KM67S3B2 Smart Card IC Security Target (ST-Lite)

Version: 1.1

Date: 13th November, 2024

Nuvoton Technology Corporation Japan

Document History

Version	Date	Changes
1.0	2024-08-22	Public version
1.1	2024-11-13	Fixed typo in the date and version

Table of Contents

1 ST Introduction

1.1 ST Reference

Title:	KM67S3B2 Smart Card IC Security Target (ST-Lite)
Version:	Version 1.1
Date:	13th November, 2024
Produced by:	Nuvoton Technology Corporation Japan
Author:	Mitsuyoshi Oya
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 KM67S3B2 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-ST-LITE].

1.2 TOE Reference

TOE:	KM67S3B2 Smart Card IC with IC Dedicated Software
Version:	1.0
Developed by:	Nuvoton Technology Corporation Japan

1.3 TOE Overview

1.3.1 TOE Class and Main Security Function

The TOE is the smart card integrated circuit (IC) called KM67S3B2, developed by Nuvoton Technology Corporation Japan (hereinafter referred to as "NTCJ"). The TOE hardware is composed of a processing unit, a cryptographic hardware, security components, a contactless smart card interface, and volatile and non-volatile memories. The TOE also includes IC Dedicated Software and documentation. The IC Dedicated Software is used for testing during production and also provides additional services to facilitate usage of the TOE hardware.

The TOE hardware is delivered in form of a sawn wafer (dice). After being modularized by the composite product manufacturer, it is embedded in a credit card-sized plastic package, plastic mold package, or booklet.

The TOE is intended for use in applications requiring high security, such as transportation and fare collection (e.g. commuter tickets), access control (e.g. ID cards), and government systems (e.g. basic-resident-register cards, health cards, driver-license cards and passports).

The TOE has the following security features.

- Physical true random number generator (TRNG) meeting Class PTG.2
- Security sensors (e.g., temperature, frequency, voltage, and light)
- Physical countermeasures (e.g., sensing shield)
- Cryptography (i.e., triple-DES and AES)
- Countermeasures against attacks (e.g., side-channel and fault-injection attacks)

The security of the development and manufacturing environment has been also designed to provide a high level of security assurance until the TOE is delivered to customers.

1.3.2 Required Non-TOE Hardware/Software/Firmware

The TOE requires a reader/writer device that supplies the power and performs transmission and reception of data commands via the protocol defined in ISO/IEC14443-3 and ISO/IEC18092 (Passive communication mode at 212/424 kbps) standards.

1.4 TOE Description

The target of evaluation (TOE) consists of:

Table 1: TOE elements

Item Type	Name	Version	Form of delivery
Hardware	KM67S3B2 Smart Card IC	RV00	Sawn wafers (dice)
Software	KM67S3B2 Smart Card IC - IC Dedicated Software	FV0C	Encrypted in electronic form (object file format or on-chip)
Document	[AGD-ES]	1.00	Encrypted in electronic form (PDF)
	[AGD-CM]	1.00	
	SC000 Technical Reference Manual	R0p0	
	ARMv6-M Architecture Reference Manual	September 2010	
	KM67S3B2 Software Library Specification	1.00	

1.4.1 TOE Physical Scope

The TOE hardware is a smart card IC that is composed of a processing unit, a cryptographic hardware, security components, a physical unclonable function (PUF), a contactless smart card interface and volatile and non-volatile memories, as shown in Figure 1-1. The hardware to perform IC testing is also included.

The software part of the TOE is the IC-designer/manufacturer proprietary IC Dedicated Software, as shown in Figure 1-2. This software (also known as IC firmware) is used for IC testing during production and also provides additional services to facilitate usage of the TOE hardware. All other software called Security IC Embedded Software is out of the scope of the TOE.

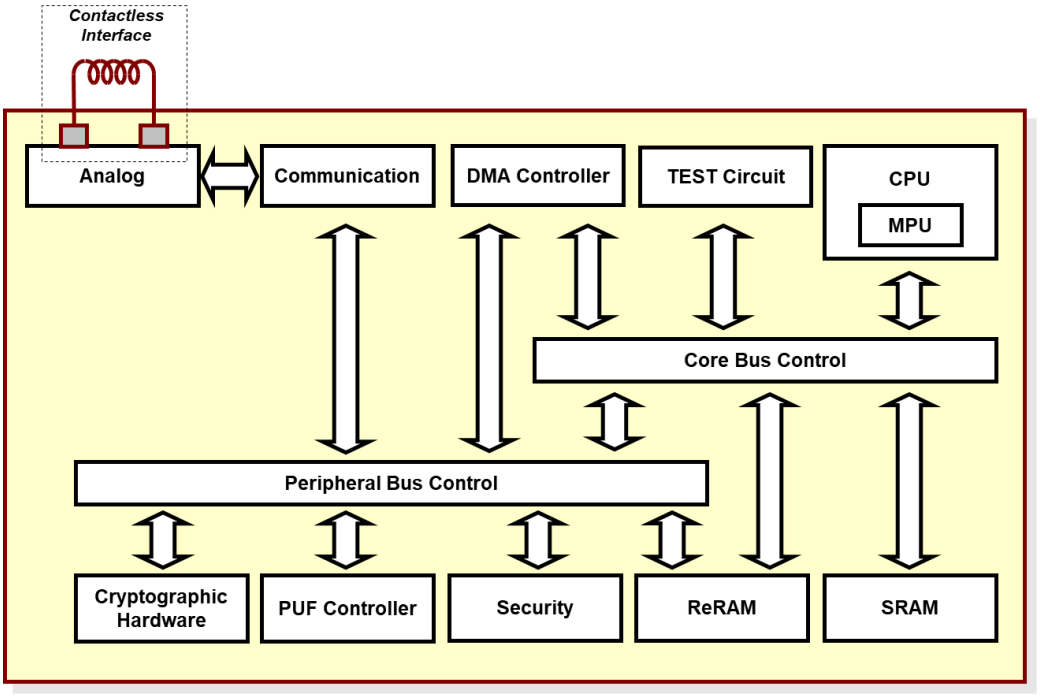

Figure 1-1: Block diagram of KM67S3B2 Smart Card IC - Hardware -

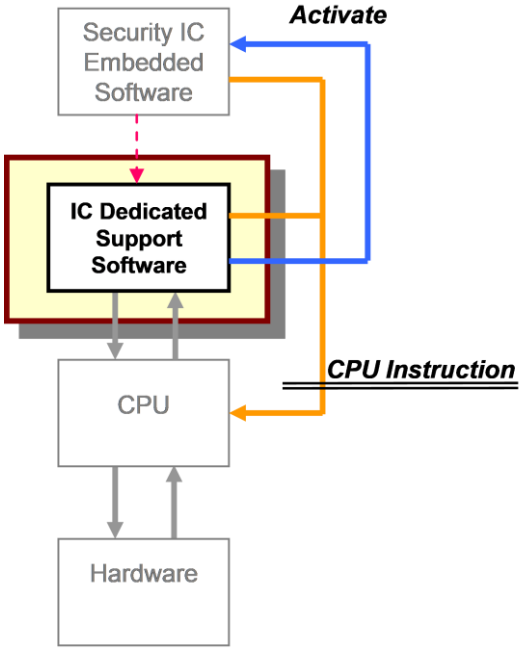

Figure 1-2: Block diagram of KM67S3B2 Smart Card IC - IC Dedicated Software -

1.4.1.1 Hardware

As depicted in Figure 1-1, the TOE includes the functional blocks (i.e., analog, communication, memory, DMA controller, cryptographic hardware, security, PUF control, test circuit, CPU, and BUS control blocks).

(1) Analog

The analog block has a contactless interface, a TRNG, sensors, filters, and a sensing shield.

The contactless interface conforms to ISO/IEC14443-2 and ISO/IEC18092 (Passive communication mode at 212/424 kbps) standards, and supports 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
- Generation of reference clock signal from 13.56 MHz carrier
- Generation of system clock signal
- Generation of power-on reset signal

The TRNG meets Class PTG.2 of [AIS31]. Random values can be used internally or by the Security IC Embedded Software.

The following sensors and filters are embedded to detect faults and incorrect electrical conditions.

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

The sensing shield is embedded to cover the entire sensitive area.

(2) Communication

The communication block controls data transmission and reception via the contactless interface. The data communication can be carried out in conformity to ISO/IEC14443 and ISO/IEC18092 (Passive communication mode at 212/424 kbps) standards.

(3) Memory

There are the following memories in the memory block.

- SRAM : 8 Kbytes
- ReRAM : 128 Kbytes

The SRAM is for the CPU and communication buffer. The ReRAM is accessed as both data and program memory.

(4) DMA Controller

The DMA control block transfers data based on the bus protocol conforming to [AHB-Lite]. There are two channels in the DMA controller block.

(5) Cryptographic Hardware

The cryptographic hardware block has dedicated accelerators and supports calculation of single-DES, dual-key or triple-key triple-DES (TDES), and AES. However, the single-DES is out of scope.

(6) Security

The security block has controllers for the circuits related to security (refer to Section 1.4.1.1 (1)).

(7) PUF Control

The PUF control block generates device-specific identifiers and keys from the PUF. These can be used to enable secure storage.

(8) Test Circuit

The test circuit block supports the Test-mode operation and is used to perform manufactural defective tests of an IC in Phase 3.

(9) CPU

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

(10) Bus Control

The bus control blocks controls data exchanges. Data is exchanged between the CPU and each block (i.e., the DMA control, ReRAM, SRAM, and peripheral bus) via the core bus. Data exchanges between blocks (i.e., the DMA control, communication, cryptographic hardware, security, PUF control, and core bus) is performed via the peripheral bus.

1.4.1.2 Firmware and Software

The TOE includes the IC Dedicated Software stored in ReRAM. There are three configurations of the IC Dedicated Software that conform to ISO/IEC14443-3 and ISO/IEC18092 (Passive communication mode at 212/424 kbps) standards, and an OS

developer selects one of the three configurations. The TOE supports single-DES operations but the single-DES is out of scope.

The IC Dedicated Software in binary form is delivered to an OS developer. The OS developer develops the Security IC Embedded Software and delivers it to the Design site. The Design site creates the image that integrates the IC Dedicated Software and Security IC Embedded Software and delivers it to the Testing site. The Testing site uploads the integrated image to the ReRAM.

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 out of the scope 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 to the external environment are coil pads to which the RF antenna is connected.

(2) Hardware Interface

For the interface to hardware, there is a CPU instruction set.

(3) IC Dedicated Software Interface

There are the interfaces to the set of functions for controlling hardware.

The usage of the IC Dedicated Software is mandatory and it is the only way to access that hardware.

(4) Security IC Embedded Software Interface

As a Security IC Embedded Software interface, there is the Security IC Embedded Software main function.

(5) Physical Interface

Although not in common use, the IC surface is an additional physical interface since it may be used by an attacker to perform electrical stimulation, electrical measurement, and analysis.

(6) Test Pads

The test pads are an electrical interface and are used for IC testing in Phase3.

1.4.1.4 Guidance Documentation

The TOE includes the following guidance documentation:

- [AGD-ES]: This documentation is provided for users developing Security IC Embedded Software.
- KM67S3B2 Software Library Specification: This documentation is provided for users developing Security IC Embedded Software.
- [AGD-CM]: This documentation is provided for users manufacturing cards 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 the following seven 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. It 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 Dedicated Software is developed and integrated with the Security IC Embedded Software delivered by the OS developer in Phase 2. The TOE hardware is delivered in form of a sawn wafer (dice) after the production test. The image that integrates the IC Dedicated Software and Security IC Embedded Software is uploaded to the ReRAM of the TOE hardware in Phase 3. Thus the TOE delivery can be at the end of Phase 3.

1.4.2.1 TOE Logical Phases

Just after power-on, the TOE hardware operates in the Normal mode, but can enter the Test mode by the predefined procedures. When the power is cycled, it again operates in the Normal mode.
When all the IC tests requested in Phase 3 are successfully done, the Test mode becomes unavailable.

1.5 TOE Environments

The production flow is shown in Figure 1-3. The development and manufacturing environments of the TOE are separated into the following six sites.

- Design site
- Mask manufacturing site
- Manufacturing site
- Wafer-Assembly and Visual Inspecting site
- Testing site
- Defective product processing site

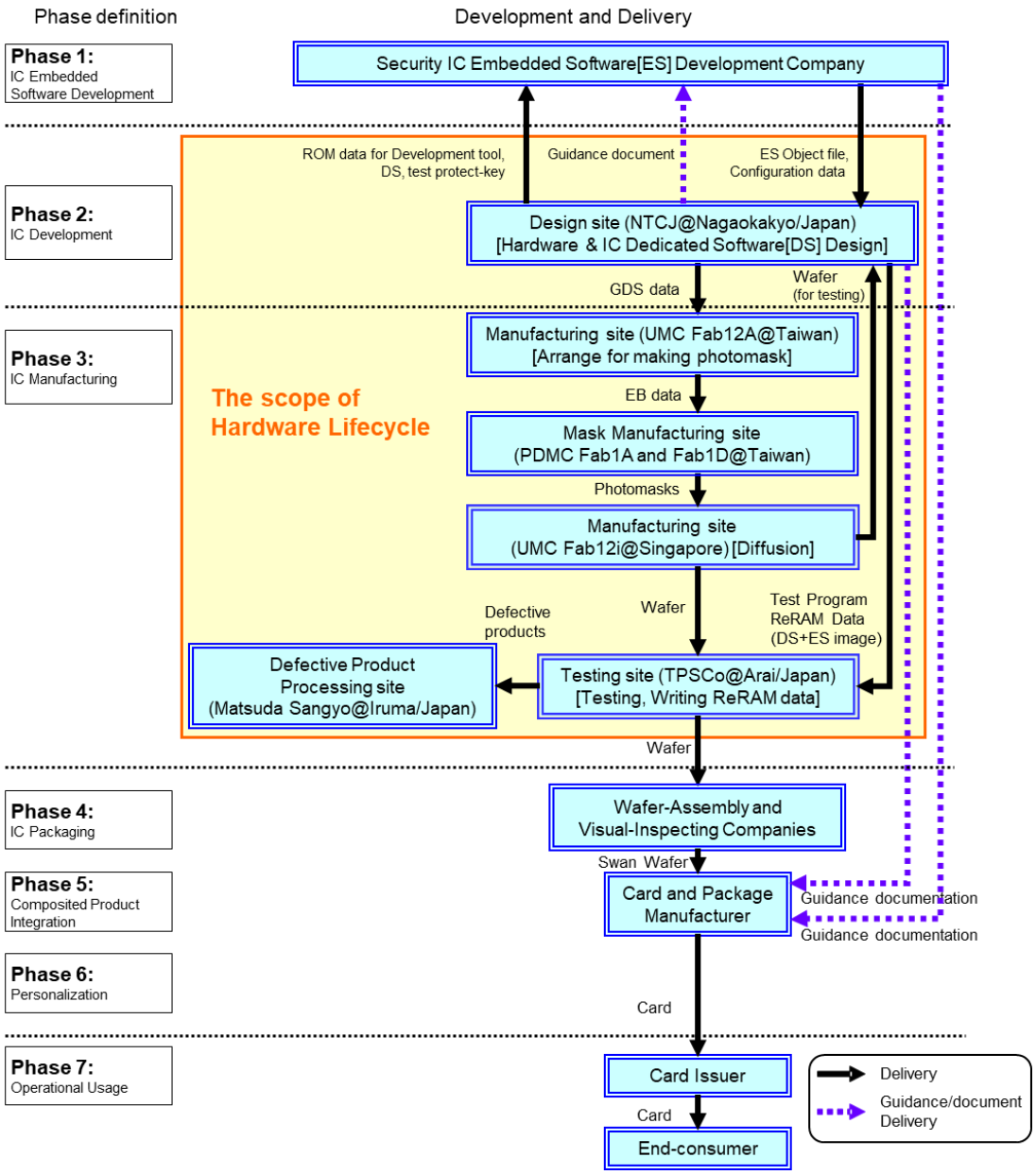

Figure 1-3: Production Flow

1.5.1 TOE Development Environment

1.5.1.1 Design Site

NTCJ's design site manages the following confidential information in accordance with the ALC_DVS security documentation.

- 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

Security in the development environment is ensured through clearly defined physical, personnel, and IT processes and procedures within the scope of evaluation.

1.5.2 TOE Production Environment

1.5.2.1 Mask Manufacturing Site

The Mask Manufacturing site, as a subcontractor, is obliged to securely handle the following confidential information under NDA with the Manufacturing site. The following confidential information is handled in accordance with the ALC_DVS security documentation.

- KM67S3B2 mask processing data (EB data)
- Photomasks
- Related documentation

1.5.2.2 Manufacturing Site

The Manufacturing site, as a subcontractor, is obliged to securely handle the following confidential information under NDA with NTCJ. The following confidential information is handled in accordance with the ALC_DVS security documentation.

- Photomasks and wafers,
- Wafer defectives
- Related documentation

Security in the development environment is ensured through clearly defined processes and procedures.

1.5.2.3 Testing Site

The Testing site, as a subcontractor, is obliged to securely handle the following confidential information under NDA with NTCJ. The following confidential information is handled in accordance with the ALC_DVS security documentation.

- Pre-personalization data
- Wafers / sawn wafers
- Test and characterization related data

- Wafer and development samples for testing
- Wafer and chip defectives
- Related documentation

1.5.2.4 Wafer-Assembly and Visual-Inspecting Site

The Wafer-Assembly and Visual-Inspecting site, as a subcontractor, is obliged to securely handle the following confidential information under NDA with NTCJ. The TSF self-protection of TOEs contained in the handled wafers/sawn wafers is already enabled.

- Wafer / sawn wafers

Wafers that are delivered from the Testing site are wafer-assembled and inspected. After the visual inspection is complete, the inspected wafers are delivered to the Testing site.

1.5.2.5 Defective Product Processing Site

The Defective Product Processing site, as a subcontractor, is obliged to securely handle the following confidential information under NDA with NTCJ. The following confidential information is handled in accordance with the ALC_DVS security documentation.

- Wafer and chip defectives

Defective wafers and chips are delivered from the Testing site to the Defective Product Processing site and securely disposed.

1.5.3 Initialization and Pre-Personalization Data

During IC testing in Phase 3, an identifier that uniquely identifies the IC is embedded in the write-lock area of the 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 [PP].

- Package “Cryptographic Services (TDES/AES)”

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 KM67S3B2. The description below is therefore adopted from [PP, 3].
In addition, the KM67S3B2 implements authentication mechanism 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

Threats are listed in the following table.

Table 3: Defined Threats in [PP] and Augmentation

Threats		
Standard and related to Security Services	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.Mem-Access	Memory Access Violation

3.2.1 Standard Threats and Threats related to Security Services

Standard Threats defined in [PP] are listed in Table 3.
The TOE shall avert the threat "Inherent Information Leakage (T.Leak-Inherent)" as specified below.

T.Leak-Inherent Inherent Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data as part of the assets.

No direct contact with the Security IC internals is required here. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. One example is Differential Power Analysis (DPA). This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from direct (contact) measurements (Numbers 6 and 7 in Figure 8 in [PP]) or measurement of emanations (Number 5 in Figure 8 in [PP]) and can then be related to the specific operation being performed.

The TOE shall avert the threat "Physical Probing (T.Phys-Probing)" as specified below.

T.Phys-Probing **Physical Probing**

An attacker may perform physical probing of the TOE in order (i) to disclose user data while stored in protected memory areas, (ii) to disclose/reconstruct the user data while processed or (iii) to disclose other critical information about the operation of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.

Physical probing requires direct interaction with the Security IC internals (Numbers 5 and 6 in Figure 8 in [PP]). Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that hardware security mechanisms and layout characteristics need to be identified (Number 3 in Figure 8 in [PP]). Determination of software design including treatment of user data of the Composite TOE may also be a pre-requisite.

This pertains to “measurements” using galvanic contacts or any type of charge interaction whereas manipulations are considered under the threat “Physical Manipulation (T.Phys-Manipulation)”. The threats “Inherent Information Leakage (T.Leak-Inherent)” and “Forced Information Leakage (T.Leak-Forced)“ may use physical probing but require complex signal processing in addition.

The TOE shall avert the threat “Malfunction due to Environmental Stress (T.Malfunction)” as specified below.

T.Malfunction **Malfunction due to Environmental Stress**

An attacker may cause a malfunction of TSF or of the Security IC Embedded Software by applying environmental stress in order to (i) modify security services of the TOE or (ii) modify functions of the Security IC Embedded Software (iii) deactivate or affect security mechanisms of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software. This may be achieved by operating the Security IC outside the normal operating conditions (Numbers 1, 2 and 9 in Figure 8 in [PP]).

The modification of security services of the TOE may e.g. affect the quality of random numbers provided by the random number generator up to undetected deactivation when the random number generator does not produce random numbers and the Security IC Embedded Software gets constant values. In another case errors are introduced in executing the Security IC Embedded Software. To exploit this an attacker needs information about the functional operation, e.g. to introduce a temporary failure within a register used by the Security IC Embedded Software with light or a power glitch.

The TOE shall avert the threat “Physical Manipulation (T.Phys-Manipulation)” as specified below.

T.Phys-Manipulation Physical Manipulation

An attacker may physically modify the Security IC in order to (i) modify user data of the Composite TOE, (ii) modify the Security IC Embedded Software, (iii) modify or deactivate security services of the TOE, or (iv) modify security mechanisms of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.

The modification may be achieved through techniques commonly employed in IC failure analysis (Numbers 1, 2 and 4 in Figure 8 in [PP]) and IC reverse engineering efforts (Number 3 in Figure 8 in [PP]). The modification may result in the deactivation of a security feature. Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of user data of the Composite TOE may also be a pre-requisite. Changes of circuitry or data can be permanent or temporary.

In contrast to malfunctions (refer to T.Malfunction) the attacker requires to gather significant knowledge about the TOE’s internal construction here (Number 3 in Figure 8 in [PP]).

The TOE shall avert the threat “Forced Information Leakage (T.Leak-Forced)“ as specified below:

T.Leak-Forced Forced Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data of the Composite TOE as part of the assets even if the information leakage is not inherent but caused by the attacker.

This threat pertains to attacks where methods described in “Malfunction due to Environmental Stress” (refer to T.Malfunction) and/or “Physical Manipulation” (refer to T.Phys-Manipulation) are used to cause leakage from signals (Numbers 5, 6, 7 and 8 in Figure 8 in [PP]) which normally do not contain significant information about secrets.

The TOE shall avert the threat “Abuse of Functionality (T.Abuse-Func)” as specified below.

T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which may not be used after TOE Delivery in order to (i) disclose or manipulate user data of the Composite TOE, (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE or (iii) manipulate (explore, bypass, deactivate or change) functions of the Security IC Embedded Software or (iv) enable an attack disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.

Threat related to Security Services defined in [PP] is listed in Table 3.
The TOE shall avert the threat "Deficiency of Random Numbers (T.RND)" as specified below

T.RND Deficiency of Random Numbers

An attacker may predict or obtain information about random numbers generated by the TOE security service for instance because of a lack of entropy of the random numbers provided.

An attacker may gather information about the random numbers produced by the TOE security service. Because unpredictability is the main property of random numbers this may be a problem in case they are used to generate cryptographic keys. The entropy provided by the random numbers must be appropriate for the strength of the cryptographic algorithm, the key or the cryptographic variable is used for. Here the attacker is expected to take advantage of statistical properties of the random numbers generated by the TOE. Malfunctions or premature ageing are also considered which may assist in getting information about random numbers.

3.2.2 Augmented Threats

Augmented Threats is listed in Table 3.

The TOE shall avert the threat "Memory Access Violation (T.Mem-Access)" as specified below.

T.Mem-Access Memory Access Violation

Parts of the Security IC Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). Any restrictions are defined by the security policy of the specific application context and must

be implemented by the Security IC Embedded Software.

3.3 Organizational Security Policies

Organizational Security Policies 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.Crypto-Service	Cryptographic services of the TOE
	P.Add-Functions	Additional Specific Security Functionality

3.3.1 Standard Organizational Security Policy

Standard Organizational Security Policy defined in [PP] is listed in Table 4.

The IC Developer / Manufacturer must apply the policy "Identification during TOE Development and Production (P.Process-TOE)" as specified below.

P.Process-TOE Identification during TOE Development and Production

An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

The accurate identification is introduced at the end of the production test in phase 3. Therefore the production environment must support this unique identification.

3.3.2 Augmented Organizational Security Policies

Augmented Organizational Security Policies are listed in Table 4.

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:

- Triple Data Encryption Standard (TDES)
- Advanced Encryption Standard (AES)

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 are listed in the following table.

Table 5: Defined Assumptions in [PP] and Augmentation

Assumptions		
Standard	A.Process-Sec-IC	Protection during packaging, finishing and personalisation
	A.Resp-Appl	Treatment of user data of the Composite TOE
Augmentation	A.Key-Function	Usage of Key-dependent Function
	A.Interpreter	Implementation of command interpreter

3.4.1 Standard Assumption

Standard Assumptions defined in [PP] are listed in Table 6.

The intended usage of the TOE is twofold, depending on the Life Cycle Phase: (i) The Security IC Embedded Software developer uses it as a platform for the Security IC software being developed. The Composite Product Manufacturer (and the consumer) uses it as a part of the Security IC. The Composite Product is used in a terminal which supplies the Security IC (with power and clock) and (at least) mediates the communication with the Security IC Embedded Software.

Before being delivered to the consumer the TOE is packaged. Many attacks require the TOE to be removed from the carrier. Though this extra step adds difficulties for the attacker no specific assumptions are made here regarding the package.

Appropriate "Protection during Packaging, Finishing and Personalisation (A.Process-Sec-IC)" must be ensured after TOE Delivery up to the end of Phase 6, as well as during

the delivery to Phase 7 as specified below.

A.Process-Sec-IC Protection during Packaging, Finishing and Personalisation

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

This means that the Phases after TOE Delivery (refer to Sections 1.2.2 and 7.1 in [PP]) are assumed to be protected appropriately. For a preliminary list of assets to be protected refer to paragraph 96 (page 29) in [PP].

The information and material produced and/or processed by the Security IC Embedded Software Developer in Phase 1 and by the Composite Product Manufacturer can be grouped as follows:

- the Security IC Embedded Software including specifications, implementation and related documentation,

- Pre-personalisation Data and Personalisation Data including specifications of formats and memory areas, test related data,

- the user data of the Composite TOE and related documentation, and

- material for software development support

as long as they are not under the control of the TOE Manufacturer.

The Security IC Embedded Software must ensure the appropriate "Treatment of user data of the Composite TOE (A.Resp-Appl)" as specified below.

A.Resp-Appl Treatment of user data of the Composite TOE

All user data of the Composite TOE are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant user data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.

The application context specifies how the user data of the Composite TOE shall be handled and protected. The evaluation of the Security IC according to this Protection Profile is conducted on generalized application context. The concrete requirements for the Security IC Embedded Software shall be defined in the Protection Profile respective

Security Target for the Security IC Embedded Software. The Security IC cannot prevent any compromise or modification of user data of the Composite TOE by malicious Security IC Embedded Software.

3.4.2 Augmented Assumption

Augmented Assumptions are listed in Table 6.

The developer of the Security IC Embedded Software must ensure the appropriate "Usage of Key dependent Function (A.Key-Function)" while developing this software in Phase 1 as specified below.

A.Key-Function **Usage of Key-dependent Function**

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.

The developer of Security IC Embedded Software must ensure the appropriate "Implementation of command interpreter (A.Interpreter)" while developing this software in Phase 1 as specified below.

A.Interpreter **Implementation of command interpreter**

The interpreter (Issuance API) is used to check that the basic functions works correctly after embedding the IC Dedicated Software and the Security IC Embedded Software in the chip and packaging it.

It is assumed that the command interpreter used for the tests in Phases 4 and 5 shall be implemented.
To prevent that an attacker abuses the test commands, it is required to authenticate sufficiently before executing these test commands. Besides, the test commands shall be deactivated after completing all of the tests.

4 Security Objectives

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

4.1 Security Objectives for the TOE

The user have 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 are listed in the following table.

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

Security Objectives for the TOE		
Standard and related to Specific Functionality	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.TDES	Cryptographic service Triple-DES
	O.AES	Cryptographic service AES
	O.PUF	Protection using PUF
	O.Mem-Access	Area based Memory Access Control

4.1.1 Standard Security Objectives for the TOE and Security Objectives related

to Specific Functionality

Standard Security Objectives for the TOE defined in [PP] are listed in Table 6.

The TOE shall provide “Protection against Inherent Information Leakage (O.Leak-Inherent)” as specified below.

O.Leak-Inherent Protection against Inherent Information Leakage

The TOE must provide protection against disclosure of confidential data stored and/or processed in the Security IC

- by measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and

- by measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or I/O lines).

This objective pertains to measurements with subsequent complex signal processing whereas O.Phys-Probing is about direct measurements on elements on the chip surface. Details correspond to an analysis of attack scenarios which is not given here.

The TOE shall provide “Protection against Physical Probing (O.Phys-Probing)” as specified below.

O.Phys-Probing Protection against Physical Probing

The TOE must provide protection against disclosure/reconstruction of user data while stored in protected memory areas and processed or against the disclosure of other critical information about the operation of the TOE.

This includes protection against

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)

with a prior reverse-engineering to understand the design and its properties and functions.

The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

The TOE shall provide "Protection against Malfunctions (O.Malfunction)" as specified below.

O.Malfunction Protection against Malfunctions

The TOE must ensure its correct operation.

The TOE must indicate or prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent malfunctions. Examples of environmental conditions are voltage, clock frequency, temperature, or external energy fields.

Remark: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective O.Phys-Manipulation) provided that detailed knowledge about the TOE´s internal construction is required and the attack is performed in a controlled manner.

The TOE shall provide "Protection against Physical Manipulation (O.Phys-Manipulation)" as specified below.

O.Phys-Manipulation Protection against Physical Manipulation

The TOE must provide protection against manipulation of the TOE (including its software and TSF data), the Security IC Embedded Software and the user data of the Composite TOE. This includes protection against

- reverse-engineering (understanding the design and its properties and functions),
- manipulation of the hardware and any data, as well as
- undetected manipulation of memory contents.

The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through

such a physical attack.

The TOE shall provide “Protection against Forced Information Leakage (O.Leak-Forced)“ as specified below:

O.Leak-Forced **Protection against Forced Information Leakage**

The Security IC must be protected against disclosure of confidential data processed in the Security IC (using methods as described under O.Leak-Inherent) even if the information leakage is not inherent but caused by the attacker

- by forcing a malfunction (refer to “Protection against Malfunction due to Environmental Stress (O.Malfunction)” and/or

- by a physical manipulation (refer to “Protection against Physical Manipulation (O.Phys-Manipulation)”.

If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.

The TOE shall provide “Protection against Abuse of Functionality (O.Abuse-Func)” as specified below.

O.Abuse-Func **Protection against Abuse of Functionality**

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical user data of the Composite TOE, (ii) manipulate critical user data of the Composite TOE, (iii) manipulate Security IC Embedded Software or (iv) bypass, deactivate, change or explore security features or security services of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

The TOE shall provide “TOE Identification (O.Identification)“ as specified below:

O.Identification **TOE Identification**

The TOE must provide means to store Initialisation Data and Pre-personalisation Data in its non-volatile memory. The Initialisation Data (or parts of them) are used for TOE identification.

Security Objectives related to Specific Functionality defined in [PP] are listed in Table 6.
The TOE shall provide “Random Numbers (O.RND)” as specified below.

O.RND **Random Numbers**

The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a sufficient entropy.

The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.

4.1.2 Augmented Security Objectives for the TOE

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

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 “Protection using PUF (O.PUF)” as specified below.

O.PUF **Protection using PUF**

The TOE provides PUF functionality in order to protect stored user data.

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

The TOE shall provide "Area based Memory Access Control (O.Mem-Access)" as specified below.

O.Mem-Access Area based Memory Access Control

The TOE shall provide the following specific security functionality to the Security IC Embedded Software. The TOE shall provide the Security IC Embedded Software with the capability to define restricted access memory areas. The TOE shall then enforce the partitioning of such memory areas so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

4.2 Security Objectives for the Security IC Embedded Software

Security objective for the Security IC Embedded Software are listed in the following table.

Table 7: Defined Security Objectives for the Security IC Embedded Software in [PP] and Augmentation

Security Objective for the Security IC Embedded Software		
Standard	OE.Resp-Appl	Treatment of user data of the Composite TOE
Augmentation	OE.Interpreter	Implementation of command interpreter

4.2.1 Standard Security Objective for the Security IC Embedded Software

Standard Security objective for the Security IC Embedded Software defined in [PP, 4.2] is listed in Table 7.

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

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

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

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.

4.2.2 Augmented Security Objective for the Security IC Embedded Software

Augmented security objective for the Security IC Embedded Software is listed in Table 7.

The Security IC Embedded Software shall provide "Implementation of command interpreter (OE.Interpreter)" as specified below.

OE.Interpreter **Implementation of command interpreter**

It is assumed that the command interpreter used for the tests in Phase 4 and 5 shall be implemented.
To prevent that an attacker abuses the test commands, it is required to authenticate sufficiently before executing these test commands. Besides, the test commands shall be deactivated after completing all of the tests.

4.3 Security Objectives for the Operational Environment

Security objectives for the operational environment are listed in the following table.

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

Security Objectives for the Operational Environment		
Standard	OE.Process-Sec-IC	Protection during composite product manufacturing

4.3.1 TOE Delivery up to the end of Phase 6

Standard Security objectives for the operational environment defined in [PP, 4.3] is listed in Table 9.

Appropriate "Protection during Packaging, Finishing and Personalisation (OE.Process-Sec-IC)" must be ensured after TOE Delivery up to the end of Phases 6, as well as during the delivery to Phase 7 as specified below.

OE.Process-Sec-IC Protection during composite product manufacturing

Security procedures shall be used after TOE Delivery up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 1.2.3) must be protected appropriately. For a preliminary list of assets to be protected refer to paragraph 96 (page 29) in [PP].

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
A.Key-Function	OE.Resp-Appl	Phase 1
A.Interpreter	**OE.Interpreter**	**Phase 1**
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.Mem-Access	**O.Mem-Access**	
P.Process-TOE	O.Identification	Phase 2 – 3 optional Phase 4
P.Crypto-Services	**O.TDES** **O.AES**	
P.Add-Functions	**O.PUF**	

Compared to [PP] a clarification has been made for the security objective "Treatment of User Data (OE.Resp-Appl)": By definition cipher or plain text data and cryptographic keys are User Data. So, the Security IC Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. It can be concluded from the above that this objective covers A.Key-Function since it ensures that any keys in use are protected from any compromises by adoption of the cryptographic functions. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realized in the environment.

Rationale added to the TOE is presented below.

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

> Since **O.TDES** and **O.AES** 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 related to the security objective "Implementation of command interpreter (**OE.Interpreter**)" is as follows:

> Since **OE.Interpreter** requires the Security IC Embedded Software developer to implement the interpreter assumed in **A.Interpreter**, the assumption is covered by the objective.

The justification related to the threat "Memory Access Violation (**T.Mem-Access**)" is as follows:

> According to **O.Mem-Access** the TOE must enforce the partitioning of memory areas so that access of software to memory areas is controlled. Any restrictions are to be defined by the Security IC Embedded Software. Thereby security violations caused by accidental or deliberate access to restricted data (which may include code) can be prevented (refer to **T.Mem-Access**). The threat T.Mem-Access is therefore removed if the objective is met.

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].

5.1 Definition of the Family FCS_RNG

To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

FCS_RNG Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

Component levelling:

FCS_RNG.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RNG.1 There are no management activities foreseen.
Audit:	FCS_RNG.1 There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a [selection: *physical, non-physical true,*

deterministic, hybrid physical, hybrid deterministic] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide [selection: bits, octets of bits, numbers [assignment: format of the numbers]] that meet [assignment: *a defined quality metric*].

5.2 Definition of the Family FMT_LIM

To define the IT security functional requirements of the TOE an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE (refer to Section 6.1) appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the component Limited Capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:

FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

Management: FMT_LIM.1, FMT_LIM.2
There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2
There are no actions defined to be auditable.

The TOE Functional Requirement “Limited capabilities (FMT_LIM.1)” is specified as follows.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 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 [assignment: Limited capability policy].

The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 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 [assignment: Limited availability policy].

5.3 Definition of the Family FAU_SAS

To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS Audit data storage

Family behaviour

This family defines functional requirements for the storage of audit data.

Component levelling

FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1
There are no management activities foreseen.

Audit: FAU_SAS.1
There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide [assignment: *list of subjects*] with the capability to store [assignment: *list of audit information*] in the [assignment: *type of persistent memory*].

5.4 Definition of the Family FDP_SDC

To define the security functional requirements of the TOE an additional family (FDP_SDC.1) of the Class FDP (User data protection) is defined here.

The family “Stored data confidentiality (FDP_SDC)” is specified as follows.

FDP_SDC Stored data confidentiality

Family behaviour

This family provides requirements that address protection of user data confidentiality while these data are stored within memory areas protected by the TSF. The TSF provides access to the data in the memory through the specified interfaces only and prevents compromise of their information bypassing these interfaces. It complements the family Stored data integrity (FDP_SDI) which protects the user data from integrity errors while being stored in the memory.

Component levelling

FDP_SDC.1 Requires the TOE to protect the confidentiality of information of the user data in specified memory areas.

Management:	FDP_SDC.1 There are no management activities foreseen.
Audit:	FDP_SDC.1 There are no actions defined to be auditable.

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

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.

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

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	Quality metric for random numbers (Class PTG.2)
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**
FDP_ACC.1	**Subset access control**
FDP_ACF.1	**Security attribute based access control**
FMT_MSA.3	**Static attribute initialization**
FMT_MSA.1	**Management of security attributes**
FMT_SMF.1	**Specification of management functions**

6.1.1 Standard Security Functional Requirements for the TOE

The following SFRs for the TOE defined in [PP, 6.1] are taken from [PP].

(1) Malfunctions

The TOE shall meet the requirement "Limited fault tolerance (FRU_FLT.2)" as specified below.

FRU_FLT.2 Limited fault tolerance

Hierarchical to: FRU_FLT.1 Degraded fault tolerance

Dependencies: FPT_FLS.1 Failure with preservation of secure state.

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1).

Refinement: The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.

The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below.

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur.

(2) Abuse of Functionality

The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be

gathered which may enable other attacks.

The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.2	**Limited availability**
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1	The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.

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.

(3) Physical Manipulation and Probing

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 shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below.

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

(4) Leakage

The TOE shall meet the requirement "Basic internal transfer protection (FDP_ITT.1)" as specified below.

FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ITT.1.1 The TSF shall enforce the Data Processing Policy 11 to prevent the disclosure of user data when it is transmitted between physically-separated parts of the TOE.

Refinement: The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.

The TOE shall meet the requirement "Basic internal TSF data transfer protection (FPT_ITT.1)" as specified below.

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE.

Refinement: The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE.

This requirement is equivalent to FDP_ITT.1 above but refers to TSF data instead of user data. Therefore, it should be understood as to refer to the same Data Processing Policy defined under FDP_IFC.1 below.

The TOE shall meet the requirement "Subset information flow control (FDP_IFC.1)" as specified below:

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1	The TSF shall enforce the Data Processing Policy on all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software.

The following Security Function Policy (SFP) Data Processing Policy is defined for the requirement "Subset information flow control (FDP_IFC.1)":

"User data of the Composite TOE and TSF data shall not be accessible from the TOE except when the Security IC Embedded Software decides to communicate the user data of the Composite TOE via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security IC Embedded Software."

(5) Random Numbers

The TOE generates random numbers. An additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined in chapter 5.1. 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)" as specified below (Common Criteria Part 2 extended).

FCS_RNG.1	**Quality metric for random numbers (Class PTG.2)**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a physical random number generator that implements:
(PTG.2.1)	A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.
(PTG.2.2)	If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.
(PTG.2.3)	The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.

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

(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered 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 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.

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 **bold type** in Table 10. These security functional components are explained below.

(1) Cryptographic Support

The security functional requirements FCS_COP.1/TDES and FCS_COP.1/AES 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;

- Triple Data Encryption Standard (TDES)
- Advanced Encryption Standard (AES)

(a) 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)".

(b) 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, or GCM mode and cryptographic key sizes 128 bits, 192 bits or 256 bits that meet the following: [FIPS-197],

[SP-800-38A], [SP-800-38B], [SP-800-38D].

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)".

(2) Memory Access Control

The security service being provided is described in the Security Function Policy (SFP) Memory Access Control Policy. The security functional requirement "Subset access control (FDP_ACC.1)" requires that this policy is in place and defines the scope were it applies. The security functional requirement "Security attribute based access control (FDP_ACF.1)" addresses security attribute usage and characteristics of policies. It describes the rules for the function that implements the Security Function Policy (SFP) as identified in FDP_ACC.1. The decision whether an access is permitted or not is taken based upon attributes allocated to the software. Examples for such attributes are "the memory area where the software is executed from, the memory area where the access is performed to, special information or properties tied to the software, and/or the operation to be performed" (refer to below). The corresponding permission control information is evaluated so that access is granted/effective or denied/inoperable.

The security functional requirement "Static attribute initialization (FMT_MSA.3)" ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. Alternative values can be specified by any subject provided that the Memory Access Control Policy allows that. This is described by the security functional requirement "Management of security attributes (FMT _MSA.1)". The attributes are determined during TOE manufacturing (FMT_MSA.3) or set at run time (FMT_MSA.1).

The following Security Function Policy (SFP) Memory Access Control Policy is defined for the requirement "Security attribute based access control (FDP_ACF.1)":

Memory Access Control Policy

The TOE shall control read, write, delete, and execute accesses of software residing in memory areas on data including code stored in memory areas.

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below.

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control.

FDP_ACC.1.1 The TSF shall enforce the Memory Access Control Policy on all subjects (software in memories), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy,

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below.

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the Memory Access Control Policy to objects based on the following:
Subjects: software in memories
Objects: data in memories
Attributes: memory address of accessed data
permission control information

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: evaluate the corresponding permission control information before, during or after the access so that accesses to be denied can not be utilised by the subject attempting to perform the operation.

FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

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

FMT_MSA.3	**Static attribute initialization**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the Memory Access Control Policy to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow no subject (provided that the Memory Access Control Policy is enforced and the necessary access is therefore allowed) to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MSA.1	**Management of security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MSA.1.1	The TSF shall enforce the Memory Access Control Policy to restrict the ability to modify the security attributes permission control information to software running

The TOE shall meet the requirement "Specification of management functions (FMT_SMF.1)" as specified below:

FMT_SMF.1 **Specification of management functions**

Hierarchical to: No other components

Dependencies: No dependencies

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

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 “Quality metric for random numbers (Class PTG.2)” 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.TDES	**- FCS_COP.1/TDES “Cryptographic operation - TDES”** **- FCS_CKM.4/TDES “Cryptographic key destruction - TDES”**

Objective	TOE Security Functional and Assurance Requirements
O.AES	**- FCS_COP.1/AES "Cryptographic operation - AES"** **- FCS_CKM.4/AES "Cryptographic key destruction - AES"**
O.PUF	**- FDP_SDC.1 "Stored data confidentiality"** **- FPT_PHP.3 "Resistance to physical attack"**
OE.Resp-Appl	not applicable
OE.Interpreter	not applicable
OE.Process-Sec-IC	not applicable
O.Mem-Access	**- FDP_ACC.1 "Subset access control"** **- FDP_ACF.1 "Security attribute based access control"** **- FMT_MSA.3 "Static attribute initialisation"** **- FMT_MSA.1 "Management of security attributes"** **- FMT_SMF.1 "Specification of management**

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 "Protection using PUF (O.PUF)" is as follows:

The SFR "Stored data confidentiality (FDP_SDC.1)" and "Resistance to physical attack (FPT_PHP.3)" exactly require the function to be implemented which is demanded by O.PUF. Therefore, FDP_SDC.1 and FPT_PHP.3 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 TDES and AES 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 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.

The justification related to the security objective "Area based Memory Access Control (O.Mem-Access)" is as follows:

The security functional requirement "Subset access control (FDP_ACC.1)" with the related Security Function Policy (SFP) "Memory Access Control Policy" exactly requires to implement an area based memory access control as demanded by O.Mem Access.
Therefore, FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1 and FMT_SMF.1 with its SFP are suitable to meet the security objective.

The security functional requirement "Static attribute initialization (FMT_MSA.3) requires that the TOE provides default values for security attributes. These default values cannot be overwritten by any subject (software) provided that the necessary access is not allowed what is further detailed in the security functional requirement "Management of security attributes (FMT_MSA.1)": The ability to update the security attributes is restricted to privileged subject(s). These management functions ensure that the required access control can be realized using the functions provided by the TOE.

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

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
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
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	None	No dependency
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)**
FDP_ACC.1	**FDP_ACF.1**	**Yes**
FDP_ACF.1	**FDP_ACC.1 FMT_MSA.3**	**Yes Yes**
FMT_MSA.3	**FMT_MSA.1 FMT_SMR.1**	**Yes See discussion below**
FMT_MSA.1	**FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1**	**Yes See discussion below 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.

The dependency FMT_SMR.1 introduced by the two components FMT_MSA.1 and FMT_MSA.3 is considered to be satisfied because the access control specified for the intended TOE is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of a security functional requirement FMT_SMR.1.

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 and Similar Devices” [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 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/TDES and FCS_COP.1/AES, require executing the cryptographic algorithms.
The security functional requirements FCS_CKM.4/TDES and FCS_CKM.4/AES require the measures destroying cryptographic key for more secure operation.
Therefore, these SFRs support the secure implementation and operation of TDES and AES.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the area based memory access control function implemented according to the security functional requirement described in the security functional requirement FDP_ACC.1 with reference to the Memory Access Control Policy and details given in FDP_ACF.1. Therefore, those security functional requirements support the secure implementation and operation of FDP_ACF.1 with its dependent security functional requirements.

7 TOE Summary Specification

7.1 TOE Security Functionality

7.1.1 TOE Security Features

(1) SF.RNG: Random Number Generator

The TRNG in the TOE generates random values, and meets Class PTG.2 of [AIS31].

The TOE features this security function by means of a random number generator that operates stably within the limits guaranteed by the security function SF.FAS.

The verified random values are used internally or by Security IC Embedded Software.

(2) SF.FAS: Filters and Sensors

The TOE prevents any malfunction and ensures its correct operation.

The TOE features the effective filters on the sensitive signal lines to eliminate electrical factors that cause faults such as glitches. The sensors, i.e., voltage, frequency, light, and temperature sensors, are featured to detect faulty electrical conditions that could cause faults and malfunctions. These filters and sensors 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

When the sensors detect an abnormality, the CPU and all the registers are initialized.

Whenever the power of the TOE hardware is turned on, each self-test is run, and when an abnormal operation of the filters and sensors is detected, the CPU and all the registers are initialized. It is therefore ensured that these filters and sensors properly operate.

All instructions executed by the CPU are monitored. An illegal instruction is assumed to be corrupted by an attack and the CPU and all the registers are initialized when detected.

Parameters set by the IC Dedicated Software are checked. When they are unauthorized values, the CPU and all the registers are initialized.

(3) SF.PHY: Physical Tamper Resistance

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

One of the countermeasures is memory scramble.

The sensing shield is also embedded. If there are any changes in the physical conditions of the IC, the sensing shield alerts a warning, and the CPU and all the registers are initialized.

The critical data is protected using the secure mechanisms mentioned above.

(4) SF.DPR: Data Protection

The TOE may be susceptible to physical attacks: therefore it has potential risk of internal data leakages. 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, the attacker may reveal their confidential data indirectly or directly from the ReRAM.

To prevent such unwanted leakages, and especially to protect from fault-injection and side-channel attacks, the TOE features the security countermeasures.

(5) SF.MCT: Mode Control

For chip, there are Test mode and Normal mode. Factory setting is Normal mode.

After all the tests in Phase 3 are over, the Test-mode entry becomes unavailable 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 supports calculation of TDES, and AES. Key sizes, and the standards for each algorithm are summarized in Table 16.

Table 16: Cryptographic Functionalities

Algorithm	Key length	Standard
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] [SP-800-38D]

(7) SF.ACC: Access Control

The Access Control function is provided to prevent unintended accesses to the specific areas where important programs and data are stored.
When the unintended address is accessed, the CPU and all registers are initialized.

(8) SF.ID: Identification

During the last function testing in Phase 3, some data to uniquely identify an IC chip are written in the write-lock area of the ReRAM. These information cannot be rewritten. Thus, the data like ID embedded in the TOE hardware is never 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 generated from the PUF data.

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) cannot 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_COP.1/TDES						✓			
FCS_CKM.4/TDES						✓			
FCS_COP.1/AES						✓			
FCS_CKM.4/AES						✓			
FDP_ACC.1							✓		
FDP_ACF.1							✓		
FMT_MSA.3							✓		
FMT_MSA. 1							✓		
FMT_SMF.1							✓		

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 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 E2PROM) 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
CRC	Cyclic Redundancy Checksum
DES	Data Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EB	Electron Beam
ECB	Electronic Code Book
FIB	Focused Ion Beam
IC	Integrated Circuit
IT	Information Technology
MAC	Message Authentication Code
NMI	Non-Maskable Interrupt
NTCJ	Nuvoton Technology Corporation Japan
PC	Program Counter
PP	Protection Profile
PUF	Physical Unclonable Function
ReRAM	Resistive Random Access Memory
RF	Radio Frequency
RNG	Random Number Generator
SFR	Security Functional Requirement
SPA	Simple Power Analysis
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-ES]	KM67S3B2 Smart Card IC Administrator Guidance for Security IC Embedded Software Developer
[AGD-CM]	KM67S3B2 Smart Card IC Administrator Guidance for Card Manufacturer
[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
[FIPS197]	U.S. Department of Commerce / National Institute of Standards and Technology, Advanced Encryption Standard (AES), FIPS PUB 197, 2001 November 26
[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/IEC18092]	Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)
[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 and , Similar Devices Version 3.1, June 2020
[JIL-ST-LITE]	ST-lite, Version 1.1, 2002, JIL
[KS2011]	A proposal for: Functionality classes for random number generators, Version 2.0, 18 September 2011
[PP]	Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084-2014.
[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-800-38D]	U.S. Department of Commerce / National Institute of Standards

Abbreviated name	References
	and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST Special Publication 800-38D, 2007 Edition
[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