Security target Lite of

Secure Chip

CIU9872B_01 V1.0

with IC Dedicated Software V1.0

Version 1.0

Date 2024-12-11

CEC Huada Electronic Design Co., Ltd.

REVISION HISTORY

1.0	2024.12.12: Release version

Content

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

The Security Target reference is "Security target Lite of Secure Chip CIU9872B_01 V1.0 with IC Dedicated Software V1.0, V1.0".

1.1.2 TOE Reference

The TOE is identified in one configuration named "Secure Chip CIU9872B_01 V1.0 with IC Dedicated Software V1.0". All components of the TOE and their respective version numbers are listed in Table 1.
In this document the TOE is abbreviated to CIU9872B_01 V1.0.

1.2 TOE Overview

1.2.1 Introduction

The TOE are the IC hardware with IC Dedicated Software which is stored in ROM and Non-user FLASH and documentations which describes the instruction set and the usage [7] [8] [9] [10].

The main usage of the TOE is for banking and finance applications. And the scope of the TOE includes the IC hardware and IC dedicated software which is constituted of Chip Management System (CMS), Cryptographic and functional library and Lib file API library. CMS implements the functionality of booting process controlling. The Cryptographic and functional library implements the arithmetic functions of RSA (with key length from 512 bits to 2048bits and 4096 bits) and TDES (with 2 keys mode) which are stored in ROM. The Lib file API library also includes a random number generation function which is in form of Lib file API library files.

The IC hardware is a microcontroller incorporating a central processing unit (CPU), instruction cache, memories accessible via Enhanced Memory Management Unit (EMMU), cryptographic coprocessors, Random Number Generator (RNG), sensors, test protection, clock/reset/power management units and communication interfaces. The CPU processor is a very low gate count and highly energy efficient processor for the use in microcontrollers and embedded applications that require an area optimized processor for the use in environments where security is an important consideration. On-chip memories are ROM，RAM and FLASH. The FLASH contains non-user FLASH and user FLASH for data and program storage. The whole FLASH consists of memory cells followed by the parity check values for data integrity check.
The documentation includes:

- CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Operational User Guidance (AGD_OPE) [7]
- CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Preparative procedures (AGD_PRE) [8]
- CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Product Datasheet [9]
- CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Crypto and Function 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 by the embedded software in the banking and finance market applications. Hence the TOE shall maintain：

- the integrity and the confidentiality of code and data stored in its memories and while processed in the device
- the memory access controlled by memory address and 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 functionalities.

The TOE provides hardware for implementations of secure applications with:

- CPU with SecurCore 32-bit microprocessors
- Security detectors including high and low temperature detectors, internal and external frequency detectors, internal and external voltage detectors, the external glitch detector and light detectors
- Active shielding against physical attacks
- TDES/DES coprocessor (2 keys TDES mode) with countermeasures against SCA
- Hardware coprocessor PKE which facilitated the RSA implementations supporting large integer arithmetic operations of modular multiplication, modular addition and modular subtraction (These operations are used by software to implement the RSA. Based on the RSA function, the countermeasures for RSA

against attacks of SCA, DFA and FA are implemented by software.)

- Memory access control
- Memory data encryption and address scrambling
- Data integrity check for ROM， RAM and FLASH
- Security-sensitive registers protection
- Bus polarity
- RNG1 module serves with a highly reliable true random number generator, which is compliant with PTG.2 class of AIS20/31[2013] [20]
- RNG2 module serves with internal random numbers
- Test mode protection
- Self-test function
- SDL

Note that the TOE contains the following hardware, but they are not claimed as security functions.

- Chinese domestic cryptographic coprocessors: SM3 and SM4
- CRC coprocessors
- TDES/DES coprocessor (DES mode) with countermeasures against SCA
- AES coprocessor with countermeasures against SCA

The TOE provides software for implementations of secure applications with:

- CMS is for booting process controlling
- Cryptographic and functional library for the functions of 2 key TDES and private key functions of RSA (with key length from 512 bits to 2048bits and 4096 bits) in ROM
- Lib file API library for the functions of a highly reliable true random number generation API interface with FA countermeasures cooperating with hardware which is compliant with PTG.2 class of AIS20/31[2013], a deterministic random number generation API with FA countermeasures which is compliant with DRG.3 class of AIS20/31[2013].

Note that the TOE contains the following cryptographic algorithms and functions, but they are not claimed as security functions.

- Power Management API
- SHA Algorithm API
- Get Algorithm API Version API
- Flash Translation Layer API
- Enhancing Chip Stability Solution API
- Get Chip Unique Serial Number API
- Get Chip Firmware Total Version API
- APIs in ECC library
- Chinese domestic cryptographic algorithms (SM2, SM3 and SM4)
- APIs in RNG library except the true/deterministic random number generation

APIs

- 3key TDES algorithm API
- DES Algorithm API not claimed as security function but implemented SCA, DFA and FA countermeasures
- AES Algorithm API
- APIs in RSA library except the private key calculation APIs

1.2.3 TOE type

The TOE is Secure Chip CIU9872B_01 V1.0 with IC Dedicated Software V1.0 intended for use as a security IC.

1.2.4 Required non-TOE hardware/software/firmware

None.

1.3 TOE Description

1.3.1 Physical Scope of TOE

A block diagram of the IC is depicted in Figure 1.

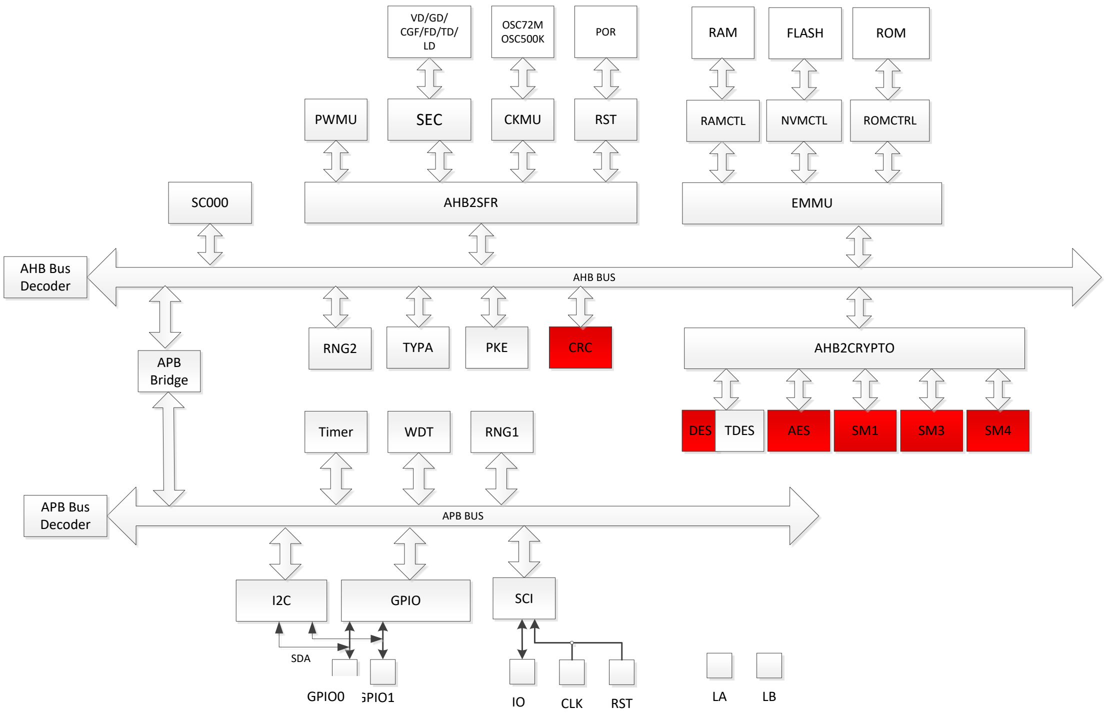

Figure 1 : Hardware Blocks of the TOE (the security-not-claimed parts are indicated with red color)

The scope of the TOE includes the IC hardware, CMS, Cryptographic and functional library and Lib file API library.

Table 1 : Components of the TOE scope

<table>
<tr><td>Type</td><td>Name</td><td colspan="2">Release</td><td colspan="2">Form of delivery</td></tr>
<tr><td>IC Hardware</td><td>CIU9872B_01</td><td colspan="2">V1.0</td><td colspan="2">Module</td></tr>
<tr><td rowspan="4">Security IC Dedicated Software</td><td>CMS</td><td rowspan="4">V1.0</td><td>V1.0</td><td colspan="2">In Flash</td></tr>
<tr><td>Cryptographic and functional library</td><td>V1.01</td><td colspan="2">In ROM
(APIs of RSA, TDES.)</td></tr>
<tr><td rowspan="2">Lib file API library</td><td rowspan="2">V1.0</td><td rowspan="2">Lib file
(APIs of random number generation function)</td><td>CIU9872B_01_V1_API_RNG.lib</td></tr>
<tr><td>CIU9872B_01_V1_API_RNG.h</td></tr>
</table>

The lib files (.lib and .h files) will be delivered as the package with pgp signed and encrypted via Email.

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	Form of delivery
Document	CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Operational User Guidance (AGD_OPE)	V1.6	The PDF Electronic Document
Document	CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Preparative procedures (AGD_PRE)	V1.3	The PDF Electronic Document
Document	CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Product Datasheet	V1.3	The PDF Electronic Document
Document	CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Crypto and Function Library User Guide	V1.3	The PDF Electronic Document

The electronic documents (.pdf files) will be delivered as the package with pgp signed and encrypted via Email.

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

The CPU used in the TOE.

Memory

RAM, ROM and Flash provided with memory data encryption and memory address scrambling.

EMMU

Area and chip mode based memory access control to ROM, RAM and FLASH is implemented by EMMU.

Coprocessors

- The TDES/DES coprocessor supports TDES and DES operations with ECB mode and CBC mode. TDES supports 2-key operation with two 56-bit keys (key length of 112 bits). The TDES/DES coprocessor supports countermeasures against SCA.
- The PKE coprocessor supplies basic arithmetic functions to support the implementation of asymmetric cryptographic algorithms RSA, ECC and SM2 in Cryptographic and functional library. Note that the security of ECC and SM2 is not claimed.
- The AES coprocessor supports the AES operations. Note that the security of this component is not claimed.
- The Chinese domestic cryptographic coprocessors. Note that the security of this component is not claimed.
- The CRC coprocessors. Note that the security of the CRC coprocessor component is not claimed.

TRNG (RNG1)

A highly reliable true random number generator compliant with PTG.2 class of AIS20/31[2013], which consists of a provable physical noise source and well-designed post-processor.

Internal random number generator (RNG2)

The random number generator is for the internal use of the chip which is invisible by the user.

TEST

The test functionalities protection is implemented in the TEST block. The test mode is protected by the TEST block and not available anymore after phase 4.

Power (PWMU)

The TOE provides 4 power modes for chip power management, which are:

- Normal power mode
- Standby power mode
- Stop clock power mode
- CPU hold power mode

SEC

Security management module supports the active shielding working and auto-check, detectors auto-check, memory data encryption key and memory address scrambling key refreshing and security features flags management.

Reset (RSTMU)

System reset management module supports the boot-up sequence and the reset mechanisms of the chip.

Clock (CKMU)

Chip clock management module supports the configurations for the clock frequency settings of system and coprocessors.

Interfaces

- SCI
- TYPEA

Detectors

Detectors are for extreme environmental conditions detection.
Detectors present the self-test feature.

Other major components

- Programmable timers
- Watchdog
- Oscillator (OSC)
- AHB2SFR, AHB2CRYPTO，APB Bridge are the connection modules between buses who supports the transferring of the bus signals for different buses.

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 Test Mode and Non-test Mode. Test Mode has unlimited access to the hardware components, and is only valid during manufacture. Non-test Mode has restricted access to the hardware components, like CPU, special function registers and the memories. Special function registers for the hardware components control for the Security IC Embedded Software are interrelated to the activities of the CPU, EMMU, interrupt control, I/O configuration, FLASH, timers, interfaces and coprocessors.

Sensitive registers protection, which is data integrity check, is performed on the sensitive registers. Bus polarity protection is performed on the bus.

The end-user will receive TOE running in Non-test Mode with disabled test functionality. The disabling of the test functionality is performed after production testing and protected by hardware countermeasures.

1.3.2.2 Software Description

The IC Dedicated Software includes CMS, cryptographic and functional library and Lib file API library.

CMS

CMS is for booting process controlling. The user program which is downloaded to the user FLASH during the manufacture will be booted at the end of CMS execution. The download process is disabled when the TOE is delivered to the end-user.

Cryptographic and functional library

Cryptographic and functional library includes the functions of TDES and RSA with key length from 512 bits to 2048bits and 4096 bits. TDES Cryptographic library supports countermeasures against TA, DFA and FA. RSA Cryptographic library supports countermeasures against SCA, DFA and FA.

Note that cryptographic and functional library also includes the functions of SHA, AES，ECC，Chinese domestic cryptographic algorithms (with SM2, SM3 and SM4 included), power management, Flash operation and version-get. However, the security of these components is not claimed.

Lib file API library

Lib file API library includes the functions of a highly reliable true random number generation API interface with FA countermeasures cooperating with hardware which is compliant with PTG.2 class of AIS20/31[2013], a deterministic random number generation API with FA countermeasures which is compliant with DRG.3 class of AIS20/31[2013].

Note that lib file API library also includes the functions of Enhancing Chip Stability Solution, chipID-get and Lib file API library version-get. However, the security of these components is not claimed.

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 and phase 5 are included in the evaluation of the IC:

- The IC Packaging (Phase 4)
  - Security IC packaging (and testing)
  - Pre-personalization if necessary
- The Composite Product finishing process, preparation and shipping to the personalization line for the Composite Product (Composite Product Integration Phase 5)

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

- Security IC Embedded Software Development (Phase 1)
- The Composite Product 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

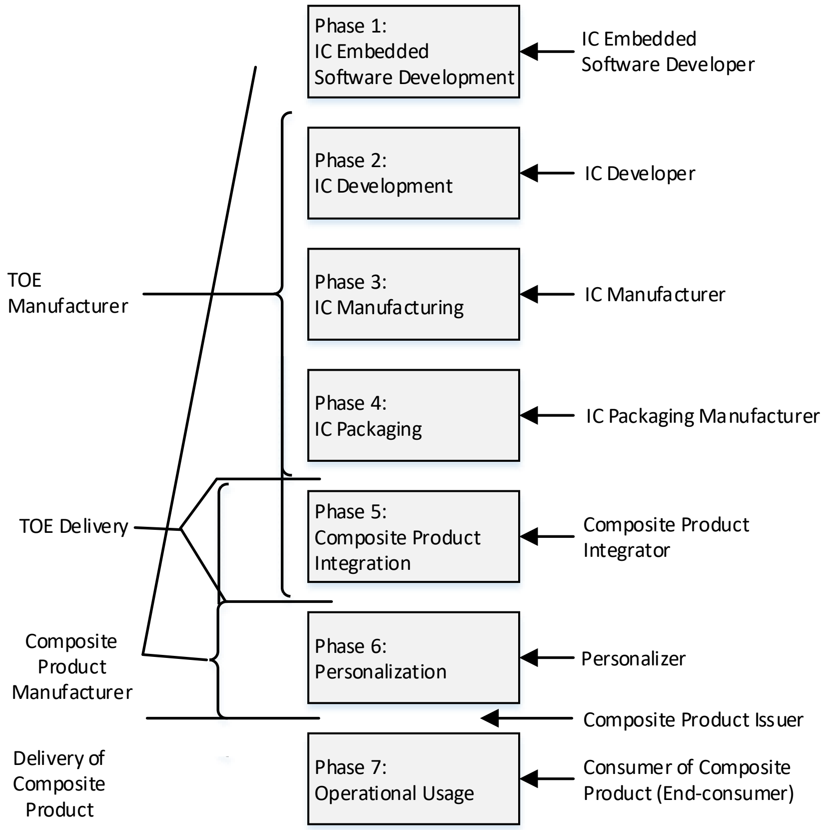

Figure 2 : Definition of “TOE Delivery” and responsible Parties

The Security IC Embedded Software is developed outside the TOE development in Phase 1. The TOE is developed in Phase 2, produced in Phase 3 and packaged in phase 4. Then the TOE is delivered after Phase 4 in packaged form or after Phase 5 in form of modules with embedded software integrated in it, depending on the customer’s order. The “Composite Product Manufacturer” includes all roles responsible of the TOE during phase 1, 5 (optional), and 6. The CMS loader function is disabled after the delivery of the TOE.

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 5, April 2017, CCMB-2017-04-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004
- Application Notes and Interpretation of the Scheme (AIS 34): Evaluation Methodology for CC Assurance Classes for EAL5+(CC v2.3 & v3.1) and EAL6(CC v3.1), Version 3, 03.09.2009

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. This Security Target also includes conformance to packages defined in the BSI-PP-0084:

- Package "TDES" (with augmentations)

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 EAL6 augmented. The augmentations to EAL6 are ALC_FLR.1.

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

The assurance level for this Security Target is EAL6 augmented with ALC_FLR.1. 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 EAL6, 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 security 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 (EAL6+) 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:

- DES/TDES encryption and decryption
- private key functions of RSA (with key length from 512 bits to 2048bits and 4096 bits)

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 of the Composite TOE

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.RSA RSA functionality

The TOE shall provide cryptographic functionality to perform an RSA signature generation and decryption with key lengths from 512bits to 2048bits and 4096 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 Chip mode and Area based Memory Access Control

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

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
OE.Resp-Appl	Treatment of user data of the Composite TOE	Phase 1

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).

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

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

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 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.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.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 chip modes and 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 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 families 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.1, FMT_LIM.1, FMT_LIM.2, FAU_SAS.1 and FDP_SDC.1 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 8.2 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 [6] 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	Random number generation	No

The above extended components FAU_SAS.1, FDP_SDC.1, FCS_RNG.1, FMT_LIM.1 and FMT_LIM.2 are introduced in PP to define the IT security functional requirements of the TOE as additional families FAU_SAS of Class FAU, FDP_SDC of Class FDP, FCS_RNG of Class FCS and FMT_LIM of the Class FMT (Security Management). This family describes the functional requirements for the Test Features of the TOE.

The above SFRs are applied entirely to the ST. The application notes from the PP are elaborated below:

- **FPT_FLS.1**

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*[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). This address Application Note 14 in 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). This address Application Note 15 in PP [6].

- **FPT_PHP.3**

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*[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. This address Application Note 19 in PP [6].

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

- **FAU_SAS.1**

The additional component FAU_SAS.1 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.

---

1 [assignment: *list of subjects*]
2 [assignment: *physical tampering scenarios*]
3 [assignment: *list of TSF devices/elements*]

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 *FLASH*[3]

- **FDP_SDI.2**

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 *inconsistencies between stored data and corresponding EDC*[4] on all objects, based on the following attributes: *EDC value for the FLASH and RAM*[5]
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall *trigger reset or exception*[6].

---

1 [assignment: *list of subjects*]
2 [assignment: *list of audit information*]
3 [assignment: *type of persistent memory*]
4 [assignment: *integrity errors*]
5 [assignment: *user data attributes*]
6 [assignment: *action to be taken*]

Dependencies: No dependencies

Application note: EDC is performed on all the memories.

Refinement: **The errors of EDC check happened to data in RAM and instructions stored in FLASH will trigger a reset, while data stored in FLASH will trigger an exception.**

- **FDP_SDC.1**

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 *FLASH and RAM*[1].

- **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]

FCS_RNG.1.1[PTG.2] The TSF shall provide a *physical*[2] 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*

[1] [assignment: *memory area*]

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

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*[1].

(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 continuously*[2]. *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*[3].

FCS_RNG.1.2[PTG.2] The TSF shall provide *octets of bits*[4] that meet:

(PTG.2.6) *Test procedure A*[5] *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)

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RNG.1.1[DRG.3] The TSF shall provide a *deterministic*[6] random number generator that implements:

(DRG.3.1) *If initialized with a random seed using PTRNG of class PTG.2 as random source*[7], *the internal state of the RNG*

---

[1] [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]*

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

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

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

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

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

[7] [selection: using a PTRNG of class PTG.2 as random source, using a PTRNG of class PTG.3 as random source,

shall have 127 bits of entropy[1].

(DRG.3.2) *The RNG provides forward secrecy.*

(DRG.3.3) *The RNG provides backward secrecy even if the current internal state is known*[2].

FCS_RNG.1.2[DRG.3] The TSF shall provide *octets of bits*[2] that meet:

(DRG.3.4) *The RNG initialized with a random seed using PTRNG of class PTG.2*[3] *generates output for which* [2^{40}][4] *strings of bit length 128 are mutually different with probability* [$1-2^{-23}$][5].

(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*[6].

By this, all assignment/selection operations are performed. This Security Target does not perform any other/further operations than stated in the PP [6].

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

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 operation
FCS_CKM.4	Cryptographic key destruction

Memory access control

The TOE provides Chip mode and Area based Memory Access Control.

The security service being provided is described in the Security Function Policy (SFP)

---

using an NPTRNG of class NTG.1 [assignment: other requirements for seeding]]

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

[2] [assignment: list of security capabilities]

[3] [assignment: requirements for seeding]

[4] [assignment: number of strings]

[5] [assignment: probability]

[6] [assignment: a defined quality metric]

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 chip mode and area based access permission control. The permission control information is evaluated by the hardware so that access is granted or denied.

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 at different chip modes on data including code stored in memory areas.

The Memory Access Control Policy is enforced on the following access ports, which are: CPU access over the bus system.

The Memory Control Policy controls access to memories by EMMU and all the memory control policies implemented in EMMU are fixed in hardware.

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: the 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.

---

[1] [assignment: access control SFP]
[2] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

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*[1] to objects based on the following: *all subjects and objects and the attributes：chip mode, memory range of the accessed object, the EMMU access permission control to control the access permission*[2].

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 chip mode and EMMU access permission control information of the chip mode and memory range of the objects during the access to determine whether the accesses can be granted to perform the operation*[3] *by the subject.*

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*[4].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[5].

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

[1] [assignment: access control SFP]
[2] [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]
[3] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[4] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]
[5] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

- 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*[1] in accordance with a specified cryptographic algorithm *TDES in ECB mode, CBC mode*[2] and cryptographic key sizes *112 bit*[3] that meet the following *NIST SP800-67[17] and NIST SP800-38A[18]*[4].

FCS_CKM.4[TDES]	**Cryptographic key destruction[TDES]**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1[TDES]	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *by overwriting the TDES key register with a random number*[5] that meets the following: *none*[6].

- **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.

1 [assignment: *list of cryptographic operations*]
2 [assignment: *cryptographic algorithm*]
3 [assignment: *cryptographic key sizes*]
4 [assignment: *list of standards*]
5 [assignment: cryptographic key destruction method]
6 [assignment: *list of standards*]

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 *signature generation, decryption*[1] in accordance with a specified cryptographic algorithm *Rivest-Shamir-Adleman (RSA)* [2] and cryptographic key sizes *from 512 to 2048 bits and 4096 bits*[3] that meet the following: *RSA standard [16]*[4].

Application Notes: The key length is determined by user based on application requirements. User shall assure the security in the application.

FCS_CKM.4[RSA] Cryptographic key destruction[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.4.1[RSA] The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *by overwriting the PKE RAM with a random number and changing the PKE RAM encryption key and address scrambling key*[5] that meets the following: *none*[6].

6.2 Security Assurance Requirements

The evaluation assurance level is EAL6 augmented with ALC_FLR.1. In the following table, the security assurance requirements are given.

Table 12: Assurance components

Aspect	**Acronym**	**Description**
Development	ADV_ARC.1	Security Architecture design

1 [assignment: *list of cryptographic operations*]
2 [assignment: *cryptographic algorithm*]
3 [assignment: *cryptographic key sizes*]
4 [assignment: *list of standards*]
5 [assignment: cryptographic key destruction method]
6 [assignment: *list of standards*]

	ADV_FSP.5	Functional specification
	ADV_IMP.2	Implementation representation
	ADV_INT.3	TSF internals
	ADV_SPM.1	Formal model of Security Policies
	ADV_TDS.5	TOE design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.5	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.3	Tools and techniques
	ALC_FLR.1	Basic flaw remediation
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.3	Analysis of coverage
	ATE_DPT.3	Depth
	ATE_FUN.2	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability testing

- **ADV_SPM**

The developer shall provide a formal security policy model.

ADV_SPM.1 **Formal TOE security policy model**

Hierarchical to: No other components

Dependencies: ADV_FSP.4 Complete functional specification

ADV_SPM.1.1D The developer shall provide a formal security policy model for the *Memory Access Control Policy (FDP_ACC.1, FDP_ACF.1.)* [1].

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, FCS_CKM.4 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" - FCS_CKM.4[TDES] "Cryptographic Key Destruction"
O.RSA	- FCS_COP.1[RSA] "Cryptographic operation" - FCS_CKM.4[RSA] "Cryptographic Key Destruction"
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 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 are provided by the environment. Keys for RSA can be provided either by the TOE or the

[1] [assignment: list of policies that are formally modeled].

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 chip modes and 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 Security IC 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 dependences 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，FCS_CKM.4 and FDP_SDI.2 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	See comment 1
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1)	See comment 1

	FCS_CKM.4	Yes
FCS_COP.1[RSA]	FCS_CKM.1	See comment 1
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1)	See comment 1
	FCS_CKM.4	Yes
FCS_CKM.4[TDES]	FCS_CKM.1	See comment 1
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1)	See comment 1
FCS_CKM.4[RSA]	FCS_CKM.1	See comment 1
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1)	See comment 1
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes See comment 2
FDP_SDI.2	None	N/A

Comment 1:
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]

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 Security IC 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[RSA] , the respective dependencies FCS_CKM.1 and FDP_ITC.1 or FDP_ITC.2 are not considered in this Security Target. This is because the decision on how to import user data and how to generate the keys shall be left to the Security IC Embedded Software.

That means that the environment shall meet the requirements FCS_CKM.1 as defined in CC part 2, section 10.1 or shall meet the requirements FDP_ITC.1 or FDP_ITC.2 as defined in CC part 2, section 11.7.
End of Comment

Comment 2:

All security attributes for the Memory Access Control Policy SFP are fixed and require no management or initialization. No objects or information can be created under the SFP, and hence there is no override of associated default values.

End of Comment

6.3.3 Rationale of the Assurance Requirements

The chosen assurance components are based on the underlying PP [6]. The Security Target uses the same augmentations as the PP [6], but chooses a higher assurance level EAL6. The level EAL6 is chosen in order to meet assurance expectations of high security applications. Additionally, the requirement of the PP [6] to choose at least EAL4 is fulfilled.

The rationale for the augmentations is the same as in the PP. The assurance level EAL6 is an elaborated pre-defined level of the CC, part 3 [3]. The assurance components in an EAL level are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL 6. Therefore, these components add additional assurance to EAL 6, but the mutual support of the requirements is still guaranteed. Therefore, the augmentation with the requirement ALC_FLR.1 were chosen in order to meet the assurance expectations explained in the following paragraphs.

As stated in the Section 6.3.3 of the PP [8], it has to be assumed that attackers with high attack potential try to attack smartcards used for high security applications. Therefore, specifically AVA_VAN.5 was chosen by the PP [6] in order to assure that even these attackers cannot successfully attack the TOE.

In Table 13 the different assurance components are shown as well as the augmentations.

- **ALC_FLR.1 Basic flaw remediation**

Flaw remediation requires that discovered security flaws be tracked and corrected by the developer. Although future compliance with flaw remediation procedures cannot be determined at the time of the TOE evaluation, it is possible to evaluate the policies and procedures that a developer has in place to track and correct flaws, and to distribute the flaw information and corrections.

ALC_FLR.1 has no dependencies.

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 Protection against 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
- Detector self-test verifies the correct functioning of the environmental detectors
- Data integrity checking verifies the correctness of the data read from memory and security sensitive registers
- Total failure checking, continuously repeat data check 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 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).
Failures such as total failure, continuously repeat data check and statistical failure are tested by self-tests for random number generator. 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).
Failures of integrity check are detected by data integrity checking. The failure of

integrity check of data reading from NVM will cause an exception. It can be dealt with in exception handler to set the chip into a security state (like reset). The failures of other data 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.

There is a security-delay-latch in TOE.

7.2 Protection against 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
- Address scrambling for memory
- Bus polarity
- SCA countermeasures for all secure cryptographic functions
- 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.

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
- Bus polarity
- SCA countermeasures for all secure cryptographic functions
- DFA countermeasures for all secure cryptographic functions

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
- Bus polarity
- SCA countermeasures for all secure cryptographic functions
- DFA countermeasures for all secure cryptographic functions

7.3 Physical protection

Physical manipulation and probing relates to the security requirement FPT_PHP.3, FDP_SDC.1 and FDP_SDI.2. 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

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 to verify the stored data integrity. When the data is fetching from memory, if the data be changed by any abnormal action, there would be a signal to lead exception or reset. The check algorithm is valid in the memory areas including: System RAM and FLASH.

7.4 Protection against abuse of functionality

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

In the test mode, a proprietary protocol is used to write the identification by the TEST administrator during the manufacturing process. The manufacturing data written into the non-user FLASH of the TOE are READ ONLY once the TOE is set from test mode to non-test mode.

FMT_LIM.1: Limited capabilities

The access to the test mode is limited, which means only by supplying an authentication code through a proprietary protocol. Furthermore, once the TOE is switched to non-test mode, the test mode is unavailable any more.

FMT_LIM.2: Limited availabilities

The access to the test mode is limited, which means only by supplying an authentication code through a proprietary protocol. Furthermore, once the TOE is switched to non-test mode, the test mode is unavailable any more. Only under test mode, functional test is able to be conducted.

7.5 Random number generator

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 AIS20/31[2013] Class DRG.3 standard and a True Random Number Generator for AIS20/31[2013] 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[RSA], FCS_CKM.4[TDES] and FCS_CKM.4[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 112bits key size. The TOE provides TDES with supporting ECB/CBC mode.

- RSA

The TSF shall perform signature generation and decryption in accordance with a specified cryptographic algorithm Rivest-Shamir-Adleman (RSA) and cryptographic key sizes from 512 to 2048 bits and 4096 bits that meet the RSA standard [16].

FCS_CKM.4: Cryptographic key destruction

- TDES

The TOE provides TDES key destruction. The TDES key destruction method is to cover the TDES key register using random number.

- RSA

The TOE provides key destruction. The method is to cover the PKE RAM using random number and change the PKE RAM encryption key and address scrambling key.

7.7 Memory access control

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

Memory access control is related to these requirements.
The EMMU is responsible for memory access control based on memory address range and chip modes.
Invalid access will be denied.

8. Bibliography

8.1 Evaluation Documents

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[4] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

[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 V1.0 with IC Dedicated Software V1.0_Operational User Guidance (AGD_OPE), version 1.6

[8] CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Preparative procedures (AGD_PRE), version 1.3

[9] CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Product Datasheet, version 1.3

[10] CIU9872B_01 V1.0 with IC Dedicated Software V1.0_Crypto and Function Library User Guide, version 1.3

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] Functionality classes and evaluation methodology for deterministic/physical random number generators, version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[21] ANSI X9.62-2005: Public Key Cryptography for The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), November 16 2005, American National Standards Institute

[22] ANSI X9.63-2011: Public Key Cryptography for The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, December 2011, American National Standards Institute

[23] IETF RFC 7748: Elliptic Curves for Security, January 2016, Internet Research Task Force (IRTF)

[24] Technical Guideline BSI TR-03111: Elliptic Curve Cryptography, Version 2.10, 1st June 2018, Federal Office for Information Security