TrustME™

W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F)

Winbond TrustME™ Secure Element

Security Target Lite

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This introductory chapter contains the following sections:

- Security Target Introduction
- TOE Reference
- TOE Overview
- TOE Description

- TOE Operating Modes and Life Cycle

1.1 Security Target Reference

Title: Security Target of W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) Winbond TrustME™ Secure Element

Authors: Winbond Technology Ltd.

Evaluator: Applus

Certified by: CCN Organismo de Certificacion

1.2 TOE Reference

The Target of Evaluation is identified as below:

Commercial Name	Winbond TrustME™ Secure Element
Product Name	W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F)
Version	A
Guidance	Described in Physical Scope

Table 1 TOE Identification

1.3 TOE Overview

1.3.1 TOE Type

The Target of Evaluation is a Secure Element.

1.3.2 TOE Intended Usage

The TOE is designed to be used in highly critical hardware devices, such as smart cards, secure elements, USB tokens, secure micro SD cards, etc. These devices include embeded secure applications, such as financial, telecommunication, identity (e-Government), etc and work in hostile environments. In particular, the TOE is dedicated to host the code and data of critical applications.

The security needs for the TOE include:

- Maintaining the integrity of the content of the Security IC memories and the confidentiality of the content of protected memory areas, as required by the application(s) the Security IC is built for
- Maintaining the correct execution of the software residing on the Security IC

1.3.3 Non-TOE Hardware/Software/Firmware

All software running on the TOE is called "Security IC Embedded Software" and is not part of the TOE, except for the software described in section 1.4.1.

1.4 TOE Description

1.4.1 Physical Scope

The TOE comprises:

- Hardware
  - A security IC W76S(2/4)MR(KD/DN/D1/Q1/Q3/4F) version IAD0056PDAA
  - Secure flash W75F32W version D
- Associated IC Dedicated Software
  - Booter - ROM code version 1.2.7
  - FlashLib - ROM code version 1.2.7
  - CryptLib OBJ - version 1.0.7
  - Loader - provided as APDUs sequence version 1.0.0
  - Chip Authentication DB (per customer)
- Guidelines for secure TOE use:
  - Operational User Guidance [15]
  - Preparative Procedure [16]
  - Datasheet [18]
  - Loader Interface User Guide [19]
  - FlashLib Interface User Guide [20]
  - Booter Interface User Guide [21]
  - CryptLib Interface User Guide [22]
  - Secure Flash Interface User Guide [23]
  - For KGD only - Assembly instructions package [24]

1.4.1.1 TOE Architecture

The architecture of the TOE is described in Figure 1.

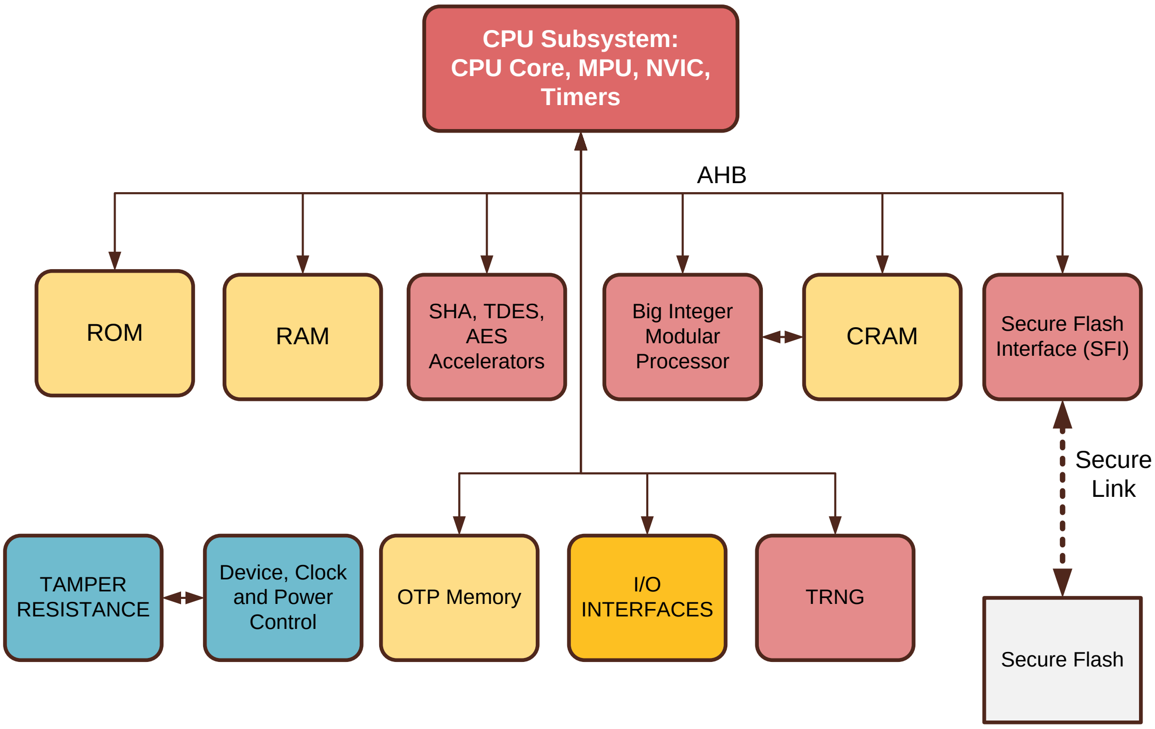

CPU Subsystem:
CPU Core, MPU, NVIC, Timers
AHB
ROM
RAM
SHA, TDES, AES Accelerators
Big Integer Modular Processor
CRAM
Secure Flash Interface (SFI)
Secure Link
TAMPER RESISTANCE
Device, Clock and Power Control
OTP Memory
I/O INTERFACES
TRNG
Secure Flash

Figure 1 TOE Architecture

The TOE consists of the following hardware components

- CPU: ARM SC000-based architecture
- Memories
  - RAM: 32Kbytes
  - ROM: 64Kbytes
  - Secure Flash: 4Mbyte
  - OTP memory: 16Kbytes
  - Cryptographic RAM (CRAM): 4Kbytes
- Interfaces
  - Compliant with ISO7816-3
  - Single Wire Protocol (SWP)
  - SPI (master and slave)
  - I2C (master and slave)
  - UART
  - GPIO
- Clock and Power Management
  - Internally generated, self calibrated clock
  - FULL, SAVE, STANDBY and SLEEP operational modes

- Cryprographic Accelators (HW)
  - TDES cryptoprocessor
  - AES cryptoprocessor
  - SHA cryptoprocessor
  - RSA and ECC Big-Integer Modular Processor (BIGIMOD)
  - True Random Number Generator
- Tamper Resistance

The TOE also includes the following dedicated software components:

- The cryptographic library (Cryplib OBJ), which provides the following features:
  - TDES encryption and decryption in CBC and EBC mode with various key sizes: 112 bits and 168 bits
  - AES encryption and decryption in CBC and ECB mode with various key sizes: 128 bis, 196 bits, and 256 bits
  - Hash computation by SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
  - RSA encryption and decryption with key sizes up to 4032 bit. Key generation is supported up to 4032 bit.
  - ECC operations, such as private scalar multiplication, public scalar multiplication, point validity check, general point addition
  - Random number generator: interface to the hardware True Random Number Generation
- The Flash Loader

1.4.1.2 Interfaces of the TOE

- The physical interface of the TOE with the external environment is the entire surface of the TOE.
- The electrical interface of the TOE with the external environment is the chip's pads (see Section 2.2 of the Datahseet).

1.4.2 Logical Scope

The main security features of the TOE are as follows:

- Unique identification data
- All Test features are disabled in the User mode
- True Random Number Generation compliant with the AIS31 PTG.2 standard
- Cryptographic services: TDES, AES, SHA
- Accelerated RSA and ECC computations
- Memory protection provide by Secure flash: confidentiality and integrity are protected in data storage and code execution
- Detection of power glitch and out-of-spec operating conditions (voltage, temperature, clock frequency)
- Active Shields against physical intrusive attacks (e.g. reverse-engineering, probing)
- Protection against side-channel attacks on TDES and AES

The logical interface of the TOE comprises:

- CPU instruction set
- IC registers
- APIs defined by Cryplib OBJ

1.4.3 Forms of Delivery

The TOE is delivered in one of the following two formats:

- Known Good Die - W76S(2/4)MR KD + W75F32W
- Packaged Device - W76S(2/4)MR(DN/D1/Q1/Q3/4F)

1.5 TOE Operating Modes

The TOE has two distinct modes of operation: Test mode and User mode.

Test mode	The TOE provides access to its test features. This mode is disabled in the phase 3 of the TOE life-cycle.
User mode	The operational mode, dedicated to the TOE user and is enabled in the Phase 3 of the TOE life-cycle. The Test features are not accessible in the User mode. Furthermore, it is not possible to switch back from the User mode to the Test mode.

Table 2 Operating modes

1.6 TOE Life-Cycle

The TOE life-cycle includes several phases (cf. Section 1.2.3 of the BSI-PP-0084 Protection Profile [5]).

Phase	Title	Description
2	IC Development	**IC Designer is responsible for:** • Designing the IC HW • Developing the IC Dedicated Software • Constructing the IC database, which is necessary for the IC photomask fabrication
3	IC Manufacturing and Testing	**The IC Manufacturer is responsible for:** • IC manufacturing **The IC Mask Manufacturer is responsible for:** • Generating the photomasks for the IC manufacturing **The IC Tester is responsible for:** • Testing the IC wafer • Disabling the Test mode **All based upon an output from the Security IC database**
4	**IC Packaging**	**The IC Packaging Manufacturer is responsible for:** • IC packaging stacked with Secure Flash. **The IC Assembled tester is responsible for:** • IC testing

Table 3 TOE Life Cycle

The TOE is delivered in two form factors:

1. W76S(2/4)MRKD is delivered after the phase 3 as a pre- packaged product (Known Good Die).
2. W76S(2/4)MR(DN/D1/Q1/Q3/4F)is delivered after phase 4 as a packed device.

2 Conformance Claim

This chapter contains the following sections:

- CC Conformance Claim
- PP Claim
- Package Claim
- Conformance Claim Rationale

2.1 CC Conformance Claim

This Security target claims to be conformant to the Common Criteria version 3.1 Release 4.

Furthermore, it claims to be CC Part 2 extended and CC Part 3 conformant.

2.2 PP Claim

This Security Target is in strict conformance to the BSI-PP-0084 Protection Profile [5] and includes the following packages:

- Package "Authentication of the Security IC"
- Package "Loader dedicated for usage in the secured environment only"
- Package "Hash-functions"

This Security Target does not claim conformance to any other Protection Profile.

2.3 Package Claim

The assurance level for this Security Target is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

2.4 Conformance Claim Rationale

The product consists of a Security IC and a Secure flash. The TOE is therefore the same as described in BSI-PP-0084 Protection Profile [5], albeit with the flash memory being a separate component.

While this architectural difference may require specific countermeasures, this does not modify the overall Security Problem Definition of the TOE, nor its intended usage:

- the TOE provides the same functionality, and is intended to be used as any Security IC in the sense of [5];
- the TOE is intended to provide the same security resistance as any Security IC in the sense of [5];

The Evaluation Assurance Level (EAL) of the Protection Profile is EAL 4 augmented with the assurance components ALC_DVS.2 and AVA_VAN.5.

The Assurance Requirements of the TOE obtain the Evaluation Assurance Level 5 augmented with the assurance components ALC_DVS.2 and AVA_VAN.5 for the TOE because the TOE is dedicated to store and execute highly critical applications and data which are submitted to advanced logical and physical attacks.

Additionally, the TOE aims at providing further cryptographic capacities to the users of the TOE. Therefore,

- The Organisational Security Policy **P.Crypto-Service** is refined to require the support of AES, TDES, RSA and ECC cryptographic functions;
- The ST include four additional security objectives **O.TDES**, **O.AES**, **O.RSA** and **O.ECC** to enforce this refined Organizational Security Policy;
- The ST includes additional SFRs **FCS_COP.1/RSA**, **FCS_CKM.1/RSA, FCS_COP.1/ECC, FCS_COP.1/TDES** and **FCS_COP.1/AES** to meet these additional objectives.

While these elements are not part of the claimed Protection Profile, they have been inserted in the PP packages related to cryptography, for the sake of clarity.

3 Security Problem Definition

This chapter contains the following sections: - Description of Assets - Threats - Organisational Security Policies - Assumptions

3.1 Assets

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
- 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.

The information and material produced and/or processed by the TOE Manufacturer in the TOE development and production environment (Phases 2 up to TOE Delivery) can be grouped as follows:

- logical design data,
- physical design data,
- IC Dedicated Software, Initialisation Data and Pre-personalisation Data,
- Security IC Embedded Software, provided by the Security IC Embedded Software developer and implemented by the IC manufacturer,
- specific development aids,
- test and characterisation related data,
- material for software development support, and
- photomasks and products in any form

as long as they are generated, stored, or processed by the TOE Manufacturer.

For more details, see Section 3.1 of the Protection Profile [5].

3.2 Threats

The following explanations help to understand the focus of the threats and objectives defined below. For example, certain attacks are only one step towards a disclosure of assets, others may directly lead to a compromise of the application security.

- Manipulation of user data (which includes user data and code of the Composite TOE, stored in or processed by the Security IC) means that an attacker is able to alter a meaningful block of data. This should be considered for the threats T.Malfunction, T.Phys-Manipulation and T.Abuse-Func.
- Disclosure of user data (which may include user data and code of the Composite TOE, stored in protected memory areas or processed by the Security IC) or TSF data means that an attacker is realistically (taking into account the assumed attack potential and for instance the probability of errors) able to determine a meaningful block of data. This should be considered for the threats T.Leak-Inherent, T.Phys-Probing, T.Leak-Forced and T.Abuse-Func.
- Manipulation of the TSF or TSF data means that an attacker is able to deliberately deactivate or otherwise change the behaviour of a specific security functionality in a manner which enables exploitation. This should be considered for the threat T.Malfunction, T.Phys-Manipulation and T.Abuse-Func.

The cloning of the functional behaviour of the Security IC on its physical and command interface is the highest level security concern in the application context.

The cloning of that functional behaviour requires to (i) develop a functional equivalent of the Security IC Embedded Software, (ii) disclose, interpret and employ the user data of the Composite TOE stored in the TOE, and (iii) develop and build a functional equivalent of the Security IC using the input from the previous steps.

The Security IC is a platform for the Security IC Embedded Software which ensures that especially the critical user data of the Composite TOE are stored and processed in a secure way (refer to below). The Security IC Embedded Software must also ensure that critical user data of the Composite TOE are treated as required in the application context (refer to Section 3.4). In addition, the personalisation process supported by the Security IC Embedded Software (and perhaps by the Security IC in addition) must be secure (refer to Section 3.4). This last step is beyond the scope of this ST. As a result the threat 'cloning of the functional behaviour of the Security IC on its physical and command interface's is averted by the combination of mechanisms which split into those being evaluated according to this ST and those being subject to the evaluation of the Security IC Embedded Software or Security IC and the corresponding personalisation process. Therefore, functional cloning is indirectly covered by the security concerns and threats described below.

The Security IC Embedded Software may be required to contribute to averting the threats. At least it must not undermine the security provided by the TOE. For detail, refer to the assumptions regarding the Security IC Embedded Software specified in Section 3.4.

The above security concerns are derived from considering the operational usage by the end-consumer (Phase 7) since

- Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by assumptions and
- the development and production environment starting with Phase 2 up to TOE Delivery are covered by an organisational security policy.

3.2.1 Standard threats

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.

Application Note:

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 or measurement of emanations and can then be related to the specific operation being performed.

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.

Application Note:

Physical probing requires direct interaction with the Security IC internals. 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. 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.

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.

Application Note:

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.

T.Phys-Manipulation

Physical Manipulation

An attacker may physically modify the Secure 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, (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.

Application Note:

The modification may be achieved through techniques commonly employed in IC failure analysis and IC reverse engineering efforts. 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.

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.

Application Note:

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 which normally do not contain significant information about secrets.

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.

3.2.2 Threats related to security services

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.

Application Note:

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.

3.2.3 Package Authentication of the Security IC

If this package "Authentication of the Security IC" is chosen the ST writer shall include the threat "Masquerade the TOE (T.Masquerade_TOE)" as specified below.

T.Masquerade_TOE
Masquerade the TOE

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

Application Note:

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

3.3 Organisational Security Policies

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

3.3.1 Standard Package

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 Packages for Cryptographic Services

P.Crypto-Service

Cryptographic services of the TOE

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

Application Note:

The TOE provides secure hardware and software based cryptographic services for the IC Embedded Software:

- Implementation of the Triple Data Encryption Standard (TDES) algorithm, without key generation or destruction
- Implementation of the Advanced Encryption Standard (AES) algorithm, without key generation or destruction
- Implementation of the Hashing (SHA) algorithm
- Implementation of the RSA algorithm, and associated key generation, without key destruction
- Implementation of the Elliptic Curve Cryptography (ECC) algorithm, without key generation or destruction

3.3.3 Packages for Loader

The organisational security policy "Limiting and Blocking the Loader Functionality (P.Lim_Block_Loader)" applies to Loader dedicated for usage in secured environment.

3.3.3.1 Package 1: Loader dedicated for usage in secured environment only

P.Lim_Block_Loader

Limiting and Blocking the Loader Functionality

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

3.4 Assumptions

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.

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
- materials for software development support as long as they are not under the control of the TOE Manufacturer.

The developer of the Security IC Embedded Software must ensure the appropriate usage of Security IC while developing this software in Phase 1 as described in the (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.

Note that particular requirements for the Security IC Embedded Software are often not clear before considering a specific attack scenario during vulnerability analysis of the Security IC (AVA_VAN). A summary of such results is provided in the document "ETR for composite evaluation" (ETR-COMP). This document will be provided for the evaluation of the composite product. The ETR-COMP may also include guidance for additional tests being required for the combination of hardware and software. The TOE evaluation must be completed before evaluation of the Security IC Embedded Software can be completed. The TOE evaluation can be conducted before and independently from the evaluation of the Security IC Embedded Software.

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 life-cylce phases after TOE delivery are assumed to be protected appropriately.

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.

4 Security Objectives

This chapter Security Objectives contains the following sections: - Security Objectives for the TOE - Security Objectives for the Security IC Embedded Software - Security Objectives for the operational Environment - Security Objectives Rationale

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.

Note, the Security IC may not distinguish between user data which are public known or kept confidential. Therefore the security IC shall protect the user data in integrity and in confidentiality if stored in protected memory areas, unless the Security IC Embedded Software chooses to disclose or modify it. Parts of the Security IC Embedded Software which do not contain secret data or security critical source code, may not require protection from being disclosed. Other parts of the Security IC Embedded Software may need kept confidential since specific implementation details may assist an attacker.

These standard high-level security goals in the context of the security problem definition build the starting point for the definition of security objectives as required by the Common Criteria. Note that the integrity of the TOE is a means to reach these objectives.

In this ST, there is the following high-level security goal related to specific functionality:

- SG4 provide true random numbers.

4.1.1 Standard Security Objectives

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).

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.

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, and 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.

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.

O.Leak-Forced

Protection against Forced Information Leakage

The TOE must be protected against disclosure of confidential data processed in the TOE (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.

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.

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.

4.1.2 Security Objectives related to Specific Functionality

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.

4.1.3 Packages for Crytographic services

4.1.3.1 Package Symmetric cryptographic services

The TOE shall provide Symmetric Cryptographic services Triple-DES (O.TDES) and AES (O.AES) as specified below.

O.TDES

Cryptographic service Triple-DES

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

Application Note: The TOE does not provide key generation or destruction.

O.AES

Cryptographic service AES

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

Application Note: The TOE does not provide key generation or destruction.

4.1.3.2 Package Hash functions

The TOE shall provide Cryptographic service Hash function (O.SHA) as specified below.

O.SHA

Cryptographic service Hash function

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

4.1.3.3 Package RSA

O.RSA

Cryptographic service RSA

The TOE provides secure cryptographic services which are based on a combined hardware and software, for the RSA for encryption and decryption. The TOE also provides prime generation and RSA key pair generation.

Application Note: The TOE does not provide key destruction.

4.1.3.4 Package ECC

O.ECC

Cryptographic service ECC

The TOE provides secure ECC cryptographic services which are based on a combined hardware and software.

Application Note: The TOE does not provide key generation or destruction.

4.1.4 Package Authentication of the Security IC

The TOE shall provide "Authentication to external entities (O.Authentication)" as specified below.

O.Authentication
Authentication to external entities

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

4.1.5 Packages for Loader

4.1.5.1 Package 1: Loader dedicated for usage in secured environment only

The TOE shall provide "Capability and availability of the Loader (O.Cap_Avail_Loader)" as specified below.

O.Cap_Avail_Loader
Capability and availability of the Loader

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

4.2 Security Objectives for the operational Environment

The development of the Security IC Embedded Software is outside the development and manufacturing of the TOE. The Security IC Embedded Software defines the operational use of the TOE. This section describes the security objective for the Security IC Embedded Software.

Note, in order to ensure that the TOE is used in a secure manner the Security IC Embedded Software shall be designed so that the requirements from the following documents are met: (i) hardware data sheet for the TOE, (ii) data sheet of the IC Dedicated Software of the TOE, (iii) TOE application notes, other guidance documents, and (iv) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as referenced in the certification report.

4.2.1 Security Objectives for the Security IC Embedded Software

The development of the Security IC Embedded Software is outside the development and manufacturing of the TOE (cf. section 1.2.3). The Security IC Embedded Software defines the operational use of the TOE. This section describes the security objective for the Security IC Embedded Software.

Note, in order to ensure that the TOE is used in a secure manner the Security IC Embedded Software shall be designed so that the requirements from the following documents are met: (i) hardware data sheet for the TOE, (ii) data sheet of the IC Dedicated Software of the TOE, (iii) TOE application notes, other guidance documents, and (iv) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as referenced in the certification report.

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.

Application Note:

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 Security Objectives for the Operational Environment

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).

4.2.3 Package Authentication of the Security IC

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

OE.TOE_Auth
External entities authenticating of the TOE

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

4.2.4 Packages for Loader

4.2.4.1 Package 1: Loader dedicated for usage in secured environment only

The operational environment of the TOE shall provide "Limitation of capability and blocking the Loader (OE.Lim_Block_Loader)" as specified below.

OE.Lim_Block_Loader
Limitation of capability and blocking the Loader

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

4.3 Security Objectives Rationale

4.3.1 Threats

4.3.1.1 Standard threats

T.Leak-Inherent Refer to the description of this threat and the objective O.Leak-Inherent for full details about rationale.

T.Phys-Probing Refer to the description of this threat and the objective O.Phys-Probing for full details about rationale.

T.Malfunction Refer to the description of this threat and the objective O.Malfunction for full details about rationale.

T.Phys-Manipulation Refer to the description of this threat and the objective O.Phys-Manipulation for full details about rationale.

T.Leak-Forced Refer to the description of this threat and the objective O.Leak-Forced for full details about rationale.

T.Abuse-Func Refer to the description of this threat and the objective O.Abuse-Func for full details about rationale.

The TOE security objective "Capability and availability of the Loader" (O.Cap_Avail_Loader) mitigates also the threat "Abuse of Functionality" (T.Abuse-Func) if attacker tries to misuse the Loader functionality in order to manipulate security services of the TOE provided or depending on IC Dedicated Support Software or user data of the TOE as IC Embedded Software, TSF data or user data of the smartcard product.

4.3.1.2 Threats related to security services

T.RND Refer to the description of this threat and the objective O.RND for full details about rationale.

4.3.1.3 Package Authentication of the Security IC

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

4.3.2 Organisational Security Policies

4.3.2.1 Standard package

P.Process-TOE O.Identification requires that the TOE has to support the possibility of a unique identification. The unique identification can be stored on the TOE. Since the unique identification is generated by the production environment, the production environment must support the integrity of the generated unique identification. The technical and organisational security measures that ensure the security of the development environment and production environment are evaluated based on the assurance measures that are part of the evaluation. The list of material produced and processed by the TOE Manufacturer includes logical/physical design data, specific development aids, test and characterisation data, photomasks and products in any form. All listed items and the associated development and production environments are subject of the evaluation. Therefore, the organisational security policy P.Process-TOE is covered by this objective, as far as organisational measures are concerned.

4.3.2.2 Packages for Cryptographic Services

P.Crypto-Service The security objective 'Cryptographic service Triple-DES (O.TDES)' & 'Cryptographic service AES (O.AES)' & 'Cryptographic service SHA (O.SHA)' & 'Cryptographic service RSA (O.RSA)' & 'Cryptographic service ECC (O.ECC)' enforces the organizational security policy P.Crypto-Service.

4.3.2.3 Packages for Loader

Package 1: Loader dedicated for usage in secured environment only

P.Lim_Block_Loader The organisational security policy Limitation of capability and blocking the Loader (P.Lim_Block_Loader) is directly implemented by the security objective for the TOE "Capability and availability of the Loader (O.Cap_Avail_Loader)" and the security objective for the TOE environment "Limitation of capability and blocking the Loader (OE.Lim_Block_Loader)".

4.3.3 Assumptions

A.Process-Sec-IC The justification related to the assumption "Protection during Packaging, Finishing and Personalisation (A.Process-Sec-IC)" is as follows:

Since OE.Process-Sec-IC requires the Composite Product Manufacturer to implement those measures assumed in A.Process-Sec-IC, the assumption is covered by this objective.

A.Resp-Appl The justification related to the assumption "Treatment of user data of the Composite TOE (A.Resp-Appl)" is as follows:

Since OE.Resp-Appl requires the Security IC Embedded Software to implement measures as assumed in A.Resp-Appl, the assumption is covered by the objective.

4.3.4 SPD and Security Objectives

4.3.4.1 Threats and Security Objectives – Coverage

Threats	Security Objectives	Rationale
T.Leak-Inherent	O.Leak-Inherent	Section 4.3.1
T.Phys-Probing	O.Phys-Probing	Section 4.3.1
T.Malfunction	O.Malfunction	Section 4.3.1
T.Phys-Manipulation	O.Phys-Manipulation	Section 4.3.1
T.Leak-Forced	O.Leak-Forced	Section 4.3.1
T.Abuse-Func	O.Abuse-Func, O.Cap_Avail_Loader	Section 4.3.1
T.RND	O.RND	Section 4.3.1
T.Masquerade_TOE	O.Authentication, OE.TOE_Auth	Section 4.3.1

Table 4 Threats and Security Objectives - Coverage

4.3.4.2 Security Objectives and Threats – Coverage

Security Objectives	Threats
O.Leak-Inherent	T.Leak-Inherent
O.Phys-Probing	T.Phys-Probing
O.Malfunction	T.Malfunction
O.Phys-Manipulation	T.Phys-Manipulation
O.Leak-Forced	T.Leak-Forced
O.Abuse-Func	T.Abuse-Func
O.Identification	
O.RND	T.RND
O.TDES	
O.AES	
O.SHA	
O.RSA	
O.ECC	
O.Authentication	T.Masquerade_TOE
O.Cap_Avail_Loader	T.Abuse-Func
OE.Resp-Appl	
OE.Process-Sec-IC	
OE.TOE_Auth	T.Masquerade_TOE
OE.Lim_Block_Loader	

Table 5 Security Objectives and Threats - Coverage

4.3.4.3 OSPs and Security Objectives – Coverage

Organisational Security Policies	Security Objectives	Rationale
P.Process-TOE	O.Identification	Section 4.3.2
P.Crypto-Service	O.TDES, O.AES, O.SHA, O.ECC, O.RSA	Section 4.3.2
P.Lim_Block_Loader	O.Cap_Avail_Loader, OE.Lim_Block_Loader	Section 4.3.2

Table 6 OSPs and Security Objectives - Coverage

4.3.4.4 Security Objectives and OSPs - Coverage

Security Objectives	Organisational Security Policies
O.Leak-Inherent	
O.Phys-Probing	
O.Malfunction	
O.Phys-Manipulation	
O.Leak-Forced	
O.Abuse-Func	
O.Identification	P.Process-TOE
O.RND	
O.TDES	P.Crypto-Service
O.AES	P.Crypto-Service
O.SHA	P.Crypto-Service
O.RSA	P.Crypto-Service
O.ECC	P.Crypto-Service
O.Authentication	
O.Cap_Avail_Loader	P.Lim_Block_Loader
OE.Resp-Appl	
OE.Process-Sec-IC	
OE.TOE_Auth	
OE.Lim_Block_Loader	P.Lim_Block_Loader

Table 7 Security Objectives and OSPs - Coverage

4.3.4.5 Assumptions and Security Objectives for the Operational Environment - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.Process-Sec-IC	OE.Process-Sec-IC	Section 4.3.3
A.Resp-Appl	OE.Resp-Appl	Section 4.3.3

Table 8 Assumptions and Security Objectives for the Operational Environment - Coverage

4.3.4.6 Security Objectives for the Operational Environment and Assumptions - Coverage

Security Objectives for the Operational Environment	Assumptions
OE.Resp-Appl	A.Resp-Appl
OE.Process-Sec-IC	A.Process-Sec-IC
OE.TOE_Auth	
OE.Lim_Block_Loader	

Table 9 Security Objectives for the Operational Environment and Assumptions - Coverage

5 Extended Requirements

5.1 Extended Families

5.1.1 Extended Family FCS_RNG - Generation of random numbers

5.1.1.1 Description

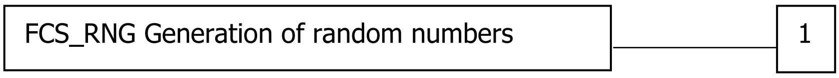
To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

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 Generation of random numbers

1

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.

5.1.1.2 Extended Components

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, [assignment: format of the numbers]] that meet [assignment: a defined quality metric].

5.1.2 Extended Family FMT_LIM - Limited capabilities and availability

5.1.2.1 Description

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.

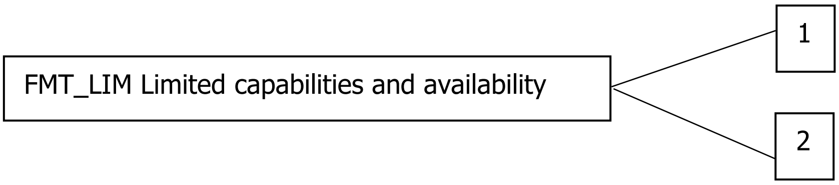
The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

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.

5.1.2.2 Extended Components

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].

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].

5.1.3 Extended Family FAU_SAS - Audit data storage

5.1.3.1 Description

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 Audit data storage
1

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.

5.1.3.2 Extended Components

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].

5.1.4 Extended Family FDP_SDC - Stored data confidentiality

5.1.4.1 Description

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 Stored data confidentiality
1

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.

5.1.4.2 Extended Components

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 **[assignment: memory areas]**.

5.1.5 Extended Family FIA_API - Authentication Proof of Identity

5.1.5.1 Description

To describe the IT security functional requirements of the TOE a functional family FIA_API (Authentication Proof of Identity) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity by the TOE and enables the authentication verification by an external entity. The other families of the class FIA address the verification of the identity of an external entity by the TOE.

The other families of the Class FIA describe only the authentication verification of users identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 (cf. [2], chapter "Extended components definition (APE_ECD)") from a TOE point of view.

FIA_API Authentication Proof of Identity

Family Behaviour

This family defines functions provided by the TOE to prove its identity and to be verified by an external entity in the TOE IT environment.

Component levelling:

FIA_API Authentication Proof of Identity

1

FIA_API.1 Authentication Proof of Identity, provides proof of the identity of the TOE, an object or an authorized user or role to an external entity.

Management FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

There are no actions defined to be auditable.

5.1.5.2 Extended Components

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [selection: [assignment: object, authorized user or role]] to an external entity.

6 Security Requirements

This chapter contains the following sections: - Description of Assets - Threats - Organisational Security Policies - Assumptions

6.1 Security Functional Requirements

In order to define the Security Functional Requirements Part 2 of the Common Criteria was used. However, some Security Functional Requirements have been refined. The refinements are described below the associated SFR.

The refinement operation is used to add detail to a requirement, and, thus, further restricts a requirement. In such a case, an extra paragraph starting with "Refinement" may be given.

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the ST author are denoted as bold and italicized.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the ST author appear in bold text. The iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

6.1.1 Malfunctions

FRU_FLT.2 Limited Fault Tolerance

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.

Application Note:

SF.OPE-COND describes in detail the secure state of the TOE.

FPT_FLS.1 Failure with Preservation of Secure State

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.**

Refinement:

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

Application Note:

SF.OPE-COND describes in detail the secure state of the TOE.

6.1.2 Abuse of Functionality

FMT_LIM.1/Test Limited Capabilities

FMT_LIM.1.1/Test The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced **Deploying 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**.

FMT_LIM.2/Test Limited Availability

FMT_LIM.2.1/Test 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 **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**.

FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide **test process before TOE delivery** with the capability to store ***Initialisation Data and Pre-personalisation Data*** in the **One Time Programmable (OTP) memory and the flash memory**.

6.1.3 Physical Manipulation and Probing

FDP_SDC.1 Stored data Confidentiality

FDP_SDC.1.1 The TSF shall ensure the confidentiality of the information of the user data while it is stored in the **ROM, RAM and Flash memory**.

FDP_SDI.2 Stored Data Integrity Monitoring and Action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for **integrity errors** on all objects, based on the following attributes: **stored in RAM and Flash memory**.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **perform a reset operation**.

FPT_PHP.3 Resistance to Physical Attack

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:

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.

6.1.4 Leakage

FDP_ITT.1 Basic Internal Transfer Protection

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

Refinement:

The different memories (RAM, ROM, Flash, OTP), the CPU and other functional units of the TOE (e.g. a cryptographic accelators) are seen as physically-separated parts of the TOE.

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

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 (RAM, ROM, Flash, OTP), the CPU and other functional units of the TOE (e.g. a cryptographic accelators) are seen as physically-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.

FDP_IFC.1 Subset Information Flow Control

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

Application Note:

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.

6.1.5 Random Numbers

FCS_RNG.1 Random Number Generation

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 *continuously*. 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.**

Refinement:

The entropy source produces random bits when enabled.
After the activation of the entropy source, a self-calibration is done. Then online tests are continuously performed on 20000-bit raw random sequences. If the tests pass, the 20000-bit vectors are processed using a post-processing module. The whitening post-processing module outputs 256 random bits. If a 20000-bit sequence does not pass the online tests then it is filtered out, an alarm is raised and no 256-bit output is generated.

FCS_RNG.1.2 The TSF shall provide **16 bits** that meet

- (PTG.2.6) Test procedure A, no additional standard test suites, 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.

Application Note:

The random number generator is compliant to the definition of PTG.2 in AIS31.

6.1.6 Packages for Crytographic services

6.1.6.1 Package Symmetric Cryptographic services

FCS_COP.1/TDES Cryptographic Operation

FCS_COP.1.1/TDES The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **TDES in ECB mode and CBC mode** and cryptographic key sizes **112 bits and 168 bits** that meet the following: **NIST SP 800-67 [25] and NIST SP 800-38A [26]**.

FCS_COP.1/AES Cryptographic Operation

FCS_COP.1.1/AES The TSF shall perform **decryption and encryption** in accordance with a specified cryptographic algorithm **AES in ECB mode and CBC mode** and cryptographic key sizes **128 bit, 192 bit and 256 bit** that meet the following: **FIPS 197 [27] and NIST SP 800-38A [26]**.

6.1.6.2 Package Hash functions

FCS_COP.1/SHA Cryptographic Operation

FCS_COP.1.1/SHA The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512** and cryptographic key sizes **none** that meet the following: **FIPS 180-4 [28]**.

Application Note:

- *The use of the SHA-1 function is restricted to HMAC-SHA1 functions. SHA-224 is maintained for legacy mechanisms.*
- *The use of these functionalities requires specific security improvement and DPA analysis by the Embedded Software, which is not part of the TOE.*

6.1.6.3 Package RSA

FCS_COP.1/RSA Cryptographic Operation

FCS_COP.1.1/RSA The TSF shall perform **RSA public and private key operation with or without CRT** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **up to 4032 bits** that meet the following: **PKCS#1 v2.2 [31]**.

Application Note:

The use of RSA is restricted to key sizes greater than 1900 bits for legacy mechanisms. The recommended key size shall be greater than 3000 bits.

Other key sizes are not covered by the certification.

FCS_CKM.1/RSA Cryptographic Key Generation

FCS_CKM.1.1/RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **prime generation and RSA key pair generation** and specified cryptographic key sizes **up to 4032 bits** that meet the following: **FIPS 140-2 [29] and FIPS 186-4 [30]**.

Application Note:

The use of RSA is restricted to key sizes greater than 1900 bits for legacy mechanisms. The recommended key size shall be greater than 3000 bits.

Other key sizes are not covered by the certification.

6.1.6.4 Package ECC

FCS_COP.1/ECC Cryptographic Operation

FCS_COP.1.1/ECC The TSF shall perform **private scalar multiplication, public scalar multiplication, point validity check, general point addition** in accordance with a specified cryptographic algorithm **Elliptic Curves Cryptography over prime fields** and cryptographic key sizes **up to 521 bits** that meet the following: **None**.

Application Note:

The ECC engine supports any valid curves over prime fields of size up to 521.
However, the recommended curves specified below fall in the scope of the evaluation (see [10], sec 4.3):
- NIST: NIST P-256, NIST P-384, NIST P-521
- Brainpool: BrainpoolP256r1, Brainpool384r1, BrainpoolP521
- FR: JORF FRP256v1

6.1.7 Package Authentication of the Security IC

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

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a **challenge-response authentication method** to prove the identity of the **TOE** to an external entity.

6.1.8 Packages for Loader

6.1.8.1 Package 1: Loader dedicated for usage in secured environment only

FMT_LIM.1/Loader Limited Capabilities

FMT_LIM.1.1/Loader The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced **Deploying Loader functionality after Load De-activation does not allow User Data to be disclosed or manipulated by unauthorized user**.

FMT_LIM.2/Loader Limited Availability

FMT_LIM.2.1/Loader The TSF shall be designed in a manner that limits its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced **The TSF prevents deploying the Loader functionality after Load De-activation**.

6.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL5 augmented with AVA_VAN.5 and ALC_DVS.2.

6.3 Security Requirements Rationale

6.3.1 Objectives

6.3.1.1 Security Objectives for the TOE

<u>Standard Security Objectives</u>

O.Leak-Inherent The refinements of the security functional requirements FPT_ITT.1 and FDP_ITT.1 together with the policy statement in FDP_IFC.1 explicitly require the prevention of disclosure of secret data (TSF data as well as user data) when transmitted between separate parts of the TOE or while being processed. This includes that attackers cannot reveal such data by measurements of emanations, power consumption or other behaviour of the TOE while data are transmitted between or processed by TOE parts.

It is possible that the TOE needs additional support by the Security IC Embedded Software (e.g. timing attacks are possible if the processing time of algorithms implemented in the software depends on the content of secret). This support must be addressed in the Guidance Documentation. Together with this FPT_ITT.1, FDP_ITT.1 and FDP_IFC.1 are suitable to meet the objective.

O.Phys-Probing The SFR FDP_SDC.1 requires the TSF to protect the confidentiality of the information of the user data stored in specified memory areas and prevent its compromise by physical attacks bypassing the specified interfaces for memory access. The scenario of physical probing as described for this objective is explicitly included in the assignment chosen for the physical tampering scenarios in FPT_PHP.3. Therefore, it is clear that this security functional requirement supports the objective.

It is possible that the TOE needs additional support by the Security IC Embedded Software (e.g. to send data over certain buses only with appropriate precautions). This support must be addressed in the Guidance Documentation. Together with this FPT_PHP.3 is suitable to meet the objective.

O.Malfunction The definition of this objective shows that it covers a situation, where malfunction of the TOE might be caused by the operating conditions of the TOE (while direct manipulation of the TOE is covered O.Phys-Manipulation). There are two possibilities in this situation: Either the operating conditions are inside the tolerated range or at least one of them is outside of this range. The second case is covered by FPT_FLS.1, because it states that a secure state is preserved in this case. The first case is covered by FRU_FLT.2 because it states that the TOE operates correctly under normal (tolerated) conditions. The functions implementing FRU_FLT.2 and FPT_FLS.1 must work independently so that their operation cannot affected by the Security IC Embedded Software (refer to the refinement). Therefore, there is no possible instance of conditions under O.Malfunction, which is not covered.

O.Phys-Manipulation The SFR FDP_SDI.2 requires the TSF to detect the integrity errors of the stored user data and react in case of detected errors. The scenario of physical manipulation as described for this objective is explicitly included in the assignment chosen for the physical tampering scenarios in FPT_PHP.3. Therefore, it is clear that this security functional requirement supports the objective.

It is possible that the TOE needs additional support by the Embedded Software (for instance by implementing FDP_SDI.1 to check data integrity with the help of appropriate checksums). This support must be addressed in the Guidance Documentation. Together with this FPT_PHP.3 is suitable to meet the objective.

O.Leak-Forced This objective is directed against attacks, where an attacker wants to force an information leakage, which would not occur under normal conditions. In order to achieve this the attacker has to combine a first attack step, which modifies the behaviour of the TOE (either by exposing it to extreme operating conditions or by directly manipulating it) with a second attack step measuring and analysing some output produced by the TOE. The first step is prevented by the same mechanisms which support O.Malfunction and O.Phys-Manipulation, respectively. The requirements FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FRU_FLT.2, FPT_FLS.1, FPT_PHP.3 covering O.Leak-Inherent also support O.Leak-Forced because they prevent the attacker from being successful if he tries the second step directly.

O.Abuse-Func This objective states that abuse of functions (especially provided by the IC Dedicated Test Software, for instance in order to read secret data) must not be possible in Phase 7 of the life-cycle. There are two possibilities to achieve this: (i) They cannot be used by an attacker (i. e. its availability is limited) or (ii) using them would not be of relevant use for an attacker (i. e. its capabilities are limited) since the functions are designed in a specific way. The first possibility is specified by FMT_LIM.2/Test and the second one by FMT_LIM.1/Test. Since these requirements are combined to support the policy, which is suitable to fulfil O.Abuse-Func, both security functional requirements together are suitable to meet the objective.

Other security functional requirements FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1 which prevent attackers from circumventing the functions implementing these two security functional requirements (for instance by manipulating the hardware) also support the objective.

It was chosen to define FMT_LIM.1/Test and FMT_LIM.2/Test explicitly (not using Part 2 of the Common Criteria) for the following reason: Though taking components from the Common Criteria catalogue makes it easier to recognise functions, any selection from Part 2 of the Common Criteria would have made it harder for the reader to understand the special situation meant here. As a consequence, the statement of explicit security functional requirements was chosen to provide more clarity.

O.Identification Obviously the operations for FAU_SAS.1 are chosen in a way that they require the TOE to provide the functionality needed for O.Identification. The Initialisation Data (or parts of them) are used for TOE identification. The technical capability of the TOE to store Initialisation Data and/or Pre-personalisation Data is provided according to FAU_SAS.1.

It was chosen to define FAU_SAS.1 explicitly (not using a given security functional requirement from Part 2 of the Common Criteria) for the following reason: The security functional requirement FAU_GEN.1 in Part 2 of the CC requires the TOE to generate the audit data and gives details on the content of the audit records (for instance data and time). The possibility to use the functions in order to store security relevant data which are generated outside of the TOE, is not covered by the family FAU_GEN or by other families in Part 2. Moreover, the TOE cannot add time information to the records, because it has no real time clock. Therefore, the new family FAU_SAS was defined for this situation.

Security Objectives related to Specific Functionality

O.RND FCS_RNG.1 requires the TOE to provide random numbers of good quality. To specify the exact metric is left to the individual Security Target for a specific TOE.

Other security functional requirements, which prevent physical manipulation and malfunction of the TOE (see the corresponding objectives listed in the table) support this objective because they prevent attackers from manipulating or otherwise affecting the random number generator.

Random numbers are often used by the Security IC Embedded Software to generate cryptographic keys for internal use. Therefore, the TOE must prevent the unauthorised disclosure of random numbers. Other security functional requirements which prevent inherent leakage attacks, probing and forced leakage attacks ensure the confidentiality of the random numbers provided by the TOE.

Depending on the functionality of specific TOEs the Security IC Embedded Software will have to support the objective by providing runtime-tests of the random number generator. Together, these requirements allow the TOE to provide cryptographically good random numbers and to ensure that no information about the produced random numbers is available to an attacker.

It was chosen to define FCS_RNG.1 explicitly, because Part 2 of the Common Criteria do not contain generic security functional requirements for Random Number generation. (Note, that there are security functional requirements in Part 2 of the Common Criteria, which refer to random numbers. However, they define requirements only for the authentication context, which is only one of the possible applications of random numbers.)

Packages for Crytographic services

Package Symmetric cryptographic services

O.TDES The FCS_COP.1/TDES meets the security objective 'Cryptographic service Triple-DES (O.TDES)'.

O.AES The FCS_COP.1/AES meets the security objective 'Cryptographic service AES (O.AES)'.

Package Hash functions

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

Package RSA

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

Package ECC

O.ECC The FCS_COP.1/ECC meets the security objective 'Cryptographic service ECC (O.ECC)'.

Package Authentication of the Security IC

O.Authentication The security objective "Authentication to external entities (O.Authentication)" is directly covered by the SFR FIA_API.1.

Packages for Loader

Package 1: Loader dedicated for usage in secured environment only

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

6.3.2 Rationale tables of Security Objectives and SFRs

6.3.2.1 Security Objectives and SFRs - Coverage

Security Objectives	Security Functional Requirements	Rationale
O.Leak-Inherent	FDP_ITT.1, FPT_ITT.1, FDP_IFC.1	Section 6.3.1
O.Phys-Probing	FPT_PHP.3, FDP_SDC.1	Section 6.3.1
O.Malfunction	FRU_FLT.2, FPT_FLS.1	Section 6.3.1
O.Phys-Manipulation	FDP_SDI.2, FPT_PHP.3	Section 6.3.1
O.Leak-Forced	FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FRU_FLT.2, FPT_FLS.1, FPT_PHP.3	Section 6.3.1
O.Abuse-Func	FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1, FMT_LIM.1/Test, FMT_LIM.2/Test	Section 6.3.1
O.Identification	FAU_SAS.1	Section 6.3.1
O.RND	FCS_RNG.1, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1	Section 6.3.1
O.TDES	FCS_COP.1/TDES	Section 6.3.1
O.AES	FCS_COP.1/AES	Section 6.3.1
O.SHA	FCS_COP.1/SHA	Section 6.3.1
O.RSA	FCS_COP.1/RSA, FCS_CKM.1/RSA	Section 6.3.1
O.ECC	FCS_COP.1/ECC	Section 6.3.1
O.Authentication	FIA_API.1	Section 6.3.1
O.Cap_Avail_Loader	FMT_LIM.1/Loader, FMT_LIM.2/Loader	Section 6.3.1

Table 10 Security Objectives and SFRs - Coverage

6.3.2.2 SFRs and Security Objectives

Security Functional Requirements	Security Objectives
FRU_FLT.2	O.Malfunction, O.Leak-Forced, O.Abuse-Func, O.RND
FPT_FLS.1	O.Malfunction, O.Leak-Forced, O.Abuse-Func, O.RND
FMT_LIM.1/Test	O.Abuse-Func
FMT_LIM.2/Test	O.Abuse-Func
FAU_SAS.1	O.Identification
FDP_SDC.1	O.Phys-Probing
FDP_SDI.2	O.Phys-Manipulation
FPT_PHP.3	O.Phys-Probing, O.Phys-Manipulation, O.Leak-Forced, O.Abuse-Func, O.RND
FDP_ITT.1	O.Leak-Inherent, O.Leak-Forced, O.Abuse-Func, O.RND
FPT_ITT.1	O.Leak-Inherent, O.Leak-Forced, O.Abuse-Func, O.RND
FDP_IFC.1	O.Leak-Inherent, O.Leak-Forced, O.Abuse-Func, O.RND
FCS_RNG.1	O.RND
FCS_COP.1/TDES	O.TDES
FCS_COP.1/AES	O.AES
FCS_COP.1/SHA	O.SHA
FCS_COP.1/RSA	O.RSA
FCS_CKM.1/RSA	O.RSA
FCS_COP.1/ECC	O.ECC
FIA_API.1	O.Authentication
FMT_LIM.1/Loader	O.Cap_Avail_Loader
FMT_LIM.2/Loader	O.Cap_Avail_Loader

Table 11 SFRs and Security Objectives

6.3.3 Dependencies

6.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FRU_FLT.2	(FPT_FLS.1)	FPT_FLS.1
FPT_FLS.1	No Dependencies	
FMT_LIM.1/Test	(FMT_LIM.2)	FMT_LIM.2/Test
FMT_LIM.2/Test	(FMT_LIM.1)	FMT_LIM.1/Test
FAU_SAS.1	No Dependencies	
FDP_SDC.1	No Dependencies	
FDP_SDI.2	No Dependencies	
FPT_PHP.3	No Dependencies	
FDP_ITT.1	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1
FPT_ITT.1	No Dependencies	
FDP_IFC.1	(FDP_IFF.1)	
FCS_RNG.1	No Dependencies	
FIA_API.1	No Dependencies	
FCS_COP.1/TDES	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	
FCS_COP.1/AES	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	
FCS_COP.1/SHA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	
FCS_COP.1/RSA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/RSA
FCS_CKM.1/RSA	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/RSA
FCS_COP.1/ECC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	
FMT_LIM.1/Loader	(FMT_LIM.2)	FMT_LIM.2/Loader
FMT_LIM.2/Loader	(FMT_LIM.1)	FMT_LIM.1/Loader

Table 12 SFRs Dependencies

Rationale for the exclusion of Dependencies

The dependency FDP_IFF.1 of FDP_IFC.1 is discarded. Part 2 of the Common Criteria defines the dependency of FDP_IFC.1 (information flow control policy statement) on FDP_IFF.1 (Simple security attributes). The specification of FDP_IFF.1 would not capture the nature of the security functional requirement nor add any detail.

As stated in the Data Processing Policy referred to in FDP_IFC.1, there are no attributes necessary. The security functional requirement for the TOE is sufficiently described using FDP_ITT.1 and its Data Processing Policy (FDP_IFC.1).

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/TDES is discarded. The security functional requirement FCS_CKM.1 and on which FCS_COP.1/TDES depends, are not included in this security target because the TOE only provides a TDES engine for encryption and decryption. The key generation should be managed by the Security IC Embedded Software.

The dependency FCS_CKM.4 of FCS_COP.1/TDES is discarded. The security functional requirement FCS_CKM.1 and on which FCS_COP.1/TDES depends, are not included in this security target because the TOE only provides a TDES engine for encryption and decryption. The key destruction should be managed by the Security IC Embedded Software.

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/AES is discarded. The security functional requirement FCS_CKM.1 and on which FCS_COP.1/AES depends, are not included in this security target because the TOE only provides an AES engine for encryption and decryption. The key generation should be managed by the Security IC Embedded Software.

The dependency FCS_CKM.4 of FCS_COP.1/AES is discarded. The security functional requirement FCS_CKM.1 and on which FCS_COP.1/AES depends, are not included in this security target because the TOE only provides a AES engine for encryption and decryption. The key destruction should be managed by the Security IC Embedded Software.

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/SHA is discarded. Because no key is used there is no need for key import as required by dependency to FDP_ITC.1, FDP_ITC.2 or key generation as required by dependency to FCS_CKM.1

The dependency FCS_CKM.4 of FCS_COP.1/SHA is discarded. Because no key is used there is no need for key destruction as required by dependency to FCS_CKM.4.

The dependency FCS_CKM.4 of FCS_COP.1/RSA is discarded. The security functional requirement FCS_CKM.4, on which FCS_COP.1/RSA depends, is not included in this security target because the TOE only provides a RSA engine for public/private key operation with or without CRT. The key destruction should be managed by the Security IC Embedded Software.

The dependency FCS_CKM.4 of FCS_CKM.1/RSA is discarded. The security functional requirement FCS_CKM.4, on which FCS_CKM.1/RSA depends, is not included in this security target because the TOE only provides a RSA engine for public/private key operation with or without CRT. The key destruction should be managed by the Security IC Embedded Software.

The dependency FCS_CKM.4 of FCS_COP.1/ECC is discarded. The security functional requirement FCS_CKM.4, on which FCS_COP.1/ECC depends, is not included in this security target because the TOE only provides a ECC engine for

- private scalar multiplication
- public scalar multiplication
- point validity check
- general point addition.

The key destruction should be managed by the Security IC Embedded Software.

The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/ECC is discarded. The security functional requirement FCS_CKM.1, on which FCS_COP.1/ECC depends, is not included in this security target because the TOE only provides a ECC engine for

- private scalar multiplication
- public scalar multiplication
- point validity check
- general point addition.

The key generation should be managed by the Security IC Embedded Software.

6.3.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.5, ADV_TDS.4
ADV_FSP.5	(ADV_IMP.1) and (ADV_TDS.1)	ADV_IMP.1, ADV_TDS.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.4, ALC_TAT.2
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1)	ADV_IMP.1, ADV_TDS.4, ALC_TAT.2
ADV_TDS.4	(ADV_FSP.5)	ADV_FSP.5
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.5
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.5, ALC_DVS.2, ALC_LCD.1
ALC_CMS.5	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.2	(ADV_IMP.1)	ADV_IMP.1

Requirements	CC Dependencies	Satisfied Dependencies
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.5, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.5, ATE_FUN.1
ATE_DPT.3	(ADV_ARC.1) and (ADV_TDS.4) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.5, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_TDS.4, AGD_OPE.1, AGD_PRE.1, ATE_DPT.3

Table 13 SARs Dependencies

6.3.4 Rationale for the Security Assurance Requirements

An assurance level of EAL5 with the augmentations AVA_VAN.5 and ALC_DVS.2 are 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 defence against such attacks, the evaluators should have access to the low level design and source code.

6.3.4.1 AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the intended use of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component.

Independent vulnerability analysis is based on highly detailed technical information. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing high attack potential.

AVA_VAN.5 has dependencies to ADV_ARC.1 "Security architecture description", ADV_FSP.2 "Security enforcing functional specification", ADV_TDS.3 "Basic modular design", ADV_IMP.1 "Implementation representation of the TSF", AGD_OPE.1 "Operational user guidance", and AGD_PRE.1 "Preparative procedures". All these dependencies are satisfied by EAL5.

It has to be assumed that attackers with high attack potential try to attack secure element used for digital signature applications or payment systems. Therefore, specifically AVA_VAN.5 was chosen in order to assure that even these attackers cannot successfully attack the TOE.

6.3.4.2 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE.

In the particular case of a secure elment the TOE is developed and produced within a complex and distributed industrial process which must especially be protected. Details about the implementation, (e.g. from design, test and development tools as well as Initialisation Data) may make such attacks easier. Therefore, in the case of a secure element, maintaining the confidentiality of the design is very important.

This assurance component is a higher hierarchical component to EAL5 (which only requires ALC_DVS.1). ALC_DVS.2 has no dependencies.

7 TOE Summary Specification

This chapter contains the following sections: - Description of the TOE security features - TOE security features rationale

7.1 TOE Summary Specification

SF.PHY-PRO

Physical Protection

SF.PHY-PRO protects the TOE against physical manipulation (including the TOE probing). SF.PHY-PRO also protects the TOE against the inherent or intentional leak of the TOE operations.

SF.OPE-MODE

Control of Operating Modes

SF.OPE-MODE ensures that the User Data is not disclosed or manipulated via the features avalailable in the Test mode.

SF.MEM-PRO

Memory Protection

SF.MEM-PRO protects the confidentiality and the integrity of the data stored in the memories (RAM, ROM, Flash).

SF.OPE-COND

Operational Conditions

SF.OPE-COND ensures the correct operation of the TOE during the execution of the IC Dedicated Support Software and Security IC Embedded Software in the normal operational conditions (which are controlled by the detectors).

SF.OPE-COND also ensures the secure state of the TOE in case of abnormal condition is detected.

SF.RNG

Random Generation

SF.RNG provides a true random generator which is compliant with the AIS31 standard, PTG.2 class. This random generation integrates the online statistical test as defined in [17].

SF.CRYPTO

Cryptographic Services

SF.CRYPTO provides the following cryptographic services:

- TDES encryption and decryption in CBC and EBC mode with various key sizes: 112 bits and 168 bits
- AES encryption and decryption in CBC and ECB mode with various key sizes: 128 bis, 196 bits, and 256 bits
- Hash computation by SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
- RSA encryption and decryption with key sizes up to 4032 bit, as well as associated key generation up to 4032 bit
- ECC private scalar multiplication, public scalar multiplication, point validity check and general point addition.

SF.SEC-ID

Secure Storage of the TOE Init Data

SF.SEC-ID protects the initialisation data and the pre-personalisation data against any illegal modification. To this end, SF.SEC-ID implements the following security mechanisms:

- SM.OTP: the initialisation and pre-personalisation data are stored in the One Time Programmable (OTP) memory.

SF.SEC-ID also enables the identification of the TOE components (the hardware but also the IC dedicated software).

7.2 SFRs and TSS

7.2.1 SFRs and TSS – Rationale

7.2.1.1 TOE Summary Specification

SF.PHY-PRO enforces the TOE resistance against physical attacks (FPT_PHP.3). SF.PHY-PRO contributes to the integrity and confidentiality protection of the User data stored in the TOE (FDP_SDI.2 and FDP_SDC.1). The cryptographic services are also protected against the physical attacks. SF.PHY-PRO protects against some attacks on the cryptographic services.

SF.OPE-MODE enforces the restriction of the TSF capabilities and availabily during the deployment of the test features after the TOE delivery (respectively FMT_LIM.1/Test and FMT_LIM.2/Test). In the same manner, it also enforces the restriction of the loading capability after the code loading (FMT_LIM.1/Loader and FMT_LIM.2/Loader). FIA_API.1 ensures that the TOE is authenticated when used during code loading.

SF.MEM-PRO By definition, SF.MEM-PRO enforces FDP_SDC.1 and FDP_SDI.2.

SF.OPE-COND enforces the TOE fault-tolerance and fail-secure (respectively FRU_FLT.2 and FPT_FLS.1).

SF.RNG enforces the true random generation.

SF.CRYPTO enforces the following SFRs:

- TDES encryption and decryption (FCS_COP.1/TDES)
- AES encryption and decryption (FCS_COP.1/AES)
- SHA (FCS_COP.1/SHA)
- RSA encryption and decryption (FCS_COP.1/RSA and FCS_CKM.1/RSA) and key generation (FCS_CKM.1/RSA)
- ECC basic functions (FCS_COP.1/ECC)

SF.SEC-ID enforces the security functional requirement FAU_SAS.1.

7.2.2 Association tables of SFRs and TSS

7.2.2.1 SFRs and TSS - Coverage

Security Functional Requirements	TOE Summary Specification
FRU_FLT.2	SF.OPE-COND
FPT_FLS.1	SF.OPE-COND
FMT_LIM.1/Test	SF.OPE-MODE
FMT_LIM.2/Test	SF.OPE-MODE
FAU_SAS.1	SF.SEC-ID
FDP_SDC.1	SF.MEM-PRO
FDP_SDI.2	SF.MEM-PRO, SF.PHY-PRO
FPT_PHP.3	SF.PHY-PRO
FDP_ITT.1	SF.PHY-PRO
FPT_ITT.1	SF.PHY-PRO
FDP_IFC.1	SF.PHY-PRO
FCS_RNG.1/PTG	SF.RNG, SF.PHY-PRO
FCS_COP.1/TDES	SF.CRYPTO, SF.PHY-PRO
FCS_COP.1/AES	SF.CRYPTO, SF.PHY-PRO
FCS_COP.1/SHA	SF.CRYPTO, SF.PHY-PRO
FCS_COP.1/RSA	SF.CRYPTO, SF.PHY-PRO
FCS_CKM.1/RSA	SF.CRYPTO, SF.PHY-PRO
FCS_COP.1/ECC	SF.CRYPTO, SF.PHY-PRO
FIA_API.1	SF.OPE-MODE
FMT_LIM.1/Loader	SF.OPE-MODE
FMT_LIM.2/Loader	SF.OPE-MODE

Table 14 SFRs and TSS - Coverage

7.2.2.2 TSS and SFRs – Coverage

TOE Summary Specification	Security Functional Requirements
SF.PHY-PRO	FDP_SDI.2, FPT_PHP.3, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FCS_RNG.1/PTG, FCS_COP.1/TDES, FCS_COP.1/AES, FCS_COP.1/SHA, FCS_COP.1/RSA, FCS_CKM.1/RSA, FCS_COP.1/ECC
SF.OPE-MODE	FMT_LIM.1/Test, FMT_LIM.2/Test, FIA_API.1, FMT_LIM.1/Loader, FMT_LIM.2/Loader
SF.MEM-PRO	FDP_SDC.1, FDP_SDI.2
SF.OPE-COND	FRU_FLT.2, FPT_FLS.1
SF.RNG	FCS_RNG.1/PTG
SF.CRYPTO	FCS_COP.1/TDES, FCS_COP.1/AES, FCS_COP.1/SHA, FCS_COP.1/RSA, FCS_CKM.1/RSA, FCS_COP.1/ECC
SF.SEC-ID	FAU_SAS.1

Table 15 TSS and SFRs - Coverage

8 Revisions

Modification	Comment
A	First version based on complete ST version J

Table 16 History of Modifications

9 ANNEX

9.1 Glossary

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.

Authentication reference data

Data used to verify the claimed identity in an authentication procedure.

Authentication verification data

Data used to prove the claimed identity in an authentication procedure.

Composite Product Integrator

Role installing or finalising the IC Embedded Software and the applications on platform transforming the TOE into the unpersonalised Composite Product after TOE delivery.

The TOE Manufacturer may implement IC Embedded Software delivered by the Security IC Embedded Software Developer before TOE delivery (e.g. if the IC Embedded Software is implemented in ROM or is stored in the non-volatile memory as service provided by the IC Manufacturer or IC Packaging Manufacturer).

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.

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 (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).

IC Dedicated Test Software

That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.

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.

Initialisation Data

Initialisation 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). If "Package Authentication of the Security IC" is used the Initialisation data contain the confidential authentication verification data of the IC. If the "Package 2: Loader dedicated for usage by authorized users only" may contain the authentication verification data or key material for the trusted channel between the TOE and the authorized users using the Loader.

Integrated Circuit (IC)

Electronic component(s) designed to perform processing and/or memory functions.

Pre-personalisation 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. If "Package 2: Loader dedicated for usage by authorized users only" is used the Pre-personalisation Data may contain the authentication reference data or key material for the trusted channel between the TOE and the authorized users using the Loader.

Security IC

(as used in this Protection Profile) Composition of the TOE, the Security IC Embedded Software, user data of the Composite TOE and the package (the Security IC carrier).

Security IC Embedded Software

Software embedded in a Security IC and normally not being developed by the IC Designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3 or in later phases of the Security IC product life-cycle.

Some part of that software may actually implement a Security IC application others may provide standard services. Nevertheless, this distinction doesn't matter here so that the Security IC Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.

Security IC Product

Composite product which includes the Security Integrated Circuit (i.e. the TOE) and the Embedded Software and is evaluated as composite target of evaluation in the sense of the Supporting Document

Secured Environment

Operational environment maintains the confidentiality and integrity of the TOE as addressed by OE.Process-Sec-IC and the confidentiality and integrity of the IC Embedded Software, TSF data or user data associated with the smartcard product by security procedures of the smartcard product manufacturer, personaliser and other actors before delivery to the smartcard end-user depending on the smartcard life-cycle.

Secure Flash Front-end (SFF)

the SPI interface on the memory chip (i.e. SPI Slave)

Secure Flash Interface (SFI)

the SPI interface on the Host device (i.e. SPI Master)

Serial Peripheral Interface (SPI)

a synchronous serial data link, a *de facto* standard, that operates in full duplex mode

Test Features

All features and functions (implemented by the IC Dedicated Test Software and/or hardware) 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.

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 for the operation of the TOE upon which the enforcement of the SFR relies. They are 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 non-volatile programmable memories (for instance EEPROM or flash memory), in specific circuitry or a combination thereof.

User data of the Composite TOE

All data managed by the Smartcard Embedded Software in the application context.

User data of the TOE

Data for the user of the TOE, that does not affect the operation of the TSF. From the point of view of TOE defined in this PP the user data comprises the Security IC Embedded Software and the user data of the Composite TOE.

9.2 Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functionality
TSFI	TSF Interface
TSP	TOE Security Policy

9.3 References

[1] Common Criteria, *Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001*

[2] Common Criteria, Part 2: *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002*

[3] Common Criteria, Part 3: *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003*

[4] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004*

[5] Eurosmart, *Security IC Platform with Augmentation Packages, Version 1.0, February 2014, BSI-PP-0084*.

[6] Joint Interpretation Library: *Application of Attack Potential to Smartcards, January 2013, Version 2.9*

[7] Supporting Document, Mandatory Technical Document: *The Application of CC to Integrated Circuits, March 2009, Version 3.0, Revision 1, CCDB-2009-03-002*

[8] Supporting Document Guidance: *Smartcard Evaluation, February 2010, Version 2.0, CCDB-2010-03-001*

[9] *Supporting Document Guidance Security Architecture requirements (ADV_ARC) for smart cards and similar devices, April 2012, Version 2.0, CCDB-2012-04-003*

[10] SOG-IS Crypto Working Group: *SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, May 2016, Version 1.0*

[11] Supporting Document Mandatory Technical Document: *Application of Attack Potential to Smartcards April 2012, Version 2.8, CCDB-2012-04-002*

[12] Supporting Document: *Composite product evaluation for Smart Cards and similar devices, April 2012, Version 2.1, CCDB-2012-04-001*

[13] Joint Interpretation Library: *Minimum Site Security Requirements (For trial use), 2013*

[14] ISO/IEC 7816-3. *Identification cards — integrated circuit cards. Part 3: Cards with contacts Electrical interface and transmission protocols*.

[15] Winbond Technology Ltd., *W76Sxx Winbond TrustME^{TM} Security Element, Operational User Guidance*.

[16] Winbond Technology Ltd., *W76Sxx Winbond TrustME^{TM}, Preparative Procedure*

[17] A proposal for: *Functionality classes for random number generators, BSI, Version 2.0 , 18 September 2011*

[18] Winbond Technology Ltd., *W76Sxx Winbond TrustME^{TM}, Datasheet*.

[19] Winbond Technology Ltd., *W76Sxx Loader Interface User Guide*

[20] Winbond Technology Ltd., *W76Sxx FlashLib Interface User Guide*

[21] Winbond Technology Ltd., *W76Sxx Booter Interface User Guide*

[22] Winbond Technology Ltd., *W76Sxx CryptLib Interface User Guide*

[23] Winbond Technology Ltd., *Secure Serial Flash Memory Secure Flash Interface (SFI) Specifications and User Guide*

[24] For KGD form only - *W76Sxx Winbond TrustME™ Secure Element: Assembly instructions package*

[25] National Institute of Standards and Technology, NIST SP 800-67: *Recommendation for Triple Data Encryption Algorithm (TDEA) Block Cipher, January 2012*.

[26] National Institute of Standards and Technology, NIST SP 800-38A: *Recommendation for Block Cipher Modes of Operation, 2001, with Addendum Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, October 2010*.

[27] US DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, *FISP 197: ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001*.

[28] US DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, *FISP 180-4: SECURE HASH STANDARD, February 11, 2011*.

[29] US DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, *FISP 140-2: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, May 25, 2001*.

[30] US DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, *FISP 186-4: Digital Signature Standard (DSS), July 2013*.

[31] RSA Laboratories, *PKCS#1 v2.2: RSA Cryptography Standard, October 27, 2012*.

9.4 Index

Preliminary Designation

The “Preliminary” designation on a Winbond datasheet indicates that the product is not fully characterized. The specifications are subject to change without notice and are not guaranteed. Winbond or an authorized sales representative should be consulted for current information before using this product.

Trademarks

Winbond, SpiFlash and TrustME are trademarks of Winbond Electronics Corporation.

ARM and SecureCore are registered trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. All rights reserved.

All other marks are the property of their respective owner.

Licenses

ICs with DPA countermeasure functionality

LICENSED DPA™ COUNTERMEASURES	WINBOND ICs containing functionality implementing countermeasures to Differential Power Analysis are produced and sold under license from Cryptography Research Inc.

Important Notice

Winbond products are not designed, intended, authorized or warranted for use as components in systems or equipment intended for surgical implantation, atomic energy control instruments, airplane or spaceship instruments, transportation instruments, traffic signal instruments, combustion control instruments, or for other applications intended to support or sustain life. Furthermore, Winbond products are not intended for applications wherein failure of Winbond products could result or lead to a situation wherein personal injury, death or severe property or environmental damage could occur. Winbond customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Winbond for any damages resulting from such improper use or sales.

Information in this document is provided solely in connection with Winbond products. Winbond reserves the right to make changes, corrections, modifications or improvements to this document and the products and services described herein at any time, without notice.

Please note that all data and specifications are subject to change without notice.
All the trademarks of products and companies mentioned in this datasheet belong to their respective owners.