MN67S3C0 Smart Card IC Security Target (ST-Lite)

Version: 1.0

Date: 24 November 2021

Nuvoton Technology Corporation Japan

Document History

Version	Date	Changes
1.0	2021-11-24	Public version

Table of Contents

1 ST Introduction

1.1 ST Reference

Title:	MN67S3C0 Smart Card IC Security Target (ST-Lite)
Version:	Version 1.0
Date:	24 November 2021
Produced by:	Nuvoton Technology Corporation Japan
Author:	Mitsuyoshi Ohya
CC version used:	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001. Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002. Part 3: Security Assurance Requirements, Version 3.1, Revision 5 April 2017, CCMB-2017-04-003. (CC V3.1), part 1 to 3
PP used:	Security IC Platform Protection profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084-2014.

This document is compiled from MN67S3C0 Smart Card IC Security Target as public version (hereafter ST-Lite). Proprietary information (e.g. about design) is removed in accordance with regulations of [JIL]

1.2 TOE Reference

TOE:	MN67S3C0 Smart Card IC including IC Dedicated Software
Developed by:	Nuvoton Technology Corporation Japan

The TOE consists of:

Table 1: TOE identification

Item Type	Name	Version	Form of delivery
Hardware	MN67S3C0 Smart Card IC	RV01	Sawn wafers (dice)
Software	MN67S3C0 Smart Card IC - IC Dedicated Software	FV05	Encrypted in electronic form
Document	[AGD-SES]	1.2	Encrypted in electronic form
	[AGD-CM]	1.0	
	ARM Core SC000 Technical Reference Manual	AT580-DA-03001	
	ARM Core SC000 Integration & Implementation Manual	AT580-DC-70047	
	ARM Core SC000 Synthesizable Verilog	AT580-MN-22110	
	ARM Core Synopsys Reference Implementation Scripts	AT580-RM-00002	
	ARM Core Cadence Reference Implementation	AT580-RM-70000	
	ARM Core Integration Synthesisable RTL Verilog	AT580-MN-70005	
	ARM Core Vector Capture and Replay Test Bench	AT580-MN-22010	
	ARM Core SC000 Integration Kit	AT580-MN-70009	
	ARM Core SC000 Port Power Indicative Test Source	AT580-VE-09001	
	ARM Core SC000 Port Functional Test Source	AT580-VE-70006	
	ARM Core SC000 Port Speed Indicative Test Source	AT580-VE-70007	
	ARM Core SC000 Port Max Power Source	AT580-VE-70025	
	MN67S3C0 Software Library Specification	1.1	

1.3 TOE Overview

1.3.1 TOE Class and Main Security Function

The TOE is the smart card integrated circuit (IC) called MN67S3C0, developed by Nuvoton Technology Corporation Japan (hereinafter referred to as "NTCJ"). TOE is composed of hardware including a processing unit, cryptographic hardware, security components, contactless smart card interfaces, contact based interfaces, and volatile and non-volatile memories. The TOE also includes IC Dedicated Software and documentation. The IC Dedicated Software is used for test purposes during production and also provides additional services to facilitate usage of hardware.

The IC is delivered in form of sawn wafer (dice). After being made into module by composite product manufacturer, it is embedded in a credit card-sized plastic package, a plastic mold package or a booklet.

The TOE is intended to be used for the applications requiring high security such as transportation and fare collection applications (e.g. the commuter ticket), access control applications (e.g. ID cards), and government applications (e.g. the basic resident register, health cards, driver license and passport).

The security features implemented by the MN67S3C0 are:

- Random number generator;

- Security sensors (temperature, frequency, voltage, light);
- Physical countermeasures (such as sensing shield);
- Cryptography (DES, Triple-DES, AES, RSA, ECC, DH, SHA); and
- Countermeasures against attacks (such as power analysis, fault analysis).

In addition, the security of the development and manufacturing environments has been designed to provide high assurance in the security of the MN67S3C0 product right through to its delivery to customers.

1.3.2 Required non-TOE hardware/software/firmware

The TOE requires a reader/writer device which supplies the power and performs transmission and reception of data commands via the protocol defined in [ISO/IEC14443-3] and [JISX6319-4].

1.4 TOE Description

1.4.1 TOE Physical Scope

The TOE is the smart card IC which is composed of hardware such as a processing unit, cryptographic hardware, security components, physical unclonable function, contactless smart card interfaces, contact based interfaces and volatile and non-volatile memories (Figure 1). The TOE also includes IC designer/manufacturer proprietary IC Dedicated Software (Figure 2). Such software (also known as IC firmware) is used for test purposes during production and also provides additional services to facilitate usage of hardware. In addition to the IC Dedicated Software, the smart card IC also includes hardware to perform testing. All other software is called Security IC Embedded Software, which is not part of the TOE.

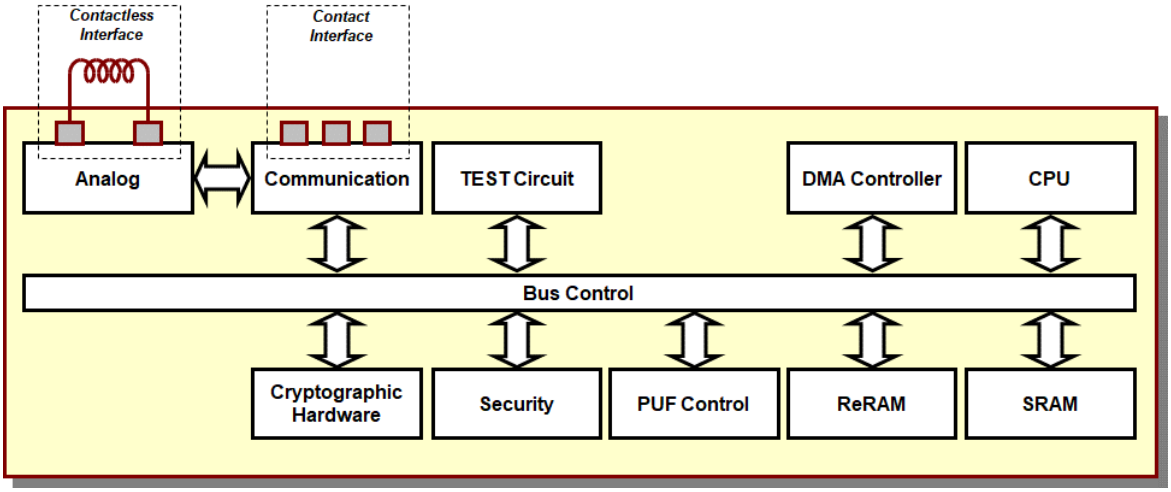

Figure 1: Block Diagram of MN67S3C0 Smart Card IC - Hardware -

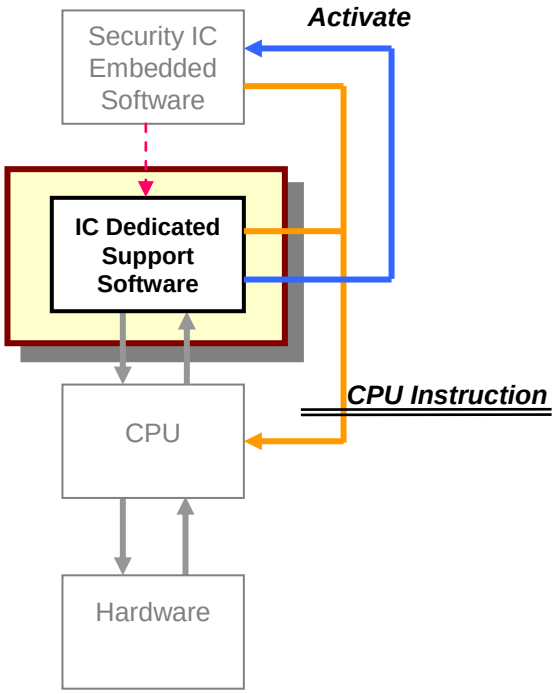

Figure 2: Block Diagram of MN67S3C0 Smart Card IC -IC Dedicated Software -

1.4.1.1 Hardware

As depicted in Figure 1, the TOE includes the following components.

(1) Analog

The Analog block has contactless interface in conformity to [ISO/IEC14443-2] and [JISX6319-4], and realizes the following functions.

- Power reception using a rectifier
- Demodulation of ASK-modulated signals
- Transmission of modulated signals using a load switch
- Generation of digital circuit power supply voltage
- Generation of analog circuit power supply voltage
- Generation of ReRAM supply voltage
- Switching external power supply voltage and internal generated power supply voltage
- Generation of reference clock signal from 13.56MHz carrier
- Generation of system clock signal
- Generation of power-on reset signal

Besides, it contains various security logics such as RNG, sensor/filter, and sensing shield.
The generated random numbers are used internally and can be used by the Security IC Embedded Software for e.g. the generation of cryptographic keys.
Sensor/filter includes the followings.

- Voltage sensor
- Voltage glitch sensor
- Light sensor
- Clock filter
- Reset filter
- Temperature sensor

The sensing shield covers the whole chip surface with shield lines, which are connected to sensors.

(2) Communication

The Communication block controls data transmission and reception through contactless interface in conformity to [ISO/IEC14443-3] and [JISX6319-4], and contact based interface through the I2C and the SPI.

(3) Memory

The smart card IC has memories consisting of the following:

- SRAM : 32 Kbytes
- ReRAM : 256 Kbytes

ReRAM can be accessed as both data memory and program memory.

(4) DMA Controller

The DMA Controller block controls 6 channels of data transmission, and the bus protocol is in conformity with [AHB-Lite].

(5) Cryptographic Hardware

The Cipher block is capable of realizing DES, TDES, AES, RSA, ECC, DH and SHA.

(6) Security

The Security block contains various control circuits to control the security logics (refer to 1.4.1.1(1)).

(7) PUF Control

The smart card IC has Physical Unclonable Function for realizing secure encryption and storage.

(8) Test Circuit

Test Circuit controls test mode operation to execute the manufactural defective tests of IC during Phase 3.

(9) CPU

CPU contains the ARM Secure Core, NVIC (Nested Vectored Interrupt Controller), debugger interface and AMBA AHB-lite Interface.

(10) Bus Control

Via the Core Bus, data between CPU and each block (DMA Controller, ReRAM, SRAM and Peripheral Bus) are exchanged.
Via the Peripheral Bus, data among blocks (DMA Controller, Communication, Cryptographic Hardware, Security, PUF Control and Core Bus) are exchanged.

1.4.1.2 Firmware and Software

The TOE includes the following IC Dedicated Software stored in ReRAM. It consists of IC Dedicated Support Software.

Table 2: IC Dedicated Software

Sorting of IC Dedicated Software	Purpose
IC Dedicated Support Software	To facilitate the use of hardware

The Security IC Embedded Software is not part of the TOE but the interface for delivery of it is included in the TOE.

1.4.1.3 Interface of the TOE

(1) Electrical Interface / Data Interface

The electrical interfaces of the TOE to the external environment are the coil pads which the RF antenna is connected, and the pads including the I2C and the SPI.

(2) Hardware Interface

For the interface to hardware, there is CPU Instruction Set.

(3) IC Dedicated Software Interface

There are the following interfaces.

- The set of function for controlling hardware

(4) Security IC Embedded Software Interface

For Security IC Embedded Software interface, there is the Security IC Embedded Software main function call from IC Dedicated Support Software.

(5) Physical Interface

Although not used for normal operation, the IC surface is an additional physical interface of the TOE that might be used by an attacker.

(6) Test Pads

The pads which are used at the test execution at Phase 3 are also electrical interface.

(7) Registers

There are the Registers which are used to control hardware functions. The functions are called by Security IC Embedded Software or IC Dedicated Software.

1.4.1.4 Guidance Documentation

The TOE includes the following guidance documentation:

- [AGD-SES]: This documentation is provided for users who develop Security IC Embedded Software.
- [AGD-CM]: This documentation is provided for users who manufacture card using the TOE.

1.4.2 TOE Life Cycle

As described in [PP, 1.2.3 & 7.1.1], the life cycle of the TOE is separated into 7 phases.

Phase 1 : IC Embedded Software Development
Phase 2 : IC Development
Phase 3 : IC Manufacturing
Phase 4 : IC Packaging
Phase 5 : Composite Product Integration
Phase 6 : Personalization
Phase 7 : Operational usage

This ST addresses Phase 2 and 3. This also includes the interfaces to the other phases where information and material is being exchanged with the partners of the development/manufacturer of the TOE.

The IC is delivered in form of sawn wafer (dice) after the production test. The TOE delivery can therefore be at the end of Phase 3.

1.4.2.1 TOE Logical Phases

Just after the power-on, the IC is in the normal mode. The IC can enter the test mode by the predefined procedures. When the power is turned off and then back on again, the IC enter into the normal mode again.
If all the requested tests are successfully done, the transition to the test mode falls into disuse by the predefined control.

1.5 TOE Environments

The development and manufacturing environments of the TOE are separated into five areas.

- Design site
- Mask manufacture site
- Manufacturing site
- Testing site
- Defective products processing site

1.5.1 TOE Development Environment

1.5.1.1 Design Site

NTCJ's design site is managed as defined in the security document related to ALC_DVS for the following confidential information.

- Logical design data
- Physical design data
- IC Dedicated Software
- Configuration data
- Pre-personalization data
- Specific development aids
- Test and characterization related data
- Material for software development support
- Wafer and development samples for testing
- Related documentation

Clearly defined physical, personnel, and IT processes and procedures within the scope of evaluation ensure the security in the development environment.

1.5.2 TOE Production Environment

1.5.2.1 Mask Manufacture Site

Mask manufacturer subcontracted with Manufacturer is forced to securely handle the following confidential information with NDA. The following confidential information is treated along the security document related to ALC_DVS.

- MN67S3C0 mask processing data (EB data)
- Photomasks
- Related documentation

1.5.2.2 Manufacturing Site

Manufacturer subcontracted with NTCJ is forced to securely handle the following confidential information with NDA. The following confidential information is treated along the security document related to ALC_DVS.

- Masks and wafers (including sawn wafer),
- Wafer defectives
- Related documentation

As with in the development environment, clearly defined processes and procedures ensure security in the production environment.

1.5.2.3 Testing Site

Testing company subcontracted with NTCJ is forced to securely handle the following confidential information with NDA. The following confidential information is treated along the security document related to ALC_DVS.

- Pre-personalization data
- wafers (including sawn wafer)
- Test and characterization related data
- Wafer and development samples for testing
- Wafer and chip defectives
- Related documentation

1.5.2.4 Defective Products Processing Site

Defective products processing company subcontracted with NTCJ are forced to securely handle the following confidential information with NDA. The following confidential information is treated along the security document related to ALC_DVS.

- Wafer and chip defectives
- Related documentation

The wafer and chip defectives are transported from manufacturing site and testing site to defective products processing company, and securely discarded.

1.5.3 Initialization and Pre-Personalization Data

During testing at Phase 3, certain data to uniquely identify the IC is injected in the write lock area of ReRAM.

2 Conformance Claims

2.1 CC Conformance Claim

This ST and the TOE claim conformance to Common Criteria for Information Technology Security Evaluation; Version 3.1, revision 5, Part 1, Part2, and Part 3.
This ST claims conformance for:
Common Criteria Part 2 extended and Common Criteria Part 3 conformant.

2.2 PP claim

This ST claims strict conformance to the following Protection Profile.

- Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084-2014.

2.3 Package Claim

This ST claims conformance to the following packages of the [PP].

- Package “Authentication of the Security IC”
- Package “Loader dedicated for usage in secured environment only”
- Package “Cryptographic Services (TDES/AES/Hash functions)”

The assurance level is **EAL5 augmented** with the following components:

- ALC_DVS.2,
- AVA_VAN.5

2.4 Conformance Rationale

In this ST, strict conformance to [PP] is claimed. This is fulfilled by including all the security objectives and requirements from [PP] (as shown in the relevant sections). The additional aspects added in this ST are consistent with [PP] as argued in section 6.3, and hence no further rationale is required in this section.

3 Security Problem Definition

The assets, threats, organizational security policies, and assumptions given in [PP] apply to the MN67S3C0. The description below is therefore adopted from [PP, 3].
In addition, the MN67S3C0 implements authentication mechanism, loader functionalities and cryptographic functionalities for which relevant threats, organizational security policies, and assumptions given in [PP, 7.2], [PP, 7.3] and [PP, 7.4].

3.1 Description of Assets

3.1.1 Assets regarding the Threats

The assets are defined in [PP, 3.1].
The assets (related to standard functionality) to be protected are

- the user data of the Composite TOE,
- the Security IC Embedded Software, stored and in operation,
- the security services provided by the TOE for the Security IC Embedded Software.

The user (consumer) of the TOE places value upon the assets related to high-level security concerns:

SC1 integrity of user data of the Composite TOE,

SC2 confidentiality of user data of the Composite TOE being stored in the TOE's protected memory areas,

SC3 correct operation of the security services provided by the TOE for the Security IC Embedded Software.

According to [PP] there is the following high-level security concern related to security service:

SC4 deficiency of random numbers.

To be able to protect these assets (SC1 to SC4) the TOE shall self-protect its TSF. Critical information about the TSF shall be protected by the development environment and the operational environment. Critical information may include:

- logical design data, physical design data, IC Dedicated Software, and configuration data,

- Initialisation data and pre-personalisation data, specific development aids, test and characterisation related data, material for software development support, and photomasks.

Note the Security IC Embedded Software is user data and shall be protected while being executed/processed and while being stored in the TOE's protected memories.

3.2 Threats

3.2.1 Standard Threats and Threats related to Security Services

Threats defined in [PP, 3.2] are listed in the following table.

Table 3: Defined Threats in [PP] and Augmentation

Threats		
Standard	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
Augmentation	T.Masquerade_TOE	Masquerade the TOE

3.2.2 Augmented Threats

Augmented Threats is listed in Table 3.

The TOE shall avert the threat "Masquerade the TOE (T.Masquerade_TOE)" as specified below. This threat is taken from package "Authentication of the Security IC" in [PP, 7.2].

T.Masquerade_TOE Masquerade the TOE

An attacker may threaten the property being a genuine TOE by producing a chip which is not a genuine TOE but wrongly identifying itself as genuine TOE sample.

The threat T.Masquerade_TOE may threaten the unique identity of the TOE as described in the P.Process-TOE or the property as being a genuine TOE without unique identity. Mitigation of masquerade requires tightening up the identification by authentication.

3.3 Organizational Security Policies

3.3.1 Standard Organizational Security Policy

Organizational Security Policies defined in [PP, 3.3] are listed in the following table.

Table 4: Defined Organizational Security Policy in [PP] and Augmentation

Organizational Security Policies		
Standard	P.Process-TOE	Identification during TOE Development and Production
Augmentation	P.Lim_Block_Loader	Limiting and Blocking the Loader Functionality
	P.Crypto-Service	Cryptographic services of the TOE
	P.Add-Functions	Additional Specific Security Functionality

3.3.2 Augmented Organizational Security Policies

Augmented Organizational Security Policies are listed in Table 4.

The organisational security policy "Limiting and Blocking the Loader Functionality (P.Lim_Block_Loader)" applies to Loader dedicated for usage in secured environment. This organisational security policy is taken from package1 "Loader dedicated for usage in secured environment only" in [PP, 7.3.1].

P.Lim_Block_Loader **Limiting and Blocking the Loader Functionality**

The composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. He limits the capability and blocks the availability of the Loader in order to protect stored data from disclosure and manipulation.

The organisational security policy "Cryptographic services of the TOE (P.Crypto-Service)" applies to cryptographic services for the Security IC Embedded Software. This organisational security policy is taken from packages for Cryptographic Services in [PP, 7.4].

P.Crypto-Service **Cryptographic services of the TOE**

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

The TOE shall provide the following specific security functionality to the Security IC Embedded Software:

- Data Encryption Standard (DES)
- Triple Data Encryption Standard (TDES)
- Advanced Encryption Standard (AES)
- Rivest Shamir Adleman (RSA)
- Elliptic Curve Cryptography (ECC)
- Diffie-Hellman (DH)
- Secure Hash Algorithm (SHA)

The IC Developer/Manufacturer must apply the policy "Additional Specific Security Functionality (P.Add-Functions)" as specified below.

P.Add-Functions Additional Specific Security Functionality

The TOE shall provide the following specific security functionality to the Security IC Embedded Software:

- PUF functionality

3.4 Assumptions

Assumptions defined in [PP, 3.4] are listed in the following table.

Table 5: Defined Assumptions in [PP]

Assumptions		
Standard	A.Process-Sec-IC	Protection during packaging, finishing and personalisation
	A.Resp-Appl	Treatment of user data of the Composite TOE

4 Security Objectives

The security objectives described below are taken from [PP, 4].

4.1 Security Objectives for the TOE

4.1.1 Standard Security Objectives for the TOE and Security Objectives related to Specific Functionality

The following security objectives for the TOE are taken from [PP, 4.1].

The user has the following standard high-level security goals related to the assets:

SG1 maintain the integrity of user data (when being executed/processed and when being stored in the TOE's memories) as well as

SG2 maintain the confidentiality of user data (when being processed and when being stored in the TOE's protected memories).

SG3 maintain the correct operation of the security services provided by the TOE for the Security IC Embedded Software.

According to [PP] there is the following high-level security goal related to specific functionality:

SG4 provide true random numbers.

Security objectives defined in [PP, 4.1] are listed in the following table.

Table 6: Defined Security Objectives for the TOE in [PP] and Augmentation

Security Objectives for the TOE		
Standard	O.Leak-Inherent	Protection against Inherent Information Leakage
	O.Phys-Probing	Protection against Physical Probing
	O.Malfunction	Protection against Malfunctions
	O.Phys-Manipulation	Protection against Physical Manipulation
	O.Leak-Forced	Protection against Forced Information Leakage
	O.Abuse-Func	Protection against Abuse of Functionality
	O.Identification	TOE Identification
	O.RND	Random Numbers
Augmentation	O.Authentication	Authentication to external entities
	O.Cap_Avail_Loader	Capability and availability of the Loader
	O.DES	Cryptographic service DES
	O.TDES	Cryptographic service Triple-DES
	O.AES	Cryptographic service AES
	O.RSA	Cryptographic service RSA
	O.ECC	Cryptographic service ECC
	O.DH	Cryptographic service DH
	O.SHA	Cryptographic service Hash function
	O.PUF	Protection using PUF

4.1.2 Augmented Security Objectives for the TOE

Augmented security objectives for the TOE are listed in Table 6.

The TOE shall provide "Authentication to external entities (O.Authentication)" as specified below. This augmented security objective is taken from package "Authentication of the Security IC" in [PP, 7.2].

O.Authentication Authentication to external entities

The TOE shall be able to authenticate itself to external entities. The Initialisation Data (or parts of them) are used for TOE authentication verification data.

The TOE shall provide "Capability and availability of the Loader (O.Cap_Avail_Loader)" as specified below. This augmented security objective is taken from package "Loader dedicated for usage in secured environment only" in [PP, 7.3.1].

O.Cap_Avail_Loader Capability and availability of the Loader

The TSF provides limited capability of the Loader functionality and irreversible termination of the Loader in order to protect stored user data from disclosure and manipulation.

The TOE shall provide “Cryptographic service DES (O.DES)” as specified below.

O.DES **Cryptographic service DES**

The TOE provides secure hardware based cryptographic services implementing the DES for encryption and decryption.

The security objective “Cryptographic service DES (O.DES)” enforces the organizational security policy P.Crypto-Service.

The TOE shall provide “Cryptographic service Triple-DES (O.TDES)” as specified below. This augmented security objective is taken from package “TDES” in [PP, 7.4.1].

O.TDES **Cryptographic service Triple-DES**

The TOE provides secure hardware based cryptographic services implementing the Triple-DES for encryption and decryption.

The security objective “Cryptographic service Triple-DES (O.TDES)” enforces the organizational security policy P.Crypto-Service.

The TOE shall provide “Cryptographic service AES (O.AES)” as specified below. This augmented security objective is taken from package “AES” in [PP, 7.4.2].

O.AES **Cryptographic service AES**

The TOE provides secure hardware based cryptographic services for the AES for encryption and decryption.

The security objective “Cryptographic service AES (O.AES)” enforces the organizational security policy P.Crypto-Service.

The TOE shall provide “Cryptographic service RSA (O.RSA)” as specified below.

O.RSA **Cryptographic service RSA**

The TOE provides secure hardware based cryptographic services for the RSA for encryption, decryption, signature generation and signature verification.

The security objective “Cryptographic service RSA (O.RSA)” enforces the organizational security policy P.Crypto-Service.

The TOE shall provide “Cryptographic service ECC (O.ECC)” as specified below.

O.ECC **Cryptographic service ECC**

The TOE provides secure hardware based cryptographic services for the ECC for signature generation, signature verification and key exchange.

The TOE shall provide “Cryptographic service DH (O.DH)” as specified below.

O.DH **Cryptographic service DH**

The TOE provides secure hardware based cryptographic services for the DH for key exchange.

The security objective “Cryptographic service DH (O.DH)” enforces the organizational security policy P.Crypto-Service.

The TOE shall provide “Cryptographic service Hash function (O.SHA)” as specified below. This augmented security objective is taken from package “Hash functions” in [PP, 7.4.3].

O.SHA **Cryptographic service Hash function**

The TOE provides secure hardware based cryptographic services for secure hash calculation.

The security objective “Cryptographic service Hash function (O.SHA)” enforces the organizational security policy P.Crypto-Service.

The TOE shall provide “Protection using PUF (O.PUF)” as specified below.

O.PUF **Protection using PUF**

The TOE provides PUF functionality in order to protect encryption/decryption of data and stored user data.

The security objective “Protection using PUF (O.PUF)” enforces the organizational security policy P.Add-Functions.

4.2 Security Objectives for the Security IC Embedded Software

Security objective for the Security IC Embedded Software defined in [PP, 4.2] is listed in the following table.

Table 7: Defined Security Objective for the Security IC Embedded Software in [PP]

Security Objective for the Security IC Embedded Software		
Standard	OE.Resp-Appl	Treatment of user data of the Composite TOE

For example the Security IC Embedded Software will not disclose security relevant user data of the Composite TOE to unauthorised users or processes when communicating with a terminal.

4.3 Security Objectives for the Operational Environment

4.3.1 Standard Security Objective for the Operational Environment

Security objectives for the Security IC Embedded Software defined in [PP, 4.3] are listed in the following table.

Table 8: Defined Security Objective for the Operational Environment in [PP] and Augmentation

Security Objectives for the Operational Environment		
Standard	OE.Process-Sec-IC	Protection during composite product manufacturing
Augmentation	OE.TOE_Auth	External entities authenticating of the TOE
	OE.Lim_Block_Loader	Limitation of capability and blocking the Loader

4.3.2 Augmented Security Objectives for the Operational Environment

Augmented Security objectives for the operational environment are listed in Table 8.

Appropriate “External entities authenticating of the TOE (OE.TOE_Auth)” must be ensured after TOE Delivery up to the Security IC end-usage (Phases 7) as specified below. This security objective for the operational Environment is taken from package “Authentication of the Security IC” in [PP, 7.2.1].

The operational environment shall provide “External entities authenticating of the TOE (OE.TOE_Auth)”.

OE.TOE_Auth External entities authenticating of the TOE

The operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE.

The threat “Masquerade the TOE (T.Masquerade_TOE)” is directly covered by the TOE security objective “Authentication to external entities (O.Authentication)” describing the proving part of the authentication and the security objective for the operational environment of the TOE “External entities authenticating of the TOE (OE.TOE_Auth)” the verifying part of the authentication.

The operational environment of the TOE shall provide “Limitation of capability and blocking the Loader (OE.Lim_Block_Loader)” as specified below. This Security Objective is taken from package 1 “Loader dedicated for usage in secured environment only” in [PP, 7.3.1]

OE.Lim_Block_Loader Limitation of capability and blocking the Loader

The Composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.

The organisational security policy Limitation of capability and blocking the Loader (P.Lim_Block_Loader) is directly implemented by the security objective for the TOE “Capability and availability of the Loader (O.Cap_Avail_Loader)” and the security objective for the TOE environment “Limitation of capability and blocking the Loader (OE.Lim_Block_Loader)”. The TOE security objective “Capability and availability of the Loader” (O.Cap_Avail_Loader)” mitigates also the threat “Abuse of Functionality “(T.Abuse-Func) if attacker tries to misuse the Loader functionality in order to manipulate security services of the TOE provided or depending on IC Dedicated Support Software or user data of the TOE as IC Embedded Software, TSF data or user data of the smartcard product.

4.4 Security Objectives Rationale

Table 9 below gives an overview, how the assumptions, threats, and organisational security policies are addressed by the objectives. The rationale justified in [PP] is not changed. Hereinafter, only the additional aspects (identified by the use of **bold type**) are justified in detail.

Table 9: Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat, or Organisational Security Policy	Security Objective	Notes
A.Resp-Appl	OE.Resp-Appl	Phase 1
A.Process-Sec-IC	OE.Process-Sec-IC	Phase 5 – 6 optional Phase 4

T.Leak-Inherent	O.Leak-Inherent	
T.Phys-Probing	O.Phys-Probing	
T.Malfunction	O.Malfunction	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Forced	O.Leak-Forced	
T.Abuse-Func	O.Abuse-Func	
T.RND	O.RND	
T.Masquerade_TOE	**O.Authentication** **OE.TOE_Auth**	**Phase 4 – 6** **optional Phase 7**
P.Process-TOE	O.Identification	Phase 2 – 3 optional Phase 4
P.Lim_Block_Loader	**O.Cap_Avail_Loader** **OE.Lim_Block_Loader**	
P.Crypto-Services	**O.DES** **O.TDES** **O.AES** **O.RSA** **O.ECC** **O.DH** **O.SHA**	
P.Add-Functions	**O.PUF**	

The justification related to the threat "Masquerade the TOE (**T.Masquerade_TOE**)" is as follows:

Since **O.Authentication** requires the TOE to implement the measure to authenticate itself to external entities.

In addition, since **OE.TOE_Auth** requires an external entity (e.g. the Composite Product Manufacturer or the Personalisation agent) to support the authentication verification mechanism and know authentication reference data of the TOE.

Consequently, the threat is covered by the above objectives.

The justification related to the organisational security policy "Limiting and Blocking the Loader Functionality (**P.Lim_Block_Loader**)" is as follows:

Since **O.Cap_Avail_Loader** requires the TOE to implement the measure to limit capability and availability of the Loader functionality.

In addition, since **OE.Lim_Block_Loader** requires the Composite Product Manufacturer to protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.

Consequently, the organisational security policy is covered by the above objectives.

The justification related to the organisational security policy "Cryptographic services of the TOE (**P.Crypto-Service**)" is as follows:

Since **O.DES**, **O.TDES**, **O.AES**, **O.RSA**, **O.ECC, O.DH** and **O.SHA** 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 above

objectives.

The justification related to the organisational security policy "Additional Specific Security Functionality (**P.Add-Functions**)" is as follows:

Since **O.PUF** require the TOE to implement exactly the same specific security functionality as required by P.Add-Functions, the organizational security policy is covered by the above objectives.

The justification of the additional threat, policy and the additional assumption show that they do not contradict to the rationale already given in [PP] for the assumptions, policy and threats defined there.

5 Extended Components Definition

There are four extended components defined 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 are used as defined and described in [PP, 5].

6 IT Security Requirements

6.1 Security Functional Requirements for the TOE

In order to define the Security Functional Requirements (SFRs), Part 2 of the Common Criteria was used.

6.1.1 Standard Security Functional Requirements for the TOE

The SFRs defined in [PP, 6.1] are shown in Table 10.

Table 10: Security Functional Requirements

Security functional requirement	
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
FDP_SDC.1	Stored data confidentiality
FDP_SDI.2	Stored data integrity monitoring and action
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
FCS_RNG.1/TRNG	Quality metric for random numbers (Class PTG.2)
FCS_RNG.1/DRNG	Quality metric for random numbers (Class DRG.3)
FIA_API.1	**Authentication proof of identity**
FCS_COP.1/DES	**Cryptographic operation - DES**
FCS_CKM.4/DES	**Cryptographic key destruction - DES**
FCS_COP.1/TDES	**Cryptographic operation - TDES**
FCS_CKM.4/TDES	**Cryptographic key destruction - TDES**
FCS_COP.1/AES	**Cryptographic operation - AES**
FCS_CKM.4/AES	**Cryptographic key destruction - AES**
FCS_COP.1/RSA	**Cryptographic operation - RSA**
FCS_CKM.4/RSA	**Cryptographic key destruction - RSA**
FCS_COP.1/ECC	**Cryptographic operation - ECC**
FCS_CKM.4/ECC	**Cryptographic key destruction - ECC**
FCS_COP.1/DH	**Cryptographic operation - DH**
FCS_COP.1/SHA	**Cryptographic operation - SHA**
FCS_COP.1/PUF-AES	**Cryptographic operation - AES using PUF**
FCS_CKM.1/PUF-AES	**Cryptographic key generation - AES using PUF**
FCS_CKM.4/PUF-AES	**Cryptographic key destruction - AES using PUF**
FCS_COP.1/PUF-ECC	**Cryptographic operation - ECC using PUF**
FCS_CKM.1/PUF-ECC	**Cryptographic key generation - ECC using PUF**
FCS_CKM.4/PUF-ECC	**Cryptographic key destruction - ECC using PUF**
FMT_LIM.1/Loader	**Limited capabilities - Loader**

FMT_LIM.2/Loader	Limited availability - Loader

Some SFRs need to be defined the selection operation and the assignment operation.

The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 extended).

FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the test process before TOE Delivery with the capability to store the Initialisation Data and/or Pre-personalisation Data and/or supplements of the Security IC Embedded Software in the ReRAM.

The TOE shall meet the requirement "Stored data confidentiality (FDP_SDC.1)" as specified below.

FDP_SDC.1	**Stored data confidentiality**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the ReRAM.

The TOE shall meet the requirement "Stored data integrity monitoring and action (FDP_SDI.2)" as specified below.

FDP_SDI.2	**Stored data integrity monitoring and action**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for bit flips on all objects, based on the following attributes: Write unlocked user area in ReRAM.
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall issue the

reset signal and CPU and all of the registers are initialized.

The TOE generates random numbers. An additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined in chapter 5. This family FCS_RNG Generation of random numbers describes the functional requirements for random number generation used for cryptographic purposes.

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

FCS_RNG.1/TRNG Quality metric for random numbers (Class PTG.2)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1/TRNG 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 [1].

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

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

(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered applied upon specified internal events. 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/TRNG The TSF shall provide 1 byte 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.

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

FCS_RNG.1/DRNG Quality metric for random numbers (Class DRG.3)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1/DRNG 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 256bit of entropy and implements: [SP-800-90A]

(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/DRNG The TSF shall provide random numbers that meet:

(DRG.3.4) The RNG, initialized with a random seed, during every startup and after 2^{48} requests, of minimal 288 bits using a PTRNG of class PTG.2, generates output for which more than 2^{51} strings of bit length 128 are mutually different with probability $w>1-2^{-16}$.

(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.

Note: This functional requirement taken from [KS2011] is seen as a refinement of the one stated in [PP].

6.1.2 Augmented Security Functional Requirements for the TOE

The additional SFRs are listed in Table 10. They are shown in **bold type.** These security functional components are listed and explained below.

(1) Authentication of the Security IC

A functional family FIA_API (Authentication Proof of Identity) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity by the TOE and enables the authentication verification by an external entity.

The TOE shall meet the requirement "Authentication Proof of Identity (FIA_API.1)" as

specified below.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a mutual authentication mechanism to prove the identity of the TOE to an external entity.

(2) Cryptographic Support

The security functional requirements FCS_COP.1/DES, FCS_COP.1/TDES, FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/ECC, FCS_COP.1/DH, FCS_COP.1/SHA, FCS_COP1/PUF-AES and FCS_COP.1/PUF-ECC require 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 dependencies are discusses in Section 6.3.

The following additional specific security functionalities are implemented in the TOE;

- Data Encryption Standard (DES)
- Triple Data Encryption Standard (TDES)
- Advanced Encryption Standard (AES)
- Rivest Shamir Adleman (RSA)
- Elliptic Curve Cryptography (ECC)
- Diffie-Hellman (DH)
- Secure Hash Algorithm (SHA)
- Advanced Encryption Standard using PUF (PUF-AES)
- Elliptic Curve Cryptography using PUF (PUF-ECC)

(a) DES operation

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

FCS_COP.1/DES Cryptographic operation - DES

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/DES The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm DES in ECB mode, CBC mode, OFB mode, CFB mode or CBC-MAC mode and cryptographic key sizes 56 bits that meet the following: [SP-800-67], [SP-800-38A].

Note: For this TOE only the side-channel resistance of DES (i.e. information leakage resistance and fault injection resistance) will be evaluated, not its cryptographic strength. If DES should be used in the security functionality of the embedded software, the corresponding strength/suitability has to be rated in the composite evaluation, in context of the attack potential claimed for the composite product.

The TOE shall meet the requirement "Cryptographic key destruction - DES (FCS_CKM.4/DES)" as specified below.

FCS_CKM.4/DES Cryptographic key destruction - DES

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/ DES The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key that meets the following: None

The FCS_COP.1/DES and FCS_CKM.4/DES meet the security objective "Cryptographic service DES (O.DES)".

(b) Triple-DES operation

The TOE shall meet the requirement "Cryptographic operation - TDES (FCS_COP.1/TDES)" 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 generation]
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 mode, CBC mode, OFB mode, CFB mode or CBC-MAC mode and cryptographic key sizes 112 bits or 168 bits that meet the following: [SP-800-67], [SP-800-38A].

The TOE shall meet the requirement "Cryptographic key destruction – TDES (FCS_CKM.4/TDES)" 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 overwriting the key that meets the following: None

The FCS_COP.1/TDES and FCS_CKM.4/TDES meet the security objective "Cryptographic service Triple-DES (O.TDES)".

(c) AES operation

The TOE shall meet the requirement "Cryptographic operation - AES (FCS_COP.1/AES)" 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 decryption and encryption in accordance with a specified cryptographic algorithm AES in ECB mode, CBC mode, OFB mode, CFB mode, CTR mode, CBC-MAC mode or CMAC mode and cryptographic key sizes 128 bits, 192 bits or 256 bits that meet the following: [FIPS-197], [SP-800-38A], [SP-800-38B].

The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4) - AES" 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 overwriting the key that meets the following: None.

The FCS_COP.1/AES and FCS_CKM.4/AES meet the security objective "Cryptographic service AES (O.AES)".

(d) RSA operation

The TOE shall meet the requirement "Cryptographic operation - RSA (FCS_COP.1/RSA)" 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 generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/RSA The TSF shall perform decryption, encryption, signature generation, signature verification and key exchange in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes 1024 bits, 2048 bits, 3072 bits or 4096 bits that meet the following: [RFC3447], [SP-800-56A], [FIPS186-4].

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

FCS_CKM.4/RSA Cryptographic key destruction - RSA

Hierarchical to: No other components.

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

FCS_CKM.4.1/RSA The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key that meets the following: None.

The FCS_COP.1/RSA and FCS_CKM.4/RSA meet the security objective "Cryptographic service RSA (O.RSA)".

(e) ECC operation

The TOE shall meet the requirement "Cryptographic operation - ECC (FCS_COP.1/ECC)" as specified below.

FCS_COP.1/ECC Cryptographic operation - ECC

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/ECC The TSF shall perform signature generation, signature verification and key exchange in accordance with a specified cryptographic algorithm ECC and cryptographic key sizes 160 bits, 224 bits, 384 bits or 521 bits that meet the following: [SEC1], [FIPS186-4].

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

FCS_CKM.4/ECC Cryptographic key destruction - ECC

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/ECC The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key that meets the following: None.

The FCS_COP.1/ECC and FCS_CKM.4/ECC meet the security objective "Cryptographic service ECC (O.ECC)".

(f) DH operation

The TOE shall meet the requirement “Cryptographic operation - DH (FCS_COP.1/DH)” as specified below.

FCS_COP.1/DH	**Cryptographic operation - DH**
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/DH	The TSF shall perform key exchange in accordance with a specified cryptographic algorithm DH and cryptographic key sizes (See in Table 16) that meet the following: [PKCS #3].

The FCS_COP.1/DH meet the security objective “Cryptographic service DH (O.DH)”.

(g) SHA operation

The TOE shall meet the requirement "Cryptographic operation - SHA (FCS_COP.1/SHA)" as specified below.

FCS_COP.1/SHA Cryptographic operation - SHA

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/SHA The TSF shall perform hashing in accordance with a specified cryptographic algorithm SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, HMAC-SHA1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384 or HMAC-SHA-512 and cryptographic key sizes (See in Table 16) that meet the following: [FIPS180-4], [FIPS198-1].

The FCS_COP.1/SHA meet the security objective "Cryptographic service SHA (O.SHA)".

(h) AES operation using PUF

The TOE shall meet the requirement "Cryptographic operation - AES using PUF (FCS_COP.1/PUF-AES)" as specified below.

FCS_COP.1/PUF-AES Cryptographic operation - AES using PUF

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/PUF-AES The TSF shall perform decryption and encryption based on PUF in accordance with a specified cryptographic algorithm AES in ECB mode, CBC mode, CTR mode, OFB mode, CBC-MAC mode or CMAC mode and cryptographic key sizes 128 bits, 192 bits or 256 bits that meet the following: [FIPS-197], [SP-800-38A], [SP-800-38B].

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1) - AES using PUF" as specified below.

FCS_CKM.1/PUF-AES Cryptographic key generation - AES using PUF

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/PUF-AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm key derivation function based on PUF and specified cryptographic key sizes 128 bits, 192 bits or 256 bits that meet the following: [PUF-KDS].

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

FCS_CKM.4/PUF-AES Cryptographic key destruction – AES using PUF

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/PUF-AES The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key that meets the following: None.

The FCS_COP.1/PUF-AES, FCS_CKM.1/PUF-AES and FCS_CKM.4/PUF-AES meet the security objective “Protection using PUF (O.PUF)”.

(i) ECC operation using PUF

The TOE shall meet the requirement "Cryptographic operation - ECC using PUF (FCS_COP.1/PUF-ECC)" as specified below.

FCS_COP.1/PUF-ECC Cryptographic operation - ECC using PUF

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/PUF-ECC The TSF shall perform signature generation and key exchange based on PUF in accordance with a specified cryptographic algorithm ECC and cryptographic key sizes 160 bits, 224 bits, 384 bits or 521 bits that meet the following: [SEC1], [FIPS186-4].

The TOE shall meet the requirement "Cryptographic key generation (FCS_CKM.1) - ECC using PUF" as specified below.

FCS_CKM.1/PUF-ECC Cryptographic key generation - ECC using PUF

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/PUF-ECC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm key derivation function based on PUF and specified cryptographic key sizes 160 bits, 224 bits, 384 bits or 521 bits that meet the following: [PUF-KDS].

The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4) – ECC using PUF" as specified below.

FCS_CKM.4/PUF-ECC Cryptographic key destruction - ECC using PUF

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/PUF-ECC The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwriting the key that meets the following: None.

The FCS_COP.1/PUF-ECC, FCS_CKM.1/PUF-ECC and FCS_CKM.4/PUF-ECC meet the security objective “Protection using PUF (O.PUF)”.

(3) Loader

The Loader may be used to load data into the ReRAM memory after delivery of the TOE. The Loader is intended to use in operational environments which are under control of the owner of the loaded data or its subcontractor. This is typically the Composite Product Manufacturer or more specifically the IC Packaging Manufacturer (cf. chapter 1.4.2).

The TOE Functional Requirement "Limited capabilities - Loader (FMT_LIM.1/Loader)" is specified as follows.

FMT_LIM.1/Loader Limited capabilities - Loader

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1/Loader The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Loader functionality after the end of Phase 3 does not allow stored user data to be disclosed or manipulated by unauthorized user.

The TOE Functional Requirement "Limited availability - Loader (FMT_LIM.2/Loader)" is specified as follows.

FMT_LIM.2/Loader Limited availability - Loader

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1/Loader The TSF shall be designed in a manner that limits its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: The TSF prevents deploying the Loader functionality after the end of Phase 3.

The security objective "Capability and availability of the Loader (O.Cap_Avail_Loader) is directly covered by the security functional requirements FMT_LIM.1/Loader and FMT_LIM.2/Loader.

6.2 Security Assurance Requirements for the TOE

The assurance level for this Security Target is **EAL5** augmented with the following components:

- ALC_DVS.2
- AVA_VAN.5

The assurance requirements are given in the following Table 11.
Augmentations compared to [PP] are marked in **bold type**.

Table 11: Assurance Requirements

Assurance Class	Assurance Family	Family name	Level	
			[PP]	[ST]
Development (Class ADV)	ADV_ARC	Architectural Design	1	1
	ADV_FSP	**Functional Specification**	**4**	**5**
	ADV_IMP	Implementation Representation	1	1
	ADV_INT	**TSF Internals**	**-**	**2**
	ADV_TDS	**TOE Design**	**3**	**4**
Guidance documents (Class AGD)	AGD_OPE	Operational User Guidance	1	1
	AGD_PRE	Preparative User Guidance	1	1
Life-cycle support (Class ALC)	ALC_CMC	CM Capabilities	4	4
	ALC_CMS	**CM Scope**	**4**	**5**
	ALC_DEL	Delivery	1	1
	ALC_DVS	Development Security	2	2
	ALC_LCD	Life-Cycle Definition	1	1
	ALC_TAT	**Tools and Techniques**	**1**	**2**
Security Target evaluation (Class ASE)	ASE_CCL	Conformance Claims	1	1
	ASE_ECD	Extended Components Definition	1	1
	ASE_INT	ST Introduction	1	1
	ASE_OBJ	Security Objectives	2	2
	ASE_REQ	Derived Security Requirements	2	2
	ASE_SPD	Security Problem Definition	1	1
	ASE_TSS	TOE Summary Specification	1	1
Tests (Class ATE)	ATE_COV	Coverage	2	2
	ATE_DPT	**Depth**	**2**	**3**
	ATE_FUN	Functional Tests	1	1
	ATE_IND	Independent Testing	2	2
Vulnerability assessment (Class AVA)	AVA_VAN	Vulnerability Analysis	5	5

6.2.1 Refinements of the TOE Assurance Requirements

Refinements list of the assurance requirements taken from [PP, 6.2.1] is shown in Table 12. For details of the refinements refer to [PP].

Table 12: Refinements list of Assurance Requirements

Refinements of the assurance requirements	Assurance Family	Augmented From [PP] to [ST]
Refinements regarding Delivery procedure	ALC_DEL	
Refinements regarding Development Security	ALC_DVS	
Refinement regarding CM scope	ALC_CMS	✔
Refinement regarding CM capabilities	ALC_CMC	
Refinements regarding Security Architecture	ADV_ARC	
Refinements regarding Functional Specification	ADV_FSP	✔
Refinements regarding Implementation Representation	ADV_IMP	
Refinement regarding Test Coverage	ATE_COV	
Refinement regarding User Guidance	AGD_OPE	
Refinement regarding Preparative User Guidance	AGD_PRE	
Refinement regarding Vulnerability Analysis	AVA_VAN	

Five refinements from [PP] have to be discussed since the assurance level of the corresponding component is increased in the Security Target.

CM Scope (ALC_CMS)

The refinement from [PP] can be applied even to the chosen assurance component ALC_CMS.5. The assurance component ALC_CMS.4 is extended to ALC_CMS.5 with regard to the scope of the configuration list. The refinement is not touched in terms of this matter.

Functional Specification (ADV_FSP)

The refinement from [PP] can be applied even to the chosen assurance component ADV_FSP.5. The assurance component ADV_FSP.4 is extended to ADV_FSP.5 with aspects regarding (i) the description of TSFI using a semi-formal style, and (ii) error messages that do not result from an invocation of a TSFI and the rationale for them.
The refinement provides the detailed description content of functional specification, and is not touched in terms of those matters.

6.3 Security Requirements Rationale

6.3.1 Rationale for the Security Functional Requirements

Table 13 gives an overview, how the SFRs are combined to meet the security objectives. The rationale justified in [PP, 6.3] is not changed. Hereinafter, only the additional

aspects (identified by the use of **bold type**) are justified in detail.

Table 13: Security Requirements versus Security Objectives

Objective	TOE Security Functional and Assurance Requirements
O.Leak-Inherent	- FDP_ITT.1 “Basic internal transfer protection” - FPT_ITT.1 “Basic internal TSF data transfer protection” - FDP_IFC.1 “Subset information flow control”
O.Phys-Probing	- FDP_SDC.1 “Stored data confidentiality” - FPT_PHP.3 “Resistance to physical attack”
O.Malfunction	- FRU_FLT.2 “Limit fault tolerance” - FPT_FLS.1 “Failure with preservation of secure state”
O.Phys-Manipulation	- FDP_SDI.2 “Stored data integrity monitoring and action” - FPT_PHP.3 “Resistance to physical attack”
O.Leak-Forced	All requirements listed for O.Leak-Inherent - FDP_ITT.1 “Basic internal transfer protection” - FPT_ITT.1 “Basic internal TSF data transfer protection” - FDP_IFC.1 “Subset information flow control” plus those listed for O.Malfunction and O.Phys-Manipulation - FRU_FLT.2 “Limit fault tolerance” - FPT_FLS.1 “Failure with preservation of secure state” - FPT_PHP.3 “Resistance to physical attack”
O.Abuse-Func	- FMT_LIM.1 “Limited capabilities” - FMT_LIM.2 “Limited availability” plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced - FDP_ITT.1 “Basic internal transfer protection” - FPT_ITT.1 “Basic internal TSF data transfer protection” - FDP_IFC.1 “Subset information flow control” - FPT_PHP.3 “Resistance to physical attack” - FRU_FLT.2 “Limit fault tolerance” - FPT_FLS.1 “Failure with preservation of secure state”
O.Identification	- FAU_SAS.1 “Audit Storage”
O.RND	- FCS_RNG.1/TRNG “Quality metric for random numbers (Class PTG.2)” - FCS_RNG.1/DRNG “Quality metric for random numbers (Class DRG.3)” plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced“ - FDP_ITT.1 “Basic internal transfer protection” - FPT_ITT.1 “Basic internal TSF data transfer protection” - FDP_IFC.1 “Subset information flow control” - FPT_PHP.3 “Resistance to physical attack” - FRU_FLT.2 “Limit fault tolerance” - FPT_FLS.1 “Failure with preservation of secure state”
O.Authentication	**- FIA_API.1 “Authentication Proof of Identity”**
OE.TOE_Auth	not applicable
O.DES	**- FCS_COP.1/DES “Cryptographic operation - DES”** **- FCS_CKM.4/DES “Cryptographic key destruction - DES”**
O.TDES	**- FCS_COP.1/TDES “Cryptographic operation - TDES”** **- FCS_CKM.4/TDES “Cryptographic key destruction - TDES”**
O.AES	**- FCS_COP.1/AES “Cryptographic operation - AES”**

Objective	TOE Security Functional and Assurance Requirements
	- FCS_CKM.4/AES "Cryptographic key destruction - AES"
O.RSA	**- FCS_COP.1/RSA "Cryptographic operation - RSA"** **- FCS_CKM.4/RSA "Cryptographic key destruction - RSA"**
O.ECC	**- FCS_COP.1/ECC "Cryptographic operation - ECC"** **- FCS_CKM.4/ECC "Cryptographic key destruction - ECC"**
O.DH	**- FCS_COP.1/DH "Cryptographic operation - DH"**
O.SHA	**- FCS_COP.1/SHA "Cryptographic operation - SHA"**
O.PUF	**- FCS_COP.1/PUF-AES "Cryptographic operation - AES using PUF"** **- FCS_CKM.1/PUF-AES "Cryptographic key generation - AES using PUF"** **- FCS_CKM.4/PUF-AES "Cryptographic key destruction - AES using PUF"** **- FCS_COP.1/PUF-ECC "Cryptographic operation - ECC using PUF"** **- FCS_CKM.1/PUF-ECC "Cryptographic key generation - ECC using PUF"** **- FCS_CKM.4/PUF-ECC "Cryptographic key destruction - ECC using PUF"**
OE.Resp-Appl	not applicable
O.Cap_Avail_Loader	**- FMT_LIM.1/Loader "Limit capabilities - Loader"** **- FMT_LIM.2/Loader "Limit availability - Loader"**
OE.Lim_Block_Loader	**not applicable**
OE.Process-Sec-IC	not applicable

The justification related to the security objective "Authentication to external entities (O.Authentication)" is as follows:

The SFR "Authentication Proof of Identity (FIA_API.1)" exactly requires the function to be implemented which is demanded by O.Authentication. Therefore, FIA_API.1 is suitable to meet the security objective.

The justification related to the security objective "Cryptographic service DES (O.DES)" is as follows:

The SFR "Cryptographic operation - DES (FCS_COP.1/DES)" exactly requires the function to be implemented which is demanded by O.DES. Therefore, FCS_COP.1/DES is suitable to meet the security objective.

The justification related to the security objective "Cryptographic service Triple-DES (O.TDES)" is as follows:

The SFR "Cryptographic operation - TDES (FCS_COP.1/TDES)" exactly requires the function to be implemented which is demanded by O.TDES. Therefore, FCS_COP.1/TDES is suitable to meet the security objective.

The justification related to the security objective "Cryptographic service AES (O.AES)" is as follows:

The SFR "Cryptographic operation - AES (FCS_COP.1/AES)" exactly requires the function to be implemented which is demanded by O.AES. Therefore,

FCS_COP.1/AES is suitable to meet the security objective.

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

The SFR “Cryptographic operation - RSA (FCS_COP.1/RSA)” exactly requires the function to be implemented which is demanded by O.RSA. Therefore, FCS_COP.1/RSA is suitable to meet the security objective.

The justification related to the security objective “Cryptographic service ECC (O.ECC)” is as follows:

The SFR “Cryptographic operation - ECC (FCS_COP.1/ECC)” exactly requires the function to be implemented which is demanded by O.ECC. Therefore, FCS_COP.1/ECC is suitable to meet the security objective.

The justification related to the security objective “Cryptographic service DH (O.DH)” is as follows:

The SFR “Cryptographic operation - DH (FCS_COP.1/DH)” exactly requires the function to be implemented which is demanded by O.DH. Therefore, FCS_COP.1/DH is suitable to meet the security objective.

The justification related to the security objective “Cryptographic service SHA (O.SHA)” is as follows:

The SFR “Cryptographic operation - SHA (FCS_COP.1/SHA)” exactly requires the function to be implemented which is demanded by O.SHA. Therefore, FCS_COP.1/SHA is suitable to meet the security objective.

The justification related to the security objective “Protection using PUF (O.PUF)” is as follows:

The SFR “Cryptographic operation - AES using PUF (FCS_COP.1/PUF-AES)” and “Cryptographic operation - ECC using PUF (FCS_COP.1/PUF-ECC)” exactly require those functions to be implemented which is demanded by O.PUF. Therefore, FCS_COP.1/PUF-AES and FCS_COP.1/PUF-ECC are suitable to meet the security objective.

Nevertheless, the developer of the Security IC Embedded Software must ensure that the additional functions are used as specified and that the user data processed by these functions are protected as defined for the application context. These issues are addressed by the specific SFRs:

- [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.

All these requirements have to be fulfilled to support OE.Resp-Appl for FCS_COP.1 in each cryptographic algorithm.

The usage of cryptographic algorithms requires the use of appropriate keys. Otherwise these cryptographic functions do not provide security. The keys have to be unique with a very high probability, and must have a certain cryptographic strength etc. In case of a key import into the TOE (which is usually after TOE delivery) it has to be ensured that quality and confidentiality are maintained. Keys for DES, TDES, AES, RSA ECC, DH, SHA, AES using PUF and ECC using PUF are provided by the environment.
In this ST the objective for the environment OE.Resp-Appl has been clarified. The Security IC Embedded Software defines the use of the cryptographic functions FCS_COP.1 provided by the TOE. The requirements for the environment FDP_ITC.1, FDP_ITC.2, FCS_CKM.1 and FCS_CKM.4 support an appropriate key management. These security requirements are suitable to meet OE.Resp-Appl.

The justification related to the security objective "Capability and Availability of the Loader (O.Cap_Avail_Loader)" is as follows:

> According to O.Cap_Avail_Loader, the TOE must limit capability and availability of the loader function to protect stored user data from disclosure and manipulation. The SFR "Limit capabilities – Loader (FMT_LIM.1/Loader)" exactly requires the function to limit capability of the loader, and the SFR "Limit availability – Loader (FMT_LIM.2/Loader)" exactly requires the function to limit availability of the loader. Therefore, FMT_LIM.1/Loader and FMT_LIM.2/Loader are suitable to meet the security objective.

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

6.3.2 Dependencies of Security Functional Requirements

Table 14 lists the SFRs defined in this ST, their dependencies and whether they are satisfied by other security requirements defined in this ST.

This rationale is adopted from [PP, 6.3.2], with additional aspects (identified by the use of **bold type**).

Table 14: Dependencies of the Security Functional Requirements

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
FRU_FLT.2	FPT_FLS.1	Yes
FPT_FLS.1	None	No dependency
FMT_LIM.1	FMT_LIM.2	Yes
FMT_LIM.2	FMT_LIM.1	Yes
FAU_SAS.1	None	No dependency
FDP_SDC.1	None	No dependency
FDP_SDI.2	None	No dependency
FPT_PHP.3	None	No dependency

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes
FPT_ITT.1	None	No dependency
FDP_IFC.1	FDP_IFF.1	See discussion in [PP, 6.3.2]
FCS_RNG.1/TRNG	None	No dependency
FCS_RNG.1/DRNG	None	No dependency
FIA_API.1	**None**	**No dependency**
FCS_COP.1/DES	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4**	**Yes (by the environment)**
FCS_CKM.4/DES	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1**	**Yes (by the environment)**
FCS_COP.1/TDES	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4**	**Yes (by the environment)**
FCS_CKM.4/TDES	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1**	**Yes (by the environment)**
FCS_COP.1/AES	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4**	**Yes (by the environment)**
FCS_CKM.4/AES	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1**	**Yes (by the environment)**
FCS_COP.1/RSA	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4**	**Yes (by the environment)**
FCS_CKM.4/RSA	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1**	**Yes (by the environment)**
FCS_COP.1/ECC	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4**	**Yes (by the environment)**
FCS_CKM.4/ECC	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1**	**Yes (by the environment)**
FCS_COP.1/DH	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4**	**Yes (by the environment)**
FCS_COP.1/SHA	**FDP_ITC.1 or FDP_ITC.2**	**Yes (by the environment)**
FCS_COP.1/PUF-AES	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4**	**Yes (by the environment)**
FCS_CKM.1/PUF-AES	**FCS_CKM.2 or FCS_COP.1 FCS_CKM.4**	**Yes (by the environment)**
FCS_CKM.4/PUF-AES	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1**	**Yes (by the environment)**
FCS_COP.1/PUF-ECC	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4**	**Yes (by the environment)**
FCS_CKM.1/PUF-ECC	**FCS_CKM.2 or FCS_COP.1 FCS_CKM.4**	**Yes (by the environment)**
FCS_CKM.4/PUF-ECC	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1**	**Yes (by the environment)**
FMT_LIM.1/Loader	**FMT_LIM.2**	**Yes**

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
FMT_LIM.2/Loader	FMT_LIM.1	Yes

The dependencies defined for FCS_COP.1 and FCS_CKM.4 in each cryptographic algorithm are addressed in the environment through the presence of OE.Resp-Appl.
These dependencies all address the appropriate management of cryptographic keys used by the specified cryptographic function and are not part of the [PP]. The requirements concerning key management shall be fulfilled by the environment since the Security IC Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE.

6.3.3 Rationale for the Assurance Requirements

The assurance level EAL5 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 were chosen in order to meet assurance expectations explained in the following paragraphs.

An assurance level of EAL5 with the augmentations ALC_DVS.2 and AVA_VAN.5 is required for this type of TOE since it is intended to defend against sophisticated attacks. This evaluation assurance package was selected to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defense against such attacks, the evaluators should have access to the low level design and source code.
Additionally the mandatory technical document “Application of Attack Potential to Smartcards” [JHAS] shall be taken as a basis for the vulnerability analysis of the TOE.

6.3.4 Security Requirements are Internally Consistent

In addition to the discussion in [PP, 6.3.4], some SFRs (identified by the use of **bold type** in Table 14) are newly added to this ST. The additional rationale to deal with those requirements is as follows.

The security functional requirement FIA_API.1 ensures that the TOE is genuine to external entities by authentication mechanism. This functionality makes it difficult to realize masquerade of the genuine TOE by an attacker.

The cryptographic function helps to protect other security features or functions including those being implemented in the Security IC Embedded Software. The security functional requirements FCS_COP.1/DES, FCS_COP.1/TDES, FCS_COP.1/AES, FCS_COP.1/RSA, FCS_COP.1/ECC, FCS_COP.1/DH, FCS_COP.1/SHA, FCS_COP.1/PUF-AES and FCS_COP.1/PUF-ECC require executing the cryptographic algorithms.
The security functional requirements FCS_CKM.1/PUF-AES and FCS_CKM.1/PUF-ECC require the measures generating cryptographic key for more

secure operation.
The security functional requirements FCS_CKM.4/DES, FCS_CKM.4/TDES, FCS_CKM.4/AES, FCS_CKM.4/RSA, FCS_CKM.4/ECC, FCS_CKM.4/PUF-AES and FCS_CKM.4/PUF-ECC require the measures destroying cryptographic key for more secure operation.
Therefore, these SFRs support the secure implementation and operation of DES, TDES, AES, RSA, ECC, DH, SHA, AES using PUF and ECC using PUF.

The combination of the security functional requirements FMT_LIM.1/Loader and FMT_LIM.2/Loader ensures that these additional functions cannot be abused by an attacker (i) to disclose or manipulate user data of the Composite TOE, (ii) to manipulate security features or services of the TOE or the Security IC Embedded Software or (iii) to enable other attacks on the assets. Hereby the binding between these two security function requirements is very important and they provide sufficient security.

7 TOE Summary Specification

7.1 TOE Security Functionality

7.1.1 TOE Security Features

(1) SF.RNG: Random Number Generator

The TOE generates true random numbers, and meets the class PTG.2 of [AIS31]. Moreover, the TOE generates deterministic random numbers, and meets the class DRG.3 of [AIS31].
The TOE implements this security function by means of a random number generator working stable within the limits guaranteed by the security function SF.FAS.
The generated random numbers are used internally and can be used by the Security IC Embedded Software for e.g. the generation of cryptographic keys.

(2) SF.FAS: Filters and Sensors

The TOE prevents any malfunction and ensures its correct operation.

The TOE incorporates effective filters on the essential signal lines so as to eliminate the cause for possible faults such as glitches. Moreover, the TOE has sensors to detect a variety of operating conditions that could lead to malfunctions, including frequency, voltages and temperatures. These filters and sensors functions are listed in the following Table 15.

Table 15: Filter and Sensor functions

Filter / Sensor	Functions
Voltage Sensor	Power-supply voltage anomaly detection
Voltage Glitch Sensor	Glitch on power-supply voltage detection
Frequency Sensor	Clock frequency anomaly detection
Clock Filter	- High frequency clock removal - Glitch on Clock removal
Reset Filter	Glitch on Reset Signal removal
Light Sensor	Light detection
Temperature Sensor	Temperature detection

If any abnormality is detected on sensors, CPU and all registers are initialized.

In addition, the TOE starts the self-test upon power-up at all times. If any abnormality is detected on the filters or sensors, CPU and all registers are initialized. It is therefore ensured that these filters and sensors properly operate.

All the instructions that are executed in CPU are being monitored. When an

illegal instruction is referenced in the CPU, it indicates a corruption due to an attack. In this case the TOE enters the reset state and CPU and all registers are initialized.

Parameter that is set up to IC Dedicated Software is checked. If it is an unauthorized value, CPU and all registers are initialized.

(3) SF.PHY: Physical Tamper Resistance

The TOE comprises various physical measures that make tamper attacks more difficult and to protect thereby data stored in the SRAM and ReRAM such as user data, Security IC Embedded Software and other critical operating information (TSF data in particular) from being modified by FIB etc. or disclosed using the physical probing.

One of the countermeasures is memory scramble.

Furthermore, sensing shield is embedded. If any abnormal physical operation is detected, CPU and all registers are initialized.

The critical data as mentioned above is protected using such secured mechanism.

(4) SF.DPR: Data Protection

The TOE may be susceptible to physical attacks: therefore it has potential risk of internal data leakage. For example, if an attacker collects measurements on the signals being used in processing user data and/or TSF data, and performs complex computation processes on them, an attacker may obtain their confidential data in the TOE thereby or possibly directly from ReRAM.
To avoid such unwanted leakage, particularly to protect against fault analysis attack, power analysis attack and timing attack, the TOE comprises the security measures:

(5) SF.MCT: Mode Control

For chip, there are test mode and normal mode. Factory setting is normal mode.

After the execution of all tests at Phase 3, test mode entry becomes impossible and the transition from normal mode to test mode falls into disuse.

Under the mode control as described above, abuse of test functions is prevented after TOE delivery.

(6) SF.CRPT: Cryptography

The TOE realizes the DES, TDES, AES, RSA, ECC, DH and SHA. Standards of each algorithm are followings:

Table 16: Cryptographic Functionalities

Algorithm	Key length	Standard
DES	56 bits	[SP-800-67] [SP-800-38A]
TDES	112 bits, 168 bits	[SP-800-67] [SP-800-38A]
AES	128 bits, 192 bits, 256 bits	[FIPS197] [SP-800-38A] [SP-800-38B]
RSA	1024 bits, 2048 bits, 3072 bits, 4096 bits	[RFC3447] [SP-800-56A] [FIPS186-4]
ECC	160 bits, 224 bits 384 bits, 521 bits	[SEC1] [FIPS186-4]
DH	32bits - 4096bits	[PKCS #3]
SHA	HMAC-SHA-1: 80 - 512bits HMAC-SHA-224: 112 - 512bits HMAC-SHA-256: 128 - 512bits HMAC-SHA-384: 128 - 512bits HMAC-SHA-512: 128 - 512bits	[FIPS180-4] [FIPS198-1]

(7) SF.ACC: Access Control

All addresses are being monitored by this security function.
Accessible/inaccessible area is controlled.
When an address is specified to an access-inhibited area, it indicates a corruption due to an attack. In this case the TOE enters the reset state and CPU and all registers are initialized

(8) SF.ID: Identification

In the last function testing at Phase 3, some data to uniquely identify the TOE are injected into the write lock area of ReRAM. This sort of information can't be rewritten. Therefore the data like ID written down in the TOE isn't changed.

(9) SF.PUF: Protection using PUF

The TOE provides a mechanism to protect user data against unintended leakage using PUF data.
The data stored in ReRAM are encrypted with a key derived from the PUF data.
Moreover, AES encryption/decryption and ECC with a key derived from the PUF data are executed.

7.2 TOE Summary Specification Rationale

Table 17 below gives an overview, how the SFRs are fulfilled by TOE security functions. This security target (ST-Lite) can't provide the rationale for the specification of TOE summary.

Table 17: Mapping of SFR to TOE Security Function

SFR \ TSF	SF.RNG	SF.FAS	SF.PHY	SF.DPR	SF.MCT	SF.CRPT	SF.ACC	SF.ID	SF.PUF
FRU_FLT.2		✓							
FPT_FLS.1		✓							
FMT_LIM.1					✓				
FMT_LIM.2					✓				
FAU_SAS.1								✓	
FDP_SDC.1			✓	✓					✓
FDP_SDI.2			✓						
FPT_PHP.3			✓	✓					✓
FDP_ITT.1				✓					
FPT_ITT.1				✓					
FDP_IFC.1				✓					
FCS_RNG.1/TRNG	✓								
FCS_RNG.1/DRNG	✓								
FIA_API.1								✓	
FCS_COP.1/DES						✓			
FCS_CKM.4/DES						✓			
FCS_COP.1/TDES						✓			
FCS_CKM.4/TDES						✓			
FCS_COP.1/AES						✓			
FCS_CKM.4/AES						✓			
FCS_COP.1/RSA						✓			
FCS_CKM.4/RSA						✓			

FCS_COP.1/ECC						✓			
FCS_CKM.4/ECC						✓			
FCS_COP.1/DH						✓			
FCS_COP.1/SHA						✓			
FCS_COP.1/PUF-AES									✓
FCS_CKM.1/PUF-AES									✓
FCS_CKM.4/PUF-AES									✓
FCS_COP.1/PUF-ECC									✓
FCS_CKM.1/PUF-ECC									✓
FCS_CKM.4/PUF-ECC									✓
FMT_LIM.1/Loader							✓		
FMT_LIM.2/Loader							✓		

8 Annex

8.1 Glossary of Vocabulary

Terms	Definitions
Application Data	All data managed by the Security IC Embedded Software in the application context. Application data comprise all data in the final Security IC.
Composite Product Manufacturer	The Composite Product Manufacturer has the following roles (i) the Security IC Embedded Software Developer (Phase 1), (ii) the Composite Product Integrator (Phase 5) and (iii) the Personaliser (Phase 6). If the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice) he has the role of the IC Packaging Manufacturer (Phase 4) in addition. The customer of the TOE Manufacturer who receives the TOE during TOE Delivery. The Composite Product Manufacturer includes the Security IC Embedded Software developer and all roles after TOE Delivery up to Phase 6 (refer to section 1.4.2 and [PP, 7.1.1]).
End-consumer	User of the Composite Product in Phase 7.
IC Dedicated Software	IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
Initialization Data	Initialization Data defined by the TOE Manufacturer to identify the TOE and to keep track of the Security IC's production and further life-cycle phases are considered as belonging to the TSF data. These data are for instance used for traceability and for TOE identification (identification data).
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
Pre-personalization Data	Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases.
Security IC	(as used in this Protection Profile) Composition of the TOE, the Security IC Embedded Software, User Data and the package (the Security IC carrier).

Terms	Definitions
Security IC Embedded Software	Software embedded in a smart card IC and normally not being developed by the IC Designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3 or in later phases of the Security IC product life-cycle. Some part of that software may actually implement a Security IC application others may provide standard services. Nevertheless, this distinction doesn't matter here so that the Security IC Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.
Test Features	All features and functions which are designed to be used before TOE Delivery only and delivered as part of the TOE.
TOE Delivery	The period when the TOE is delivered which is either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.
TOE Manufacturer	The TOE Manufacturer must ensure that all requirements for the TOE and its development and production environment are fulfilled. The TOE Manufacturer has the following roles: (i) IC Developer (Phase 2) and (ii) IC Manufacturer (Phase 3). If the TOE is delivered after Phase 4 in form of packaged products, he has the role of the (iii) IC Packaging Manufacturer (Phase 4) in addition.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE. This includes information about the TOE's configuration, if any is coded in non-volatile non-programmable memories (ROM), in specific circuitry, in non-volatile programmable memories (for instance E^2PROM) or a combination thereof.
User Data	All data managed by the Security IC Embedded Software in the application context. User data comprise all data in the final smart card IC except the TSF data.

8.2 List of Abbreviations

Abbreviations	Meanings
AES	Advanced Encryption Standard
API	Application Programming Interface
ASK	Amplitude Shift Keying
CBC	Cipher Block Chaining
CC	Common Criteria Version 3.1
DES	Data Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EB	Electron Beam
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
FIB	Focused Ion Beam
DH	Diffie-Hellman
IC	Integrated Circuit
IT	Information Technology
MAC	Message Authentication Code
NMI	Non-Maskable Interrupt
NTCJ	Nuvoton Technology Corporation Japan
PP	Protection Profile
PUF	Physical Unclonable Function
ReRAM	Resistive Random Access Memory
RF	Radio Frequency
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
SPI	Serial Peripheral Interface
ST	Security Target
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation
Triple-DES	Triple Data Encryption Standard
TSF	TOE Security functionality

8.3 Related Documents

Abbreviated name	References
[AGD-SES]	MN67S3C0 Smart Card IC Operational User Guidance, - for Security IC Embedded Software Developer -
[AGD-CM]	MN67S3C0 Smart Card IC Preparative User Guidance, - for Card Manufacturer -
[PUF-KDS]	MN67S3C0 Smart Card IC PUF Key Derivation Specification
[AHB-Lite]	AMBA3 AHB-Lite Protocol v1.0 Specification
[AIS31]	Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, AIS31, Version 3.0, 15.05.2013
[CC]	Common Criteria for Information Technology Security Evaluation; Version 3.1
[CC-1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1 Revision 5
[CC-2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1 Revision 5
[CC-3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1 Revision 5
[FIPS180-4]	U.S. Department of Commerce / National Institute of Standards and Technology, Secure Hash Standard (SHS), FIPS PUB 180-4, March 2012
[FIPS186-4]	U.S. Department of Commerce / National Institute of Standards and Technology, Digital Signature Standard (DSS), FIPS PUB 186-4, Issued July 2013
[FIPS197]	U.S. Department of Commerce / National Institute of Standards and Technology, Advanced Encryption Standard (AES), FIPS PUB 197, 2001 November 26
[FIPS198-1]	U.S. Department of Commerce / National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), FIPS PUB 198-1, July 2008
[ISO/IEC14443-2]	Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface
[ISO/IEC14443-3]	Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision
[ISO/IEC9797-1]	ISO/IEC 9797-1 Information technology - Security techniques - Message Authentication Codes (MACs) – Part1: Mechanisms using a block cipher
[JHAS]	Joint Interpretation Library, Application of Attack Potential to Smartcards, Version 2.9, January 2013
[JISX6319-4]	JAPANESE INDUSTRIAL STANDARD, Specification of implementation for integrated circuit(s) cards – Part 4: High speed proximity cards JISX6319-4: 2010
[KS2011]	A proposal for: Functionality classes for random number generators, Version 2.0, 18 September 2011

Abbreviated name	References
[PP]	Smartcard IC Platform Protection Profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084-2014.
[RFC3447]	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, published in 2003
[SEC1]	SEC 1: Elliptic Curve Cryptography, May 21, 2009, Version 2.0
[SP-800-38A]	U.S. Department of Commerce / National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, NIST Special Publication 800-38A, 2001 Edition
[SP-800-38B]	U.S. Department of Commerce / National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, The CMAC Mode for Authentication, NIST Special Publication 800-38B, 2005 Edition
[SP-800-56]	U.S. Department of Commerce / National Institute of Standards and Technology, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication 800-56A, Revision 2, May 2013
[SP-800-67]	U.S. Department of Commerce / National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST Special Publication 800-67, Revision 1, Revised January 2012
[PKCS #3]	PKCS #3: Diffie-Hellman Key-Agreement Standard, RSA Laboratories Technical Note Version 1.4, Revised November 1, 1993
[SP-800-90A]	NIST Special Publication 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators. January 2012