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

ASE_ST - Security Target Lite

TESIC-SC-02.1

D-SPD-402-511-2.0

Security Level 1: Public

Revision: 2.0

Date: 27/07/2017

Tiempo Trademarks and Copyright Information

Contents

Figures and Tables

Version

Version	Date	Description
2.0	27/07/2017	Release 2.0 of ASE_ST - Security Target Lite

1 Security Target Introduction

1 This chapter 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 "ASE_ST - Security Target Lite", is in its version 2.0 and is dated 27/07/2017. The Security Target comprises the Tiempo Security IC TESIC-SC-02.1 with specific IC-dedicated firmware and with optional cryptographic library. The Target of Evaluation (TOE) TESIC-SC-02.1 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+.

Title:	ASE_ST - Security Target Lite
Target of Evaluation	TESIC-SC-02.1
TOE reference:	TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC25 TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC40 TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC55 TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC70
Provided by:	TIEMPO-IC
Evaluation schema:	France (ANSSI)
Evaluator:	LETI CEA France
Common Criteria version:	[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; September 2012, Version 3.1, Revision 4, CCMB-2012-09-001. [3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; September 2012, Version 3.1, Revision 4, CCMB-2012-09-002. [4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; September 2012, Version 3.1, Revision 4, CCMB-2012-09-003. [5] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; September 2012, Version 3.1, Revision 4, CCMB-2012-09-004.

1.2 TOE Overview and TOE Description

1.2.1 Introduction

5 The Target of Evaluation (TOE) is the TESIC-SC-02.1. It is a chip with dual interfaces (contact ISO7816 and contactless ISO14443) and Flash memory up to 504 Kbytes supporting various secured transactions – payments, ticketing and identification - with high performance and enforced security.

1.2.2 TOE Definition

6 The TESIC-SC-02.1 is a Security IC based on Tiempo TESIC-SC asynchronous platform, built around an 8/16-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-SC-02.1 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.
- Physical True Random Number Generator (PTRNG) that meets some of ANSSI requirements (RGS_B1).
- Pseudo Random Number Generator (PRNG): no compliance to any specific metric
- 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.

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

8 The operating temperature range is defined as:

- -25°C to +85°C

9 The operating voltage range is defined as:

- Support class A operations: 4.5 V – 5.5 V
- Support class B operations: 2.7 V – 3.3 V

1.2.3 TOE Hardware

10 The overview of the hardware architecture is presented on Figure 1-1.

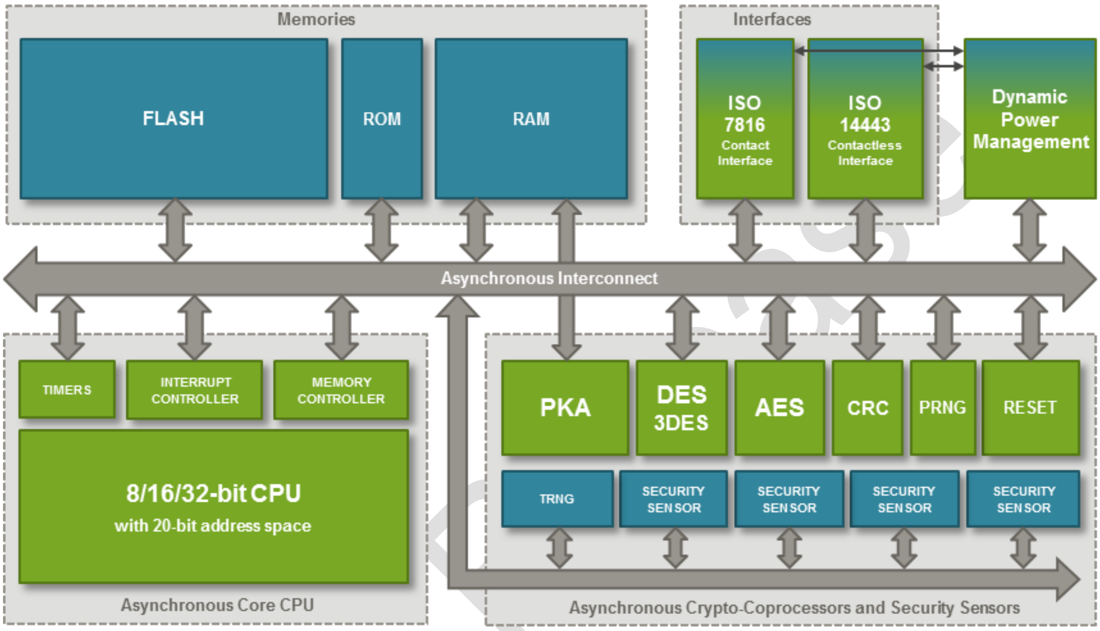


Figure 1-1: Block diagram of the TOE

11 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]
- Hardware contactless interface compliant with ISO14443-3 [7]
- Hardware AES cryptographic coprocessor compliant with the AES-128, AES-192 and AES-256 standards [8].
- Hardware DES/Triple DES cryptographic coprocessor with 56 bits, 112 bits and 168 bits of key sizes [9].
- 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 [12].
- CRC-16 block compliant with ISO/IEC 13239 with additional recommendation in CCITTv41 [13].

- Security sensors.
- Physical True Random Number Generator (PTRNG) that meets some of ANSSI requirements (RGS_B1).
- Pseudo Random Number Generator (PRNG): no compliance to any specific metric
- Shield.
- Flash memory up to 504 Kbytes
- RAM of 8 Kbytes.
- Read-Only Memory of 16 Kbytes.
- Power on reset.
- Reset block.
- Memory controller block (BUS).
- Oscillator.
- Memory protection unit (MPU).

1.2.4 TOE Software

12 The software component contained in the TOE is listed below:

- The IC Dedicated Test software. It is used to support testing of the IC during production and does not provide any security functionality to be used after TOE delivery. The IC Dedicated Test Software is integrated in ROM, it includes programs that enable to support test mode. **Those programs are not part of the TOE**; they are only available in test mode and are deactivated after the test.
- 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 start the product.
  - The Admin Loader used to download user software.
  - The Crypto Library (optional).

13 The overview of the Crypto Library is presented in the block diagram in Figure 1-2.

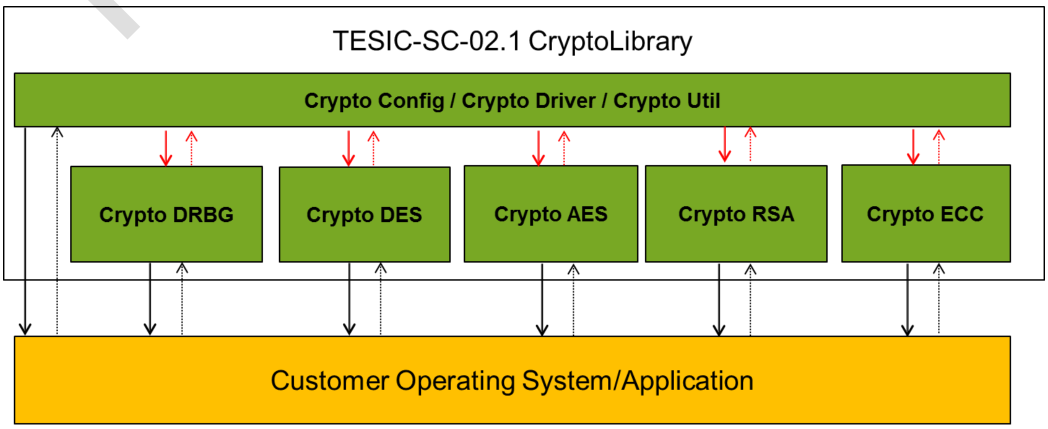


Figure 1-2 Crypto Library Software Components of the TOE

14 The software components of the Crypto Library are described below.

- The optional secure DRBG library built on top of the TESIC-SC-02.1 cryptographic coprocessors and PTRNG. 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 NRBG seed matching a 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-SC-02.1 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-SC-02.1 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.
- The optional secure RSA library built on top of the TESIC-SC-02.1 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-SC-02.1 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.

1.2.5 TOE Configuration

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

Component	Version	Date
Hardware, delivered as wafer, die or smartcard package		
TESIC-SC-02.1 IC, with tuning capacitance of 40 pF TESIC-SC-02.1 IC, with tuning capacitance of 55 pF TESIC-SC-02.1 IC, with tuning capacitance of 70 pF TESIC-SC-02.1 IC, with tuning capacitance of 25 pF	2.1	
Software, integrated in ROM memory		
TESIC-SC-02.1 Secure Bootloader	1	
Software, delivered as Embedded software		
TESIC-SC-02.1 Admin Loader TESIC-SC-02.1 Cryptographic Library	1.0.0 1.0.D	28/06/2017
Guidance, delivered as electronic document		
TESIC-SC-02.1 AGD_OPE - Operational User Guidance	2.0	12/07/2017
TESIC-SC-02.1 Hardware User Manual	2.0	21/07/2017
TESIC-SC-02.1 Crypto Library User Manual	2.0	12/07/2017
TESIC-SC-02.1 Software Development Kit User Manual	5.0	03/11/2016
TESIC-SC-02.1 - Admin Loader User Manual	2.0	12/07/2017
TESIC-SC-02.1 AGD_OPE - Developer role	2.0	12/07/2017
TESIC-SC-02.1-CL AGD_OPE - Security Guidelines	2.0	12/07/2017
TESIC-SC-02.1 AGD_OPE - Loader role	2.0	12/07/2017
TESIC-SC-02.1 AGD_PRE - Loader role	2.0	12/07/2017
TESIC-SC-02.1 AGD_PRE - Packaging - Specifications for assembly	2.0	21/07/2017

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

16 The Table 1-2 gives the expected values of the TOE hardware identifiers for the TOE Reference TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC40.

Identifier	Expected value
IC TYPE	0x0005
ROM ID	0x0001
Mask Revision	0x2
Tuning Capacitance	0x0 (40 pF)

Table 1-2: TOE Hardware identification for the TOE Reference TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC40

17 The Table 1-3 gives the expected values of the TOE hardware identifiers for the TOE Reference TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC55.

Identifier	Expected value
IC TYPE	0x0005
ROM ID	0x0001
Mask Revision	0x2
Tuning Capacitance	0x1 (55 pF)

Table 1-3: TOE Hardware identification for the TOE Reference TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC55

18 The Table 1-4 gives the expected values of the TOE hardware identifiers for the TOE Reference TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC70.

Identifier	Expected value
IC TYPE	0x0005
ROM ID	0x0001
Mask Revision	0x2
Tuning Capacitance	0x2 (70 pF)

Table 1-4: TOE Hardware identification for the TOE Reference TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC70

19 The Table 1-5 gives the expected values of the TOE hardware identifiers for the TOE Reference TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC25.

Identifier	Expected value
IC TYPE	0x0005

ROM ID	0x0001
Mask Revision	0x2
Tuning Capacitance	0x3 (25 pF)

Table 1-5: TOE Hardware identification for the TOE Reference TESIC-SC-02.1-HW02.1.2-BL01-AL01.0.0-CL01.0.D-TC25

1.2.6 TOE Life Cycle

20 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 - IC Design - IC Dedicated Software development.	TIEMPO SAS	110 rue Blaise Pascal Bâtiment Viseo –Inovallée 38330 Montbonnot Saint Martin FRANCE T : +33 4 76 61 10 00 F : +33 4 76 44 19 69
Phase 3	IC Manufacturing - Mask preparation - Integration and photo mask fabrication. - IC production	LFOUNDRY COMPUGRAPHICS International Ltd LFOUNDRY	Herrngasse 379-381 84028 Landshut GERMANY Newark Road North Eastfield industrial Estate Glenrothes Fife, KY7 4NT SCOTLAND Via A. Pacinotti 7 67051 Avezzano (AQ) ITALIA T : +39 0863 4231 F : +39 0863 412763
Phase 3	IC testing - Preparation and Pre-personalization	PRESTO-Engineering	Arteparc de Bachasson – Bât A Rue de la carrière de Bachasson 13590 Meyreuil FRANCE
Phase 4	IC Packaging - Security IC packaging	SPS Micro-PackS HCM	Avenue de la Plaine ZI de Rousset 13106 Rousset FRANCE T : + 351 252 246 000 F : + 351 252 246 001 Centre de Microélectronique de Provence 880 avenue de Mimet 13451 Gardanne FRANCE T : +33 4 42 61 66 00 F : +33 4 42 61 65 96 Z.I. Périgny

			34 Avenue Joliot-Curie 17185 PERIGNY FRANCE T : +33 5 46 45 12 70 F : +33 5 46 45 04 44
		PRESTO UTAC-TH	UTAC Thai Limited (UTL3) C1 (Building C, 1st floor) 73 Moo 5 Wellgrow Industrial Estate Bangsamak, Bangpakong Chachoengsao, 24180 THAILAND
		NedCard B.V.	Bijsterhuizen 2529 6604 LM Wijchen THE NETHERLANDS
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. - The Composite Product finishing process, preparation and shipping to the personalization line for the Composite Product		
Phase 6	Personalization - The Composite Product personalization and testing stage where the User Data is loaded into the Security IC's memory.		
Phase 7	Operational Usage - The Composite Product usage by its issuers and consumers which may include loading and other management of applications in the field.		

Table 1-6: Life cycle phases & development location

21 The definition of “TOE Delivery” and the responsible parties are presented in Figure 1-3. It also includes for each life cycle phase the state (security domain) of the TOE.

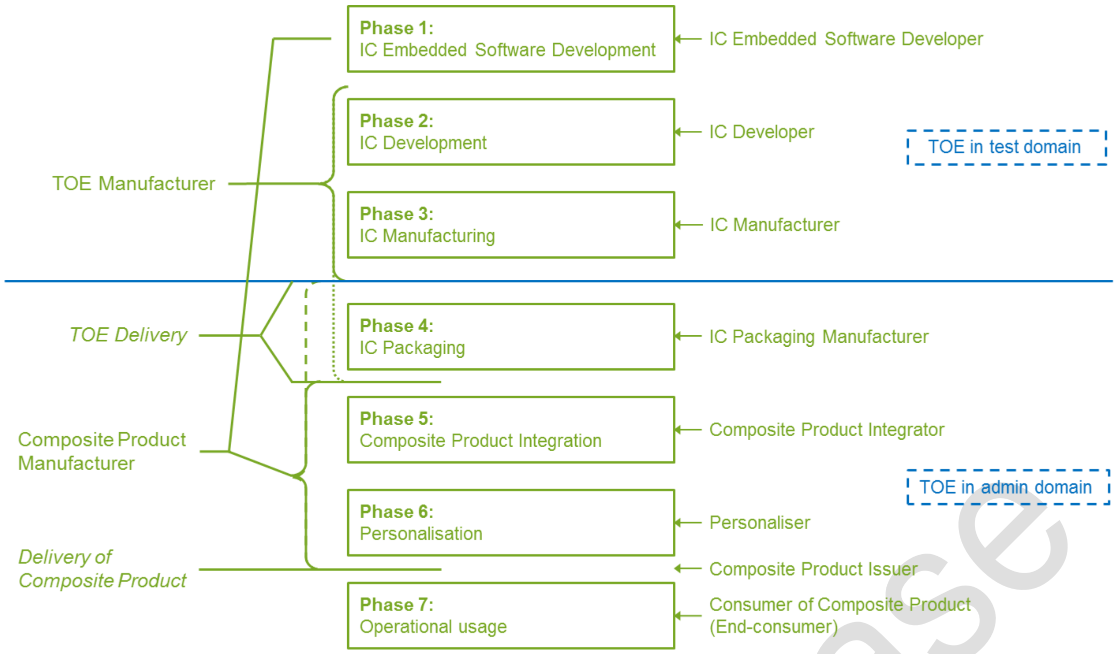


Figure 1-3: Definition of "TOE Delivery" and responsible Parties

22 The Security IC Embedded Software is developed outside the TOE development in Phase 1. The TOE is developed in Phase 2 and produced in Phase 3. Then the TOE is delivered in form of wafers or sawn wafers (dice). The TOE can also be delivered in form of packaged products. In this case the corresponding assurance requirements for the development and production of the TOE not only pertain to Phase 2 and 3 but to Phase 4 in addition.

23 In the following the term "TOE Delivery" (refer to Figure 1-3) is uniquely used to indicate:

- after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or
- after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.

24 The Protection Profile uniquely uses the term "TOE Manufacturer" (refer to Figure 1-3) which includes the following roles:

- the IC Developer (Phase 2) and

  the IC Manufacturer (Phase 3)

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

- the IC Developer (Phase 2),

  the IC Manufacturer (Phase 3) and

  the IC Packaging Manufacturer (Phase 4)

if the TOE is delivered after Phase 4 in form of packaged products.

25 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.

26 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).

27 The loader is intended to be used in Phases 3 to 5, and must be locked in Phase 6 before the Personalisation starts.

1.2.7 TOE security domains

28 The TOE integrates two separated domains:

- Test domain: It is the default domain after manufacturing (wafer and test). This domain contains the test mode used for validation, characterization and industrial tests. This mode of operation is available up to the end of phase 3 of TOE life cycle (subsection 1.2.4). This mode of operation is disabled by wafer saw.
- Admin domain: this domain comes after the test domain. It contains the following modes:
  - The admin mode. It is used to modify the default settings of the chip and for downloading operating system (firmware). The TOE is delivered in administration mode either at the end of phase 3 or at the end of phase 4. This mode of operation is available throughout the life cycle of the TOE.
  - The kernel mode: this mode is the privileged mode in which the loaded firmware is started. In this mode, a firmware can configure the MPU to allow accesses to resources. This mode of operation is available during all the life cycle of the TOE.
  - The user mode: this mode is the unprivileged mode, it is the last mode used by the final user. In this mode the chip is configured with operating system and application (composite product) which the user can execute with less rights. This mode of operation is available during all the life cycle of the TOE.

The test mode of the test domain and the admin mode of the admin domain both require to follow an authentication process.

1.3 Interfaces of the TOE

29 The interface of the TOE are listed below:

- The physical interface of the TOE with the external environment is the entire surface of the IC
- The electrical interface of the TOE with the external environment is made of the pads of the chip: VCC, RST, CLK, GND, IO (Input / Output for the contact interface), LA and LB as well as the contactless radio-frequency interface
- The data interface of the TOE is made of the Contact I/O pads and the Contactless I/O pads

1.3.1 Software Interfaces

30 The software interfaces consist of interfaces between hardware and software. It is made of interface registers. All TESIC-SC-02.1 blocks, particularly the crypto-processors integrate such registers which enable together with software drivers to access into TESIC-SC-02.1 hardware functions. The details of these registers are given in [14].

31 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)

1.4 TOE intended Usage

35 The TESIC-SC-02.1 is intended to support the following applications:

- Banking and payment applications.
- NFC/Mobile transactions.
- Transport and ticketing services.
- Identification and health applications.
- Digital rights management (DRM) applications.

2 Conformance Claims

36 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)

2.1 CC Conformance Claim

37 This Security Target claims to be conformant to the Common Criteria version 3.1 R4 [2], [3], [4], and [5].

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

39 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; September 2012, Version 3.1, Revision 4, CCMB-2012-09-001.

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; September 2012, Version 3.1, Revision 4, CCMB-2012-09-002.

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; September 2012, Version 3.1, Revision 4, CCMB-2012-09-003.

40 The

[5] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; September 2012, Version 3.1, Revision 4, CCMB-2012-09-004.

has been taken into account.

2.2 PP Claim

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

42 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.

43 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

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

2.3 PP Additions

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

- T.Mem-Access
- T.Open_Samples_Diffusion
- A.Key-Function
- O.Mem-Access
- O.PKA
- O.RSA
- O.ECC
- O.Prot_TSF_Confidentiality
- 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_CKM.1/RSA
- FCS_CKM.1/ECDSA

2.4 Package Claim

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

47 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

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

49 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.

50 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].

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

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

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

- Threats
- Organisational 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 6 of this Security Target.

3 Security Problem Definition

54 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

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

- the user data of the composite TOE,
- the Security IC Embedded Software, stored and in operation,
- the security services provided by the TOE for the Security IC Embedded Software.

56 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.

57 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.

58 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.

59 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.

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

SC4 deficiency of random numbers.

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

- logical design data, physical design data, IC Dedicated Software, and configuration data,
- Initialization Data and Pre-personalization Data, specific development aids, test and characterization related data, material for software development support, and photo masks.

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

63 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.

64 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.

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

- logical design data,
- physical design data,
- IC Dedicated Software, Security IC Embedded Software, 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,

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

3.2 Threats

66 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.

67 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.

68 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.

69 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.

70 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.

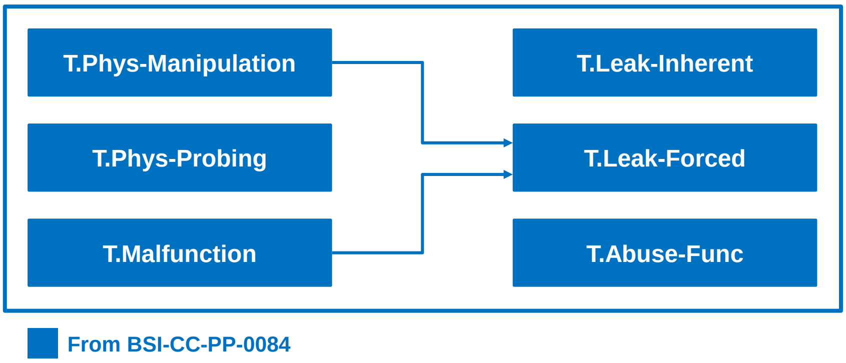


Figure 3-1: Standard Threats

71 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).

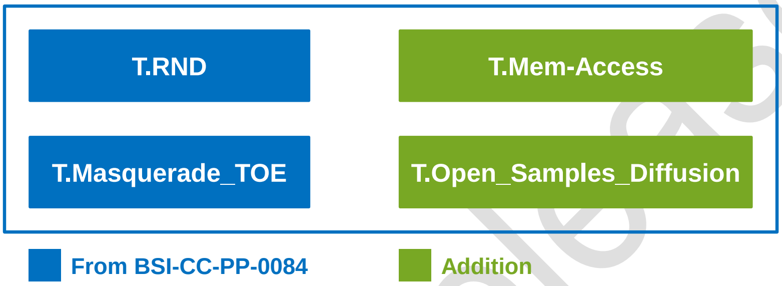


Figure 3-2: Threats related to security service

72 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 3.4.

73 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.

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

75 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.

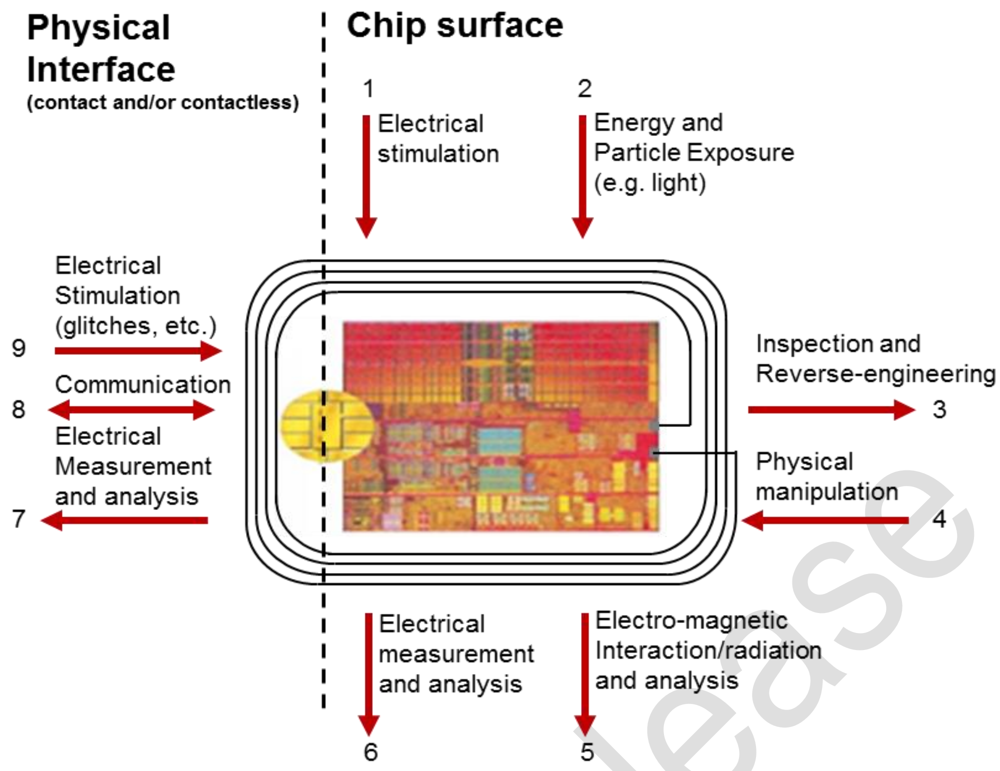


Figure 3-3: Interactions between the TOE and its outer world

76 An interaction with the TOE can be done through the physical interfaces (Number 7–9 in Figure 3-3) which are realized using contacts and/or a contactless 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 behavior 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

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

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

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.

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

T.Phys-Probing — Physical Probing

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

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 pre- requisite.

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.

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

T.Malfunction — Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of the Security IC Embedded Software by applying environmental stress in order to (i) modify security services of the TOE or (ii) modify functions of the Security IC Embedded Software (iii) deactivate or affect security mechanisms of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software. This may be achieved by operating the Security IC outside the normal operating conditions (Numbers 1, 2 and 9 in Figure 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.

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

T.Phys-Manipulation — Physical Manipulation

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

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).

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

T.Leak-Forced Forced Information Leakage

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

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.

82 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

83 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

84 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 the TOE memory access rules (refer to T.Abuse-Func but for functions available after TOE delivery), (ii) introduce flaws by forcing operational conditions (refer to T.Malfunction) and/or by physical manipulation (refer to T.Phys-Manipulation). This attacker is expected to have a high level potential of attack.

3.2.4 Threats related to Authentication of the Security IC

85 The TOE shall avert the additional threat "Masquerade the TOE (T.Masquerade-TOE)" as specified below.

T.Masquerade-TOE	Masquerade the TOE An attacker may threaten the property being a genuine TOE by producing a chip which is not a genuine TOE but wrongly identifying itself as genuine TOE sample.

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

3.2.5 Threats related to Package 2 for Loader

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

3.3 Organizational Security Policies

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

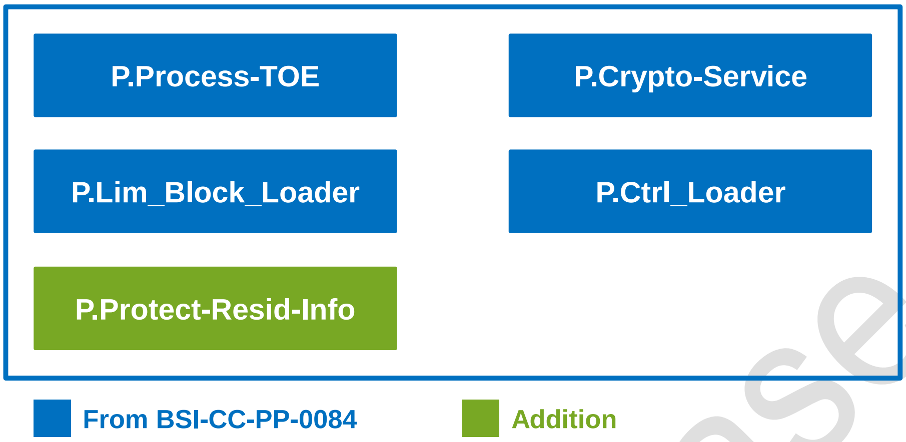


Figure 3-4: Policies

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

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

90 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, Security IC Embedded 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.

91 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 The TOE shall provide an additional security functionality to the Security IC Embedded Software to ensure the protection of

residual information.

92 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

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 Smartcard 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).

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).

93 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

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.

94 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

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

3.4 Assumptions

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

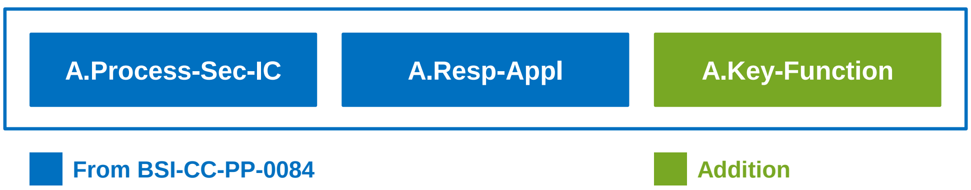


Figure 3-5: Assumptions

96 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. The Composite Product is used in a terminal which supplies the Security IC (with power and clock) and (at least) mediates the communication with the Security IC Embedded Software.

97 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.

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

99 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.

100 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.

101 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.

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

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

103 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.

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

A.Key-Function	Usage of Key-dependent Functions Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced).

105 Note that here the routines which may compromise keys when being executed are part of the Smartcard Embedded Software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE and (ii) the processing of User Data including cryptographic keys

4 Security Objectives

106 This chapter Security Objectives contains the following sections:

Security Objectives for the TOE (4.1)

Security Objectives for the Security IC Embedded Software development environment (4.2)

Security Objectives for the operational Environment (4.3)

Security Objectives Rationale (4.4)

4.1 Security Objectives for the TOE

107 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.

108 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.

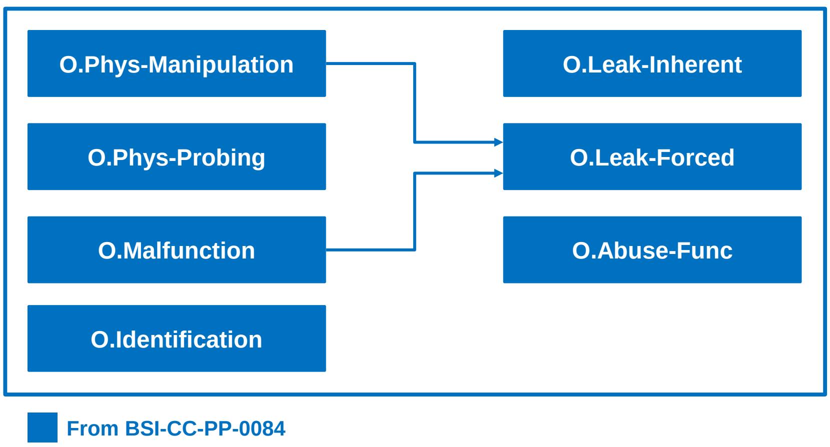


Figure 4-1: Standard Security Objectives

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

SG4 Provide true random numbers.

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

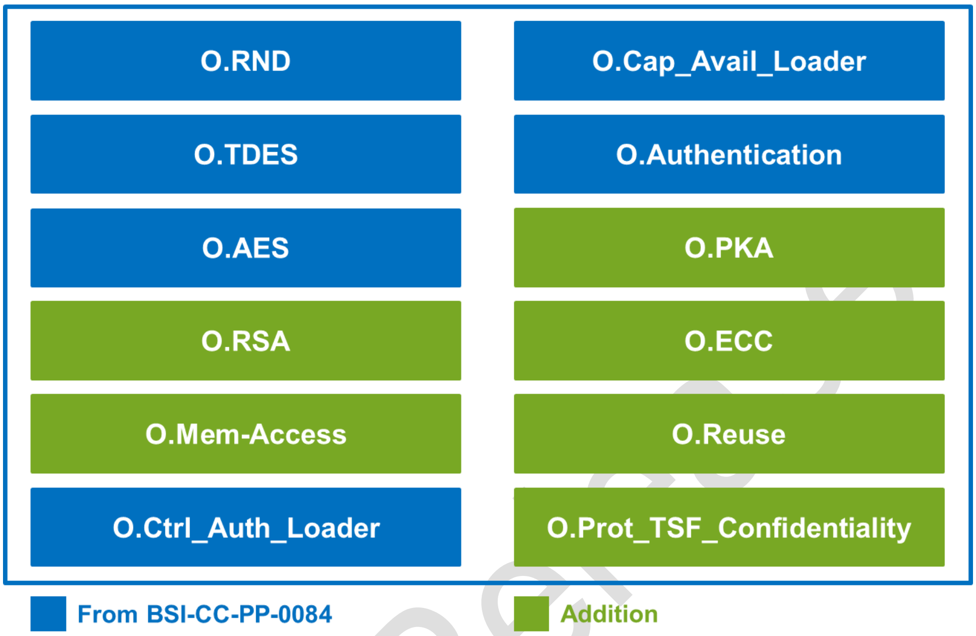


Figure 4-2: Security Objectives related to Specific Functionality

Standard Security Objectives

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

O.Leak-Inherent Protection against Inherent Information Leakage

The TOE must provide protection against disclosure of confidential data stored and/or processed in the Security IC

by measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and

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

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

112 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.

113 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.

114 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.

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

O.Leak-Forced — Protection against Forced Information Leakage

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

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

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

116 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.

117 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 Specific Functionality (referring to SG4)

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

O.RND — Random Numbers

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

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

Security Objectives for Cryptographic Services

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

O.TDES — Cryptographic service Triple-DES

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

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

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

O.AES	Cryptographic service AES The TOE provides secure hardware based cryptographic services for the AES for encryption and decryption.

122 The security objective "Cryptographic service AES (O.AES)" enforces the organizational security policy P.Crypto-Service.

123 The TOE shall provide "Cryptographic service PKA (O.PKA)" as specified below.

O.PKA	Cryptographic service PKA The TOE shall provide the following specific security functionality to the Smartcard 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).

124 The security objective "Cryptographic service PKA (O.PKA)" enforces the organizational security policy P.Crypto-Service.

125 The TOE shall provide "Cryptographic service RSA (O.RSA)" as specified below.

O.RSA	Cryptographic service RSA The TOE provides shall provide the following specific security functionality to the Smartcard Embedded Software: 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.

126 The security objective "Cryptographic service RSA (O.RSA)" enforces the organizational security policy P.Crypto-Service.

127 The TOE shall provide "Cryptographic service RSA (O.ECC)" as specified below.

O.ECC	Cryptographic service ECC The TOE provides shall provides the following specific security functionality to the Smartcard Embedded Software: 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).

128 The security objective "Cryptographic service ECC (O.ECC)" enforces the organizational security policy P.Crypto-Service.

Security Objectives for Added Function

129 The TOE shall provide "Area based Memory Access Control (O.Mem-Access)" as specified below.

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

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

O.Reuse	Cryptographic reuse of memory
	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.

131 The TOE shall provide "Capability and availability of the Loader (O.Cap-Avail-Loader)" as specified below.

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

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

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

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

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

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

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

4.2 Security Objectives for the Security IC Embedded Software development environment

135 The development of the Security IC Embedded Software is outside the development and manufacturing of the TOE (cf. section 1.2.4). 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.

136 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

137 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 Security relevant user data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context. For example the Security IC Embedded Software will not disclose security relevant user data of the Composite TOE to unauthorized users or processes when communicating with a terminal.

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

138 User Data are defined but not limited to cipher or plain text data and cryptographic keys. These data shall be manipulated appropriately by the Smartcard 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.

139 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).

140 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

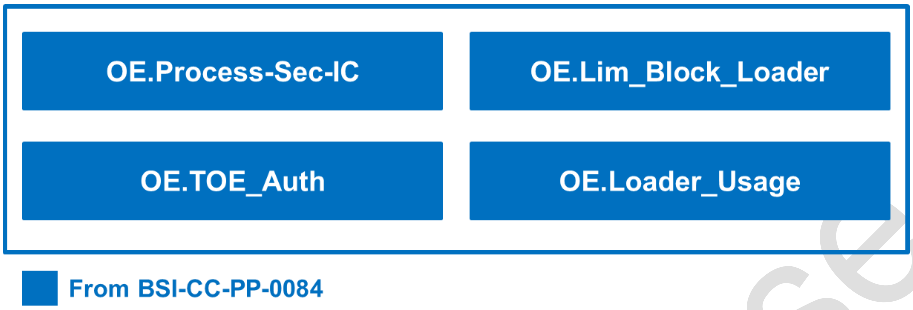


Figure 4-4: Security Objectives for the operational Environment

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

141 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 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). This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 1.2.4) must be protected appropriately. For a preliminary list of assets to be protected refer to Section 3.4.

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

142 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.

143 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)"

144 The operational environment of the TOE shall provide "Limitation of capability and blocking the Loader (OE.Lim_Block_Loader)" as specified below.

OE.Lim_Block_Loader	Limitation of capability and blocking the loader The Composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.

145 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)"

146 The Loader functionality during phases 3 to 6 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.

147 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 6 of the life cycle.

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

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

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

149 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.

150 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)"

151 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 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

152 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 O.AES O.PKA O.RSA O.ECC	
A.Key-Function	OE.Resp-Appl	
P.Lim_Block_Loader	O.Cap_Avail_Loader OE.Lim_Block_Loader	Phase 3 to phase 6
T.Masquerade_TOE	O.Authentication OE.TOE_Auth	
T.Open_Samples_Diffusion	O.Prot_TSF_Confidentiality O.Leak-Inherent O.Leak-Forced	
P.Ctrl_Loader	O.Ctrl_Auth_Loader OE.Loader_Usage	Phase 3 to phase 5

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

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

154 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.

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

156 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.

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

158 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.

159 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:

160 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.

161 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 Smartcard 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.

162 The Smartcard 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 Smartcard Embedded Software access control functions. Clarification "Treatment of User Data (OE.Resp-Appl)” emphasizes this point by reminding that the Smartcard Embedded Software must not bypass access memory restrictions. This clarification allows covering the threat T.Mem-Access.

163 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.

164 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)" and "Cryptographic service ECC (O.ECC)" is as follows:

165 Since the objectives O.TDES, O.AES, O.PKA, O.RSA and O.ECC 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.

166 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.

167 The clarification has been made for the security objective "Treatment of User Data (OE.Resp-Appl)". The Smartcard 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.

168 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.

169 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.

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

171 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)".

172 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)".

5 Extended Components Definition

173 This chapter presents the extended component definition. The extended components are listed as follows:

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

5.1 Definition of the Family FCS_RNG

174 To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

FCS_RNG Generation of random numbers

Family behavior

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component levelling:

FCS_RNG Generation of random numbers	1

FCS_RNG.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic] random number generator that implements: [assignment: list of security capabilities].

FCS_RNG.1.2 The TSF shall provide [selection: bits, octets of bits, numbers [assignment: format of the numbers]] that meet [assignment: a defined quality metric].

5.2 Definition of the Family FMT_LIM

175 To define the IT security functional requirements of the TOE an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements are defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE (refer to Section 6.1) appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

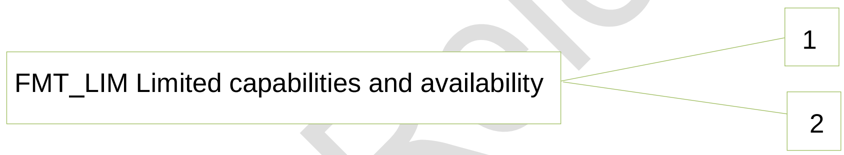
176 The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

FMT_LIM Limited capabilities and availability

Family behavior

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the component Limited Capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



FMT_LIM.1	Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
FMT_LIM.2	Limited availability requires that the TSF restricts the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.
Management:	FMT_LIM.1, FMT_LIM.2 There are no management activities foreseen.
Audit:	FMT_LIM.1, FMT_LIM.2 There are no actions defined to be auditable.

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

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 its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: Limited capability policy].

178 The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

FMT_LIM.2	**Limited capabilities**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited availability.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: Limited availability policy].

5.3 Definition of the Family FAU_SAS

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

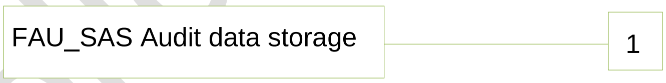
180 The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS Audit data storage

Family behavior

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

Component levelling:



FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management:	FAU_SAS.1 There are no management activities foreseen.
Audit:	FAU_SAS.1 There are no actions defined to be auditable.
FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide [assignment: list of subjects] with the capability to store [assignment: list of audit information] in the [assignment: type of persistent memory].

5.4 Definition of the Family FDP_SDC

181 To define the security functional requirements of the TOE an additional family (FDP_SDC.1) of the Class FDP (User data protection) is defined here.

182 The family “Stored data confidentiality (FDP_SDC)” is specified as follows.

FDP_SDC Stored data confidentiality

Family behavior

This family provides requirements that address protection of user data confidentiality while these data are stored within memory areas protected by the TSF. The TSF provides access to the data in the memory through the specified interfaces only and prevents compromising of this information by bypassing these interfaces. It complements the family Stored data integrity (FDP_SDI) which protects the user data from integrity errors while being stored in the memory.

Component levelling:

FDP_SDC Stored data confidentiality — 1

FDP_SDC.1 Requires the TOE to protect the confidentiality of information of the user data in specified memory areas.

Management: FDP_SDC.1

There are no management activities foreseen.

Audit: FDP_SDC.1

There are no actions defined to be auditable.

FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDC.1.1 The TSF shall ensure the confidentiality of the information of the user data while it is stored in the [assignment: memory area].

5.5 Definition of the Family FIA_API

183 To describe the IT security functional requirements of the TOE a functional family FIA_API (Authentication Proof of Identity) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity by the TOE and enables the authentication verification by an external entity. The other families of the class FIA address the verification of the identity of an external entity by the TOE.

184 To describe the IT security functional requirements of the TOE a functional family FIA_API (Authentication Proof of Identity) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity by the TOE and enables the authentication

verification by an external entity. The other families of the class FIA address the verification of the identity of an external entity by the TOE.

185 The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [3], chapter "Extended components definition (APE_ECD)") from a TOE point of view.

FIA_API Authentication Proof of Identity

Family behavior

This family defines functions provided by the TOE to prove its identity and to be verified by an external entity in the TOE IT environment

Component levelling:

FIA_API.1 Authentication Proof of Identity — 1

FIA_API.1	Authentication Proof of Identity, provides proof of the identity of the TOE, an object or an authorized user or role to an external entity.
Management:	FIA_API.1 The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.
Audit:	FIA_API.1 There are no actions defined to be auditable.

FIA_API.1	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1	The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [selection: *TOE*, [assignment: *object, authorized user or role*]] to an external entity.

6 IT Security Requirements

186 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

187 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 T.Leak-Forced T.Abuse-Func T.RND
2	FPT_FLS.1	Failure with preservation of secure state	BSI-CC-PP-0084	T.Malfunction T.Leak-Forced T.Abuse-Func 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	FDP_SDC.1	Stored data confidentiality	BSI-CC-PP-0084 (extended component)	T.Phys-Probing T.Phys-Manipulation
7	FDP_SDI.2	Stored data integrity monitoring and action	BSI-CC-PP-0084	T.Phys-Probing T.Phys-Manipulation
8	FPT_PHP.3	Resistance to physical attack	BSI-CC-PP-0084	T.Phys-Probing T.Phys-Manipulation T.Leak-Forced T.Abuse-Func T.RND
9	FDP_ITT.1	Basic internal transfer protection	BSI-CC-PP-0084	T.Leak-Inherent T.Leak-Forced T.Abuse-Func T.RND
10	FPT_ITT.1	Basic internal TSF data transfer protection	BSI-CC-PP-0084	T.Leak-Inherent T.Leak-Forced T.Abuse-Func T.RND
11	FDP_IFC.1	Subset information flow control	BSI-CC-PP-0084	T.Leak-Inherent T.Leak-Forced T.Abuse-Func 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	Random number	BSI-CC-PP-0084	T.RND

	/DRBG	generation – DRBG	(extended component)	
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
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	T.Masquerade_TOE

			of the Security IC")	
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

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

188 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

189 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.**

190 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

191 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.***

192 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.

193 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.***

194 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.***

195 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 the test process before TOE Delivery with the capability to store ***the initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software 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

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

FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDC.1.1 The TSF shall ensure the confidentiality of the information of the user data while it is stored in ***the ROM, CRAM, RAM or FLASH memories***.

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

FDP_SDI.2	**Stored data integrity monitoring and action**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for ***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 Flash, RAM and CRAM memories***.
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF ***shall reset the TOE or generates a maskable interrupt signal***.
Refinement:	**The TOE needs additional support by the Embedded Software to check data integrity on Flash memory with the help of CRC coprocessor.**

198 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 the TOE reset or generates a Maskable Interrupt. These features enable to meet the security functional requirement of FPT_PHP.3.

6.1.4 Leakage

199 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.**

200 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.**

201 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.

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

FDP_IFC.1 **Subset information flow control**

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes.

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

203 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

204 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 [16] and the recommendation RecomArchiGVA-1 of [16], total failure tests and online tests.***
FCS_RNG.1.2/RGS-IC	The TSF shall provide ***random numbers*** that meet ***the rule RègleArchiGVA-2 of [16].***
Warning	**The TSF fulfills some but not all the necessary rules to comply with [16] regarding random numbers generators (RNG). The composite product's RNG will comply with [16] only when all the rules of §2.4 "Génération d'aléa cryptographique" of [16] are addressed. In particular, a cryptographic post-processing must be implemented by the composite developer.**
Application note:	The PTRNG integrates a post-processing function with features that enable to perform online tests and statistical tests.

205 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:** **(DRBG.1) the rule *RègleArchiGDA-4 of [16] and* the recommendation *RecomArchiGDA-1 of [16].*** **(DRBG.2) the rule *RègleAlgoGDA-1 of [16].***
FCS_RNG.1.2/DRBG	The TSF shall provide ***random numbers*** that meet ***the rules RègleAlgoGDA-2 and RègleAlgoGDA-3 of [16].***
Application note	The DRBG relies on a random seed provided by the PTRNG.

6.1.6 Memory Access Control

206 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.

207 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, administrator mode, kernel mode and user mode), all objects (data including code stored in ROM, CRAM, RAM and FLASH memories) and all the operations among subjects and objects covered by the SFP.***

208 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 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: ***ROM, CRAM, RAM, FLASH Data and FLASH Code memories. 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***.

209 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 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.

210 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 FDP_IFC.1 Subset information flow control FMT_SMF.1 Specification of management functions 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****.*

211 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

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

213 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

214 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.

215 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)

216 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 [10], NIST SP 800-38A [11]***.

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 [10], NIST SP 800-38A [11]***.

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 and CBC modes*** and cryptographic key sizes: ***128 bit, 192 bit and 256 bit*** that meet the following standard: ***FIPS 197 [8], NIST SP 800-38A [11]***.

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 and CBC modes*** and cryptographic key sizes: ***128 bit, 192 bit and 256 bit*** that meet the following standard: ***FIPS 197 [8], NIST SP 800-38A [11]***.

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] 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] 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***.

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]

	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] 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

217 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

218 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.***

219 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 unauthorised disclosure.

220 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.

221 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 (1) the subjects : ***Loader role***, (2) the objects user data in ***Flash***, (3) the operation deployment of Loader

222 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: (1) the subjects : ***Loader role*** with security attributes : ***writing access rights***. (2) the objects user data in ***Flash*** with security attributes : ***data are located in Flash main arrays***.
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.**

6.2 Security Assurance Requirements for the TOE

223 The Security Target will be evaluated according to

Security Target evaluation (Class ASE)

224 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+”

225 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

226 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

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

	- FCS_CKM.1/RSA “Cryptographic key generation - RSA”
O.ECC	- FCS_COP.1/ECDSA “Cryptographic operation - ECDSA” - FCS_COP.1/ECDH “Cryptographic operation - ECDH” - FCS_CKM.1/ECDSA “Cryptographic key generation - ECDSA”
OE.Resp-Appl	Not applicable
OE.Process-Sec-IC	Not applicable
O.Mem-Access	- FDP_ACC.1 “Subset access control” - FDP_ACF.1 “Security attribute based access control” - FMT_MSA.3 “Static attribute initialisation” - FMT_MSA.1 “Management of security attributes” - FMT_SMF.1 “Specification of Management Functions”
O.Cap_Avail_Loader	- FMT_LIM.1/Loader “Limited capabilities - loader” - 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” - FDP_UCT.1 “Basic data exchange confidentiality” - FDP_UIT.1 “Data exchange integrity” - FDP_ACC.1/Loader “Subset access control - Loader” - FDP_ACF.1/Loader “Security attribute based access control - Loader”
O.Ctrl_Auth_Loader	- FTP_ITC.1 “Inter-TSF trusted channel” - FDP_UCT.1 “Basic data exchange confidentiality” - FDP_UIT.1 “Data exchange integrity” - FDP_ACC.1/Loader “Subset access control - Loader” - FDP_ACF.1/Loader “Security attribute based access control - Loader”
OE.Loader_Usage	Not applicable

Table 6-2: Security Requirements versus Security Objectives

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

229 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.

230 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.

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

232 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.

233 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.

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

235 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.

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

237 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.

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

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

240 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.

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

242 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.

243 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.

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

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

246 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.

247 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.

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

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

250 FCS_RNG.1 requires the TOE to provide random numbers of good quality. The exact metric are defined in [16].

251 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.

252 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.

253 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.

254 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.).

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

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

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

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

259 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.

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

261 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.

262 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.

263 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.

264 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.

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

266 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-SC-02.1 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.

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

268 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.

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

270 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.

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

272 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.

273 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.

274 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.

6.3.2 Dependencies of security functional requirements

275 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	FDP_IFF.1	See discussion below
FPT_ITT.1	None	No dependency
FDP_SDC.1	None	No dependency
FDP_SDI.2	None	No dependency
FCS_RNG.1/RGS-IC	None	No dependency
FCS_RNG.1/DRBG	None	No dependency
FCS_COP.1/[HW]TDES	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes, see discussion below
FCS_COP.1/[SW]TDES	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes, see discussion below
FCS_COP.1/[HW]AES	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes, see discussion below
FCS_COP.1/[SW]AES	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes, see discussion below
FCS_COP.1/PKA	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes See discussion below
FCS_COP.1/RSA	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes See discussion below
FCS_COP.1/ECDSA	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes See discussion below
FCS_COP.1/ECDH	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes See discussion below
FCS_CKM.1/RSA	FCS_CKM.2 or FCS.COP.1 FCS_CKM.4	Yes See discussion below

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_CKM.1/ECDSA	FCS_CKM.2 or FCS.COP.1 FCS_CKM.4	Yes See discussion below
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes See discussion below
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes See discussion below 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 FDP_ACC.1 or FDP_IFC.1	Yes Yes
FDP_UIT.1	FTP_ITC.1 or FTP_TRP.1 FDP_ACC.1 or FDP_IFC.1	Yes Yes
FDP_ACC.1/Loader	FDP_ACF.1	Yes
FDP_ACF.1/Loader	None	No dependency

Table 6-3 : Dependencies of the Security Functional Requirements

276 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).

277 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.

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

279 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.

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

281 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 decryption 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).

282 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).

283 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).

6.3.3 Rationale for the Assurance Requirements

284 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.

285 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

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

287 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.

288 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

289 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.

290 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.

291 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”.

292 All these dependencies are satisfied by EAL5.

293 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

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

295 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.

296 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.

297 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.

298 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).

299 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.

300 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.

301 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.

302 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.

303 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.

304 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.

305 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.

306 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.

7 TOE Summary Specification

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

7.1 List of Security Functional Requirements

SFR	SFR description	TOE security features meeting SFR
1	FRU_FLT.2 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 behavior of the TOE.
2	FPT_FLS.1 Failure with preservation of secure state.	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 Limited capabilities	The limited capabilities are used for accessing and definitely locking the test mode.
4	FMT_LIM.2 Limited availabilities	Different modes are integrated inside the TOE: test mode, administrator mode, kernel mode and user mode. The test mode uses specific protocol for industrial test, the administrator mode is used for loading firmware and kernel and user modes are available for running consumer applications. 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 Audit Storage	Audit Storage requirement is covered by the following security features: • 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. • Identification/authentication values are written in non-volatile memory in order to ensure the traceability of the TOE. The Loader implements an authentication function. • Non-reversibility of normal or functional mode. It is the functional mode of the TOE. It is controlled by the operating system embedded inside the TOE.
6	FDP_SDC.1 Stored data confidentiality	This requirement is covered by the following security features integrated in TOE: • Shield.

		• Security mechanisms for memory protection. • MPU for memory access control. • Non-reversibility to prevent confidential data from being read outside the test mode.
7	FDP_SDI.2 Stored data integrity monitoring and action	This requirement is covered by the CRC checksum modules
8	FPT_PHP.3 Resistance to physical attacks	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 enhanced the security of the TOE by making the reverse-engineering unpredictable or very difficult to realize.
9	FDP_ITT.1 Basic internal transfer protection	The security features integrated in the TOE enable to achieve this requirement: • Security mechanisms for memory protection. • Asynchronous logic.
10	FPT_ITT.1 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	FDP_IFC.1 Subset information flow control	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.
12.1	FCS_RNG.1/RGS-IC Random number generation - RGS_IC	The PTRNG module integrated in the TOE covers this requirement. The PTRNG follows some of the ANSSI RGS_B1 requirements (French scheme).
12.2	FCS_RNG.1/DRBG Random number generation – DRBG	The DRBG developed in the crypto library part of the TOE covers this requirement. It relies on the PTRNG to generate the seed. The DRBG library meets some of the ANSSI requirements (RGS_B1).
13	FDP_ACC.1 Subset access control	The Subset access control is met by integrating the following secure features inside the TOE: • Security mechanisms for memory protection. • Memory protection unit (MPU) for secure memory access. • Mode protection. • Restriction of use of TOE functionalities.
14	FDP_ACF.1 Security attributes based access control	The Memory Access Control Policy is enforced by the MPUs, the non-reversibility and the bootloader, features which implement different access rights.
15	FMT_MSA.3 Static attribute initialization	When the TOE is reset, all sensitive register functions are initialized (by hardware) with default value.
16	FMT_MSA.1 Management of security	Management of security attributes is covered by the security features integrated in TOE's memory

	attributes	protection unit (MPU).
17	FMT_SMF.1 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 Subset residual information protection	This requirement is achieved by all the software components of the TOE which clear sensible content.
19	FCS_COP.1 Cryptography operation	This requirement is fulfilled by the following cryptography operation functions: • 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). • 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). • 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. • 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). • 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).
20.1	FCS_CKM.1/RSA 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 Cryptographic key generation - ECDSA	The ECC key generation part of the optional Crypto library meets this requirement. It implement ECC key generation for size up to 640-bit.
21	FMT_LIM.1/Loader Limited capabilities - Loader	The limited capabilities of Loader are met by the secure authentication system
22	FMT_LIM.2/Loader Limited availabilities - Loader	The limited availabilities of Loader are met by implementing a secure blocking system
23	FIA_API.1 Authentication Proof of Identity	The authentication proof of identity is implemented by the IC Dedicated Software.
24	FTP_ITC.1 Inter-TSF trusted channel	The Inter-TSF trusted channel is implemented using the Global Platform Secure Channel Protocol 03,

		which provides assured identification of its end point and protection of the channel data from modification or disclosure.
25	FTP_UCT.1 Basic data exchange confidentiality	The confidentiality during basic data exchange is ensured by AES encryption and decryption.
26	FDP_UIT.1 Data exchange integrity	The integrity of data exchange is ensured by the CMAC/AES-128 hash algorithm.
27	FDP_ACC.1/Loader Subset access control - Loader	The subset access control is defined for the Loader role and for user data in Flash memory.
28	FDP_ACF.1/Loader Security attribute based access control - Loader	Access control for the Loader functionality is implemented by the Loader authentication mechanism.

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. 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. 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 to Figure 1-3 and subsection 7.1).
End-consumer	User of the Composite Product in Phase 7.
IC Dedicated Software	IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
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.

	Some part of that software may actually implement a Security IC application others may provide standard services. Nevertheless, this distinction doesn't matter here so that the Security IC Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.
Security IC Product	Composite product which includes the Security Integrated Circuit (i.e. the TOE) and the Embedded Software and is evaluated as composite target of evaluation in the sense of the Supporting Document
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. 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 Smartcard 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; September 2012, Version 3.1, Revision 4, CCMB-2012-09-001.

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; September 2012, Version 3.1, Revision 4, CCMB - 2012-09-002.

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; September 2012, Version 3.1, Revision 4, CCMB-2012-09-003.

[5] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; September 2012, Version 3.1, Revision 4, CCMB-2012-09-004.

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

[7] ISO14443, ISO_IEC_14443-3, 2011_Amd_1; 2011(E)-Character_PDF_document.pdf

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

[9] 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.

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

[11] 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.

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

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

[14] TESIC-SC-02.1 Hardware User Manual, revision 1.0 from November, 2016. This guidance describes the hardware functions and electrical characteristics for users.

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

[16] Règles et recommandations concernant le choix et le dimensionnement de mécanismes cryptographiques.
Annexe B1 du RGS 2.0. Version 2.03, 21/02/2014, ANSSI.
http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf

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

8.3 List of Abbreviations

AL	Admin Loader
BL	Bootloader
CC	Common Criteria
CL	Crypto Library
EAL	Evaluation Assurance Level
HW	Hardware
IC	Integrated Circuit
IT	Information Technology
PP	Protection Profile
ST	Security Target
TC	Tuning Capacitance
TOE	Target of Evaluation
TSC	TSF Scope OF Control
TSF	TOE Security Functionality
ETR	Evaluation Technical Report
SAR	Security Assurance Requirement
SFR	Security Functional Requirements