SHHIC secure microcontroller SHC1302 / 2907M4 with crypto library V1.10

Security Target

(V1.0)

文档创建信息(Document Creation Information)

责任者角色 (Role)	姓名 (Name)	职位 (Position)	完成日期 (Date)
编写人员 (Created by)	Si Gang, Bao	Security Technology Department Manager	2012-July-03
校对人员 (Checked by)	Yue Gang, Liu	Project Director	2012-July-12
	Xue Qing, Zhou	Product Marketing Manager	2012-July-12
审核人员 (Approved by)	Xin Hua, Ji	Vice General Manager	2012-July-13

文档修改信息(Document Modification Information)

发行（申报）版本 (Release Version)	日期 (Release Date)	作者 (Author)	修改 (Modification)
V0.5	2012-July-13	Si Gang, Bao	Draft for CC application
V0.6	2012-Dec-31	Si Gang, Bao	1. Quote new version for RNG standard (Dec 2, 2011, AIS31, version 2.1) 2. Update information for Memory size
V0.7	2013-Feb-26	Si Gang, Bao	1. Use SHC1302 / 2907M4 instead of SHC1302 for TOE identification 2. In 1.4.1, Update Figure 1 and related descriptions 3. In 1.4.2, add ITCOS description 4. In 1.5, add TOE conformance claim
V0.8	2013-Mar-04	Si Gang, Bao	1. In 1.5.2, remove TOE conformance claim
V1.0	2013-Aug-28	Si Gang, Bao	1. Rename the document name to “SHHIC secure microcontroller SHC1302 / 2907M4 with crypto library V1.10 Security Target” 2. update crypto library version from “V1.00” to “V1.10” 3. add security function “Security configuration checking” in section 4.1

References

[1] Security IC Platform Protection Profile BSIPP-0035, Version 1.0, June 15, 2007 published by Bundesamt für Sicherheit in der Informationstechnik (BSI)

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, July 2009, version 3.1, revision 3, CCMB-2009-07-001

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, July 2009, version 3.1, revision 3, CCMB-2009-07-002

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, July 2009, version 3.1, revision 3, CCMB-2009-07-003

[5] Common Criteria for Information Technology Security Evaluation, Evaluation methodology, July 2009, version 3.1, revision 3, CCMB-2009-07-004

[6] Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Dec 2, 2011, AIS31, version 2.1

[7] Supporting Document Mandatory Technical Document Application of Attack Potential to Smartcards, Version 2.7, Revision 1, March 2009, CCDB-2009-03-001

[8] SHHIC Application Note for SHC1302 / 2907M4 IC Security Guide, Aug 28, 2013, V1.15

[9] SHHIC SHC1302 / 2907M4 IC Data Sheet, Jun 19, 2013, V1.12

[10] SHHIC SHC1302 / 2907M4 Crypto Library User Guide, Aug 28, 2013, V1.12

[11] SHHIC Application Note for SHC1302 / 2907M4 Crypto Library Check Guide, Aug 28, 2013, V1.03

[12] U.S. Department of Commerce / National Bureau of Standards, Data Encryption Standard (DES), FIPS PUB 46_3, 1999, October 25, keying option 1 and 2.

[13] PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 14, 2002.

Content

1. ST Introduction

This chapter describes the TOE and is divided into three sections providing different levels of abstraction.

1.1. ST reference

SHHIC secure microcontroller SHC1302 / 2907M4 with crypto library V1.10 security target V1.0, Aug 28, 2013.

1.2. TOE reference

The TOE is identified by: "SHC1302 / 2907M4 with Crypto Library V1.10 and ITCOS V1.00".

1.3. TOE overview

This chapter provides a brief overview of the TOE's functionality and security features.

1.3.1. Usage and major security features of the TOE

The TOE is a high-end dual-interface secure smart card integrated circuit suitable for (amongst others) banking, e-passport, social security, pay-TV and mobile payment applications. The TOE consists of the IC hardware and IC dedicated support software providing cryptographic functions. The hardware is based on a 32-bit CPU with volatile, non-volatile and read-only memory. The microcontroller incorporates cryptographic coprocessors for acceleration of symmetric and asymmetric encryption algorithms.

The device supports the following communication interfaces:

- ISO7816 contact interface,
- ISO14443 contactless interface
- General purpose IO (GPIO).

Also part of the TOE is documentation consisting of IC data sheet, guidance document for secure software development and guidance document for using crypto library.

The TOE has been designed to protect the integrity of its functional behaviour and protect the confidentiality and integrity of user data against physical and logical attacks.

The TOE provides test functionality for hardware testing which can be disabled forever after testing.

A summary of the security features of the TOE:

- Data Encryption Standard support up to triple length key,
- RSA asymmetric cryptography support,
- True physical random number generator,

- Cyclic Redundancy Check coprocessor,
- Protection against side channel analysis attacks,
- Protection against perturbation attacks,
- Protection against physical attacks

The features above are directly visible and can be controlled by the security IC embedded software. In addition security mechanisms have been implemented to reduce side channel leakage, provide resistance against perturbation attacks and to provide detection mechanisms to maintain integrity and confidentiality. The detection mechanisms allow the software to perform risk analysis and take appropriate measures.

1.3.2. TOE type

The TOE is SHC1302 / 2907M4 with IC dedicated support software intended for use as a smart card IC.

1.3.3. Required non-TOE hardware/software/firmware

For use of the ISO14443 contactless interface an antenna is required. This antenna is connected to the antenna contacts of the TOE but is not part of the TOE itself.

1.4. TOE description

The TOE SHC1302 / 2907M4 is intended for use in smart card based applications. The TOE consists of the IC, which is the hardware part of the TOE, and IC dedicated support software and IC dedicated test software and boot software, which is the software part of the TOE. All other software that might be running on the TOE is called “Security IC Embedded Software” and is not part of the TOE. The dedicated software is divided into two parts, the ITCOS for test and boot and the Crypto Library for cryptographic support.

1.4.1. Physical scope of the TOE

The SHC1302 / 2907M4 is manufactured in 0.18µm CMOS technology. *Figure 1* shows the block diagram of the IC.

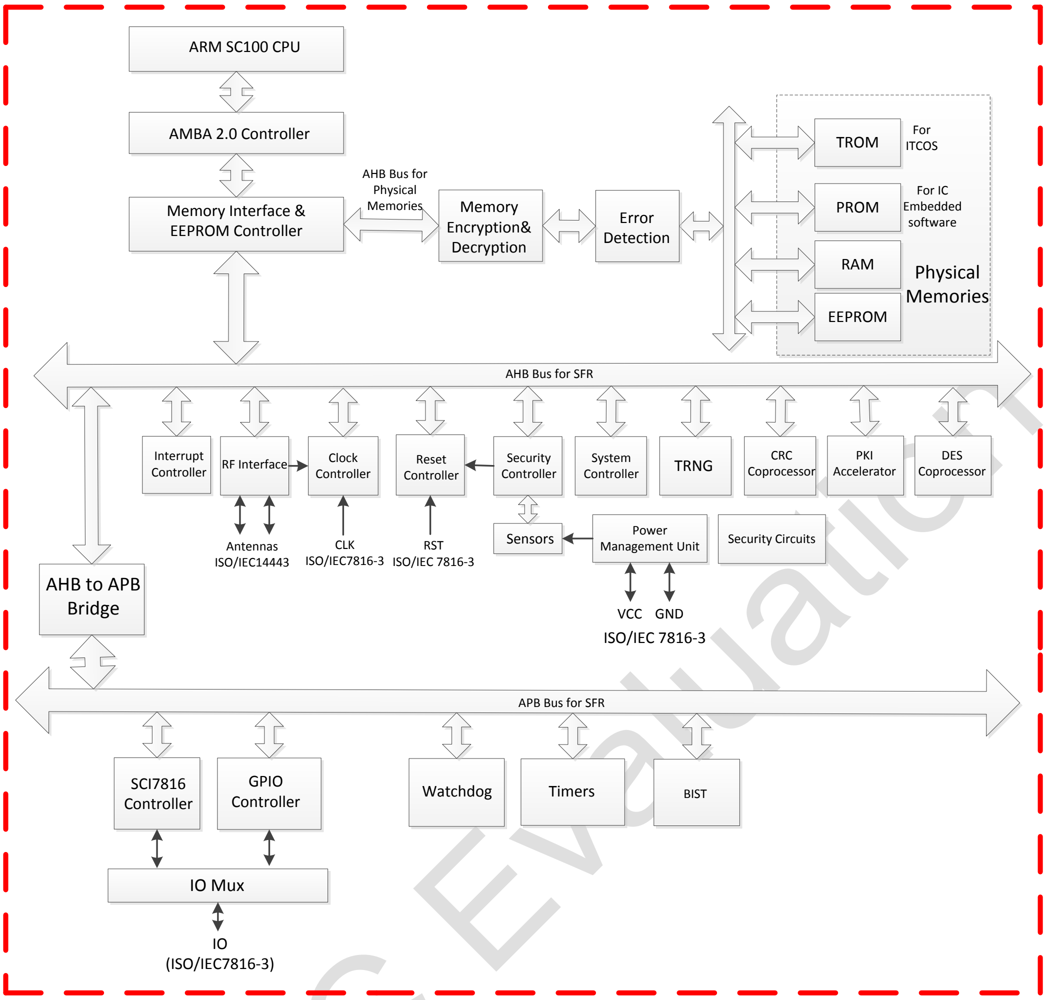

Figure 1Block diagram of SHC1302 / 2907M4 with the actual TOE inside the red dashed box

The TOE consists of an IC and dedicated software. The different components of the TOE are listed in the following table.

TOE Component	Name	Version	Type
IC	SHC1302	HHIC2907M4	Wafer or modules
IC dedicated support software	Crypto Library	1.10	Software library
IC dedicated test software and boot software	ITCOS	1.00	On-chip ROM content
IC security guidance	Application Note for SHC1302 / 2907M4 IC Security Guide	1. 15	Document
IC data sheet	SHC1302 / 2907M4	1.12	Document

	IC Data Sheet		
Crypto library user guidance	SHC1302 / 2907M4 Crypto Library User Guide	1.12	Document
Crypto library integrity check guidance	Application Note for SHC1302 / 2907M4 Crypto Library Check Guide	1.03	Document

All other software is called security IC embedded software and is not part of the TOE.

The TOE’s on-chip memories are:

- PROM 256 kbytes for security IC embedded software
- TROM 32 kbytes for IC dedicated test software and boot software (ITCOS)
- RAM 10 kbytes for stack, heap
- EEPROM 80 kbytes for non-volatile data storage

The central processing unit is a 32-bit ARM SC100. For cryptographic computations a CRC coprocessor (ISO/IEC13239), DES coprocessor (FIPS PUB 46-3), PKI accelerator and physical random number generator (AIS31) has been added.

Other major components are:

- AMBA 2.0 compliant bus matrix
- ISO14443 Interface
- ISO7816 Interface
- General Purpose IO
- Interrupt controller
- Three Programmable Interval Timers
- Watchdog
- Power Management
- Reset Control
- Clock Network
- Access Control for Special Function Registers
- Security Controller for detection of extreme environmental conditions
- Watchdog
- Timers
- BIST circuit for CPU testing

The TOE can be configured by software using special function registers that influence the hardware behaviour of the TOE. The registers shall be set according the corresponding software guidance [8] [9].

For security reasons the data sheet and security guidance will not be published but only delivered to the security IC embedded software developer of the composite product. The TOE supports 3 IC modes, which are Boot Mode, Product Test Mode and Application Mode. The end-user will receive TOE running in Boot Mode and Application Mode with disabled test functionality. The disabling of the test functionality is performed after production testing. The boot software part of ITCOS will perform the actual switch from Boot Mode to Application Mode at the end of the boot sequence. The PROM but no part of the TROM will be executed in the Application Mode.

The IC hardware protects internally stored secret data against physical tampering and provides features used by the IC dedicated support software to protect the security functionality of the TOE. The functions provided by the IC dedicated support software are secure. That does not automatically mean that applications that use these functions are secure as well. They must be implemented according to the IC security guidance [8] and crypto library user guidance [10].

1.4.2. Logical scope of the TOE

Software execution is performed by the ARM SC100 CPU core. The security IC embedded software shall use the IC dedicated support software to perform security critical operations. *Figure 2* shows an overview about the logical structure of the TOE.

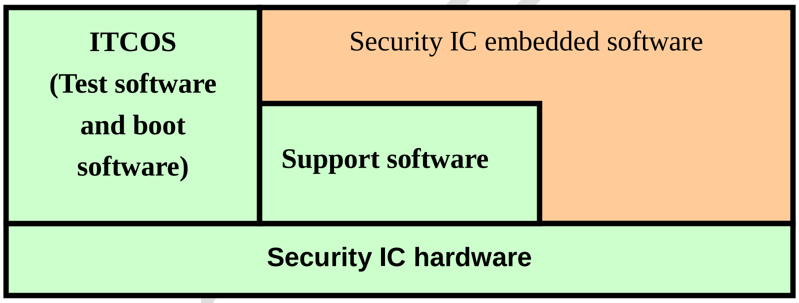

Figure 2 Logical overview of the TOE software and the security IC embedded software

This support software provides security functionality for:

- RSA cryptographic functions
  - Key generation
  - Modular exponentiation in a straightforward way with key lengths from 512 to 2048 bits in 64 bit steps
  - Modular exponentiation in CRT way with key lengths from 512 to 2048 bits in 64 bit steps
- DES cryptographic functions
  - DES encryption/decryption with key length of 56 bits, ECB mode and CBC mode

- Triple-DES encryption/decryption with key lengths of 112 and 168 bits, ECB mode and CBC mode

- Random Number Generation
  - Generate random number with variable lengths starting from 1 byte, and the randomness of each requested random number is verified by an online statistical test.
- Security configuration checking
  - Provide the security configuration check function for checking the setting of security features.

For any functionality which is not provided by this support software, the Security IC embedded software developer should implement it according to the IC security guidance [8] and IC data sheet [9].

The ITCOS comprises:

- IC dedicated Test Software which performs the mass production testing functionality
- Boot Software which performs the boot sequence.

The Security IC embedded software running in the Application Mode is not able to access the ITCOS due to the mode separation of the chip.

1.5. Conformance claims

This chapter presents conformance claims and their conformance claim rationale.

1.5.1. CC Conformance

This Security Target and TOE are conformant to the Common Criteria, version 3.1, revision 3, July 2009.

The conformance of this Security Target and TOE is Common Criteria Part 2 extended and Common Criteria Part 3 conformant.

1.5.2. Package claims

This Security Target claims conformance with the Security IC Platform Protection Profile [1].

The assurance level for this Security Target is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2. This assurance level conforms to the Security IC Platform Protection Profile.

1.5.3. Conformance claim rationale

This TOE is equivalent to the conformance claim stated in a Security IC Platform Protection Profile.

2. Security Problem Definition

This assets, threats, assumptions and organisational security policies are taken from the "Security IC Platform Protection Profile" [1]. In this chapter these items are listed and extensions are described.

2.1. Assets

The assets of the TOE are all assets described in section 3.1 of "Security IC Platform Protection Profile" [1].

2.2. Threats

The threats that apply to this Security Target are all threats described in section 3.2 of the "Security IC Platform Protection Profile" [1], which are:

Table 1 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

2.3. Organisational security policies

The organisational security policies that apply to this Security Target are all organisational security policies described in section 3.3 of the "Security IC Platform Protection Profile" [1], which are:

P.Process-TOE Protection during TOE development and production

In accordance with Application Note 6 in [1] 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.

Therefore the IC developer / manufacturer applies the policy: "Additional Security Functionality as specified below.

P.Add-Sec-Fun Additional Specific Security Functionality

The TOE shall provide the following security functionality to the security IC embedded software:

- Data Encryption Standard (DES)
- RSA

2.4. Assumptions

The assumptions that apply to this Security Target are all assumptions described in section 3.4 of the "Security IC Platform Protection Profile" [1], which are:

Table 2 Assumption defined in the Protection Profile

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

The following assumption is added in this Security Target according to application notes 7 and 8 in the "Security IC Platform Protection Profile" [1].

A.Key-Function Usage of Key-dependent Functions

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

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

2.5. Security objectives for the TOE

The security objectives that apply to this Security Target are all security objectives described in section 4.1 of the “Security IC Platform Protection Profile” [1], which are:

Table 3 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

The following additional security objectives are defined based on the additional functionality provided by the TOE:

O.DES DES functionality

The TOE shall provide cryptographic functionality to perform a DES encryption and decryption with double (112 bits) or triple length (168 bits) keys to the Security IC Embedded Software.

O.RSA RSA functionality

The TOE shall provide cryptographic functionality to perform an RSA encryption and decryption with key lengths from 512 bits up to 2048 bits to the Security IC Embedded Software.

2.6. Security objectives for the Security IC Embedded Software development environment

The security objectives for the Security IC Embedded Software development environment that apply to this Security Target are all security objectives described in section 4.2 of the “Security IC Platform Protection Profile” [1], which are:

Table 4 Security objectives for the Security IC Embedded Software defined in the Protection Profile

Security Objective	Title
OE.Plat-Appl	Usage of Hardware Platform
OE.Resp-Appl	Treatment of User Data

Clarification of “Usage of Hardware Platform (OE.Plat-Appl)”

The TOE supports cipher schemes as additional specific security functionality. If required the Security IC Embedded Software shall use these cryptographic services of the TOE and their interface as specified. When key-dependent functions implemented in the Security IC Embedded Software are just being executed, the Security IC Embedded Software must provide protection against disclosure of confidential data (User Data) stored and/or processed in the TOE by using the methods described under “Inherent Information Leakage (T.Leak-Inherent)” and “Forced Information Leakage (T.Leak-Forced)“.

If the Random Number Generator is used for leakage countermeasures, cryptographic operations (e.g. key generation) or cryptographic protocols (e.g. challenge response) these random numbers must be tested appropriately.

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

By definition cipher or plain text data and cryptographic keys are User Data. The Security IC Embedded Software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the TOE and use keys and functions appropriately in order to ensure the strength of cryptographic operation.

This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. For example, if asymmetric algorithms are used, it must be ensured that it is not possible to derive the private key from a related public key using the attacks defined in this Security Target. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realised in the environment.

2.7. Security objectives for the operational environment

The security objectives for the Security IC Embedded Software development Environment that apply to this Security Target are all security objectives described in section 4.3 of the “Security IC Platform Protection Profile” [1], which are:

Table 5 Security objectives for the operational environment defined in the Protection Profile

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

2.8. Security objectives rationale

Section 4.4 in the PP “Security IC Platform Protection Profile” [1] provides a rationale how the assumptions, threats, and organisational security policies are addressed by the objectives that are specified in the PP [1]. The following Table 14 reproduces the table in section 4.4 of [1].

Table 6 Security objectives versus Assumptions, Threats and Organisational Security Policies

Assumption, Threat or Organisational Security Policy	Security Objective
A.Plat-Appl	OE.Plat-Appl
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
P.Add-Sec-Fun	O.DES O.RSA
A.Key-Function	OE.Plat-Appl

The justification related to the organisational security policy “Additional Specific Security Functionality (P.Add-Sec-Fun)” is as follows:

Since these objectives require the TOE to implement exactly the same specific security functionality as required by P.Add-Functions, the organisational security policy is covered by the objectives.

3. Security requirements

In this chapter addresses the security requirements for the TOE and the security requirements rationale, as defined in “Security IC Platform Protection Profile” [1].

3.1. Definitions

In the next sections the following the notation used

- Whenever iteration is denoted, the component has an additional identification [XXX].
- When the refinement, selection or assignment operation is used these cases are indicated by italic text and explained in footnotes.

3.2. Security Functional Requirements (SFR)

The Security Functional Requirements of the TOE are presented in the following sections to support a better understanding of the combination of this Security Target and the Protection Profile.

3.3. Security Functional Requirements defined by the Protection Profile

The following table shows the Security Functional Requirements that are directly taken from the “Security IC Platform Protection Profile” [1].

Table 7 Security Functional Requirements defined by the 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”

FCS_RNG.1	“Quality metric for random numbers”

Except for FAU_SAS.1 and FCS_RNG.1 all assignments and selections are completely defined in the “Security IC Platform Protection Profile” [1]. The following statements define the two exceptions.

For the SFR FAU_SAS.1 the Protection Profile [1] leaves the assignment for memory type open. The following statement fills in this assignment.

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 *the Initialisation Data and/or Pre-personalisation Data and/or supplements of the security IC embedded software*[2] in the *EEPROM*[3].

Dependencies: No dependencies.

For the SFR FCS_RNG1.1 the Protection Profile [1] leaves the assignment for additional security capabilities. For the SFR FCS_RNG1.2 the Protection Profile [1] leaves the assignment for the quality metric. The following statements fill in this assignment.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

FCS_RNG.1.1 The TSF shall provide a *physical* random number generator that implements *total failure test of the random source* and *none*[4].

FCS_RNG.1.2 The TSF shall provide random numbers that meet *Class PTG.2 of AIS31 [6]*[5].

Dependencies: No dependencies.

The following statements describe the Security Functional Requirements for the added specific functionality.

[1] [assignment: list of subjects]
[2] [assignment: list of audit information]
[3] [assignment: type of persistent memory]
[4] [assignment: list of additional security capabilities]
[5] [assignment: other comparable quality metric]

FCS_COP.1 [DES] Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform *encryption and decryption*[6] in accordance with a specified cryptographic algorithm *Triple Data Encryption Standard (3DES – supporting both ECB and CBC mode*[7] and cryptographic key sizes *of 112 bit and 168 bit*[8] that meet the following:

U.S. Department of Commerce / National Bureau of Standards, Data Encryption Standard (DES), FIPS PUB 46-3, 1999, October 25, keying option 1 and 2[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.

FCS_COP.1 [RSA] Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform *encryption and decryption*[10] in accordance with a specified cryptographic algorithm *Rivest, Shamir and Adleman (RSA)*[11] and cryptographic key sizes *from 512 bits to 2048*[12] *bits* according to the following:

PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 14, 2002[13].

Note1: Cryptographic primitives (Chapter5 of PKCS #1 v2.1) are implemented by TOE. The security IC embedded software developer should implement the schemes listed in PKCS #1 v2.1 based on cryptographic primitives.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or

[6] [assignment: list of cryptographic operations]
[7] [assignment: cryptographic algorithm]
[8] [assignment: cryptographic key sizes]
[9] [assignment: list of standards]
[10] [assignment: list of cryptographic operations]
[11] [assignment: cryptographic algorithm]
[12] [assignment: cryptographic key sizes]
[13] [assignment: list of standards]

FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.

3.4. Security Assurance Requirements (SAR)

The Security Assurance Requirements that apply to this Security Target are all Security Assurance Requirements described in section 6.2 of the “Security IC Platform Protection Profile” [1].

This Security Target will be evaluated according to

- Security Target evaluation (Class ASE).

Security Assurance Requirements for the TOE for the evaluation of the TOE are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following components:

- ALC_DVS.2, and AVA_VAN.5.

Table 8 Security Assurance Requirements as listed in the Protection Profile

Security assurance requirements	Titles
Class ADV: Development	
ADV_ARC.1	Architectural design
ADV_FSP.4	Functional specification
ADV_IMP.1	Implementation representation
ADV_TDS.3	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.4	CM scope
ALC_DEL.1	Delivery
ALC_DVS.2	Development security
ALC_LCD.1	Life-cycle definition
ALC_TAT.1	Tools and techniques

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

3.5. Security Requirements Rationale

3.5.1. Rationale for the Security Functional Requirements

Table 9 shows the mapping of the Security Objectives versus the Security Functional Requirements.

Table 9 Mapping of Security Objective to Security Functional Requirements

Security Objectives for the TOE	Security Functional Requirements	Fulfilment of mapping
O.Leak-Inherent	FDP_ITT.1 FDP_IFC.1 FPT_ITT.1	See PP
O.Phys-Probing	FPT_PHP.3	See PP
O.Malfunction	FRU_FLT.2 FPT_FLS.1	See PP
O.Phys-Manipulation	FPT_PHP.3	See PP
O.Leak-Forced	FDP_ITT.1 FDP_IFC.1	See PP

	FPT_ITT.1 FRU_FLT.2 FPT_FLS.1 FPT_PHP.3	
O.Abuse-Func	FMT_LIM.1 FMT_LIM.2 FDP_ITT.1 FDP_IFC.1 FPT_ITT.1 FRU_FLT.2 FPT_FLS.1 FPT_PHP.3	See PP
O.Identification	FAU_SAS.1	See PP
O.RNG	FCS_RNG.1 FDP_ITT.1 FPT_ITT.1 FDP_IFC.1 FPT_PHP.3 FRU_FLT.2 FPT_FLS.1	See PP
O.DES	FCS_COP.1 [DES]	See below
O.RSA	FCS_COP.1 [RSA]	See below
OE.Process-Sec-IC		
OE.Plat-Appl		
OE.Resp-Appl		
Security Objectives for the TOE	Dependencies	Fulfilment of dependencies

The justification related to the security objective “DES Functionality (O.DES)” is as follows:

O.DES requires the TOE to support DES encryption and decryption with its specified key lengths. Exactly this is the requirement of FCS_COP.1 [DES]. Therefore FCS_COP.1 [DES] is suitable to meet O.DES.

The justification related to the security objective “RSA Functionality (O.RSA)” is as follows:

O.RSA requires the TOE to support RSA encryption and decryption with its specified key lengths. Exactly this is the requirement of FCS_COP.1 [RSA]. Therefore FCS_COP.1 [RSA] is suitable to meet O. RSA.

3.5.2. Dependencies of the Security Functional Requirements

The dependencies listed in the Protection Profile [1] are independent of the additional dependencies listed in *Table 10* and are fulfilled within the Protection Profile.

Table 10 Dependencies for added Security Functional Requirements

Security functional requirement	Dependencies	Fulfilled by security requirements in this Security Target
FCS_COP.1 [DES]	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 additional security functional requirements FCS_COP.1 [DES] and FCS_COP.1 [RSA] 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 of FCS_COP.1 [DES] and FCS_COP.1 [RSA] completely 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.

3.5.3. Security Assurance Requirements (SAR)

The Security Assurance Requirements as defined in 3.4 are in line with the Security Assurance Requirements defined in the Protection Profile [1]. The context of this Security Target is equivalent to the context described in the Protection Profile and therefore these Security Assurance Requirements are also applicable for this Security Target.

4. TOE summary specification

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

4.1. Malfunction

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

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

- Environmental sensors to verify if the environmental conditions are within the specified range.
- Sensor self-tests
  Verifies the correct functioning of the environmental sensors.
- Data integrity checking
  Verifies the correctness of the data read from memory and written to memory.
- Total failure checking and statistical tests on random number generator data
  Verifies the quality of the generated random data.
- Security configuration checking
  Verifies the correctness of the security configuration.

If one of the sensors or mechanisms detects an exception the TOE will enter reset state or enter exception modes of CPU or return error message to the security IC embedded software, resulting in a secure situation.

4.2. Leakage

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

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

- Data and address bus encryption of physical memories
- Data and key masking
- DFA countermeasures for all secure cryptographic functions

4.3. Physical manipulation and probing

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

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

- Hardware design
- Hardware integrity checking

In case of hardware integrity failure the TOE will enter reset state resulting in a secure situation.

4.4. Abuse of functionality and identification

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

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

4.5. Random numbers

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

The random number generator fulfils the requirements of AIS31 class PTG.2 [6].

4.6. Cryptographic functionality

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