity of the data stored in the external memory needs to be identified before any user data is accessed. By providing the mechanism required by these two SFRs, the security objective O.Mem-Clone-Replace-Protection is directly supported.

### 6.3.2 Dependencies of security functional requirements

336 Table 6-3 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.

| Security Functional Requirement | Dependencies | Fulfilled by security requirements |
|---|---|---|
| FRU_FLT.2 | FPT_FLS.1 | Yes |
| FPT_FLS.1 | None | No dependency |
| FMT_LIM.1 | FMT_LIM.2 | Yes |
| FMT_LIM.2 | FMT_LIM.1 | Yes |
| FAU_SAS.1 | None | No dependency |
| FPT_PHP.3 | None | No dependency |
| FDP_ITT.1 | FDP_ACC.1 or FDP_IFC.1 | Yes |
| FDP_IFC.1/IM | FDP_IFF.1 | See discussion below |
| FDP_IFC.1/PM | FDP_IFF.1 | |
| FPT_ITT.1 | None | No dependency |
| FDP_SDC.1/IM | None | No dependency |
| FDP_SDC.1/PM | None | No dependency |
| FDP_SDI.2/IM | None | No dependency |
| FDP_SDI.2/PM | None | No dependency |
| FCS_RNG.1/RGS-IC | None | No dependency |
| FCS_RNG.1/DRBG | None | No dependency |
| FCS_RNG.1/PRNG | None | No dependency |

| Security Functional Requirement | Dependencies | Fulfilled by security requirements |
|---|---|---|
| FCS_COP.1/[HW]TDES | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | Yes, see discussion below |
| FCS_COP.1/[SW]TDES | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | Yes, see discussion below |
| FCS_COP.1/[HW]AES | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | Yes, see discussion below |
| FCS_COP.1/[SW]AES | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | Yes, see discussion below |
| FCS_COP.1/PKA | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | Yes<br>See discussion below |
| FCS_COP.1/RSA | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | Yes<br>See discussion below |
| FCS_COP.1/ECDSA | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | Yes<br>See discussion below |
| FCS_COP.1/ECDH | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | Yes<br>See discussion below |
| FCS_COP.1/SHA | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1<br>FCS_CKM.4 | Yes<br>See discussion below |
| FCS_CKM.1/RSA | FCS_CKM.2 or FCS.COP.1<br>FCS_CKM.4 | Yes<br>See discussion below |
| FCS_CKM.1/ECDSA | FCS_CKM.2 or FCS.COP.1<br>FCS_CKM.4 | Yes<br>See discussion below |
| FDP_ACC.1 | FDP_ACF.1 | Yes |
| FDP_ACF.1 | FDP_ACC.1<br>FMT_MSA.3 | Yes<br>Yes |
| FMT_MSA.3 | FMT_MSA.1<br>FMT_SMR.1 | Yes<br>See discussion below |
| FMT_MSA.1 | FDP_ACC.1 or FDP_IFC.1<br>FMT_SMR.1<br>FMT_SMF.1 | Yes<br>See discussion below<br>Yes |
| FMT_SMF.1 | None | No dependency |
| FDP_RIP.1 | None | No dependency |
| FMT_LIM.1/Loader | FMT_LIM.2/Loader | Yes |
| FMT_LIM.2/Loader | FMT_LIM.1/Loader | Yes |
| FIA_API.1 | None | No dependency |
| FTP_ITC.1 | None | No dependency |
| FDP_UCT.1 | FTP_ITC.1 or FTP_TRP.1<br>FDP_ACC.1 or FDP_IFC.1 | Yes<br>Yes |
| FDP_UIT.1 | FTP_ITC.1 or FTP_TRP.1<br>FDP_ACC.1 or FDP_IFC.1 | Yes<br>Yes |

| Security Functional Requirement | Dependencies | Fulfilled by security requirements |
|---|---|---|
| FDP_ACC.1/Loader | FDP_ACF.1 | Yes |
| FDP_ACF.1/Loader | None | No dependency |
| FPT_RPL.1/PM | None | No dependency |
| FDP_URC.1/PM | None | No dependency |
| FDP_IRA.1/PM | None | No dependency |
| FDP_DAU.2/PM | FIA_UID.1/PM | Yes |
| FIA_UID.1/PM | None | No dependency |

*Table 6-3 : Dependencies of the Security Functional Requirements*

337 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).

338 Components FMT_MSA.1 and FMT_MSA.3 introduce FMT_SMR.1 requirement for security management roles. This requirement, defined on Part 2 of the Common Criteria, is considered to be satisfied because the access control specified for the intended TOE is not based on roles but enforced for each subject. Therefore, there is no need to identify roles in form of a security functional requirement FMT_SMR.1.

339 As Table 6-3 shows, all other dependencies of functional requirements are fulfilled by security requirements defined in this Protection Profile.

340 The discussion in Section 6.3.1 has shown how the security functional requirements support each other in meeting the security objectives of this Protection Profile. 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.

341 Together with the discussion of the dependencies above this shows that the security functional requirements build a mutually supportive whole.

342 The functional requirements FCS_CKM.1 and FCS_CKM.4 which are dependent to FCS_COP.1/[HW]TDES, FCS_COP.1/[SW]TDES and FCS_COP.1/[HW]AES and FCS_COP.1/[SW]AES are not included in this Security Target since the TOE only provides an engine for encryption and decryption. But the Security Embedded Software may fulfil 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).

343 The FCS_CKM.1 which is dependent to FCS_COP.1/ECDH is not included in this Security Target. But the Security IC Embedded Software may fulfil these requirements related to the needs of the implemented application. The dependent requirements of FCS_COP.1/ECDH concerning these functions shall be fulfilled by the environment (Security IC Embedded Software).

344 The functional requirement FCS_CKM.4 which is dependent to FCS_COP.1/PKA, FCS_COP.1/RSA, FCS_COP.1/ECDSA and FCS_COP.1/ECDH is not included in this Security Target. But the Security IC Embedded Software may fulfil these requirements related to the needs of the implemented application. The dependent requirements of FCS_COP.1/RSA, FCS_COP.1/ECDSA and FCS_COP.1/ECDH concerning these functions shall be fulfilled by the environment (Security IC Embedded Software).

345 The functional requirements FCS_CKM.1 and FCS_CKM.4 which are dependent to FCS_COP.1/SHA are not included in this Security Target. However, the Security IC Embedded Software may fulfil these requirements related to the needs of the implemented application. The

dependent requirements of FCS_COP.1/SHA concerning these functions shall be fulfilled by the environment (Security IC Embedded Software).

### 6.3.3 Rationale for the Assurance Requirements

346 The assurance level EAL5 and the augmentation with the requirements ALC_DVS.2, and AVA_VAN.5 were chosen in order to meet assurance expectations explained in the following paragraphs.

347 An assurance level of EAL5 with the augmentations AVA_VAN.5 and ALC_DVS.2 are required for this type of TOE since it is intended to defend against sophisticated attacks. This evaluation assurance package was selected 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 source code.

**ALC_DVS.2 Sufficiency of security measures**

348 Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE.

349 In the particular case of a Security IC the TOE is developed and produced within a complex and distributed industrial process which must especially be protected. Details about the implementation, (e.g. from design, test and development tools as well as Initialization Data) may make such attacks easier. Therefore, in the case of a Security IC, maintaining the confidentiality of the design is very important.

350 This assurance component is a higher hierarchical component to EAL5 (which only requires ALC_DVS.1). ALC_DVS.2 has no dependencies.

**AVA_VAN.5 Advanced methodical vulnerability analysis**

351 Due to the intended use of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component.

352 Independent vulnerability analysis is based on highly detailed technical information. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing high attack potential.

353 AVA_VAN.5 has dependencies to ADV_ARC.1 “Security architecture description”, ADV_FSP.4 “Complete functional specification”, ADV_TDS.3 “Basic modular design”, ADV_IMP.1 “Implementation representation of the TSF”, AGD_OPE.1 “Operational user guidance”, and AGD_PRE.1 “Preparative procedures” and ATE_DPT.1 “Testing: basic design”.

354 All these dependencies are satisfied by EAL5.

355 It has to be assumed that attackers with high attack potential try to attack Security ICs like smart cards used for digital signature applications or payment systems. Therefore, specifically AVA_VAN.5 was chosen in order to assure that even these attackers cannot successfully attack the TOE.

### 6.3.4 Security Requirements are Internally Consistent

356 The discussion of security functional requirements and assurance components in the preceding sections has shown that consistency is 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.

357 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.

358 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 TOE 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 and FCS_RNG.1/RGS-IC.

359 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 TOE 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 and FCS_RNG.1/RGS-IC.

360 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).

361 Physical probing (refer to FPT_PHP.3) shall directly avert the disclosure of primary assets identified in Section 3.1. 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) helps to protect other security features or functions. Details depend on the implementation.

362 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 or provided by the TOE (FPT_ITT.1). Details depend on the implementation.

363 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.

364 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 (i) to 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.

365 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 limit 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.

366 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.

367 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.

368 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.

369 The contents of the passive external NVM (user data, TSF data and code) need to be protected, considering that the passive external NVM may be more accessible to attackers than the internal (embedded in the same chip) one.

370 Confidentiality and integrity of the contents stored in the passive external NVM are given by FDP_SDC.1/PM and FDP_SDI.2/PM. Also, the contents stored in the NVM require a guarantee of “data freshness”, namely that the contents are the last ones stored under control of the Security IC). The TOE needs to be capable of detecting the replay of old write, erase, and read operations to the passive external NVM. This requirement is provided by FPT_RPL.1/PM.

371 The non-volatile mutable irreversibility anchor provides a mechanism for protection against reverting passive external NVM contents to old non-fresh versions of them is given by FDP_IRA.1/PM. In addition, the extended component FDP_URC.1/PM provides protection against an unauthorized rollback of the NVM contents to old versions of them, and the components FDP_DAU.2/PM, FIA_UID.1/PM ensure protection against cloning or replacement of the passive external NVM.

# 7 TOE Summary Specification

372 This chapter lists all the Security Functional Requirements (SFR) and all security features which meet the Security Functional Requirements.

| SFR | SFR description | TOE security features meeting SFR |
|---|---|---|
| 1 | FRU_FLT.2<br>Limited fault tolerance | This SFR is ensured by a TOE functional design stable within the limits of the operational conditions. The asynchronous logic contributes to fault tolerance therefore ensuring a correct behaviour of the TOE. |
| 2 | FPT_FLS.1<br>Failure with preservation of secure state. | Hardware TOE<br>The TOE integrates mechanisms that enable to detect abnormal/failure events before the secure state is compromised. Secure state is maintained by the TOE which monitors all abnormal and failure events. |
| 3 | FMT_LIM.1<br>Limited capabilities | The TSF ensures that the test mode and test capabilities are locked. |
| 4 | FMT_LIM.2 Limited availabilities | Different modes are integrated inside the TOE: *TEST* mode, the *PRE-PERSO* mode, *ADMIN* mode, and the *FIRMWARE* mode. The *TEST* mode uses specific protocol for industrial test, the *PRE-PERSO* mode is used for pre-personalization and loading the admin services, the *ADMIN* mode used to load the firmware to the memory outside the TOE boundary (Flash) and the firmware mode is available for running consumer applications.<br>All these modes require an authentication and are non-reversible. Each mode restricts the use of functions integrated in the TOE. |
| 5 | FAU_SAS.1<br>Audit Storage | Hardware TOE<br>Audit Storage requirement is covered by the following security features:<br>• Non-reversibility of test mode. An authentication is required to enter to test mode. This mode is locked by writing non-volatile memory after the test phase has been accomplished successfully. It is used only once during the manufacturing process for ensuring the non-reversibility of this mode.<br>• Identification/authentication values are written in non-volatile memory in order to ensure the traceability of the TOE. The Admin loader implements an authentication function.<br>• Non-reversibility of the Firmware mode. It is the functional mode of the TOE. It is controlled by the operating system embedded inside the TOE.<br>Software ADMIN loader TOE<br>Audit Storage requirement is covered by the ability offered by the ADMIN services to read and write TSF and user data in external memory. |

| | | |
|---|---|---|
| 6.1 | FDP_SDC.1/IM<br>Stored data confidentiality for internal memories | Hardware TOE<br>This requirement is covered by the following security features integrated in TOE:<br>• Shield.<br>• Security mechanisms for memory protection.<br>• MPU for memory access control.<br>Software TOE<br>This SFR is covered by the AEAD mechanisms in ROM and ADMIN code which protects the confidentiality of internal memory (OTP). |
| 6.2 | FDP_SDC.1/PM<br>Stored data confidentiality for passive external memory | The confidentiality of the external NVM is ensured by the AEAD services. |
| 7.1 | FDP_SDI.2/IM<br>Stored data integrity monitoring and action for internal memories | Hardware TOE<br>This requirement is covered by the CRC checksum modules on each RAM memory. Sensitive data stored in OTP are also AEAD protected. |
| 7.2 | FDP_SDI.2/PM<br>Stored data integrity monitoring and action for passive external memory | The integrity of the external NVM is ensured by the AEAD services. |
| 8 | FPT_PHP.3<br>Resistance to physical attacks | Hardware TOE<br>The integration inside the TOE of the shield module enables to meet this requirement. The physical manipulation or the physical probing is detected or made very difficult by using techniques that enhance the security of the TOE by making the reverse-engineering unpredictable or very difficult to realize. |
| 9 | FDP_ITT.1<br>Basic internal transfer protection | Hardware TOE<br>The security features integrated in the TOE enable to achieve this requirement:<br>• Security mechanisms for memory protection<br>• Asynchronous logic. |
| 10 | FPT_ITT.1<br>Basic internal TSF data transfer protection | This requirement is achieved by the same security features used for covering security functional requirement FDP_ITT.1. |
| 11.1 | FDP_IFC.1/IM<br>Subset information flow control for internal memories | Hardware TOE<br>This requirement is covered by the memory encryption units for protecting all confidential data processing or transferring by the TOE or by the security IC embedded software.<br>Software TOE<br>Sensitive data such as keys are encrypted in OTP using the AEAD mechanism from ROM. |

| | | |
|---|---|---|
| 11.2 | FDP_IFC.1/PM<br>Subset information flow control for passive external memory | This requirement is covered by the AEAD mechanism for protecting all confidential data processing or transferring by the TOE from/to the passive external NVM. |
| 12.1 | FCS_RNG.1/RGS-IC<br>Random number generation - RGS_IC | The TRNG module integrated in the TOE covers this requirement. The TRNG follows some of the ANSSI RGS_B1 requirements (French scheme). |
| 12.2 | FCS_RNG.1/DRBG<br>Random number generation – DRBG | The DRBG developed in the crypto library part of the TOE covers this requirement. It relies on the TRNG to generate the seed. The DRBG library meets some of the ANSSI requirements (RGS_B1). |
| 12.3 | FCS_RNG.1/PRNG Pseudo-Random number generation – PRNG | The PRNG module integrated in the TOE covers this requirement. |
| 13 | FDP_ACC.1<br>Subset access control | Hardware TOE<br>The Subset access control is met by integrating the following secure features inside the TOE<br>• Security mechanisms for memory protection.<br>• Memory protection unit (MPU) for secure memory access.<br>• Mode protection.<br>• Restriction of use of TOE functionalities.<br>Software TOE<br>This SFR is covered by both the PRE-PERSO and ADMIN loaders which verify the authenticity of the commands and the loaded data. |
| 14 | FDP_ACF.1<br>Security attributes based access control | Hardware TOE<br>The Memory Access Control Policy is enforced by the MPUs, the non-reversibility and the bootloader, features which implement different access rights.<br>Software TOE<br>This SFR is covered by the loaders which uses cryptographic means to optionally authenticate users. |
| 15 | FMT_MSA.3<br>Static attribute initialization | Hardware TOE<br>When the TOE is reset, all sensitive register functions are initialized (by hardware) with default value.<br>Software TOE<br>The MPU is initialized by software by the ROM code at boot, by the ADMIN loader when started, or by the composite application. |
| 16 | FMT_MSA.1<br>Management of security attributes | Management of security attributes is covered by the security features integrated in TOE's memory protection unit (MPU). |

| | | |
|---|---|---|
| 17 | FMT_SMF.1<br>Specification of management functions | This requirement is achieved by the possibilities offered by the TOE to access to control registers of TOE's MPU. |
| 18 | FDP_RIP.1<br>Subset residual information protection | Software TOE<br>This requirement is achieved by all the software components of the TOE which clear the sensible content. |
| 19 | FCS_COP.1<br>Cryptography operation | This requirement is fulfilled by the following cryptography operation functions:<br>• Triple Data Encryption Standard (TDES) with 112 bits or 168 bits of key. This operation is fulfilled either by hardware functions or by software functions (through the secure crypto library using the secure hardware coprocessor).<br>• Advanced Encryption Standard (AES) with 128, 192 and 256 bits of key. This operation is fulfilled either by hardware functions or by software functions (through the secure crypto library using the secure hardware coprocessor).<br>• Public Key Accelerator (PKA) for RSA and ECC in GF(p) with key size from 128 up to 4096 bits. This module integrates 3 exponentiations functions for RSA key cryptosystem.<br>• RSA with key size from 128 up to 4096 bits. This operation is fulfilled by software functions through the optional secure crypto library using the Public Key Accelerator (PKA).<br>• ECC with key size from 128 up to 521 bits. This operation is fulfilled by software functions through the optional secure crypto library using the Public Key Accelerator (PKA).<br>• SHA hashing software function which implements the following algorithms: SHA2-224, SHA2-256, SHA2-384, SHA2-512. |
| 20.1 | FCS_CKM.1/RSA<br>Cryptographic key generation - RSA | The RSA key generation part of the optional Crypto library meets this requirement. It allows generating RSA key with size in the range 1280-bit and up to 4096-bit with 32-bit granularity. |
| 20.2 | FCS_CKM.1/ECDSA<br>Cryptographic key generation - ECDSA | The ECC key generation part of the optional Crypto library meets this requirement. It implements ECC key generation for size up to 640-bit. |
| 21 | FMT_LIM.1/Loader<br>Limited capabilities - Loader | The limited capabilities of Loader (this includes Test mode loader, pre-perso loader and admin loader) are met by the secure authentication system. |
| 22 | FMT_LIM.2/Loader<br>Limited availabilities - Loader | The limited availabilities of Loader (this includes Test mode loader, pre-perso loader and admin loader) are met by implementing a secure lock. |

| | | |
|---|---|---|
| 23 | FIA_API.1<br>Authentication Proof of Identity | The authentication proof of identity of the TOE to an external entity is provided by the loaders using the SCP03 protocol. |
| 24 | FTP_ITC.1<br>Inter-TSF trusted channel | The Inter-TSF trusted channel is supported by loaders using the SCP03 protocol. |
| 25 | FTP_UCT.1<br>Basic data exchange confidentiality | The confidentiality during basic data exchange is ensured by AES encryption and decryption. |
| 26 | FDP_UIT.1<br>Data exchange integrity | The integrity of data exchange is ensured by the AES-CMAC algorithm. |
| 27 | FDP_ACC.1/Loader<br>Subset access control - Loader | The access control is ensured by verifying the signature of the data to be sent to the PRE-PERSO and ADMIN loaders. |
| 28 | FDP_ACF.1/Loader<br>Security attribute based access control - Loader | The access control for both the PRE-PERSO and ADMIN loaders is ensured by the authentication of the loader commands. |
| 29 | FDP_URC.1 Protection against an unauthorized rollback of stored contents in Passive external NVM | The ADMIN loader and services are contained in a load package loaded in external NVM by the PRE-PERSO loader in phase 5. This package, provided by TIEMPO, is encrypted and can be loaded only once, following the procedure described in the guidance « AGD_OPE – eNVM Loader user role ». This package is the only package generated by TIEMPO which is signed and encrypted for each batch of PRE-PERSO loader keys.<br>The composite software is loaded in external NVM later in phase 5 by the ADMIN loader (TOE in ADMIN mode), and following the procedure described in the guidance « AGD_OPE – Admin loader user role ». The external NVM content is programmed using the ADMIN services which implement the anti-rollback protection. |
| 30 | FDP_IRA.1 Irreversibility Anchor of passive external NVM contents | The non-volatile irreversibility anchor is based on the internal monotonic counter. |
| 31 | FIA_UID.1 Timing of Identification | The TOE integrates a unique per device key which is used to decrypt and authenticate the passive external NVM content before using it. |
| 32 | FDP_DAU.2 Data Authentication with Identity of Guarantor | The passive external NVM content is identified by cryptographic means using a unique per device key. |
| 33 | FPT_RPL.1 Replay detection from passive external NVM | The TOE implements the replay detection by authenticating the external memory content along with a version information of the content based on the irreversibility anchor. The content authentication is performed using the AEAD services of the ROM code at boot, and the ADMIN services when started. |

# 8 ANNEX

## 8.1 Glossary

| | |
|---|---|
| **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 finalizing the IC Embedded Software and the applications on platform transforming the TOE into the unpersonalized Composite Product after TOE delivery.<br><br>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.<br><br>The customer of the TOE Manufacturer who receives the TOE during TOE Delivery. The Composite Product Manufacturer includes the Security IC Embedded Software developer and all roles after TOE Delivery up to Phase 6 (refer [1] and section 7). |
| **End-consumer** | User of the Composite Product in Phase 7. |
| **Hard Macro** | Is an intellectual property (IP) block stored in a set of files (e.g. gds-file) that includes final layout information (physical design, placement, routing, etc) of a component (or part of a component). A Hard macro is targeted towards a specific technology (e.g., SoC or IC manufacturing technology, or programmable logic device), and is predictable in terms of operational ranges such as performance, timing, area, and power. |
| **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. |
| **Initialization Data** | Initialization 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-personalization 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** | (as used in the Protection Profile) 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.<br><br>Some parts 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 |
| **System-On-Chip** | A System-On-Chip is an integrated circuit (also known as a "chip") that integrates all or most components of a computer or other electronic system. |
| **Test Features** | All features and functions (implemented by the IC Dedicated Test Software and/or hardware) which are designed to be used before TOE Delivery only and delivered as part of the TOE. |
| **TOE Delivery** | The period when the TOE is delivered which is (refer to Figure 2 on page 10) 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.<br><br>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 EEPROM) or a combination thereof. |
| **User data of the Composite TOE** | All data managed by the Security IC Embedded Software in the application context. |
| **User data of the TOE** | Data for the user of the TOE, that does not affect the operation of the TSF. From the point of view of TOE defined in this PP the user data comprises the Security IC Embedded Software and the user data of the Composite TOE. |

## 8.2 Literature

[1] Eurosmart Smartcard IC Platform Protection Profile with Augmentation Packages, Version 1.0, 2014, BSI-CC-PP-0084

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; April 2017, Version 3.1, Revision 5, CCMB-2017-04-001.

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; April 2017, Version 3.1, Revision 5, CCMB-2017-04-002.

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; April 2017, Version 3.1, Revision 5, CCMB-2017-04-003.

[5] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation

Methodology; April 2017, Version 3.1, Revision 5, CCMB-2017-04-004.

[6] ISO7816, ISO+IEC 7816-3-2006.pdf

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

[8] Federal Information Processing Standards Publication FIPS PUB 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed 1999 October 25, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology.

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

[10] 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.

[11] Laboratories RSA RSA Cryptography Standard, PKCS #1 v2.1, 2002.

[12] Internal Standard ISO/IEC 13239, third edition, July 2002.

[13] Smartcard Integrated Circuit Platform Augmentations, version 1.00, March 8, 2002, developed by Atmel, Hitachi Europe, Infineon Technologies, and Philips Semiconductors.

[14] Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques.
Annexe B1 du RGS 2.0. Version 2.04, 01/01/2020, ANSSI.
https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf

[15] GlobalPlatform Secure Channel Protocol 03 – Card Specification v2.2 – Amendment D.

[16] Federal Information Processing Standards Publication 180-4 SECURE HASH STANDARD U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 2011 February, 11

[17] NIST SP 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005.

[18] GSM Association, Official Document SGP.01 - Embedded SIM Remote Provisioning Architecture, Version 4.2, 05 June 2020.

## 8.3 List of Abbreviations

| | |
|---|---|
| AFE | Analog Front End |
| AL | Admin Loader |
| BL | Bootloader |
| CC | Common Criteria |
| CL | Crypto Library |
| DCXO | Digital Controlled Crystal Oscillators |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| HW | Hardware |
| I2S | Inter-IC Sound |
| IC | Integrated Circuit |
| IT | Information Technology |
| MCU | Microcontroller Unit |
| MSSR | Minimal Site Security Requirements |
| MSSPI | Multiple Slave Serial Peripheral Interface |
| OTP | One Time Programmable |
| PCM | Pulse-code modulation |
| PMU | Power Management Unit |
| PP | Protection Profile |
| PSRAM | Pseudo-Static Random Access Memory |
| QSPI | Quad Serial Peripheral Interface |
| SAR | Security Assurance Requirement |
| SE | Security Enclave |
| SFR | Security Functional Requirements |
| SoC | System on Chip |
| ST | Security Target |
| TC | Tuning Capacitance |
| TCXO | Temperature Controlled Crystal Oscillator |

| | |
|---|---|
| TOE | Target of Evaluation |
| TSC | TSF Scope OF Control |
| TSF | TOE Security Functionality |
| VCO | Voltage Controlled Oscillator |
| WDT | Watch Dog Timer |