Common Criteria
Information Technology
Security Evaluation

Project Cahokia7
Security Target

Memory Management Unit of
Samsung S3FT9KF/ S3FT9KT/ S3FT9KS
16-bit RISC Microcontroller
for Smart Card with
optional Secure RSA and ECC Library
including specific IC Dedicated Software

Version 1.5

ELECTRONICS

TABLE OF CONTENTS

LIST OF TABLES

TABLE OF FIGURES

1 ST INTRODUCTION

2 This introductory chapter contains the following sections:

1.1 Security Target and TOE Reference

1.2 TOE Overview and TOE Description

1.3 Interfaces of the TOE

1.4 TOE Intended Usage

1.1 Security Target and TOE Reference

3 The Security Target version is 1.5 and dated 20th March 2013.

4 The Security Target is based on

[5] Eurosmart Security IC Platform Protection Profile, Version 1.0, June 2007, BSI-PP-0035.

[22] Security Target of S3FT9KF/ S3FT9KT/ S3FT9KS 16-Bit RISC Microcontroller for Smart Cards, Version 2.0, June, 2012, Samsung Eletronics

5 The Protection Profile and the Security Target are built on *Common Criteria version 3.1*.

- Title: Security Target of Memory Management Unit of S3FT9KF/ S3FT9KT/ S3FT9KS 16-Bit RISC Microcontroller for Smart Cards
- Target of Evaluation: Memory Management Unit of S3FT9KF/ S3FT9KT/ S3FT9KS
- Provided by: Trusted Labs.
- Common Criteria version :

[1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 3, July 2009, CCMB-2009-07-001

[2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 3, July 2009, CCMB-2009-07-002

[3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009, CCMB-2009-07-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009, CCMB-2009-07-004

1.2 TOE Overview and TOE Description

1.2.1 Introduction to the product

6 The product, the S3FT9KF/ S3FT9KT/ S3FT9KS microcontroller featuring the TORNADO™2MX2 cryptographic coprocessor, is a smartcard integrated circuit which is composed of a processing unit, security components, contactless and contact based I/O ports, hardware circuit for testing purpose during the manufacturing process and volatile and non-volatile memories (hardware). The product also includes any IC Designer/Manufacturer proprietary IC Dedicated Software as long as it physically exists in the smartcard integrated circuit after being delivered by the IC Manufacturer. Such software (also known as IC firmware) is used for testing purpose during the manufacturing process but also provides additional services to facilitate the usage of the hardware and/or to provide additional services, including optional RSA/ECC public key cryptographic library, an [7]AIS20 compliant random number generation library and an [6]AIS31 compliant random number generator. The RSA/ECC library further includes the functionality of hash computation. The use for keyed hash operations like HMAC or similar security critical operations involving keys and other secrets requires specific security improvements and DPA analysis including the operating system. However, this functionality is intended to be used for signature generation and verification only.

7 Regarding the RSA and ECC library the user has the possibility to tailor this IC Dedicated Software part of the IC during the manufacturing process by deselecting the RSA and ECC library. Hence the product can be delivered with or without the functionality of the RSA and ECC library what's resulting in two configurations.

1.2.2 TOE Definition

8 The TOE is part of the product, namely its Memory Management Unit which is in charge of the area-based memory access control provided by the product that ensures that a Smartcard IC Embedded Software cannot accidentally or deliberately access to the outside of its reserved memory space. For example, a Smartcard OS can use this security feature to provide the application isolation for free (no software code is necessary). In case of an unauthorized access by some application, an un-maskable interrupt is raised and the access is denied. The embedded software is hence informed about the violation and may take appropriate actions.

9 The main hardware blocks of the S3FT9KF/ S3FT9KT/ S3FT9KS Integrated Circuit are described in **Figure 1** below:

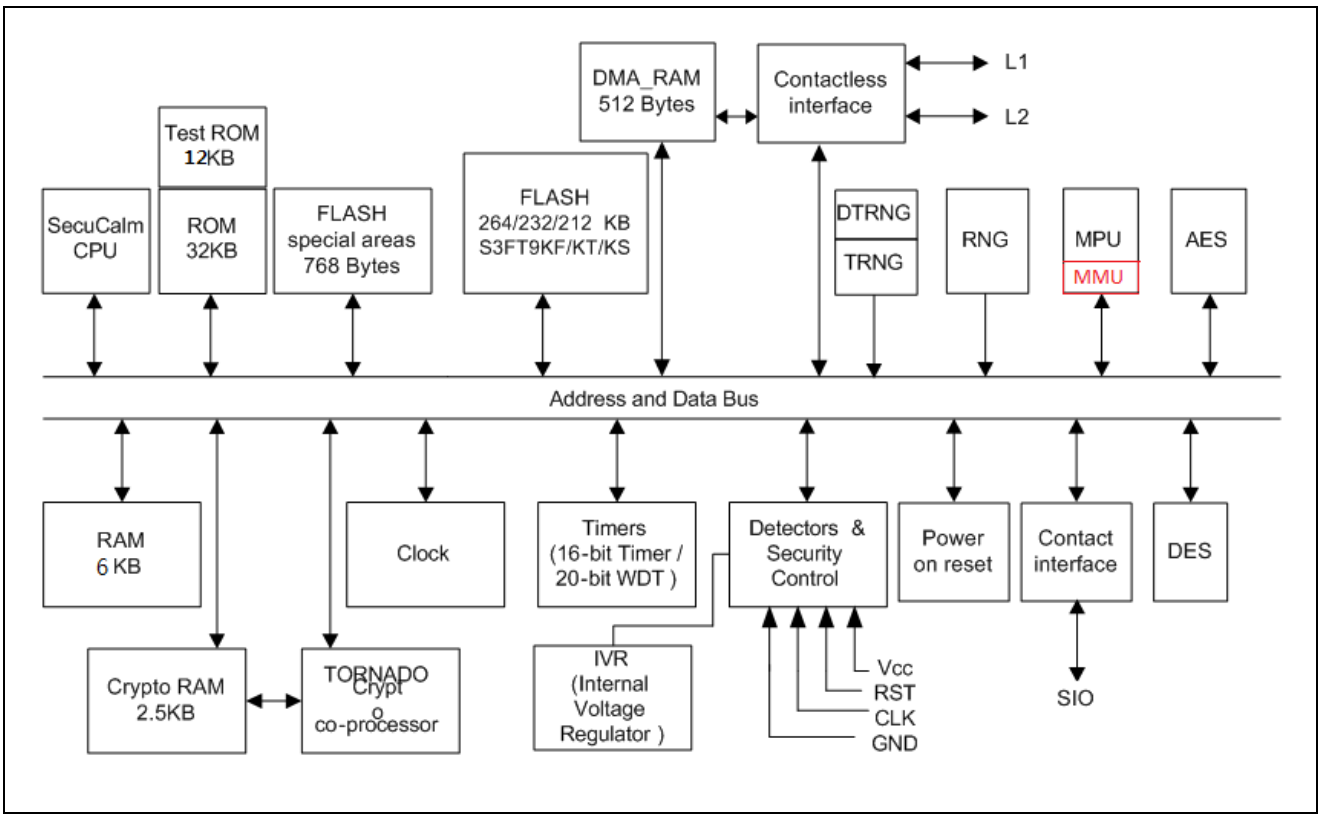

Figure 1 **TOE inside S3FT9KF/ S3FT9KT/ S3FT9KS IC**

10 *Note that only the Triple DES algorithm belongs to the IC, not the Single DES.

11 The TOE consists of the Memory Management Unit (MMU) that is configured and used in two CPU modes described in Table 2. The MMU enforces the access control to the IC memory areas. The TOE is part of the Memory Protection Unit (MPU) that also includes the other security features such as memory ciphering.

12 The product configuration is summarized in table 1 below:

Item Type	Item	Version	Form of delivery
Hardware	S3FT9KF/ S3FT9KT/ S3FT9KS 16-Bit RISC Microcontroller for Smart Card	1	Wafer or Module

Software	Test ROM Code	1.0	Included in S3FT9KF/ S3FT9KT/ S3FT9KS Test ROM
Software	Secure Boot loader code	0.0	Included in S3FT9KF/ S3FT9KT/ S3FT9KS in ROM
Software (optional)	Secure RSA/ ECC Library	3.0	Software Library. This library is delivered as object file and is optionally integrated into user NVM code.
Software	DRNG	1	Software Library. This library is delivered as object file and is optionally integrated into user NVM code.
Software	TRNG	1	Software Library. This library is delivered as object file and is optionally integrated into user NVM code.
Software	DTRNG	1	Software Library. This library is delivered as object file and is optionally integrated into user NVM code.
Document	Tornado-2Mx2 RSA/ECC Library API Manual	3.0	Softcopy
Document	DRNG Software Library Application Note	1.0	Softcopy
Document	TRNG and AIS31 online test library application note	1.1	Softcopy
Document	HW DTRNG and DTRNG library application note	1.0	Softcopy
Document	Hardware User's manual	1.20	Softcopy
Document	Security Application Note	1.4	Softcopy
Document	Chip Delivery Specification	1.1	Softcopy
Document	Boot Loader Specification	0.6	Softcopy
Document	Architecture Reference: SecuCalm CPU Core	14	Softcopy

Table 1 **Product Configuration**

13 Note: The product can be delivered without the RSA/ECC crypto library. In this case the product does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography and Elliptic Curve Cryptography (ECC) and Secure Hash Algorithm (SHA).

PRIVILEGE mode and USER mode

PRIVILEGE mode	USER mode
Protected mode for the operating system. All the control registers including security related special registers can be read or written only if CPU runs in this mode. Memory Management Unit can be configured in this Privilege Mode. When the CPU enters an interrupt service routine, it goes into Privilege Mode. Switching to User Mode will be done automatically when it returns from interrupt service routine. But the only way to switch from User Mode to Privilege Mode is via interrupts including SWI instructions. The 16-bit Status Register (SR) contains the "Interrupt Enable" (IE) bit, "FIQ Enable" (FE) bit, and the "Privilege Mode" (PM) bit. Those bits can be modified only when PM = 1 (i.e. the product is in privilege mode).	This mode cannot access all control registers. Interrupts including SWI is only way to switch from User Mode to Privilege Mode. When the program returns from an interrupt service routine, it goes back to User Mode again.

Table 2 **Privilege and User Modes basic description**

1.2.3 TOE Features

14 The MMU allow the CPU to access memories through channels. Each channel can allow the access to a contiguous range of address.

The following channels are provided:

- 3 NVM Program Memory channels: allow program fetch in NVM memories
- 1 RAM Program Memory channel
- 2 NVM Data Memory channels: allow data access in NVM memories
- 3 RAM Data Memory channels

  Fixed Data Memory channels for each special memory block: DMA_RAM, CRYPTO_RAM, SFLASH (FLASH products only), and PERI (list of peripheral registers).

15 In user mode, a memory access is decided upon the access address (with respect to pre-defined channels) and upon the access operation (with respect to the corresponding permissions). If the address and the operation match with one of the channels, then the access is allowed. Otherwise, the memory access is denied and the corresponding error is always reported to the IC Embedded Software (through an un-maskable interrupt).

1.2.4 TOE Life cycle

16 The TOE is a hardware component of the S3FT9KF/ S3FT9KT/ S3FT9KS product and shares the same life-cycle (see also [22]) when this product is combined with an IC embedded software in a (composite) smart card.

17 The complex development and manufacturing processes of a Composite Product can be separated into seven distinct phases. The phases 2 and 3 of the Composite Product life cycle cover the IC development and production:

- IC Development (Phase 2):
  - IC design,
  - IC Dedicated Software development,
- the IC Manufacturing (Phase 3):
  - integration and photomask fabrication,
  - IC production,
  - IC testing,
  - preparation and
  - Pre-personalisation if necessary

The Composite Product life cycle phase 4 can be included in the evaluation of the IC as an option:

- the IC Packaging (Phase 4):
  - Security IC packaging (and testing),
  - Pre-personalisation if necessary.

18 In addition, three important stages have to be considered in the Composite Product life cycle:

- Security IC Embedded Software Development (Phase 1),
- the Composite Product finishing process, preparation and shipping to the personalisation line for the Composite Product (Composite Product Integration Phase 5),
- the Composite Product personalisation and testing stage where the User Data is loaded into the Security IC's memory (Personalisation Phase 6),
- the Composite Product usage by its issuers and consumers (Operational Usage Phase 7) which may include loading and other management of applications in the field.

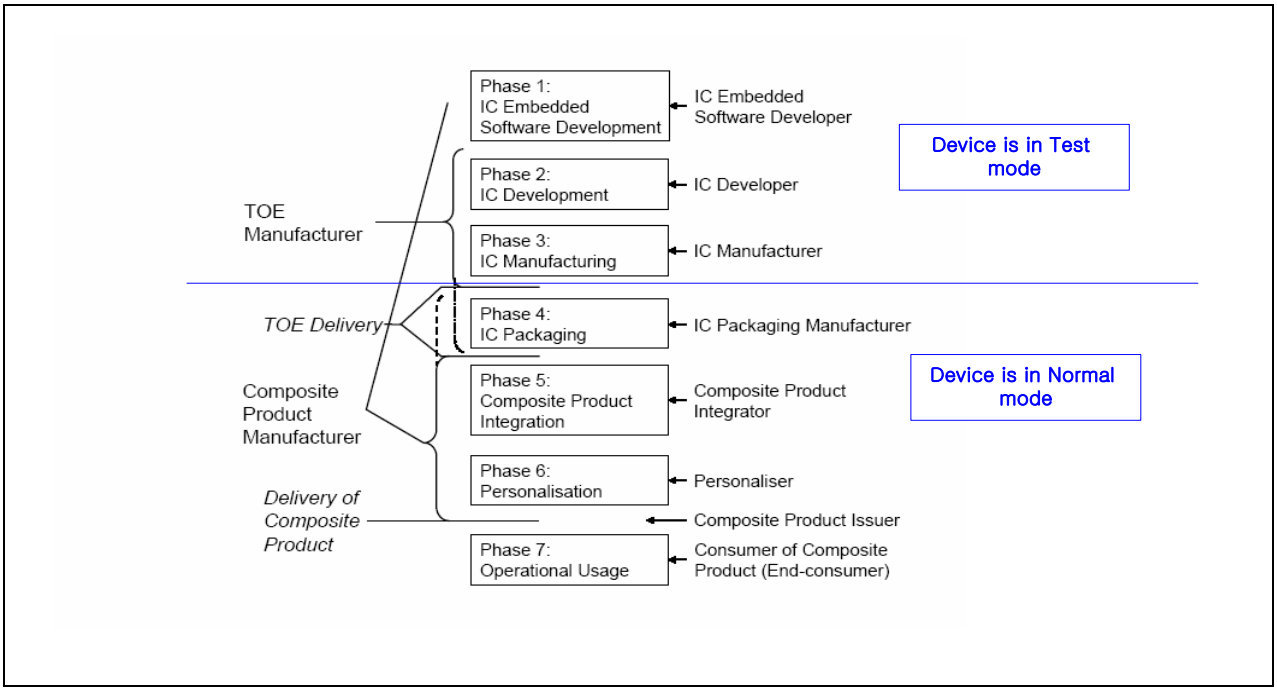

Figure 2 **Definition of "TOE Delivery" and responsible Parties**

19 The Security IC Embedded Software is developed outside the TOE development in Phase 1. The TOE is developed in Phase 2 and produced in Phase 3. Then the TOE is delivered in inside wafers. The TOE can also be delivered inside packaged products. In this case, the development and production of the TOE not only pertain to Phase 2 and 3 but to Phase 4 in addition.

1.3 Interfaces of the TOE

20 The TOE is an internal component of the S3FT9KF/ S3FT9KT/ S3FT9KS product and does not have direct interface with the external environment. However, the TOE has the indirect interfaces that are the interface of the product (see also [22]) i.e.

- The physical (indirect) interface of the TOE with the external environment is the entire surface of the IC
- The electrical (indirect) interface of the TOE with the external environment is made of the chip's pads including the Vdd, RESETB, XCLK, GND, IO1, IO2, L1 and L2 pads as well as the contactless radio-frequency interface
- The data (indirect) interface of the TOE is made of the Contact I/O pads and Contactless I/O pads.
- The software (indirect) interface of the TOE with the hardware consists of the input and output signals of the MMU. Those signals provide access to the Special Function Registers that are used to manage the memory. In particular,
  - The input Special Function Registers are described in Section 6.3 of the User's Manual [23].
  - The output is composed of 3 bits PA_FIQ, DA_FIQ and DAWR_FIQ bits of the FIQMONH register (see Section 7.2.2.3.1 of the User's Manual [23]).
- The DRNG (indirect) interface of the TOE is defined by the DRNG library interface.
- The TRNG (indirect) interface of the TOE is defined by the TRNG and DTRNG library interface.
- The RSA (indirect) interface of the TOE is defined by the RSA/ECC library interface (optional).
- The (indirect) interface to the ECC and SHA calculations is defined from the RSA/ECC library interface (optional)

1.4 TOE Intended Usage

21 The TOE is part the S3FT9KF/ S3FT9KT/ S3FT9KS product and has the same intended usage as this product i.e. it is dedicated to applications such as (see also [22]):

- Banking and finance applications for credit or debit cards, electronic purse (stored value cards) and electronic commerce.
- Network based transaction processing such a mobile phones (GSM SIM cards), pay TV (subscriber and pay-per-view cards), communication highways (Internet access and transaction processing).
- Transport and ticketing applications (access control cards).
- Governmental cards (ID cards, health cards, driving licenses).
- Multimedia applications and Digital Right Management protection.

2 CONFORMANCE CLAIMS

22 This chapter 2 contains the following sections:

2.1 CC Conformance Claim

2.2 PP Claim

2.3 Package Claim

2.4 Conformance Claim Rationale

2.1 CC Conformance Claim

23 This Security Target claims to be conformant to the Common Criteria version 3.1.

24 Furthermore, it claims to be conformant to the CC Part 2 [2] and CC Part 3 [3].

25 This *Security Target* has been built with the Common Criteria for Information Technology Security Evaluation; Version 3.1 which comprises

[1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 3, July 2009, CCMB-2009-07-001

[2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 3, July 2009, CCMB-2009-07-002

[3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009, CCMB-2009-07-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009, CCMB-2009-07-004

2.2 PP Claim

26 This Security Target is is a subset of the Security IC Platform Protection Profile [5]. The Security IC Platform Protection Profile is registered and certified by the Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035, Version 1.0, dated 15.06.2007.

2.3 Package Claim

27 The assurance level for this Security Target is EAL 7.

2.4 Conformance Claim Rationale

28 The Evaluation Assurance Level (EAL) of the PP [5] 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 7.

29 The security problem definition of this security target is with a subset of the statement of the security problem definition in the PP [5]. The security objectives of this security target are a subset of the security objectives in the PP [5]. The security requirements of this security target are a subset of the security requirements in the PP [5].

3 SECURITY PROBLEM DEFINITION

30 This chapter 3 contains the following sections:

3.1 Description of Assets

3.2 Threats

3.3 Organizational Security Policies

3.4 Assumptions

3.1 Description of Assets

Assets regarding the Threats

31 The assets (related to standard functionality) to be protected are

- the User Data,
- the Security IC Embedded Software,
- the security services provided by the TOE but also the complete product (i.e. IC) for the Security IC Embedded Software.

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

SC1 integrity of User Data and of the Security IC Embedded Software (while being executed/processed and while being stored in the TOE's memories),

SC2 confidentiality of User Data and of the Security IC Embedded Software (while being processed and while being stored in the IC's memories)

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

33 The Security IC may not distinguish between User Data which are public or confidential. Therefore the security IC shall protect the confidentiality and integrity of the User Data, unless the Security IC Embedded Software chooses to disclose or modify it.

34 In particular integrity of the Security IC Embedded Software means that it is correctly being executed which includes the correct operation of the TOE's and IC's functionality. Though the Security IC Embedded Software (normally stored in the ROM) will in many cases not contain secret data or algorithms, it must be protected from being disclosed, since for instance knowledge of specific implementation details may assist an attacker.

35 To be able to protect these assets the IC shall protect its security functionality. Therefore critical information about the IC shall be protected. Critical information includes:

- 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.

Such information and the ability to perform manipulations assist in threatening the above assets.

36 Note that there are many ways to manipulate or disclose the User Data: (i) An attacker may manipulate the Security IC Embedded Software or the IC. (ii) An attacker may cause malfunctions of the IC or abuse Test Features provided by the IC. Such attacks usually require design information of the IC to be obtained. They pertain to all information about (i) the circuitry of the IC (hardware including the physical memories), (ii) the IC Dedicated Software with the parts IC Dedicated Test

Software (if any) and IC Dedicated Support Software (if any), and (iii) the configuration data for the security functionality. The knowledge of this information enables or supports attacks on the assets. Therefore the TOE Manufacturer must ensure that the development and production of the IC is secure so that no information is unintentionally made available for the operational phase of the IC.

37 The TOE Manufacturer must apply protection to support the security of the IC. This not only pertains to the IC but also to all information and material exchanged with the developer of the Security IC Embedded Software. This covers the Security IC Embedded Software itself if provided by the developer of the Security IC Embedded Software or any authentication data required to enable the download of software. This includes the delivery (exchange) procedures for Phase 1 and the Phases after TOE Delivery as far as they can be controlled by the TOE Manufacturer. These aspects enforce the usage of the supporting documents and the refinements of SAR defined in the protection profile.

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

- logical design data,
- physical design data,
- IC Dedicated Software, Security IC Embedded Software, Initialisation Data and Pre-personalisation Data,
- 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.

3.2 Threats

39 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 data (which may comprise any data, including code, 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.

- Manipulation of the IC means that an attacker is able to deliberately deactivate or otherwise change the behaviour of a specific function in a manner which enables exploitation. This should be considered for the threat T.Malfunction, T.Phys-Manipulation and T.Abuse-Func.

- Disclosure of data (which may comprise any data, including code, stored in or processed by the Security IC) means that an attacker is realistically[1] 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.

40 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.

41 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 secret User Data stored in the IC, and (iii) develop and build a functional equivalent of the Security IC using the input from the previous steps.

[1] taking into account the assumed attack potential (and for instance the probability of errors)

42 The Security IC is a platform for the Security IC Embedded Software which ensures that especially the critical User Data are stored and processed in a secure way (refer to below). The Security IC Embedded Software must also ensure that critical User Data are treated as required in the application context. In addition, the personalisation process supported by the Security IC Embedded Software (and perhaps by the Security IC in addition) must be secure. This last step is beyond the scope of the Protection Profile. As a result the threat "cloning of the functional behaviour of the Security IC on its physical and command interface" is averted by the combination of measures which split into those being evaluated according to the Protection Profile (Security IC) 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.

43 The high-level security concerns are refined below by defining threats as required by the Common Criteria (refer to Figure 3). Note that manipulation of the IC is only a means to threaten User Data or the Security IC Embedded Software and is not a success for the attacker in itself.

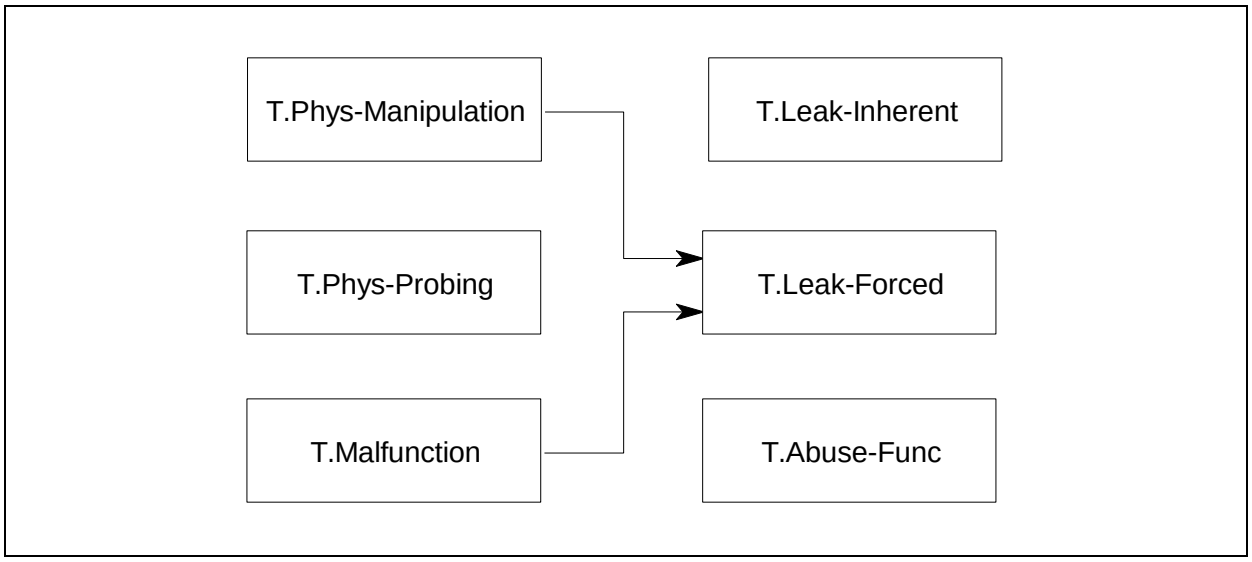

Figure 3 **Standard Threats**

44 The high-level security concern related to security service is refined below by defining threats as required by the Common Criteria (refer to Figure 4).

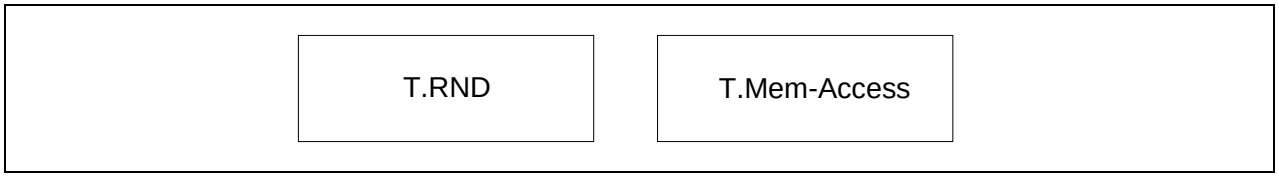

Figure 4 **Threats related to security service**

45 The Security IC Embedded Software must contribute to averting the threats: At least it must not undermine the security provided by the IC.

46 The above security concerns are derived from considering the end-usage phase (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.

47 The IC's countermeasures are designed to avert the threats described below. Nevertheless, they may be effective in earlier phases (Phases 4 to 6).

48 The IC is exposed to different types of influences or interactions with its outer world. Some of them may result from using the IC only but others may also indicate an attack. The different types of influences or interactions are visualised in Figure 5. Due to the intended usage of the IC all interactions are considered as possible.

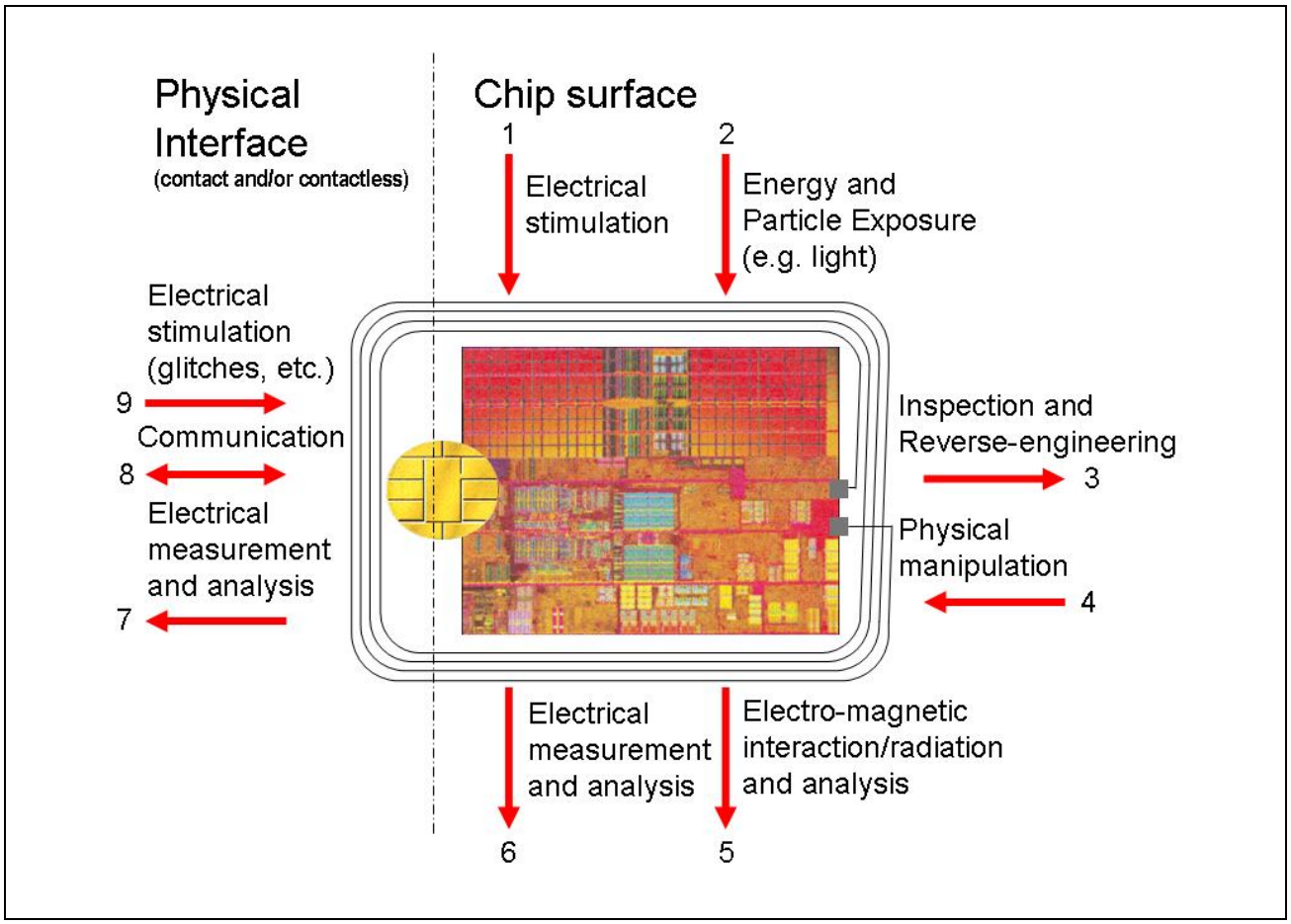

Figure 5 **Interactions between the IC and its outer world**

49 An interaction with the IC can be done through the physical interfaces (Number 7 – 9 in Figure 5) which are realised using contacts or a contactless interface. Influences or interactions with the IC also occur through the chip surface (Number 1 – 6 in Figure 5). In Number 1 and 6 galvanic contacts are used. In Number 2 and 5 the influence (arrow directed to the chip) or the measurement (arrow starts from the chip) does not require a contact. Number 3 and 4 refer to specific situations where the IC and its functional behaviour is not only influenced but definite changes are made by applying mechanical, chemical and other methods (such as 1, 2). Many attacks require a prior inspection and some reverse-engineering (Number 3). This demonstrates the basic building blocks of attacks. A practical attack will use a combination of these elements.

3.2.1 Standard Threats

50 The IC shall avert the threat "Inherent Information Leakage (T.Leak-Inherent)" as specified below.

T.Leak-Inherent	Inherent Information Leakage An attacker may exploit information which is leaked from the IC during usage in order to disclose confidential data as part of the assets.

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

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

T.Phys-Probing	Physical Probing An attacker may perform physical probing of the IC in order (i) to disclose User Data, (ii) to disclose/reconstruct the Security IC Embedded Software or (iii) to disclose other critical information about the operation of the IC to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software.

Physical probing requires direct interaction with the Security IC internals (Numbers 5 and 6 in Figure 5). Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that hardware security mechanisms and layout characteristics need to be identified (Number 3 in Figure 5). Determination of software design including treatment of User Data 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.

52 The IC shall avert the threat "Malfunction due to Environmental Stress (T.Malfunction)" as specified below.

T.Malfunction	Malfunction due to Environmental Stress An attacker may cause a malfunction of IC or of the Security IC Embedded Software by applying environmental stress in order to (i) modify security services of the IC or (ii) modify functions of the Security IC Embedded Software (iii) deactivate or affect security mechanisms of the IC to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software. This may be achieved by operating the Security IC outside the normal operating conditions (Numbers 1, 2 and 9 in Figure 5).

The modification of security services of the IC 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.

53 The IC shall avert the threat "Physical Manipulation (T.Phys-Manipulation)" as specified below.

T.Phys-Manipulation	Physical Manipulation An attacker may physically modify the IC in order to (i) modify User Data, (ii) modify the Security IC Embedded Software, (iii) modify or deactivate security services of the IC, or (iv) modify security mechanisms of the IC to

enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software.

The modification may be achieved through techniques commonly employed in IC failure analysis (Numbers 1, 2 and 4 in Figure 5) and IC reverse engineering efforts (Number 3 in Figure 5). 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 may also be a pre-requisite. Changes of circuitry or data can be permanent or temporary.

In contrast to malfunctions (refer to T.Malfunction) the attacker requires to gather significant knowledge about the IC's internal construction here (Number 3 in Figure 5).

54 The IC shall avert the threat "Forced Information Leakage (T.Leak-Forced)" as specified below:

T.Leak-Forced Forced Information Leakage

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

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

55 The IC shall avert the threat "Abuse of Functionality (T.Abuse-Func)" as specified below.

T.Abuse-Func Abuse of Functionality

An attacker may use functions of the IC which may not be used after TOE Delivery in order to (i) disclose or manipulate User Data, (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 or the Security IC Embedded Software.

3.2.2 Threats related to security services

56 The IC 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 IC for instance because of a lack of entropy of the random numbers provided.

An attacker may gather information about the produced random numbers which might be a problem because they may be used for instance to generate cryptographic keys.

Here the attacker is expected to take advantage of statistical properties of the random numbers generated by the IC without specific knowledge about the IC's generator. Malfunctions or premature ageing are also considered which may assist in getting information about random numbers.

3.2.3 Threats related to additional IC Specific Functionality

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

T.Mem-Access Memory Access Violation

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

Clarification: This threat does not address the proper definition and management of the security rules implemented by the Security IC Embedded Software, this being software design and correctness issue. This threat addresses the reliability of the abstract machine targeted by the software implementation. To avert the threat, the set of access rules provided by this IC should be undefeated if operated according to the provided guidance. The threat is not realized if the Security IC Embedded Software is designed or implemented to grant access to restricted information. It is realized if an implemented access denial is granted under unexpected conditions or if the execution machinery does not effectively control a controlled access.

Here the attacker is expected to (i) take advantage of flaws in the design and/or the implementation of the IC memory access rules (refer to T.Abuse-Func but for functions available after TOE delivery), (ii)introduce flaws by forcing operational conditions (refer to T.Malfunction) and/or by physical manipulation (refer to T.Phys-Manipulation). This attacker is expected to have a high level potential of attack.

3.3 Organizational Security Policies

58 The following Figure 6 shows the policies applied in this Security Target.

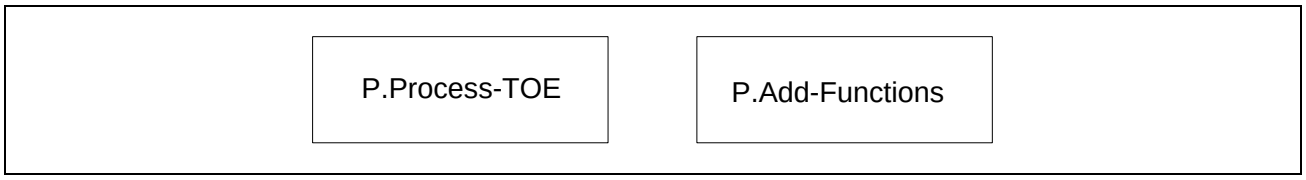

Figure 6 **Policies**

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

P.Process-TOE Protection 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.

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

61 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, Security IC Embedded Software, Initialisation Data and Pre-personalisation Data,
- 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.

62 The IC provides specific security functionality which can be used by the Smartcard Embedded Software. In the following specific security functionality is listed which is not derived from threats identified for the IC's environment because it can only be decided in the context of the smartcard application, against which threats the Smartcard Embedded Software will use the specific security functionality.

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

P.Add-Functions Additional Specific Security Functionality

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

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)
- Rivest-Shamir-Adleman (RSA) public key asymmetric cryptography (optional)
- Elliptic Curve Cryptography (ECC) and Secure Hash Algorithm (SHA) (optional)

64 Note: The IC can be delivered without the RSA/ECC crypto library. In this case the IC does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography and Elliptic Curve Cryptography (ECC) and Secure Hash Algorithm (SHA).

3.4 Assumptions

65 The following Figure 6 shows the assumptions applied in this Security Target.

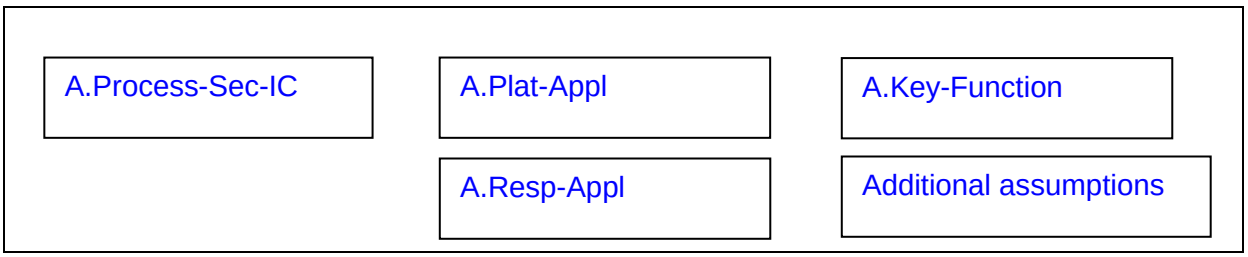

Figure 7 **Assumptions**

66 The intended usage of the IC 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.

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

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

A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation It is assumed that security procedures are used after delivery of the IC by the TOE Manufacturer up to delivery to the consumer to maintain confidentiality and integrity of the IC and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Phases after TOE Delivery are assumed to be protected appropriately.

69 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 and personalisation data including specifications of formats and memory areas, test related data,
- the User Data and related documentation, and
- material for software development support

as long as they are not under the control of the TOE Manufacturer. Details must be defined in the Protection Profile or Security Target for the evaluation of the Security IC Embedded Software and/or Security IC.

70 The developer of the Security IC Embedded Software must ensure the appropriate "Usage of Hardware Platform (A.Plat-Appl)" while developing this software in Phase 1 as specified below.

A.Plat-Appl	Usage of Hardware Platform The Security IC Embedded Software is designed so that the requirements from the following documents are met: (i) IC 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 IC evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.

71 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 can 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 IC evaluation must be completed before evaluation of the Security IC Embedded Software can be completed. The IC evaluation can be conducted before and independent from the evaluation of the Security IC Embedded Software.

72 The developer of the Security IC Embedded Software must ensure the appropriate "Treatment of User Data (A.Resp-Appl)" while developing this software in Phase 1 as specified below.

A.Resp-Appl Treatment of User Data

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

The application context specifies how the User Data shall be handled and protected. The evaluation of the Security IC according to this Security Target is conducted on generalized application context. The concrete requirements for the Security IC Embedded Software shall be defined in the Protection Profile respective Security Target for the Security IC Embedded Software. The Security IC can not prevent any compromise or modification of User Data by malicious Security IC Embedded Software. The assumption A.Resp-Appl ensures that the Security IC Embedded Software follows the security rules of the application context.

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

A.Key-Function Usage of Key-dependent Functions

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

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

3.4.1 Additional assumptions

74 In addition to the assumptions mentioned in the PP [5], this TOE also includes the following additional assumptions that are added because the corresponding security objectives are moved from the TOE to its operational environment.

A.Leak-Inherent Protection against Inherent Information Leakage

The IC must provide protection against disclosure of the confidential data (User Data or TSF data) stored and/or processed in it

- 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)

A.Phys-Probing Protection against Physical Probing

The IC must provide protection against disclosure of the User Data, against the disclosure/reconstruction of the Smartcard Embedded Software or against the disclosure of other critical operational information. 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.

A.Malfunction Protection against Malfunctions

The IC must ensure its correct operation.

The IC must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent errors. The environmental conditions may include voltage, clock frequency, temperature, or external energy fields.

A.Phys-Manipulation Protection against Physical Manipulation

The IC, the Smartcard Embedded Software and the User Data are protected against manipulation. This includes protection against

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

The IC 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.

A.Leak-Forced Protection against Forced Information Leakage

The IC must be protected against disclosure of confidential data processed in the IC (using methods as described under A.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 (A.Malfunction)" and/or
- by a physical manipulation (refer to "Protection against Physical Manipulation (A.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.

A.Abuse-Func Protection against Abuse of Functionality

The IC must prevent that its functions which may not be used after the TOE Delivery can be abused in order (i) to disclose critical User Data, (ii) to manipulate critical User Data of the Smartcard Embedded Software, (iii) to manipulate Soft-coded Smartcard Embedded Software or (iv) bypass,

deactivate, change or explore security features or functions. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

A.Identification IC Identification

The IC 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 Security IC identification.

A.RND Random Numbers

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

The IC 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.

A.Add-Functions Additional Specific Security Functionality

The IC must provide the following specific security functionality to the Smartcard Embedded Software:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)
- Rivest-Shamir-Adleman (RSA) public key asymmetric cryptography (optional)
- Elliptic Curve Cryptography (ECC) and Secure Hash Algorithm (SHA).(optional)

Note: The IC can be delivered without the RSA/ECC crypto library. In this case the Security IC does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography and Elliptic Curve Cryptography (ECC) and Secure Hash Algorithm (SHA).

4 SECURITY OBJECTIVES

75 This chapter Security Objectives contains the following sections:

4.1 Security Objectives for the TOE

4.2 Security Objectives for the IC components that are not part of the TOE

4.3 Security Objectives for the IC Embedded Software development Environment

4.4 Security Objectives for the operational Environment

4.5 Security Objectives Rationale

4.1 Security Objectives for the TOE

According to the Protection Profile[BSI-PP-0035] there are the following standard high-level security.

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

O.Mem-Access	Area based Memory Access Control The TOE must provide the Smartcard Embedded Software with the capability to define restricted access memory areas. The TOE must then enforce the partitioning of such memory areas so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

4.2 Security Objectives for the IC components that are not part of the TOE

77 The TOE being part of the IC, the other components provide the security objectives that are not ensured by the TOE. These components are TOE environment and these security objectives are security objectives of the TOE environment.

78 The TOE environment shall provide "Protection against Inherent Information Leakage (OE.Leak-Inherent)" as specified below.

OE.Leak-Inherent	Protection against Inherent Information Leakage The TOE environment must provide protection against disclosure of confidential data (User Data or TSF data) stored and/or processed in the Smartcard IC • by measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and • by measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or I/O lines). This objective pertains to measurements with subsequent complex signal processing whereas OE.Phys-Probing is about direct measurements on elements on the chip surface. Details correspond to an analysis of attack scenarios which is not given here.

79 The TOE environment shall provide "Protection against Physical Probing (OE.Phys-Probing)" as specified below.

OE.Phys-Probing	Protection against Physical Probing

The TOE environment must provide protection against disclosure of User Data, against the disclosure/reconstruction of the Smartcard Embedded Software or against the disclosure of other critical operational information. 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 environment 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.

80 The TOE environment shall provide "Protection against Malfunctions (OE.Malfunction)" as specified below.

OE.Malfunction Protection against Malfunctions

The TOE environment must ensure its correct operation.

The TOE environment must prevent the IC operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent errors. The environmental conditions may include voltage, clock frequency, temperature, or external energy fields.

Remark: A malfunction of the Security IC 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 OE.Phys-Manipulation) provided that detailed knowledge about the IC´s internal construction is required and the attack is performed in a controlled manner.

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

OE.Phys-Manipulation Protection against Physical Manipulation

The TOE environment must provide protection against manipulation of the Security IC (including its software and data), the Smartcard Embedded Software and the User Data. This includes protection against

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

The TOE environment 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.

82 The TOE environment shall provide "Protection against Forced Information Leakage (OE.Leak-Forced)" as specified below:

OE.Leak-Forced Protection against Forced Information Leakage

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

- by forcing a malfunction (refer to "Protection against Malfunction due to Environmental Stress (OE.Malfunction)" and/or
- by a physical manipulation (refer to "Protection againstPhysical Manipulation (OE.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.

83 The TOE environment shall provide "Protection against Abuse of Functionality (OE.Abuse-Func)" as specified below.

OE.Abuse-Func Protection against Abuse of Functionality

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

84 The TOE environment shall provide "TOE Identification (OE.Identification)" as specified below:

OE.Identification IC Identification

The TOE environment 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 Security IC identification.

85 The TOE environement shall provide "Random Numbers (OE.RND)" as specified below.

OE.RND Random Numbers

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

The TOE environment 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.

86 The TOE environment shall provide "Additional Specific Security Functionality (OE.Add-Functions)" as specified below.

OE.Add-Functions Additional Specific Security Functionality

The TOE environment must provide the following specific security functionality to the Smartcard Embedded Software:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)
- Rivest-Shamir-Adleman (RSA) public key asymmetric cryptography (optional)
- Elliptic Curve Cryptography (ECC) and Secure Hash Algorithm (SHA).(optional)

Note: The Security IC can be delivered without the RSA/ECC crypto library. In this case the TOE environment does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography and Elliptic Curve Cryptography (ECC) and Secure Hash Algorithm (SHA).

4.3 Security Objectives for the Security IC Embedded Software Development Environment

87 The development of the Security IC Embedded Software is outside the development and manufacturing of the IC. The Security IC Embedded Software defines the operational use of the IC. This section describes the security objectives for the operational environment enforced by the Security IC Embedded software.

Phase 1

88 The Security IC Embedded Software shall provide "Usage of Hardware Platform (OE.Plat-Appl)" as specified below.

OE.Plat-Appl Usage of Hardware Platform

To ensure that the IC 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 IC, (ii) data sheet of the IC Dedicated Software of the IC, (iii) IC application notes, other guidance documents, and (iv) findings of the IC evaluation reports relevant for the Security IC Embedded Software as referenced in the certification report.

89 The Security IC Embedded Software shall provide "Treatment of User Data (OE.Resp-Appl)" as specified below.

OE.Resp-Appl Treatment of User Data

Security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as required by the security needs of the specific application context.

For example the Smartcard Embedded Software will not disclose security relevant user data to unauthorised users or processes when communicating with a terminal.

4.3.1 Clarification of "Usage of Hardware Platform (OE.Plat-Appl)"

90 Regarding the area based access control this objective of the environment has to be clarified. For the separation of different applications the Smartcard Embedded Software (Operating System) may implement a memory management scheme based upon security mechanisms of the TOE.

91 For the separation of different applications the Smartcard Embedded Software may implement a memory management scheme based upon security mechanisms of the TOE as required by the security policy defined for the specific application context.

4.3.2 Clarification of "Treatment of User Data (OE.Resp-Appl)"

92 Regarding the area based access control this objective of the environment has to be clarified. The treatment of User Data is also required when a multi-application operating system is implemented as part of the Smartcard Embedded Software on the TOE. In this case the multi-application operating system should not disclose security relevant user data of one application to another application when it is processed or stored on the TOE.

93 The treatment of User Data is still required when a multi-application operating system is implemented as part of the Smartcard Embedded Software on the TOE. In this case the multi-application operating system should not disclose security relevant user data of one application to another application when it is processed or stored on the TOE.

4.4 Security Objectives for the Operational Environment

TOE Delivery up to the End of Phase 6

94 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 "consumer" to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that Phases after TOE Delivery up to the end of Phase 6 must be protected appropriately.

4.4.1 Clarification of "Protection during Composite Product Manufacturing (OE.Process-Sec-IC)"

95 The protection during packaging, finishing and personalization includes also the personalization process and the personalization data during Phase 4, Phase 5 and Phase 6.

96 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.

4.5 Security Objectives Rationale

97 Table 3 below gives an overview, how the assumptions, threats, and organisational security policies are addressed by the objectives. The text following after the table justifies this in detail.

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
A.Plat-Appl	OE.Plat-Appl	Phase 1
A.Resp-Appl	OE.Resp-Appl	Phase 1
P.Process-TOE	OE.Identification	Phase 2 – 3 optional Phase 4
A.Process-Sec-IC	OE.Process-Sec-IC	Phase 5 – 6 optional Phase 4
T.Leak-Inherent	OE.Leak-Inherent	
T.Phys-Probing	OE.Phys-Probing	
T.Malfunction	OE.Malfunction	
T.Phys-Manipulation	OE.Phys-Manipulation	
T.Leak-Forced	OE.Leak-Forced	
T.Abuse-Func	OE.Abuse-Func	
T.RND	OE.RND	
P.Add-Functions	OE.Add-Functions OE.Plat-Appl OE.Resp-Appl	
A.Key-Function	OE.Plat-Appl OE.Resp-Appl	
T.Mem-Access	O.Mem-Access OE.Plat-Appl OE.Resp-Appl	
A.Leak-Inherent	OE.Leak-Inderent	
A.Phys-Probing	OE.Phys-Probing	
A.Malfunction	OE.Malfunction	
A.Phys-Manipulation	OE.Phys-Manipulation	
A.Leak-Forced	OE.Leak-Forced	
A.Abuse-Func	OE.Abuse-Func	
A.Identification	OE.Identification	
A.RND	OE.RND	
A.Add-Fucntion	OE.Add-function	

Table 3 **Security Objectives versus Assumptions, Threats or Policies**

98 Since OE.Plat-Appl requires the Smartcard Embedded Software developer to implement those measures assumed in A.Plat-Appl, the assumption is covered by the objective.

99 Since OE.Resp-Appl requires the developer of the Smartcard Embedded Software to implement measures as assumed in A.Resp-Appl, the assumption is covered by the objective.

100 OE.Identification requires that the Security IC 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. For a list of material produced and processed by the TOE Manufacturer refer to paragraph 46 (page 19). 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.

101 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.

102 The justification related to the threats "Inherent Information Leakage (T.Leak-Inherent)", "Physical Probing (T.Phys-Probing)", "Malfunction due to Environmental Stress (T.Malfunction)", "Physical Manipulation (T.Phys-Manipulation)", "Forced Information Leakage (T.Leak-Forced)", "Abuse of Functionality (T.Abuse-Func)" and "Deficiency of Random Numbers (T.RND)" is as follows:

103 For all threats the corresponding objectives are stated in a way, which directly corresponds to the description of the threat. It is clear from the description of each objective, that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds.

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

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

106 The clarification of "Usage of Hardware Platform (OE.Plat-Appl)" makes clear that it is up to the Smartcard Embedded Software to implement the memory management scheme by appropriately administrating the TSF. This is also expressed both in T.Mem-Access and O.Mem-Access. The TOE shall provide access control functions as a means to be used by the Smartcard Embedded Software. This is further emphasised by the clarification of "Treatment of User Data (OE.Resp-Appl)" which reminds that the Smartcard Embedded Software must not undermine the restrictions it defines. Therefore, the clarifications contribute to the coverage of the threat T.Mem-Access.

107 The justification related to the security objective "Additional Specific Security Functionality (OE.Add-Functions)" is as follows:

108 Since OE.Add-Functions requires the Security IC to implement exactly the same specific security functionality as required by P.Add-Functions, the organisational security policy is covered by the objective.

109 Nevertheless the security objectives OE.Leak-Inherent, OE.Phys-Probing, OE.Malfunction, OE.Phys-Manipulation and OE.Leak-Forced define how to implement the specific security functionality required by P.Add-Functions. (Note that these objectives support that the specific security functionality is provided in a secure way as expected from P.Add-Functions.) Especially OE.Leak-Inherent and OE.Leak-Forced refer to the protection of confidential data (User Data or TSF data) in general. User Data are also processed by the specific security functionality required by P.Add-Functions.

110 Compared to Smartcard IC Platform Protection Profile a clarification has been made for the security objective "Usage of Hardware Platform (OE.Plat-Appl)": If required the Smartcard Embedded Software shall use these cryptographic services of the Security IC and their interface as specified. In addition, the Smartcard Embedded Software must implement functions which perform operations on keys (if any) in such a manner that they do not disclose information about confidential data. The non disclosure due to leakage A.Key-Function attacks is included in this objective OE.Plat-Appl. This addition ensures that the assumption A.Plat-Appl is still covered by the objective OE.Plat-Appl although additional functions are being supported according to OE.Add-Functions.

111 Compared to Smartcard IC Platform Protection Profile a clarification has been made for the security objective "Treatment of User Data (OE.Resp-Appl)": By definition cipher or plain text data and

cryptographic keys are User Data. So, the Smartcard Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realised in the environment. That is expressed by the assumption A.Key—Function which is covered from OE.Resp–Appl. These measures make sure that the assumption A.Resp-Appl is still covered by the security objective OE.Resp-Appl although additional functions are being supported according to P.Add-Functions.

112 The justification of the additional policy and the additional assumption show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there. In particular,

- A.Leak-Inherent assumption is upheld by OE.Leak-Inderent
- A.Phys-Probing assumption is upheld by OE.Phys-Probing
- A.Malfunction assumption is upheld by OE.Malfunction
- A.Phys-Manipulation assumption is upheld by OE.Phys-Manupulation
- A.Leak-Forced assumption is upheld by OE.Leak-Forced
- A.Abuse-Func assumption is upheld by OE.Abuse-Func
- A.Identification assumption is upheld by OE.Identification
- A.RNG assumption is upheld by OE.RND
- A.Add-Funtions assumption is upheld by OE.Add-Functions

5 IT SECURITY REQUIREMENTS

113 This chapter 5 IT Security Requirements contains the following sections:

5.1 Security Functional Requirements for the TOE

5.2 TOE Assurance Requirements

5.3 Security Requirements Rationale

5.1 Security Functional Requirements for the TOE

114 In order to define the Security Functional Requirements the 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 operations completed in the ST are marked in italic font.

Memory Access Control

115 Usage of multiple applications in one Smartcard often requires separating code and data in order to prevent that one application can access code and/or data of another application. To support this the TOE provides Area based Memory Access Control.

116 The security service being provided is described in the Security Function Policy (SFP) **Memory Access Control Policy**. The security functional requirement **"Subset access control (FDP_ACC.1)"** requires that this policy is in place and defines the scope were it applies. The security functional requirement **"Security attribute based access control (FDP_ACF.1)"** defines addresses security attribute usage and characteristics of policies. It describes the rules for the function that implements the Security Function Policy (SFP) as identified in FDP_ACC.1. The decision whether an access is permitted or not is taken based upon attributes allocated to the software. The user software defines the attributes and memory areas. The corresponding permission control information is evaluated "on-the-fly" by the hardware so that access is granted/effective or denied/inoperable.

117 The security functional requirement **"Static attribute initialization (FMT_MSA.3)"** ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. The attributes are determined during TOE manufacturing (FMT_MSA.3) or set at run-time (FMT_MSA.1).

118 From TOE´s point of view the different roles in the user software can be distinguished according to the memory based access control. However the definition of the roles belongs to the user software.

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

Memory Access Control Policy

The TOE shall control *read, write, delete, execute accesses of software running at between two different modes (privilege and user mode)* on *data including code stored in memory areas.*

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

FDP_ACC.1	Subset access control
Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the *Memory Access Control Policy* on *all subjects (software with privilege mode and user mode), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy*.

Refinement

The objects and subjects of the policy are:

Subject/Object	Description	Attributes
O.Data	A data memory areain RAM or Flash	Zone_id, Type, Base, Limit, Permission
O.Code	A code memory area in RAM or flash	Zone_id, Type, Base, Limit, Permission
O.Register	Set of Special Functional Registers	Register_id
S.ES	An embedded software	Address

Dependencies: FDP_ACF.1 Security attribute based access control

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

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the *Memory Access Control Policy* to objects based on the *memory area where the software is executed from and/or the memory area where* the *access is performed to and/or the operation to be performed.*

Refinement

The attributes of these objects and subjects are:

Attribute	Description	Value
Zone_id	memory area name	DMA_RAM, PKRAM, SEC_NVM, PERI, NVM_DM0, NVM_DM1, NVM_DM2, RAM_DM0, RAM_DM1, RAM_DM2, NVM_PM0, NVM_PM1, NVM_PM2, RAM_PM
Register_id	The address of a peripheral register	$NVM_PM_{\{0,1,2\}}$_BASEH_16, $NVM_PM_{\{0,1,2\}}$_BASEL_16, $NVM_PM_{\{0,1,2\}}$_LIMITH_16, $NVM_PM_{\{0,1,2\}}$_LIMITL_16, $NVM_DM_{\{0,1\}}$_BASEH_16, $NVM_DM_{\{0,1\}}$_BASEL_16, $NVM_DM_{\{0,1\}}$_LIMITH_16, $NVM_DM_{\{0,1\}}$_LIMITL_16, RAM_PM_BASE_16, RAM_PM_LIMIT_16, $RAM_DM_{\{0,1,2\}}$_BASE_16, $RAM\_DM_{\{0,1,2\}}$ LIMIT 16,

		PROTA_16, PROTB_16
Type	Memory type	"RAM", "NVM"
Base	Base address of a channel of a flash zone	24-bit values
Limit	Limit address of a channel of a flash zone	24-bit values
Permission	Access permission from User mode	No access or R for O.Code and O.Data "R/W" is only for O.Data
Address	Target address	24-bit values

The operations of the policy are:

- Read
- Update (i.e., Write or Delete)
- Execute

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

Refinement

The access rules are:

Rule_1: S.ES may freely perform Read on O.Register (if Address is Register_id of some register).

Rule_2: If its Mode is "User", then S.ES may perform Read on O.Code, O.Data if Address is between Base and Limit, and Permission is "R" or "R/W".

Rule_3: If its Mode is "User", then S.ES may perform Update on O.Data if

1. Address is between Base and Limit, and Permission is "R/W", and
2. there is no other area with Permission "R" such that Address is between its Base and Limit

Rule_4: If its Mode is "User", then S.ES may perform Execute on O.Code if Address is between Base and Limit, and Permission is "R".

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

FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Rule_5**: None of the six rules from **Rule_1** to **Rule_4** is applied.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

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

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

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

FMT_MSA.1	Management of security attributes
Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the *Memory Access Control Policy* to restrict the ability to *change default values of the* the security attributes *permission control information* to *no subject*. *Refinement* The default values are fixed by the TOE and assigned to the security attributes at RESET. These values are provided in Section 6.3.1 of the product User's Manual [23].
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

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

FMT_SMF.1	Specification of management functions
Hierarchical to:	No other components
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions*: access the control registers of the MPU*.
Dependencies:	No dependencies

5.2 TOE Assurance Requirements

125 The Security Target will be evaluated according to

Security Target evaluation (Class ASE)

126 The TOE Assurance Requirements for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 7 (EAL7)

127 All refinements from *Protection Profile BSI-PP-0035 version 1.0* for the assurance requirements (ALC_DEL, ALC_DVS, ALC_CMS, ALC_CMC, ADV_ARV, ADV_FSP, ADV_IMP, ATE_COV, AGD_OPE, AGD_PRE and ADV_VAN) have to be taken into consideration. *In particular the document [13] is used in the context of vulnerability analysis*

128

Class ADV: Development

Architectural design	(ADV_ARC.1)
Security Policy Model	(ADV_SPM.1)
Functional Specification	(ADV_FSP.6)
Implementation Representation	(ADV_IMP.2)
TSF Internals	(ADV_INT.3)
TOE Design	(ADV_TDS.6)

Class AGD: Guidance documents activities

Operational User Guidance	(AGD_OPE.1)
Preparative procedures	(AGD_PRE.1)

Class ALC: Life-cycle support

CM Capabilities	(ALC_CMC.5)
CM Scope	(ALC_CMS.5)
Delivery	(ALC_DEL.1)
Development Security	(ALC_DVS.2)
Life Cycle Definition	(ALC_LCD.2)
Tools and Techniques	(ALC_TAT.3)

Class ASE: Security Target evaluation

Conformance claims	(ASE_CCL.1)
Extended components definition	(ASE_ECD.1)
ST introduction	(ASE_INT.1)
Security objectives	(ASE_OBJ.2)
Derived security requirements	(ASE_REQ.2)
Security problem definition	(ASE_SPD.1)
TOE summary specification	(ASE_TSS.1)

Class ATE: Tests

Coverage	(ATE_COV.3)
Depth	(ATE_DPT.4)
Functional Tests	(ATE_FUN.2)
Independent Testing	(ATE_IND.3)

Class AVA: Vulnerability assessment
Vulnerability Analysis (AVA_VAN.5)

5.3 Security Requirements Rationale

5.3.1 Rationale for the Security Functional Requirements

129 Table 6 below gives an overview, how the security functional requirements are combined to meet the security objectives. The detailed justification follows after the table.

Objective	TOE Security Functional and Assurance Requirements
O.Mem-Access	- FDP_ACC.1 "Subset access control" - FDP_ACF.1 "Security attribute based access control" - FMT_MSA.3 "Static attribute initialisation" - FMT_MSA.1 "Management of security attributes" - FMT_SMF.1 "Specification of Management Functions"

Table 4 **Security Requirements versus Security Objectives**

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

131 The security functional requirement "Subset access control (FDP_ACC.1)" with the related Security Function Policy (SFP) "Memory Access Control Policy" exactly require the implementation of an area based memory access control, which is a requirement from O.Mem-Access. Therefore, FDP_ACC.1 with its SFP is suitable to meet the security objective.

132 The security functional requirement "Static attribute initialisation (FMT_MSA.3)" requires that the TOE provides default values for the security attributes. Since the TOE is a hardware platform these default values are generated by the reset procedure. Therefore FMT_MSA.3 is suitable to meet the security objective O.Mem-Access.

133 The security functional requirement "Management of security attributes (FMT_MSA.1)" requires that no subject can modify the default values of the security attributes.. It ensures that the access control required by O.Mem-Access can be realised using the functions provided by the TOE. Therefore FMT_MSA.1 is suitable to meet the security objective O.Mem_Access.

134 Finally, the security functional requirement "Specification of Management Functions (FMT_SMF.1)" is used for the specification of the management functions to be provided by the TOE as required by O.MEM_ACCESS. Therefore, FMT_SMF.1 is suitable to meet the security objective O.Mem_Access.

5.3.2 Dependencies of Security Functional Requirements

135 Table 7 below lists the security functional requirements defined in this Protection Profile, their dependencies and whether they are satisfied by other security requirements defined in this Protection Profile. The text following the table discusses the remaining cases.

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

Table 5 **Dependencies of the Security Functional Requirements**

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

5.3.3 Rationale for the Assurance Requirements

137 The assurance level EAL 7 was chosen to demonstrate that the TOE fulfills the most stringent Common Criteria requirements. In particular, the TOE design is formally described and its behavior is formally proved to correctly ensure its security objective i.e. the area-based memory access control. Furthermore, the TOE is protected against sophisticated software and physical attacks.

ADV_SPM.1 Formal TOE Security Policy Model

138 The formally modeled security policy consists of the area-based memory access control, in particular, in user-mode:

- The access control with respect to the memory areas is correctly enforced, in particular
  - A data is accessible if and only if its address is included in one of the Data Memory areas and this area has the access right (i.e. Read-only or Writing);
  - A data is writable if and only if
    - its address is included in one of the Data Memory areas and this area has the Writing right, and
    - its address is not included in any Data Memory area that has the Read-only right;
  - A code element is executable if and only if its address is included in one of the Program Memory areas and this area has the Execute right;
  - Any other access is a violation and is detected by the TSF;
- The consistency of the memory areas is correctly enforced i.e.
  - All memory areas and access rights are correctly initialized at the IC reset
  - Each fixed data area is completely contained in the physical memory space of its memory type:
    - DMA_RAM, CRYPTO_RAM must be included in RAM space
    - SFLASH and PERI must be included in NVM space

5.3.4 Security Requirements are Internally Consistent

139 The discussion of security functional requirements and assurance components in the preceding sections has shown that mutual support and consistency are given for both groups of requirements. The arguments provided for the adequacy of the assurance components for the functionality of the TOE also shows that the security functional requirements and assurance requirements support each other and that there are no inconsistencies between these groups.

140 Parts of the Smartcard IC Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). In order to avert the memory access violation it is important to the security functional requirement defining the scope where the Memory Access Policy is applied (FDP_ACC.1) and the security functional requirement defining the Memory Access Policy(FDP_ACF.1), and the security functional requirement ensuring the default value of security attribute(FMT_MSA.3) and the security functional requirement managing security attribute (FMT_MSA.1) and the security functional requirement performing security management function(FMT_SMF.1) are effective and bind well.

141 Five refinements from the PP [5] have to be discussed here in the ST as the assurance level is increased.

- The refinement for ALC_CMC from the PP [5] can still be applied at the assurance level EAL 7 augmented with ALC_CMC.5. The assurance component ALC_CMC.4 is augmented to ALC_CMC.5 with advanced features of the configuration management. The refinement is not touched.
- The refinement for ALC_CMS from the PP [5] can still be applied at the assurance level EAL 7 augmented with ALC_CMS.5. The assurance component ALC_CMS.4 is augmented to ALC_CMS.5 with aspects regarding the configuration control system for the TOE. The refinement is not impacted.
- The refinement for ADV_FSP from the PP [5] can still be applied at the assurance level EAL 7 augmented with ADV_FSP.6. The assurance component ADV_FSP.4 is extended to ADV_FSP.6 with aspects regarding the description level. The level is increased from informal to formal with informal description. The refinement is not impacted by this measure.
- The refinement for ADV_IMP from the PP [5] can still be applied at the assurance level EAL 7 augmented with ADV_IMP.2. The assurance component ADV_IMP.1 is extended to ADV_IMP.2 that requires the mapping from the TOE design to the entire implementation representation. The refinement is not impacted by this measure.
- The refinement for ATE_COV from the PP [5] can still be applied at the assurance level EAL 7 augmented with ATE_COV.3. The assurance component ATE_COV.2 is extended to ATE_COV.3 that requires a rigorous analysis of test coverage. The refinement is not impacted by this measure.

6 TOE SUMMARY SPECIFICATION

142 This chapter 6 TOE Summary Specification contains the following sections:

6.1 List of Security Functional Requirements

6.1 List of Security Functional Requirements

SFR4: FDP_ACC.1: Subset access control

143 This requirement is achieved by security register access control, invalid address access and access right for the code executed in FLASH.

144 **1) Invalid address access:** This function detects invalid address access occurrence. In case of an invalid address access is detected, an FIQ is evoked. The memory access rights are defined and configured through the control register MASCON and the Memory Management Unit (MMU). The MMU provide the Embedded Software the ability to define different access rights for different data and program memory areas. In case of an illegal memory access, a non-maskable interrupt (FIQ) is generated, allowing the embedded software to take dedicated and appropriate actions.

145 **2) Access rights for the code executed in FLASH:** This security function manages the code execution in FLASH, through access control security attributes in MPU. If an invalid access is detected, then a FIQ occurs.

SFR5: FDP_ACF.1: Security attributes based access control.

146 This is covered by the TOE and in particular the Memory Management Unit (MMU).

SFR6: FMT_MSA.3: Static attribute initialization.

147 All Special Function Registers including MMU have DEFAULT values after Power on Reset.

SFR7: FMT_MSA.1: Management of security attributes.

148 This is achieved with the MMU feature. The Memory Management Unit enables user to partition memory and set individual protection attributes for each partition. This allows the operating system to control the memory regions accessible by a User mode application process. The MMU enables user to divide memory into 8 regions, each with their own access permission attributes. If access against the set condition is performed, chip automatically generates FIQ, and sets a specific bit of FIQIMON register.

SFR8: FMT_SMF.1: Specification of management functions.

149 This is achieved via access to Special Function Registers of Memory Management Unit (MMU). MMU provides Special Function Registers which defines the base address and the limit address for a partition. The Registers exist for Flash, and RAM. Additional Registers exist for defining the protection attribute for each partition.

7 ANNEX

7.1 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.

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.

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

hat 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).

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.

Security IC

Composition of the product, the Security IC Embedded Software, User Data 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

TOE Delivery

The period when the TOE is delivered which is either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.

TOE Manufacturer

The TOE Manufacturer must ensure that all requirements for the TOE and its development and production environment are fulfilled. The TOE Manufacturer has the following roles: (i) IC Developer (Phase 2) and (ii) IC Manufacturer (Phase 3). If the TOE is delivered after Phase 4 in form of packaged products, he has the role of the (iii) IC Packaging Manufacturer (Phase 4) in addition.

TSF data

Data created by and for the TOE, that might affect the operation of the TOE. This includes information about the TOE's configuration, if any is coded in non-volatile non-programmable memories (ROM), in specific circuitry, in non-volatile programmable memories (for instance E2PROM) or a combination thereof.

User data

All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.

7.2 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

7.3 References

[1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 3, July 2009, CCMB-2009-07-001

[2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 3, July 2009, CCMB-2009-07-002

[3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009, CCMB-2009-07-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009, CCMB-2009-07-004

[5] Eurosmart Security IC Platform Protection Profile, Version 1.0, June 2007, BSI-PP-0035.

[6] AIS31: Functionality classes and evaluation methodology for true (physical) random number generators, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

[7] AIS20: Functionality classes and evaluation methodology for deterministic random number generators, Version 1, 2.12.1999, Bundesamt für Sicherheit in der Informationstechnik

[8] ALGO: Federal Gazette No 19, Notification in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance (overview of suitable algorithms), Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway, 2008-11-17

[10] [FIPS SP800-67] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, version 1.1

[11] [FIPS 197] Advanced Encryption Standard (AES), 2001-11-26

[12] [ISO/IEC 14888-2:2008] - Information technology -- Security techniques-- Digital signatures with appendix -- Part 2: Integer factorization based mechanisms.

[13] CC Supporting Document, Mandatory Technical Document, Application of Attack Potential to Smartcards, Version 2.5, Revision 1, April 2008, CCDB-2008-04-001

[14] [ANS X9.62] American National Standard X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), November 16, 2005.

[15] [ANS X9.63] American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, November 20, 2001

[16] [FIPS PUB 180-3] U.S. Department of Commerce / National Bureau of Standards, Secure Hash Algorithm, FIPS PUB 180-3, 2008-October

[17] [Brainpool curves] ECC Brainpool Standard Curves and Curve generation, M. Lochter, v1.0, www.ecc-brainpool.org

[18] [NIST curves] Federal Information Processing Standards Publication FIPS PUB 180-3, Digital Signature Standard; U.S. department of Commerce / National Institute of Standards and Technology (NIST), June 2009

[19] [SEC-recommended curves] SEC2: Recommended Elliptic Curve Domain Parameters, Certicom Research, v1.0, September 20, 2000.

[20] [ETSI TS 102 176-1] Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, 2007-11, version 2.0.0

[21] [SCA on Prime Gen] T. Finke, M. Gebhardt and W. Schindler, A New Side-Channel Attack on RSA Prime Generation, CHES 2009, LNCS 5747, pp. 141-155, 2009.

[22] Security Target of S3FT9KF/ S3FT9KT/ S3FT9KS 16-Bit RISC Microcontroller for Smart Cards, Version 2.0, June 2012, Samsung Electronics.

[23] Users Manual of S3FT9KF/ S3FT9KT/ S3FT9KS 16-Bit CMOS Microcontroller for Smart Cards, Revision 1.20, November 2011, Samsung Electronics.