

# Smartcard IC Platform Protection Profile

Version 1.0

July 2001

# developed by

Atmel Smart Card ICs
Hitachi Europe Ltd.
Infineon Technologies AG
Philips Semiconductors

Registered and Certified by
Bundesamt für Sicherheit in der Informationstechnik (BSI)
under the reference BSI-PP-0002.

This page is intentionally left blank.

# **Table of Contents**

1	PP Introd	duction	5	
1.1	PP Identification			
1.2	PP Overview			
	1.2.1 In	troduction	7	
	1.2.2 Lii Pr	fe-Cycle versus Scope and Organisation of this Protection of the control of the c	8	
		pecific Issues of Smartcard Hardware and the Common riteria	12	
1.3	Evaluatio	n Assurance Level	15	
2	TOE Des	cription	15	
2.1	TOE Defi	nition	15	
2.2	Further D	efinitions and Explanations	19	
3	TOE Sec	urity Environment	20	
3.1	Description	on of Assets	20	
3.2	Assumptions			
3.3	Threats			
3.4	Organisational Security Policies			
4	Security Objectives			
4.1	Security Objectives for the TOE			
4.2	Security (	Objectives for Environment	37	
5	IT Securi	ity Requirements	39	
5.1	TOE Security Requirements			
	5.1.1 TO	DE Functional Requirements	39	
	5.1.2 TO	DE Assurance Requirements	50	
	5.1.3 Re	efinements of the TOE Assurance Requirements	51	
5.2	Security Requirements for the Environment			
	5.2.1 Se	ecurity Requirements for the IT-Environment	67	
	5.2.2 Se	ecurity Requirements for the Non-IT-Environment	67	
6	PP Appli	cation Notes	68	

7	Rationale			
7.1	Secur	Security Objectives Rationale		
7.2	Security Requirements Rationale			
	7.2.1	Rationale for the security functional requirements	70	
	7.2.2	Dependencies of security functional requirements	76	
	7.2.3	Rationale for the Assurance Requirements and the Strength of Function Level	78	
7.3	Security Requirements are Mutually Supportive and Internally Consistent			
8	Anne	x	83	
8.1	Development and Production Process (life-cycle)			
	8.1.1	Life-Cycle Description	83	
	8.1.2	Description of Assets of the Integrated Circuits Designer/Manufacturer	87	
8.2	Security Aspects of the Smartcard Embedded Software			
	8.2.1	Further Information regarding A.Resp-Appl	88	
	8.2.2	Examples of Specific Functional Requirements for the Smartcard Embedded Software	90	
8.3	Exam	Examples of Attack Scenarios		
8.4	Defini	Definition of the Family FCS_RND		
8.5	Defini	Definition of the Family FMT_LIM		
8.6	Definition of the Family FAU_SAS			
8.7	Glossary of Vocabulary			
8.8	List of Abbreviations10			

# 1 PP Introduction

This chapter *PP Introduction* contains the following sections:

PP Identification (1.1)

PP Overview (1.2)

Introduction (1.2.1)

Life-Cycle versus Scope and Organisation of this Protection Profile (1.2.2)

Specific Issues of Smartcard Hardware and the Common Criteria (1.2.3)

Evaluation Assurance Level (1.3)

### 1.1 PP Identification

Title: Smartcard IC Platform Protection Profile

Version number: Version 1.0 of July 2001

Provided by: Atmel Smart Card ICs, Hitachi Europe Ltd., Infineon Technologies AG,

and Philips Semiconductors

Technical editors: debis Systemhaus Information Security Services GmbH,

Rabinstraße 8, 53111 Bonn, Germany

in co-operation with the above mentioned IC manufacturers

Certified by: Bundesamt für Sicherheit in der Informationstechnik (BSI)

under registration number BSI-PP-0002

- 1 This Smartcard IC Platform Protection Profile has been developed on the basis of
  - [1] Protection Profile Smartcard Integrated Circuit (Version 2.0, Issue September 1998), Registered at the French Certification Body under the number PP/9806 and
  - [2] Smartcard Protection Profile of the Smartcard Security User Group; SCSUG, Draft Version 2.1d, March 21, 2001.

Version 1.0 (July 2001) Page 5 (of 100)

- A product compliant with this Protection Profile may also offer additional security functions. A list of possible augmentations is given in
  - [3] Smartcard Integrated Circuit Platform Augmentations provided by the Atmel Smart Card ICs, Hitachi Europe Ltd., Infineon Technologies AG, and Philips Semiconductors
- 3 This Smartcard IC Platform Protection Profile has been built with the
  - [4] Common Criteria for Information Technology Security Evaluation; Version 2.1 (ISO 15408)

### which comprises

- [5] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.1 (ISO 15408)
- [6] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.1 (ISO 15408)
- [7] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.1 (ISO 15408)
- 4 The
  - [8] Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology; Version 1.0, August 1999

has been taken into account.

5 Chapter 2 contains definitions used in this *Smartcard IC Platform Protection Profile*. A *Glossary* is given in the annex (Section 8.7). A *List of Abbreviations* is also given in the annex (Section 8.8).

Version 1.0 (July 2001) Page 6 (of 100)

### 1.2 PP Overview

### 1.2.1 Introduction

- 6 This Protection Profile is the work of the following Integrated Circuits manufacturers:
  - Atmel,
  - Hitachi Europe,
  - Infineon Technologies, and
  - Philips Semiconductors.

in co-operation with debis Systemhaus Information Security Services GmbH (T-Systems IT Security Services).

- The increase in the number and complexity of applications in the smartcard market is reflected in the increase of the level of data security required. The security needs for a smartcard can be summarised as being able to counter those who want to defraud, gain unauthorised access to data and control a system using a smartcard. Therefore it is mandatory to:
  - maintain the integrity and the confidentiality of the content of the smartcard memory as required by the application(s) the smartcard is built for and
  - maintain the correct execution of the software residing on the card.
- 8 This requires that the smartcard integrated circuit especially maintains the integrity and the confidentiality of its security enforcing and security relevant architectural components.
- Protected information are in general secret data as Personal Identification Numbers, Balance Value (Stored Value Cards), and Personal Data Files. Other protected information are the data representing the access rights; these include any cryptographic algorithms and keys needed for accessing and using the services provided by the system through use of the smartcard.
- The intended environment is very large; and generally once issued the smartcard can be stored and used anywhere in the world, at any time, and no control can be applied to the smartcard and the card operational environment.
- 11 For the sake of better understanding the definition of the TOE is copied from chapter 2 (which contains details) and already given here:

The Target of Evaluation (TOE) is a *smartcard integrated circuit* which is composed of a processing unit, security components, I/O ports (contact and/or contactless) and volatile and non-volatile memories (hardware). The TOE also includes any IC Designer/Manufacturer proprietary IC Dedicated Software as long as it physically exists in the smartcard integrated circuit after being delivered by the IC Manufacturer. Such software (also known as IC firmware) is often used for testing purposes during

Version 1.0 (July 2001) Page 7 (of 100)

production only but may also provide additional services to facilitate usage of the hardware and/or to provide additional services (for instance in the form of a library). In addition to the IC Dedicated Software the Smartcard Integrated Circuit may also comprise hardware to perform testing. All other software is called Smartcard Embedded Software and is not part of the TOE.

The typical Smartcard integrated circuit product as the TOE is composed of a processing unit, security components, I/O ports and volatile and non-volatile memories as depicted in Figure 1.

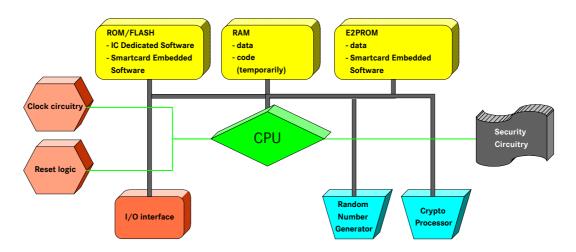


Figure 1: Typical Smartcard IC Product (especially the Cryptographic Processors are optional)

The evaluation of the smartcard integrated circuit according to this Protection Profile is independent of the evaluation of the Smartcard Embedded Software. The developer of the Smartcard Embedded Software decides if the platform (evaluated smartcard integrated circuit) is suitable for the application. An evaluation of a Smartcard can be built on the results of the evaluation of the smartcard integrated circuit conforming to this Protection Profile.

# 1.2.2 Life-Cycle versus Scope and Organisation of this Protection Profile

# Introduction to and Coverage of the Life-Cycle

- 14 The complex development and manufacturing processes of a smartcard can be separated into three distinct stages:
  - the development stage:
    - Smartcard Embedded Software development (Phase 1),
    - integrated circuit (hereafter "IC") design, IC Dedicated Software development, integration and photomask fabrication (Phase 2),

Version 1.0 (July 2001) Page 8 (of 100)

- the IC production stage: IC manufacturing, testing, preparation and shipping to the IC assembly line (Phase 3),
- the smartcard production stage:
  - smartcard IC packaging (and testing) (Phase 4),
  - smartcard product finishing process, printing (and testing), smartcard preparation and shipping to the personalisation line (Phase 5),
- 15 In addition, two important stages have to be considered in the smartcard life cycle:
  - the smartcard personalisation and testing stage where the User Data is loaded into the smartcard's memory (Phase 6),
  - the smartcard usage by its issuers and end-user (Phase 7) which may include loading and other management of applications in the field.
- This should be understood as covering multi-application approaches. A detailed description of the life-cycle is given in Section 8.1.
- The whole life-cycle of the card will be considered during evaluations using this Protection Profile as far as the developer/manufacturer of the TOE is directly involved. An organisational security policy (refer to Section 3.4) and a security objective (refer to Section 4) is defined to ensure that this is covered. However, a complex of details is given in terms of refinements of the Common Criteria assurance components since they are built to cover the development and production processes.
- The scope of those assurance components referring the product's life-cycle is limited to Phases 2 and 3. These phases are under the control of the Integrated Circuits manufacturer. All procedures within these phases are covered by the Protection Profile. This includes the interfaces to the other phases where information and material is being exchanged with the partners of the developer/manufacturer of the TOE.
- 19 Phase 4 (IC Packaging and Testing) is also included if the developer/manufacturer of the TOE delivers modules.
- The Common Criteria [5] states: "Evaluation focuses on the IT security parts of the product or system and those parts of the operational environment that may directly affect the secure use of IT elements." "... refinements may be made to ISO/IEC 15408-3" elements as required." [5] A refinement is the addition of details to a (assurance) component. And [7] reads: Development security (ALC\_DVS) "deals with measures to remove or reduce threats existing at the developer's site. Conversely, threats to be countered at the TOE user's site are normally covered in the security environment subclause of a PP or ST." Therefore, in this Protection Profile security

Version 1.0 (July 2001) Page 9 (of 100)

issues related to the development and production environment will not be specified in terms of threats but in terms of an organisational security policy.

The principles are visualised in Figure 2 and will be explained in the remainder of this section. Other requirements may also be mentioned here to correctly interface to a Protection Profile for the Smartcard Embedded Software and vice versa.

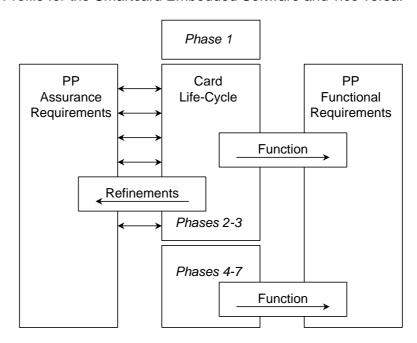


Figure 2: Card Life-Cycle versus PP Requirements

# **Delivery and External Interfaces of the Integrated Circuits manufacturer**

- The Common Criteria depict an ideal development process starting with a definition of the requirements and then having the design process, implementation, test, acceptance, delivery and usage. However, the smartcard development and production process is more complex.
- For instance the external interfaces of the IC designer / IC manufacturer are complex: Not only the delivery of the final product ("die" or wafer to smartcard embedding and personalisation) must be considered. The IC designer / IC manufacturer interacts with the Smartcard Embedded Software development, the mask manufacturer and may also exchange critical information with the card manufacturer.
- Therefore, Common Criteria assurance requirements will be refined in Section 5.1.3
  - to ensure that this Protection Profile exactly reflects the requirements for the exchange of information and material between the developer/manufacturer of the TOE and its partners.

Version 1.0 (July 2001) Page 10 (of 100)

In particular, the Common Criteria assurance requirement ADO\_DEL (delivery) is refined. So, the details regarding secure exchange (delivery and receipt) of assets are not specified in terms of threats. The necessity of appropriate security measures is established and emphasised by an organisational security policy.

Application Note 1:

Note: The TOE may provide functions supporting the card's life-cycle (for instance secure/authentic delivery). In this case the corresponding requirements will be specified in the Security Target in terms of security objectives and functional requirements. This is visualised in Figure 2.

# **Security during Development and Production**

- There are a lot of assets which need suitable protection during development and production process. Otherwise the security provided by the TOE's security functions can not be maintained.
- 27 Therefore, Common Criteria assurance requirements will be refined in Section 5.1.3
  - to ensure that this Protection Profile exactly reflects the requirements regarding the protection of critical assets by the developer/manufacturer of the TOE during development and production.
- In particular, the Common Criteria assurance requirement ALC\_DVS (development security) is refined. So, the details regarding the security in the development and production process are not specified in terms of threats. The necessity of appropriate security measures is established and emphasised by an organisational security policy.
- It may be necessary to state requirements for other parties if they use assets generated by the developer/manufacturer of the TOE. However, it can not be assessed during an evaluation according to this Protection Profile whether the requirements are met.
  - Consequently, these requirements must be taken into account during the evaluation of the Smartcard Embedded Software or Smartcard, respectively.
- For assumptions regarding the usage of the TOE (its environment) made in this Protection Profile refer to Section 3.2.

Version 1.0 (July 2001) Page 11 (of 100)

# 1.2.3 Specific Issues of Smartcard Hardware and the Common Criteria

- The smartcard integrated circuit is a platform to be used by the Smartcard Embedded Software. The smartcard integrated circuit itself may not possess any asset (such as critical data). All assets are those of the Smartcard Embedded Software. However, the hardware platform must
  - maintain the integrity and the confidentiality of the content of the smartcard memory as required by the context of the Smartcard Embedded Software and
  - maintain the correct execution of the Smartcard Embedded Software.
- This requires that the smartcard integrated circuit especially maintains the integrity and the confidentiality of its security enforcing and security relevant architectural components.
- The TOE security mechanisms need to work together in different combinations to counter attacks. Owing to complex dependencies, these combinations are only apparent in the context of a specific attack scenario. Often the composition of a security function only becomes clear when considering a specific attack path during vulnerability analysis (AVA\_VLA). A security mechanism may be needed in different security functions depending on the attack path. This has to be considered during the TOE evaluation.
- Detailed specification of the (implementation dependent) security measures and associated binding aspects are beyond the scope of this Protection Profile.
- This Protection Profile will describe the security problems related to smartcard integrated circuits (and the corresponding security objectives and requirements) in a more general way though addressing all important issues. Attack scenarios will be mentioned whenever appropriate but only to illustrate the corresponding security problem. The information about attack scenarios can not be considered as being complete.
- It is not possible (because of differences between the chips) nor desirable (confidentiality; do not instruct the attackers) to specify all the specific attack scenarios and all the security features on a Protection Profile level. The Security Target may describe the Smartcard IC in more detail without necessarily disclosing construction details.
- 37 This Protection Profile will highlight some specific security features or functions though breaking them would not necessarily affect the primary assets in a direct way.
- It is necessary and helpful to raise these second-level security issues already on the level of the Protection Profile or Security Target since appropriate countermeasures are mandatory for a smartcard integrated circuit.
- This Protection Profile will address all the relevant security issues either in a general way (while not disclosing too much details) or in more detail (if possible though often being related to second-level security problems).

Version 1.0 (July 2001) Page 12 (of 100)

### Application Note 2:

Note: The security features of smartcard integrated circuits differ. Some functionality may exist on one chip but not on another (example: cryptographic co-processor). To take this into account this Protection Profile will contain common requirements for smartcard integrated circuits. A Security Target shall take over all the requirements stated here (compliance) but may add functional security requirements for instance from the document *Smartcard Integrated Circuit Platform Augmentations* [3] as appropriate. This is indicated by "Func. Augm." in Figure 3. Therefore, the Security Target used for the evaluation of a smartcard integrated circuit will be created by taking this Protection Profile and adding, for example, appropriate paragraphs from [3] and then adding TOE specific information.

- Hardware and software together shall build an integrated secure whole. There can be a lot of interdependencies between the two. Requirements for the Smartcard Embedded Software should normally be described as Security Requirements for the Environment (Section 5.2) if they are necessary to ensure secure operation of the TOE (here: the smartcard integrated circuit).
- However, particular requirements for the software are often not clear before considering a specific attack scenario during vulnerability analysis (AVA\_VLA). Therefore, such results from the evaluation of the smartcard integrated circuit (contained in the Evaluation Technical Report (ETR)) must be given to the developer of the Smartcard Embedded Software and be taken into account during the evaluation of the software (refer to Figure 3). This may also hold for additional tests being required for the combination of hardware and software.
- In consequence, the Security Requirements for the Environment (Section 5.2) cannot be expected to exactly specify all requests for the Smartcard Embedded Software. In addition, a comprehensive list in a Security Target could disclose too much information about possible vulnerabilities. Instead a separate document must be prepared and handed over to the developer of the Smartcard Embedded Software which gives all the information for developing secure software. In this way modularity for evaluations is supported without making public vulnerabilities of the smartcard integrated circuit or details about the implementation. Refer to A.Plat-Appl in Section 3.2 for more detail.

Version 1.0 (July 2001) Page 13 (of 100)

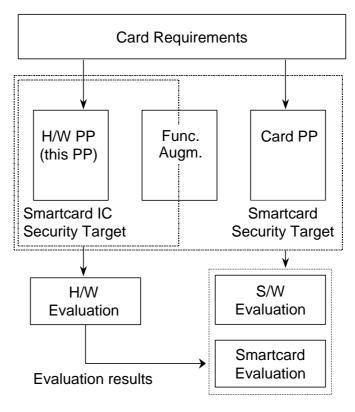


Figure 3: Relationship between Hardware and Smartcard Embedded Software (The term "H/W" means the TOE of this Protection Profile as defined in chapter 2.)

- The TOE serves as a platform for the Smartcard Embedded Software. 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 (contacts or contactless). After production the TOE is tested where communication is performed via the pads which mostly become part of the ISO interface during packaging. Therefore, the roles "user" and "administrator" must be interpreted in a specific way for the TOE. Regarding a definition of the terms "user" and "administrator" refer to Sections 5.1.3.8 and 5.1.3.9, respectively.
- Configuration management (CM) requires "discipline and control in the processes of refinement and modification of the TOE and the related information. CM systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorised." [7] For a standard software development the integrity of the TOE (including authorisation of changes) is very important. In addition, for Smartcard Integrated Circuits the confidentiality of the design (as reflected by the Common Criteria assurance component of the family ALC\_DVS) is a primary goal.
- As an example cryptographic attacks are not only possible taking a purely theoretical (mathematical) approach but also by recording and interpreting information related to the execution of cryptographic operations. Details about the implementation may make such attacks easier. Therefore, in the case of a Smartcard Integrated Circuit, maintaining the confidentiality of the design is very important. This is in contrast

Version 1.0 (July 2001) Page 14 (of 100)

to Kerckhoff's principle, where the security of a cryptographic algorithm should rely solely on the secrecy of the keys and not on the secrecy of the algorithm itself.

If details of the design and layout of the integrated circuit are freely available this would considerably reduce the effort to mount an attack, since reverse-engineering would not be required. The security of the TOE is therefore also based upon concealing information.

### 1.3 Evaluation Assurance Level

The minimum assurance level for this Protection Profile is EAL4 augmented (refer to Section 5.1.2 for more detail). The minimum strength of security functions for the TOE is SOF-high (Strength of Functions High).

Application Note 3:

Revise: If the Security Target goes beyond EAL4 augmented (for instance EAL5 augmented, refer for example to the Smartcard Integrated Circuit Platform Augmentations), add some reference to that in the Security Target.

### 2 TOE Description

This chapter TOE Description contains the following sections:

TOE Definition (2.1)

Further Definitions and Explanations (2.2)

### 2.1 TOE Definition

The Target of Evaluation (TOE) is a *smartcard integrated circuit* which is composed of a processing unit, security components, I/O ports (contact and/or contactless) and volatile and non-volatile memories (*hardware*). The TOE also includes any IC Designer/Manufacturer proprietary IC Dedicated Software as long as it physically exists in the smartcard integrated circuit after being delivered by the IC Manufacturer. Such software (also known as IC firmware) is often used for testing purposes during production only but may also provide additional services to facilitate usage of the hardware and/or to provide additional services (for instance in the form of a library). In addition to the IC Dedicated Software the Smartcard Integrated Circuit may also comprise hardware to perform testing. All other software is called Smartcard Embedded Software and is not part of the TOE. Refer to Figure 1 on page 8.

Version 1.0 (July 2001) Page 15 (of 100)

- 49 Therefore, the TOE comprises
  - the circuitry of the IC (hardware including the physical memories),
  - TSF data<sup>1</sup>

and, if delivered,

- the IC Dedicated Software with the parts
  - IC Dedicated Test Software,
  - IC Dedicated Support Software and
- module packaging if TOE Delivery is after Phase 4 and
- the associated guidance documentation.

The TOE is designed, produced and/or generated by the TOE Manufacturer.

- Note that whenever this Protection Profile describes functions and behaviour of the TOE, it refers to the device only and not to the associated guidance documentation.
- The TSF data (including information about the TOE's configuration, if any) are coded in non-volatile non-programmable memories (ROM), in specific circuitry, in non-volatile programmable memories (for instance E<sup>2</sup>PROM) or a combination thereof. By definition the TSF data<sup>2</sup> belong to the TOE.
- The TOE is developed in Phase 2. The integrated circuit is produced in Phase 3. Then the TOE can be delivered in form of wafers or sawn wafers (dice). The TOE can also be delivered in form of modules. In this case the corresponding assurance requirements of this Protection Profile for the development and production of the TOE not only pertain to Phase 2 and 3 but to Phase 4 in addition. Refer to the life cycle description in Section 8.1.1.

Version 1.0 (July 2001)

Page 16 (of 100)

which may also be coded in specific circuitry of the IC; for a definition refer to the Glossary 8.7

for a definition refer to the Glossary 8.7

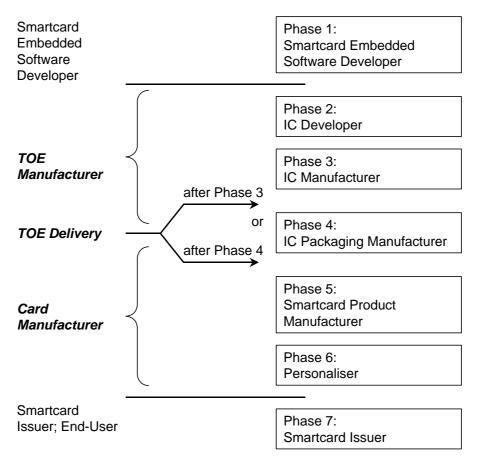


Figure 4: Definition of "TOE Delivery" and responsible Parties

- In the following the term "TOE Delivery" (refer to Figure 4) is uniquely used which indicates
  - after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or
  - after Phase 4 (or before Phase 5) if the TOE is delivered in form of modules.
- The Protection Profile uniquely uses the term "TOE Manufacturer" (refer to Figure 4) which includes the following roles:
  - the IC Developer (Phase 2) and the IC Manufacturer (Phase 3)

if the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice) or

- the IC Developer (Phase 2),
   the IC Manufacturer (Phase 3) and
   the IC Packaging Manufacturer (Phase 4)
  - if the TOE is delivered after Phase 4 in form of modules.

Version 1.0 (July 2001) Page 17 (of 100)

- Hence the "TOE Manufacturer" comprise all roles before "TOE Delivery". Starting with "TOE Delivery" another party takes over the control of the TOE. This Protection Profile defines requirements for the TOE's development and production environment up to "TOE Delivery". Refer to Figure 4.
- The Protection Profile uniquely uses the term "Card Manufacturer" which includes all roles after TOE Delivery (refer to Figure 4) which are the following:
  - the IC Packaging Manufacturer (Phase 4)
    if the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice)
    the Smartcard Product Manufacturer (Phase 5) and
    the Personaliser (Phase 6).
- Note that depending on the application context this may also include tasks of the Smartcard Issuer. However, this is outside the scope of this Protection Profile.
- Application Note 4: Revise: The Security Target must explicitly state whether (i) TOE Delivery is after Phase 3 only or (ii) after Phase 4 as well. This can be done by using the relevant information from the paragraphs above.
- So, in this Protection Profile the following roles are used (i) Smartcard Embedded Software Developer, (ii) TOE Manufacturer and (iii) Card Manufacturer.
- The Target of Evaluation (TOE) is intended to be used in a smartcard product, independent of the physical interface and the way it is packaged. Generally, a smartcard product may include other optional elements (such as specific hardware components, batteries, capacitors, antennae,...) but these are not in the scope of this Protection Profile.
- The IC Dedicated Software is part of the TOE, if it exists on the Smartcard after TOE Delivery. The IC Dedicated Software may comprise (i) IC Dedicated Test Software and (ii) IC Dedicated Support Software:
- The "IC Dedicated Test Software" is not usable after TOE Delivery. Therefore, this software (or parts of it) is seen only as a "test tool" though being delivered as part of the TOE. The IC Dedicated Test Software does not provide TSF after TOE Delivery and is only used to support production of the TOE according to the Common Criteria assurance class ATE (tests). However, it must be verified that it cannot be abused after TOE Delivery: this is evaluated according to the Common Criteria assurance family AVA\_VLA.
- In contrast, the "IC Dedicated Support Software" does provide functions after TOE Delivery. Therefore, during evaluation it is treated as all other parts of the TOE.

Version 1.0 (July 2001) Page 18 (of 100)

Application Note 5:

Revise: If the TOE provides functionality to be used after TOE Delivery this is part of the IC Dedicated Support Software. Then such functions must be specified in the Security Target of the actual TOE possibly using input from the document *Smartcard Integrated Circuit Platform Augmentations* [3]. Revise the above paragraphs in the Security Target to make clear if the TOE comprises IC Dedicated Support Software.

# 2.2 Further Definitions and Explanations

- The Smartcard Embedded Software is normally stored in non-volatile non-programmable memories (ROM). But some parts of it (called supplements for the Smartcard Embedded Software, refer to Section 8.1) may also be stored in non-volatile programmable memories (for instance E<sup>2</sup>PROM). All data managed by the Smartcard Embedded Software is called User Data. In addition, Pre-personalisation Data (refer to Section 8.1) belongs to the User Data.
- Therefore, not included in the TOE, but part of the smartcard (refer to below) there is
  - the Smartcard Embedded Software comprising
    - Hard-coded Smartcard Embedded Software (normally stored in ROM)
    - Soft-coded Smartcard Embedded Software (normally stored in E<sup>2</sup>PROM) and
  - User Data (especially personalisation data and other data generated and used by the Smartcard Embedded Software)
- The Smartcard Embedded Software is not designed and the User Data are not generated by the TOE Manufacturer.
- 66 The "Smartcard" comprises
  - the TOE,
  - the Smartcard Embedded Software,
  - User Data (including Pre-personalisation Data), and
  - its package (the smartcard carrier).
- Note that it is assumed here that the chip is packed. However, the way it is packaged is not specified here.
- Further terms are explained in the Glossary (refer to Section 8.7).

Version 1.0 (July 2001) Page 19 (of 100)

- The following explanations help to understand the focus of the threats and objectives defined below. For example, certain attacks are only one step towards a disclosure of assets, others may directly lead to a compromise of the application security.
  - Manipulation of data (which may comprise any data, including code, stored in or processed by the smartcard integrated circuit) means that an attacker is able to alter a meaningful block of data. This should be considered for the threats T.Malfunction, T.Phys-Manipulation and T.Abuse-Func.
  - Manipulation of the TOE means that an attacker is able to deliberately deactivate or otherwise change the behaviour of a specific function in a manner which enables exploitation. This should be considered for the threat T.Malfunction, T.Phys-Manipulation and T.Abuse-Func.
  - Disclosure of data (which may comprise any data, including code, stored in or processed by the smartcard integrated circuit) means that an attacker is realistically<sup>3</sup> able to determine a meaningful block of data. This should be considered for the threats T.Leak-Inherent, T.Phys-Probing, T.Leak-Forced and T.Abuse-Func.

# **3 TOE Security Environment**

This chapter *TOE Security Environment* contains the following sections:

Description of Assets (3.1)

Assumptions (3.2)

Threats (3.3)

Organisational Security Policies (3.4)

### 3.1 Description of Assets

# **Assets regarding the Threats**

Application Note 6:

Note: This Protection Profile deals with the standard set of assets (both primary and secondary ones) related to standard functionality (refer to paragraphs 70 and 71). Other assets are related to specific functionality. One additional primary asset is already defined here. Other primary and secondary assets may be added to paragraphs 77 and 78 by using for instance the document *Smartcard Integrated Circuit Platform Augmentations* [3].

- 70 The primary assets (related to standard functionality) to be protected are
  - the User Data.

<sup>3</sup> taking into account the assumed attack potential (and for instance the probability of errors)

Version 1.0 (July 2001) Page 20 (of 100)

- Fig. 21 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.

- 72 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.
- 74 Additional assets (secondary ones) are critical information about the TOE which include
  - logical design data, physical design data, IC Dedicated Software, and TSF Data.
- 75 In addition,
  - Initialisation Data and Pre-personalisation Data, specific development aids, test and characterisation 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 (if any) and IC Dedicated Support Software (if any), and (iii) the TSF data.
- 77 Other primary assets (related to specific functionality) are
  - the random numbers generated by the TOE 4.

Version 1.0 (July 2001) Page 21 (of 100)

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.

- 78 Other secondary assets (related to specific functionality) are
  - none.

Application Note 7:

Revise: If the TOE provides further functions or services to the Smartcard Embedded Software it might be necessary to define additional primary and secondary assets. In this case the above paragraphs 77 and 78 are to be revised.

# Assets regarding the Organisational 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, Initialisation Data and Pre-personalisation Data,
  - specific development aids,
  - test and characterisation related data,
  - material for software development support, and
  - photomasks and products in any form

as long as they are generated, stored, or processed by the TOE Manufacturer. Explanations can be found in Section 8.1.2.

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

Version 1.0 (July 2001) Page 22 (of 100)

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

# 3.2 Assumptions

The following Figure 5 shows the assumptions applied in this Protection Profile.

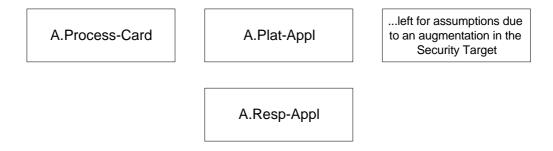


Figure 5: Assumptions

**Application Note 8:** 

Note: The TOE may provide specific security functionality which can be used by the Smartcard Embedded Software. Examples are given in the document *Smartcard Integrated Circuit Platform Augmentations* [3]. In this case it can be required to add additional assumptions in the Security Target.

- 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. 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 and clock) 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.
- Appropriate "Protection during Packaging, Finishing and Personalisation (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 Pr

Protection during Packaging, Finishing and Personalisation

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-user to maintain confidentiality and integrity of the TOE

Version 1.0 (July 2001) Page 23 (of 100)

and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

This means that the Phases after TOE Delivery (refer to Sections 2.1 and 8.1) are assumed to be protected appropriately. For a preliminary list of assets to be protected refer to paragraph 80 (page 22).

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: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the 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 authorised 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.

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 Section 8.2.1, all being directly related to and covered by A.Resp-Appl.

Version 1.0 (July 2001) Page 24 (of 100)

Application Note 9:

Add: If needed further assumptions must be added in the Security Target. Such assumptions might be required if the TOE provides specific security functionality which can be used by the Smartcard Embedded Software. Refer to the document *Smartcard Integrated Circuit Platform Augmentations* [3].

### 3.3 Threats

- The cloning of the functional behaviour of the Smartcard on its ISO command interface is the highest level security concern in the application context.
- The cloning of that functional behaviour requires to (i) develop a functional equivalent of the 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 personalisation 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 Protection Profile. As a result the threat "cloning of the functional behaviour of the smartcard on its ISO command interface" is averted by the combination of measures which split into those being evaluated according to this Protection Profile (smartcard integrated circuit) and those being subject to the evaluation of the Smartcard Embedded Software or Smartcard and the corresponding personalisation process. Therefore, functional cloning is indirectly covered by the security concerns and threats described below.
- According to this Protection Profile 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 E<sup>2</sup>PROM.

Version 1.0 (July 2001) Page 25 (of 100)

These high-level security concerns are refined below by defining threats as required by the Common Criteria (refer to Figure 6). 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.

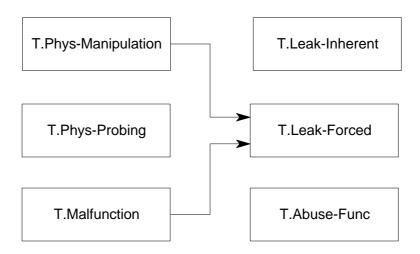


Figure 6: Standard Threats

- According to this Protection Profile 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 (refer to Figure 7).



Figure 7: Threats related to Specific Functionality

Application Note 10:

Add: If the TOE provides further functions or services to the Smartcard Embedded Software (such as cryptographic functions) this would result in having additional high-level security concerns in the Security Target which must also be refined. Examples are given in the document *Smartcard Integrated Circuit Platform Augmentations* [3]. In this case add the appropriate text to the above paragraph.

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.

Version 1.0 (July 2001) Page 26 (of 100)

- The above security concerns are derived from considering the end-usage phase (Phase 7) since
  - Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by assumptions and
  - the development and production environment starting with Phase 2 up to TOE Delivery are covered by an organisational security policy.
- Refer to Figure 4 on page 17. The TOE's countermeasures are designed to avert the threats described below. Nevertheless, they may be effective in earlier phases (Phases 4 to 6).
- 97 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 visualised in Figure 8.

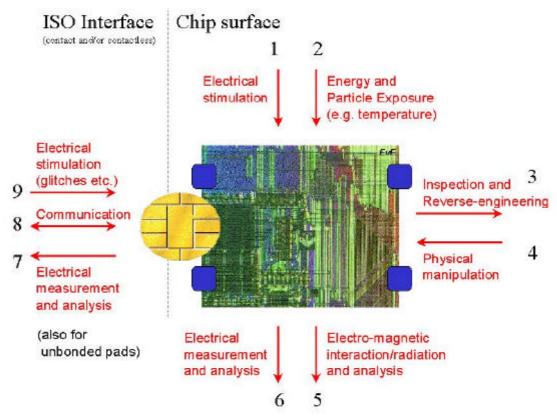


Figure 8: Attack Model for the TOE

An interaction with the TOE can be done through the ISO interfaces (Number 7 – 9 in Figure 8) which are realised using contacts and/or a contactless interface. Influences or interactions with the TOE also occurs through the chip surface (Number 1 – 6 in Figure 8). In Number 1 and 6 galvanic contacts are used. In Number 2 and 5 the

Version 1.0 (July 2001) Page 27 (of 100)

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 behaviour is not only influenced but definite changes are made by applying mechanical, chemical and other methods (such as 1, 2). Many attacks require a prior inspection and some reverse-engineering (Number 3).

99 Examples for specific attacks are given in Section 8.3.

# Standard Threats (referring to SC1 and SC2)

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

T.Leak-Inherent Inherent Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the 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 8) or measurement of emanations (Number 5 in Figure 8) and can then be related to the specific operation being performed.

101 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 8). Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that hardware security mechanisms and layout characteristics need to be identified (Number 3 in Figure 8). Determination of software

Version 1.0 (July 2001) Page 28 (of 100)

design including treatment of User Data may also be a prerequisite.

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

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

### T.Malfunction Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of the 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 8).

To exploit this an attacker needs information about the functional operation.

103 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 8) and IC reverse engineering efforts (Number 3 in Figure 8). 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 to gather significant knowledge about the TOE's internal construction here (Number 3 in Figure 8).

Version 1.0 (July 2001) Page 29 (of 100)

104 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 8) which normally do not contain significant information about secrets.

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

T.Abuse-Func Abuse of Functionality

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

### Threats related to Specific Functionality (referring to SC3)

106 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.

Version 1.0 (July 2001) Page 30 (of 100)

Application Note 11:

Add: Other threats related to specific functionality must be added in the Security Target if this Protection Profile is augmented. This augmentation may be taken from the document *Smartcard Integrated Circuit Platform Augmentations* [3].

### 3.4 Organisational Security Policies

107 The following Figure 9 shows the policies applied in this Protection Profile.

P.Process-TOE

...left for policies due to an augmentation in the Security Target

Figure 9: Policies

Application Note 12:

Add: The TOE may provide specific security functionality which can be used by the Smartcard Embedded Software. Particular specific security functionality may not necessarily be 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. Therefore, the necessity of some specific functionality may not derived from a threat. Instead specific security functionality can be provided according to a security policy to be specified here in this case (refer to the document *Smartcard Integrated Circuit Platform Augmentations* [3]). Such security policies may be added in the Security Target if this Protection Profile needs to be augmented.

108 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 2.1) 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 authorised 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.

Version 1.0 (July 2001) Page 31 (of 100)

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 paragraph 79 (page 22).

# **4 Security Objectives**

This chapter Security Objectives contains the following sections:

Security Objectives for the TOE (4.1)

Security Objectives for Environment (4.2)

# 4.1 Security Objectives for the TOE

- According to this Protection Profile 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 E<sup>2</sup>PROM.

110 These standard high-level security goals are refined below by defining security objectives as required by the Common Criteria (refer to Figure 10). Note that the integrity of the TOE is a means to reach these objectives.

Version 1.0 (July 2001) Page 32 (of 100)

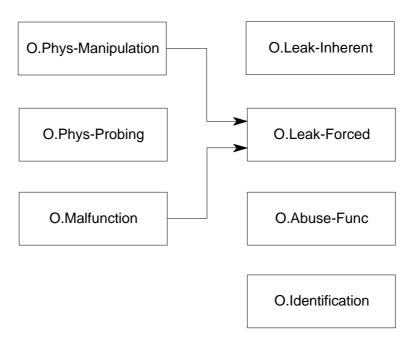


Figure 10: Standard Security Objectives

- According to this Protection Profile there are the following high-level security goals related to specific functionality:
  - SG3 provide random numbers.
- The additional high-level security considerations are refined below by defining security objectives as required by the Common Criteria (refer to Figure 11).



Figure 11: Security Objectives related to Specific Functionality

Application Note 13: Add: If the TOE provides further functions or services to the Smartcard Embedded Software (such as cryptographic functions) this may result in having additional high-level security goals in the Security Target which must also be refined. Examples are given in the document Smartcard Integrated Circuit Platform Augmentations [3].

Version 1.0 (July 2001) Page 33 (of 100)

# Standard Security Objectives (referring to SG1 and SG2)

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

O.Leak-Inherent Protection against Inherent Information Leakage

The TOE must provide protection against disclosure of confidential data (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.

114 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

Version 1.0 (July 2001) Page 34 (of 100)

time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

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

O.Malfunction Protection against Malfunctions

The TOE must ensure its correct operation.

The TOE must 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.

116 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.

Version 1.0 (July 2001) Page 35 (of 100)

117 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.

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. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

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

### O.Identification TOE Identification

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

Version 1.0 (July 2001) Page 36 (of 100)

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

120 The TOE shall provide "Random Numbers (O.RND)" as specified below.

O.RND Random Numbers

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

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

Application Note 14:

Add: If the TOE provides further functions or services to the Smartcard Embedded Software (such as cryptographic functions) this may result in having additional security objectives in the Security Target. Add further security objectives in the Security Target if this Protection Profile is augmented for instance using the document *Smartcard Integrated Circuit Platform Augmentations* [3].

# 4.2 Security Objectives for Environment

#### Phase 1

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

OE.Plat-Appl Usage of Hardware Platform

To ensure that the TOE is used in a secure manner the Smartcard Embedded Software shall be designed so that the requirements from the following documents are met: (i) hardware data sheet for the TOE, (ii) TOE application notes, and (iii) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.

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 unauthorised users or processes when communicating with a terminal.

Version 1.0 (July 2001) Page 37 (of 100)

## Phase 2 up to TOE Delivery

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 2.1) 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 authorised 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 paragraph 79 (page 22).

# **TOE** Delivery up to the end of Phase 6

124 Appropriate "Protection during Packaging, Finishing and Personalisation (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 Personalisation

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 unauthorised use).

This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 2.1) must be protected appropriately. For a preliminary list of assets to be protected refer to paragraph 80 (page 22).

Version 1.0 (July 2001) Page 38 (of 100)

# 5 IT Security Requirements

This chapter *IT Security Requirements* contains the following sections:

TOE Security Requirements (5.1)

TOE Functional Requirements (5.1.1)

TOE Assurance Requirements (5.1.2)

Refinements of the TOE Assurance Requirements (5.1.3)

Security Requirements for the Environment (5.2)

Note that Section 5.1.3 is not mandatory according to the Common Criteria. The *Refinements of the TOE Assurance Requirements* take into account the peculiarities of the smartcard development and production process (card's life-cycle).

# 5.1 TOE Security Requirements

# **5.1.1 TOE Functional Requirements**

- In order to define the Security Functional Requirements the Part 2 of the Common Criteria was used. However, some Security Functional Requirements have been newly created and are not taken from Part 2 of the Common Criteria. Therefore, this Protection Profile is characterised by "Part 2 extended".
- 127 The standard Security Functional Requirements are shown in Figure 12. These security functional components are listed and explained below.

Version 1.0 (July 2001) Page 39 (of 100)

## Standard SFRs which

- protect User Data and
- also support the other SFRs

#### **Malfunctions**

Limited fault tolerance (FRU\_FLT.2)

Failure with preservation of secure state (FPT\_FLS.1)

Domain separation (FPT\_SEP.1)

#### Leakage

Basic internal transfer protection (FDP\_ITT.1) Basic internal TSF data transfer protection (FPT\_ITT.1) Subset information flow control (FDP\_IFC.1)

Physical Manipulation and Probing

Resistance to physical attack (FPT\_PHP.3)

## Standard SFRs which

- support the TOE's life-cycle
- and prevent abuse of functions

#### **Abuse of Functionality**

Limited capabilities (FMT\_LIM.1)

Limited availability (FMT\_LIM.2)

#### Identification

Audit storage (FAU\_SAS.1)

Figure 12: Standard Security Functional Requirements

The Security Functional Requirements related to Specific Functionality are shown in Figure 13. These security functional components are listed and explained below.

# SFRs related to Specific Funtionality

## **Random Numbers**

Quality metric for random numbers (FCS\_RND.1)

left for functional requirements due to an augmentation in the Security Target

Figure 13: Security Functional Requirements related to Specific Functionality

Version 1.0 (July 2001) Page 40 (of 100)

Application Note 15:

Revise: If the TOE provides further functions or services to the Smartcard Embedded Software (such as cryptographic functions) this would result in having additional Security Functional Requirements in the Security Target. Examples are given in the document *Smartcard Integrated Circuit Platform Augmentations* [3].

#### **Malfunctions**

There are different ranges of operating conditions such as supply voltage, external frequency and temperature. The TOE can be operated within the limits visualised as the inner dashed rounded rectangle in Figure 14 and must operate correctly there. The limits have been reduced to ensure correct operation. This is visualised by the outer dotted rounded rectangle in the figure.

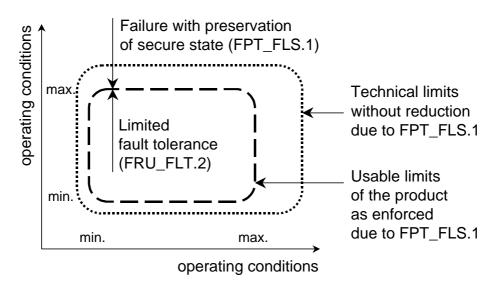


Figure 14: Paradigm regarding Operating Conditions

- Figure 14 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 visualised by the inner dashed rounded rectangle in Figure 14 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 14) 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

Version 1.0 (July 2001) Page 41 (of 100)

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.
- 134 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) 5.

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.

Version 1.0 (July 2001) Page 42 (of 100)

<sup>&</sup>lt;sup>5</sup> [assignment: list of type of failures]

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 6.

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.

Application Note 16: The Common Criteria suggest that the TOE generates audit data for the

security functional requirements Limited fault tolerance (FRU\_FLT.2) and Failure with preservation of secure state (FPT\_FLS.1). This may be advantageous or even required for the application context. The author of the

Security Target should consider this especially for FPT FLS.1.

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.

Version 1.0 (July 2001) Page 43 (of 100)

<sup>6 [</sup>assignment: list of types of failures in the TSF]

## **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 Section 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 Initialisation Data and/or Pre-personalisation Data and of supplements of the Smartcard Embedded Software as described in Section 8.1.1. After TOE Delivery the identification data (injected as part of the Initialisation Data) and the Pre-personalisation 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.
- Application Note 17: Revise: If the TOE provides specific functions to protect these data or to process them, appropriate security functional requirements can be specified in the Security Target. Then the above paragraph needs to be revised in addition.
- The TOE shall prevent functions (provided by the IC Dedicated Test Software or 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 IC Dedicated Test Software and/or 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 Section 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 a specification of requirements.
- The TOE is tested after production in Phase 3 (refer to Section 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 Protection Profile regarding testing.

Version 1.0 (July 2001) Page 44 (of 100)

- The implementation of the Test Features must be analysed to ascertain the existence and exploitability of vulnerabilities. This is subject to the Vulnerability Assessment (AVA). All necessary information about the Test Features (including the IC Dedicated Software) must be provided for Vulnerability Assessment (AVA). For further information of how to handle the Test Features refer to Section 5.1.3.
- 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.

Dependencies: FMT\_LIM.2 Limited availability.

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.

Dependencies: FMT\_LIM.1 Limited capabilities.

Version 1.0 (July 2001) Page 45 (of 100)

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.

FAU SAS.1.1 The TSF shall provide test personnel before TOE Delivery<sup>7</sup>

with the capability to store the Initialisation Data and/or Prepersonalisation Data and/or supplements of the Smartcard

Embedded Software 8 in the audit records.

Dependencies: No dependencies.

# **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. Refer to paragraph 69 (on page 20) for further explanations.
- 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.3.9

Version 1.0 (July 2001) Page 46 (of 100)

<sup>&</sup>lt;sup>7</sup> [assignment: authorised users]

<sup>8 [</sup>assignment: list of audit information]

This must be evaluated for the final smartcard product.

The TOE shall meet the requirement "Resistance to physical attack (FPT\_PHP.3)" as 150 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  $^{10}$  to the TSF  $^{11}$  by responding automatically such that

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.

## Leakage

151 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 Section 8.3.

152 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.

Version 1.0 (July 2001) Page 47 (of 100)

<sup>[</sup>assignment: physical tampering scenarios]

<sup>[</sup>assignment: list of TSF devices/elements]

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* <sup>12</sup> to prevent

the *disclosure*<sup>13</sup> 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.

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

FPT\_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT\_ITT.1.1 The TSF shall protect TSF data from disclosure 14 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.

Version 1.0 (July 2001) Page 48 (of 100)

<sup>&</sup>lt;sup>12</sup> [assignment: access control SFP(s) and/or information flow control SFP(s)]

<sup>&</sup>lt;sup>13</sup> [selection: disclosure, modification, loss of use]

<sup>&</sup>lt;sup>14</sup> [selection: disclosure, modification]

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 15 on all

confidential data when they are processed or transferred by the

TOE or by the Smartcard Embedded Software <sup>16</sup>.

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.

## **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 chapter 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 Section 5.1.3.

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 [assignment: a defined quality metric].

Dependencies: No dependencies.

Version 1.0 (July 2001) Page 49 (of 100)

<sup>&</sup>lt;sup>15</sup> [assignment: information flow control SFP]

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

#### **5.1.2 TOE Assurance Requirements**

159 The Security Target to be developed based upon this Protection Profile will be evaluated according to

Security Target evaluation (Class ASE)

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

Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

ADV IMP.2, ALC DVS.2, AVA MSU.3, and AVA VLA.4.

161 The assurance requirements are:

Development activities (Class ADV)

Functional Specification (Component ADV\_FSP.2)

Security Policy Modelling (Component ADV\_SPM.1)

High-Level Design (Component ADV\_HLD.2)

Low-Level Design (Component ADV\_LLD.1)

Implementation Representation (Component ADV\_IMP.2)

Representation Correspondence (Component ADV\_RCR.1)

Tests activities (Class ATE)

Coverage (Component ATE\_COV.2)

Depth (Component ATE\_DPT.1)

Functional Tests (Component ATE\_FUN.1)

Independent Testing (Component ATE\_IND.2)

Delivery and operation activities (Class ADO)

Delivery (Component ADO\_DEL.2)

Installation, generation, and start-up (Component ADO\_IGS.1)

Guidance documents activities (Class AGD)

Administrator Guidance (Component AGD\_ADM.1)

User guidance (Component AGD USR.1)

Configuration management activities (Class ACM)

CM automation (Component ACM\_AUT.1)

CM Capabilities (Component ACM CAP.4)

CM Scope (Component ACM\_SCP.2)

Life cycle support activities (Class ALC)

Development Security (Component ALC DVS.2)

Life Cycle Definition (Component ALC LCD.1)

Tools and Techniques (Component ALC\_TAT.1)

Version 1.0 (July 2001) Page 50 (of 100)

Vulnerability assessment activities (Class AVA)

Misuse (Component AVA\_MSU.3)

Strength of TOE Security Functions (Component AVA\_SOF.1)

Vulnerability Analysis (Component AVA\_VLA.4)

Application Note 18:

This Protection Profile requires EAL4 augmented but allows to add higher hierarchical components. To support this most parts of the Protection Profile are, whenever possible, formulated independently from possible augmentations (for instance those to reach EAL5 augmented): Therefore, this Protection Profile often refers to "the Common Criteria assurance component of the family XY" instead of referring to the specific components listed above. If the Security Target uses further augmentations this must be identified in this section (and possibly in Section 1.3). The authors of the Security Target shall also review the rationale of this Protection Profile and extend it as appropriate.

The minimum strength of security functions for the TOE is SOF-high (Strength of Functions High).

# 5.1.3 Refinements of the TOE Assurance Requirements

The following refinements shall support the comparability of evaluations according to this Protection Profile. Other standards as those issued for a specific certification scheme may not be replaced.

Refinements regarding Delivery (ADO\_DEL)

Refinements regarding Development Security (ALC\_DVS)

Refinement regarding CM scope (ACM\_SCP)

Refinement regarding CM capabilities (ACM\_CAP)

Refinements regarding Functional Specification (ADV\_FSP)

Refinement regarding Test Coverage (ATE\_COV)

Refinement regarding Installation, Generation and Start-up (ADO\_IGS)

Refinement regarding User Guidance (AGD\_USR)

Refinement regarding Administrator Guidance (AGD\_ADM)

Additional Guidance regarding Vulnerability Analysis (AVA\_VLA)" and Strength of Functions (AVA\_SOF)

Application Note 19:

The refinements as defined below may also be applicable to a hierarchically higher assurance component of the specific family. If a Security Target includes an additional augmentation, the author of the Security Target has to examine that the refinements as defined below are still applicable.

Version 1.0 (July 2001) Page 51 (of 100)

# 5.1.3.1 Refinements regarding Delivery (ADO\_DEL)

#### Introduction

- The Common Criteria assurance component of the family ADO\_DEL (delivery) refer to the delivery of (i) the TOE or parts of it (ii) to the user or user's site. The Common Criteria assurance component ADO\_DEL.2 requires procedures and technical measures to detect modifications.
- In the particular case of a Smartcard Integrated Circuit more "material and information" than the TOE itself (which by definition includes the necessary guidance) is exchanged with "users". Therefore, considering the definition of the Common Criteria (refer to Paragraph 20, page 10) the following refinement is made regarding the items "TOE" and "to the user or user's site":
- The following text reflects the requirements of the selected component ADO\_DEL.2:

Developer action elements:

ADO\_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO\_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO\_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO\_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the <u>developer's</u> master copy and the version received at the user site.

ADO\_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

#### Evaluator action elements:

ADO\_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Version 1.0 (July 2001) Page 52 (of 100)

#### Refinement

- For delivery "to the user" or "the user's site", all the external interfaces of the TOE Manufacturer have to be taken into account. These are:
  - the interface with the Smartcard Embedded Software Developer (Phase 1) where information about the smartcard integrated circuit, development software and/or tools for software development, IC pre-personalisation requirements, the Smartcard Embedded Software and possible information about mask options are exchanged and
  - the interface with the Phase after TOE Delivery (Phase 4 or 5) where prepersonalisation data, information about tests, and the product in form of wafers, sawn wafers (dice) or modules are exchanged.
- All assets identified in Section 3.1 and additionally described in 8.1.2 (if being exchanged) have to be taken into account in order to avoid any tampering with the actual version or substitution of a false version (including unauthorised modification or replacement) as specified in the Common Criteria.

# 5.1.3.2 Refinements regarding Development Security (ALC\_DVS)

#### Introduction

- The Common Criteria assurance component of the family ALC\_DVS refer (i) to "development environment", (ii) to the "TOE" or "TOE design and implementation". The component ALC\_DVS.2 requires additional evidence for the sufficiency of the security measures.
- In the particular case of a Smartcard Integrated Circuit the TOE is developed and produced within a complex industrial process which must especially be protected. Therefore, considering the definition of the Common Criteria (refer to Paragraph 20, page 10) the following refinement is made regarding the items "development environment", "TOE" or "TOE design and implementation" and the confirmation of the application of the security measures:
- 171 The following text reflects the requirements of the selected component ALC DVS.2:

Developer action elements:

ALC\_DVS.2.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC\_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of

Version 1.0 (July 2001) Page 53 (of 100)

the <u>TOE design and implementation</u> in its <u>development environment</u>.

ALC\_DVS.2.2C The development security documentation shall provide evidence that these security measures are followed during the

development and maintenance of the TOE.

ALC\_DVS.2.3C The evidence shall justify that the security measures provide

the necessary level of protection to maintain the confidentiality

and integrity of the TOE.

## Evaluator action elements:

ALC\_DVS.2.1E The evaluator shall confirm that the information provided meets

all requirements for content and presentation of evidence.

ALC\_DVS.2.2E The evaluator shall confirm that the security measures are

being applied.

## Refinement

- The "development environment" as referred to in the Common Criteria covers both, the development (Phase 2) and the production (at least Phase 3) of the TOE. The scope of the requirement of "Development Security (ALC\_DVS)" pertains to the Phase 2 up to TOE Delivery. These phases are under the control of the TOE Manufacturer.
- The IC Designer or IC Manufacturer is responsible to guarantee confidentiality and authenticity on the interface within Phase 3 where the necessary part of the smartcard IC database is delivered to the IC Mask Manufacturer and the IC photomasks are received by the IC manufacturer.
- Mask manufacturing is covered by this Protection Profile and considered under the Common Criteria assurance component of the family ALC\_DVS (development security) since the manufacturer of the TOE can not delegate any responsibility here. The certification body has to decide on a case by case decision how to handle this if the mask manufacturing is outsourced.
- "TOE design and implementation" must be understood as comprising all material and information related to the development and production of the TOE. Therefore, all assets identified in Section 3.1 and 8.1.2 (referred to as information and material in the following paragraphs) have to be taken into account in order to ensure confidentiality and integrity (including unauthorised disclosure, unauthorised modification or replacement and theft) as specified in the Common Criteria.
- The evaluator action includes assessment of all sites being involved in the development and production of the product. Sometimes standard cells (such as standard gates, standard memories) are used for the TOE as well as in other products. The corresponding items are produced and/or processed (also) in other sites where not all requirements may be applicable for practical reasons. For those

Version 1.0 (July 2001) Page 54 (of 100)

- assets, the certification body has to decide on a case by case decision how to handle these assets within a specific evaluation.
- 177 Whenever material and information is given to external partners (such as the developer of the Smartcard Embedded Software) the latter must be obliged by an Non Disclosure Agreement to treat the material and information as it is required for the TOE Manufacturer.

#### Guidance

- Additionally, the following guidance is given, in order to fulfil the requirements of the Common Criteria assurance family ALC\_DVS. There are restrictions resulting from the nature of the material and information. But in addition there are general requirements for the organisation of an industrial complex like a semiconductor manufacturer.
- All sensitive information and material shall be forwarded on a need-to-know basis. To guarantee the confidentiality of information each department must have a clear interface to other departments or partners. It must be ensured that the material and information being exchanged is limited to what is absolutely needed by the other partner to do the work he is responsible for.
- Roles and responsibilities of departments and teams shall be well-defined. This includes the content and the extent of the work to be done. Responsibilities and competence of individuals (including managers) shall be defined. All departments should consider that they contribute to develop and produce a security product.
- Defined procedures must be adhered to and their significance has to be understood by the personnel. The process procedures shall especially define requirement for secure communication and distribution of data, documents and material between the different development and production departments and to external companies and their departments the chip manufacturer works with. Confidentiality and integrity of data have to be preserved during the whole developing and manufacturing cycle.
- The hardware design department shall provide sufficient information to the department developing the IC Dedicated Software regarding inherent hardware security mechanisms in order to allow the latter to appropriately use the hardware. On the other hand this information shall be limited as far as possible.
- All sensitive information and material must be stored in a secure way to ensure confidentiality and to avert unauthorised access. Appropriate measures for physical protection include but are not limited to admittance control, airlock, fences, camera supervision, locked doors and windows, safes, locked cupboards, alarm systems, burglary proof buildings. Appropriate measures to protect data files include but are not limited to logon procedures, access control, encryption, firewall systems, isolation of computers and local networks, audit and accountability.
- Appropriate procedures and means for the disposal and destruction of wafers, dies and chips failed during the performed tests have to be provided in co-ordination with

Version 1.0 (July 2001) Page 55 (of 100)

the requirements for traceability (refer to the sub-section "Refinement regarding 'Configuration Management (ACM)").

Whenever material and information is given to external partners (such as the developer of the Smartcard Embedded Software) the latter must be obliged by an Non Disclosure Agreement to treat the material and information as it is required for the TOF Manufacturer.

# 5.1.3.3 Refinement regarding CM scope (ACM\_SCP)

#### Introduction

- The Common Criteria assurance component of the family ACM\_SCP (CM scope) refers to the tracking of specific configuration items within the developers configuration management system.
- In the particular case of a Smartcard Integrated Circuit it is helpful to clarify the scope of the configuration item "TOE implementation representation":
- The following text reflects the requirements of the selected component ACM\_SCP.2:

Developer action elements:

ACM SCP.2.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM\_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the <u>TOE implementation representation</u>, design documentation, test documentation, user documentation, administrator documentation, and CM documentation, and security flaws.

ACM\_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

ACM\_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Version 1.0 (July 2001) Page 56 (of 100)

#### Refinement

- The "TOE implementation representation" within the scope of the CM shall include at least:
  - logical design data,
  - physical design data,
  - IC Dedicated Software,
  - Smartcard Embedded Software,
  - final physical design data necessary to produce the photomasks, and
  - photomasks.

# 5.1.3.4 Refinement regarding CM capabilities (ACM\_CAP)

#### Introduction

- 190 The Common Criteria assurance component of the family ACM\_CAP (CM capabilities) refers to the capabilities of a CM system. The component ACM\_CAP.4 refers to "configuration items" and "configuration list" and uses the term "TOE" in addition.
- In the particular case of a Smartcard Integrated Circuit the scope of "configuration items" and the meaning of "TOE" in this context need to be clarified:
- 192 The following text reflects the requirements of the selected component ACM\_CAP.4:

Developer action elements:

ACM_CAP.4.1D	The developer shall provide a reference for the <u>TOE</u> .

ACM\_CAP.4.2D The developer shall use a CM system.

ACM\_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM\_CAP.4.1C The reference for the <u>TOE</u> shall be unique to each version of the TOE.

ACM\_CAP.4.2C The TOE shall be labelled with its reference.

ACM\_CAP.4.3C The CM documentation shall include a <u>configuration list</u>, a CM plan, and an acceptance plan.

Version 1.0 (July 2001) Page 57 (of 100)

ACM_CAP.4.4C	The configuration list shall describe the $\underline{\text{configuration items}}$ that comprise the $\underline{\text{TOE}}.$
ACM_CAP.4.5C	The CM documentation shall describe the method used to uniquely identify the <u>configuration items</u> .
ACM_CAP.4.6C	The CM system shall uniquely identify all configuration items.
ACM_CAP.4.7C	The CM plan shall describe how the CM system is used.
ACM_CAP.4.8C	The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.4.9C	The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.4.10C	The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.4.11C	The CM system shall support the generation of the <u>TOE</u> .
ACM_CAP.4.12C	The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the <u>TOE</u> .

#### Evaluator action elements:

ACM\_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### Refinement

- 193 "configuration items" comprise all items defined and refined under ACM\_SCP (see above) to be tracked under CM.
- The item "Smartcard Embedded Software" is only relevant for the configuration list as far as the TOE manufacturer can control it since the Smartcard Embedded Software is developed by another company and not part of the TOE though delivered together with it.
- 195 If specific requirements are not applicable for standard cells (such as standard gates, standard memories) being also used in other products, the certification body has to decide on a case by case decision how to handle them within the evaluation.
- A production control system has to be applied to guarantee the traceability and completeness of different production charges or lots. The number of wafers, dies and chips must be tracked by this system. Appropriate administration procedures have to be provided for managing wafers, dies or complete chips, which are being removed from the production-process in order to verify and to control predefined quality standards and production parameters. It has to be controlled that these wafers or

Version 1.0 (July 2001) Page 58 (of 100)

dies are returned to the same production stage from which they are taken; otherwise they have to be destroyed.

# 5.1.3.5 Refinements regarding Functional Specification (ADV\_FSP)

#### Introduction

- 197 The Common Criteria assurance component of the family ADV\_FSP (functional specification) refer to the user-visible interface and behaviour of the TSF. It is an instantiation of the TOE security functional requirements. The functional specification has to show that all the TOE security functional requirements are addressed. It is a basis for the Test Coverage Analysis.
- In the particular case of a Smartcard Integrated Circuit specific design measures, which are non-functional in nature, provide security and additionally, a test tool is delivered to the user as a part of the TOE. Therefore, refinements are provided.
- The following text reflects the requirements of the selected component ADV\_FSP.2:

Developer action elements:

ADV\_FSP.2.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.2.1C	The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.2.2C	The functional specification shall be internally consistent.
ADV_FSP.2.3C	The functional specification shall describe the <u>purpose and</u> <u>method of use of all external TSF interfaces</u> , providing complete details of all effects, exceptions and error messages.
ADV_FSP.2.4C	The functional specification shall <u>completely represent the TSF</u> .
ADV_FSP.2.5C	The functional specification shall include <u>rationale that the TSF</u> <u>is completely represented</u> .

## Evaluator action elements:

ADV_FSP.2.1E	The evaluator shall confirm that the information provided meets
	all requirements for content and presentation of evidence.

ADV\_FSP.2.2E The evaluator shall determine that the functional specification is an <u>accurate and complete instantiation of the TOE security functional requirements</u>.

Version 1.0 (July 2001) Page 59 (of 100)

#### Refinement

- The Functional Specification is expected also to specify the operating conditions of the TOE. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature.
- The Functional Specification is expected to refer to measures against physical attacks in a more general way only, but detailed enough to be able to support Test Coverage Analysis also for those measures where inspection of the layout is of relevance.
- Although the IC Dedicated Test Software is a part of the TOE, the test functions of the IC Dedicated Test Software are not described in the Functional Specification because the IC Dedicated Test Software is considered as a test tool delivered with the TOE but not providing security functions for the operational phase of the TOE.
- All functions and mechanisms which control access to the functions provided by the IC Dedicated Test Software (refer to the security functional requirement Limited availability (FMT\_LIM.2)) must at least be referred to within the Functional Specification. Details can be given in the document for "Installation, Generation and Start-up (ADO\_IGS)", refer to Section 5.1.3.7. In addition, all these functions and mechanisms must subsequently be refined according to all relevant requirements of the Common Criteria assurance class ADV because these functions and mechanisms are active after TOE Delivery and need to be part of the assurance aspects Tests (class ATE) and Vulnerability Assessment (class AVA). Therefore, all necessary information must be provided to allow tests and vulnerability assessment.

## 5.1.3.6 Refinement regarding Test Coverage (ATE\_COV)

## Introduction

- The Common Criteria assurance component of the family ATE\_COV (test coverage) "addresses the extent to which the TSF is tested, and whether or not the testing is sufficiently extensive to demonstrate that the TSF operates as specified."
- The following text reflects the requirements of the selected component ATE\_COV.2:

Developer action elements:

ATE\_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE\_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Version 1.0 (July 2001) Page 60 (of 100)

ATE COV.2.2C

The analysis of the test <u>coverage</u> shall demonstrate that the correspondence between the TSF as described in the functional specification and the <u>tests identified in the test</u> documentation is complete.

#### Evaluator action elements:

ATE COV.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### Refinement

- The TOE must be tested under different operating conditions (at least) within the specified ranges. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature. This means that "Limited fault tolerance (FRU\_FLT.2)" must be proven for all TSF (including the TOE's random number generator, refer to the functional requirement FCS\_RND.1). The tests must also cover functions which may be affected by "ageing" (such as E<sup>2</sup>PROM writing).
- The existence and effectiveness of measures against physical attacks (as specified by the functional requirement FPT\_PHP.3) can not be tested in a straightforward way. Instead the TOE Manufacturer shall provide evidence that the TOE actually has the particular physical characteristics (especially layout design principles). This can be done by checking the layout (implementation or actual integrated circuit) in an appropriate way. The required evidence pertains to the existence of measures against physical attacks (unless being obvious) but will cover only a subset of the characteristics against physical attacks.
- The IC Dedicated Test Software is seen as a "test tool" being delivered as part of the TOE. However, the Test Features do not provide security functions and are not used after TOE Delivery. Therefore, Test Features need not to be covered by the Test Coverage Analysis but all functions and mechanisms which control access to the functions provided by the IC Dedicated Test Software must be part of the Test Coverage Analysis.

## 5.1.3.7 Refinement regarding Installation, Generation and Start-up (ADO\_IGS)

#### Introduction

- The life-cycle model to be described under the Common Criteria assurance component of the family ALC\_LCD refers to organisational and procedural controls such as design methods, review procedures, project management controls, change control procedures, test methods and acceptance procedures. TOE configuration and administration is subject to the Common Criteria assurance component of the families ADO\_IGS and AGD\_ADM.
- The requirements of the Common Criteria assurance family ADO\_IGS "call for a secure transition from the TOE's implementation representation being under

Version 1.0 (July 2001) Page 61 (of 100)

configuration control to its initial operation in the user environment." "The requirements in this assurance family are presented separately from those in the AGD\_ADM family, due to the infrequent, possibly one-time use of the installation, generation and start-up procedures."

- Though the TOE is not delivered and then configured, its configuration needs to be addressed as a specific aspect since these procedures may affect the overall security. Therefore, the terms "installation" and "generation" need to be refined:
- The following text reflects the requirements of the selected component ADO\_IGS.1:

Developer action elements:

ADO\_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO\_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO\_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO\_IGS.1.2E The evaluator shall determine that the <u>installation</u>, <u>generation</u>, and start-up procedures result in a secure configuration.

## Refinement

- The TOE may be configured after production before the Smartcard is delivered to the end-user (this would be addressed by security functional requirement Limited availability (FMT\_LIM.2)). In this case, these configuration aspects have to be considered. Differences between the TOE before first use (normally done during wafer test) and Phase 7 must be summarised. Guidance to change that behaviour must exist. Regarding technical details, the documentation provided by the developer can refer to documents provided for the Common Criteria class ADV.
- Note that most of the security functions will already be effective before TOE Delivery. However, guidance to determine the behaviour of Security Functions, to disable, to enable or to modify the behaviour of Security Functions must be given as follows:
  - If configuration of a Security Function of the TOE done before TOE Delivery (that means by the TOE Manufacturer) the corresponding guidance is given under the assurance component of the family ADO\_IGS. Note that this document is an internal document of the TOE Manufacturer and not delivered to their customers.
  - If administration of a Security Function of the TOE is done after TOE Delivery (that means by the Card Manufacturer) the corresponding guidance must be in the Administrator Guidance (refer to the Common Criteria assurance component

Version 1.0 (July 2001) Page 62 (of 100)

of the family AGD\_ADM) as it shall describe how to administer the TOE in a secure manner. This guidance document is delivered by the TOE Manufacturer.

Guidance documents must not contain security relevant details which are not absolutely necessary for the administration actually to be done.

## 5.1.3.8 Refinement regarding User Guidance (AGD\_USR)

## Introduction

- The Common Criteria assurance components of the families AGD\_USR (user guidance) and AGD\_ADM (administrator guidance) "describe all relevant aspects for the secure application of the TOE." The terms "user" and "administrator" are used.
- In the case of a Smartcard Integrated Circuit the meaning of the terms "user" and "administrator" are not obvious. Therefore, the following refinements are given regarding guidance.
- User guidance refers to material that is intended to be used by non-administrative human users of the TOE, and by others (e.g. programmers) using the TOE's external interfaces. User guidance describes the security functions provided by the TSF and provides instructions and guidelines, including warnings, for its secure use.
- 219 The following text reflects specific requirements of the selected component AGD\_USR.1:

Developer action elements:

AGD\_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C	The user guidance shall describe the functions and interfaces
	available to the non-administrative <u>users of the TOE</u> .

- AGD\_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.
- AGD\_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
- AGD\_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

Version 1.0 (July 2001) Page 63 (of 100)

AGD\_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD\_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD\_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

#### Refinement

- 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.
  - User Guidance (refer to the Common Criteria assurance component of the family AGD\_USR) must be given to the developer of the Smartcard Embedded Software to ensure that the Smartcard Embedded Software properly uses the TOE.
- 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 Guidance (refer to the Common Criteria assurance component of the family AGD\_USR) must be given to the developer of the terminal. However, this is only little information about the physical characteristics of the device, the ISO interface and perhaps standard protocols (such as T=1 if implemented in the TOE). Other information could be needed if the TOE provides other services in the end-user phase (Phase 7, refer to Section 8.1) which may be augmented to this Protection Profile.
- The User Guidance documents should provide only the information which is necessary for using the TOE. Depending on the recipient of that guidance documentation User and Administrator Guidance can be given in the same document.
- After production the TOE is tested where communication is performed by directly contacting the pads that mostly become part of the ISO interface during packaging. Here no guidance document according to Common Criteria class AGD is required (provided that the tests are performed by the TOE Manufacturer). Note that test procedures are described under the Common Criteria assurance component of the family ATE FUN.

Version 1.0 (July 2001) Page 64 (of 100)

# 5.1.3.9 Refinement regarding Administrator Guidance (AGD\_ADM)

#### Introduction

- Administrator guidance refers to written material that is intended to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security.
- The following text reflects specific requirements of the selected component AGD\_ADM.1:

Developer action elements:

AGD\_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

- AGD\_ADM.1.1C The administrator guidance shall describe the <u>administrative</u> functions and interfaces available to the administrator of the TOE.
- AGD\_ADM.1.2C The administrator guidance shall <u>describe how to administer</u> the TOE in a secure manner.
- AGD\_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
- AGD\_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
- AGD\_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
- AGD\_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
- AGD\_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.
- AGD\_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Version 1.0 (July 2001) Page 65 (of 100)

#### Evaluator action elements:

AGD\_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

## Refinement

- 226 If the TOE provides security functions which can or need to be administrated (i) by the Smartcard Embedded Software or (ii) using services of the TOE after TOE Delivery (refer to Section 2.1) an Administrator Guidance must be given in addition.
- 227 Most of the security functions will already be effective before TOE Delivery. However, guidance to determine the behaviour of Security Functions, to disable, to enable or to modify the behaviour of Security Functions must be given if administration of a Security Function is done after TOE Delivery (that means by the Card Manufacturer). This guidance document is delivered by the TOE Manufacturer.
- Guidance documents must not contain security relevant details which are not absolutely necessary for the administration actually to be done. Depending on the recipient of that guidance documentation User and Administrator Guidance can be given in the same document.

# 5.1.3.10 Additional Guidance regarding Vulnerability Analysis (AVA\_VLA)" and Strength of Functions (AVA\_SOF)

- When rating attack potential according to the Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology [8] for the assurance aspects Vulnerability Analysis and Strength of Functions, as expertise of an attacker it is distinguished between "expert", "proficient" and "laymen". With respect to the knowledge of the TOE it is distinguished between "no information about the TOE", "public information concerning the TOE", and "sensitive information about the TOE". The information gained from a user guide is given as an example for public information concerning the TOE. This is not applicable here since the protection of such information is demanded according to this Protection Profile (refer to refinement regarding "Development Security (ALC\_DVS)").
- During the Vulnerability Analysis it must be assessed that the functions provided by the IC Dedicated Test Software can not be abused after TOE Delivery (refer to the security functional requirements FMT\_LIM.1 and FMT\_LIM.2). All necessary information must be provided to allow that assessment.

Version 1.0 (July 2001) Page 66 (of 100)

## **5.2 Security Requirements for the Environment**

## **5.2.1 Security Requirements for the IT-Environment**

The security objectives for the environment will be ensured by Non-IT security requirements only (refer to the next subsection, Section 5.2.2, and the rationale, Section 7.2).

# 5.2.2 Security Requirements for the Non-IT-Environment

- 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 Personalisation (Phases after TOE Delivery up to Phase 7).
- The Smartcard Embedded Software is developed in Phase 1 and must support the security functionality of the TOE. This Protection Profile 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) hardware data sheet for the TOE, (ii) TOE application notes, and (iii) 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.<sup>17</sup>

The requirement RE.Phase-1 also addresses the fact that the Smartcard Embedded Software may need to support the security functions of the TOE (refer also to Figure 3 on page 14). Examples for such security functional requirements for the Smartcard Embedded Software are given in Section 8.2.2.

Version 1.0 (July 2001) Page 67 (of 100)

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.

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 Personalisation

The Card Manufacturer (after TOE Delivery up to the end of 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 unauthorised use).

# 6 PP Application Notes

- In this Protection Profile operations are completed for all security functional components except the component FCS\_RND.1 (Quality metric for random numbers). To complete the latter is left to the Security Target.
- This Protection Profile contains other application notes distributed through the paper. The application notes are separated paragraphs which are marked with "Application Note" following a number.

## 7 Rationale

This chapter *Rationale* contains the following sections:

Security Objectives Rationale (7.1)

Security Requirements Rationale (7.2)

Rationale for the security functional requirements (7.2.1)

Dependencies of security functional requirements (7.2.2)

Rationale for the Assurance Requirements and the Strength of Function Level (7.2.3)

Security Requirements are Mutually Supportive and Internally Consistent (7.3)

Version 1.0 (July 2001) Page 68 (of 100)

## 7.1 Security Objectives Rationale

Table 1 below gives an overview, how the assumptions, threats, and organisational security policies are addressed by the objectives. The text following after the table justifies this in detail.

Assumption, Threat or Organisational Security Policy	Security Objective	Note
A.Plat-Appl	OE.Plat-Appl	(Phase 1)
A.Resp-Appl	OE.Resp-Appl	(Phase 1)
P.Process-TOE	OE.Process-TOE	(Phase 2 – 3)
	O.Identification	
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	

Table 1: Security Objectives versus Assumptions, Threats or Policies

- 239 The justification related to the assumption "Usage of Hardware Platform (A.Plat-Appl)" is as follows:
- 240 Since OE.Plat-Appl requires the Smartcard Embedded Software developer to implement those measures assumed in A.Plat-Appl, the assumption is covered by the objective.
- The justification related to the assumption "Treatment of User Data (A.Resp-Appl)" is as follows:
- 242 Since OE.Resp-Appl requires the developer of the Smartcard Embedded Software to implement measures as assumed in A.Resp-Appl, the assumption is covered by the objective.
- The justification related to the organisational security policy "Protection during TOE Development and Production (P.Process-TOE)" is as follows:
- OE.Process-TOE requires the TOE Manufacturer to implement those measures assumed in P.Process-TOE. Therefore, the organisational security policy is covered by this objective, as far as organisational measures are concerned. The only issue not completely covered by these measures is the fact that the TOE has to support the

Version 1.0 (July 2001) Page 69 (of 100)

- possibility of unique identification. This is the content of O.Identification. Therefore, the organisational security policy is covered by OE.Process-Card and O.Identification.
- The justification related to the assumption "Protection during Packaging, Finishing and Personalisation (A.Process-Card)" is as follows:
- 246 Since OE.Process-Card requires the Card Manufacturer to implement those measures assumed in A.Process-Card, the assumption is covered by this objective.
- The justification related to the threats "Inherent Information Leakage (T.Leak-Inherent)", "Physical Probing (T.Phys-Probing)", "Malfunction due to Environmental Stress (T.Malfunction)", "Physical Manipulation (T.Phys-Manipulation)", "Forced Information Leakage (T.Leak-Forced)", "Abuse of Functionality (T.Abuse-Func)" and "Deficiency of Random Numbers (T.RND)" is as follows:
- For all threats the corresponding objectives (refer to Table 1) are stated in a way, which directly corresponds to the description of the threat (refer to Section 3.3). It is clear from the description of each objective (refer to Section 4.1), that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds.

# 7.2 Security Requirements Rationale

# 7.2.1 Rationale for the security functional requirements

Table 2 below gives an overview, how the security functional requirements are combined to meet the security objectives. The detailed justification follows after the table.

Version 1.0 (July 2001) Page 70 (of 100)

Objective	TOE Security Functional Requirements	Security Requirements for the environment	
O.Leak-Inherent	- FDP_ITT.1 "Basic internal transfer protection"	RE.Phase-1 "Design and Implementation of the	
	- FPT_ITT.1 "Basic internal TSF data transfer protection"	Smartcard Embedded Software"	
	- FDP_IFC.1 "Subset information flow control"		
O.Phys-Probing	- FPT_PHP.3 "Resistance to physical attack"	RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software"	
O.Malfunction	- FRU_FLT.2 "Limited fault tolerance		
	- FPT_FLS.1 "Failure with preservation of secure state"		
	- FPT_SEP.1 "TSF domain separation"		
O.Phys-Manipulation	- FPT_PHP.3 "Resistance to physical attack"	RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software" (e. g. by implementing FDP_SDI.1 Stored data integrity monitoring)	
O.Leak-Forced	All requirements listed for O.Leak-Inherent	RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software"	
	- 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		
O.Abuse-Func	- FMT_LIM.1 "Limited capabilities"		
	- FMT_LIM.2 "Limited availability"		
	plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced		

Version 1.0 (July 2001) Page 71 (of 100)

Objective	TOE Security Functional Requirements	Security Requirements for the environment	
	- 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 "Audit storage"		
O.RND	- FCS_RND.1 "Quality metric for random numbers"	RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software" (e. g. by implementing FPT_AMT.1 "Abstract machine testing")	
	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		
OE.Plat-Appl		RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software"	
OE.Resp-Appl		RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software"	
OE.Process-TOE	- FAU_SAS.1 "Audit storage"	Assurance Components:	
		refer to below .	
OE.Process-Card		RE.Process-Card possibly supported by RE.Phase-1	

Table 2: Security Requirements versus Security Objectives

- \* 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 justification related to the security objective "Protection against Inherent Information Leakage (O.Leak-Inherent)" is as follows:
- The refinements of the security functional requirements FPT\_ITT.1 and FDP\_ITT.1 together with the policy statement in FDP\_IFC.1 explicitly require the prevention of disclosure of secret data (TSF data as well as User Data) when transmitted between

Version 1.0 (July 2001) Page 72 (of 100)

- separate parts of the TOE or while being processed. This includes that attackers cannot reveal such data by measurements of emanations, power consumption or other behaviour of the TOE while data are transmitted between or processed by TOE parts.
- Of course this has also to be supported by the Smartcard Embedded Software. For example timing attacks were possible if the processing time of algorithms implemented in the software would depend on the content of secret variables. The requirement RE.Phase-1 makes sure that this is avoided.
- The justification related to the security objective "Protection against Physical Probing (O.Phys-Probing)" is as follows:
- The scenario of physical probing as described for this objective is explicitly included in the assignment chosen for the physical tampering scenarios in FPT\_PHP.3. Therefore, it is clear that this security functional requirement supports the objective.
- It is possible that the TOE needs additional support by the Smartcard Embedded Software (e. g. to send data over certain buses only with appropriate precautions). If necessary this support is provided according to RE.Phase-1. Together with this FPT\_PHP.3 is suitable to meet the objective.
- The justification related to the security objective "Protection against Malfunctions (O.Malfunction)" is as follows:
- The definition of this objective shows that it covers a situation, where malfunction of the TOE might be caused by the operating conditions of the TOE (while direct manipulation of the TOE is covered O.Phys-Manipulation). There are two possibilities in this situation: Either the operating conditions are inside of the tolerated range or at least one of them is outside of this range. The second case is covered by FPT\_FLS.1, because it states that a secure state is preserved in this case. The first case is covered by FRU\_FLT.2 because it states that the TOE operates correctly under normal (tolerated) conditions. To support this, FPT\_SEP.1 the functions implementing FRU\_FLT.2 and FPT\_FLS.1 must work independently so that their operation can not affected by the Smartcard Embedded Software (refer to the refinement). Therefore, there is no possible instance of conditions under O.Malfunction, which is not covered.
- 258 The justification related to the security objective "Protection against Physical Manipulation (O.Phys-Manipulation)" is as follows:
- The scenario of physical manipulation as described for this objective is explicitly included in the assignment chosen for the physical tampering scenarios in FPT\_PHP.3. Therefore, it is clear that this security functional requirement supports the objective.
- It is possible that the TOE needs additional support by the Embedded Software (for instance by implementing FDP\_SDI.1 to check data integrity with the help of appropriate checksums, refer to Section 8.2.2). This support is provided according to RE.Phase-1. Together with this FPT\_PHP.3 is suitable to meet the objective.

Version 1.0 (July 2001) Page 73 (of 100)

- 261 The justification related to the security objective "Protection against Forced Information Leakage (O.Leak-Forced)" is as follows:
- This objective is directed against attacks, where an attacker wants to force an information leakage, which would not occur under normal conditions. In order to achieve this the attacker has to combine a first attack step, which modifies the behaviour of the TOE (either by exposing it to extreme operating conditions or by directly manipulating it) with a second attack step measuring and analysing some output produced by the TOE. The first step is prevented by the same measures which support O.Malfunction and O.Phys-Manipulation, respectively. The requirements covering O.Leak-Inherent also support O.Leak-Forced because they prevent the attacker from being successful if he tries the second step directly.
- The justification related to the security objective "Protection against Abuse of Functionality (O.Abuse-Func)" is as follows:
- This objective states that abuse of functions (especially provided by the IC Dedicated Test Software, for instance in order to read secret data) must not be possible in Phase 7 of the life-cycle. There are two possibilities to achieve this: (i) They cannot be used by an attacker (i. e. its availability is limited) or (ii) using them would not be of relevant use for an attacker (i. e. its capabilities are limited) since the functions are designed in a specific way. The first possibility is specified by FMT\_LIM.2 and the second one by FMT\_LIM.1. Since these requirements are combined to support the policy, which is suitable to fulfil O.Abuse-Func, both security functional requirements together are suitable to meet the objective.
- Other security functional requirements which prevent attackers from circumventing the functions implementing these two security functional requirements (for instance by manipulating the hardware) also support the objective. The relevant objectives are also listed in Table 2.
- It was chosen to define FMT\_LIM.1 and FMT\_LIM.2 explicitly (not using Part 2 of the Common Criteria) for the following reason: Though taking components from the Common Criteria catalogue makes it easier to recognise functions, any selection from Part 2 of the Common Criteria would have made it harder for the reader to understand the special situation meant here. As a consequence, the statement of explicit security functional requirements was chosen to provide more clarity.
- The justification related to the security objective "TOE Identification (O.Identification)" is as follows:
- Obviously the operations for FAU\_SAS.1 are chosen in a way that they require the TOE to provide the functionality needed for O.Identification. The Initialisation Data (or parts of them) are used for TOE identification.
- It was chosen to define FAU\_SAS.1 explicitly (not using a given security functional requirement from Part 2 of the Common Criteria) for the following reason: The security functional requirement FAU\_GEN.1 in Part 2 of the CC requires the TOE to generate the audit data and gives details on the content of the audit records (for instance data and time). The possibility to use the functions in order to store security

Version 1.0 (July 2001) Page 74 (of 100)

relevant data which are generated outside of the TOE, is not covered by the family FAU\_GEN or by other families in Part 2. Moreover, the TOE cannot add time information to the records, because it has no real time clock. Therefore, the new family FAU\_SAS was defined for this situation.

- 270 The justification related to the security objective "Random Numbers (O.RND)" is as follows:
- FCS\_RND.1 requires the TOE to provide random numbers of good quality. To specify the exact metric is left to the individual Security Target for a specific TOE.
- Other security functional requirements, which prevent physical manipulation and malfunction of the TOE (see the corresponding objectives listed in the table) support this objective because they prevent attackers from manipulating or otherwise affecting the random number generator.
- 273 Random numbers are often used by the Smartcard Embedded Software to generate cryptographic keys for internal use. Therefore, the TOE must prevent the unauthorised disclosure of random numbers. Other security functional requirements which prevent inherent leakage attacks, probing and forced leakage attacks ensure the confidentiality of the random numbers provided by the TOE.
- Depending on the functionality of specific TOEs the Smartcard Embedded Software will have to support the objective by providing runtime-tests of the random number generator (for instance by implementing FPT\_AMT.1, refer to Section 8.2.2). Together, these requirements allow the TOE to provide cryptographically good random numbers and to ensure that no information about the produced random numbers is available to an attacker.
- It was chosen to define FCS\_RND.1 explicitly, because Part 2 of the Common Criteria do not contain generic security functional requirements for Random Number generation. (Note, that there are security functional requirements in Part 2 of the Common Criteria, which refer to random numbers. However, they define requirements only for the authentication context, which is only one of the possible applications of random numbers.)
- The justification related to the security objective "Usage of Hardware Platform (OE.Plat-Appl)" is as follows:
- 277 RE.Phase-1 requires the Smartcard Embedded Software developer to design and implement the software in a way, which is suitable to meet OE.Plat-Appl.
- The justification related to the security objective "Treatment of User Data (OE.Resp-Appl)" is as follows:
- 279 RE.Phase-1 requires the developer of the Smartcard Embedded Software to design and implement the software in a way, which is suitable to meet OE.Resp-Appl.

Version 1.0 (July 2001) Page 75 (of 100)

- The justification related to the security objective "Protection during TOE Development and Production (OE.Process-TOE)" is as follows:
- The objective OE.Process-TOE has mainly to be fulfilled by organisational and other measures, which the TOE Manufacturer has to implement. These measures are a subset of those measures, which are examined during the evaluation of the assurance requirements of the classes ACM, AGD, ALC and ADO. The technical capability of the TOE to store Initialisation Data and/or Pre-personalisation Data is provided according to FAU\_SAS.1. Together these security requirements are suitable to meet the objective.
- The justification related to the security objective "Protection during Packaging, Finishing and Personalisation (OE.Process-Card)" is as follows:
- RE.Process-Card requires the Card Manufacturer to use adequate measures to fulfil OE.Process-Card. Depending on the security needs of the application, the Smartcard Embedded Software may have to support this for instance by using appropriate authentication mechanisms for personalisation functions. Therefore, RE.Phase-1 may support RE.Process-Card in fulfilling the objective in addition.
- Note that there is a detailed explanation for each security functional requirement in Section 5.1.1.

## 7.2.2 Dependencies of security functional requirements

Table 3 below lists the security functional requirements defined in this Protection Profile, their dependencies and whether they are satisfied by other security requirements defined in this Protection Profile. The text following the table discusses the remaining cases.

Version 1.0 (July 2001) Page 76 (of 100)

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this PP	
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 below	
FPT_ITT.1	None	No dependency	
FCS_RND.1	None	No dependency	

Table 3: Dependencies of the Security Functional Requirements

Part 2 of the Common Criteria defines the dependency of FDP\_IFC.1 (information flow control policy statement) on FDP\_IFF.1 (Simple security attributes). The specification of FDP\_IFF.1 would not capture the nature of the security functional requirement nor add any detail. As stated in the *Data Processing Policy* referred to in FDP\_IFC.1 there are no attributes necessary. The security functional requirement for the TOE is sufficiently described using FDP\_ITT.1 and its *Data Processing Policy* (FDP\_IFC.1). Therefore the dependency is considered satisfied.

287 As Table 3 shows, all other dependencies are fulfilled by security requirements defined in this Protection Profile.

Application Note 20:

Add: Regarding the security functional requirement "Failure with preservation of secure state (FPT\_FLS.1)" the Common Criteria give the following explanation: The term "secure state" refers to a state in which the TSF data are consistent and the TSF continues correct enforcement of the TSP. The "secure state" should be defined in the TSP model (ADV\_SPM.1). The author of the Security Target should give some rationale (and a clear definition of the secure state if possible) here and add a reference to the TSP model.

The discussion in Section 7.2.1 has shown, how the security functional requirements support each other in meeting the security objectives of this Protection Profile. In particular the security functional requirements providing resistance of the hardware against manipulations (e. g. FPT\_PHP.3) support all other more specific security functional requirements (e. g. FCS\_RND.1) because they prevent an attacker from disabling or circumventing the latter. Together with the discussion of the dependencies above this shows that the security functional requirements build a mutually supportive whole.

Version 1.0 (July 2001) Page 77 (of 100)

## 7.2.3 Rationale for the Assurance Requirements and the Strength of Function Level

- The assurance level EAL4 and the augmentation with the requirements ADV\_IMP.2, ALC\_DVS.2, AVA\_MSU.3, and AVA\_VLA.4 were chosen in order to meet assurance expectations explained in the following paragraphs.
- An assurance level of EAL4 is required for this type of TOE since it is intended to defend against sophisticated attacks. This evaluation assurance level was selected since it is designed to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defence against such attacks, the evaluators should have access to the low level design and source code.

# ADV\_IMP.2 Implementation of the TSF

- This assurance component is a higher hierarchical component to EAL 4 (which only requires ADV\_IMP.1). It is important for a smartcard IC that the evaluation includes the implementation representation of the entire TSF and determines whether the functional requirements in the Security Target are addressed by the representation of the TSF. IC dedicated software source code and IC hardware drawings are examples of TSF implementation representation.
- The implementation representation is used to express the notion of the least abstract representation of the TSF, specifically the one that is used to create the TSF itself without further design refinement.
- ADV\_IMP.2 has dependencies with ADV\_LLD.1 "Descriptive Low-Level design", ADV\_RCR.1 "Informal correspondence demonstration", ALC\_TAT.1 "Well defined development tools". These assurance components are included in EAL4, then these dependencies are satisfied.

# **ALC\_DVS.2 Sufficiency of security measures**

- Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE.
- In the particular case of a Smartcard Integrated Circuit the TOE is developed and produced within a complex and distributed industrial process which must especially be protected. Details about the implementation, (e.g. from design, test and development tools as well as Initialisation Data) may make such attacks easier. Therefore, in the case of a Smartcard Integrated Circuit, maintaining the confidentiality of the design is very important.

Version 1.0 (July 2001) Page 78 (of 100)

This assurance component is a higher hierarchical component to EAL4 (which only requires ALC\_DVS.1). ALC\_DVS.2 has no dependencies.

## AVA\_MSU.3 Analysis and testing for insecure states

- The user guidance must be correct and sufficent to ensure that the TOE can be used in a secure way and that vulnerabilities are not introduced.
- This component is included to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. In this component, an analysis of the guidance documentation provided by the developer is validated and confirmed through testing by the evaluator to provide additional assurance.
- This assurance component is a higher hierarchical component to EAL4 (which only requires AVA MSU.2).
- AVA\_MSU.3 has dependencies with ADO\_IGS.1 "Installation, generation, and start-up procedures", ADV\_FSP.1 "Informal functional specification", AGD\_ADM.1 "Administrator guidance" and AGD\_USR.1 "User guidance". The dependencies are satisfied in EAL4.

#### **AVA VLA.4 Highly resistant**

- 301 Due to the intended use of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA\_VLA.4 component.
- Independent vulnerability analysis is based on highly detailed technical information and goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a high attack potential.
- AVA\_VLA.4 has dependencies with ADV\_FSP.1 "Informal functional specification", ADV\_HLD.2 "Security enforcing high-level design", ADV\_LLD.1 "Descriptive low-level design", ADV\_IMP.1 "Subset of the implementation of the TSF", AGD\_ADM.1 "Administrator Guidance", AGD\_USR.1 "User Guidance".
- 304 All these dependencies are satisfied by EAL4.
- Application Note 21: For the assurance level EAL5 augmented refer to the document Smartcard Integrated Circuit Platform Augmentations [3]. The Security Target used for the evaluation of a smartcard integrated circuit will be created by taking this Protection Profile and add additional assurance requirements for EAL5 augmented.

Version 1.0 (July 2001) Page 79 (of 100)

- It has to be assumed that attackers with high attack potential try to attack smart cards used for digital signature applications or payment systems. Therefore, specifically AVA\_VLA.4 was chosen in order to assure that even these attackers cannot successfully attack the TOE. For the same reason the Strength of Function level "SOF-high" is required.
- The assurance components in an evaluation assurance level (EAL) are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL4. Therefore, these components add additional assurance to EAL4, but the mutual support of the requirements is still guaranteed.
- Note that detailed refinements for assurance requirements are given in Section 5.1.3.

# 7.3 Security Requirements are Mutually Supportive and Internally Consistent

- The discussion of security functional requirements and assurance components in the preceding sections has shown that mutual support and consistency are given for both groups of requirements. The arguments given for the fact that the assurance components are adequate for the functionality of the TOE also shows that the security functional requirements and assurance requirements support each other and that there are no inconsistencies between these groups.
- The security functional requirement FPT\_PHP.3 makes it harder to manipulate User Data and TSF Data. This protects the primary assets identified in Section 3.1 and other security features or functions which use these data.
- Though a manipulation of the TOE (refer to FPT\_PHP.3) is not of great value for an attacker in itself, it can be an important step in order to threaten the primary assets identified in Section 3.1. Therefore, the security functional requirement FPT\_PHP.3 is not only required to meet the security objective O.Phys-Manipulation. Instead it protects other security features or functions of both the TOE and the Smartcard Embedded Software from being bypassed, deactivated or changed. In particular this may pertain to the security features or functions being specified using FDP\_ITT.1, FPT\_ITT.1, FPT\_FLS.1, FMT\_LIM.2, FCS\_RND.1, and those implemented in the Smartcard Embedded Software.
- A malfunction of TSF (refer to FRU\_FLT.2 and FPT\_FLS.1) can be an important step in order to threaten the primary assets identified in Section 3.1. Therefore, the security functional requirements FRU\_FLT.2 and FPT\_FLS.1 are not only required to meet the security objective O.Malfunction. Instead they protect other security features or functions of both the TOE and the Smartcard Embedded Software from being bypassed, deactivated or changed. In particular this pertains to the security features or functions being specified using FDP\_ITT.1, FPT\_ITT.1, FMT\_LIM.1, FMT\_LIM.2, FCS\_RND.1, and those implemented in the Smartcard Embedded Software.

Version 1.0 (July 2001) Page 80 (of 100)

- In a forced leakage attack the methods described in "Malfunction due to Environmental Stress" (refer to T.Malfunction) and/or "Physical Manipulation" (refer to T.Phys-Manipulation) are used to cause leakage from signals which normally do not contain significant information about secrets. Therefore, in order to avert the disclosure of primary assets identified in Section 3.1 it is important that the security functional requirements averting leakage (FDP\_ITT.1, FPT\_ITT.1) and those against malfunction (FRU\_FLT.2 and FPT\_FLS.1) and physical manipulation (FPT\_PHP.3) are effective and bind well. The security features and functions against malfunction ensure correct operation of other security functions (refer to above) and help to avert forced leakage themselves in other attack scenarios. The security features and functions against physical manipulation make it harder to manipulate the other security functions (refer to above).
- Physical probing (refer to FPT\_PHP.3) shall directly avert the disclosure of primary assets identified in Section 3.1. In addition, physical probing can be an important step in other attack scenarios if the corresponding security features or functions use secret data. For instance the security functional requirement FMT\_LIM.2 may use passwords. Therefore, the security functional requirement FPT\_PHP.3 (against probing) help to protect other security features or functions including those being implemented in the Smartcard Embedded Software. Details depend on the implementation.
- Leakage (refer to FDP\_ITT.1, FPT\_ITT.1) shall directly avert the disclosure of primary assets identified in Section 3.1. In addition, inherent leakage and forced leakage (refer to above) can be an important step in other attack scenarios if the corresponding security features or functions use secret data. For instance the security functional requirement FMT\_LIM.2 may use passwords. Therefore, the security functional requirements FDP\_ITT.1 and FPT\_ITT.1 help to protect other security features or functions implemented in the Smartcard Embedded Software (FDP\_ITT.1) or provided by the TOE (FPT\_ITT.1). Details depend on the implementation.
- According to the assumption Usage of Hardware Platform (A.Plat-Appl) the Smartcard Embedded Software will correctly use the functions provided by the TOE. Hereby the User Data are treated as required to meet the requirements defined for the specific application context (refer to Treatment of User Data (A.Resp-Appl)). However, the TOE may implement additional functions. This can be a risk if their interface can not completely be controlled by the Smartcard Embedded Software. Therefore, the security functional requirements FMT\_LIM.1 and FMT\_LIM.2 are very important. They ensure that appropriate control is applied to the interface of these functions (limited availability) and that these functions, if being usable, provide limited capabilities only.
- The combination of the security functional requirements FMT\_LIM.1 and FMT\_LIM.2 ensures that (especially after TOE Delivery) these additional functions can not be abused by an attacker to (i) disclose or manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or

Version 1.0 (July 2001) Page 81 (of 100)

of the Smartcard Embedded Software or (iii) to enable an attack. Hereby the binding between these two security functional requirements is very important:

- The security functional requirement Limited Capabilities (FMT\_LIM.1) must close gaps which could be left by the control being applied to the function's interface (Limited Availability (FMT\_LIM.2)). Note that the security feature or function which limits the availability can be bypassed, deactivated or changed by physical manipulation or a malfunction caused by an attacker. Therefore, if Limited Availability (FMT\_LIM.2) is vulnerable 18, it is important to limit the capabilities of the functions in order to limit the possible benefit for an attacker.
- The security functional requirement Limited Availability (FMT\_LIM.2) must close gaps which could result from the fact that the function's kernel in principle would allow to perform attacks. The TOE must limit the availability of functions which potentially provide the capability to disclose or manipulate User Data, to manipulate security features or functions of the TOE or of the Smartcard Embedded Software or to enable an attack. Therefore, if an attacker could benefit from using such functions<sup>19</sup>, it is important to limit their availability so that an attacker is not able to use them.
- No perfect solution to limit the capabilities (FMT\_LIM.1) is required if the limited availability (FMT\_LIM.2) alone can prevent the abuse of functions. No perfect solution to limit the availability (FMT\_LIM.2) is required if the limited capabilities (FMT\_LIM.1) alone can prevent the abuse of functions. Therefore, it is correct that both requirements are defined in a way that they together provide sufficient security.
- It is important to avert malfunctions of TSF and of security functions implemented in the Smartcard Embedded Software (refer to above). There are two security functional requirements which ensure that malfunctions can not be caused by exposing the TOE to environmental stress. First it must be ensured that the TOE operates correctly within some limits (Limited fault tolerance (FRU\_FLT.2)). Second the TOE must prevent its operation outside these limits (Failure with preservation of secure state (FPT\_FLS.1)). Both security functional requirements together prevent malfunctions. The two functional requirements must define the "limits". Otherwise there could be some range of operating conditions which is not covered so that malfunctions may occur. Consequently, the security functional requirements Limited fault tolerance (FRU\_FLT.2) and Failure with preservation of secure state (FPT\_FLS.1) are defined in a way that they together provide sufficient security.

Version 1.0 (July 2001) Page 82 (of 100)

or, in the extreme case, not being provided

the capabilities are not limited in a perfect way (FMT\_LIM.1)

#### 8 Annex

This chapter *Annex* contains the following sections:

Development and Production Process (life-cycle) (8.1)

Life-Cycle Description (8.1.1)

Description of Assets of the Integrated Circuits Designer/Manufacturer (8.1.2)

Security Aspects of the Smartcard Embedded Software (8.2)

Further Information regarding A.Resp-Appl (8.2.1)

Examples of Specific Functional Requirements for the Smartcard Embedded Software (8.2.2)

Examples of Attack Scenarios (8.3)

Definition of the Family FCS\_RND (8.4)

Definition of the Family FMT\_LIM (8.5)

Definition of the Family FAU\_SAS (8.6)

Glossary (8.7)

List of Abbreviations (8.8)

Note that Section 8.1 contains additional information which is used for the refinements of the standard assurance requirements (refer to Section 5.1.2) defined in the separate Section 5.1.3.

# 8.1 Development and Production Process (life-cycle)

# 8.1.1 Life-Cycle Description

322 The smartcard product life-cycle is visualised in Figure 15.

Version 1.0 (July 2001) Page 83 (of 100)

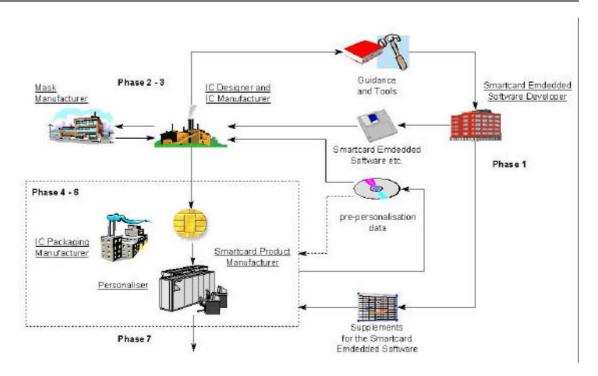


Figure 15: Smartcard Life-Cycle

323 The smartcard product life-cycle is decomposed into seven phases where the following authorities are involved:

Phase 1	Smartcard Embedded Software Development	The Smartcard Embedded Software Developer is in charge of
		<ul> <li>the smartcard embedded software development and</li> </ul>
		<ul> <li>the specification of IC pre-personalisation requirements, though the actual data for IC pre-personalisation come from Phase 6 (or Phase 4 or 5).</li> </ul>

Phase 2	IC Development	The IC Designer	
		designs the IC,	
		develops IC Dedicated Software,	
		provides information, software or tools to the Smartcard Embedded Software Developer, and	
	from the developer	<ul> <li>receives the smartcard embedded software from the developer, through trusted delivery and verification procedures.</li> </ul>	

Version 1.0 (July 2001) Page 84 (of 100)

		From the IC design, IC Dedicated Software and Smartcard Embedded Software, the IC Designer		
		constructs the smartcard IC database, necessary for the IC photomask fabrication.		
Phase 3	Phase 3 IC Manufacturing and Testing	The IC Manufacturer is responsible for		
and Testing		producing the IC through three main steps: IC manufacturing, IC testing, and IC prepersonalisation.		
		The IC Mask Manufacturer		
		generates the masks for the IC manufacturing		
		based upon an output from the smartcard IC database.		

Phase 4	IC Packaging and Testing	The IC Packaging Manufacturer is responsible for
• the I		the IC packaging and testing.
Phase 5	Smartcard Product Finishing Process	The <b>Smartcard Product Manufacturer</b> is responsible for
		the smartcard product finishing process and testing.
Phase 6	Smartcard Personalisation	The <b>Personaliser</b> is responsible for  • the smartcard personalisation and final tests.  Other smartcard embedded software may be loaded onto the chip at the personalisation process,
Phase 7	Smartcard End-usage	The <b>Smartcard Issuer</b> is responsible for  • the smartcard product delivery to the smartcard end-user, and the end of life process.

The relation between the semiconductor industry (TOE Manufacturer, refer to Section 2.1, in particular comprising the roles IC Designer / IC Manufacturer and IC Mask Manufacturer) and the other parties being involved in the Smartcard development and production (especially the Smartcard Embedded Software Developer) are visualised in Figure 16.

Version 1.0 (July 2001) Page 85 (of 100)

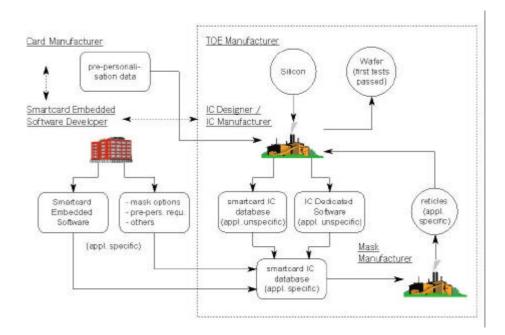


Figure 16: Development and Wafer Production including Testing

- The development process of the TOE starts with a process qualification. In parallel the concept of the integrated circuit and the corresponding logical design is developed. The design uses standard library elements (circuitry and layout) which could be used for other (non security) integrated circuits but may include full custom elements specially designed for the TOE as well. Some cells have parameters: For instance the concrete layout of a ROM cell is determined by its contents which in turn is determined by the software or the data to be stored within.
- All these "cells" not only differ in their logical or physical behaviour but also in their structure size which may range from very few elements such as simple gates up to physical units or sub-circuitry which may represent whole independent logical processing units. The physical "cells" (physical layout information is used) are placed on the chip area and then connected by wires (routing). Information about the physical layout of "cells", about their position, about the shape of connecting wires and other process information define the physical layout of the chip.
- These development steps are very complex. Only the development of the logical design might be similar to standard software development. However, technological constraints (such as timing) make this process more complicated and require for instance simulations which take technological and layout information into account. So, logical and physical design are developed in close relation.
- 328 The development of the information which defines the physical layout of an integrated circuit is a very complex matter. The masks or reticles required for wafer production are basically produced based upon this information. However, a bunch of technology related parameters (possible even some depending on the wafer foundry) are taken into account in addition.

Version 1.0 (July 2001) Page 86 (of 100)

- The masks or reticles are used to realise the integrated circuitry on/in a substrate. This again comprises tens of process steps each effecting the final result. Not only layout principles but process information is proprietary to IC Designers / IC Manufacturers. The evaluator will not be able to comprehend the details of wafer processing. Each single chip (die or dice) is being tested after production.
- The development and production is based upon a well established process of the manufacturer of the TOE. The processes are continuously developed and improved mainly in order to increase yield and reliability.
- During integrated circuit development and production many information and material is produced as summarised in Section 8.1.2. The evaluator must concentrate on the most important assets and exactly assess their storage and handling. It is not sufficient to assess a company as a whole, arguing that personnel is trustworthy and exchange of information and material with external partners is properly controlled.

# 8.1.2 Description of Assets of the Integrated Circuits Designer/Manufacturer

- The assets of the manufacturer of the TOE to be protected during development and production of the TOE were already identified in paragraph 79 (page 22). Further explanatory text is given here.
- 333 The **logical design data** are those used to design the schematics of the chip (schematics or HDL sources and design documents). With the logical design data the functionality of the chip can be understood. The logical design data can be regarded as being independent from the actual implementation (layout) though they contain the timing characteristics of some functional units (circuitry blocks).
- 334 The **physical design data** comprises all topographic information (three dimensional) about parts of the chip or the whole chip. Topographic information is the absolute or relative position, form, thickness, length and size of any structures realised on the chip surface. These structures are pads, connecting wires, isolation layers, vias, and implants.
- The IC Dedicated Software, Smartcard Embedded Software, Initialisation Data and Pre-personalisation Data comprises the source code including the related documents and the corresponding binaries as well as other data to be injected into the TOE before TOE Delivery.
- The **specific development aids** comprise all tools especially developed to produce the product. One important example is the "ROM translator" which produces the physical memory content from the software binaries.
- 337 The **test and characterisation related data** comprise all information, which is used for testing including test results (pre-layout, post layout and product) and the characterisation of the final chip.

Version 1.0 (July 2001) Page 87 (of 100)

- 338 The material for software development support comprises all information and material given to the Smartcard Embedded Software Developer to support the development of the Smartcard Embedded Software.
- The **photomasks and products** comprises the photomasks or reticles (usable and scrap) and chips (usable and scrap) in different forms.
- 340 The requirements of the Common Criteria assurance family ALC\_DVS apply to all the above items. This includes assessment of all sites being involved in the development and production of the product. Exceptions must be agreed with the certification body.

# 8.2 Security Aspects of the Smartcard Embedded Software

# 8.2.1 Further Information regarding A.Resp-Appl

- When defining the Protection Profile or Security Target for the evaluation of the Smartcard Embedded Software appropriate threats must be defined which depend on the application context. These security needs are condensed in the assumption A.Resp-Appl (refer to Section 3.2) of this Protection Profile which is very general since the application context is not known and the evaluation of the Smartcard Embedded Software is not covered by this Protection Profile. Refer to the requirement RE.Phase-1 (Section 5.2.2) in addition.
- For better understanding of the assumption A.Resp-Appl (and the requirement RE.Phase-1), examples are given in below, all being directly related to and covered by A.Resp-Appl as shown in Figure 17. Note that this figure the explanatory text below refers to assumptions here (TOE perspective) though these are requirements for the Smartcard Embedded Software (perspective of that software).

Version 1.0 (July 2001) Page 88 (of 100)

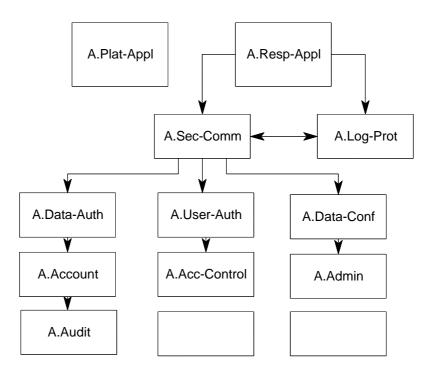


Figure 17: Examples for Implementations of A.Resp-Appl

- Note that this Protection Profile only specifies (and further refers to) the assumptions A.Plat-Appl and A.Resp-Appl for the usage of the TOE. All other assumption on the development of the Smartcard Embedded Software are only given for the sake of information and are examples which must be selected and refined in the application context. The evaluation of the smartcard integrated circuit according to this Protection Profile is conducted independent from the application context and evaluation results must be available before the evaluation of the Smartcard Embedded Software can be completed.
- 344 The next level of security aspects for the Smartcard Embedded Software (TOE security environment) are expected to cover the following:
- 345 Secure Communications (A.Sec-Com)

The Smartcard Embedded Software must support secure communication protocols and procedures between the smartcard and a terminal or a remote host as required by the application context. This prevents

- unauthorised usage of functions and/or data by intercepting data on the I/O-lines,
- disclosure or undetected manipulation of data exchanged via the I/O-lines.
- replay of exchanged data through the I/O-lines

Version 1.0 (July 2001) Page 89 (of 100)

which would cause for instance financial loss or at least affect the reputation of the system. Details must be specified in the application context.

# 346 Logical Protection (A.Log-Prot)

The Smartcard Embedded Software must prevent logical compromise through attacks on its logical operation visible on the external I/O interface. This includes protection against

- release of information though the analysis of responses to repetitive challenges<sup>20</sup>,
- causing faults by stimulating the card and interrupting its operation, and
- disclosure of data by measuring and analysis as described in O.Leak.

Details must be specified in the application context.

Further concrete requirements for the Smartcard Embedded Software may include but is not limited to (i) Data Authenticity (A.Data-Auth), (ii) User Authentication (A.User-Auth), (iii) Stored Data Confidentiality (A.Data-Conf), (iv) Accountability (A.Account), (v) Access Control (A.Acc-Control), (vi) Administration (A.Admin), (vii) Audit and Accountability (A.Audit). The concrete requirements are to be defined in the Protection Profile / Security Target for the Smartcard Embedded Software.

# 8.2.2 Examples of Specific Functional Requirements for the Smartcard Embedded Software

- 348 The following two Security Functional Requirements are typical examples of functionality to be provided by the Smartcard Embedded Software in order to support the security provided by the TOE.
- Example 1: The Smartcard Embedded Software shall meet the requirement "Stored data integrity monitoring (FDP\_SDI.1)" as specified below.

FDP\_SDI.1 Stored data integrity monitoring

Hierarchical to: No other components.

FDP\_SDI.1.1 The TSF shall monitor user data stored within the TSC for

integrity errors after writing and before usage (and if necessary

Version 1.0 (July 2001) Page 90 (of 100)

This objective could also work through the detection of such attacks and the initiation of corrective actions to counter such attempts.

after processing) <sup>21</sup> on all objects, based on the following attributes: data are considered as being critical <sup>22</sup>.

Dependencies: No dependencies.

Refinement: The wording "and if necessary after processing" refers to

situations where errors occurred during a calculation<sup>23</sup> (though the TOE provides FRU\_FLT.2 and FPT\_FLS.1). In this case it might be necessary that the Smartcard Embedded Software supports the overall security for instance by redundant

calculations and verification after that.

Example 2: The Smartcard Embedded Software shall meet the requirement "Abstract machine testing (FPT\_AMT.1)" as specified below.

**FPT\_AMT.1** Abstract machine testing

Hierarchical to: No other components.

FPT\_AMT.1.1 The TSF shall run a suite of tests at initial start-up or before use

of the random number generator if being used by the Smartcard Embedded Software <sup>24</sup> to demonstrate the correct operation of the security assumptions provided by the abstract

machine that underlies the TSF.

Dependencies: No dependencies.

# 8.3 Examples of Attack Scenarios

In this section background information is given to better understand the threats defined in Section 3.3. The different types of influences on or interactions with the Smartcard were already visualised in Figure 8. The contents of this section shall not be considered as being complete nor as a comprehensive guidance for the evaluation.

352 A standard tool used for electrical measurement (and application of voltage and injection of current) is the needle probe workstation. Often appropriate contact areas must be prepared before using the methods described above (refer to the threat

Version 1.0 (July 2001) Page 91 (of 100)

<sup>&</sup>lt;sup>21</sup> [assignment: integrity errors]

<sup>&</sup>lt;sup>22</sup> [assignment: user data attributes]

for instance due to exposure to specific "radiation"

<sup>&</sup>lt;sup>24</sup> [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]

- T.Phys-Manipulation). The actual measurement is done using standard tools such as voltmeters, oscilloscopes and signal analysers.
- In addition, there are indirect methods for measurements not requiring a direct (metallic) contact. Examples are voltage contrast imaging and electron probe microscopy. These methods are also referred to as physical probing since the Smartcard must be prepared before using the methods described above (refer to the threat T.Phys-Manipulation).
- 354 The interface for the attack is (the smartcard carrier and then) the surface of the integrated circuit.
- The application of appropriate combinations of such methods in order to reveal information (via a non-standard interface) are addressed by the threat **T.Phys-Probing**.
- Malfunctions of the TOE may cause some of its TSF to fail to be effective. Often more critical, security functions (or mechanisms) of the Smartcard Embedded Software may fail to be effective. This can be utilised by an attacker. The most straightforward way to cause malfunctions are irregular operating conditions in amplitude, shape, timing, occurrence etc. on the ISO interface (for instance such as glitches). Malfunctions can be due to errors or premature ageing.
- 357 The attacker stimulates the ISO interface (power supply, the external clock, reset and/or I/O). The attacker may also consider other types of influences on the Smartcard or directly onto the surface of the integrated circuit. In the latter case it might be required to manipulate the Smartcard (refer to the threat T.Phys-Manipulation). In addition, the attacker needs to observe the behaviour of the Smartcard and immediately take advantage of a possible malfunction. This requires to have additional equipment such as a terminal and communication software, but may include other things depending on the application to be attacked.
- The application of appropriate combinations of such methods in order to manipulate the Smartcard Embedded Software (or the IC Dedicated Test Software) while being executed (via a standard interface) are addressed by the threat **T.Malfunction**.
- Specific sorts of malfunctions are a means to reveal information about cryptographic keys or other critical data. Such methods are addressed by the threat T.Leak-Forced.
- 360 Standard tools used for the manipulation of circuitry are the Focused Ion Beam (FIB) and the laser cutter. The contents of programmable memories (such as E<sup>2</sup>PROM) may be modified for instance by manipulation of circuitry, by exposing cells to charged particle beams, by using electromagnetic waves or by electrical probing (application of voltage and injection of current).
- Manipulations require prior extensive reverse-engineering. The methods being applied are for instance optical inspection, voltage contrast imaging, image processing and pattern matching. In order to analyse circuitry the chip hardware must be removed from its carrier and then de-layered using appropriate methods (wet etching, plasma etching, grinding).

Version 1.0 (July 2001) Page 92 (of 100)

- 362 The interface for the attack is (the smartcard carrier and then) the surface of the integrated circuit.
- The application of appropriate combinations of such methods in order to perform manipulations are addressed by the threat **T.Phys-Manipulation**.
- When the Smartcard processes User Data and other critical data information about these data may be contained in signals which can be measured on the ISO contacts of the Smartcard using standard tools such as voltmeters, oscilloscopes and signal analysers. The Smartcard may also produce emanation which can be received using an antenna and analysed. For the analysis of the measured data specific tools (software) are required.
- The interface for the attack is the ISO interface (contacts of the Smartcard) but other interfaces may also be used.
- The application of appropriate combinations of such methods in order to reveal information (without affecting the TOE's operation or the TOE itself) are addressed by the threat **T.Leak-Inherent**. Public known attack scenarios are for instance the Simple Power Analysis (SPA) and the Differential Power Analysis (DPA).
- An attacker may also apply methods in order to cause the TOE to leak information. For instance the attacker must in addition cause faults. The interface for the attack can be more complex in this case. The ISO interface (contacts of the Smartcard), the Smartcard itself and/or the surface of the integrated circuit may be used to cause faults (refer to the threat T.Malfunction for more detail). Physical manipulations may also be done (refer to the threat T.Phys-Manipulation).
- The application of appropriate combinations of such methods in order to reveal information (by affecting the TOE's operation or manipulating the TOE itself) are addressed by the threat **T.Leak-Forced** not being related to attacks on cryptographic algorithms only. Public known attack scenarios are for instance the Differential Fault Analysis (DFA) and the Bellcore type of attacks.
- The evaluation of the TOE will in many cases not lead to final results for smartcard products built using the TOE. Tests must be repeated with the actual Smartcard Embedded Software.
- Test Features (including other non-application related function) implemented in the TOE might be abused in order 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 IC Dedicated Test Software which are not specified here.
- 371 If the IC Dedicated Test Software offers commands via the ISO I/O interface an attacker needs to communicate with the Smartcard using a terminal and the communication software. If other interfaces are used and/or if the usage of such commands is protected, it can be necessary to manipulate the TOE (refer to the threat T.Phys-Manipulation for more detail) and/or to circumvent authentication mechanisms. An attacker may also reveal information by physical probing (refer to

Version 1.0 (July 2001) Page 93 (of 100)

the threat T.Phys-Probing) or analysing data (refer to the threats T.Leak-Inherent and T.Leak-Forced). If the TOE provides a command interface it can be subject to manipulations as described under the threat T.Malfunction and the software must not be susceptible to invalid inputs and other types of logical attacks being specific for software. Details depend on the way the Test Features are provided and protected by the TOE which is not specified here.

The application of appropriate combinations of methods in order to reveal information or perform manipulations are addressed by the threat **T.Abuse-Func**.

## 8.4 Definition of the Family FCS\_RND

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

#### FCS RND Generation of random numbers

Family behaviour

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

#### Component levelling:

FCS RND Generation of random numbers

FCS\_RND.1 Generation of random numbers requires that random numbers

meet a defined quality metric.

Management: FCS RND.1

There are no management activities foreseen.

Audit: FCS\_RND.1

There are no actions defined to be auditable.

FCS\_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

FCS\_RND.1.1 The TSF shall provide a mechanism to generate random

numbers that meet [assignment: a defined quality metric].

Dependencies: No dependencies.

Version 1.0 (July 2001) Page 94 (of 100)

## 8.5 Definition of the Family FMT\_LIM

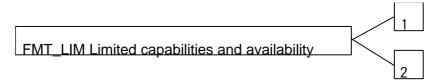
- To define the IT security functional requirements of the TOE an additional family (FMT\_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE (refer to Section 5.1.1) show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.
- 375 The family "Limited capabilities and availability (FMT\_LIM)" is specified as follows.

## FMT LIM Limited capabilities and availability

# Family behaviour

This family defines requirements that limits the capabilities and availability of functions in a combined manner. Note that FDP\_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

# Component levelling:



FMT LIM.1 Limited capabilities requires that the TSF is built to provide only

the capabilities (perform action, gather information) necessary

for its genuine purpose.

FMT LIM.2 Limited availability requires that the TSF restrict the use of

functions (refer to Limited capabilities (FMT\_LIM.1)). This can be achieved, for instance, by removing or by disabling functions

in a specific phase of the TOE's life-cycle.

Management: FMT\_LIM.1, FMT\_LIM.2

There are no management activities foreseen.

Audit: FMT\_LIM.1, FMT\_LIM.2

There are no actions defined to be auditable.

Version 1.0 (July 2001) Page 95 (of 100)

376 The TOE Functional Requirement "Limited capabilities (FMT\_LIM.1)" is specified as follows.

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 [assignment:

Limited capability and availability policy].

Dependencies: FMT\_LIM.2 Limited availability.

377 The TOE Functional Requirement "Limited availability (FMT\_LIM.2)" is specified as follows.

FMT\_LIM.2 Limited availability

Hierarchical to: No other components.

FMT\_Llm.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 [assignment:

Limited capability and availability policy].

Dependencies: FMT\_LIM.1 Limited capabilities.

- Application note: The functional requirements FMT\_LIM.1 and FMT\_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that
  - (i) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced

or conversely

(ii) the TSF is designed with high functionality but is removed or disabled in the product in its user environment.

The combination of both requirements shall enforce the policy.

#### 8.6 Definition of the Family FAU\_SAS

To define the security functional requirements of the TOE an additional family (FAU\_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU\_GEN, because it does not necessarily require the data to be

Version 1.0 (July 2001) Page 96 (of 100)

generated by the TOE itself and because it does not give specific details of the content of the audit records.

The family "Audit data storage (FAU\_SAS)" is specified as follows.

# FAU\_SAS Audit data storage

Family behaviour

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

## Component levelling

	]	
FAU_SAS Audit data storage		1_

FAU\_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU\_SAS.1

There are no management activities foreseen.

Audit: FAU\_SAS.1

There are no actions defined to be auditable.

**FAU\_SAS.1** Audit storage

Hierarchical to: No other components.

FAU\_SAS.1.1 The TSF shall provide [assignment: authorised users] with the

capability to store [assignment: list of audit information] in the

audit records.

Dependencies: No dependencies.

# 8.7 Glossary of Vocabulary

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 TOE during TOE Delivery. The Card Manufacturer

Version 1.0 (July 2001) Page 97 (of 100)

includes all roles after TOE Delivery up to Phase 7 (refer to Figure 4 on page 17 and Section 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 Protection Profile) Composition of the TOE, the Smartcard Embedded Software, User Data and the package (the smartcard carrier).

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.

Version 1.0 (July 2001) Page 98 (of 100)

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 (refer to Figure 4 on page 17) 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 (as defined in Section 2.1) and its development and production environment are fulfilled (refer to Figure 4 on page 17).

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 [5] (for example configuration data). Note that the TOE is the Smartcard IC (refer to definition in paragraph 48).

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

Version 1.0 (July 2001) Page 99 (of 100)

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.

## 8.8 List of Abbreviations

CC Common Criteria Version 2.0 or Version 2.1. Note that the

Version 2.1 (ISO 15408) is technically identical with Version 2.0

of the Common Criteria.

EAL Evaluation Assurance Level.

IC Integrated circuit.

IT Information Technology.

PP Protection Profile.

SOF Strength of function.

ST Security Target.

TOE Target of Evaluation.

TSC TSF Scope of control.

TSF TOE Security functions.

TSP TOE Security Policy.

Version 1.0 (July 2001) Page 100 (of 100)