# THD89 Secure Microcontroller with Crypto Library

# Security Target Lite

Version 1.0

Beijing Tongfang Microelectronics Co.,Ltd.
2018 – 08

Revision History

| No. | Version | Date | Change | By |
|---|---|---|---|---|
| 1 | 1.0 | Aug. 22th.2018 | Create | Xingchen Li |

# Contents

# 1. ST Introduction

This Security Target (ST) is built upon the Security IC Platform Protection Profile with Augmentation Packages [1], registered and Certified by BundesamtfürSicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014.

This chapter presents the ST reference, the reference for the Target of Evaluation (TOE), a TOE overview description and a description of the logical and physical scope of the TOE.

## 1.1. ST and TOE reference

**Table 1 Description of ST reference and TOE reference**

| | |
|---|---|
| ST reference: | THD89 Secure Microcontroller with Crypto Library Security Target Lite, version 1.0, August 2018 |
| TOE reference: | THD89 Secure Microcontroller version 1.0 with Crypto Library version 1.01 |

## 1.2. TOE overview

The TOE is a secure microcontroller with crypto library suitable for instance to support ID cards, Banking cards, ePassport applications, etc.

The TOE consists of hardware and IC dedicated software. The hardware is based on a 32-bit CPU with ROM (Non-Volatile Read-Only Memory), NVM (Non-volatile Programmable Memory) and RAM (Volatile Memory). The hardware of the TOE also incorporates communication peripherals and cryptographic coprocessors for execution and acceleration of symmetric and asymmetric cryptographic algorithms. The IC dedicated software consists of boot code and a library of cryptographic services.

The TOE supports the following communication interfaces:

- ISO/IEC 7816 contact interface.
- ISO/IEC 14443 contactless interface
- SPI interface
- I2C interface

The TOE is delivered to a composite product manufacturer. The security IC embedded software is developed by the composite product manufacturer. The security IC embedded software is not part of the TOE.

The TOE has been designed to provide a platform for Security IC Embedded Software which ensures that the critical user data of the Composite TOE are stored and processed in a secure way. To this end the TOE has the following security features:

- Hardware coprocessor for DES/TDES
- True Random Number Generator
- Hardware for RSA support
- Protection against power analysis,

- Protection against physical attacks,
- Protection against perturbation attacks,
- Software library with cryptographic services for DES/TDES, RSA and TRNG.

## 1.3. TOE description

This section presents the physical and logical scope of the TOE.

### 1.3.1. Physical architecture

The main functional blocks of the TOE hardware is depicted below.

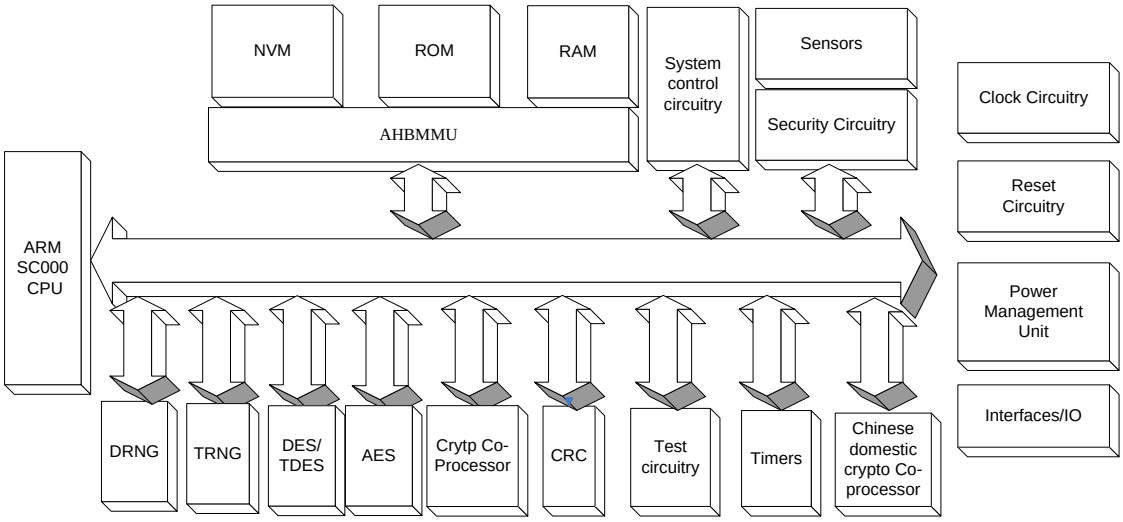


**Figure 1 The block diagram of the TOE hardware**

The hardware of the TOE has the following components:

- ARMSC000 CPU
- NVM (192kB)
- ROM (384kB)
- RAM (14kB)
- AHBMMU
- Interfaces I/O
    - ISO/IEC 14443 contactless interface
    - ISO/IEC 7816 contact interface
    - SPI interface
    - I2C interface
- True Random Number Generator
- Deterministic Random Number Generator
- DES/TDES Co-Processor
- AES Co-Processor
- Hardware Crypto Co-Processor for RSA support
- CRC Co-Processor

- Chinese domestic crypto Co-Processor
- System control circuitry
- Test circuitry
- Timers
- Security Circuitry
- Sensors
    - Voltage sensor
    - Glitch sensor
    - Frequency sensor
    - High frequency filter
    - Temperature sensor
    - Light sensor
- Power Management Circuitry
- Clock circuitry
- Reset circuitry

The AHBMMU is a bus component which also provides user controllable bus masking.

The TOE contains the following functions, but then security of these functions are not claimed.

- Chinese domestic crypto Co-Processor
- AES Co-Processor
- Deterministic Random Number Generator.
- CRC Co-Processor

ISO/IEC 14443 contactless interface and ISO/IEC 7816 contact interface are the interfaces available for the user. SPI and I2C interfaces are not valid to the user for this TOE.

### 1.3.2. Logical Scope

The TOE distinguishes three modes:

1. Boot mode
2. Test mode
3. Normal mode

Boot mode is the initial mode after the chip is powered up. This mode is not available to the Security IC embedded software. It can either switch to test mode under the purpose of testing or initialization, or switch to normal mode.

Test mode is also not available for the Security IC embedded software. It is utilized to perform the TOE testing before the TOE is delivered to the end user. Test mode is strictly protected by a combination of hardware and software security features.

Normal mode is utilized for the end user, Security IC embedded software can be executed under this mode. Normal mode can not switch back to boot mode and test mode.

The TOE provides ROM for executing the boot code and crypto library code, NVM for the code and data access, and RAM for the temporary data access.

The Memory management unit is performed by the AHBMMU, and it also performs the access control of boot mode, test mode and normal mode.

There are two communication interfaces available, including ISO/IEC 14443 contactless interface, ISO/IEC 7816 contact interface. SPI interface and I2C interface are not available to the user.

The TOE provides the system control functions to handle the reset, clock, interrupt signals, etc.

The TOE provides the test circuitry to perform the TOE testing under the test mode.

The TOE provides the timers for the security IC embedded software to abort irregular executions of the program.

The TOE provides power management functionality under boot mode, test mode, and normal mode, also contact and contactless interfaces.

The TOE provides strong security functionalities against malfunction, including the environmental sensors to monitor if environmental conditions are within the specified range, the abnormality check of TRNG to verify the quality of the generated random data, also the integrity to monitor if the data is manipulated.

The TOE provides strong security functionalities against leakage, including memory encryption and bus masking, ARMSC000 random branch insertion to obscures the cycle timing of code by inserting branch to self-instruction, and random OSC clock jitter to configure the oscillator frequency to a random value for each cycle.

The TOE provides strong security functionalities against physical manipulation and probing, including the dedicated shielding techniques, data integrity check for verifying the integrity of the data, also the memory and bus encryption.

The TOE provides strong security functionalities against abuse of functionality and identification by the means of test access control mechanism. It is implemented by a combination with hardware fuse and software access control mechanism.

The TOE provides a true random number generator, which is accessible by the crypto library. The true random number generator is composed of entropy sources, self-test circuit and post-processing circuit. The self-test circuit includes the total failure test and online test. The total failure test is performed on the entropy source. The on line testing is performed on the raw random number sequence, aiming to prevent malfunctioning. The true random number also fulfils the AIS20/31 PTG.2 level.

The TOE provides the following cryptographic services to the Security IC embedded software:

- DES/TDES
- RSA

The TOE implements the Triple-DES algorithm by means of a hardware co-processor and the software crypto library. It supports the DES algorithm with a single 56 bit key supporting ECB mode. It supports the Triple-DES algorithm with three 56 bit keys for 3-key Triple DES supporting ECB mode. The keys for the DES algorithms shall be provided by the security IC embedded software.

The TOE provides the RSA CRT algorithm according to the paper [11] to meet the security requirement FCS_COP.1[RSA]. The TSF implement the RSA CRT algorithm with the cryptographic key sizes is 256 bits to 4096 bits. The RSA CRT algorithm is accessed by the crypto library.

The TOE crypto library also includes functionality for SHA1, SHA256, ECC, AES and Chinese domestic crypto algorithms. The security of these is not claimed by the TOE.

### 1.3.3. TOE components

The TOE consists of the following components that are delivered to the composite product manufacturer:

**Table 2 List of TOE components**

| Type | Name | Version | Package |
|---|---|---|---|
| Hardware | THD89 | 1.0 | Module |
| Software | Crypto Library | 1.01 | Software library in ROM |
| | Boot code | 1.0 | Boot code in ROM |
| | Header file | 0.1 | cryptolib.h |
| Document | Operational guidance[6] | 0.9 | Document |
| | Preparatory guidance[7] | 0.9 | Document |
| | Security guidelines[12] | 0.8 | Document |
| | Cryptographic Algorithm API[13] | 1.7 | Document |

## 1.4. Life cycle and delivery

The end-consumer environment of the TOE is phase 7 of the Security IC product life-cycle as defined in the PP [1]. In this phase the TOE is in usage by the end-consumer. Its method of use now depends on the Security IC Embedded Software. Examples of use cases are ID cards or Bank cards.

The scope of the assurance components referring to the TOE's life cycle is limited to phases 2, 3 and 4. These phases are under the control of the TOE manufacturer. At the end of phase 4 the TOE components described in 1.3.3 are delivered to the Composite Manufacturer.

# 2. Conformance claim

This chapter presents conformance claim and the conformance claim rationale.

## 2.1. CC Conformance

This Security Target and the TOE claim to be conformant to the Common Criteria version 3.1:

- Part 1 revision 5 [2].
- Part 2 revision 5 [3]
- Part 3 revision 5 [4]

For the evaluation will be used the methodology in Common Criteria Evaluation Methodology version 3.1 CEM revision 5 [5]

This Security Target and the TOE claim to be CC Part 2 extended and CC Part 3 conformant.

## 2.2. PP Claim

This Security Target claims **strict** conformance to the Security IC Platform Protection Profile [1].

The TOE also provides additional functionality, which is not covered in [1].

## 2.3. Package claim

This Security Target claims conformance to the assurance package **EAL5** augmented with AVA_VAN.5 and ALC_DVS.2. This assurance level is in line with the Security IC Platform Protection Profile [1].

## 2.4. Conformance claim rationale

The TOE is a Security IC equivalent to the TOE type defined in [1] as it is composed by:

- Processing unit (ARM SC000 CPU)
- Security components (e.g. sensors)
- I/O ports (contact and contactless interfaces)
- Volatile memory (e.g. RAM)
- Non-Volatile memory ( e.g. NVM)
- Dedicated software (Crypto library)

The TOE provides additionally cryptographic functionalities which are not part of the claimed Security IC Platform Protection Profile [1]:

- Organisational Security Policy P.Crypto-Service is defined to require TDES and RSA cryptographic functions
- Security Objectives O.TDES and O.RSA are included in the ST to meet P.Crypto-Service

- Security Functional Requirements FCS_COP.1[TDES] and FCS_COP.1[RSA] are included in the ST to meet O.TDES and O.RSA.

# 3. Security problem definition

This chapter presents the threats, organisational security policies and assumptions for the TOE.

The Assets, Assumptions, Threats and Organisational Security Policies are completely taken from the Security IC Platform Protection Profile [1].

## 3.1. Description of Assets

Since this Security Target claims conformance to the Security IC Platform Protection Profile [1], the assets defined in section 3.1 of the Protection Profile are applied.

## 3.2. Threats

This Security Target claims conformance to the Security IC Platform Protection Profile [1]. The Threats that apply to this Security Target are defined in section 3.2 of the Protection Profile. The following table lists the threats of the Protection Profile.

**Table 3 Threats defined in the Protection Profile**

| Threat | 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 |

## 3.3. Organisational security policies

This Security Target claims conformance to the Security IC Platform Protection Profile [1]. The Organisational Security Policies that apply to this Security Target are defined in section 3.3 of the Protection Profile, they are:

P.Process-TOE Protection during TOE Development and Production

The following Organisational Security is the additional Organisational security policy defined by the TOE：

P.Crypto-Service Cryptographic services of the TOE

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

## 3.4. Assumptions

This Security Target claims conformance to the Security IC Platform Protection Profile [1]. The assumptions claimed in this Security Target defined in section 3.4 of the Protection Profile. They are specified below.

**Table 4 Assumptions defined in the Protection Profile**

| Assumption | Title |
|---|---|
| A.Process-Sec-IC | Protection during Packaging, Finishing and Personalisation |
| A.Resp-Appl | Treatment of User Data |

# 4. Security objectives

This chapter provides the statement of security objectives and the security objective rationale. For this chapter the Security IC Platform Protection Profile [1] can be applied completely. Only a short overview is given in the following.

## 4.1. Security objectives for the TOE

All objectives described in the section 4.1 of the Security IC Platform Protection Profile [1] are claimed for the TOE, these are:

**Table 5 Security objectives for the TOE defined in the Protection Profile**

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

In addition the TOE defines the following objectives:

O.TDES TDES functionality

The TOE shall provide secure cryptographic services implementing the TDES cryptographic algorithm for encryption and decryption.

O.RSA RSA functionality

The TOE shall provide secure cryptographic services implementing the RSA cryptographic algorithm for encryption and decryption.

## 4.2. Security objectives for the security IC embedded software

The security IC Embedded Software defines the operational use of the TOE. This section describes the security objective for the Security IC Embedded Software, which is taken from section 4.2 of the Security IC Platform Protection Profile [1].

**Table 6 Security Objectives for the security IC embedded software environment defined in the Protection Profile**

| Security Objective | Title |
|---|---|
| OE.Resp-Appl | Treatment of User Data of the composite TOE |

## 4.3. Security objectives for the operational environment

This section describes the security objective for the operational environment, which is taken from section 4.3 of the Security IC Platform Protection Profile [1].

**Table 7 Security Objectives for the operational environment defined in the Protection Profile**

| Security Objective | Title |
|---|---|
| OE.Process-Sec-IC | Protection during composite product manufacturing |

## 4.4. Security objectives rationale

Section 4.4 in the Protection Profile provides a rationale how the assumptions, threats and organisational security policies are addressed by the objectives. The table below shows this relationship.

**Table 8 Addressing of assumptions, threats and organisational security policies to objectives**

| Assumption, Threat or Organisational 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 |

For the justification of the above mapping please refer to the Protection Profile.

The table below shows how the additional organisational security policies are addressed by objectives for the TOE.

**Table 9 Addressing of assumptions, threats and organisational security policies to additional objectives**

| Assumption, Threat or Organisational Security Policy | Security Objective |
|---|---|
| P.Crypto-Service | O.TDES<br>O.RSA |

| | |
|---|---|

The objective O.TDES and O.RSA implements specific crypto services as required by P.Crypto-Service.

# 5. Extended Components Definitions

This Security Target uses the extended security functional requirements defined in chapter 5 of the Security IC Platform Protection Profile [1].

This Security Target does not define extended components in addition to the Protection Profile.

# 6. Security requirements

This chapter presents the statement of security requirements for the TOE and the security requirements rationale. This chapter applies the Security IC Platform Protection Profile [1].

## 6.1. Definitions

In the next sections the following notation is used:

- The iteration operation is used when a component is claimed with varying operations, it is denoted by adding "[XXX]" to the component name.
- Refinement, selection or assignment operations are used to add details or assign specific values to components, they are indicated by italic text and explained in footnotes.

## 6.2. Security Functional Requirements (SFR)

To support a better understanding of the combination Security IC Platform Protection Profile vs. Security Target, the TOE Security Functional Requirements are presented in the following several different sections.

### 6.2.1. SFRs derived from the Security IC Platform Protection Profile

The table below lists the Security Functional Requirements that are directly taken from the Security IC Platform Protection Profile.

**Table 10 List of Security Functional Requirements on the security IC platform Protection Profile**

| Security functional requirement | 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" |
| FAU_SAS.1 | "Audit storage" |
| FPT_PHP.3 | "Resistance to physical attack" |
| FDP_ITT.1 | "Basic internal transfer protection" |
| FDP_IFC.1 | "Subset information flow control" |
| FPT_ITT.1 | "Basic internal TSF data transfer protection" |
| FDP_SDC.1 | "Stored data confidentiality" |
| FDP_SDI.2 | "Stored data integrity monitoring and action" |
| FCS_RNG.1[PTG.2] | "Quality metric for random numbers" |

Except for FAU_SAS.1, FDP_SDC.1, FDP_SDI.2 and FCS_RNG.1[PTG.2] all assignment and selection operations are defined in the Protection Profile. As required by … and …

- ☐ In FAU_SAS.1 the left open assignment is the type of persistent memory;
- ☐ In FDP_SDC.1 the left open assignment is the memory area;
- ☐ In FDP_SDI.2 the left open assignments are the user data attributes and the action to be taken;
- ☐ In the FCS_RNG.1[PTG.2] the left open definition is the quality metric for the random numbers.

The following statements define these completed SFRs.

| | |
|---|---|
| **FAU_SAS.1** | Audit storage |
| Hierarchical to: | No other components. |
| FAU_SAS.1.1 | The TSF shall provide *the test process before TOE Delivery*[1] with the capability to store *Initialisation Data*[2] in the *OTP*[3]. |
| Dependencies: | No dependencies. |

| | |
|---|---|
| **FDP_SDC.1** | Stored data confidentiality |
| Hierarchical to: | No other components. |
| FDP_SDC.1.1 | The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *NVM, ROM and RAM*[4]. |
| Dependencies: | No dependencies. |

| | |
|---|---|
| **FDP_SDI.2** | Stored data integrity monitoring and action |
| Hierarchical to: | FDP_SDI.1 Stored data integrity monitoring |
| FDP_SDI.2.1 | The TSF shall monitor user data stored in containers controlled by the TSF *for integrity errors*[5] *on* all objects, based on the following attributes: *redundancy bits*[6]. |
| FDP_SDI.2.2 | Upon detection of a data integrity error, the TSF shall *reset*[7]. |
| Dependencies: | No dependencies. |

**FCS_RNG.1 [PTG.2]** Random number generation

Hierarchical to: No other components.

FCS_RNG.1.1[PTG.2] The TSF shall provide a *physical*[8] random number generator that Implements:

- 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.

[1] [assignment: list of subjects]
[2] [assignment: list of audit information]
[3] [assignment: type of persistent memory]
[4][assignment: memory area]
[5][assignment: integrity errors]
[6][assignment: user data attributes]
[7] [assignment: action to be taken]
[8] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]

- 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*[9].
- 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.
- The online test procedure shall be effective to detect non-tolerable weakness of the random numbers soon.
- The online test procedure checks the quality of the raw random number sequence. It is triggered *applied upon specified internal events*[10]. 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 *32 bit random number words*[11] that meet:

- test procedure A *and no other test suites*[12] does not distinguish the internal random numbers from output sequences of an ideal RNG.
- The average Shannon entropy per internal random bit exceeds 0.997.

Dependencies: No dependencies.

**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*[13].

*Refinement:* *The term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.*

Application note: The occurred failures will cause the alarm signals to be triggered, which will result in a reset (secure state).

**FPT_PHP.3 Resistance to physical attack**

Hierarchical to: No other components.

[9][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].
[10][selection: externally, at regular intervals, continuously, applied upon specified internal events].
[11][selection: bits, octets of bits, numbers [assignment: format of the numbers]]
[12][assignment: additional standard test suites]
[13] [assignment: list of types of failures in the TSF]

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist *physical manipulation and physical probing*[14] to the *TSF*[15] by responding automatically such that the SFRs are always enforced.

*Refinement:* *The TSF will implement appropriate mechanism to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attack is required ensuring that security functional requirements are enforced. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.*

Application note: 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.

### 6.2.2. SFRs regarding cryptographic functionality

**FCS_COP.1 [TDES]** Cryptographic operation – TDES

Hierarchical to: No other components.

FCS_COP.1.1 [TDES] The TSF shall perform *encryption and decryption*[16] in accordance with a specified cryptographic algorithm *TDES in ECB mode*[17] and cryptographic key sizes of *112/168 bit*[18] that meet the following: *NIST SP800-67[8] and NIST SP800-38A*[19] *[9]*.

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

**Application note:** The TOE also supports single DES. However the security of the single DES algorithm is not resistant against attacks with a high attack potential. Therefore the application of single DES shall not be used in parts of the Security Embedded Software that require high security.

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

Hierarchical to: No other components.

FCS_COP.1.1[RSA] The TSF shall perform *encryption and decryption*[20] operation in accordance with a specified cryptographic algorithm *RSA*[21] and

[14] [assignment: physical tampering scenarios]
[15] [assignment: list of TSF devices/elements]
[16][assignment: list of cryptographic operations]
[17][assignment: cryptographic algorithm]
[18] [assignment: cryptographic key sizes]
[19][assignment: list of standards]
[20] [assignment: list of cryptographic operations]
[21] [assignment: cryptographic algorithm]

| | |
|---|---|
| | cryptographic key sizes of *256 bits to 4096 bits*[22] that meet the following: *RSA standard [11]*[23]. |
| Dependencies: | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| Application note: | The security IC embedded software shall make a choice regarding the RSA key length. Key lengths >= 1900 bits is the legacy mechanism only, and key lengths >= 3000 bits is the recommended. |

## 6.3. Security Assurance Requirements (SAR)

The Security Assurance Requirements claimed for the TOE are the SARs claimed in section 6.2 of the Security IC Protection Profile [1].

This Security Target will be evaluated according to Security Target evaluation (Class ASE)

The Security Assurance Requirements for the evaluation of the TOE are the components in Assurance Evaluation level EAL5 augmented by the components ALC_DVS.2 and AVA_VAN.5. The table below shows the details of these assurance requirements.

**Table 11 TOE assurance requirements**

| Security assurance requirements | Titles |
|---|---|
| Class ADV: Development | |
| ADV_ARC.1 | Architectural design |
| ADV_FSP.5 | Functional specification |
| ADV_IMP.1 | Implementation representation |
| ADV_INT.2 | TSF internals |
| ADV_TDS.4 | TOE design |
| Class AGD: Guidance documents | |
| AGD_OPE.1 | Operational user guidance |
| AGD_PRE.1 | Preparative user guidance |
| Class ALC: Life-cycle support | |
| ALC_CMC.4 | CM capabilities |
| ALC_CMS.5 | CM scope |
| ALC_DEL.1 | Delivery |
| ALC_DVS.2 | Development security |
| ALC_LCD.1 | Life-cycle definition |
| ALC_TAT.2 | Tools and techniques |
| Class ASE: Security Target evaluation | |
| ASE_CCL.1 | Conformance claims |

[22] [assignment: cryptographic key sizes]
[23] [assignment: list of standards]

| | |
|---|---|
| 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 |
| Class ATE: Tests | |
| ATE_COV.2 | Coverage |
| ATE_DPT.3 | Depth |
| ATE_FUN.1 | Functional testing |
| ATE_IND.2 | Independent testing |
| Class AVA: Vulnerability analysis | |
| AVA_VAN.5 | Vulnerability analysis |

## 6.4. Security requirements rationale

### 6.4.1. Security Functional Requirements (SFR)

The table below provides an overview of how the security functional requirements are combined to meet the security objectives.

**Table 12 Mapping of security functional requirements to security objectives**

| Security Objectives for the TOE | Security Functional Requirements | Fulfilment of mapping |
|---|---|---|
| O.Leak-Inherent | FDP_ITT.1<br>FDP_IFC.1<br>FPT_ITT.1 | See PP |
| O.Phys-Probing | FDP_SDC.1<br>FPT_PHP.3 | See PP |
| O.Malfunction | FRU_FLT.2<br>FPT_FLS.1 | See PP |
| O.Phys-Manipulation | FDP_SDI.2<br>FPT_PHP.3 | See PP |
| O.Leak-Forced | FDP_ITT.1<br>FDP_IFC.1<br>FPT_ITT.1<br>FRU_FLT.2<br>FPT_FLS.1<br>FPT_PHP.3 | See PP |
| O.Abuse-Func | FMT_LIM.1<br>FMT_LIM.2<br>FDP_ITT.1<br>FPT_ITT.1<br>FDP_IFC.1<br>FPT_PHP.3<br>FRU_FLT.2<br>FPT_FLS.1 | See PP |

| | | |
|---|---|---|
| O.Identification | FAU_SAS.1 | See PP |
| O.RND | FCS_RNG.1[PTG.2]<br>FDP_ITT.1<br>FPT_ITT.1<br>FDP_IFC.1<br>FPT_PHP.3<br>FRU_FLT.2<br>FPT_FLS.1 | See PP |
| O.TDES | FCS_COP.1 [TDES] | O.TDES requires the TOE to support DES encryption and decryption with its specified key lengths. The claim for FCS_COP.1 [TDES] is suitable to meet the objective O.TDES. |
| O.RSA | FCS_COP.1 [RSA] | O.RSA requires the TOE to support RSA CRT encryption and decryption with its specified key lengths. The claim for FCS_COP.1 [RSA] is suitable to meet the objective O. RSA. |

### 6.4.2. Dependencies of the SFRs

The dependencies for the SFRs claimed according to the Protection Profile are all satisfied in the set of SFRs claimed in the Protection Profile.

In the following table the dependencies of the SFRs claimed in addition to Protection Profile is indicated.

**Table 13 Dependencies of SFRs in addition to PP**

| Security functional requirement | Dependencies | Fulfilled by security requirements in this Security Target |
|---|---|---|
| FCS_COP.1[TDES] | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4 | See explanation below this table |
| FCS_COP.1[RSA] | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4 | See explanation below this table |

The developer of the Security IC Embedded Software must ensure that the implemented additional security functional requirements FCS_COP.1[TDES] and FCS_COP.1[RSA] and FCS_RNG.1[PTG.2] are used as specified and that the User Data processed by the related security functionality is protected as defined for the application context.

The dependent requirements for FCS_COP.1[TDES] and FCS_COP.1[RSA] address the appropriate management of cryptographic keys used by the specified cryptographic function.

All requirements concerning these management functions shall be fulfilled by the environment (Security IC Embedded Software).

The functional requirements [FDP_ITC.1, or FDP_ITC.2 or FCS_CKM.1] and FCS_CKM.4 are not included in this Security Target since the TOE only provides a pure engine for encryption and decryption without additional features for the handling of cryptographic keys. Therefore the Security IC Embedded Software must fulfil these requirements related to the needs of the realised application.

### 6.4.3. Security Assurance Requirements (SAR)

The SARs as defined in section 6.3 are in line with the SARs in the Security IC Platform Protection Profile. The context of this ST is equivalent to the context described in the Protection Profile and therefore these SARs are also applicable for this ST.

# 7. TOE summary specification

This chapter provides general information to potential users of the TOE on how the TOE implements the Security Functional Requirements in terms of "Security Functionality".

## 7.1. Malfunction

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

The TOE ensures its correct operation and prevents any malfunction while the security IC embedded software is executed by implementation of the following security features:

- Environmental sensors

## 7.2. Leakage

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

- Bus masking
- ARMSC000 random branch insertion
- Random OSC clock jitter

## 7.3. Physical manipulation and probing

Physical manipulation and probing relates to the security functional requirements 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 security measures protect the TOE against manipulation of

(i) The hardware.
(ii) The security IC embedded software in the ROM
(iii) The application data in the NVM including the configuration data.

It also protects User Data or TSF data against disclosure by physical probing when stored or while being processed by the TOE.

The protection of the TOE comprises different features within the design and construction, which make reverse-engineering and tamper attacks more difficult. These features comprise of

- Active shielding

- Data integrity checking
- Memory encryption

## 7.4. Abuse of functionality and Identification

Abuse of functionality and Identification relates to the security functional requirements FMT_LIM.1, FMT_LIM.2, FAU_SAS.1 by implementation of a test mode access control mechanism that prevents abuse of test functionality delivered as part of the TOE.

## 7.5. Random numbers

Random numbers relate to the security requirement FCS_RNG.1[PTG.2]. The TOE meets this SFR by providing a random number generator.

## 7.6. Cryptographic functionality

The TOE provides the single and Triple-DES algorithm according to the *NIST SP800-67[8], NIST SP800-38A*[24]*[9]* Standard to meet the security requirement FCS_COP.1[TDES].

The TOE provides the RSA CRT algorithm according to the paper [11] to meet the security requirement FCS_COP.1[RSA]. The TSF implement the RSA CRT algorithm with the cryptographic key sizes is 256 bits to 4096 bits.

# 8. References

| Ref | Title | Version | Date |
|---|---|---|---|
| [1] | Security IC Platform Protection Profile, BSI-CC-PP-0084-2014 | Version 1.0 | 13.01.2014 |
| [2] | Common Criteria for Information Technology Security Evaluation,<br>Part 1: Introduction and General Model<br>CCMB-2012-09-001 | Version 3.1 Revision 5 | April 2017 |
| [3] | Common Criteria for Information Technology Security Evaluation,<br>Part 2: Security Functional Requirements<br>CCMB-2012-09-002 | Version 3.1 Revision 5 | April 2017 |
| [4] | Common Criteria for Information Technology Security Evaluation, | Version 3.1 Revision 5 | April 2017 |

[24][assignment: list of standards]

| | | | |
|---|---|---|---|
| | Part 3: Security Assurance Requirements CCMB-2012-09-003 | | |
| [5] | Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology CCMB-2012-09-004 | Version 3.1 Revision 5 | April 2017 |
| [6] | THD89 Operational Guidance v0.9 | Version 0.9 | June, 2018 |
| [7] | THD89 Preparative Guidance v0.9 | Version 0.9 | June, 2018 |
| [8] | NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised January 2012, National Institute of Standards and Technology | Revision 1 | January 2012 |
| [9] | NIST SP 800-38A Recommendation for Block Cipher Modes of Operation, 2001, with Addendum Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, October 2010 | 2001 ED | October 2010 |
| [10] | SC000 Detailed Description | Revision: r0p0-01re10 | 2011 |
| [11] | PKCS #1: RSA Cryptography Standard, RSA Laboratories | Version 2.2 | 2012 |
| [12] | THD89 Secure Microcontroller Security guideline_v0.8 | Version 0.8 | June, 2018 |
| [13] | THD89 Cryptographic Algorithm API | Version 1.7 | June, 2018 |