Security Target Lite of

CIU9872B_01 C12

Secure Chip

Version 1.2

Date 2017-10-11

CEC Huada Electronic Design Co., Ltd.

REVISION HISTORY

1.0	2017.09.29: Generated the last version from Security Target of CIU9872B_01_C12 Secure Chip version 1.0
1.1	2017.10.09: Complete the modified sections.
1.2	2017.10.11: Change the AGD_PRE and AGD_OPE version information.

Content

Abbreviation 5
Glossary 6
1 ST INTRODUCTION 7
1.1 ST Reference and TOE Reference 7
1.1.1 ST Reference 7
1.1.2 TOE Reference 7
1.2 TOE Overview 8
1.2.1 Introduction 8
1.2.2 TOE usage and major security functionality 8
1.2.3 TOE type 9
1.2.4 Required non-TOE hardware/software/firmware 9
1.3 TOE Description 10
1.3.1 Physical Scope of TOE 10
1.3.2 Logical Scope of TOE 11
1.3.3 TOE Life Cycle 13
2. Conformance Claims 14
2.1 CC Conformance Claim 14
2.2 PP Claim 15
2.3 Package Claim 15
2.4 Conformance Claim Rationale 16
3. Security Problem Definition 16
3.1 Description of Assets 17
3.2 Threats 17
3.3 Organizational Security Policies 18
3.4 Assumptions 18
4. Security Objectives 18
4.1 Security Objectives for the TOE 19
4.2 Security Objectives for the Operational Environment 20
4.3 Security Objectives Rationale 20
5. Extended Components Definition 22
6. Security Requirements 22
6.1 Security Functional Requirements for the TOE 23

6.2 Security Assurance Requirements 31
6.3 Security Requirements Rationale 32
6.3.1 Rationale for the Security Functional Requirements 32
6.3.2 Dependencies of Security Functional Requirements 34
6.3.3 Rationale of the Assurance Requirements 36
7 TOE summary specification 37
7.1 Malfunction 37
7.2 Leakage 38
7.3 Physical manipulation and probing 38
7.4 Abuse of functionality and identification 39
7.5 Random numbers 40
7.6 Cryptographic functionality 40
7.7 Memory access control policy 41
8. Bibliography 41
8.1 Evaluation Documents 41
8.2 Developer Documents 42
8.3 Other Documents 42

Abbreviation

CBC	Cipher Block Chaining
CC	Common Criteria
CKMU	ClocK Management Unit
CMS	Chip Management System
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DES/TDES	Data Encryption Standard/Triple Data Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
ECB	Electronic Codebook
EDC	Error Data Check
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMMU	Enhanced Memory Management Unit
FA	Fault Attack
GPIO	General Purpose IO
IC	Integrated Circuit
LD	Laser Detector
PKE	Public Key Engine
PWMU	PoWer Management Unit
PP	Protection Profile
RAM	Random Access Memory
ROM	Read-Only Memory
RSA	Rivest-Shamir-Adleman
SFR	Security Functional Requirements
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
TRNG	True Random Number Generator

Glossary

AHB2SFR
AHB2SFR module executes SFR bus decoding and access control.

End-user
User of the composite product in phase 7.

IC Dedicated Software
IC dedicated software which is normally recognized as IC firmware, is developed by IC developer and embedded in a security IC. The IC dedicated software is mainly used 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).

NVR
NVR is the abbreviation of Nov-Volatile Register, which is implemented by a special block of EEPROM. The special block of EEPROM will not occupy the address space which user can see.

Security IC
Composition of TOE, the security IC embedded software, user data and package (the security IC carrier).

Security IC Embedded Software
Security IC embedded software supplies the security IC application and standard services and normally is developed other than IC designer. The embedded software is designed in phase 1 and embedded into the security IC in phase 3 or later phases of the security IC product life-cycle.

Security IC Product
Integration of security IC and Embedded software is evaluated as composite target of evaluation in sense of supporting document.

TOE Delivery
The TOE is delivered in the period of either in form of wafers or sawn wafers (dice) after phase 3 or in form of packaged product after phase 4.

1 ST INTRODUCTION

This introduction chapter contains the following sections:
1.1 Security Target Reference and TOE Reference
1.2 TOE Overview
1.3 TOE Description

1.1 ST Reference and TOE Reference

1.1.1 ST Reference

"Security Target of CIU9872B_01 C12 Secure Chip, Version 1.0, 29 September 2017"

The Security Target is based on Eurosmart Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13th Jan. 2014, BSI-CC-PP-0084-2014.

The Protection Profile and the Security Target are built on Common Criteria version 3.1.

Common Criteria version:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 4, September 2012

1.1.2 TOE Reference

The TOE is named "HED Secure Chip CIU9872B_01 C12 with IC Dedicated Software".

In this document the TOE is abbreviated to HED Secure Chip CIU9872B_01 C12.

1.2 TOE Overview

1.2.1 Introduction

The TOE is the IC hardware with IC Dedicated Software which are stored in ROM and documentation describing the Instruction Set and the usage [7][8][9][10].

The main usage of the TOE is for e-passport applications. And the scope of the TOE includes the IC hardware and IC dedicated software which is constitutive of Chip Management System (CMS), cryptographic library and API library. CMS supports two functionalities, which are booting process controlling and chip module function testing. The cryptographic library implements the arithmetic function like RSA, AES and TDES with cooperating of hardware. The API library includes random number generation function. The whole IC dedicated software is programed with C language and assembly language.

The IC hardware is a microcontroller incorporating a central processing unit (CPU), memories accessible via an Enhanced Memory Management Unit (EMMU), cryptographic coprocessors, other security components and two communication interfaces. The CPU (ARM SC000) processor is a very low gate count, highly energy efficient processor for use in microcontroller and deeply embedded applications that require an area optimized processor for use in environments where security is an important consideration. On-chip memories are ROM, RAM and EEPROM. The EEPROM can be used as data and program memory. It consists of high reliable memory cells with data integrity check. The EEPROM is optimized for applications requiring high reliability for data and program code.

The documentation includes:

- CIU9872B_01 C12_Operational_User_Guidance (AGD_OPE) [7]
- CIU9872B_01 C12_Preparative_procedures (AGD_PRE) [8]
- CIU9872B_01 C12_Product_Datasheet [9]
- CIU9872B_01 C12_Crypto_library_User_Guide [10]

1.2.2 TOE usage and major security functionality

Since a security IC is intended to be used in a potential insecure environment, it must provide high security in particular when being used in the banking and finance market, electronic commerce or in governmental applications (such as banking, e-passport, social security, pay-TV and mobile payment applications). Hence the TOE shall maintain：

- The integrity and the confidentiality of code and data stored in its memories
- The memory access can be controlled by different chip modes

- The integrity, the correct operation and the confidentiality of security functionality provided by the TOE

This is ensured by the construction of the TOE and its security functionality.

HED Secure Chip CIU9872B_01 C12 provides hardware for an implementation of a secure application with:

- ARM SC000 CPU with security mechanisms is a member of the ARM family of SecurCore 32-bit microprocessors supporting two modes: unprivilege and privilege
- Security detectors including high and low temperature detectors, internal and external frequency detectors, internal and external voltage detectors, internal and external glitch detectors, light detectors
- Active shielding that against physical attacks
- TDES(2 keys) with countermeasures against SPA, DPA, and FA
- AES with countermeasures against SPA, DPA, and FA
- Hardware coprocessor of asymmetric algorithms supports large integer arithmetic operations like modular multiplication, modular addition, modular subtraction, point addition and point doubling. These operations are used by software to realize the function of public key cryptography (RSA) with countermeasures against the attack of SPA, DPA and DFA
- Memory access controlled by EMMU
- Memory data encryption and address scrambling
- Data integrity check for RAM, ROM and EEPROM
- Bus polarity switching
- A highly reliable true random number generator compliant with PTG.2 class of AIS20[2011][20]
- A deterministic random number generator compliant with DRG.3 class of AIS20[2011]
- Test mode protection
- Self-test function
- Cyclic Redundancy Check (CRC) coprocessor

1.2.3 TOE type

The TOE is HED Secure Chip CIU9872B_01 C12 with IC dedicated software intended for use as a secure IC.

1.2.4 Required non-TOE hardware/software/firmware

For use of the ISO/IEC14443 contactless interface an antenna is required. This antenna is connected to the antenna contacts of the TOE but is not part of the TOE itself.

1.3 TOE Description

1.3.1 Physical Scope of TOE

A block diagram of the HED Secure Chip CIU9872B_01 C12 is depicted in Figure 1.

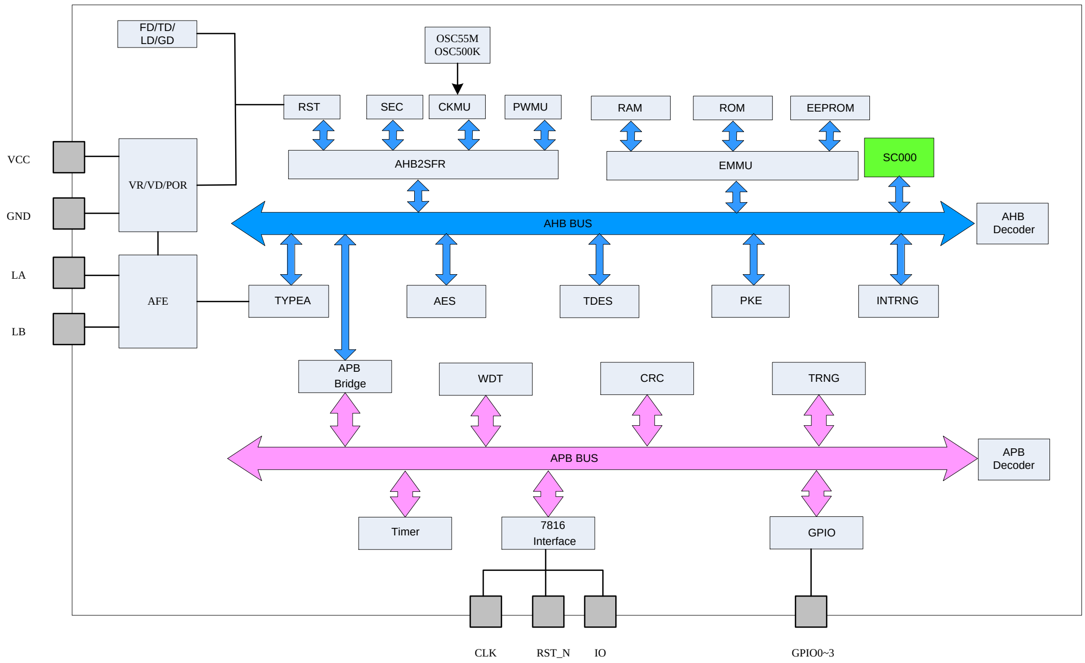

Figure 1 : Hardware Blocks of the TOE

The scope of the TOE includes the IC hardware, CMS, cryptographic library and API library.

Table 1 : Components of the TOE scope

Type	Name	Release	Date	Form of delivery
IC Hardware	CIU9872B_01	C12	2017.05.15	Module
Security IC Dedicated Software	CMS	1.0	2017.01.20	In ROM
	Cryptographic library	1.0	2017.01.20	Lib file (only for AES)
		1.0	2017.01.20	In ROM (for other parts in Cryptographic library)
	API library	1.0	2017.01.20	Lib file

The components of the TOE scope are listed in Table 1. The common components of the TOE are listed in Table 2:

Table 2 : Common Components of the TOE

Type	Name	Release	Date	Form of delivery
Document	CIU9872B_01 C12_Operational_User_Guidance (AGD_OPE)	1.1	2017.10.11	Electronic Document
Document	CIU9872B_01 C12_Preparative_procedures (AGD_PRE)	1.1	2017.10.11	Electronic Document
Document	CIU9872B_01 C12_Product_Datasheet	1.0	2017.09.29	Electronic Document
Document	CIU9872B_01 C12_Crypto_Library_User_Guide	1.0	2017.09.29	Electronic Document

1.3.2 Logical Scope of TOE

1.3.2.1 Hardware Description

The hardware blocks of the TOE are shown in figure 1. The main blocks are described as following:

CPU (SC000)

The CPU used in the TOE is ARM SC000

Memory

10 kBytes RAM, 384 kBytes ROM and 96 kBytes EEPROM are presented in the TOE.

EMMU

Access control to RAM, ROM, EEPROM, and NVR is enforced by an Enhanced Memory Management Unit.

Coprocessor

- The TDES coprocessor supports TDES operations, ECB mode and CBC mode. The TDES is in 2-key operation with two 56-bit keys (112-bit)
- The AES coprocessor supports AES encryption/decryption with key length of 128/192/256 bits, ECB mode and CBC mode
- The PKE coprocessor supplies basic arithmetic functions to support implementation of asymmetric cryptographic algorithms (RSA) by the Security IC Embedded Software
- The CRC coprocessor provides CRC generation polynomial CRC-16 ($X^{16} + X^{12} + X^5 + 1$)

TRNG

A highly reliable true random number generator compliant with PTG.2 class of AIS20[2011].

Power (PWMU)

PWMU: Power management unit.

Clock (CKMU)

CKMU: Clock management unit
The clock frequency of co-processors and CPU is configurable.

Other major components

- ISO/IEC 14443 Type A Interface
- ISO/IEC 7816 Interface
- GPIO
- Programmable timers
- Watchdog
- Reset management unit
- Detectors for extreme environmental conditions detection

The TOE can be configured by software using special function registers that influence the hardware behavior of the TOE. The registers shall be set according the corresponding software guidance [7].

For security reasons the data sheet and security guidance will not be published but only delivered to the security IC embedded software developer of the composite product. The TOE supports 2 chip modes, which are Test Mode and Application Mode. The end-user will receive TOE running in Application Mode with disabled test functionality. The hardware components are controlled by the Security IC Embedded Software via Special Function Registers. Special Function Registers are interrelated to the activities of the CPU, the Enhanced Memory Management Unit, interrupt control, I/O configuration, EEPROM, timers, the contactless interface and the coprocessors.

1.3.2.2 Software Description

The IC Dedicated Software including CMS, cryptographic library and API library. CMS is for booting process controlling.

DRNG

API library provides a deterministic random number generation API which is compliant with DRG.3.

1.3.3 TOE Life Cycle

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:

- IC Development (Phase 2)
  - IC design
  - IC Dedicated Software development
- The IC Manufacturing (Phase 3)
  - Integration and photomask fabrication
  - IC production
  - IC testing
  - Preparation and pre-personalization if necessary

The Composite Product life cycle phase 4 is included in the evaluation of the IC:

- The IC Packaging (Phase 4)
  - Security IC packaging (and testing)
  - Pre-personalization if necessary

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

- Security IC Embedded Software Development (Phase 1)
- The Composite Product finishing process, preparation and shipping to the personalization line for the Composite Product (Composite Product Integration Phase 5)
- The Composite Product personalization and testing stage where the User Data is loaded into the Security IC's memory (Personalization Phase 6)
- The Composite Product usage by its issuers and consumers (Operational Usage Phase 7) which may include loading and other management of applications in the field

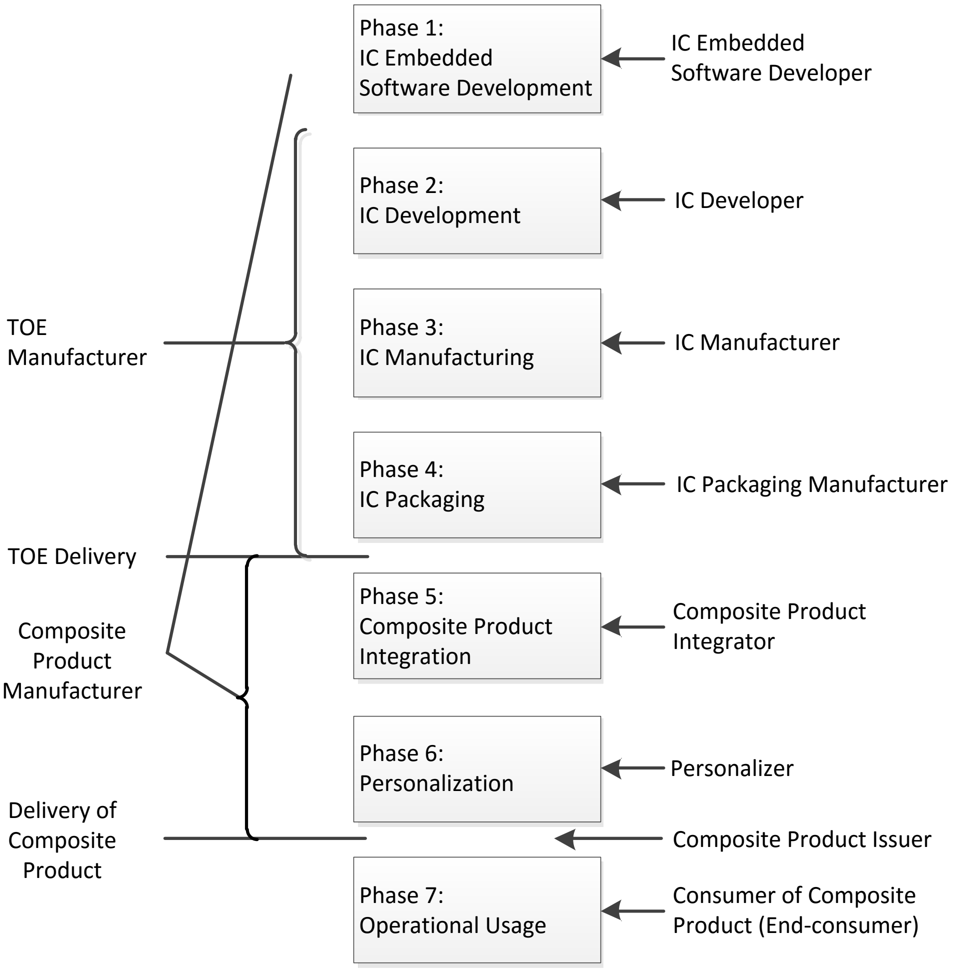

Figure 2 : Definition of "TOE Delivery" and responsible Parties

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. After the packing in Phase 4, the TOE is delivered in form of modules.

2. Conformance Claims

This chapter is divided into the following sections:
2.1 CC Conformance Claim
2.2 PP Claim
2.3 Package Claim
2.4 Conformance Claim Rationale

2.1 CC Conformance Claim

This Security Target and the TOE claims conformance to version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004

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

2.2 PP Claim

This Security Target is strict compliant to the Protection Profile:

- Security IC Platform Protection Profile, Version 1.0, 13.01.2014, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084

The short term for this Protection Profile used in this document is “BSI-PP-0084” or “PP”.

Since the Security Target claims conformance to this PP, the concepts are used in the same sense. For the definition of terms refer to the BSI-PP-0084. These terms also apply to this Security Target.

The TOE provides additional functionality, which is not covered in PP. In accordance with Application Note 4 of the BSI-PP-0084, this additional functionality is added using the policy “P.Crypto-Service” (see Section 3.3 of this Security Target for details).

This ST does not claim conformance to any other protection profile.

2.3 Package Claim

This Security Target claims conformance to the assurance package EAL5 augmented. The augmentations to EAL5 are ALC_DVS.2 and AVA_VAN.5.

This Security Target claims conformance with the Security IC Platform Protection Profile BSI-PP-0084.

The assurance level for this Security Target is EAL5 augmented with AVA_VAN.5 and ALC_DVS.2. This assurance level conforms to the Security IC Platform Protection Profile.

Note: The BSI-PP-0084 “Security IC Protection Profile” to which this Security Target claims conformance (for details refer to section 2.3) requires assurance level EAL4 augmented. The changes, which are needed for EAL5, are described in the relevant sections of this Security Target.

2.4 Conformance Claim Rationale

This Security Target claims strict conformance to the Security IC Platform Protection Profile (BSI-PP-0084).

The TOE type defined in this Security Target is secure IC which is consistent with the TOE definition in Security IC Platform Protection Profile.

All sections of this Security Target, in which security problem definition, objectives and security requirements are defined, clearly state which of these items are taken from PP and which are added in this Security Target. Therefore this is not repeated here. Moreover, all additionally stated items in this Security Target do not contradict the items included from the BSI-PP-0084 (see the respective sections in this document). The operations done for the SFRs taken from PP are also clearly indicated.

The evaluation assurance level claimed for this target (EAL5+) is shown in section 6.2 to include respectively exceed the requirements claimed by the BSI-PP-0084.

These considerations show that the Security Target correctly claims strict conformance to PP.

3. Security Problem Definition

This Security Target claims conformance to the BSI-PP-0084 “Security IC Protection Profile”. Assets, threats, assumptions and organizational security policies are taken from PP. This chapter lists these assets, threats, assumptions and organizational security policies, and describes extensions to these elements in detail.

3.1 Description of Assets

The assets of the TOE are all assets described in section 3.1 of "Security IC Platform Protection Profile".

3.2 Threats

Since this Security Target claims strict conformance to the BSI-PP-0084 "Security IC Protection Profile" the threats defined in section 3.2 of PP are valid for this Security Target. The threats defined in PP are listed below in Table 3:

Table 3 : Threats defined by the BSI-PP-0084

Name	**Title**
T.Leak-Inherent	Inherent Information Leakage
T.Phys-Probing	Physical Probing
T.Malfunction	Malfunction due to Environmental Stress
T.Phys-Manipulation	Physical Manipulation
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

The TOE provides access control to the memories and to hardware resources.

The TOE shall avert the threat "Unauthorized Memory or Hardware Access (T.Unauthorized-Access)" as specified below.

T.Unauthorized-Access Unauthorized Memory or Hardware Access

Adverse action: An attacker may try to read, modify or execute code or data stored in restricted memory areas. And or an attacker may try to access or operate hardware resources that are restricted by executing code.

Threat agent: Attacker

Asset: Execution of code or data belonging to the Security IC Dedicated Software

Table 4: Additional threats averted by the TOE

Name	**Title**
T.Unauthorized-Access	Unauthorized Memory or Hardware Access

3.3 Organizational Security Policies

Since this Security Target claims strict conformance to the BSI-PP-0084 "Security IC Protection Profile" the policy P.Process-TOE "Protection during TOE Development and Production" in PP is applied here as well.

In accordance with Application Note 5 in PP there is one additional policy defined in this Security Target as detailed below.

The TOE provides specific security functionality, which can be used by the Security IC Embedded Software. In the following, specific security functionality is listed, which is not derived from threats identified for the TOE's environment. It can only be decided in the context of the application against which threats the Security IC Embedded Software will use this specific security functionality.

The IC Developer/Manufacturer therefore applies the policies as specified below:

P.Crypto-Service Cryptographic services of the TOE

The TOE provides secure hardware based cryptographic services for the IC Embedded Software:

- TDES encryption and decryption
- AES encryption and decryption
- RSA

3.4 Assumptions

Since this Security Target claims strict conformance to the BSI-PP-0084 "Security IC Protection Profile" the assumptions defined in section 3.4 of PP are valid for this Security Target. The following table lists these assumptions.

Table 5: Assumptions defined in the BSI-PP-0084

Name	**Title**
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization
A.Resp-Appl	Treatment of User Data

4. Security Objectives

This chapter contains the following sections: "Security Objectives for the TOE", "Security Objectives for the Operational Environment" and "Security Objectives Rationale".

4.1 Security Objectives for the TOE

The TOE shall provide the following security objectives, which are taken from the BSI-PP-0084 “Security IC Protection Profile”.

Table 6 : Security objectives defined in the BSI-PP-0084

Name	Title
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunctions
O.Phys-Manipulation	Protection against Physical Manipulation
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality
O.Identification	TOE Identification
O.RND	Random Numbers

The following additional security objectives are defined based on package functionality provided by the TOE as specified below:

O.TDES TDES Functionality

The TOE shall provide the cryptographic functionality to calculate a Triple DES encryption and decryption to the Security IC Embedded Software. The TOE supports directly the calculation of TDES with up to two keys.

Note: The TOE will ensure the confidentiality of the User Data (and especially cryptographic keys) during Triple DES operation. This is supported by O.Leak-Inherent.

O.AES AES functionality

The TOE shall provide cryptographic functionality to perform an AES encryption and decryption with 128/192/256 bits keys to the Security IC Embedded Software.

O.RSA RSA functionality

The TOE shall provide cryptographic functionality to perform an RSA encryption and decryption with key lengths up to 2048 bits to the Security IC Embedded Software.

Regarding Application Notes 8 and 9 in PP the following additional security objectives are defined based on additional functionality provided by the TOE as specified below:

O.MEM-ACCESS Area based Memory Access Control

Access by processor instructions to memory areas is controlled by the TOE. The TOE decides based on the area access permissions control of the Enhanced Memory Management Unit.

4.2 Security Objectives for the Operational Environment

The following security objectives for the operational environment are specified according to the BSI-PP-0084 “Security IC Protection Profile”.

Table 7 : Security objectives for the operational environment, taken from PP

Security objective	**Description**	**Applies to phase…**
OE.Process-Sec-IC	Protection during composite product manufacturing	TOE delivery up to the end of phase 6

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).

4.3 Security Objectives Rationale

Section 4.4 in the BSI-PP-0084 “Security IC Protection Profile” provides a rationale how the assumptions, threats, and organizational security policies are addressed by the objectives that are specified in the BSI-PP-0084. Table 8 reproduces the table in section 4.4 of PP.

Table 8 : Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or	**Security Objective**	**Notes**

Organizational Security Policy		
A.Resp-Appl	OE.Resp-Appl	Phase 1
P.Process-TOE	O.Identification	Phase 2 – 3 optional Phase 4
A.Process-Sec-IC	OE.Process-Sec-IC	Phase 5 – 6 optional Phase 4
T.Leak-Inherent	O.Leak-Inherent	
T.Phys-Probing	O.Phys-Probing	
T.Malfunction	O.Malfunction	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Forced	O.Leak-Forced	
T.Abuse-Func	O.Abuse-Func	
T.RND	O.RND	

The following table provides the justification for the additional security objectives. They are in line with the security objectives of the BSI-PP-0084 and supplement these according to the additional threats and organizational security policies.

Table 9 provides the justification for the additional security objectives. They are in line with the security objectives of PP and supplement these according to the additional assumptions, threat and organizational security policy.

Table 9 : Additional Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or OSP	**Security Objective**	**Note**
T.Unauthorized-Access	O.Mem-Access	
P.Crypto-Service	O.TDES O.AES O.RSA	

The justification of the additional policy, threat and assumption is given in the following description.

The justification related to the threat “Unauthorized Memory or Hardware Access (T.Unauthorized-Access)” is as follows:

According to O.Mem-Access the TOE must enforce the partitioning of memory areas so that access to memory areas is controlled. Restrictions are controlled by the EMMU. Thereby security violations caused by accidental or deliberate access to restricted data (which may include code) can be prevented (refer to T.Unauthorized-Access). The threat T.Unauthorized-Access is therefore countered if the objective is met.

The justification related to the security objectives O.TDES, O.AES and O.RSA is as follows: Since these objectives require the TOE to implement exactly the same specific security functionality as required by P.Crypto-Service, the organizational security policy is covered by the objectives.

The justification of the additional policy and the additional assumptions show that they do not contradict to the rationale already given in the BSI-PP-0084 for the assumptions, policy and threats defined there.

5. Extended Components Definition

There are four extended components defined and described for the TOE:

- the family FCS_RNG at the class FCS Cryptographic Support
- the family FMT_LIM at the class FMT Security Management
- the family FAU_SAS at the class FAU Security Audit
- the family FDP_SDC at the class FDP User data protection

The extended components FCS_RNG, FMT_LIM FAU_SAS and FDP_SDC are defined and described in the BSI-PP-0084 section 5.

6. Security Requirements

This part of the Security Target defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE. This chapter consists of the sections "Security Functional Requirements", "Security Assurance Requirements" and "Security Requirements Rationale".

The CC allows several operations to be performed on security requirements (on the component level); refinement, selection, assignment, and iteration are defined in paragraph 8.1 of Part 1 of the CC [1]. These operations are used in the PP [6] and in this Security Target, respectively.

The **refinement** operation is used to add details to requirements, and, thus, further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in bold text and changed words are crossed out.

The **selection** operation is used to select one or more options provided by the PP [6] or CC in stating a requirement. Selections having been made are denoted as italic text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made are denoted by showing as italic text.

The **iteration** operation is used when a component is repeated with varying operations. It is denoted by showing brackets “[*iteration indicator*]” and the *iteration indicator* within the brackets.

6.1 Security Functional Requirements for the TOE

The security functional requirements (SFR) for the TOE are defined and described in PP section 6.1 and in the following description.

The Table 10 provides an overview of the functional security requirements of the TOE, defined in PP section 6.1. In the last column it is marked if the requirement is refined. The refinements are also valid for this ST.

Table 10 : Security functional requirements defined in PP

SFR	**Title**	**Refined in PP**
FRU_FLT.2	Limited fault tolerance	Yes
FPT_FLS.1	Failure with preservation of secure state	Yes
FMT_LIM.1	Limited capabilities	No
FMT_LIM.2	Limited availability	No
FAU_SAS.1	Audit storage	No
FPT_PHP.3	Resistance to physical attack	Yes
FDP_SDI.2	Stored data integrity monitoring and action	No
FDP_SDC.1	Stored data confidentiality	No
FDP_ITT.1	Basic internal transfer protection	Yes
FPT_ITT.1	Basic internal TSF data transfer protection	Yes
FDP_IFC.1	Subset information flow control	No
FCS_RNG.1	Quality metric for random numbers	No

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[1].

Application note: The failures will cause an alarm signals to be triggered, which will result in a special function register bit to be set and a reset (secure state).

Regarding Application Note 15 of the PP [6] generation of additional audit data is not defined for "Limited fault tolerance" (FRU_FLT.2) and "Failure with preservation of secure state" (FPT_FLS.1).

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*[2] to the *TSF*[3] by responding automatically such that the SFRs are always enforced.

Application note: If a physical manipulation or physical probing attack is detected, an alarm will be automatically triggered by the hardware, which will cause the chip to be reset.

The Table 11 provides an overview about the augmented security functional requirements, which are added additional to the TOE and defined in this ST. All requirements are taken from Common Criteria Part 2 [2].

Table 11: Augmented security functional requirements

SFR	**Title**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FCS_COP.1	Cryptographic support

All assignments and selections of the security functional requirements of the TOE are done in PP and in the following description.

The above marked extended components FMT_LIM.1 and FMT_LIM.2 are introduced in PP to define the IT security functional requirements of the TOE as an additional family (FMT_LIM) of the Class FMT (Security Management). This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses

[1] [assignment: list of types of failures in the TSF]

[2] [assignment: physical tampering scenarios]

[3] [assignment: list of TSF devices/elements]

the management of functions of the TSF.

The additional component FAU.SAS is introduced to define the security functional requirements of the TOE of the Class FAU (Security Audit). This family describes the functional requirements for the storage of audit data and is described in the following.

- **FAU_SAS**

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.

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*[1]with the capability to store the *Initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software*[2] in the *EEPROM*[3]

- **FCS_RNG.1**

The TOE shall meet the requirement "Quality metric for random numbers (FCS_RNG.1)" as specified below (Common Criteria Part 2 extended).

FCS_RNG.1[PTG.2]	**Random number generation (Class PTG.2)**
Hierarchical to:	No other components
Dependencies:	No dependencies

Note: The definition of the Security Functional Requirement FCS_RNG.1 has been taken from [5]

Note: The functional requirement FCS_RNG.1 is a refinement of FCS_RNG.1 defined in PP [6] according to [5]

[1] [assignment: *list of subjects*]
[2] [assignment: *list of audit information*]
[3] [assignment: *type of persistent memory*]

FCS_RNG.1.1[PTG.2] The TSF shall provide a *physical*[1] random number generator that implements:

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

(PTG.2.2) *If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source*[2]*.*

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

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

(PTG.2.5) *The online test procedure checks the quality of the raw random number sequence. It is triggered at regular intervals or continuously*[3]*. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time*[4]*.*

FCS_RNG.1.2[PTG.2] The TSF shall provide *octets of bits*[5] that meet:

(PTG.2.6) *Test procedure A*[6] *does not distinguish the internal random numbers from output sequences of an ideal RNG.*

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

FCS_RNG.1[DRG.3] **Random number generation (Class DRG.3)**

FCS_RNG.1.1[DRG.3] The TSF shall provide a *deterministic*[7] random number generator that implements:

(DRG.3.1) *If initialized with a random seed using PTRNG of class*

[1] [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]

[2] [selection: *prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy]*

[3] [selection*: externally, at regular intervals, continuously, applied upon specified internal events]*

[4] [assignment: *list of security capabilities*]

[5] [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*]

[6] [assignment: *additional standard test suites*] Note: according §295 in [5] the assignment may be empty

[7] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

PTG.2 as random source[1]*, the internal state of the RNG shall have 127bits entropy*[2]*.*

(DRG.3.2) The RNG provides forward secrecy.

(DRG.3.3) The RNG provides backward secrecy even if the current internal state is known[3]*.*

FCS_RNG.1.2[DRG.3] The TSF shall provide random numbers that meet:

(DRG.3.4) The RNG initialized with a random seed using PTRNG of class PTG.2[4] *generates output for which* $[2^{40}]$[5] *strings of bit length 128 are mutually different with probability* $[1\text{-}2^{-n}]$[6]*.*

(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A[7]*.*

By this, all assignment/selection operations are performed. This Security Target does not perform any other/further operations than stated in [8].

Considering Application Note 12 of the PP [6] in the following paragraphs the additional functions for cryptographic support and access control are defined. These SFRs are not required by the PP [6].

Memory access control

The TOE provides Area based Memory Access Control.

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

[1] [selection: using a PTRNG of class PTG.2 as random source, using a PTRNG of class PTG.3 as random source, using an NPTRNG of class NTG.1 [assignment: other requirements for seeding]]

[2] [selection: have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]]

[3] [assignment: list of security capabilities]

[4] [assignment: requirements for seeding]

[5] [assignment: number of strings]

[6] [assignment: probability, 16<n<49]

[7] [assignment: a defined quality metric]

The following Security Function Policy (SFP) Memory Access Control Policy is defined for the requirement “Security attribute based access control (FDP_ACF.1)”:

Memory Access Control Policy

The TOE shall control read, write and execute accesses of software running at different mode (CMS mode, user mode) and different CPU modes (privilege and unprivilege) on data including code stored in memory areas and special function registers.

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*[1] on *all subjects: privileged and unprivileged software, all objects: defined regions in memory and all the operations: read, write, execute defined in the Memory Access Control Policy*[2].

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*[3] to objects based on the following: *all subjects and objects and the attributes： chip mode, the EMMU access permission control, the Special Function Registers to control the access permission and the Special Function Registers related to system management*[4].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *evaluate the corresponding EMMU access permission control information of the memory range of the objects during*

[1] [assignment: access control SFP]
[2] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[3] [assignment: access control SFP]
[4] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

the access to determine whether the accesses can be granted to perform the operation[1] *by the subject.*

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*[2]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[3]

Cryptographic Support

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

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

- Triple Data Encryption Standard (TDES) with 112 bit key size
- Advanced Encryption Standard (AES) with 128/192/256 bits key size
- Rivest-Shamir-Adleman (RSA)

● TDES Operation

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

FCS_COP.1[TDES] Cryptographic operation

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 management], FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1[TDES] The TSF shall perform *encryption and decryption*[4] in accordance with a specified cryptographic algorithm *TDES in ECB/CBC mode*[5] and cryptographic key sizes *112 bit*[6] that meet the following *NIST SP800-67[17] and NIST SP800-38A[18]*[7].

[1] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

[2] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[3] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[4] [assignment: list of cryptographic operations]

[5] [assignment: cryptographic algorithm]

[6] [assignment: *cryptographic key sizes*]

[7] [assignment: *list of standards*]

- **AES Operation**

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

FCS_COP.1 [AES] **Cryptographic operation**

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[AES] The TSF shall perform *encryption and decryption*[1] in accordance with a specified cryptographic algorithm *AES in ECB/CBC mode*[2] and cryptographic key sizes *128 bit, 192 bit and 256 bit*[3] that meet the following *FIPS PUB 197[19]*[4] *and NIST SP800-38A[18]*[5].

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

The Modular Arithmetic Operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1[RSA] **Cryptographic operation**

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 management], FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1[RSA] The TSF shall perform *encryption, decryption* [6] in accordance with a specified cryptographic algorithm *Rivest-Shamir-Adleman (RSA)* [7] and cryptographic key sizes *from 512 to 2048 bits* [8] that meet the following: *RSA standard [16]*[9].

Application Notes: The key length is determined by user based on application

[1] [assignment: list of cryptographic operations]
[2] [assignment: cryptographic algorithm]
[3] [assignment: cryptographic key sizes]
[4] [assignment: list of standards]
[5] [assignment: list of standards]
[6] [assignment: *list of cryptographic operations*]
[7] [assignment: *cryptographic algorithm*]
[8] [assignment: *cryptographic key sizes*]
[9] [assignment: *list of standards*]

requirements. User shall assure the security in the application.

Data Integrity

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

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for *inconsistencies between stored data and corresponding EDC*[1] on all objects, based on the following attributes: *EDC value for the RAM, ROM and EEPROM*[2]

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall *adjust the memory operation*[3].

Dependencies: No dependencies
Refinement: **Each memory block is considered as one container and the adjustment is done for one complete memory block.**

Data Confidentiality

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 *EEPROM, ROM and RAM*[4].

6.2 Security Assurance Requirements

The evaluation assurance level is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5. In the following table, the security assurance requirements are given.

Table 12: Assurance components

[1] [assignment: *integrity errors*]
[2] [assignment: *user data attributes*]
[3] [assignment: *action to be taken*]
[3] [assignment: *action to be taken*]
[4] [assignment: *memory area*]

Aspect	Acronym	Description
Development	ADV_ARC.1	Security Architecture design
	ADV_FSP.5	Functional specification
	ADV_IMP.1	Implementation representation
	ADV_INT.2	TSF internals
	ADV_TDS.4	TOE design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.4	CM capabilities
	ALC_CMS.5	CM scope
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Development security
	ALC_LCD.1	Life-cycle definition
	ALC_TAT.2	Tools and techniques
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.3	Depth
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability testing

6.3 Security Requirements Rationale

6.3.1 Rationale for the Security Functional Requirements

The security functional requirements rationale of the TOE are defined and described in PP section 6.3 for the following security functional requirements: FDP_ITT.1, FDP_IFC.1, FPT_ITT.1, FPT_PHP.3, FDP_SDI.2, FDP_SDC.1, FPT_FLS.1, FRU_FLT.2, FMT_LIM.1, FMT_LIM.2, FCS_RNG.1, and FAU_SAS.1.

The security functional requirements FDP_ACC.1, FDP_ACF.1, and FCS_COP.1 are defined in the following description:

Table 13: Rational for additional SFR in the ST

Objective	TOE Security Functional Requirements
O.TDES	- FCS_COP.1[TDES] "Cryptographic operation"
O.AES	- FCS_COP.1[AES] "Cryptographic operation"
O.RSA	- FCS_COP.1[RSA] "Cryptographic operation"
O.Mem-Access	- FDP_ACC.1 "Subset access control" - FDP_ACF.1 "Security attribute based access control"

The table above gives an overview, how the security functional requirements are combined to meet the security objectives. The detailed justification is given in the following:

The security functional requirement(s) "Cryptographic operation (FCS_COP.1)" exactly requires those functions to be implemented which are demanded by O.TDES, O.ASE and O.RSA. Therefore, FCS_COP.1 is suitable to meet the security objective.

The usage of cryptographic algorithms requires the use of appropriate keys. Otherwise these cryptographic functions do not provide security. The keys have to be unique with a very high probability, and must have a certain cryptographic strength etc. In case of a key import into the TOE (which is usually after TOE delivery) it has to be ensured that quality and confidentiality are maintained. Keys for TDES and AES are provided by the environment. Keys for RSA algorithm can be provided either by the TOE or the environment.

The justification of the security objective and the additional requirements (both for the TOE and its environment) show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there.

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 as required by O.Mem-Access. The related TOE security functional requirements FDP_ACC.1, FDP_ACF.1 cover this security objective. The implementation of these functional requirements is represented by the dedicated privilege level concept.

The justification of the security objective and the additional requirements show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there. Moreover, these additional security functional requirements cover the requirements by CC part 2 user data protection of chapter 11 which are not refined by the BSI-PP-0084.

Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context. The TOE only provides the tool to implement the policy defined in the context of the application.

6.3.2 Dependencies of Security Functional Requirements

The dependence of security functional requirements are defined and described in PP section 6.3.2 for the following security functional requirements: FDP_ITT.1, FDP_IFC.1, FPT_ITT.1, FPT_PHP.3, FDP_SDI.2, FDP_SDC.1, FPT_FLS.1, FRU_FLT.2, FMT_LIM.1, FMT_LIM.2, FCS_RNG.1 and FAU_SAS.1.

The dependence of security functional requirements for the security functional requirements FDP_ACC.1, FDP_ACF.1, FCS_COP.1 and FDP_SDI.1 are defined in the following description.

Table 14 : Dependency for cryptographic operation requirement

Security Functional Requirement	**Dependencies**	**Fulfilled by security requirements**
FCS_COP.1[TDES]	FCS_CKM.1	Yes, see comment 2
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	Yes, see comment 2
FCS_COP.1[AES]	FCS_CKM.1	Yes, see comment 2
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	Yes, see comment 2
FCS_COP.1[RSA]	FCS_CKM.1	Yes, see comment 2
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	Yes, see comment 2
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes Yes, see comment 1
FDP_SDI.1	None	N/A

Comment 1:

The dependency FMT_MSA.3 introduced by the components FDP_ACF.1 is considered to be satisfied because the access control specified for the intended TOE is based on static parameters that cannot be changed. Therefore, FMT_MSA.3 is not applicable.

End of Comment

Comment 2:
The security functional requirement “Cryptographic operation (FCS_COP.1)” met by the TOE have the following 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

These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function and are not part of the BSI-PP-0084. Most requirements concerning key management shall be fulfilled by the environment since the Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE.

For the security functional requirement FCS_COP.1 [TDES], FCS_COP.1[AES] and the respective dependencies FCS_CKM.1, FCS_CKM.4 and FDP_ITC.1 or FDP_ITC.2 have to be fulfilled by the environment. That mean, that the environment shall meet the requirements FCS_CKM.1 and FCS_CKM.4 as defined in CC part 2, section 10.1 and shall meet the requirements FDP_ITC.1 or FDP_ITC.2 as defined in CC part 2, section 11.7.

For the security functional requirement FCS_COP.1[RSA], the respective dependencies FCS_CKM.4 and FDP_ITC.1 or FDP_ITC.2 have to be fulfilled by the environment. That mean, that the environment shall meet the requirements FDP_ITC.1 or FDP_ITC.2 as defined in CC part 2, section 11.7. The respective dependency FCS_CKM.1 has to be fulfilled by the TOE with the security functional requirement FCS_CKM.1[RSA] (for FCS_COP.1[RSA]) as defined in section 7.1.4. Additionally the requirement FCS_CKM.1 can be fulfilled by the environment as defined in CC part 2, section 10.1.

For the security functional requirement FCS_CKM.1[RSA] the respective dependency FCS_COP.1 is fulfilled by the TOE. The environment covers the respective dependency FCS_CKM.4. That mean, that the environment shall meet the requirement FCS_CKM.4 as defined in CC part 2, section 10.1.

End of Comment

6.3.3 Rationale of the Assurance Requirements

The chosen assurance level EAL5 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 were chosen in order to meet the assurance expectations explained in the following paragraphs. In Table 12 the different assurance levels are shown as well as the augmentations. The augmentations are in compliance with the BSI-PP-0084.

- **ALC_DVS.2 Sufficiency of security measures**

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

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.

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**

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.

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.

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

All these dependencies are satisfied by EAL5.

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.

7 TOE summary specification

This chapter provides information to potential users of the TOE how the TOE satisfies the Security Functional Requirements. In addition to the SFRs the TOE has security mechanisms that add to implement the security policies.

7.1 Malfunction

Malfunctioning relates to the security functional requirements FRU_FLT.2 and FPT_FLS.1. The TOE meets these SFRs by a group of security measures that guarantee correct operation of the TOE.

The TOE maintains its correct functioning by the following security mechanisms:

- Environmental detectors to verify if the environmental conditions are within the specified range
- Sensor self-tests verifies the correct functioning of the environmental detectors
- Total failure checking and statistical tests on random number generator data verifies the quality of the generated random data

If one of the detectors or mechanisms detects an alarm event, the TOE will enter reset state or trigger an exception or return error message to the security IC embedded software to make sure a secure situation.

FPT_FLS.1: Failure with preservation of secure state

Failures such as frequency, voltage, temperature，light and power glitch that are out of the special range are detected by TOE’s detectors. The failures will cause an alarm signals to be triggered, which will result in a special function register bit to be set and a reset (secure state).

FRU_FLT.2: Limited fault tolerance

In order to prevent malfunction, the operation signals (clock, reset, supply voltage) are filtered/regulated. The detectors that prevent noise, glitches and extremely high/low frequency in the external reset or clock pad are implemented as hardware.

7.2 Leakage

Leakages relate to the security requirements FDP_ITT.1, FDP_IFC.1 and FPT_ITT.1. The TOE meets these SFRs by implementing several measures that provides logical protection against leakage.

The TOE prevents information leakage by means of the following security measures:

- Memory encryption
- Memory address scramble
- Data and key masking
- DFA countermeasures for all secure cryptographic functions

FDP_IFC.1: Subset information flow control

To prevent data analysis from information stored in memory as well as information on internally transmitted, memory encryption function is applied. The algorithms for the memory encryption are proprietary, and the key used in ROM encryption is static while the one used in RAM and EEPROM is dynamic. Furthermore the EEPROM/RAM encryption key can be changed by the embedded software.

FDP_ITT.1: Basic internal transfer protection

The combination of TOE features listed below achieves the effective protection of access to the internal signals.

- Address scrambling for memory
- Memory encryption
- Synthesizable processor core
- Bus polarity switching

FPT_ITT.1: Basic internal TSF data transfer protection

The combination of TOE features listed below achieves the effective protection of access to the internal signals.

- Address scrambling for memory
- Memory encryption
- Synthesizable processor core
- Bus polarity switching

7.3 Physical manipulation and probing

Physical manipulation and probing relates to the security requirement FPT_PHP.3. The TOE meets this SFR by implementing security measures that provides physical protection against physical probing and manipulation.

The following security measures protect the TOE against physical manipulation and probing:

- Active shielding
- Memory integrity checking
- Memory encryption
- Bus polarity switching

If a physical manipulation or physical probing attack is detected, an alarm will be automatically triggered by the hardware, which will cause the chip to be reset.

FPT_PHP.3: Resistance to physical attack

This requirement focuses on the security features when the active shield is manipulated so that the features prevent the TOE from physical intrusive attacks. The TOE resets once the physical manipulations or physical probing attacks are detected.

Synthesizable processor core with glue logic makes reverse engineering and signal identification unpractical.

Memory encryption and bus polarity switching prevents memory and address/data buses from probing attacks. Moreover, routing the sensitive signals such as alarm signals or buses in middle layer is effective.

FDP_SDC.1: Stored data confidentiality

All of the data that stored within memory areas are encrypted, thus the attacker can only get the cipher-text data. The encrypt algorithm is not publicity. The address of the stored data is also be encrypted, so it is very difficult to get the stored data by the attacker.

FDP_SDI.2: Stored data integrity monitoring and action

The data stored in memory with checksum code using cyclic redundancy check algorithm to verify the stored data integrity. The check algorithm is valid in the memory areas including: EEPROM, System RAM and ROM.

7.4 Abuse of functionality and identification

Abuse of functionality and identification relates to the security requirements FMT_LIM.1, FMT_LIM.2 and FAU_SAS.1. The TOE meets these SFRs by implementing a complicated test mode control mechanism that prevents abuse of test functionality delivered as part of the TOE.

Test functionality is permanently disabled after production by a combination of physical and logical security measures.

FAU_SAS.1: Audit storage

The manufacturing data written into the EEPROM of the TOE are READ ONLY once the TOE is set from test mode to application mode.

FMT_LIM.1: Limited capabilities

The access to the test mode is limited. Furthermore, once the TOE is switched to application mode, the test mode is unavailable any more.

FMT_LIM.2: Limited availabilities

The access to the test mode is limited. Furthermore, once the TOE is switched to application mode, the test mode is unavailable any more. Only under test mode, functional test is able to be conducted.

7.5 Random numbers

Random numbers relate to the security requirement FCS_RNG.1. The TOE meets this SFR by providing a random number generator.

FCS_RNG.1: Random number generation

Random number generation algorithm that follows the requirements and the metric of the AIS20 Class DRG.3 standard and a True Random Number Generator for AIS20 Class PTG.2 Random Number Generator fulfills this requirement.

7.6 Cryptographic functionality

Cryptographic functionality relates the security requirements FCS_COP.1 [TDES], FCS_COP.1 [AES] and FCS_COP.1 [RSA]. The TOE meets these SFRs by providing cryptographic functionality by means of a combination of accelerating hardware and IC dedicated support software.

FCS_COP.1: Cryptographic operation

- TDES

The TOE provides TDES symmetric algorithm according to the NIST SP800-67[17] and NIST SP800-38A[18] standard. TDES symmetric algorithm is used for the TOE in encrypting and decrypting data. The TDES symmetric algorithm works with 112 bits key size. The TOE provides TDES with supporting ECB/CBC mode.

- AES

The TOE shall provide cryptographic functionality to perform an AES encryption and decryption with 128/192/256 bits keys to the Security IC Embedded Software. The AES algorithm meets the following FIPS PUB 197[19] and NIST SP800-38A[18].

- RSA

The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Rivest-Shamir-Adleman (RSA) and cryptographic key sizes from 512 to 2048 bits that meet the RSA standard [16].

7.7 Memory access control policy

FDP_ACC.1: Subset access control
FDP_ACF.1: Security attributes based access control

Special function register access control and memory access control are related to these requirements.

Invalid access will be denied and triggers a hardfault exception.

8. Bibliography

8.1 Evaluation Documents

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003

[4] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004

[5] A proposal for: Functionality classes for random number generators, Version 2.0, 18 September 2011

[6] Security IC Platform Protection Profile, Version 1.0, 13th Jan. 2014, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084

8.2 Developer Documents

[7] CIU9872B_01 C12_Operational_User_Guidance (AGD_OPE)

[8] CIU9872B_01 C12_Preparative_procedures (AGD_PRE)

[9] CIU9872B_01 C12_Product_Datasheet

[10] CIU9872B_01 C12_Crypto_Library_User_Guide

8.3 Other Documents

[11] FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION DATA ENCRYPTION STANDARD (DES) Reaffirmed 1999 October 25

[12] ISO/IEC 7816-2:1996 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of contacts

[13] ISO/IEC 7816-3:1997 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols

[14] ISO/IEC 14443-3:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision

[15] ISO/IEC 14443-4:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol

[16] PKCS #1: RSA Cryptography Standard, RSA Laboratories, Version 2.2, 2012

[17] National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST SP800-67, Revision 1.1, revised January 2012

[18] National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, Recommendation for Block Cipher Modes of Operation, NIST SP800-38A, December 2001

[19] U.S. Department of Commerce / National Bureau of Standards, Advanced Encryption Standard (AES), FIPS PUB 197, 2001, November 26.

[20] A proposal for: Functionality classes for random number generators, Version 2.0, 18th September 2011