Common Criteria for Information Technology Security Evaluation

---

Protection Profile

Smartcard Integrated Circuit

Version 2.0

Issue September 1998

Registered at the French Certification Body under the number PP/9806

Any correspondence about this document should be referred to the following organisations:

- Motorola Semiconductors

  8, Rue Grange Dame Rose
  BP 95 F- 78143 Velizy
  Telephone : (+33) 1 34 63 59 66 Fax : (+33) 1 34 63 58 61 www.mot.com

- Philips Semiconductors

  Röhren -und Halbleiterwerke Stresemannallee 101
  D- 22529 Hamburg
  Telephone : (+49) 40 5613 26 24 Fax : (+49) 40 5613 3045

- Service Central de la Sécurité des Systèmes d'Information

  Information Technology Security Certification Centre
  18, rue du Docteur Zamenhof F-92131 Issy-Les-Moulineaux
  Telephone : (+33) 1 41 46 37 84 Fax : (+33) 1 41 46 37 01

- Siemens AG Semiconductors

  HL CC M
  P.O. Box 801760
  D-81617 Munich
  Telephone : (+49) 89 636 48964 Fax : (+49) 89 636 222 14

- STMicroelectronics

  ZI de Rousset B.P. 2
  F- 13106 Rousset Cedex
  Telephone : (+33) 4 42 25 89 44 Fax : (+33) 4 42 25 87 29 www.st.com

- Texas-Instruments Semiconductors

  BP5
  F- 06271 Villeneuve Loubet Cedex
  Telephone : (+33) 4 93 22 22 20 Fax : (+33) 4 93 22 26 37

For any kind of request for comments, please e-mail at ssi20@calva.net

Common Criteria are available at the following address: http://www.crsc.nist.gov/cc

This document is paginated from i to ii and from 1 to 54

Table of contents

Chapter 1

PP introduction

1.1 PP identification

Title: Smartcard Integrated Circuit Protection Profile.

Version number: V2.0, issue September 1998.

Registration: registered at French Certification Body under the number PP/9806.

Registration	Version number	Common Criteria
PP/9704	V1.0	version 1.0
PP/9806	V2.0	version 2.0

1 A glossary of terms used in the PP is given in annex A.

2 This PP has been built with Common Criteria Version 2.0.

3 A product compliant with this PP may also offer additional security functional requirements, depending on the application type.

1.2 PP overview

4 This Protection Profile conducted under the french IT Security Evaluation and Certification Scheme is the work of a group composed of the following Integrated Circuits manufacturers:

- Motorola Semiconductors,
- Philips Semiconductors,
- Siemens Semiconductors,
- STMicroelectronics,
- Texas-Instruments Semiconductors.

5 The intent of this Protection Profile is to specify functional and assurance requirements applicable to a smartcard integrated circuit.

6 A smartcard is usually seen as a credit card sized card having a non volatile memory and a processing unit embedded within it. This Protection Profile is dedicated to microcontroller based smartcards integrated circuits whatever will be the interface and communication protocol with the intended usage environment (contact or contact-less smartcards or a combination of both).

7 The complex development and manufacturing processes of a smartcard before it is issued to the users can be separated into three distinct stages:

- the development stage: integrated circuit (hereafter “IC”) design, smartcard embedded software development, application software development, integration and photomask fabrication,
- the IC production stage: IC manufacturing, testing, preparation and shipping to the IC assembly line,
- the smartcard production stage: smartcard IC packaging (and testing), smartcard product finishing process, printing (and testing), smartcard preparation and shipping to the personalisation line,

8 In addition, two important stages are to be considered in the smartcard life cycle:

- the smartcard personalisation and testing stage where the end-user data is loaded into the smartcard's memory,
- the smartcard usage by its issuers and end-user.

9 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 summarized as being able to counter those who want to defraud, gain unauthorized 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 non-volatile memory (program and data memories),
- maintain the integrity and the confidentiality of the security enforcing and security relevant architectural components (security mechanisms and associated functions) embedded into the integrated circuit.

10 Protected information are in general secret data as Personal Identification Numbers, Balance Value (Stored Value Cards), and Personal Data Files. Another set of protected information is 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.

11 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 end-user. An exception to this are the controls that

are applicable when the smartcard is in its end usage in the system working according to its specifications.

12 Presently the major smartcard applications are:

- banking and finance market for credit/debit cards, electronic purse (stored value cards) and electronic commerce,
- network based transaction processing such as mobile phones (GSM SIM cards), pay-TV (subscriber and pay-per-view cards), communication highways (Internet access and transaction processing),
- transport and ticketing market (access control cards),
- governmental cards (ID-cards, healthcards, driver license etc.),
- new emerging sectors such as the multimedia commerce and Intellectual Proprietary Rights protection.

13 One of the key market drivers for smartcards is standardization of specifications such as the EMV specifications (Europay-Mastercard-Visa) for banking applications, the current revision of ETSI prN and GSM 11 which both include parts of the ISO 7816, and the specifications SET or C-SET for electronic commerce. Due to market demands, the major cryptographic schemes such as those using DES, RSA, DSA, are also now included in standard specifications.

14 The main objectives of this Protection Profile is:

- to describe the Target of Evaluation (TOE) as a product and position it in the life cycle of the smartcard. The PP includes the development and the production phase of the IC with its dedicated software, without the smartcard embedded software development phase,
- to describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by the operational environment during the development, production and user phases,
- to describe the security objectives for the TOE and for its environment in terms of integrity and confidentiality of application data and programs, protection of the TOE and associated documentation during the development and production phases,
- to specify the security requirements which includes the TOE security functional requirements and the TOE security assurance requirements.

15 The assurance level for this PP is EAL 4 augmented. The minimum strength level for the TOE security functions is SOF-high (Strength of Functions High).

Chapter 2

TOE Description

16 This part of the PP describes the TOE as an aid to the understanding of its security requirements and address the product type, the intended usage and the general IT features of the TOE.

2.1 Product type

17 The Target of Evaluation (TOE) is the single chip microcontroller unit 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 PP[1].

18 The typical TOE is composed of a processing unit, security components, I/O ports and volatile and non-volatile memories. The TOE includes any IC designer/ manufacturer proprietary IC dedicated software which is required for testing purpose. This IC dedicated software may be either IC embedded software (also known as IC firmware) or security-relevant parts of tests programmes outside the IC. The TOE may include any IC pre-personalisation data.

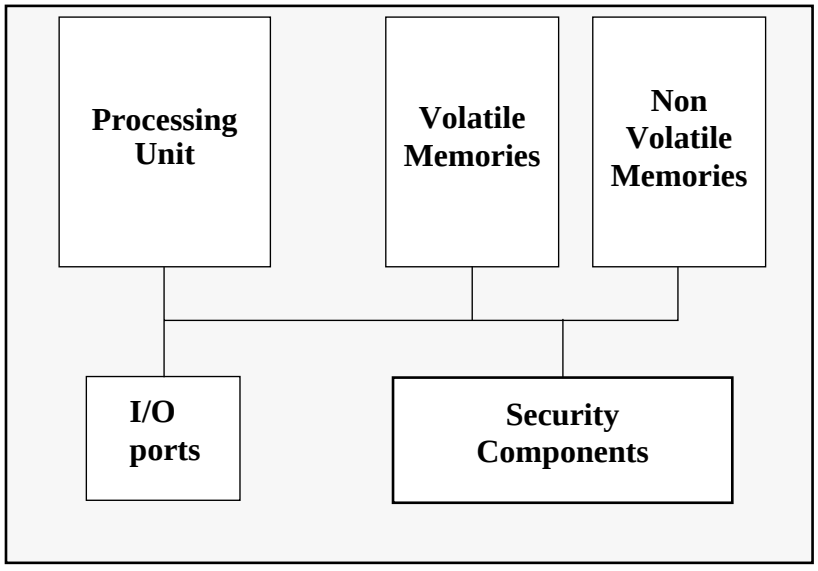

Fig. 2.1 - Typical Smartcard IC Product

1. Editorial note: Standard memory cards are outside the scope of this PP.

2.2 Smartcard Product Life-cycle

19 The smartcard product life-cycle is decomposed into 7 phases where the following authorities are involved:

Phase 1	Smartcard embedded software development	**the smartcard embedded software developer** is in charge of the smartcard embedded software development and the specification of IC pre-personalisation requirements,
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 receives the smartcard embedded software from the developer, through trusted delivery and verification procedures. From the IC design, IC dedicated software and smartcard embedded software, he constructs the smartcard IC database, necessary for the IC photomask fabrication,
Phase 3	IC manufacturing and testing	**the IC manufacturer** is responsible for producing the IC through three main steps : IC manufacturing, IC testing, and IC pre-personalisation,
Phase 4	IC packaging and testing	**the IC packaging manufacturer** is responsible for the IC packaging and testing,
Phase 5	Smartcard product finishing process	**the smartcard product manufacturer** is responsible for the smartcard product finishing process and testing,
Phase 6	Smartcard personalisation	**the personaliser** 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 smartcard issuer** is responsible for the smartcard product delivery to **the smartcard end-user**, and the end of life process.

20 The limits of the Protection Profile correspond to phases 2 and 3, including the phase 1 delivery and verification procedures and the TOE delivery to the IC

packaging manufacturer ; procedures corresponding to phases 1, 4, 5, 6 and 7 are outside the scope of this PP.

21 Nevertheless, in certain cases, it would be of great interest to include the phase 4 (IC packaging and testing), within the limits of the evaluation. However, for the time being, this option remains outside the scope of this Protection Profile.

22 The figure 2.2 describes the Smartcard product life-cycle.

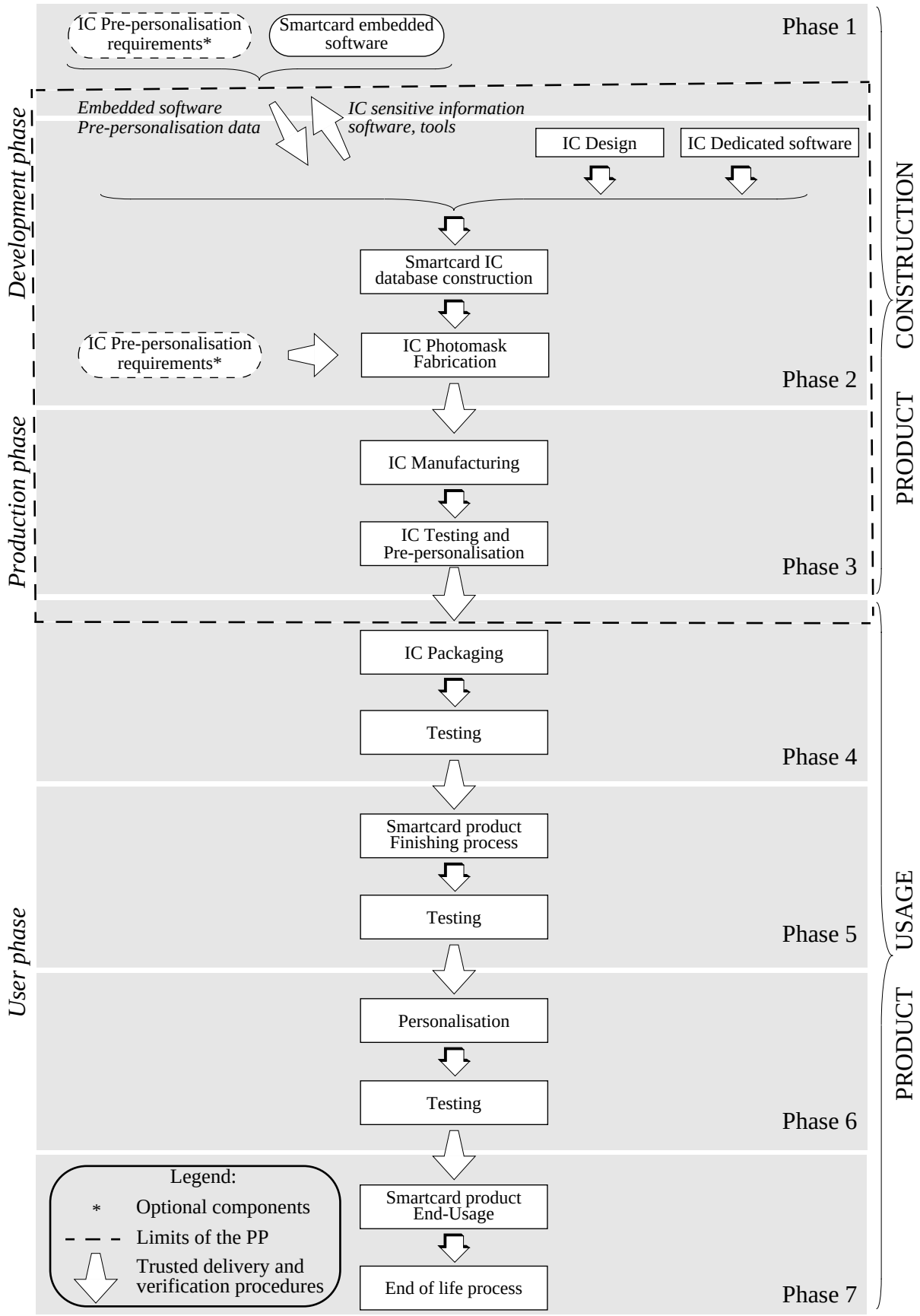

Fig. 2.2 - Smartcard product life-cycle

23 These different phases may be performed at different sites; procedures on the delivery process of the TOE shall exist and be applied for every delivery within a phase or between phases. This includes any kind of delivery performed from phase 1 to phase 7, including:

- intermediate delivery of the TOE or the TOE under construction within a phase,
- delivery of the TOE or the TOE under construction from one phase to the next.

24 These procedures shall be compliant with the assumptions [A_DLV] developed in section 3.2.2.

2.3 TOE environment

25 Considering the TOE, three types of environments are defined :

- Development environment corresponding to phase 2,
- Production environment corresponding to phase 3,
- User environment, from phase 4 to phase 7.

2.3.1 TOE Development Environment

26 To assure security, the environment in which the development takes place shall be made secured with controllable accesses having traceability. Furthermore, it is important that all authorised personnel involved fully understand the importance and the rigid implementation of defined security procedures.

27 The development begins with the TOE's specification. All parties in contact with sensitive information are required to abide by Non-Disclosure Agreement's.

28 Design and development of the IC then follows. The engineer uses a secure computer system (preventing unauthorised access) to make his design simulations, circuit performance verifications and generation of the TOE's IC photomask databases. Sensitive documents, databases on tapes, diskettes, and printed circuit layout information are stored in appropriate locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

29 Reticles and photomasks are generated from the verified IC databases; the former are used in the silicon Wafer-fab processing. When reticles and photomasks are generated off-site, they shall be transported and worked on in a secure environment with accountability and traceability of all (good and bad) products. During the transfer of sensitive data electronically, procedures shall be established to ensure that the data arrive only at the destination and are not accessible at intermediate

stages (e.g. stored on a buffer server where system administrators make backup copies).

2.3.2 TOE Production environment

30 As high volumes of product commonly go through such environments, adequate control procedures are necessary to account for all product at all stages of production.

31 Production starts within the Wafer-fab; here the silicon wafers undergo the diffusion processing typically in 50-wafer lots. Computer tracking at wafer level throughout the process is commonplace. The wafers are then taken into the test area. Testing and security programming (optional) of each TOE occurs. After fabrication, the TOE is tested to assure conformance with the device specification. The wafers will then be delivered for assembly onto the smartcard.

32 Whether carried out under the control of the IC manufacturer or the packaging manufacturer, wafers shall be scribed and broken such as to separate the functional from the non-functional ICs. The latter is discarded in a controlled accountable manner. The good ICs are then packaged. When testing, programming and deliveries are done offsite, ICs shall be transported and worked on in a secure environment with accountability and traceability of all (good and bad) products. Further testing occurs, followed by smartcard personalisation, retesting then delivery to the smartcard issuer.

2.3.3 TOE user environment

33 The TOE user environment is the environment of phases 4 to 7.

34 At phases 4, 5 and 6, the TOE user environment is a controlled environment.

End-user environment (phase 7)

35 Smartcards are used in a wide range of applications to assure authorised conditional access. Examples of such are Pay-TV, Banking Cards, Portable communication SIM cards, Health cards, Transportation cards.

36 The end-user environment therefore covers a wide sprectum of very different functions, thus making it difficult to avoid and monitor any abuse of the TOE.

2.4 TOE logical phases

37 During its construction usage, the TOE may be under several life logical phases. These phases are sorted under a logical controlled sequence. The change from one phase to the next shall be under the TOE control.

2.5 TOE Intended usage

38 The TOE can be incorporated in several applications such as:

- banking and finance market for credit/debit cards, electronic purse (stored value cards) and electronic commerce,
- network based transaction processing such as mobile phones (GSM SIM cards), pay-TV (subscriber and pay-per-view cards), communication highways (Internet access and transaction processing),
- transport and ticketing market (access control cards),
- governmental cards (ID-cards, healthcards, driver license etc.),
- new emerging sectors such as multimedia commerce and Intellectual Property Rights protection.

39 During the phases 1, 2, 3, the TOE is being developed and produced. The **administrators** are the following:

- the smartcard embedded software developer,
- the IC designer,
- the IC manufacturer.

40 During phases 4 to 7, the users of the TOE are the following:

41 Phase 4:

- the IC packaging manufacturer (**administrator**),
- the smartcard embedded software developer,
- the system integrators such as the terminal software developer.

42 Phase 5:

- the smartcard product manufacturer **(administrator**),
- the smartcard embedded software developer,
- the system integrators such as the terminal software developer.

43 Phase 6:

- the personaliser (**administrator**),
- the smartcard issuer (**administrator**),
- the smartcard embedded software developer,
- the system integrators such as the terminal software developer.

44 Phase 7:

- the smartcard issuer **(administrator**),
- the smartcard end-user,
- the smartcard embedded software developer,
- the system integrators such as the terminal software developer.

The IC manufacturer and the smartcard product manufacturer may also receive ICs for analysis should problems occur during the smartcard usage.

2.6 General IT features of the TOE

45 The TOE IT functionalities consist of data storage and processing such as:

- arithmetical functions (e.g. incrementing counters in electronic purses, calculating currency conversion in electronic purses...);
- data communication;
- cryptographic operations (e.g. data encryption, digital signature verification).

Chapter 3

TOE Security Environment

46 This section describes the security aspects of the environment in which the TOE is intended to be used and addresses the description of the assumptions, the assets to be protected, the threats and the organisational security policies.

3.1 Assets

47 Assets are security relevant elements of the TOE that include:

- the application data of the TOE (such as IC pre-personalisation requirements, IC and system specific data),
- the smartcard embedded software,
- the IC dedicated software,
- the IC specification, design, development tools and technology.

48 The TOE itself is therefore an asset.

49 Assets have to be protected in terms of confidentiality and integrity.

3.2 Assumptions

50 It is assumed that this section concerns the following items:

- due to the definition of the TOE limits, any assumption for the smartcard embedded software development (phase 1 is outside the scope of the TOE),
- any assumption from phases 4 to 7 for the secure usage of the TOE, including the TOE delivery procedures.

51 Security is always the matter of the whole system: the weakest element of the chain determines the total system security. Assumptions described hereafter have to be considered for a secure system using smartcard products:

- assumptions on phase 1,
- assumptions on the TOE delivery process (phases 4 to 7),
- assumptions on phases 4-5-6,
- assumptions on phase 7.

3.2.1 Assumptions on phase 1

A.SOFT_ARCHI	The smartcard embedded software shall be developed in a secure manner, that is focusing on integrity of program and data.
A.DEV_ORG	Procedures dealing with physical, personnel, organisational, technical measures for the confidentiality and integrity of smartcard embedded software (e.g. source code and any associated documents) and IC designer proprietary information (tools, software, documentation...) shall exist and be applied in software development.

3.2.2 Assumptions on the TOE delivery process (phases 4 to 7)

52 Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives as described in the following assumptions.

A.DLV_PROTECT	Procedures shall ensure protection of TOE material/ information under delivery and storage.
A.DLV_AUDIT	Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
A.DLV_RESP	Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

3.2.3 Assumptions on phases 4 to 6

A.USE_TEST It is assumed that appropriate functionality testing of the IC is used in phases 4, 5 and 6.

A.USE_PROD It is assumed that security procedures are used during all manufacturing and test operations through phases 4, 5, 6 to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

3.2.4 Assumptions on phase 7

A.USE_DIAG It is assumed that secure communication protocols and procedures are used between smartcard and terminal.

A.USE_SYS It is assumed that the integrity and the confidentiality of sensitive data stored/handled by the system (terminals, communications...) is maintained.

3.3 Threats

53 The TOE as defined in chapter 2 is required to counter the threats described hereafter; a threat agent wishes to abuse the assets either by functional attacks, environmental manipulations, specific hardware manipulations or by any other types of attacks.

54 Threats have to be split in:

- threats against which specific protection within the TOE is required (class I),
- threats against which specific protection within the environment is required (class II).

3.3.1 Unauthorized full or partial cloning of the TOE

T.CLON	Functional cloning of the TOE (full or partial) appears to be relevant to any phases of the TOE life-cycle, from phase 1 to phase 7. Generally, this threat is derived from specific threats combining unauthorized disclosure, modification or theft of assets at different phases.

3.3.2 Threats on phase 1 (delivery and verification procedures)

55 During phase 1, three types of threats have to be considered:

a) threats on the smartcards embedded software and its environment of development, such as:

- unauthorized disclosure, modification or theft of the smartcard embedded software and any additional data at phase 1.

  Considering the limits of the TOE, these previous threats are outside the scope of this protection profile.

b) threats on the assets transmitted from the IC designer to the smartcard embedded software developer during the smartcard development;

c) threats on the smartcard embedded software and any additional application data transmitted during the delivery process from the smartcard embedded software developer to the IC designer.

56 The previous types b and c threats are described hereafter:

T.DIS_INFO	Unauthorized disclosure of the assets delivered by the IC designer to the smartcard embedded software developer such as sensitive information on IC specification, design and technology, software and tools if applicable;
T.DIS_DEL	Unauthorized disclosure of the smartcard embedded software and any additional application data (such as IC pre-personalisation requirements) during the delivery process to the IC designer;

T.MOD_DEL	Unauthorized modification of the smartcard embedded software and any additional application data (such as IC pre-personalisation requirements) during the delivery process to the IC designer;
T.T_DEL	Theft of the smartcard embedded software and any additional application data (such as IC pre-personalisation requirements) during the delivery process to the IC designer.

3.3.3 Threats on phases 2 to 7

57 During these phases, the assumed threats could be described in three types:

- unauthorized disclosure of assets,
- theft or unauthorised use of assets,
- unauthorized modification of assets.

Unauthorized disclosure of assets

58 This type of threats covers unauthorized disclosure of assets by attackers who may possess a wide range of technical skills, resources and motivation. Such attackers may also have technical awareness of the product.

T.DIS_DESIGN	Unauthorized disclosure of IC design. This threat covers the unauthorized disclosure of proprietary elements such as IC specification, IC design, IC technology detailed information, IC hardware security mechanisms specifications.
T.DIS_SOFT	Unauthorized disclosure of smartcard embedded software and data such as access control, authentication system, data protection system, memory partitioning, cryptographic programs.
T.DIS_DSOFT	Unauthorized disclosure of IC dedicated software. This threat covers the unauthorized disclosure of IC dedicated software including security mechanisms specifications and implementation.
T.DIS_TEST	Unauthorized disclosure of test information such as full results of IC testing including interpretations.

T.DIS_TOOLS	Unauthorized disclosure of development tools. This threat covers potential disclosure of IC development tools and testing tools (analysis tools, microprobing tools).
T.DIS_PHOTOMASK	Unauthorized disclosure of photomask information, used for photoengraving during the silicon fabrication process.

Theft or unauthorized use of assets

59 Potential attackers may gain access to the TOE and perform operations for which they are not authorized. For example, such attackers may personalise the TOE in an unauthorized manner, or try to gain fraudulous access to the smartcard system.

T.T_SAMPLE	Theft or unauthorized use of TOE silicon samples (e.g. bond out chips, ...).
T.T_PHOTOMASK	Theft or unauthorized use of TOE photomasks.
T.T_PRODUCT	Theft or unauthorized use of smartcard products.

Unauthorized modification of assets

60 The TOE may be subjected to different types of logical or physical attacks which may compromise security. Due to the intended usage of the TOE (the TOE environment may be hostile), the TOE security parts may be bypassed or compromised reducing the integrity of the TOE security mechanisms and disabling their ability to manage the TOE security. This type of threats includes the implementation of malicious trojan horses.

T.MOD_DESIGN	Unauthorized modification of IC design. This threat covers the unauthorized modification of IC specification, IC design including IC hardware security mechanisms specifications and realisation...
T.MOD_PHOTOMASK	Unauthorized modification of TOE photomasks.
T.MOD_DSOFT	Unauthorized modification of IC dedicated software including modification of security mechanisms.
T.MOD_SOFT	Unauthorized modification of smartcard embedded software and data.

61 The table 3.1 indicates the relationships between the smartcard phases and the threats.

Threats	**Phase 1**	**Phase 2**	**Phase 3**	**Phase 4**	**Phase 5**	**Phase 6**	**Phase 7**
Functional cloning							
T.CLON	Class II	Class II	Class I/II	Class I	Class I	Class I	Class I
Unauthorized disclosure of assets							
T.DIS_INFO	Class II						
T.DIS_DEL	Class II						
T.DIS_SOFT		Class II	Class I/II	Class I	Class I	Class I	Class I
T.DIS_DSOFT		Class II	Class I/II	Class I	Class I	Class I	Class I
T.DIS_DESIGN		Class II	Class I/II	Class I	Class I	Class I	Class I
T.DIS_TOOLS		Class II	Class II				
T.DIS_PHOTOMASK		Class II	Class II				
T.DIS_TEST			Class I/II	Class I	Class I	Class I	
Theft or unauthorised use of assets							
T.T_DEL	Class II						
T.T_SAMPLE		Class II	Class I/II	Class I	Class I		
T.T_PHOTOMASK		Class II	Class II				
T.T_PRODUCT			Class I/II	Class I	Class I	Class I	Class I
Unauthorized modification threats							
T.MOD_DEL	Class II						
T.MOD_SOFT		Class II	Class I/II	Class I	Class I	Class I	Class I
T.MOD_DSOFT		Class II	Class I/II	Class I	Class I	Class I	Class I
T.MOD_DESIGN		Class II	Class I/II	Class I	Class I	Class I	Class I
T.MOD_PHOTOMASK		Class II	Class II				

Tab. 3.1 - Threats and phases

3.4 Organisational Security policies

62 An organisational security policy is mandatory for the smartcard product usage. Nevertheless, no organisational security policy has been defined in the scope of this PP since their specifications depend essentially on the applications in which the TOE is incorporated.

Chapter 4

Security objectives

63 The security objectives of the TOE cover principally the following aspects:

- integrity and confidentiality of assets,
- protection of the TOE and associated documentation during development and production phases.

4.1 Security objectives for the TOE

64 The TOE shall use state of art technology to achieve the following IT security objectives:

O.TAMPER	The TOE must prevent physical tampering with its security critical parts.
O.CLON	The TOE functionality needs to be protected from cloning.
O.OPERATE	The TOE must ensure the continued correct operation of its security functions.
O.FLAW	The TOE must not contain flaws in design, implementation or operation.
O.DIS_MECHANISM	The TOE shall ensure that the hardware security mechanisms are protected against unauthorized disclosure.
O.DIS_MEMORY	The TOE shall ensure that sensitive information stored in memories is protected against unauthorized disclosure.
O.MOD_MEMORY	The TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorized modification.

4.2 Security objectives for the environment

4.2.1 Objectives on phase 1

O.DEV_DIS	The IC designer must have procedures to control the sales, distribution, storage and usage of the software and hardware development tools and classified documentations, suitable to maintain the integrity and the confidentiality of the assets of the TOE. It must be ensured that tools are only delivered to the parties authorized personnel. It must be ensured that confidential information such as data sheets and general information on defined assets are only delivered to the parties authorized personnel on the need to know basis.
O.SOFT_DLV	The smartcard embedded software must be delivered from the smartcard embedded software developer (Phase 1) to the IC designer through a trusted delivery and verification procedure that shall be able to maintain the integrity of the software and its confidentiality, if applicable.
O.SOFT_MECH	To achieve the level of security required by a given security target based on this Protection Profile, the smartcard embedded software shall use IC security features and security mechanisms as specified in the smartcard IC documentation (e.g. sensors,...).
O.DEV_TOOLS	The smartcard embedded software shall be designed in a secure manner, by using exclusively software development tools (compilers, assemblers, linkers, simulators etc...) and software-hardware integration testing tools (emulators) that will grant the integrity of program and data.

4.2.2 Objectives on phase 2 (development phase)

O.SOFT_ACS	Smartcard embedded software shall be accessible only by authorized personnel within the IC designer on the need to know basis.
O.DESIGN_ACS	IC specifications, detailed design, IC databases, schematics/layout or any further design information shall be accessible only by authorized personnel within the IC designer on the basis of the need to know (physical, personnel, organisational, technical procedures).
O.DSOFT_ACS	Any IC dedicated software specification, detailed design, source code or any further information shall be accessible only by authorized personnel within the IC designer on the need to know basis.
O.MASK_FAB	Physical, personnel, organisational, technical procedures during photomask fabrication (including deliveries between photomasks manufacturer and IC manufacturer) shall ensure the integrity and confidentiality of the TOE.
O.MECH_ACS	Details of hardware security mechanisms specifications shall be accessible only by authorized personnel within the IC designer on the need to know basis.
O.TI_ACS	Security relevant technology information shall be accessible only by authorized personnel within the IC designer on the need to know basis.

4.2.3 Objectives on phase 3 (manufacturing phase)

O.TOE_PRT The manufacturing process shall ensure the protection of the TOE from any kind of unauthorized use such as tampering or theft.
During the IC manufacturing and test operations, security procedures shall ensure the confidentiality and integrity of :
- TOE manufacturing data (to prevent any possible copy, modification, retention, theft or unauthorized use)
- TOE security relevant test programs, test data, databases and specific analysis methods and tools.
These procedures shall define a security system applicable during the manufacturing and test operations to maintain confidentiality and integrity of the TOE by control of:
- packaging and storage,
- traceability,
- storage and protection of manufacturing process specific assets (such as manufacturing process documentation, further data, or samples),
- access control and audit to tests, analysis tools, laboratories, and databases,
- change/modification in the manufacturing equipment, management of rejects.

O.IC_DLV The delivery procedures from the IC manufacturer shall maintain the integrity and confidentiality of the TOE and its assets.

4.2.4 Objectives on the TOE delivery process (phases 4 to 7)

O.DLV_PROTECT Procedures shall ensure protection of TOE material/ information under delivery including the following objectives:

- non-disclosure of any security relevant information,
- identification of the elements under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgement),
- physical protection to prevent external damage.
- secure storage and handling procedures are applicable for all TOEs (including rejected TOEs)
- traceability of TOE during delivery including the following parameters:
  - origin and shipment details,
  - reception, reception acknowledgement,
  - location material/information.

O.DLV_AUDIT Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non conformance to this process.

O.DLV_RESP Procedures shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and to act to be fully in accordance with the above expectations.

4.2.5 Objectives on phases 4 to 6

O.TEST_OPERATE Appropriate functionality testing of the IC shall be used in phases 4 to 6.

During all manufacturing and test operations, security procedures shall be used through phases 4, 5, 6 to maintain confidentiality and integrity of the TOE and of its manufacturing and test data.

4.2.6 Objectives on phase 7

O.USE_DIAG	Secure communication protocols and procedures shall be used between smartcard and terminal.
O.USE_SYS	The integrity and the confidentiality of sensitive data stored/ handled by the system (terminals, communications...) shall be maintained.

Chapter 5

TOE security functional requirements

65 The TOE security functional requirements define the functional requirements for the TOE using only functional requirements components drawn from the Common Criteria part 2.

66 The permitted operations such as iteration, assignment, selection, or refinement will have to be defined in a Security Target, compliant with this Protection Profile. The rules defined by the TOE Security Policy, the access control Security Functions Policy and the information flow control Security Functions Policy could be different at phase 3 compared to phases 4 to 7. The minimum strength of function level for the TOE security requirements is SOF-high.

5.1 Functional requirements applicable to phase 3 only (testing phase)

5.1.1 User authentication before any action (FIA_UAU.2)

67 The TOE security functions shall require each user to be successfully authenticated before allowing any other TOE security functions-mediated actions on behalf of that user.

5.1.2 User Identification before any action (FIA_UID.2)

68 The TOE security functions shall require each user to identify itself before allowing any other TOE security functions-mediated actions on behalf of that user.

5.1.3 User Attribute Definition (FIA_ATD.1)

69 The TOE security functions shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].

5.1.4 TOE Security Functions Testing (FPT_TST.1)

70 The TOE security functions shall run a suite of self tests [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]] to demonstrate the correct operation of the TOE security functions.

71 The TOE security functions shall provide authorised users with the capability to verify the integrity of TOE security functions data.

72 The TOE security functions shall provide authorised users with the capability to verify the integrity of stored TOE security functions executable code.

5.1.5 Stored Data Integrity Monitoring (FDP_SDI.1)

73 The TOE security functions shall monitor user data stored within the TOE scope of control for [assignment: integrity errors] on all objects, based on the following attributes: [assignment: user data attributes].

5.2 Functional requirements applicable to phases 3 to 7

Security Management

Functions	Actions to be considered
FIA_UAU.2	- management of the authentication data by an administrator, - management of the authentication data by the user associated with this data.
FIA_UID.2	- management of the user identities.
FPT_TST.1	- management of the conditions under which TOE security functions self-testing occurs, such as during initial start-up, regular interval, or under specified conditions.
FMT_MOF.1	- managing the group of roles that can interact with the functions in the TOE security functions.
FMT_MSA.1	- managing the group of roles that can interact with the security attributes.
FMT_SMR.1	- managing the group of users that are part of a role.
FMT_MSA.3	- managing the group of roles that can specify initial values. - managing the permissive or restrictive setting of default values for a given access control Security Functions Policy.
FDP_ACF.1	- managing the attributes used to make explicit access or denial based decisions.
FDP_IFF.1	- managing the attributes used to make explicit access based decisions.

Tab. 5.1 - Actions to be considered for the management functions in FMT Management class

5.2.1 Management of security functions behaviour (FMT_MOF.1)

74 The TOE security functions shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: list of functions] to [assignment: the authorised identified roles].

5.2.2 Management of security attributes (FMT_MSA.1)

75 The TOE security functions shall enforce the [assignment: access control security functions policy, information flow control security functions policy] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles].

5.2.3 Security roles (FMT_SMR.1)

76 The TOE security functions shall maintain the roles [assignment: the authorised identified roles].

77 The TOE security functions shall be able to associate users with roles.

5.2.4 Static Attribute Initialisation (FMT_MSA.3)

78 The TOE security functions shall enforce the [assignment: access control security functions policy, information flow control security functions policy] to provide [selection: restrictive, permissive, other property] default values for security attributes that are used to enforce the security functions policy.

79 The TOE security functions shall allow the [assignment: the authorised identified roles] to specify alternate initial values to override the default values when an object or information is created.

5.2.5 Complete Access Control (FDP_ACC.2)

80 The TOE security functions shall enforce the [assignment: access control security functions policy] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the security functions policy.

81 The TOE security functions shall ensure that all operations between any subject in the TOE scope of control and any object within the TOE scope of control are covered by an access control security functions policy.

5.2.6 Security Attribute Based Access Control (FDP_ACF.1)

82 The TOE security functions shall enforce the [assignment: access control security functions policy] to objects based on [assignment: security attributes, named groups of security attributes].

83 The TOE security functions shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed [assignment:

rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

84 The TOE security functions shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].

85 The TOE security functions shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

5.2.7 Subset Information Flow Control (FDP_IFC.1)

86 The TOE security functions shall enforce the [assignment: information flow control security functions policy] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled objects covered by the security functions policy].

87 *Note: this security functional requirement is applicable to the IC dedicated software.*

5.2.8 Simple Security Attributes (FDP_IFF.1)

88 The TOE security functions shall enforce the [assignment: information flow control security functions policy] based on the following types of subject and information security attributes [assignment: the minimum number and type of security attributes].

89 The TOE security functions shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

90 The TOE security functions shall enforce the [assignment: additional information flow control security functions policy rules].

91 The TOE security functions shall provide the following [assignment: list of additional security functions policy capabilities].

92 The TOE security functions shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

93 The TOE security functions shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

94 *Note: this security functional requirement is applicable to the IC dedicated software.*

5.2.9 Potential Violation Analysis (FAU_SAA.1)

95 The TOE security functions shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TOE security policy.

96 The TOE security functions shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment: subset of defined auditable events] known to indicate a potential security violation;

b) [assignment: any other rules].

5.2.10 Unobservability (FPR_UNO.1)

97 The TOE security functions shall ensure that [assignment: list of users and/or subjects] are unable to observe the operation [assignment: list of operations] on [assignment: list of objects] by [assignment: list of protected users and/or subjects].

5.2.11 Notification of Physical Attack (FPT_PHP.2)

98 The TOE security functions shall provide unambiguous detection of physical tampering that might compromise the TOE security functions.

99 The TOE security functions shall provide the capability to determine whether physical tampering with the TOE security functions’s devices or TOE security functions' s elements has occurred.

100 For [assignment: list of TOE security functions devices/elements for which active detection is required], the TOE security functions shall monitor the devices and elements and notify [assignment: a designated user or role] when physical tampering with the TOE security functions’s devices or TOE security functions's elements has occurred.

5.2.12 Resistance to Physical Attack (FPT_PHP.3)

101 The TOE security functions shall resist [assignment: physical tampering scenarios] to the [assignment: list of TOE security functions devices/elements] by responding automatically such that the TOE security policy is not violated.

102 *Note: as described in the CC part 2 annexes, technology limitations and relative physical exposure of the TOE must be considered.*

Chapter 6

TOE security assurance requirements

103 The assurance requirements is EAL 4 augmented of additional assurance components listed in the following sections.

104 These components are hierarchical ones to the components specified in EAL 4.

6.1 ADV_IMP.2 Implementation of the TSF

Developer actions elements:

105 The developer shall provide the implementation representation for the entire TOE security functions.

Content and presentation of evidence elements:

106 The implementation representation shall unambiguously define the TOE security functions to a level of detail such that the TOE security functions can be generated without further design decisions.

107 The implementation representation shall be internally consistent.

108 The implementation representation shall describe the relationships between all portions of the implementation.

Evaluator action elements:

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

110 The evaluator shall determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

6.2 ALC_DVS.2 Sufficiency of security measures

Developer actions elements:

111 The developer shall produce development security documentation.

Content and presentation of evidence elements:

112 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 the TOE design and implementation in its development environment.

113 The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

114 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:

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

116 The evaluator shall confirm that the security measures are being applied.

6.3 AVA_VLA.4 Highly resistant

Developer actions elements:

117 The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TOE security policy.

118 The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

119 The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

120 The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

121 The evidence shall show that the search for vulnerabilities is systematic.

122 The analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

Evaluator action elements:

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

124 The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

125 The evaluator shall perform an independent vulnerability analysis.

126 The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

127 The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a high attack potential.

Chapter 7

Rationale

7.1 Introduction

128 This chapter presents the evidence used in the PP evaluation. This evidence supports the claims that the PP is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment.

7.2 Security Objectives rationale

129 This section demonstrates that the stated security objectives address all of the security environment aspects identified.

7.2.1 Threats and security objectives

130 The following tables show which security objectives counter which threats phase by phase.

Phase 1

131 During Phase 1, the smartcard embedded software is being developed and the IC pre-personalisation requirements are specified. Phase 1 is outside the scope of this Protection Profile and only threats on the assets exchanged between the IC designer and the smartcard embedded software developer are relevant to this PP.

132 Such threats are identified in sections 3.3.1 and 3.3.2 of the PP:

- T.CLON,
- T.DIS_INFO,
- T.DIS_DEL,
- T.MOD_DEL,
- T.T_DEL.

133 Since the TOE is under construction during this phase, only security objectives for the environment are described during this phase.

134 Table 7.1 indicates that each to be countered threat during phase 1 is mapped to at least one security objective. No organisational security policy has to be considered.

Threats/ Objectives	O.DEV_DIS	O.SOFT_DLV	O.DEV_TOOLS	O.SOFT_MECH
T.CLON	X	X	X	X
T.DIS_INFO	X			
T.DIS_DEL		X		
T.MOD_DEL		X		
T.T_DEL		X		

Tab. 7.1 - Mapping of security objectives to threats at phase 1

135 O.DEV_DIS addresses all the threats on the assets transmitted from the IC designer to the smartcard embedded software developer during the smartcard development which is the major concern of T.DIS_INFO. This objective also partially addresses the T.CLON threat since it requires well defined and controlled procedures to the delivery of any IC proprietary assets.

136 O.SOFT_DLV addresses all the threats applicable to the delivery of the smartcard embedded software to the IC designer since it requires the application of a trusted delivery and verification procedure (T.T_DEL) maintaining the integrity (T.MOD_DEL) and the confidentiality of the software if applicable (T.DIS_DEL, T.T_DEL).

137 The threats identified at phase 1 are countered by the security objectives in the way described above; nevertheless, T.CLON is partially countered by the four objectives which prevent the functional cloning of the TOE but can not avoid it completely.

Phase 2

138 Since the TOE is under construction during this phase (the IC is being developed), only security objectives for the environment are described during this phase. There is also no assumption for this phase.

139 Table 7.2 shows the mapping of security objectives to threats during phase 2. T.T_PRODUCT and T.DIS_TEST are not applicable to this phase as referred by the table 3.1 of the PP. No organisational security policy has to be considered.

Threats/Objectives	O.SOFT _ACS	O.DESIGN _ACS	O.DSOFT _ACS	O.MASK _FAB	O.MECH _ACS	O.TI_ ACS
T.CLON	X	X	X	X	X	X
T.DIS_DESIGN		X			X	X
T.DIS_SOFT	X					

Tab. 7.2 - Mapping of security objectives to threats at phase 2

Threats/Objectives	O.SOFT_ACS	O.DESIGN_ACS	O.DSOFT_ACS	O.MASK_FAB	O.MECH_ACS	O.TI_ACS
T.DIS_DSOFT			X			
T.DIS_TOOLS		X				
T.DIS_PHOTOMASK				X		
T.T_SAMPLE		X				
T.T_PHOTOMASK				X		
T.MOD_DESIGN		X			X	X
T.MOD_DSOFT			X			
T.MOD_SOFT	X					
T.MOD_PHOTOMASK				X		

Tab. 7.2 - Mapping of security objectives to threats at phase 2

140 O.SOFT_ACS addresses the threats T.DIS_SOFT and T.MOD_SOFT by restricting access to the smartcard embedded software when delivered to the IC designer only to authorized personnel.

141 O.DESIGN_ACS addresses the threats T.DIS_DESIGN, T.DIS_TOOLS, T.MOD_DESIGN, T.T_SAMPLE by restricting access to the IC design assets only to authorized personnel.

142 O.MECH_ACS addresses the threats T.DIS_DESIGN and T.MOD.DESIGN by limiting access to the hardware security mechanisms specifications only to authorized personnel.

143 O.TI_ACS addresses the threats T.DIS_DESIGN, T.MOD_DESIGN by restricting access to the security relevant information on IC technology during the IC design to authorized personnel.

144 O.DSOFT_ACS addresses the threats T.DIS_DSOFT, T.MOD_DSOFT by restricting access to the IC dedicated software information only to authorized personnel.

145 O.MASK_FAB addresses T.DIS_PHOTOMASK, T.T_PHOTOMASK, T.MOD_PHOTOMASK by providing procedures to ensure the confidentiality and the integrity of the TOE during photomask fabrication and delivery between the IC manufacturer and the photomasks manufacturer.

146 The T.CLON threat is partially countered by all of the objectives described above since they limit the possibility to access any sensitive security relevant information of the TOE during phase 2.

Phases 3 to 7

Security objectives for the environment at phase 3

147 At phase 3, the TOE is constructed and tested then operational. Security Objectives for the environment have been developed for phase 3 and address the TOE environment during this phase.

148 This section explains the mapping of security objectives for the environment to threats during the manufacturing process, as detailed in table 7.3. The mapping of TOE security objectives to threats during phase 3 is described in table 7.4.

Threats/Objectives	O.TOE_ PRT	O.IC_ DLV
T.CLON	X	X
T.DIS_DESIGN	X	
T.DIS_SOFT	X	
T.DIS_DSOFT	X	
T.DIS_TEST	X	
T.DIS_TOOLS	X	
T.DIS_PHOTOMASK	X	
T.T_SAMPLE	X	X
T.T_PHOTOMASK	X	
T.T_PRODUCT	X	X
T.MOD_DESIGN	X	
T.MOD_DSOFT	X	
T.MOD_SOFT	X	
T.MOD_PHOTOMASK	X	

Tab. 7.3 - Mapping security objectives for the environment to threats at phase 3

149 O.TOE_PRT addresses all the threats by ensuring the protection of the TOE during the manufacturing process, pre-personnalisation and testing, since it provides a security system applicable to the IC manufacturing and testing phase to ensure the confidentiality and integrity of the TOE.

150 O.IC_DLV addresses the threats T.T_SAMPLE, T.T_PRODUCT by providing a well defined and controlled delivery procedure of the TOE.

151 The T.CLON threat is partially countered by all of the objectives described above since they limit the possibility to access any sensitive security relevant information on the TOE during the manufacturing and testing phase (phase 3).

TOE security objectives from phases 3 to 7

152 The table 7.4 maps the TOE security objectives to the threats identified at phases 3 to 7.

Threats/ Objectives	O.TAMPER	O.CLON	O. OPERATE	O.FLAW	O.DIS_ MECHANISM	O.DIS_ MEMORY	O.MOD_ MEMORY
T.CLON		X					
T.DIS_DESIGN	X				X		
T.DIS_SOFT	X					X	
T.DIS_DSOFT	X					X	
T.DIS_TEST	X					X	
T.T_SAMPLE			X				
T.T_PRODUCT			X				
T.MOD_DESIGN	X		X	X			
T.MOD_DSOFT	X		X	X			X
T.MOD_SOFT	X		X	X			X

Tab. 7.4 - Mapping TOE security objectives to threats at phase 3 to 7

153 O.TAMPER addresses the threats T.DIS_DESIGN, T.DIS_SOFT, T.DIS_DSOFT, T.DIS_TEST, T.MOD_DESIGN, T.MOD_DSOFT, T.MOD_SOFT by ensuring the integrity protection of the security critical parts of the TOE and protecting them from any disclosure.

154 O.CLON addresses the threat T.CLON.

155 O.OPERATE addresses the threats T.T_SAMPLE, T.T_PRODUCT, T.MOD_DESIGN, T.MOD_DSOFT, T.MOD_SOFT by providing the TOE protection against unauthorized use (modification of the TOE or theft as an example).

156 O.FLAW addresses the threats T.MOD_DESIGN, T.MOD_DSOFT, T.MOD_SOFT by preventing any unauthorized modification of the TOE during its design, production or operation.

157 O.DIS_MECHANISM addresses the threats T.DIS_DESIGN by preventing any unauthorized disclosure of the hardware security mechanisms.

158 O.DIS_MEMORY addresses the threats T.DIS_SOFT, T.DIS_DSOFT, T.DIS_TEST by protecting all information contained in memories from unauthorized access.

159 O.MOD_MEMORY addresses the threats T.MOD_DSOFT, T.MOD_SOFT by protecting all information contained in memories from any unauthorized modification.

160 It has to be noted that the threats T.DIS_TOOLS, T.T_PHOTOMASK, T.DIS_PHOTOMASK, T.MOD_PHOTOMASK are countered by security objectives for the environment during the manufacturing and testing phase (phase 3).

7.2.2 Assumptions and security objectives

161 The following tables show which security objectives counter which threats phase by phase.

Phase 1

162 Table 7.5 indicates the relationships between assumptions and security objectives for the environment. It shows that each assumption is covered by at least one security objective for the environment.

Assumptions/ Objectives	O.DEV_DIS	O.SOFT_DLV	O.DEV_TOOLS	O.SOFT_MECH
A.SOFT_ARCHI			X	X
A.DEV_ORG		X	X	

Tab. 7.5 - Mapping of security objectives to assumptions at phase 1

TOE delivery process (phase 4 to 7)

163 Table 7.6 indicates the relationships between assumptions and security objectives for the environment. It shows that each assumption is covered by at least one security objective for the environment.

Assumptions/ Objectives	O.DLV_PROTECT	O.DLV_AUDIT	O. DLV_RESP
A.DLV_PROTECT	X		
A.DLV_AUDIT		X	
A.DLV_RESP			X

Tab. 7.6 - Mapping of security objectives to assumptions at phases 4 to 7

Phases 4 to 6

164 Table 7.7 indicates the relationships between assumptions and security objectives for the environment. It shows that each assumption is covered by at least one security objective for the environment.

Assumptions/ Objectives	O.TEST_OPERATE
A.USE_TEST	X
A.USE_PROD	X

Tab. 7.7 - Mapping of security objectives to assumptions at phases 4 to 6

Phase 7

165 Table 7.8 indicates the relationships between assumptions and security objectives for the environment at phase 7. It shows that each assumption is covered by at least one security objective for the environment.

Assumptions/ Objectives	O.USE_SYS	O.USE_DIAG
A.USE_SYS	X	
A.USE_DIAG		X

Tab. 7.8 - Mapping of security objectives to assumptions at phase 7

7.3 Security requirements rationale

166 The **Security requirements rationale** shall demonstrate that the set of security requirements (TOE and environment) is suitable to meet the security objectives.

7.3.1 Security functional requirements rationale

167 This section demonstrates that the combination of the security requirements is suitable to satisfy the identified TOE security objectives.

168 Each of the TOE security objectives is addressed by either functional or assurance requirements.

169 The following table demonstrates which requirements contribute to the satisfaction of each TOE security objective.

Requirements	O.TAMPER	O.CLON	O.OPERATE	O.FLAW	O.DIS_ MECHANISM	O.DIS_ MEMORY	O.MOD_ MEMORY
EAL4 requirements				X			
FIA_UAU.2 (Phase 3)	X	Partial	X		X	X	X
FIA_UID.2 (Phase 3)	X	Partial	X		X	X	X
FIA_ATD.1 (Phase 3)	X	Partial	X		X	X	X
FPT_TST.1 (Phase 3)			X				X
FDP_SDI.1 (Phase 3)							X
FMT_MOF.1			X				
FMT_MSA.1			X				
FMT_SMR.1			X				
FMT_MSA.3			X				
FDP_ACC.2		Partial	X		X	X	X
FDP_ACF.1		Partial	X		X	X	X
FDP_IFC.1		Partial	X		X	X	X
FDP_IFF.1		Partial	X		X	X	X
FAU_SAA.1		Partial	X				
FPR_UNO.1	X	Partial	X		X	X	
FPT_PHP.2	X	Partial	X		X	X	X
FPT_PHP.3	X	Partial	X		X	X	X

Tab. 7.9 - Mapping of security requirements and TOE security objectives

170 This section describes why the security requirements are suitable to meet each of the TOE security objectives.

171 The EAL4 assurance requirements contribute to the satisfaction of the O.FLAW security objective. They are suitable because they provide the assurance that the TOE is designed, implemented and operates so that the IT functional requirements are correctly provided.

172 At phase 3 (testing phase), the identification and authentication functions (FIA_UAU.2, FIA_UID.2, FIA_ATD.1) are necessary to ensure that the testing operations of the TOE are done under control and that only authorized employees/ processes will be able to run the testing operations of the TOE. This set of functional requirements is required by all the TOE security objectives during this phase (the case of O.FLAW is described in paragraph 171). FIA_UID.2, FIA_ATD.1, FIA_UAU.2 provide the capability to identify and authenticate the user prior to performing any functions for the user.

173 The objective O.CLON is partially countered by the functional requirements listed in the table 7.9 since they provide the capability to limit the operations on the TOE to a set of authorised operations by authorised users, but in fact, this objective would require a specific function to avoid the functional cloning of the TOE which is in fact not the case.

174 At phase 3, FPT_TST.1 ensures the correct operation of security functions by providing security functionalities testing during phase 3, required by the objective O. OPERATE and O.MOD_MEMORY (integrity of TOE security functions data that are stored in memories). This is important for the TOE especially for the security controls when changing from phase 3 to the others.

175 At phase 3, FDP_SDI.1 provides protection against integrity errors that may affect all user information stored in memories, required by the O.MOD_MEMORY objective.

176 At all phases, FAU_SAA.1 provides the capability of indicating a potential violation of the TOE Security Policy. The rules defined by the TOE Security Policy could be different at phase 3 compared to phases 4 to 7. This security function works in support of the O.OPERATE.

177 At all phases, FDP_ACC.2 will provide the protection of all information contained in memories and of the hardware security mechanisms, required by the objectives O.DIS_MEMORY, O.MOD_MEMORY, O.DIS_MECHANISM and O.OPERATE. The rules defined by the Access control security functions policy could be different at phase 3 compared to phases 4 to 7. FDP_ACF.1 enforces also these objectives. For the IC dedicated software, FDP_IFC.1 and FDP_IFF.1 are also applicable to provide the capability to ensure a subset information flow control, required by the objectives listed above.

178 At all phases, the functions FMT_MOF.1, FMT_MSA.1, FMT_SMR.1, FMT_MSA.3 provide the administration of security functions and security attributes during all the phases, required by the O.OPERATE objective. This is a major concern for the TOE especially for changes from one phase to another under the TOE control.

179 At all phases, the unobservability functional requirement FPR_UNO.1 provides the protection against unauthorized disclosure and use of sensitive information, required by the objectives O.TAMPER, O.OPERATE, O.DIS_MEMORY, O.DIS_MECHANISM since unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used. There is no potential conflict with identification and authentication requirements (FIA_UAU.2, FIA_UID.2, FIA_ATD.1) because there is only one authenticated user at a time and internal operations on behalf of that user shall not be observable for unauthorized users.

180 At all phases, FPT_PHP.2 provides the capability to notify physical attacks to some extents, required, due to the TOE definition, by all the objectives (the case of O.FLAW is described in paragraph 171).

181 At all phases, FPT_PHP.3 provides the capability to resist to physical attacks, required, due to the TOE definition, by all the objectives (the case of O.FLAW is described in paragraph 171).

7.3.2 Security functional requirements dependencies

182 This section demonstrates that all dependencies between security functional requirements components included in this PP are satisfied.

183 The following table lists all functional components, with a numeric number. The dependencies of each component are listed alongside that component with a reference to the line number of the component which satisfies them. Component reference line numbers followed by (H) indicate that the dependency is satisfied by a hierarchical component to that referenced.

Number	NAME	Dependent on	Line number
1	FIA_UAU.2	FIA_UID.1	H(2)
2	FIA_UID.2	no dependencies	-
3	FIA_ATD.1	no dependencies	-
4	**FPT_TST.1**	**FPT_AMT.1**	**See para. 186**
5	FDP_SDI.1	no dependencies	-
5	FAU_SAA.1	**FAU_GEN.1**	**See para. 185**
6	FMT_MOF.1	FMT_SMR.1	8
7	FMT_MSA.1	FMT_SMR.1, FDP_ACC.1 or FDP_IFC.1	8, H(10), 12
8	FMT_SMR.1	FIA_UID.1	H(2)
9	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	7, 8
10	FDP_ACC.2	FDP_ACF.1	11
11	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	H(10), 9
12	FDP_IFC.1	FDP_IFF.1	13
13	FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	12, 9
14	FPR_UNO.1	no dependencies	-
15	FPT_PHP.2	FMT_MOF.1	6
16	FPT_PHP.3	no dependencies	-

Tab. 7.10 -Functional dependencies analysis

184 Table 7.10 shows that the functional components dependencies are satisfied by any functional components of the PP except for the components stated in bold characters, which are discussed hereafter.

185 The dependency of FAU_SAA.1 with FAU_GEN.1 is not applicable to the TOE; the FAU_GEN component forces many security relevant events to be recorded (due to dependencies with other functional security components) and this is not achievable to a smartcard IC considering state-of-the-art implementation. It is then assumed that the function FAU_SAA.1 may still be used and the specific audited events will have to be defined in the ST independently with FAU_GEN.1.

186 The dependency of FPT_TST.1 with FPT_AMT.1 is not clearly relevant for a smartcard IC; FPT_TST.1 is self consistent for the TOE (hardware and firmware) and does not require the FPT_AMT.1 function (Abstract Machine Testing) which seems to be more appropriate for operating systems TOEs.

7.3.3 Strength of function level rationale

187 Due to the definition of the TOE, it is very important that the claimed SOF should be high since the product critical security mechanisms have to be only defeated by attackers possessing a high level of expertise, opportunity and resources, successful attack being judged to be beyond normal practicality.

7.3.4 Security assurance requirements rationale

188 The assurance requirements of this Protection Profile are summarized in the following table 7.11.

Requirement	Name	Type
EAL4	Methodically Designed, Tested and Reviewed	Assurance level
ADV_IMP.2	Implementation of the TSF	Higher hierarchical component
ALC_DVS.2	Sufficiency of security measures	Higher hierarchical component
AVA_VLA.4	Highly resistant	Higher hierarchical component

Tab. 7.11 - PP assurance requirements

Evaluation assurance level rationale

189 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. EAL4 represents the highest practical level of assurance expected for a commercial grade product. 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.

190 The assurance level of EAL4 is achievable, since it requires no specialist techniques on the part of the developer.

Assurance augmentations rationale

191 Additional assurance requirements are also required due to the definition of the TOE.

192 ADV_IMP.2 Implementation of the TSF

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. IC dedicated software source code and IC hardware drawings are examples of TSF implementation representation.

This assurance component is a higher hierarchical component to EAL 4 (only ADV_IMP.1). It is important for a smartcard IC that the evaluator evaluates the implementation representation of the entire TSF and determine if the functional requirements in the Security Target are addressed by the representation of the TSF.

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.

193 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.

This assurance component is a higher hierarchical component to EAL4 (only ALC_DVS.1). Due to the nature of the TOE, there is a need for any justification of the sufficiency of these procedures to protect the confidentiality and integrity of the TOE.

ALC_DVS.2 has no dependencies.

194 AVA_VLA.4 Highly resistant

Due to the definition 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. The attacker is assumed to be thoroughly familiar with the specific

implementation of the TOE. The attacker is presumed to have a high level of technical sophistication.

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”. All these dependencies are satisfied by EAL4.

7.3.5 Security requirements are mutually supportive and internally consistent

195 The purpose of this part of the PP Rationale is to show that the security requirements are mutually supportive and internally consistent.

196 EAL4 is an established set of mutually supportive and internally consistent assurance requirements.

197 The dependencies analysis for the additional assurance components in the previous section has shown that the assurance requirements are mutually supportive and internally consistent (all the dependencies have been satisfied).

198 The dependencies analysis for the functional requirements described above demonstrates mutual support and internal consistency between the functional requirements.

199 Inconsistency between functional and assurance requirements can only arise if there are functional-assurance dependencies that are not met, a possibility which has been shown not to arise.

Annex A

Glossary

Embedded software

Software embedded in a smartcard IC. Embedded software may be in any part of the non-volatile memory of the IC.

Integrated Circuit (IC)

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

IC Dedicated Software

IC proprietary software which is required for testing purpose ; it may either be IC embedded software (also known as IC firmware) or tests programmes outside the IC.

IC designer

Institution (or its agent) responsible for the IC development.

IC manufacturer

Institution (or its agent) responsible for the IC manufacturing, testing, and pre-personalisation.

IC packaging manufacturer

Institution (or its agent) responsible for the IC packaging and testing.

IC prepersonnalisation data

Any data that is stored in the non-volatile memory for shipment between phases.

Personaliser

Institution (or its agent) responsible for the smartcard personalisation and final testing.

Smartcard

A card according to ISO 7816 requirements which has a non volatile memory and a processing unit embedded within it.

Smartcard embedded software

Composed of embedded software in charge of generic functions of the Smartcard IC such as Operating system, general routines and interpreters (smartcard basic software) and embedded software dedicated to the applications (smartcard application software).

Smartcard embedded software developer

Institution (ot its agent) responsible for the smartcard embedded software development and the specification of IC pre-personalisation requirements.

System integrator

Institution (ot its agent) responsible for the smartcart product system integration (terminal software developper, system developper ...).

Abbreviations

CC

Common Criteria Version 2.0.

EAL

Evaluation Assurance Level.

IT

Information Technology.

PP

Protection Profile.

SF

Security function.

SOF

Strength of function.

ST

Security Target.

TOE

Target of Evaluation.

TSC

TSF Scope of control.

TSF

TOE Security functions.

TSFI

TSF Interface.

TSP

TOE Security Policy.