MN67S140 Smartcard IC
Security Target
(ST–Lite)

- EAST JAPAN RAILWAY COMPANY

SuicaII contactless Smart Card IC chip -

Version: 1.2

Date: 2 February 2006

Matsushita Electric Industrial Co., Ltd.

Document History

Version	Date	Changes
1.0	06.12.2005	Public version
1.1	25.01.2006	Tailoring of the title (cover, Section 1.1, 2.1)
1.2	02.02.2006	Change of the explanation on TOE (Section 2.1)

Table of Contents

1 ST Introduction

1.1 ST Identification

Title	: MN67S140 Smartcard IC Security Target (ST-Lite) - EAST JAPAN RAILWAY COMPANY SuicaII contactless Smart Card IC chip -
Version	: Version 1.2
Date	: February 2, 2006
Produced by	: Matsushita Electric Industrial Co., Ltd.
Author	: Mitsuyoshi Ohya
CC version used	: ISO/IEC 15408:1999(E) (CC V2.1), part 1 to 3
TOE	: MN67S140 Smartcard IC
TOE version	: V1.0

This document is compiled from MN67S140 Smartcard IC Security Target as public version (hereafter ST-Lite). Proprietary information (e.g. about design) is removed in accordance with regulations of [JIL].

1.2 ST Overview

This document is focused on the Security Target (ST) for the smartcard integrated circuit (IC) called MN67S140, manufactured by Matsushita Electric Industrial Co., Ltd using 0.18um process. The Target of Evaluation (TOE) is composed of hardware including a processing unit, Cryptographic Hardware, security components, RF interface, and volatile and non-volatile memories. The TOE also includes IC Dedicated Software and documentation. The IC Dedicated Software is used for test purposes during production but also provide additional services to facilitate usage of hardware.

The IC can be delivered in form of sawn wafers (dice). After making into module by card manufacturer, it is embedded in a credit card-sized plastic package.

The MN67S140 is intended to be used for the applications requiring high security such as transportation and fare collection applications (the Commuter ticket), access control applications (ID cards), and government applications (the Basic Resident Register, health cards and driver license). These are only a few examples and its potentiality can be considered finite.
The security features implemented by the MN67S140 are:

- True random number generator;
- Security sensors (temperature, frequency, voltage, light);
- Physical countermeasures (such as sensing shield);
- Cryptography (Triple-DES), mutual authentication; and

- Countermeasures for DFA, DPA, and SPA attacks.

In addition, the security of the development and manufacturing environments have been designed to provide high assurance in the security of the MN67S140 product right through to its delivery to customers.

The main objectives of this ST are:

- To define the scope of the TOE;
- To describe the security enforcing functions of the TOE; and
- To show how the TOE meets the requirements.

1.3 CC Conformance

This Security Target is compliant with:
[CC] Common Criteria for Information Technology Security Evaluation; Version 2.1 (ISO 15408), which comprises

[CC-1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.1 (ISO 15408)
[CC-2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.1 (ISO 15408)
[CC-3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.1 (ISO 15408).

This Security Target claims conformance to the following Protection Profile.

- [SSVG] Smartcard IC Platform Protection Profile, BSI-PP-0002, Version 1.0, July 2001.

It is therefore Part2 extended and Part3 conformant according to Common Criteria.

The assurance level is EAL4 augmented with the following components:

- ADV_IMP.2,
- ALC_DVS.2,
- AVA_MSU.3, and
- AVA_VLA.4.

2 TOE Description

2.1 Product Description

The Target of Evaluation (TOE) is a *smartcard integrated circuit* which is composed of hardware such as a processing unit, Cryptographic Hardware, security components, RF Interface and volatile and non-volatile memories (Figure 1). The TOE also includes IC Designer/Manufacturer proprietary *IC Dedicated Software* (Figure 2 and Figure 3). Such software (also known as IC firmware) is used for test purposes during production but also provides additional services to facilitate usage of hardware. In addition to the IC Dedicated Software the Smartcard Integrated Circuit also includes hardware to perform testing. All other software is called Smartcard Embedded Software, which is not part of the TOE.

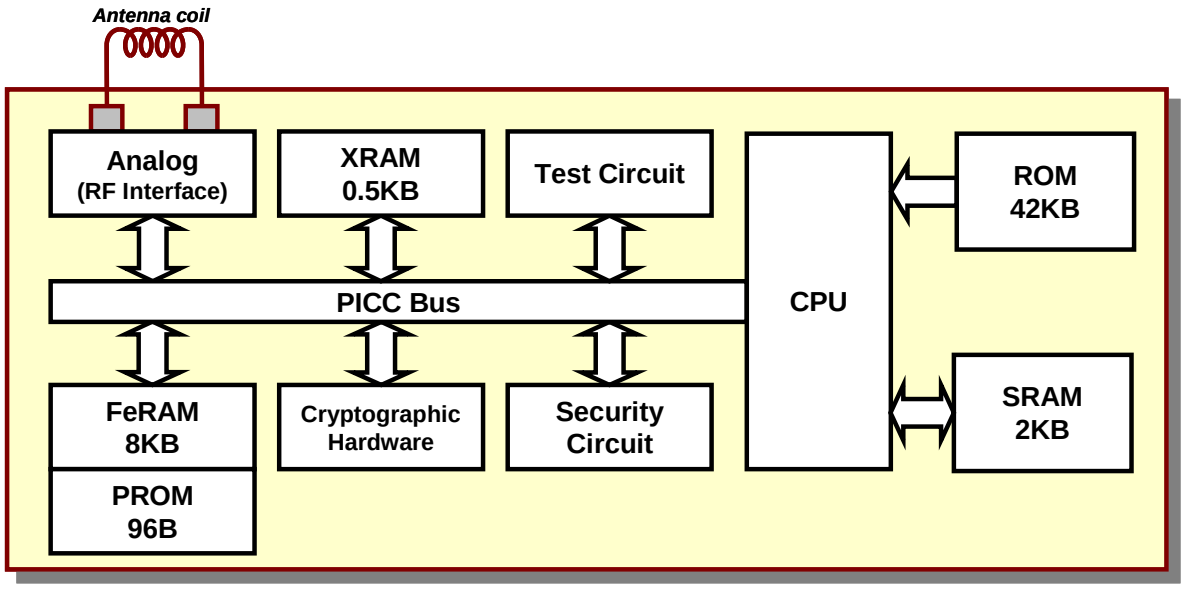

Figure 1: Block Diagram 1 of MN67S140 Smartcard IC - Hardware -

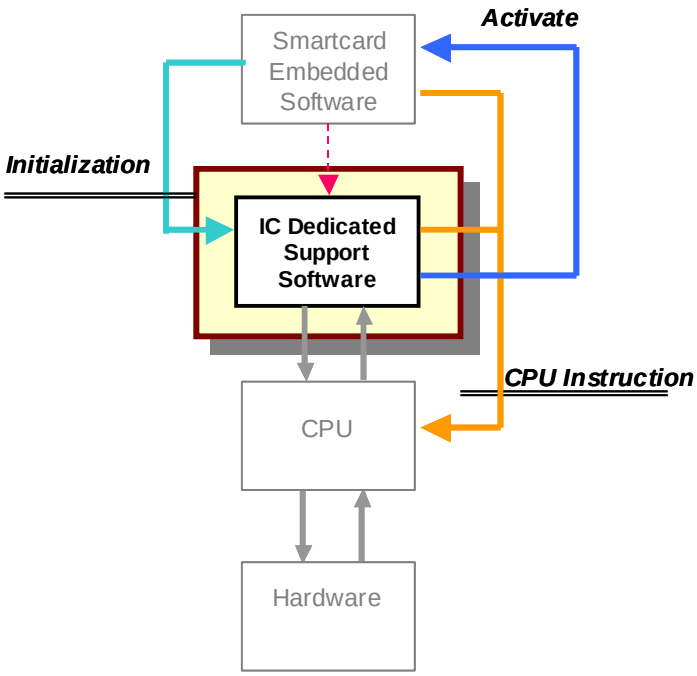

Figure 2: Block diagram 2 of MN67S140 Smartcard IC -IC Dedicated Software in Normal operation-

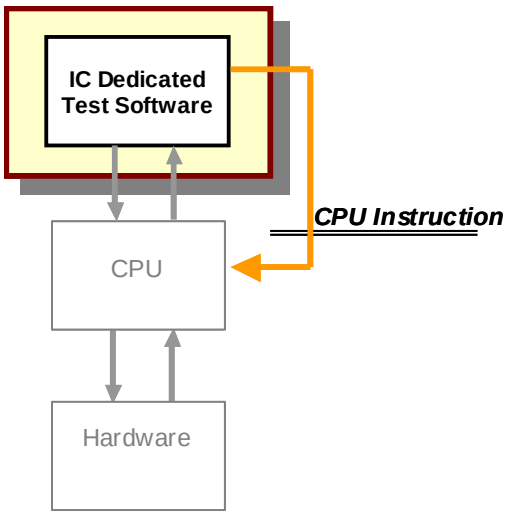

Figure 3: Block diagram 3 of MN67S140 Smartcard IC - IC Dedicated Software in testing

The TOE components are as follows.

Table 1: Components of the TOE

Item Type	Name	Version	Form of delivery
Hardware	MN67S140 Smartcard IC - Hardware	MN67S140, RV3	Sawn wafers (dice)
Software	MN67S140 Smartcard IC - IC Dedicated Software	FV12	ROM on the IC
Document	[Guide-SES]	1.0	Hardcopy
Document	[Guide-CM]	1.0	Hardcopy

The TOE is MN67S140, RV3, FV12 - EAST JAPAN RAILWAY COMPANY SuicaII contactless Smart Card IC chip -.

2.1.1 Hardware

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

(1) Analog

Analog is RF Interface in conformity to ISO/IEC 14443-2 TypeB and [JICSAP, 6], and realizes the following functions.

- Power reception using a rectifier
- Demodulation of ASK-modulated receive signals
- Transmission of modulated signals using a load switch
- Generation of stabilized power supply voltage VDD
- Generation of FeRAM supply voltage VPP
- Generation of reference clock signal from 13.56MHz carrier
- Generation of power-on reset signal

Besides, it contains various security logics such as RNG, random current generator, sensor/filter, and sensing shield.

Sensor/filter includes the followings.

- Voltage sensors (High & low)
- Voltage glitch sensor
- Low frequency sensor
- Light sensor
- Clock filters (High frequency & glitch)
- Reset filter
- Temperature sensors (High & low)

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

(2) Memory

The device has memories consisting of the following:

- ROM: 42Kbytes
- SRAM: 2Kbytes
- XRAM: 0.5Kbytes (a buffer for reception and transmission)
- FeRAM: 8Kbytes, PROM: 96Bytes

In ROM, IC Dedicated Software and Smartcard Embedded Software are stored. FeRAM can be accessed as both data memory and program memory. In PROM, data not allowed to be overwritten is stored.

(3) Cryptographic Hardware

The Cryptographic Hardware is capable of realizing the DES functionality in accordance with the single-DES and Triple-DES; however, the single-DES is outside the scope of evaluation.

(4) Security Circuit

Security Circuit contains access control circuit and various control circuits to control the Security logic (refer to 2.1.1(1)).

There are two modes for access control, and areas to which accesses are possible vary depending on each mode.

- User mode
- API mode

(5) CPU

CPU contains the Core AM13C, Interrupt function that processes interrupt.
The main features of AM13C CPU are:

- Simple and highly efficient instruction set
  (Number of basic instructions: 37; number of addressing modes: 9)
- Configuration that can increment variable instruction length by 4 bits based on minimum instruction length of 1 byte
- Minimum instruction execution time of 1 clock cycle
- Support for linear address space of up to 256KBytes

The interrupt function speeds up interrupt response with circuitry that automatically loads the branch address to the corresponding interrupt processing program from an interrupt vector table, and processes non-maskable interrupts (NMI) and level interrupts.

(6) Test Circuit

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

2.1.2 Firmware and Software

The TOE includes the following IC Dedicated Software stored in ROM.

Sorting of IC Dedicated Software	Purpose
IC Dedicated Support Software	To facilitate the use of hardware
IC Dedicated Test Software	To execute the functional tests after production

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

2.1.2.1 Interface of the TOE

(1) Electrical Interface

The electrical interface of the TOE to the external environment is the coil pads to which the RF antenna is connected.
Besides, the pads which are used at the test execution at Phase 3 are also electrical interface.

(2) Hardware Interface

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

(3) Firmware Interface

There are the following interfaces according to the modes.

- In the Test mode (during test at Phase 3)
  - In case that the functionality is tested directly from pad: None
  - In case that the test is conducted by using the Contact Test Software: test instruction set
- In the Normal mode
  - The set of functions for controlling hardware

(4) Software Interface

For Software Interface, there is the Smartcard Embedded Software main function call from IC Dedicated Support Software.

(5) Physical Interface

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

2.1.3 Documentation

The TOE includes the following documentation:

- [Guide-SES]: This documentation is provided for users who develop Smartcard Embedded Software.
- The guidance for secure use of IC is given in [Guide-CM].

2.2 TOE Life Cycle

As described in [SSVG, 2.1 & 8.1.1], the life cycle of TOE is separated into 7 phases.

Phase 1: Smartcard Embedded Software Develop
Phase 2: IC Development
Phase 3: IC Manufacturing and Testing
Phase 4: IC Packing and Testing
Phase 5: Smartcard Product Finishing Process
Phase 6: Smartcard Personalization
Phase 7: Smartcard End-usage

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

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

2.2.1 TOE Logical Phases

The default set after production is the Normal mode. IC can enter the test mode by the predefined procedures.
When the power is off, the IC returns to the Normal mode, which requires the predefined procedure to be repeated to complete as many tests as requested.
If all the requested tests are successfully done, the transition to the Test mode falls into disuse by the predefined control.

2.3 TOE Environments

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

- Design sites
- Mask manufacture site
- Manufacturing sites

2.3.1 TOE Development Environment

2.3.1.1 Design sites

Matsushita's design sites are managed with "Information Security Management Basic Rules" for the following assets.

Table 2: Assets at the design site

Assets	
Primary assets	The Smartcard Embedded Software
	Its correct operation
	The random numbers generated by the TOE
Secondary assets	Logical design data
	Physical design data
	IC Dedicated Software
	ROM Data
	TSF Data
	Specific development aids
	Test and characterization related data
	Material for software development support
	Related documentation

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

2.3.2 TOE Production Environment

2.3.2.1 Mask Manufacture site

Mask manufacturer subcontracted with Matsushita is forced to securely handle the following assets with NDA.

- MN67S140 mask processing data (EB data)
- Photomasks

2.3.2.2 Manufacturing sites

In Matsushita's manufacturing sites the following assets are managed securely with "Information Security Management Basic Rules"

- Reticles
- Masks and wafers (including sawn wafer),
- Test and characterization related data

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

2.3.3 Initialization and pre-personalization Data

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

2.4 TOE Intended Usage

The TOE is intended to be used for the applications requiring high security such as transportation and fare collection applications (the Commuter ticket), access control applications (ID cards), and government applications (the Basic Resident Register, health cards, driver license).

3 TOE Security Environment

The assets, assumptions, threats, and organizational security policies given in [SSVG] apply to the MN67S140. The description below is therefore adopted from [SSVG, 3].
In addition, the MN67S140 implements cryptographic functions for which relevant assumptions, threats and organizational security policies have been adopted from [PA].

3.1 Description of Assets

3.1.1 Assets regarding the Threats

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

- the User Data

Especially the User Data can be subject to manipulation and disclosure while being stored or processed by the TOE. However, also

- the Smartcard Embedded Software

needs to be protected to prevent manipulation and disclosure.

It is also essential that the TOE (including its Random Number Generator) guarantees

- its correct operation.

In particular this means that the Smartcard Embedded Software is correctly being executed which includes the correct operation of the TOE's functions.

Additional assets (secondary ones) are critical information about the TOE which include

- logical design data, physical design data, IC Dedicated Software, and TSF Data.

In addition,

- Initialization Data and Pre-personalization Data, specific development aids, test and characterization related data, material for software development support, and photomasks

will also contain information about the TOE. Such information and the ability to perform manipulations assist in threatening the above primary assets.

Note that there are many ways to manipulate or disclose the User Data. (i) An attacker may manipulate the Smartcard Embedded Software or the TOE. (ii) An attacker may cause malfunctions of the TOE or abuse Test Features provided by the TOE. Such attacks usually require design information of the TOE to be obtained. Therefore, the

design information is a secondary asset. 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 and IC Dedicated Support Software, and (iii) the TSF data.

Other primary assets (related to specific functionality) are

- the random numbers generated by the TOE[1].

3.1.2 Assets regarding the Organizational Security Policy P.Process-TOE

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, Smartcard Embedded Software, Initialization Data and Pre-personalization Data,
- Specific development aids,
- Test and characterization 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. Explanations can be found in [SSVG, 8.1.2].

3.1.3 Assets regarding the Assumption A.Process-Card

The information and material produced and/or processed by the Smartcard Embedded Software Developer in Phase 1 and by the Card Manufacturer can be grouped as follows:

- the Smart Card Embedded Software including specifications, implementation and related documentation,
- pre-personalization and personalization 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.

[1] Note that random numbers are to be protected in terms of confidentiality for instance against the threat of leakage because they might be used to generate cryptographic keys.

3.2 Assumptions

3.2.1 Assumptions from [SSVG]

The following descriptions and assumptions are taken from [SSVG, 3.2].

The intended usage of the TOE is twofold, depending on the Life Cycle Phase :(i) The Smartcard Embedded Software developer uses it as a platform for the smartcard software being developed. (ii) The Card Manufacturer (and the end-user) uses it as a part of the Smartcard. The Smartcard is used in a terminal which supplies the card (with power [2]) and (at least) mediates the communication with the Smartcard Embedded Software.

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

1) Appropriate “Protection during Packaging, Finishing and Personalization (A.Process-Card)” 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-Card Protection during Packaging, Finishing and Personalization

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

   This means that the Phases after TOE Delivery (refer to Sections 2.2 and [SSVG, 8.1]) are assumed to be protected appropriately.

2) The developer of the Smartcard 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 Smartcard Embedded Software is designed so that the requirements from the following documents are met:

[2] In case of contactless card the terminal does no supply the clock.

(i) *[Guide-SES]*, and

(ii) Findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.

Note that particular requirements for the Smartcard Embedded Software are often not clear before considering a specific attack scenario during vulnerability analysis of the smartcard integrated circuit (AVA_VLA). Therefore, such results from the TOE evaluation (as contained in the Evaluation Technical Report (ETR)) must be given to the developer of the Smartcard Embedded Software in an appropriate and authorized form and be taken into account during the evaluation of the software. This may also hold for additional tests being required for the combination of hardware and software. The TOE evaluation must be completed before evaluation of the Smartcard Embedded Software can be completed. The TOE evaluation can be conducted before and independent from the evaluation of the Smartcard Embedded Software.

3) The developer of the Smartcard 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 Smartcard Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as defined for the specific application context.

Details must be specified in the application context. Examples are given in [SSVG, 8.2.1], all being directly related to and covered by A.Resp-Appl.

3.2.2 Assumption from [PA]

The following assumption is taken from [PA, 2.2.2].

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

A.Key-Function Usage of Key-dependent Function

Key-dependent functions (if any) shall be implemented in the 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 TOE and (ii) the processing of User Data including cryptographic keys.

3.2.3 Additional Assumptions

The TOE-specific assumptions are as follows:

5) The developer of Smartcard Embedded Software must ensure the appropriate "Usage of triple-DES (A.DES)" while developing this software in Phase 1 as specified below.

A.DES Usage of triple-DES

It is assumed that the triple-DES algorithm shall be used as encryption algorithm though products support single-DES algorithm if it is necessary to keep high-level security, because the algorithm is to be attackable by high-level attacker.
When single-DES is used, it shall be justified that there is no security violations for purposes.

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

A.Interpreter Implementation of command interpreter

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

3.3 Threats

The cloning of the functional behavior of the Smartcard on its ISO command interface and [JICSAP] command interface[3] is the highest level security concern in the application context.

The cloning of that functional behavior requires to (i) develop a functional equivalent of the Smartcard Embedded Software, (ii) disclose, interpret and employ the secret User Data stored in the TOE, and (iii) develop and build a functional equivalent of the smartcard using the input from the previous steps.

The smartcard integrated circuit is a platform for the Smartcard Embedded Software which ensures that especially the critical User Data are stored and processed in a secure way (refer to below). The Smartcard Embedded Software must also ensure that critical User Data are treated as required in the application context (refer to Section 3.2). In addition, the personalization process supported by the Smartcard Embedded Software (and perhaps by the smartcard integrated circuit in addition) must be secure (refer to Section 3.2). This last step is beyond the scope of this Security Target. As a result the threat "cloning of the functional behavior of the smartcard on its ISO and [JICSAP] command interface[4]" is averted by the combination of measures which split into those being evaluated according to this Security Target and those being subject to the evaluation of the Smartcard Embedded Software or Smartcard and the corresponding personalization process. Therefore, functional cloning is indirectly covered by the security concerns and threats described below.

As in [SSVG, 3.3] there are the following standard high-level security concerns:

SC1 manipulation of User Data and of the Smartcard Embedded Software (while being executed/processed and while being stored in the TOE's memories) and

SC2 disclosure of User Data and of the Smartcard Embedded Software (while being processed and while being stored in the TOE's memories).

Though the Smartcard 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. In many cases critical User Data will be stored in the FeRAM[5].

[3] MN67S140 has ISO command interface and [JICSAP] command interface.

[4] MN67S140 has ISO command interface and [JICSAP] command interface.

[5] For MN67S140, data is stored in FeRAM.

These high-level security concerns are refined below by defining threats as required by the Common Criteria. Note that manipulation of the TOE is only a means to threaten User Data or the Smartcard Embedded Software and is not a success for the attacker in itself.

According to this Security Target there are the following high-level security concerns related to specific functionality:

SC3 deficiency of random numbers.

These high-level security concerns being related to specific functionality are refined below by defining threats as required by the Common Criteria.

The Smartcard Embedded Software must contribute to averting the threats: At least it must not undermine the security provided by the TOE. For detail refer to the assumptions regarding the Smartcard Embedded Software specified in Section 3.2.

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 organizational security policy.

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

The TOE is exposed to different types of influences or interactions with its outer world. Some of them may result from using the TOE only but others may also indicate an attack. The different types of influences or interactions are visualized in Figure 4.

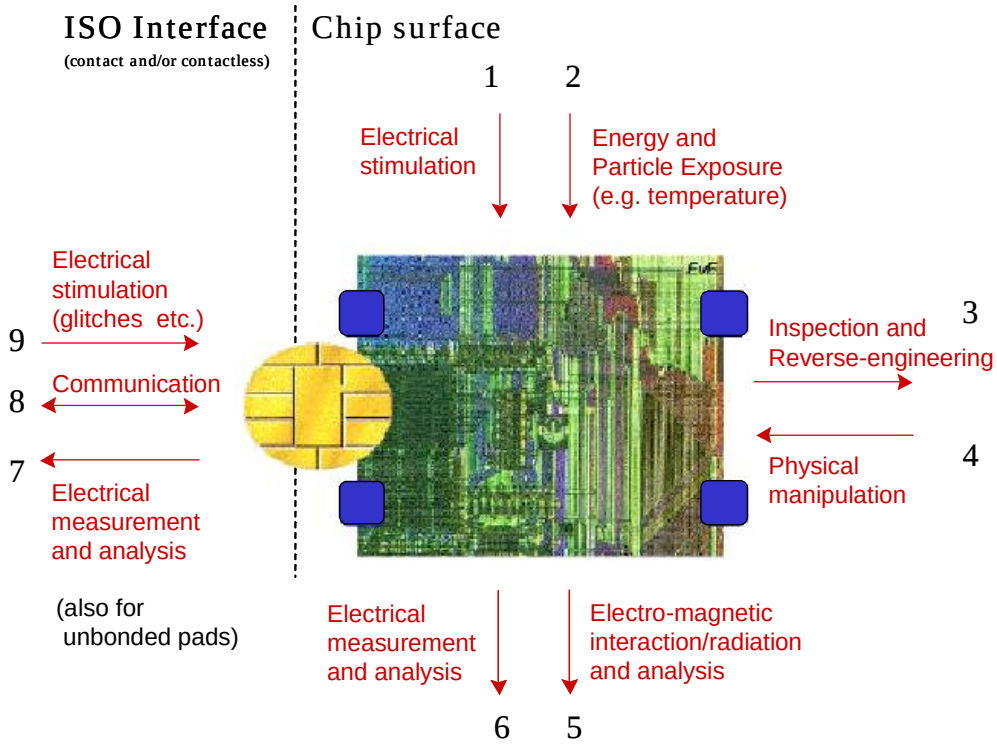

Figure 4: Attack Model for the TOE

An interaction with the TOE can be done through the ISO interfaces (Number 7 – 9 in Figure 4) which are realized using a contactless interface[6]. Influences or interactions with the TOE also occur through the chip surface (Number 1 – 6 in Figure 4). 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 TOE and its functional behavior 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).

Examples for specific attacks are given in [SSVG, 8.3].

3.3.1 Standard Threats (referring to SC1 and SC2)

1) The TOE shall avert the threat “Inherent Information Leakage (T.Leak-Inherent)” as specified below.

T.Leak-Inherent Inherent Information Leakage

[6] The MN67S140 has only a contactless interface.

An attacker may exploit information which is leaked from the TOE during usage of the Smartcard in order to disclose confidential data (User Data or TSF data).

No direct contact with the Smartcard 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 4) or measurement of emanations (Number 5 in Figure 4) and can then be related to the specific operation being performed.

In accordance with [PA, 2.2.3], this threat pertains to the disclosure of cryptographic keys while being used to perform cryptographic algorithms (or operations used to build them).

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

T.Phys-Probing Physical Probing

An attacker may perform physical probing of the TOE in order (i) to disclose User Data, (ii) to disclose/reconstruct the Smartcard Embedded Software or (iii) to disclose other critical operational information especially TSF data.

Physical probing requires direct interaction with the Smartcard Integrated Circuit internals (Numbers 5 and 6 in Figure 4). 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 4). 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.

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

T.Malfunction Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of the Smartcard Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) deactivate or modify security -functions of the Smartcard Embedded Software. This may be achieved by operating the Smartcard outside the normal operating conditions (Numbers 1, 2 and 9 in Figure 4).

To exploit an attacker needs information about the functional operation.

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

T.Phys-Manipulation Physical Manipulation

An attacker may physically modify the Smartcard in order to (i) modify security features or functions of the TOE, (ii) modify security functions of the Smartcard Embedded Software or (iii) to modify User Data.

The modification may be achieved through techniques commonly employed in IC failure analysis (Numbers 1, 2 and 4 in Figure 4) and IC reverse engineering efforts (Number 3 in Figure 4). The modification may result in the deactivation of a security function. 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 gathering significant knowledge about the TOE’s internal construction here (Number 3 in Figure 4).

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

T.Leak-Forced Forced Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Smartcard in order to disclose confidential data (User Data or TSF data) 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 4) which normally do not contain significant information about secrets.

In accordance with [PA, 2.2.3], this threat pertains to the disclosure of cryptographic keys while being used to perform cryptographic algorithms (or operations used to build them).

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

T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which may not be used after TOE Delivery in order to (i) disclose or manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or of the Smartcard Embedded Software or (iii) to enable an attack.

3.3.2 Threats related to Specific Functionality (referring to SC3)

7) The TOE shall avert the threat "Deficiency of Random Numbers (T.RND)" as specified below.

T.RND Deficiency of Random Numbers

An attacker may predict or obtain information about random numbers generated by the TOE 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 TOE without specific knowledge about the TOE's generator. Malfunctions or premature ageing are also considered which may assist in getting information about random numbers.

3.4 Organizational Security Policies

3.4.1 Organizational Security Policies from [SSVG]

The following organizational Security Policy is taken from [SSVG, 3.4].

1) 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

The TOE Manufacturer must ensure that the development and production of the Smartcard Integrated Circuit (Phase 2 up to TOE Delivery, refer to Section 2.2) is secure so that no information is unintentionally made available for the operational phase of the TOE. For example, the confidentiality and integrity of design information and test data shall be guaranteed; access to samples, development tools and other material shall be restricted to authorized persons only; scrap will be destroyed etc. This not only pertains to the TOE but also to all information and material exchanged with the developer of the Smartcard Embedded Software and therefore especially to the Smartcard Embedded Software itself. 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.

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

For a list of assets refer to section 3.1.

3.4.2 Organizational Security Policies from [PA]

The following organizational Security Policy is taken from [PA, 2.2.4].

The following specific security functionality is listed which is not derived from threats identified for the TOE’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.

2) The IC Developer/Manufacturer must apply the policy “Additional Specific Security

Functionality (P.Add-Functions)" as specified below.

P.Add-Functions Additional Specific Security Functionality

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

- Ø Triple Data Encryption Standard (3DES)
- Ø Mutual Authentication Function (in conformity with [JICSAP])

4 Security Objectives

The security objectives described below are drawn from [SSVG, 4] and [PA, 2.3].

4.1 Security Objectives for the TOE

4.1.1 Security Objectives for the TOE from [SSVG]

The following Security Objectives for the TOE are taken from [SSVG, 4.1].

There are the following standard high-level security goals:

SG1 maintain the integrity of User Data and of the Smartcard Embedded Software (when being executed/processed and when being stored in the TOE's memories) as well as

SG2 maintain the confidentiality of User Data and of the Smartcard Embedded Software (when being processed and when being stored in the TOE's memories).

Though the Smartcard 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. In many cases critical User Data will be stored in the FeRAM[7].

These standard high-level security goals are refined below by defining security objectives as required by the Common Criteria. Note that the integrity of the TOE is a means to reach these objectives.

There are the following high-level security goals related to specific functionality:

SG3 provide random numbers.

Standard Security Objectives (referring to SG1 and SG2)

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

O.Leak-Inherent Protection against Inherent Information Leakage

The TOE must provide protection against disclosure of

[7] For MN67S140, data is stored in FeRAM.

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 O.Phys-Probing is about direct measurements on elements on the chip surface. Details correspond to an analysis of attack scenarios which is not given here.

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

O.Phys-Probing Protection against Physical Probing

The TOE must provide protection against disclosure 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 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.

3) The TOE shall provide “Protection against Malfunctions (O.Malfunction)” as specified below.

O.Malfunction Protection against Malfunctions

The TOE must ensure its correct operation.

The TOE must 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.

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

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

O.Phys-Manipulation Protection against Physical Manipulation

The TOE must provide protection against manipulation of the TOE (including its software and TSF data), the 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 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.

5) The TOE shall provide “Protection against Forced Information Leakage

(O.Leak-Forced)“ as specified below:

O.Leak-Forced Protection against Forced Information Leakage

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

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

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

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

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

O.Abuse-Func Protection against Abuse of Functionality

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order (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 TOE.

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

O.Identification TOE Identification

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

4.1.2 Security Objectives related to Specific Functionality (referring to SG3)

8) The TOE shall provide “Random Numbers (O.RND)” as specified below.

O.RND Random Numbers

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

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

4.1.3 Security Objectives for the TOE from [PA]

The following Security Objective for the TOE is taken from [PA, 2.3.1].

9) The TOE shall provide “Additional Specific Security Functionality (O.Add-Functions)” as specified below.

O.Add-Functions Additional Specific Security Functionality

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

- Triple Data Encryption Standard (3DES)
- Mutual Authentication Function (in conformity with [JICSAP])

4.2 Security Objectives for Environment

In this section Security Objectives for Environment are taken from [SSVG, 4.2]. But to explicitly cover cryptographic algorithms the clarification taken from [PA, 2.3.2] are made for OE.Plat-Appl and OE.Resp-Appl.
Furthermore, OE.DES and OE.Interpreter are added as TOE-specific objectives.

4.2.1 Phase 1

1) The Smartcard Embedded Software shall provide “Usage of Hardware Platform (OE.Plat-Appl)” as specified below.

OE.Plat-Appl Usage of Hardware Platform

The Smartcard Embedded Software shall be designed so that the requirements from the following documents are met:

(i) *[Guide-SES]*, and

(ii) Findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.

Because the TOE supports cipher schemes as additional specific security functionality (O.Add-Functions), these security objectives for environment (OE.Plat-Appl) are clarified as follow.

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

2) The Smartcard 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 unauthorized users or

processes when communicating with a terminal.

Because the TOE supports cipher schemes as additional specific security functionality (O.Add-Functions), these security objectives for environment (OE.Resp-Appl) are clarified as follow.

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

This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realized in the environment.

3) The Smartcard Embedded Software shall provide “Usage of triple-DES (OE.DES)” as specified below.

OE.DES Usage of triple-DES

The triple-DES algorithm shall be used as encryption algorithm though products support single-DES algorithm if it is necessary to keep high-level security, because the algorithm is to be attackable by high-level attacker.
When single-DES is used, it shall be justified that there is no security violations for purposes.

5) The Smartcard Embedded Software shall provide “Implementation of command interpreter (OE.Interpreter)” as specified in below.

OE.Interpreter Implementation of command interpreter

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

4.2.2 Phase 2 up to TOE Delivery

4) The TOE Manufacturer shall ensure the “Protection during TOE Development and Production (OE.Process-TOE)” as specified below.

OE.Process-TOE Protection during TOE Development and Production

The TOE Manufacturer must ensure that the development and production of the Smartcard Integrated Circuit (Phases 2 and 3 up to TOE Delivery, refer to Section 2.2) is secure so that no information is unintentionally made available for the operational phase of the TOE. For example, the confidentiality and integrity of design information and test data must be guaranteed, access to samples, development tools and other material must be restricted to authorized persons only, scrap must be destroyed. This not only pertains to the TOE but also to all information and material exchanged with the developer of the Smartcard Embedded Software and therefore especially to the Smartcard Embedded Software itself. 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.

An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification. In order to make this practical, electronic identification shall be possible.

For a list of assets refer to section 3.1.

4.2.3 TOE Delivery up to the end of Phase 6

5) Appropriate “Protection during Packaging, Finishing and Personalization (OE.Process-Card)” 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-Card Protection during Packaging, Finishing and Personalization

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

This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 2.2) must be protected appropriately.

For a preliminary list of assets to be protected refer to section 3.1.

5 IT Security Requirements

5.1 TOE Security Requirements

5.1.1 TOE Functional Requirements

In order to define the Security Functional Requirements Part 2 of the Common Criteria was used. However, some additional Security Functional Requirements are defined in [SSVG]. Therefore, this Security Target is characterized as “Part 2 extended”.

The Security Functional Requirements are shown in Table 3. The additional Security Functional Requirements adopted from [PA] are shown in bold type. These security functional components are listed and explained below.

Table 3: Security Functional Requirements

Security functional requirement	
FRU_FLT.2	Limited fault tolerance
FPT_FLS.1	Failure with preservation of secure state
FPT_SEP.1	Domain separation
FDP_ITT.1	Basic internal transfer protection
FPT_ITT.1	Basic internal TSF data transfer protection
FDP_IFC.1	Subset information flow control
FPT_PHP.3	Resistance to physical attack
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FAU_SAS.1	Audit storage
FCS_RND.1	Quality metric for random numbers
FCS_COP.1A	**Cryptographic operation**
FCS_COP.1B	**Cryptographic operation**

5.1.1.1 TOE Functional Requirements from [SSVG]

The following TOE Functional Requirements are taken from [SSVG, 5.1.1].

(1) Malfunctions

There are different ranges of operating conditions such as supply voltage, external frequency and temperature. The TOE can be operated within the limits visualized as the inner dashed rounded rectangle in Figure 5 and must operate correctly there. The limits have been reduced to ensure correct operation. This is visualized by the outer dotted rounded rectangle in the figure.

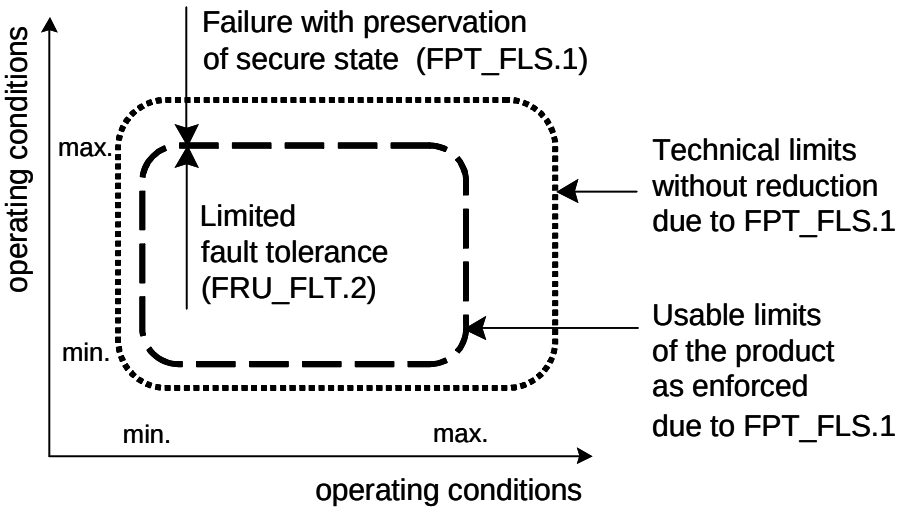

Figure 5: Paradigm regarding Operating Conditions

Figure 5 must not be understood as being two-dimensional and defining static limits only. Reality is multi-dimensional and includes a variety of timing aspects. Note that the limit of the operating conditions visualized by the inner dashed rounded rectangle in Figure 5 is not necessarily exactly reflected by the limits identified in the TOE's data sheet. Instead this limit marks the boundary between the "tolerance reaction" of the TOE and the "active reaction" of sensors (and perhaps other circuitry).

The security functional component Limited fault tolerance (FRU_FLT.2) has been selected in order to address the robustness within some limit (as shown by the inner dashed rectangle in Figure 5) before active reaction takes place. Note that the TOE does not (in most cases) actually detect faults or failures and then correct them in order to guarantee further operation of all the TOE's capabilities. This is the way software

would implement Limited fault tolerance (FRU_FLT.2). Instead the TOE will achieve exactly the same by eliminating the cause for possible faults (by means of filtering for instance) and by being resistant against influences (robustness). In the case of the TOE the "reaction to a failure" is replaced by the "reaction to operating conditions" which could cause a malfunction without the reaction of the TOE's countermeasure.

If the TOE is exposed to other operating conditions this may not be tolerated. Then the TOE must detect that and "preserve a secure state" (use of detectors and cause a reset for instance). The security functional component Failure with preservation of secure state (FPT_FLS.1) has been selected to ensure that. The way the secure state is reached depends on the implementation. Note that the TOE can monitor both external operating conditions and other internal conditions and then react appropriately. Exposure to specific "out of range" external operating conditions (environmental stress) may actually cause failure conditions internally which can be detected by FPT_FLS.1. Referring to external operating conditions the TOE is expected to respond if conditions are detected which may cause a failure. Examples for implementations of the security functional requirement Failure with preservation of secure state (FPT_FLS.1) are a voltage detector (external condition) and a circuitry which detects accesses to address areas which are not used (internal condition).

Those parts of the TOE which support the security functional requirements "Limited fault tolerance (FRU_FLT.2)" and "Failure with preservation of secure state (FPT_FLS.1)" shall be protected from interference of the Smartcard Embedded Software. The security functional component TSF Domain Separation (FPT_SEP.1) has been selected to ensure that.

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

FRU_FLT.2	Limited fault tolerance
Hierarchical to:	FRU_FLT.1
FRU_FLT.2.1	The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: exposure *to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1)*[8].
Dependencies:	FPT_FLS.1 Failure with preservation of secure state
Refinement:	The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.

[8] [assignment: list of type of failures]

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

FPT_FLS.1	Failure with preservation of secure state
Hierarchical to:	No other components.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: *exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur*[9].
Dependencies:	ADV_SPM.1 Informal TOE security policy model
Refinement:	The term “failure” above also covers “circumstances”. The TOE prevents failures for the “circumstances” defined above.

3) The TOE shall meet the requirement “TSF domain separation” state (FPT_SEP.1)” as specified below.

FPT_SEP.1	TSF domain separation
Hierarchical to:	No other components.
FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.
Dependencies:	No dependencies.
Refinement:	Those parts of the TOE which support the security functional requirements “Limited fault tolerance (FRU_FLT.2)” and “Failure with preservation of secure state (FPT_FLS.1)” shall be protected from interference of the Smartcard Embedded Software.

[9] [assignment: list of types of failures in the TSF]

(2) Abuse of Functionality

During testing at the end of Phase 3 before TOE Delivery, the TOE shall be able to store some data (for instance about the production history or identification data of the individual die or other data to be used after delivery). Therefore, the security functional component Audit storage (FAU_SAS.1) has been added. The security functional component FAU_SAS.1 has been newly created (refer to [SSVG, 8.6]) and is used instead of FAU_GEN.1 which is too comprehensive to be applicable in this context.

The requirement FAU_SAS.1 shall be regarded as covering the injection of Initialization Data and/or Pre-personalization Data and of supplements of the Smartcard Embedded Software as described in [SSVG, 8.1.1]. After TOE Delivery the identification data (injected as part of the Initialization Data) and the Pre-personalization Data are available to the Smartcard Embedded Software. These data are protected by the TOE as all other User Data. It's up to the Smartcard Embedded Software to use these data stored and provided by the TOE.

The TOE shall prevent functions (provided by hardware features) from being abused after TOE Delivery in order to compromise the TOE's security. (All such functions are called "Test Features" below.) This includes but is not limited to: disclose or manipulate User Data and bypass, deactivate, change or explore security features or functions of the TOE. Details depend on the capabilities of the Test Features provided by the hardware.

This can be achieved (i) by limiting the capabilities of these Test Features after Phase 3, (ii) by limiting the availability of these Test Features after Phase 3 or (iii) by a combination of both. The security functional components Limited capabilities (FMT_LIM.1) and Limited availability (FMT_LIM.2) have been newly created (refer to [SSVG, 8.5]) to address this.

Examples of the technical mechanism used in the TOE are user authentication ("passwords"), non-availability (for instance through removal or disabling by "fusing") or a combination of both. A detailed technical specification would unnecessarily disclose details and is beyond the scope of the Security Target.

The TOE is tested after production in Phase 3 (refer to [SSVG, 8.1.1]) using means provided by the IC Dedicated Software and/or specific hardware. Testing is evaluated according to the requirements of the Common Criteria assurance class ATE. The IC Dedicated Software is considered as being a test tool delivered as part of the TOE and used before TOE Delivery only. It does not provide functions in later phases of the card's life-cycle. Therefore, no security functional requirement is mandatory according to this Security Target regarding testing.

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

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

FMT_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: *Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks*[10].

Dependencies: FMT_LIM.2 Limited availability.

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

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: *Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks*[11].

Dependencies: FMT_LIM.1 Limited capabilities.

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

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

[10] [assignment: Limited capability and availability policy]

[11] [assignment: Limited capability and availability policy]

FAU_SAS.1.1 The TSF shall provide *test personnel before TOE Delivery*[12] with the capability to store *the Initialization Data and/or Pre-personalization Data and/or supplements of the Smartcard Embedded Software*[13] in the audit records.

Dependencies: No dependencies.

(3) Physical Manipulation and Probing

The TOE can be subject to "tampering" which here pertains to (i) manipulation of the chip hardware and its security features with (ii) prior reverse-engineering to understanding the design and its properties and functions, (iii) determination of critical data through measuring using galvanic contacts, (iv) determination of critical data not using galvanic contacts and (v) calculated manipulation of memory contents.

The TOE is not always powered and therefore not able to detect, react or notify that it has been subject to tampering. Nevertheless, its design characteristics make reverse-engineering and manipulations etc. more difficult. This is regarded as being an "automatic response" to tampering. Therefore, the security functional component Resistance to physical attack (FPT_PHP.3) has been selected. The TOE may also provide features to actively respond to a possible tampering attack which is also covered by FPT_PHP.3

The TOE may also leave it up to the Smartcard Embedded Software to react when a possible tampering has been detected. Comprehensive guidance (refer to Common Criteria assurance class AGD) will be given for the developer of the Smartcard Embedded Software in this case. Taking the assumption "Usage of Hardware Platform (A.Plat-Appl)" into consideration this case shall therefore also be covered by FPT_PHP.3[14].

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

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

FPT_PHP.3.1 The TSF shall resist *physical manipulation and physical probing*[15] to the *TSF*[16] by responding automatically such that

[12] [assignment: authorised users]

[13] [assignment: list of audit information]

[14] This must be evaluated for the final smartcard product.

[15] [assignment: physical tampering scenarios]

the TSP is not violated.

Dependencies: No dependencies.

Refinement: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, “automatic response” means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

(4) Leakage

When the Smartcard processes User Data and/or TSF Data, information about these data may be leaked by signals which can be measured externally (especially the ISO contacts of the Smartcard). An attacker may also cause malfunctions or perform manipulations of the TOE in order to cause the TOE to leak information. The analysis of those measurement data can lead to the disclosure of User Data and other critical data. Examples are given in [SSVG, 8.3].

The security functional requirements “Basic internal transfer protection (FDP_ITT.1)” and “Basic internal TSF data transfer protection (FPT_ITT.1)” have been selected to ensure that the TOE must resist leakage attacks (both for User Data and TSF data). The corresponding security policy is defined in the security functional requirement “Subset information flow control (FDP_IFC.1)”. These security functional requirements address inherent leakage. With respect to forced leakage they have to be considered in combination with the security functional requirements “Limited fault tolerance (FRU_FLT.2)” and “Failure with preservation of secure state (FPT_FLS.1)” on the one hand and “Resistance to physical attack (FPT_PHP.3)” on the other.

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

FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the *Data Processing Policy* [17] to prevent

[16] [assignment: list of TSF devices/elements]

[17] [assignment: access control SFP(s) and/or information flow control SFP(s)]

the *disclosure*[18] of user data when it is transmitted between physically-separated parts of the TOE.

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

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

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

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure*[19] when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies.

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

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

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

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the *Data Processing Policy*[20] on *all confidential data when they are processed or transferred by the TOE or by the Smartcard Embedded Software*[21].

[18] [selection: disclosure, modification, loss of use]

[19] [selection: disclosure, modification]

[20] [assignment: information flow control SFP]

[21] [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]

Dependencies: FDP_IFF.1 Simple security attributes

The following Security Function Policy (SFP) Data Processing Policy is defined for the requirement “Subset information flow control (FDP_IFC.1)”: User Data and TSF data shall not be accessible from the TOE except when the Smartcard Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Smartcard Embedded Software.

(5) Random Numbers

The TOE generates random numbers. To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined in [SSVG, 8.4]. This class FCS_RND Generation of random numbers describes the functional requirements for random number generation used for cryptographic purposes. For details on tests refer to the refinement of the assurance component of the family ATE_COV in [SSVG, 5.1.3].

11) The TOE shall meet the requirement “Quality metric for random numbers (FCS_RND.1)” as specified below (Common Criteria Part 2 extended).

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet *class P2 SOF-high in [AIS31]*[22]

Dependencies: No dependencies.

[22] [assignment: a defined quality metric]

5.1.1.2 TOE Functional Requirements from [PA]

The following TOE Functional Requirements are taken from [PA, 2.4.1.1].

(1) Cryptographic Support

FCS_COP.1A and FCS_COP.1B Cryptographic operation require a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard. The dependencies are discusses in Section 8.2.

The following additional specific security functionality is implemented in the TOE;

- Triple Data Encryption Standard (3DES)
- Mutual Authentication

(a) [Triple-DES operation]

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

FCS_COP.1A	Cryptographic operation
Hierarchical to:	No other components.
FCS_COP.1.1A	The TSF shall perform encryption and decryption [23] in accordance with a specified cryptographic algorithm *Triple Data Encryption Standard (3DES)*[24] and *cryptographic key sizes of 112/168 bits*[25] that meet the following *standards*[26]: *U.S. Department of Commerce/National Bureau of Standards Data Encryption Standard (DES), FIPS PUB 46-3, 1999 October 25.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes

[23] [assignment : list of cryptographic operations]

[24] [assignment : cryptographic algorithm]

[25] [assignment : cryptographic key sizes]

[26] [assignment : list of standards]

(b) [Mutual Authentication]

13) The mutual authentication of the TOE shall meet the requirement “Cryptographic operation (FCS_COP.1B)” as specified below.

FCS_COP.1B	Cryptographic operation
Hierarchical to:	No other components.
FCS_COP.1.1B	The TSF shall perform *mutual authentication*[27] in accordance with a specified cryptographic algorithm *encryption specified by applications*[28] and *specific cryptographic key sizes* [29] that meet the following *standards*[30]: *Cryptographic algorithm specified by applications*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes

[27] [assignment : list of cryptographic operations]

[28] [assignment : cryptographic algorithm]

[29] [assignment : cryptographic key sizes]

[30] [assignment : list of standards]

5.1.2 TOE Assurance Requirements

The assurance level for this Security Target is EAL4 augmented with the following components:

- ADV_IMP.2,
- ALC_DVS.2
- AVA_MSU.3, and
- AVA_VLA.4.

The assurance requirements are given in the following Table 4.

Table 4: Assurance Requirements

Assurance class	ID	Family name
Development (Class ADV)	ADV_FSP.2	Functional Specification
	ADV_SPM.1	Security Policy Modeling
	ADV_HLD.2	High-Level Design
	ADV_LLD.1	Low-Level Design
	ADV_IMP.2	Implementation Representation
	ADV_RCR.1	Representation Correspondence
Tests (Class ATE)	ATE_COV.2	Coverage
	ATE_DPT.1	Depth
	ATE_FUN.1	Functional Tests
	ATE_IND.2	Independent Testing
Delivery and operation (Class ADO)	ADO_DEL.2	Delivery
	ADO_IGS.1	Installation, generation, and start-up
Guidance documents (Class AGD)	AGD_ADM.1	Administrator Guidance
	AGD_USR.1	User guidance
Configuration management (Class ACM)	ACM_AUT.1	CM automation
	ACM_CAP.4	CM Capabilities
	ACM_SCP.2	CM Scope
Life cycle support (Class ALC)	ALC_DVS.2	Development Security
	ALC_LCD.1	Life Cycle Definition
	ALC_TAT.1	Tools and Techniques
Vulnerability assessment (Class AVA)	AVA_MSU.3	Misuse
	AVA_SOF.1	Strength of TOE Security Functions
	AVA_VLA.4	Vulnerability Analysis

The minimum strength of security functions for the TOE is SOF-high.

5.1.3 Refinements of the TOE Assurance Requirements

Refinements list of the assurance requirements taken from [SSVG, 5.1.3] is shown in Table 5. For details of the refinements refer to [SSVG].

Table 5: Refinements list of Assurance Requirements

Refinements of the assurance requirements	Family name	Abbreviated name
Refinements regarding Delivery	Delivery	ADO_DEL
Refinements regarding Development Security	Development Security	ALC_DVS
Refinement regarding CM scope	CM Scope	ACM_SCP
Refinement regarding CM capabilities	CM Capabilities	ACM_CAP
Refinements regarding Functional Specification	Functional Specification	ADV_FSP
Refinement regarding Test Coverage	Coverage	ATE_COV
Refinement regarding Installation, Generation, and Start-up	Installation, generation, and start-up	ADO_IGS
Refinement regarding User Guidance	Administrator Guidance	AGD_USR
Refinement regarding Administrator Guidance	User Guidance	AGD_ADM
Additional Guidance regarding Vulnerability Analysis and Strength of Functions	Vulnerability Analysis	AVA_VLA
	Strength of TOE Security Functions	AVA_SOF

5.2 Security Requirements for the Environment

5.2.1 Security Requirements for the IT-Environment

5.2.1.1 Security Requirements for the IT-Environment from [SSVG]

The security requirements for the IT-environment from [SSVG] are none.

5.2.1.2 Security Requirements for the IT-Environment from [PA]

The security functional requirement “Cryptographic operation (FCS_COP.1A and FCS_COP.1B)” met by TOE has the following dependencies

- [FDP_ITC.1 Import of user data without security attributes or
  FDP_ITC.2 Import of user data with security attributes or
  FCS_CKM.1 Cryptographic key generation],
- FCS_CKM.4 Cryptographic key destruction,
- FMT_MSA.2 Secure security attributes.

These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function. All requirements concerning key management shall be fulfilled by the environment since the Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE.

1) The environment shall meet the requirement “Import of user data without security attributes (FDP_ITC.1)” or “Import of user data with security attributes (FDP_ITC.2)” or “Cryptographic key generation (FCS_CKM.1)” as specified below.

FDP_ITC.1	Import of user data without security attributes
Hierarchical to:	No other components.
FDP_ITC.1.1	The TSF shall enforce the *Access Control Policy or Information Flow Control Policy*[31] when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *Data*

[31] [assignment: access control SFP and/or information flow control SFP]

Control Policy Supplement [32].

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialization

FDP_ITC.2 Import of user data with security attributes

Hierarchical to: No other components.

FDP_ITC.2.1 The TSF shall enforce the *Access Control Policy or Information Flow Control Policy* [33] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall enforce that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall enforce that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *Data Control Policy Supplement* [34].

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

[32] [assignment: additional importation control rules]

[33] [assignment: access control SFP and/or information flow control SFP]

[34] [assignment: additional importation control rules]

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with *Key generation algorithm that fits international, domestic, and organization standard such as 3DES*[35] and *112/168 bits length key*[36] that meet the following[37]:
Application's proprietary specification

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Note: Depending on an application, cryptographic keys are generated outside the smartcard.

2) The environment shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with *change key and change key with certificate verification*[38] that meets the following[39]:
Application's proprietary specification

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

Note: Cryptographic keys are destroyed in response to external command.

[35] [assignment: cryptographic key generation algorithm]

[36] [assignment: cryptographic key sizes]

[37] [assignment: list of standards]

[38] [assignment: cryptographic key destruction method]

[39] [assignment: list of standards]

3) The environment shall meet the requirement “Secure security attributes (FMT_MSA.2)” as specified below.

FMT_MSA.2	Secure security attributes
Hierarchical to:	No other components.
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.
Dependencies:	ADV_SPM.1 Informal TOE security policy model [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Note:	Prior to execution of each command, password authentication is performed, and the IC accepts a command only if it is verified OK: therefore, only secure values are accepted.

5.2.2 Security Requirements for the Non-IT-Environment

5.2.2.1 Security Requirements for the Non-IT-Environment from [SSVG]

In the following security requirements for the Non-IT-Environment are defined for the development of the Smartcard Embedded Software (in Phase 1) and the Smartcard Packaging, Finishing and Personalization (Phases after TOE Delivery up to Phase 7).

1) The Smartcard Embedded Software is developed in Phase 1 and must support the security functionality of the TOE. This Security Target does not directly define obligatory security functional requirements for the Smartcard Embedded Software itself, because this might restrict the implementation possibilities for the developer. Instead the following general requirement for the design and implementation of the software is stated.

RE.Phase-1 Design and Implementation of the Smartcard Embedded Software

The developers shall design and implement the Smartcard Embedded Software in such way that it meets the requirements from the following documents:
(i) *[Guide-SES]*, and
(ii) Findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.

The developers shall implement the Smartcard Embedded Software in a way that it protects security relevant User Data (especially cryptographic keys) as required by the security needs of the specific application context[40].

The requirement RE.Phase-1 also addresses the fact that the Smartcard Embedded Software may need to support the security functions of the TOE. Examples for such security functional requirements for the Smartcard Embedded Software are given in [SSVG, 8.2.2].

2) The responsible parties for the Phases 4-6 are required to support the security of the TOE by appropriate measures:

RE.Process-Card Protection during Packaging, Finishing and Personalization

The Card Manufacturer (after TOE Delivery up to the end of

[40] In particular, the Smartcard Embedded Software shall not disclose secret User Data to unauthorised users or processes as defined for the application context. Similarly the Smartcard Embedded Software shall not allow unauthorised users or processes to use or modify security relevant User Data.

Phase 6) shall use adequate security measures to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

5.2.2.2 Security Requirements for the Non-IT-Environment from [PA]

3) The Smartcard Embedded Software shall meet the requirements “Cipher Schemas (RE.Cipher)” as specified below.

RE.Cipher Cipher Schemas

The developers of Smartcard Embedded Software must not implement routines in a way which may compromise keys when the routines are executed as part of the smartcard Embedded Software. Performing functions which access cryptographic keys could allow an attacker to misuse these functions to gather information about the key which is used in the computation of the function.

Keys must be kept confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that an appropriate key management has to be realized in the environment.

6 TOE Summary Specification

6.1 TOE security functionality

6.1.1 TOE Security Functions

(1) SF.RNG: Random Number Generator

The TOE generates true random numbers, and meets the randomness quality criteria for the P2 class SOF-high in [AIS31].
The TOE implements this security function by means of a physical hardware random number generator working stable within the limits guaranteed by the security function SF.FAS.
The generated random number can be used for the generation of cryptographic keys and other critical security mechanisms.

(2) SF.FAS: Filters and Sensors

The TOE ensures its correct operation and prevents any malfunction.

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

- VDDA voltage sensor (high & low)
- VDD voltage sensor (high & low)
- VPP voltage sensor (high & low)
- VDD voltage glitch sensor
- Low frequency sensor
- Light sensor
- Clock filter (high frequency & glitch)
- Reset filter (elimination of glitch)
- Temperature sensors (high & low)

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

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

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

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

(3) SF.PHY: Tamper Resistance

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

One of the countermeasures is memory scramble.

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

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

(4) SF.DPR: Data Protection

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

(5) SF.MCT: Mode Control

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

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

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

(6) SF.DES: DES

The TOE realizes the DES encryption/decryption as specified by the following standard.

- *U.S. Department of Commerce / National Bureau of Standards Data*

Encryption Standard (DES), FIPS PUB 46-3, 1999 October 25

A series of processes required for DES encryption/decryption are executed by hardware when relevant command codes such as ECB/CBC, single/triple and encryption/decryption, ciphertext/plaintext and cryptographic keys are set to the Cryptographic Hardware. Plaintext/ciphertext and cryptographic keys are provided from the Smartcard Embedded Software.

(7) SF.AUTH: Mutual Authentication Function

The TOE realizes the mutual authentication function as specified by the following standard.

- *JICSAP IC card specification V2.0 Part 4 IC card for high-speed processing, July 2001 ,IC Card System Application Council*

This security function authenticates whether TOE and the upper level side communicating with TOE hold the identical key.

In this TOE, the encryption that is stipulated by applications is used.

(8) SF.ACU: Access Control Unit

All addresses are being monitored by this security function.
For this function, there are settable 2 modes such as User mode and API mode. Accessible/inaccessible area is controlled in accordance with a selected mode.
When an address is specified to point to an access-inhibited area, it indicates a corruption due to an attack. In this case, the TOE enters the reset state and CPU and all registers are initialized

(9) SF.ID: ID Injection

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

6.1.2 Permutation/Probabilistic effects

The SF.RNG and SF.DPR use probabilistic or permutational effects and have to be included in the AVA_SOF analysis with SOF high.
The cryptographic algorithm of SF.DES and the mutual authentication algorithm of SF.AUTH are scope of the evaluation but it isn't rated.

6.2 Assurance Measures

The Table 6 below shows the mapping of assurance requirements to the documents including necessary information.

Table 6: Mapping of documents to the related assurance requirements

Assurance class	Assurance Family	Documentation
Security Target	ASE	MN67S140 Smartcard IC Security Target
Configuration management	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2	MN67S140 Smartcard IC Configuration Management
Delivery and operation	ADO_DEL.2 ADO_IGS.1	MN67S140 Smartcard IC, The document of Delivery and Operation
Development	ADV_FSP.2	MN67S140 Smartcard IC Functional Specification
	ADV_HLD.2	MN67S140 Smartcard IC Design Specification, HLD
	ADV_LLD.1	MN67S140 Smartcard IC Design Specification, LLD
	ADV_IMP.2	MN67S140 Smartcard IC Implementation
	ADV_RCR.1	MN67S140 Smartcard IC Representation Correspondence
	ADV_SPM.1	MN67S140 Smartcard IC Security Policy Modeling
Guidance documents	AGD_ADM.1 AGD_USR.1	1) MN67S140 Smartcard IC Administrator Guidance, for Smartcard Embedded Software Developer 2) MN67S140 Smartcard IC Administrator Guidance, for Card Manufacturer
Life cycle support	ALC_DVS.2	MN67S140 Smartcard IC Development Security Documentation
	ALC_LCD.1	MN67S140 Smartcard IC The life-cycle definition documentation
	ALC_TAT.1	MN67S140 Smartcard IC The document of the development tools
Tests	ATE	MN67S140 Smartcard IC Test Documentation
Vulnerability assessment	AVA_MSU.3 AVA_SOF.1 AVA_VLA.4	MN67S140 Smartcard IC Vulnerability Assessment

7 PP claim

7.1 PP reference

This Security Target claims conformance to the following Protection Profile.

- Smartcard IC Platform Protection Profile, BSI-PP-0002, Version 1.0, July 2001.

7.2 PP tailoring

7.2.1 FCS_RND.1

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet *class P2 SOF-high in [AIS31].*

7.3 PP additions

Those that are taken from [SSVG] are clearly described in the beginning of the each section. The followings are the others of the additional assumptions, organizational security policies, security objectives, and requirements.

Additions from [PA]:

PP addition	Added section
A.Key-Function	to Section 3.2.2
P.Add-Functions	to Section 3.4.2
O.Add-Functions	to Section 4.1.3
OE.Plat-Appl	to Section 4.2.1
OE.Resp-Appl	
FCS_COP.1A, FCS_COP.1B	to Section 5.1.1.2
FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	to Section 5.2.1.2
FCS_CKM.4	
FMT_MSA.2	
RE.Cipher	to Section 5.2.2.2

TOE proprietary:

PP addition	Added section
A.DES	to Section 3.2.3
A.Interpreter	
OE.DES	to Section 4.2.1
OE.Interpreter	

8 Rationale

8.1 Security Objectives Rationale

Table 7 gives an overview, how the assumptions, threats, and organizational security policies are addressed by the objectives.
The rationale justified in [SSVG, 7.1] is not changed. Hereinafter, only the additional aspects adopted from [PA] and aspects added to the TOE (identified by the use of bold type) are justified in detail.

Table 7: Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat, or Organizational Security Policy	Security Objective	Note
A.Plat-Appl	OE.Plat-Appl	(Phase 1)
A.Resp-Appl	OE.Resp-Appl	(Phase 1)
A.Key-Function	**OE.Plat-Appl** **OE.Resp-Appl**	**(Phase 1)**
A.DES	**OE.DES**	**(Phase 1)**
A.Interpreter	**OE.Interpreter**	**(Phase 1)**
P.Process-TOE	OE.Process-TOE O.Identification	(Phase 2 – 3)
A.Process-Card	OE.Process-Card	(Phase 4 – 6)
T.Leak-Inherent	O.Leak-Inherent	
T.Phys-Probing	O.Phys-Probing	
T.Malfunction	O.Malfunction	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Forced	O.Leak-Forced	
T.Abuse-Func	O.Abuse-Func	
T.RND	O.RND	
P.Add-Functions	**O.Add-Functions**	

The following rationale is adopted from [PA, 2.6.1].

The justification related to the security objective “Additional Specific Security Functionality (O.Add-Functions)” is as follows:

> Since O.Add-Function requires the TOE to implement exactly the same specific security functionality as required by P.Add-Functions, the organizational security policy is covered by the objective.

Nevertheless the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.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 O.Leak-Inherent and O.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.

Compared to [SSVG] 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 TOE 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. This means that this objective covers A.Key-Function in that Key-dependent Functions ensure confidential data or information is protected against leakage attacks. 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 O.Add-Functions.

Compared to [SSVG] 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. It can be concluded from the above that this objective covers A.Key-Function since it ensures that any keys in use are protected from any compromises by adoption of the cryptographic functions. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realized in the environment.
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.

Rationale added to the TOE is presented below.

The justification related to the security objective “Usage of triple-DES (OE.DES)” is as follows:

> Since OE.DES requires the Smartcard Embedded Software developer to implement those function assumed in A.DES, the assumption is covered by the objective.

The justification related to the security objective “Implementation of command interpreter (OE.Interpreter)” is as follows:

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

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.

8.2 Security Requirements Rationale

8.2.1 Rationale for the security functional requirements

Table 8 below gives an overview of how the security functional requirements are combined to meet the security objectives.
The rationale justified in [SSVG, 7.2] is not changed. Hereinafter, only the additional aspects adopted from [PA], and aspects added to the TOE (identified by the use of bold type) are justified in detail.

Table 8: Security Requirements versus Security Objectives

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.Leak-Inherent	- FDP_ITT.1 - FPT_ITT.1 - FDP_IFC.1	RE.Phase-1
O.Phys-Probing	- FPT_PHP.3	RE.Phase-1
O.Malfunction	- FRU_FLT.2 - FPT_FLS.1 - FPT_SEP.1	
O.Phys-Manipulation	- FPT_PHP.3	RE.Phase-1
O.Leak-Forced	All requirements listed for O.Leak-Inherent - FDP_ITT.1, - FPT_ITT.1, - FDP_IFC.1 plus those listed for O.Malfunction and O.Phys-Manipulation - FRU_FLT.2, - FPT_FLS.1, - FPT_SEP.1, - FPT_PHP.3	RE.Phase-1
O.Abuse-Func	- FMT_LIM.1 - FMT_LIM.2 plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced - FDP_ITT.1, - FPT_ITT.1, - FDP_IFC.1, - FPT_PHP.3, - FRU_FLT.2, - FPT_FLS.1, - FPT_SEP.1	
O.Identification	- FAU_SAS.1	

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.RND	- FCS_RND.1 plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced“ - FDP_ITT.1, - FPT_ITT.1, - FDP_IFC.1, - FPT_PHP.3, - FRU_FLT.2, - FPT_FLS.1, - FPT_SEP.1	RE.Phase-1
O.Add-Functions	- **FCS_COP.1A** - **FCS_COP.1B**	**RE.Phase-1 with RE.Cipher**
OE.Plat-Appl		RE.Phase-1
OE.Resp-Appl		- RE.Phase-1 - **FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1** - **FCS_CKM.4** - **FMT_MSA.2**
OE.DES		**RE.Phase-1**
OE.Interpreter		**RE.Phase-1**
OE.Process-TOE	- FAU_SAS.1	Assurance components: refer to below (*)
OE.Process-Card		RE.Process-Card possibly supported by RE.Phase-1

(*) Assurance Components: Delivery (ADO_DEL); Installation, generation, and start-up (ADO_IGS) (using Administrator Guidance (AGD_ADM), User guidance (AGD_USR)); CM automation (ACM_AUT); CM Capabilities (ACM_CAP); CM Scope (ACM_SCP); Development Security (ALC_DVS); Life Cycle Definition (ALC_LCD); Tools and Techniques (ALC_TAT)

The following rationale is adopted from [PA, 2.6.2].

The justification related to the security objective “Additional Specific Security Functionality (O.Add-Functions)” is as follows:

The security functional requirements “Cryptographic operation (FCS_COP.1A and FCS_COP.1B)” exactly require those functions to be implemented which are demanded by O.Add-Functions. Therefore, FCS_COP.1A and FCS_COP.1B are suitable to meet the security objective.

Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context. These issues are addressed by the requirement RE.Phase-1 and more specific by

the security functional requirements

- [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation],
- FCS_CKM.4 Cryptographic key destruction,
- FMT_MSA.2 Secure security attributes.

to be met by the environment.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality. However, key-dependent functions could be implemented in the Smartcard Embedded Software. In this case RE.Cipher requires that these functions ensure that confidential data (User Data) can not be disclosed while they are just being processed by the Smartcard Embedded Software. Therefore, with respect to the Smartcard Embedded Software the issues addressed by the objectives just mentioned are addressed by the requirement RE.Cipher.

The usage of cryptographic algorithms requires using appropriate keys. Otherwise they do not provide security. The requirement RE.Cipher addresses these specific issues since cryptographic keys and other data are provided by the Smartcard Embedded Software. RE.Cipher requires that keys must be kept confidential. They must be unique with a very high probability, cryptographically strong etc. If keys are imported into the TOE (usually after TOE Delivery), it must be ensured that quality and confidentiality is maintained. Therefore, with respect to the environment the issues addressed (i) by the objectives just mentioned and (ii) implicitly by O.Add-Functions are addressed by the requirement RE.Cipher.

Rationale added to the TOE is presented below.

The justification related to the security objective “Treatment of User Data (OE. Resp-Appl)” is as follows:

RE.Phase-1 requires the Smartcard Embedded Software developer to design and implement the software in a way. Besides, Environment Security Objectives, FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4, and FMT_MSA.2 realize an appropriate key management. These security requirements are suitable to meet OE.Resp-Appl.

The justification related to the security objective “Usage of triple-DES (OE.DES)” is as follows:

RE.Phase-1 requires the Smartcard Embedded Software developer to design and implement the software in a way, which is suitable to meet OE.DES.

The justification related to the security objective "Implementation of command interpreter (OE.Interpreter)" is as follows:

RE.Phase-1 requires the Smartcard Embedded Software developer to design and implement the software in a way, which is suitable to meet OE.Interpreter.

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

Note that there is a detailed explanation for each security functional requirement in Section 5.1.1.

8.2.2 Dependencies of security functional requirements

Table 9 below lists the security functional requirements defined in this Security Target, their dependencies and whether they are satisfied by other security requirements defined in this Security Target.

This rationale is adopted from [SSVG, 7.2.2], with additional aspects (identified by the use of bold type) adopted from [PA, 2.6.2.2].

Table 9: Dependencies of the Security Functional Requirements

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
FRU_FLT.2	FPT_FLS.1	Yes
FPT_FLS.1	ADV_SPM.1	Yes (Part of EAL4)
FPT_SEP.1	None	No dependency
FMT_LIM.1	FMT_LIM.2	Yes
FMT_LIM.2	FMT_LIM.1	Yes
FAU_SAS.1	None	No dependency
FPT_PHP.3	None	No dependency
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes
FDP_IFC.1	FDP_IFF.1	See discussion in [SSVG, 7.2.2]
FPT_ITT.1	None	No dependency
FCS_RND.1	None	No dependency
FCS_COP.1A	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2**	**Yes (by the environment)**
FCS_COP.1B	**FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2**	**Yes (by the environment)**

The dependencies defined for FCS_COP.1A and FCS_COP.1B are addressed in the environment through the presence of RE.Cipher (see section 5.2.2).

8.2.3 Rationale for the Assurance Requirements and the Strength of Function Level

This ST adopts the rationale in [SSVG, 7.2.3] for the choice of the EAL4 augmentations and SOF-high.

8.2.4 Security Requirements are Mutually Supportive and Internally Consistent

In addition to the discussion in [SSVG, 7.3], the security functional requirement FCS_COP.1A and FCS_COP.1B are newly added to this Security Target. The additional rationale to deal with FCS_COP.1A and FCS_COP.1B is adopted from [PA, 2.6.3] as follows.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms implemented according to the security functional requirement FCS_COP.1A and FCS_COP.1B. Therefore, these security functional requirements support the secure implementation and operation of FCS_COP.1A and FCS_COP.1B.

8.3 TOE Summary Specification Rationale

Table 10 below gives an overview, how the security functional requirements are fulfilled by TOE security functions. The text following after the table justifies in detail.
This security target (ST-Lite) can't provide the rationale for the specification of TOE summary.

Table 10: mapping of SFR to TOE Security Function

SFR \ TSF	SF.RNG	SF.FAS	SF.PHY	SF.DPR	SF.MCT	SF.DES	SF.AUTH	SF.ACU	SF.ID
FRU_FLT.2		ü							
FPT_FLS.1		ü							
FPT_SEP.1		ü						ü	
FDP_ITT.1			ü	ü					
FPT_ITT.1			ü	ü					
FDP_IFC.1			ü	ü					
FDP_PHP.3			ü						
FMT_LIM.1					ü				
FMT_LIM.2					ü				
FAU_SAS.1									ü
FCS_RND.1	ü								
FCS_COP.1A						ü			
FCS_COP.1B							ü		

8.4 PP Claims Rationale

In this Security target, all the security objectives and requirements from [SSVG] are adopted by inclusion (as shown in the relevant sections). The additional aspects adopted from [PA] are consistent with [SSVG] as argued in section 8.2.4, and hence no further rationale is required.

9 Annex

9.1 Glossary of Vocabulary

Terms	Definitions
Administrator	(in the sense of the Common Criteria) The TOE may provide security functions which can or need to be administrated (i) by the Smartcard Embedded Software or (ii) using services of the TOE after delivery to Phases 4-6. Then a privileged user (in the sense of the Common Criteria, refer to definition below) becomes an administrator.
Card Manufacturer	The customer of the TOE Manufacturer who receives the Delivery. The Card Manufacturer includes all roles after TOE Delivery up to Phase 7 (refer to section 2.2 and [SSVG, 8.1.1]). The Card Manufacturer has the following roles (i) the Smartcard Product Manufacturer (Phase 5) and (ii) 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.
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
IC Dedicated Software	IC proprietary software embedded in a smartcard IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
Initialisation Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and for TOE identification (identification data).
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.
Smartcard	(as used in this Security Target) Composition of the TOE, the Smartcard Embedded Software, User Data and the package (the smartcard carrier).

Terms	Definitions
Smartcard Embedded Software	Software embedded in a smartcard IC and not being developed by the IC Designer. The Smartcard Embedded Software is designed in Phase 1 and embedded into the Smartcard IC in Phase 3 or in later phases of the smartcard product life-cycle. Some part of that software may actually implement a smartcard application others may provide standard services. Nevertheless, this distinction doesn't matter here so that the Smartcard Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.
Test Features	All features and functions (implemented by the IC Dedicated Test Software and/or hardware) which are designed to be used before TOE Delivery only and delivered as part of the TOE.
TOE Delivery	The period when the TOE is delivered which is either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of modules.
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 modules, 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 [CC-1] (for example configuration data). Note that the TOE is the Smartcard IC (refer to definition in section 2.1). Initialisation Data defined by the Integrated Circuits manufacturer to identify the TOE and to keep track of the product's production and further life-cycle phases are also considered as belonging to the TSF data.
User	(in the sense of the Common Criteria) The TOE serves as a platform for the Smartcard Embedded Software. Therefore, the "user" of the TOE (as used in the Common Criteria assurance class AGD: guidance) is the Smartcard Embedded Software. Guidance is given for the Smartcard Embedded Software Developer. On the other hand the Smartcard (with the TOE as a major element) is used in a terminal where communication is performed through the ISO interface provided by the TOE. Therefore, another "user" of the TOE is the terminal (with its software).
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.

9.2 List of Abbreviations

Abbreviations	Meanings
ASK	Amplitude Shift Keying
CBC	Cipher Block Chaining
CC	Common Criteria Version 2.1
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EB	Electron Beam
ECB	Electronic Code Book
FIB	Focused Ion Beam
IC	Integrated Circuit
IT	Information Technology
NMI	Non-Maskable Interrupt
PP	Protection Profile
RF	Radio Frequency
RNG	Random Number Generator
SOF	Strength of function
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of control
TSF	TOE Security functions
TSP	TOE Security Policy

9.3 Related Documents

Abbreviated name	References
[AIS31]	Functionality classes and evaluation methodology for physical random number generators, AIS31, Version 1, 25.9.2001.
[CC]	Common Criteria for Information Technology Security Evaluation; Version 2.1 (ISO 15408)
[CC-1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.1 (ISO 15408)
[CC-2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.1 (ISO 15408)
[CC-3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.1 (ISO 15408).
[Guide-SES]	MN67S140 Smartcard IC Administrator Guidance, - for Smartcard Embedded Software Developer -
[Guide-CM]	MN67S140 Smartcard IC Administrator Guidance, - for Card Manufacturer -
[PA]	Smartcard Integrated Circuit Platform Augmentations, v1.0, Atmel, Hitachi Europe, Infineon Technologies & Philips Semiconductors, 8 March 2002
[SSVG]	Smartcard IC Platform Protection Profile, BSI-PP-0002, Version 1.0, July 2001.
[ISO/IEC 14443]	ISO/IEC 14443: Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards --
[JICSAP]	JICSAP IC card specification V2.0, Part 4 IC card for high-speed processing, July 2001, IC Card System Application Council
[JIL]	Joint Interpretation Library, ST-lite, Version1.0, December 2001