Security Target Lite of Security Chip GSEA01.x.D00 with IC Dedicated Software V1.31

Shenzhen Goodix Technology Co., Ltd

Revision History

Date	Version	Comment
21 Jan 2022	1.31	Derived from full Security Target v1.31

Table of Content

Document information

Information	Content
Keywords	Goodix, GSEA01, Secure Element, Crypto Library, Common Criteria, Security Target
Abstract	This document is the Security Target of the Security Chip of the GSEA01 family with IC Dedicated Software, developed and provided by Goodix Ltd. GSEA01 conforms to Evaluation Assurance Level 5 of the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5 with augmentations ALC_DVS.2 and AVA_VAN.5.

Glossary

AES	Advanced Encryption Standard
APB	Advanced Peripheral Bus
API	Application Process Interface
CBC	Cipher Block Chaining Mode
CFB	Cipher Feedback Mode
CRC	Cyclic Redundancy Checks
CRT	Chinese Remainder Theorem
CTR	Counter Mode
DES/TDES	Data Encryption Standard/Triple Data Encryption Standard
DMAC	Direct Memory Access Controller
DPA	Differential Power Analysis
DRNG	Deterministic Random Number Generation
ECB	Electronic Code Book Mode
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
eID	Electronic Identification
ES	Embedded Software
HAL	Hardware Abstraction Layer
LDO	Low Drop Out Regulator
MMU	Memory Management Unit
NIR	Near Infrared
NVIC	Nested Vector Interrupt Controller
OFB	Output Feedback Mode
OSCCA	China Office of State Commercial Cryptography Administration
PKCC	Public-Key Cryptographic Coprocessor
PKCRAM	PKCC Random Access Memory

RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read-Only Memory
RSA	Rivest-Shamir-Adleman Algorithm
SAHB	Secure Advanced High-performance Bus
SAPB	Secure Advanced Peripheral Bus
SCA	Side Channel Analysis
SFR	Special Function Register, as well as Security Functional Requirement
SPI	Serial Peripheral Interface
SYSRAM	System Random Access Memory
TRNG	True Random Number Generator

1 ST Introduction

1.1 ST Reference

The ST reference is "Security Target Lite of Security Chip GSEA01.x.D00 with IC Dedicated Software", version 1.31.

The Security Target claims a strict conformance to Eurosmart Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13th Jan. 2014, BSI-CC-PP-0084-2014.

1.2 TOE Reference

The TOE is named "Security Chip GSEA01.x.D00 with IC Dedicated Software". It consists of

- The Security Chip GSEA01
- IC Dedicated Software (Crypto Library, HAL, Flash Loader, IC Support Software)
- Guidance documents of TOE

In this document and the TOE guidance documents, the TOE name is abbreviated to "GSEA01".

1.3 TOE Overview

1.3.1 TOE Introduction

The TOE is an Embedded-Flash-based secure microcontroller platform with IC Dedicated Software. The applications can be executed securely and with good performance in this platform.

The TOE hardware has three bus masters: ARM SC300 security processor, DMAC and PKCC asymmetric coprocessor for big number calculation. All memory/register access requests from the bus masters are controlled by MMU. The TOE also has on-chip memories (RAMs, ROM and Flash), bus systems (SAHB, SAPB, APB), hardware peripherals including (T)DES and AES symmetric coprocessors, TRNG, CRC engine, communication interfaces (ISO/IEC 7816, SPI, I2C and GPIO), Timer and Watchdog. In addition, the TOE implements Metal Shielding and security sensors for the protection against physical and perturbation attacks.

The TOE software consists Service Software (Boot OS, Root0, and Analysis OS), Crypto Library, Flash Loader and HAL Library. Root0, Analysis OS and Flash Loader cannot be used in the field.

1.3.2 TOE Type and Usage

The TOE is a Security Integrated Circuit Platform for various operating systems and applications with high security requirements, including but not limited to secure element, secure storage, TPM, bankcard, eID and so on.

1.3.3 TOE Security Functionality

The TOE provides the following major security functionalities:

- ARM SC300 processor supporting unprivileged and privileged modes for access control
- CPU Monitor that further protects CPU
- SAHB with masking and integrity protection
- MMU supporting access control to memories and SFRs of the hardware components
- Memory encrypted and integrity protection for all embedded memories
- Register integrity protection
- AES with countermeasures against SCA and DFA attacks
- TDES with countermeasures against SCA and DFA attacks
- RSA cryptography with countermeasures against SCA and DFA attacks
- ECC cryptography with countermeasures against SCA and DFA attacks
- Galois/Counter Mode (GCM) and Galois Message and Authentication Code (GMAC) for AES
- TRNG conforming to class PTG.2 of AIS-20/31 [14]
- DRNG conforming to class DRG.3 of AIS-20/31 [14]
- Metal Shielding resisting physical attacks
- Security Sensors
- Test Mode, Analysis Mode and Flash Loader Mode protection

1.3.4 Security during Development and Production

The Security IC development and production life cycle is scheduled in phases, which are defined in the Protection Profile [PP].

At the end of Phase 1, which is out of the evaluation scope, the ES developer can optionally send the ES to Goodix, in a secure manner, to be programmed in Phase 4.

Phase 2 IC Development, Phase 3 IC Manufacturing as well as Phase 4 IC Packaging of this life cycle are in the evaluation scope.

In Phase 2 IC Development of GSEA01, access to sensitive design data of GSEA01 is restricted to who are involved in the development of the product.

In Phase 3 IC Manufacturing, the wafer of GSEA01 is produced and tested on wafers. The confidentiality and integrity of any design and configuration data in this phase will be ensured. This includes secure treatment and insertion of configuration data as well as manufacturing data, which are generated by Goodix.

In Phase 4 IC Packaging, the TOE is embedded into packages. The IC Dedicated Software is programmed into the Flash, the ES is loaded to the user Flash area and the Flash Loader is disabled. At the end of IC Packing phase, the TOE is delivered to the client in a secure manner.

1.3.5 TOE Configuration

The TOE configuration is identified below:

Name	Symbol	Description
Series	GSE	Series identifier of Goodix
IC version	A0	A: hardware base layer identifier 0: fixed metal masks identifier
Software version	1	software combination identifier, identifies the IC Dedicated Software
Hardware configuration	.x	identifier of the hardware configuration
Documentation version	D00	Identifier of the documentations

Table 1 TOE Configuration Identifier

Evaluated TOE is **GSEA01.**
Evaluated configuration of the TOE are **GSEA01.0** and **GSEA01.1**

The following configurations can be chosen by the client:

Configuration option	Configuration value (.x)	Configurable in the field
Interface select: SPI or I2c	- 0: SPI - 1: I2C	No

Table 2 TOE Configuration Options

1.3.6 Required non-TOE Hardware/Software/Firmware

The non-TOE hardware, software and firmware required by the TOE is the Security IC Embedded Software.

1.4 TOE Description

1.4.1 Physical scope of the TOE

The TOE GSEA01 consists of IC hardware, IC Dedicated Software and guidance documentation.

Category	Component	Version	Format
IC Hardware	IC	A0	Diced wafer
IC Dedicated Software	Boot OS	0101	binary in memory
	Root0		binary in memory
	Analysis OS		binary in memory
	HAL	0101	binary in memory
	Flash Loader	0101	binary in memory
	Crypto Library	0102	binary in memory
Documentation	GSEA0 Datasheet	[21]	.pdf file
	GSEA01 Preparative Procedures	[22]	.pdf file
	GSEA01 User Manual	[23]	.pdf file
	GSEA01 Security User Guidance Manual	[24]	.pdf file
Header File	HAL and Crypto Library Header File	0101	.zip package

Table 3 TOE physical scope

1.4.2 Logical scope of the TOE

The logical scope of TOE hardware is the functionality of the hardware components described in the section 1.4.2.1. The logical scope of the IC Dedicated Software is described in this the section 1.4.2.2.

1.4.2.1 Hardware Description

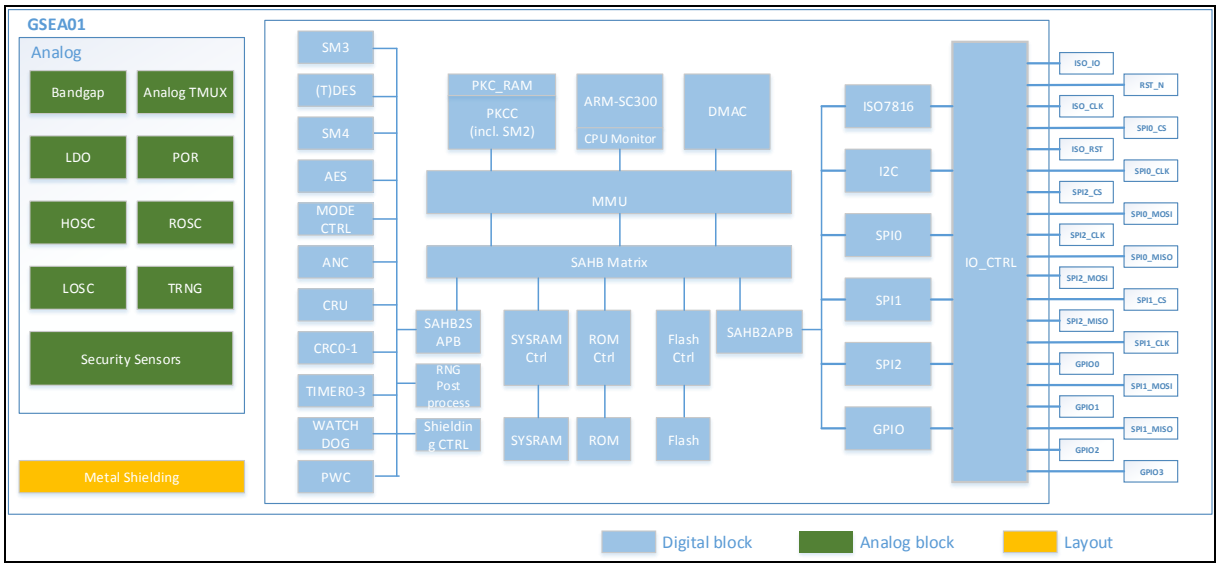

Figure 1 Block Diagram of the TOE

The ARM SC300 processor is a security enhanced version of the ARM Cortex M3. It includes the SC300 core and the Nested Vector Interrupt Controller (NVIC). The core implements the ARMv7-M architecture, which supports a subset of the Thumb instruction set. The SC300 Instruction set and Register interface follows the ARM official document: "ARM®v7-M Architecture Reference Manual, DDI 0403D (ID021310), www.arm.com" . The SC300 processor is monitored by CPU Monitor to ensure the correct execution of the program.

The DMAC module is in charge of managing data transfers between communication interfaces (i.e. ISO/IEC 7816 compliant interface, I2C or Serial Peripheral Interface (SPI)) and the on-chip memories. All the transmission is under access control of MMU.

The MMU implements memory and register access control. The access right of the code is controlled by the MMU, based on address of the code and the chip mode, while accessing different memory windows. Each window has its start and end addresses. The start and end addresses of three memory windows in the Flash memory can be managed by the ES running in CPU Privileged Level.

The On-chip memories in the TOE are ROM, Flash, SYSRAM and PKCRAM. The content is encrypted/decrypted by the hardware on the fly. All these memories are accessed through the bus system using SAHB bus, except that the PKCC can access PKCRAM directly with dedicated buses.

The bus system consists of SAHB, SAPB and APB, which implement high-performance data and address buses in the TOE. The SAHB2SAPB and SAHB2APB act as the bridges between SAHB and SAPB/APB.

(T)DES coprocessor provides 2-key or 3-key Triple-DES encryption and decryption with key lengths of 112 or 168 bits. AES coprocessor provides AES encryption and decryption with key lengths of 128, 192 or 256 bits. There is also a Galois Multiplier in AES coprocessor, which can be utilized by Crypto Library to realize GCM and GMAC.

The PKCC implements big number operations, including arithmetic operation, modular operation and logical operations, which can be utilized by the Crypto Library of IC Dedicated Software to

implement the asymmetric-key cryptographic functions with good performance.

The RNG generates true random numbers by harvesting the entropy from an analog noise source, which are compliant to AIS31[14].

In addition to the above mentioned cryptographic coprocessors, the TOE provide various peripherals as described below:

The Metal Shielding is designed to protect the TOE from physical attacks.

The security sensors are implemented to monitor the environmental conditions.

MODE_CTRL controls the chip mode transaction for different life cycle.

CRU is used to configure the clock frequency and provide reset signals for all blocks in the system. It also handles the error signals collected from all blocks.

WATCHDOG is a counter with time-out mechanism that can be utilized by the software to abort irregular program executions. TIMER0-3 are 4 identical general purpose timers.

IO_CTRL implemented a flexible programmable interconnect between I/O peripherals and I/O pins.

ANC provides configuration and trimming interface for Analog circuits.

PWC controls the power mode of TOE that can set the TOE to sleep and wake up for power saving.

The CRC0/1 support CRC-8/16/32 calculation with configurable generator polynomial, which can be used for data transmission and storage integrity.

SM3 and SM4 coprocessor can provide Chinese domestic cryptography algorithms, which is not in the evaluation scope.

Analog circuits, apart from aforementioned security sensors and random noise source, also provides the power regulator (Bandgap, LDO), clock and reset signal (HOSC, LOSC, ROSC, POR) and multiplexer for analog testing-only signals (Analog TMUX) for the TOE.

Note: the TOE implements the following functions, but these are not in the evaluation scope.

- Single DES cryptographic function
- Chinese domestic cryptographic functions: SM3, SM4
- CRC function

1.4.2.2 Software Description

The IC Dedicated Software can be used by the Embedded Software except those disabled at the end of the manufacturing phase. The IC Dedicated Software is composed of:

- IC Support Software
  - Boot OS
  - Root0 (disabled in the field)

  - Analysis OS
- HAL Library
- Crypto Library
- Flash loader Software (blocked in the field)

After chip powering-up or reset, the TOE starts executing Boot OS. Then Boot OS will jump to only one of Root0, Analysis OS, Flash loader and Security IC Embedded Software. This process can only be done once per power cycle or reset of the device. However, Root0 and Flash Loader are disabled at the end of the manufacturing phase. They cannot be accessed in the field.

Boot OS performs TOE initialization and manages the operation mode of TOE. Boot OS is not accessible for the Embedded Software.

The second part is Root0, which implements all functionality used for internal testing and validation on the TOE. This is not accessible by the Embedded Software after manufacturing.

The third part is Analysis OS, which provides functions for customer return chip analysis. Analysis OS is not accessible for the Embedded Software. The functions of the Analysis OS can only be accessed by Goodix.

The fourth part is HAL software, the drivers for the hardware, including communication interfaces' driver (ISO/IEC 7816, SPI, I2C, and GPIO), MMU, CRC, Timer, DMAC, Watchdog, self-test (Sensors, Metal Shielding), power management, Flash basic operations and memory operation for high level implementation.

The fifth part is Crypto Library. The Crypto Library provides following functionalities. *(Note: all the following items without remark implemented the countermeasures against side-channel and fault injection attacks)*

- AES with support of key length 128 bits, 192 bits and 256 bits in ECB/CBC/OFB/CFB/CTR and GCM mode that meets FIPS-197[9], NIST SP800-38A[1][2] and NIST SP800-38D[3]
- TDES with support of 2 key and 3 keys in ECB/CBC mode that meets the following: NIST SP 800-67[13] and NIST SP800-38A[1][2]
- RSA with supported key length from 512 bits up to 4096 bits with the step size of 64 bits meets the PKCS #1, v2.2[11] and FIPS PUB 186-4-2013[8]
  - RSA-plain and RSA-CRT both supported.
  - RSA decryption/encryption function (RSA encryption has no countermeasures against DPA or FI attack)
  - RSA signature/verification supported for padding-ready message
  - RSA key generation[8]
- ECC with supported key length from 128 bits up to 512 bits.
  - ECDSA (ECC over GF(p)) signature generation and verification with complying to ISO/IEC 14888 [15] , ANSI X9.62[17] and FIPS PUB 186-4[8]
  - ECDH (key exchange) without compressed point supports. meet the following: ISO/IEC 11770-3-2015 [16] , and ANSI X9.63 [20]
  - ECC over GF(p) key generation meets FIPS PUB 186-4[8]
- DRG.3 compliant DRNG (deterministic random number generator)
- Other functionalities: secure copy, secure memory compare, secure Exclusive-OR (XOR).

Note: the Crypto Library also implements APIs for SHA-1, SHA-2, HMAC, CRC, OSCCA SM2, SM3 SM4 and SM9. However, these APIs are not in the evaluation scope.

The last part, Flash Loader is disabled at the end of the manufacturing phase. It cannot be used in the field.

1.4.3 Interfaces of the TOE

1.4.3.1 Electrical interface

- 3 Serial Peripheral Interfaces (SPI)
- 1 ISO/IEC 7816 compliant interface
- 1 GPIO interface
- 1 I2C interface

1.4.3.2 Logical interface

As illustrated in Figure 2, the logical interface of GSEA01 is composed of the following:

- SC300 Instruction set and Register interface, which can be accessed by the Security IC Embedded Software as well as Security IC dedicated Software.
- Native Special Function Register Interface, which can be accessed by the Security IC Embedded Software as well as Security IC Dedicated Software.
- Special Function Registers, which can be accessed by the Security IC Dedicated Software
- Crypto Library and HAL Software APIs, which can be accessed by the Security IC Embedded Software

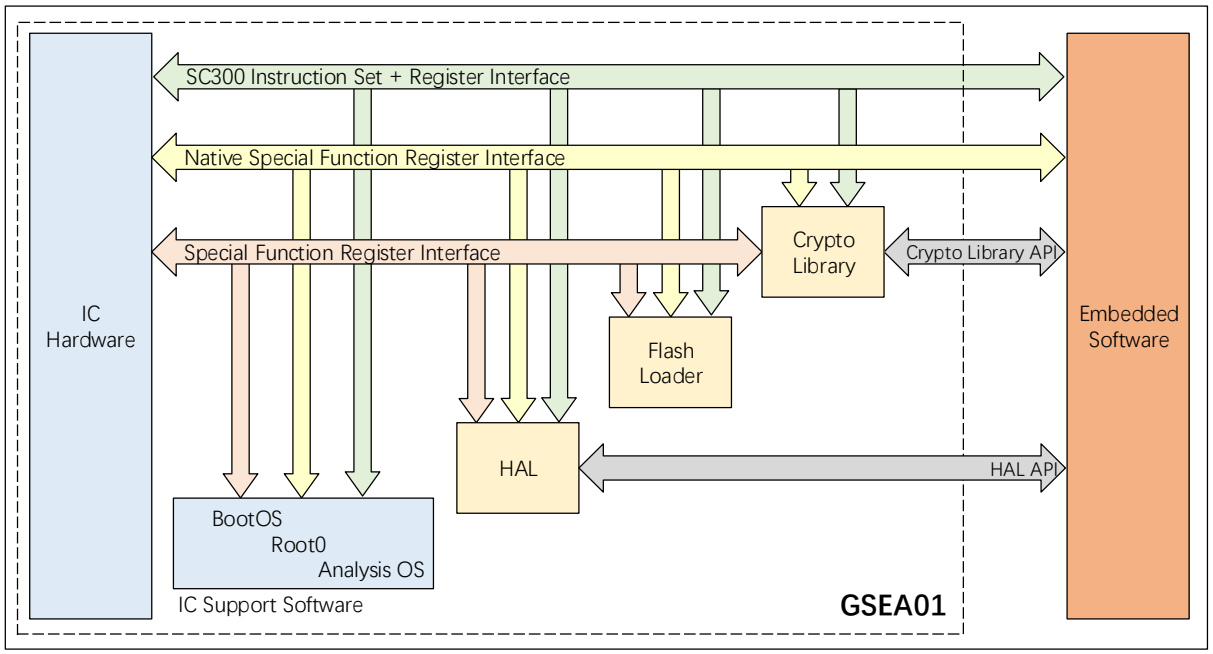

Figure 2 Logical Interface of TOE

NOTE: Analysis OS can only be used by Goodix through APDU interface

1.4.3.3 Physical interface

The chip surfaces are the interface of the TOE as well. This interface is monitored by the security sensors and protected by Metal Shielding. This interface could be exposed to environmental stress or physically manipulated by an attacker.

1.4.4 Form of Delivery

The IC hardware will be delivered together with IC dedicated software stored on chip memory to the Embedded Software developer. The delivery package will be sealed with secure tape. The delivery process will also be trackable with signature.

The user guidance and datasheet documents are delivered in electronic form to the user on request as encrypted and signed email attachment.

2 Conformance Claim

2.1 CC Conformance Claim

This Security Target (ST) and the TOE claim conformance to Common Criteria Version 3.1 Part 1[CC1], Part 2[CC2] and Part 3[CC3]:

- 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

Conformance of this ST is claimed for:

Common Criteria Part 2 extended and Common Criteria Part 3 conformant.

2.2 PP Claim

This Security Target is strict compliant to the Protection Profile [PP]:

- Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, registered and certified by Bundesamtfür Sicherheitinder Informationstechnik (BSI) under the reference BSI-PP-0084-2014.

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-0084-2014. 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-0084-2014, this additional functionality is added using the policy "P.Crypto-Service" (see Section 3.3 of this Security Target for details).

The following additional security functional requirements and cryptographic security services defined in [PP] appendix are claimed in this Security Target:

- Package: "TDES"
- Package: "AES"

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

2.3 Package Claim

The assurance level for the TOE is EAL5 augmented with the components ALC_DVS.2 and AVA_VAN.5.

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 [PP]. The operations done for the SFRs taken from [PP] are also clearly indicated.

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

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

3 Security Problem Definition

3.1 Description of Assets

The assets of the TOE are all assets described in section 3.1 of the BSI-PP-0084 [PP].

3.2 Description of Threats

The threats defined in section 3.2 of the Protection Profile [PP] are listed in Table below. They entirely apply to this Security Target.

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

Table 4 Threats defined in the Protection Profile

The threat T.RND explicitly includes both deficiencies of hardware (true) random numbers as well as deficiency of software (pseudo) random numbers provided by the Crypto Library.

The TOE shall also 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: the code or data in restricted memory areas and the restricted hardware resources.

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 security hardware based cryptographic services for the IC Embedded Software:

- TDES cryptographic service
- AES cryptographic service
- RSA cryptographic service
- ECC cryptographic service

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 5 lists these assumptions.

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

Table 5: Assumption according to [PP]

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE defined in section 4.1, section 7.2.1 and section 7.4 of the Protection Profile are listed in Table 6. They entirely apply to this Security.

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

Table 6 Security objectives for the TOE defined in the Protection Profile

The TOE provides register and memory access control function. The security objectives are listed in Table 7.

Name	Title
O.MEM-ACCESS	Memory Access Control
O.SFR-ACCESS	Special Function Register Access Control

Table 7 Security Objectives for the TOE added in this Security Target

The Crypto Library provides security functionality that results in the additional security objectives for the TOE listed in Table 8.

Name	Title
O.RSA	RSA encryption, decryption and RSA key pair generation
O.ECC	ECDSA signature generation & verification, ECC Diffie-Hellman key

	exchange, ECC key pair generation

Table 8 Security Objectives for the TOE related to Crypto Library added in this Security

The security objectives in Table 7 and Table 8 are defined as follows:

O.MEM-ACCESS Memory Access Control

The TOE controls access of the SC300 processor, DMAC and PKCC over the bus system to ROM, Flash, SYSRAM and PKCRAM. The control of access is enforced by restrictions based on system operation modes and CPU privilege levels.

O.SFR-ACCESS Special Function Register Access Control

The TOE controls access of the SC300 processor, DMAC and PKCC over the bus system to the Special Function Registers of the hardware components. The control of access is enforced by restrictions based on system operation modes and CPU privilege levels.

O.RSA RSA

The TOE includes functionality to provide encryption, decryption, signature creation, signature verification using the RSA algorithm, and RSA key pair generation.

O.ECC ECC

The TOE includes functionality to provide signature generation, signature verification, and Diffie-Hellman key exchange using the ECC over GF(p) algorithm, and generate ECC over GF(p) key pairs.

4.2 Security Objectives for the operational environment

The security objectives for the security IC Embedded Software development environment and the operational environment is defined in [PP] section 4.2 and 4.3. The table below lists the security objectives for the operational environment.

Name	Title
OE.Resp-Appl	Treatment of User Data of Composite TOE
OE.Process-Sec-IC	Protection during composite product manufacturing

Table 9 Security Objectives for the operational environment

4.3 Security Objectives Rational

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.

Assumption, Threat or Organizational Security Policy	**Security Objective**
A.Resp-Appl	OE.Resp-Appl
P.Process-TOE	O.Identification
A.Process-Sec-IC	OE.Process-Sec-IC
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

Table 10: Security Objectives versus Assumptions, Threats or Policies from [PP]

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 11 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.

Assumption, Threat or Organizational Security Policy	**Security Objective**
T.Unauthorized-Access	O.MEM-ACCESS O.SFR-ACCESS
P.Crypto-Service	O.TDES O.AES

	O.RSA O.ECC

Table 11: Addition Security Objectives versus Assumptions, Threats or Policies

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. According to O.SFR-ACCESS the TOE must restrict the access to the restricted hardware registers. Restrictions are controlled by the MMU and peripherals themselves. 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, O.RSA and O.ECC 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 assumption show that they do not contradict to the rationale already given in the Protection Profile 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 the CC Part1 [CC1]. These operations are used in [PP] 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 removed/changed words are crossed out as ~~crossed-out 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 **selection** operation is used to select one or more options provided by [PP] or CC in stating a requirement. Selections having been made are denoted as *underlined italic*.

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 after the slash.

Security functional requirements from the Protection Profile are applied to this Security Target. In compliance with Application Note 12 in the Protection Profile

6.1 Security Functional Requirements

6.1.1 Security Functional Requirements from the Protection Profile [PP]

Table 12 lists the security functional requirements for the TOE, which are defined in section 6.1 and in sections 7.4.1 and 7.4.2 of the Protection Profile [PP]. They entirely apply to this Security Target.

Name	Title
FRU_FLT.2	Limited fault tolerance

FPT_FLS.1	Failure with preservation of secure state
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FPT_PHP.3	Resistance to physical attack
FDP_ITT.1	Basic internal transfer protection
FPT_ITT.1	Basic internal TSF data transfer protection
FDP_IFC.1	Subset information flow control

Table 12 Security Functional Requirements from the Protection Profile [PP]

According to the application notes of FPT_FLS.1 and FPT_PHP.3 defined in [PP], the ST provide further information below.

Regarding Application Note 14 of the [PP], the Security Target shall describe the secure state for FPT_FLS.1.

FPT_FLS.1 Failure with preservation of secure state

Application note: When alarm is triggered, the TOE will reset or generate an interrupt for maintaining the secure state.

Regarding Application Note 15 of the [PP], the TOE does not generate audit data for FRU_FLT.2 and/or FPT_FLS.1.

Regarding Application Note 19 of the [PP], the Security Target shall describe the automatic response of the TOE for FPT_PHP.3.

FPT_PHP.3 Resistance to physical attack

Application note: If a physical attack is detected, an alarm is triggered and the chip will reset or generate an interrupt.

On some further Security Functional Requirements from the Protection Profile [PP] operations are made. Table 13 gives an overview on the Security Functional Requirement that were subject to refinement, selection, assignment and/or iteration operations in this Security Target

Name	**Title**
FAU_SAS.1	Audit storage
FDP_SDI.2	Stored data integrity monitoring and action
FDP_SDC.1	Stored data confidentiality
FCS_RNG.1:	Random number generation

•FCS_RNG.1/PTG.2	
FCS_COP.1: •FCS_COP.1/TDES •FCS_COP.1/AES	Cryptographic operation
FCS_CKM.4: •FCS_CKM.4/TDES •FCS_CKM.4/AES	Cryptographic key destruction

Table 13 Security Functional Requirements from [PP] with operations

- **FAU_SAS**

This Security Target performs selection and assignment operations on FAU_SAS.1 according to Application Note 17 in the Protection Profile [PP].

FAU_SAS.1 Audit Storage

Hierarchical to: No other components

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide *the test process before TOE Delivery with the capability to store the Initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software in the not changeable configuration page area and non-volatile memory.*

- **FDP_SDI**

This Security Target performs assignment operations on FDP_SDI.2 according to Application Note 18 in the Protection Profile [PP].

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* on all objects, based on the following attributes: *EDC value for the RAM, PKCRAM, ECC value for FLASH.*

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall *correct the content or trigger an alarm*" .

Application note: When detection of an EDC error, the TOE will be in reset or interrupt to CPU. When detection of the ECC error, the TOE will correct the data with ECC code when possible and interrupt to CPU

- **FDP_SDC**

This Security Target performs one assignment operation on FDP_SDC.1 according to Application Note 18 in the Protection Profile [PP].

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, RAM and PKCRAM.*

- **FCS_RNG**

This Security Target performs two iteration operations on FCS_RNG.1, which complies with section 8.1 in CC Part 1 [CC1]. It also performs selection and assignment operations on each iteration of FCS_RNG.1 according to Application Note 21 in the Protection Profile [PP] and [14].

FCS_RNG.1/PTG.2 Random Number Generation (Class PTG.2)

Hierarchical to: No other components

Dependencies: No dependencies

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

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

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

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

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

(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered externally. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

FCS_RNG.1.2/PTG.2 The TSF shall provide *numbers of 32 bits* that meet:

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

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

Note: FCS_RNG.1/DRG.3 is described in the next section since it is not from [PP].

- **FCS_COP.1**

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:

- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard (TDES)
- Elliptic Curve Cryptography (ECC)
- Rivest-Shamir-Adleman (RSA)

Note: The RSA and ECC iteration operations for FCS_COP.1 are described in the next section since they are not from [PP].

TDES Function

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

FCS_COP.1/TDES Cryptographic operation (TDES)

Hierarchical to: No other components.

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* in accordance with a specified cryptographic algorithm *TDES in ECB/CBC mode* and cryptographic key sizes *112 bits and 168 bits* that meet the following *NIST SP 800-67[13] and NIST SP800-38A[1][2]*

AES Function

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

FCS_COP.1/AES Cryptographic operation (AES)

Hierarchical to: No other components.

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* in accordance with a specified cryptographic algorithm *AES in ECB/CBC/OFB/CFB/CTR/GCM mode* and cryptographic key sizes *128 bit, 192 bit and 256 bit* that meet the following *FIPS-197[9], NIST SP800-38A[1][2] and NIST SP800-38D[3]*

- **FCS_CKM.4**

TDES key destruction

The TDES of the TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

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: *overwrite the key buffer and registers with random numbers* that meets the following: *none.*

AES key destruction

The AES of the TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4/AES Cryptographic key destruction (AES)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1/AES The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: *overwrite the key buffer and registers with random numbers* that meets the following: *none*

6.1.2 Security Functional Requirements added in this Security Target

List all the SFRs introduced by this Security Target.

Name	Title
FCS_RNG.1/DRG.3	Random number generation (DRG.3)
FCS_COP.1/RSA	Cryptographic operation (RSA)
FCS_COP.1/ECDSA	Cryptographic operation (ECDSA)
FCS_COP.1/ECDH	Cryptographic operation (ECDH)
FCS_CKM.1/RSA	Cryptographic key generation (RSA)
FCS_CKM.1/ECC	Cryptographic key generation (ECC)
FCS_CKM.4/CL	Cryptographic key destruction (CL)
FDP_ACC.1	Subset access control-memory access control
FDP_ACF.1	Security attribute based access control-memory access control
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of management functions

Table 14 Security Functional Requirements added in this Security Target

6.1.2.1 Random Number Generator

- **FCS_RNG.1**

The DRNG of the TOE shall meet the requirement "Random Number Generation (FCS_RNG.1)" as specified below.

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* random number generator that implements:

(DRG.3.1) If initialized with a random seed using a PTRNG of class PTG.2 as random source, the internal state of the RNG shall have at least 112 bits entropy.

Note: The seed is provided by a certified PTG.2 physical TRNG with guaranteed 7.976 bit of entropy per byte.

(DRG.3.2) The RNG provides forward secrecy.

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

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

(DRG.3.4) The RNG, initialized with a random seed from a PTRNG of class PTG.2, generates output for which 2^{48} strings of bit length 128 are mutually different with probability at least $1-2^{-24}$.

(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.

6.1.2.2 Cryptographic Functions

- **FCS_COP.1**

RSA Function

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 (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 management], FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/RSA The TSF shall perform *encryption, decryption* in accordance with a specified cryptographic algorithm *Rivest-Shamir-Adleman (RSA)* and cryptographic key sizes from *512 to 4096 bits with the step size of 64 bits* that meet the following: *PKCS #1, v2.2[11] and FIPS PUB 186-4-2013[8]*

ECDSA Function

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

FCS_COP.1/ECDSA Cryptographic operation (ECDSA)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ECDSA The TSF shall perform *signature generation* and *signature verification* in accordance with a specified cryptographic algorithm *ECDSA* and cryptographic key sizes *128 bits up to 512 bits* that meet the following *ISO/IEC 14888 [15] , ANSI X9.63[17] and FIPS PUB 186-4[8].*

ECDH Function

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

FCS_COP.1/ECDH Cryptographic operation (ECDH)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ECDH The TSF shall perform *Diffie-Hellman Key Exchange* in accordance with a specified cryptographic algorithm *ECC over GF(p)* and cryptographic key sizes *128 bits up to 512 bits* that meet the following: *ISO/IEC 11770-3-2015[16] and ANXI X9.63[20].*

Application Note: The security functionality does not provide the complete key exchange procedure, but only the point multiplication which is used for the multiplication of the private key with the communication partner' s public key. Therefore, this function can be used as part of a Diffie-Hellman key exchange as well pure point multiplication

- **FCS_CKM.1**

RSA key generation

The RSA key generation function shall meet the requirement "Cryptographic key generation (FCS_CKM.1)"

FCS_CKM.1/RSA Cryptographic key generation (RSA)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/RSA The TSF shall perform *key generation* in accordance with *RSA* cryptographic key sizes *512 bits up to 4096 bits with the step size of 64 bits* that meet the following: *PKCS #1[11] and FIPS PUB 186-4[8].*

Note: Although FIPS PUB 186-4 key generation only allows the key size of 1024, 2048 and 3072 bits, the TOE can support key generation with various size that followed the generation method in FIPS PUB 186-4.

Elliptic Curve key generation

The ECC key generation function shall meet the requirement "Cryptographic key generation (FCS_CKM.1)"

FCS_CKM.1/ECC Cryptographic key generation (ECC)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1/ECC The TSF shall perform *key generation* in accordance with *Elliptic Curve EC* cryptographic key sizes *128 bits up to 512 bits* that meet the following *FIPS PUB 186-4[8].*

- **FCS_CKM.4**

Crypto Library key destruction

The Crypto Library key destruction function shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)"

FCS_CKM.4/CL Cryptographic key destruction (CL)

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/CL The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method*: overwrite the key buffer and registers with random numbers or zeros* that meets the following: none.

Application Note: The TOE provides the Security IC Embedded Software with Crypto Library calls to perform various cryptographic algorithms that involve keys (e.g., RSA, ECDSA, ECDH, etc.). Through the parameters of the Crypto Library calls, the Security IC Embedded Software provides keys for the cryptographic algorithms. To perform its cryptographic algorithms Crypto Library copies these keys, or a transformation thereof, to the working-buffer (supplied by the Security IC Embedded Software) and/or the memory/special function registers of the TOE. Crypto Library will overwrite these keys before returning control to the Security IC Embedded

Software.

Note: Clearing of keys that are provided by the Security IC Embedded Software to the Crypto Library is the responsibility of the Security IC Embedded Software.

6.1.2.3 Memory and Register Access Control

The security functional requirements in Table 14 address the Memory and Register Access Control Policy of the TOE. It is enforced by restriction based on the following system operation modes:

- Boot Mode
- Test Mode
- Analysis Mode
- FlashLoader Mode
- Application Mode

and the following CPU privilege levels:

- Privileged
- Unprivileged

The Memory and Register Access Control Policy controls access to two groups of objects, which are *objects for access control to memories* and *objects for access control to Special Function Registers*. The objects of each group are detailed below.

Objects for access control to memories are as follows:

- Basic Windows:

  Default address windows, which do not overlap in their address ranges with each other. All address ranges are fixed in hardware.

- Application Windows:

  Software-controlled address windows, which must overlap with Basic Windows. They can be configured by application software as an option.

Objects for access control to Special Function Registers are as follows:

- The Special Function Registers (SFR) of hardware components are composed of:
  - SFR_SPI: SFRs of the SPI communication interface
  - SFR_I2C: SFRs of the I2C communication interface
  - SFR_ISO7816: SFRs of the ISO7816 UART communication interface
  - SFR_GPIO: SFRs of the Port IO communication interface

- SFR_IOCTRL: SFRs of IO controller
- SFR_CRC: SFRs of CRC co-processer 0/1
- SFR_TIMER: SFRs of Timer 0/1/2/3
- SFR_WDG: SFRs of Watchdog Timer
- SFR_DMAC: SFRs of DMA controller
- SFR_MMU: SFRs of Memory Management Unit

The *objects for access control to memories* are controlled against access rights in read (r) and write (w) and for CPU access also against access rights in execute (e). The *objects for access control to Special Function Registers* are controlled against access rights in read (r) and write (w).

The Memory and Register Access Control Policy is applied to the following *subjects of access control to memories and Special Function Registers*.

Subjects of access control to memories and Special Function Registers are these:

- CPU access over the bus system:

  It accesses via 6 types of software component types as follows:

  - BootOS: executed in Boot Mode
  - Root0: executed Test Mode
  - AnalysisOS: executed in Analysis Mode
  - FlashLoader: executed in FlashLoader Mode
  - Application software in CPU Privileged level: executed in Application Mode with CPU in Privileged level
  - Application software in CPU Unprivileged level: executed in Application Mode with CPU in Unprivileged level
- DMA controller access over the bus system:

  It accesses in the system operation mode in which the actual CPU runs.
- PKCC co-processor access over the bus system:

  It accesses in the system operation mode in which the actual CPU runs.

Note: Detailed information of all subjects and all objects for access control to memories and Special Function Registers is given in Datasheet [21].

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 and Register Access Control Policy* on *all subjects, all objects for access control to memories and Special Function Registers, and all operations on the objects for access control to memories and Special Function Registers.*

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 and Register Access Control Policy* to objects based on the following*: the subjects access the objects according to the following memory and register access control rules.*

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 access permission control information of the memory range or register address of the objects during the access to determine whether the accesses can be granted to perform the operation by the subject.*

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

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

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

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 security roles

FMT_MSA.3.1 The TSF shall enforce the *Memory Access Control Policy* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow *no subject* to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the *Memory and Register Access Control Policy* to restrict the ability to *modify* the security attributes *to the application software running in CPU privileged level*.

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

- *The application software in CPU Privileged level shall be able to call the configuration in HAL to configure the MMU*
- *Change in the CPU privilege level*

6.2 Security Assurance Requirements

The evaluation assurance level is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5. In the following Table 15, the security assurance requirements are given.

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

Table 15: Assurance components

6.3 Security Requirements Rationale

6.3.1 Rationale for 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, FMT_MSA.1. FMT_MSA.3, FMT_SMF.1, FCS_COP.1, FCS_CKM.1 and FCS_CKM.4 are defined in the following description:

Objective	**TOE Security Functional Requirements**
O.TDES	- FCS_COP.1/TDES “Cryptographic operation” - FCS_CKM.4/TDES “Cryptographic key destruction”
O.AES	- FCS_COP.1/AES “Cryptographic operation” - FCS_CKM.4/AES “Cryptographic key destruction”
O.RSA	- FCS_CKM.1/RSA “Cryptographic key generation”

	- FCS_COP.1/RSA "Cryptographic operation" - FCS_CKM.4/CL "Cryptographic key destruction"
O.ECC	- FCS_CKM.1/ECC "Cryptographic key generation" - FCS_COP.1/ECDSA "Cryptographic operation" - FCS_COP.1/ECDH "Cryptographic operation" - FCS_CKM.4/CL "Cryptographic key destruction"
O.MEM-ACCESS O.SFR-ACCESS	- FDP_ACC.1 "Subset access control" - FDP_ACF.1 "Security attribute based access control" - FMT_MSA.1 "Management of security attributes" - FMT_MSA.3 "Static attribute initialization" - FMT_SMF.1 "Specification of management functions"

Table 16: Rational for Additional Security Functional Requirements in the ST

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.AES, O.ECC and O.RSA. Therefore, FCS_COP.1 is suitable to meet the security objective.

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 and Register Access Control Policy" exactly require the implementation of an area/address based memory and register access control as required by O.MEM-ACCESS and O.SFR-ACCESS. The related TOE security functional requirements FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3 and FMT_SMF.1 cover these security objectives. 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 [CC2] user data protection of chapter 11 which are not refined by the [PP].

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, FMT_MSA.1. FMT_MSA.3, FMT_SMF.1, FCS_COP.1 and FDP_SDI.2 is defined in the following description.

Security Functional Requirement	**Dependencies**	**Fulfilled by security requirements**
FCS_COP.1/TDES	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	No, see comment 1
	FCS_CKM.4	FCS_CKM.4/TDES
FCS_COP.1/AES	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	No, see comment 1
	FCS_CKM.4	FCS_CKM.4/AES
FCS_COP.1/RSA	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1/RSA (for keys if generated by this SFR) otherwise see comment 1
	FCS_CKM.4	FCS_CKM.4/CL
FCS_CKM.1/RSA	FCS_CKM.2 or FCS_COP.1	Yes,FCS_COP.1/RSA
	FCS_CKM.4	FCS_CKM.4/CL
FCS_COP.1/ECDSA	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1/ECC (for keys if generated by this SFR) otherwise see comment 1
	FCS_CKM.4	FCS_CKM.4/CL

FCS_COP.1/ECDH	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1/ECC (for keys if generated by this SFR) otherwise see comment 1
	FCS_CKM.4	FCS_CKM.4/CL
FCS_CKM.1/ECC	FCS_CKM.2 or FCS_COP.1	Yes,FCS_COP.1/ECDSA, FCS_COP.1/ECDH
	FCS_CKM.4	FCS_CKM.4/CL
FDP_ACC.1	FDP_ACF.1	Yes, FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes, FDP_ACC.1 Yes, FMT_MSA.3
FMT_MSA.3	FMT_MSA.1	Yes, FMT_MSA.1
	FMT_SMR.1	No, see comment 2
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Yes, FDP_ACC.1
	FMT_SMR.1	No, see comment 2
	FMT_SMF.1	Yes, FMT_SMF.1
FMT_SMF.1	None	N/A
FDP_SDI.2	None	N/A

Table 17: Dependency for cryptographic operation requirement

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]

For the security functional requirements FCS_COP.1/TDES and FCS_COP.1/AES, the respective dependencies FCS_CKM.1 and FDP_ITC.1 or FDP_ITC.2 have to be fulfilled by the environment. That means, that the environment shall meet the requirements FCS_CKM.1 or 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, FCS_COP.1/ECDSA, and FCS_COP.1/ECDH, the respective dependencies FDP_ITC.1 or FDP_ITC.2 have to be fulfilled by the environment if the key is not generated by FCS_CKM.1/RSA or FCS_CKM.1/ECC.

End of Comment

Comment 2:

The dependency FMT_SMR.1 introduced by the two components FMT_MSA.1 and FMT_MSA.3 is not considered in this Security Target. Because the security attributes shall be managed by Security IC Embedded Software based on which the Security IC Embedded Software shall be capable to maintain roles and assign users to roles appropriate to its needs.

End of Comment

6.3.3 Rationale for Security 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 16: Assurance components the different assurance levels are shown as well as the augmentations. The augmentations are in compliance with the Protection Profile.

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.

6.3.4 Security Requirements are internally Consistent

For this chapter [PP] section 6.3.4 can be applied completely.

In addition to the discussion in section 6.3 of [PP] the security functional requirement FCS_COP.1 is introduced. The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms implemented according to the security functional requirement FCS_COP.1. Therefore, these security functional requirements support the secure implementation and operation of FCS_COP.1.

The implemented level concept represents the area based memory access protection enforced by the TOE or MMU. As an attacker could attempt to manipulate the privilege level definition as defined and present in the TOE, the functional requirement FDP_ACC.1 and the related other requirements have to be protected themselves. The security functional requirements required to meet the security objectives O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.SFR-ACCESS and O.MEM-ACCESS also protect the area based memory access control function implemented according to the security functional requirement described in the security functional requirement FDP_ACC.1 with reference to the Memory Access Control Policy and details given in FDP_ACF.1. Therefore, those security functional requirements support the secure implementation and operation of FDP_ACF.1 with its dependent security functional requirements.

The requirement FDP_SDI.2.1 allows detection of integrity 1 errors of data stored in memory. FDP_SDI.2.2 in addition allows correction of one-bit errors or taking further action. Both meet the security objective O.Malfunction. The requirements FRU_FLT.2, FPT_FLS.1, and FDP_ACC.1 which also meet this objective are independent from FDP_SDI.2 since they deal with the observation of the correct operation of the TOE and not with the memory content directly.

In order to support Capability and availability of the Loader the security functional requirements FMT_LIM.1 [Loader] and FMT_LIM.2 [Loader] are introduced. The security functional requirements required to meet the security objectives Capability and availability of the Loader (O.Cap_Avail_Loader) also protect the Capability and availability of the Loader implemented according to the following security functional requirements.

The requirements FMT_LIM.1/Loader in conjunction with FMT_LIM.2/Loader limits its capability and

availability, allowing for non-overlapping loading of user data and protecting the TSF against misuse of the Loader for attacks against the TSF. The requirements FMT_LIM.2/Loader is the easiest variant of Loader functionality relying on secure boot loading procedures in secure environment before TOE delivery to the assigned customer and preventing deploying the Loader of the TOE after blocking of Loader for TOE delivery to the client.

7 TOE Summary Specification

7.1 Security Functionality of the TOE

The TOE Security Functionality (TSF) is composed of Security Features (SF) and Security Mechanisms (SM). They together fulfill the security functional requirements (SFR) for the TOE.

The Security Functions and Security Mechanisms related to SFRs of the TOE are summarized in Table 18 and described in section 7.2 and section 7.3.

Security Function / Security Mechanism	Name	Fulfilled SFR
SF.RNG	Random Number Generator	FCS_RNG.1/PTG.2 FCS_RNG.1/DRG.3
SF.TDES	TDES coprocessor and TDES function library	FCS_COP.1/TDES FCS_CKM.4/TDES
SF.AES	AES coprocessor and AES function library	FCS_COP.1/AES FCS_CKM.4/AES
SF.RSA	PKC coprocessor and RSA security function library and RSA Key Generator	FCS_COP.1/RSA FCS_CKM.1/RSA FCS_CKM.4/CL
SF.ECC	Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Diffie-Hellman (ECDH) and ECC Key Generator	FCS_COP.1/ECDSA FCS_COP.1/ECDH FCS_CKM.1/ECC FCS_CKM.4/CL
SF.OPC	Operating condition monitoring	FRU_FLT.2 FPT_FLS.1
SF.SST	Sensor self-test	
SF.SHD	Metal shielding	FPT_PHP.3 FDP_SDC.1 FDP_SDI.2
SM.MED	Memory encryption	
SM.ASC	Memory address scrambling	
SM.MIT	Memory integrity check	
SM.DIT	Data integrity check	
SM.BBL	Bus data blinding	FPT_PHP.3 FDP_ITT.1 FPT_ITT.1 FDP_IFC.1
SM.MSK	crypto algorithm blinding countermeasure	
SM.DMY	crypto algorithm dummy operation	
SSM.MSK	crypto algorithm blinding countermeasure RSA/ECC	
SSM.FLA	Flash loader entry protection	FMT_LIM.1 FMT_LIM.2
SSM.TMP	Test Mode entry protection	
SF.STO	Secure storage	FAU_SAS.1

SF.MAC	Memory Access Control	FDP_ACC.1 FDP_ACF.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1
SF.RAC	Register Access Control	

Table 18 Security Functions/Mechanisms of the TOE

7.2 Security Functions

7.2.1 SF.RNG

SF.RNG provides random number generation functions: TRNG and DRNG.

The TOE implements the physical hardware True Random Number Generator (TRNG) which conforms to class PTG.2 of the pre-defined RNG classes in AIS 20/31[14]. TRNG fulfills the total failure test and online test requirements defined in AIS-20/31[14]. It is suitable for generation of signature key pairs, generation of session keys for symmetric encryption mechanisms, random padding bits, zero-knowledge proofs, seeds for Deterministic Random Number Generation (DRNG).

The Crypto Library also implements the Deterministic Random Number Generation (DRNG) with seeds generated by the TRNG. DRNG conforms to DRG.3 class of the pre-defined RNG classes AIS-20/31 [14].

7.2.2 SF.TDES

By utilizing the DES/TDES Crypto coprocessor, Crypto Library provides security service for TDES supporting 2 key (112 bits) and 3 keys (168 bits) in Electronic Code Book (ECB) mode, Cipher Block Chaining (CBC) mode that meets the following NIST SP 800-67[13] and NIST SP800-38A[1][2] standards. It resists against Side Channel Analysis and Fault Attack.

7.2.3 SF.AES

By utilizing the AES Crypto coprocessor, Crypto Library provides security service for AES supporting 128-bit, 192-bit and 256-bit key in Electronic Code Book (ECB) mode, Cipher Block Chaining (CBC) mode, Output Feedback (OFB) mode, Cipher Feedback (CFB) mode, Counter (CTR) mode and Galois/Counter mode (GCM) that meets FIPS-197[9], NIST SP800-38A[1][2] and NIST SP800-38D[3] standards. It resists against Side Channel Analysis and Fault Attack.

7.2.4 SF.RSA

By utilizing the PKCC Crypto coprocessor, Crypto Library provides RSA security services that implement the RSA algorithm and the RSA-CRT algorithm for key generation, data encryption, decryption, signature and verification that meets PKCS #1, v2.2[11] and FIPS PUB 186-4-2013[8] standards. The supported key length is from 512 bits up to 4096 bits with the step size of 64 bits. It resists against Side Channel Analysis and Fault Attack.

Crypto Library also provides RSA key generation function with RSA cryptographic key sizes 512 bits up to 4096 bits with the step size of 64 bits, which conforms to FIPS PUB 186-4 [8] standard. It resists against Side Channel Analysis and Fault Attack.

7.2.5 SF.ECC

By utilizing the PKCC Crypto coprocessor, Crypto Library provides ECDSA (ECC over GF(p)) signature generation and verification services that meets ISO/IEC 14888 [15], ANSI X9.62[17] and FIPS PUB 186-4[8] standards, and the point multiplication function for ECDH (key exchange) without compressed point supports that meets ISO/IEC 11770-3-2015 [16] , and ANSI X9.63 [20]. The supported key length is from 128 bits up to 512 bits. It resists against Side Channel Analysis and Fault Attack.

Crypto Library also provides ECC over GF(p) key generation with Elliptic Curve EC cryptographic key sizes 128 bits up to 512 bits, which conforms to FIPS PUB 186-4[8] standard. It resists against Side Channel Analysis and Fault Attack.

7.2.6 SF.OPC

SF.OPC controls operating conditions of the TOE by security functionality that actively monitors certain electrical parameters. Such security functionality raises an error message whenever a monitored parameter drops out of its valid range. In addition, exposure of the device to laser is explicitly controlled by security functionality that senses abnormal Near Infrared (NIR) laser over its whole surface, raising an error message when detected.

7.2.7 SF.SST

The TOE implements sensor self-test function, which can be called by user to check whether the sensors can correctly send alarm signals.

7.2.8 SF.SHD

The TOE is protected from physical probing and physical manipulation of its hardware, its IC Dedicated Software, its TSF data and the Security IC Embedded Software stored to its Flash memory including user data of the Composite TOE. This is achieved by appropriate shielding techniques for all elements in the physical design of the TOE.

7.2.9 SF.STO

TOE provides test procedure to store initialization data or pre-personalization data before TOE delivery.

7.2.10 SF.MAC

SF.MAC controls access to the memories of the TOE. This is done based on MMU in the bus system that block certain access ports for particular memories.

7.2.11 SF.RAC

SF.RAC controls access to the Special Function Registers of the TOE. This is done based on physical restrictions in the bus system and the access control logic inside each peripherals.

7.3 Security Mechanisms

7.3.1 SM.MED

The data stored in memories is encrypted by the hardware to protect the confidentiality of the data from physical probing or observation on the memories.

7.3.2 SM.ASC

The data stored in memories is disarranged by the hardware to protect the confidentiality of the data from physical probing or observation on the memories.

7.3.3 SM.MIT

The integrity of the data stored in memories is checked by the hardware to protect the integrity of the data from manipulation.

7.3.4 SM.DIT

The integrity of the data transmitting on the SAHB and SAPB, the data stored in security relevant registers and the security relevant signals is checked by the hardware to protect data integrity.

7.3.5 SM.BBL

The data on SAHB and SAPB are masked with random numbers to prevent data leakage.

7.3.6 SM.MSK

Masking scheme is implemented to protect coprocessors from side channel attack.

7.3.7 SM.DMY

Dummy operations are performed in coprocessors to hide sensitive operations while performing cryptographic operations.

7.3.8 SSM.MSK

Masking scheme is implemented in Crypto Library to protect itself from side channel attack.

7.3.9 SSM.FLA

The Flash Loader is disabled at the end of the manufacturing phase. The TOE performs redundant operations to prevent re-enabling the loader function with life-cycle status checking.

7.3.10 SSM.TMP

The Test Mode function is disabled at the end of the manufacturing phase. The TOE performs redundant operations to prevent re-enabling the Test Mode function with life-cycle status checking.

8 Bibliography

8.1 Standards

[CC1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001
[CC2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002
[CC3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003
[PP]	Security IC Platform Protection Profile, Version 1.0, 13th Jan. 2014, registered and certified by Bundesamtfür Sicherheitinder Informationstechnik (BSI) under the reference BSI-PP-0084
[1]	NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation, National Institute of Standards and Technology, Edition 2001
[2]	Addendum to NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, National Institute of Standards and Technology, October 2010
[3]	NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007, Morris Dworkin, National Institute of Standards and Technology
[4]	NIST SP 800-90A, Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015, Elaine Barker and John Kelsey, National Institute of Standards and Technology
[5]	ISO/IEC 9797-1: 2011 Information technology -- Security techniques – Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
[6]	FIPS PUB 81-1980: DES modes of operation, Federal Information Processing Standards Publication, December 2nd, 1980, US Department of Commerce/National Institute of Standards and Technology
[7]	FIPS PUB 180-4-2011: Secure Hash Standard, Federal Information Processing Standards Publication, February 2011, US Department of Commerce/National Institute of Standards and Technology
[8]	FIPS PUB 186-4-2013: Digital Signature Standard, Federal Information Processing Standards Publication, 2013, July, National Institute of Standards and Technology
[9]	FIPS PUB 197-2001: ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197, November 26, 2001, U.S. Department of Commerce/National Institute of Standards and Technology
[10]	ANSI X9.62-1998: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), September 1998, American National Standards Institute
[11]	PKCS#1 v2.2: RSA Cryptography Standard, October 2012, RSA Laboratories
[12]	PKCS#1 v1.5: RSA Encryption, March 1998, RSA Laboratories
[13]	NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, National Institute of Standards and Technology, Revised January 2012

[14]	Anwendungshinweise und Interpretationen zum Schema (AIS), Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[15]	ISO/IEC 14888-3-2015: Information technology – Security techniques – Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms, 2016
[16]	ISO/IEC 11770-3-2015: Information technology – Security techniques – Key management -- Part 3: Mechanisms using asymmetric techniques, 2015
[17]	ANSI X9.62: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), September 1998, American National Standards Institute
[18]	ISO/IEC 15946-1-2008: Information technology – Security techniques Cryptographic techniques based on elliptic curves – Part 1: General, 2008
[19]	JIL-ATT-SC: Attack Methods for Smartcards and Similar Devices, Joint Interpretation Library, Version 1.5, February 2009
[20]	ANSI X9.63: Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, December 2011, American National Standards Institute

8.2 Developer Documents

[21]	GSEA0 Datasheet, Version 1.7, 30 Dec 2021, Shenzhen Goodix Technology Co., Ltd.
[22]	GSEA01 Preparative Procedures, Version 1.1, 18 Jan 2022, Shenzhen Goodix Technology Co., Ltd.
[23]	GSEA01 User Manual, Version 1.0, 11 Jan 2022, Shenzhen Goodix Technology Co., Ltd.
[24]	GSEA01 Security User Guidance Manual, Version 1.11, 18 Jan 2022, Shenzhen Goodix Technology Co., Ltd.

9 Legal and Contact Information

Trademarks and Permissions

GOODiX and other Goodix trademarks are trademarks of Shenzhen Goodix Technology Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Disclaimer

Information contained in this document is intended for your convenience only and is subject to change without prior notice. It is your responsibility to ensure its application complies with technical specifications.

Shenzhen Goodix Technology Co., Ltd. (hereafter referred to as "Goodix") makes no representation or guarantee for this information, express or implied, oral or written, statutory or otherwise, including but not limited to representation or guarantee for its application, quality, performance, merchantability or fitness for a particular purpose. Goodix shall assume no responsibility for this information and relevant consequences arising out of the use of such information.

Without written consent of Goodix, it is prohibited to use Goodix products as critical components in any life support system. Under the protection of Goodix intellectual property rights, no license may be transferred implicitly or by any other means.

Shenzhen Goodix Technology Co., Ltd.
Headquarters: 2F. & 13F., Tower B, Tengfei Industrial Building, Futian Free Trade Zone, Shenzhen, China
TEL: +86-755-33338828 FAX: +86-755-33338099
Website: http://www.goodix.com