Common Criteria for IT Security Evaluation
Protection Profile

Smartcard Integrated Circuit
Protection Profile

Issue October 1997

Registered at the French Certification Body under the number PP/9704

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

- Motorola Semiconductors

18, Rue Grange Dame Rose
BP 95 78143 VELIZY
Telephone : (+33) 1 34 63 59 66 Fax : (+33) 1 34 63 58 61

- Philips Semiconductors

Röhren -und HalbleiterwerkeStresemannallee 101
D- 22529 Hamburg
Telephone : (+49) 40 5613 2430 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 Semiconductors AG

HL CC PE
P.O. Box 801760
D-81617 Munich
Telephone : (+49) 89 636 253 20 Fax : (+49) 89 636 222 14

- SGS-Thomson Microelectronics

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

- Texas-Instruments Semiconductors

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

This document is paginated from i to ii and from 1 to 37

Table of contents

Chapter 5

Chapter 6

Annex A

Chapter 1

PP introduction

1.1 PP Identification

Title: Smartcard Integrated Circuit Protection Profile.

Registration: registered at French Certification Body under the number PP/9704.

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

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

1.2 PP overview

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

- Motorola Semiconductors,
- Philips Semiconductors,
- Siemens Semiconductors,
- SGS-Thomson Microelectronics,
- Texas-Instruments Semiconductors.

4 The intent of this Protection Profile is to specify functional and assurance requirements applicable to a smartcard Integrated Circuit.

5 A smartcard could be considered as a credit card sized plastic cards 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).

6 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 design, embedded software development (firmware), application software development, integration and co-testing and mask fabrication.

- the IC production stage: IC manufacturing, testing, preparation and shipping to the IC assembly line.

- the smartcard production stage: smartcard IC assembly (and testing), smartcard manufacturing, printing (and testing), smartcard preparation and shipping to the personalisation line.

7 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.

8 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.

9 The assets protected are in general secret data as Personal Identification Numbers, Balance Value (Stored Value Cards), and Personal Data Files. Another set of assets 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.

10 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 with the exception of those that are applicable when the smartcard is its end usage in the system working according to its specifications.

11 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.

12 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.

13 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 integrated circuit with its firmware, without the application embedded software development sub-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 of the TOE and its supporting 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 IT functional requirements, the TOE IT Assurance requirements and the security requirements for the IT environment.

14 The Assurance level for this PP is EAL 4 augmented.

Chapter 2

TOE Description

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 features of the TOE.

2.1 Product type

15 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 Protection Profile[1].

16 The typical TOE is composed of a processing unit, security components, I/O ports and volatile and non-volatile memories.The TOE may optionally include any IC designer/manufacturer proprietary firmware and/or pre-personalisation data.

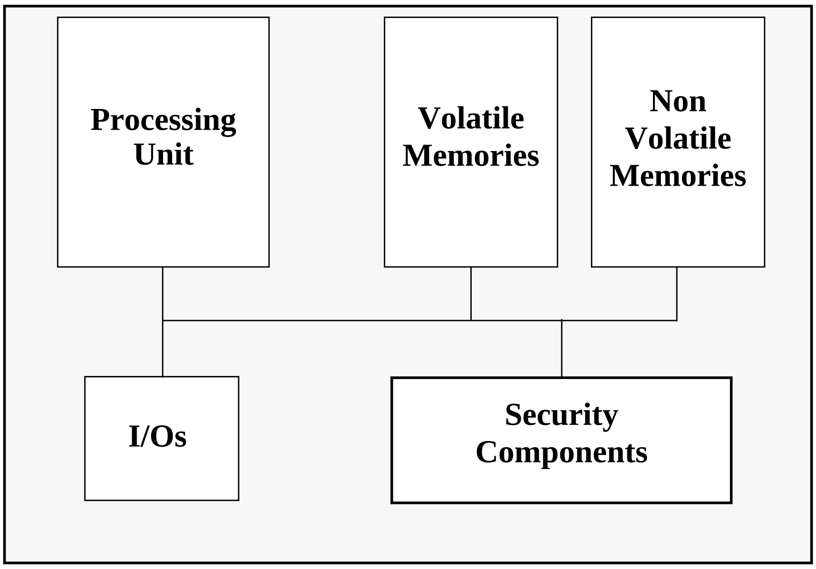

Fig. 2.1 - Typical Target of Evaluation

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

2.2 Smartcard Product Life-cycle

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

Phase 1	Smartcard software development	**the smartcard software developer** is in charge of the smartcard embedded software development and the specification of pre-personalisation requirements,
Phase 2	IC Development	**the IC designer** designs the integrated circuit, develops IC firmware if applicable, provides information, software or tools to the smartcard software developer, and receives the software from the developer, through **trusted delivery and verification procedures**. From the IC design, IC firmware 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, testing, and 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 application 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.

18 The limits of the TOE 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.

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

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

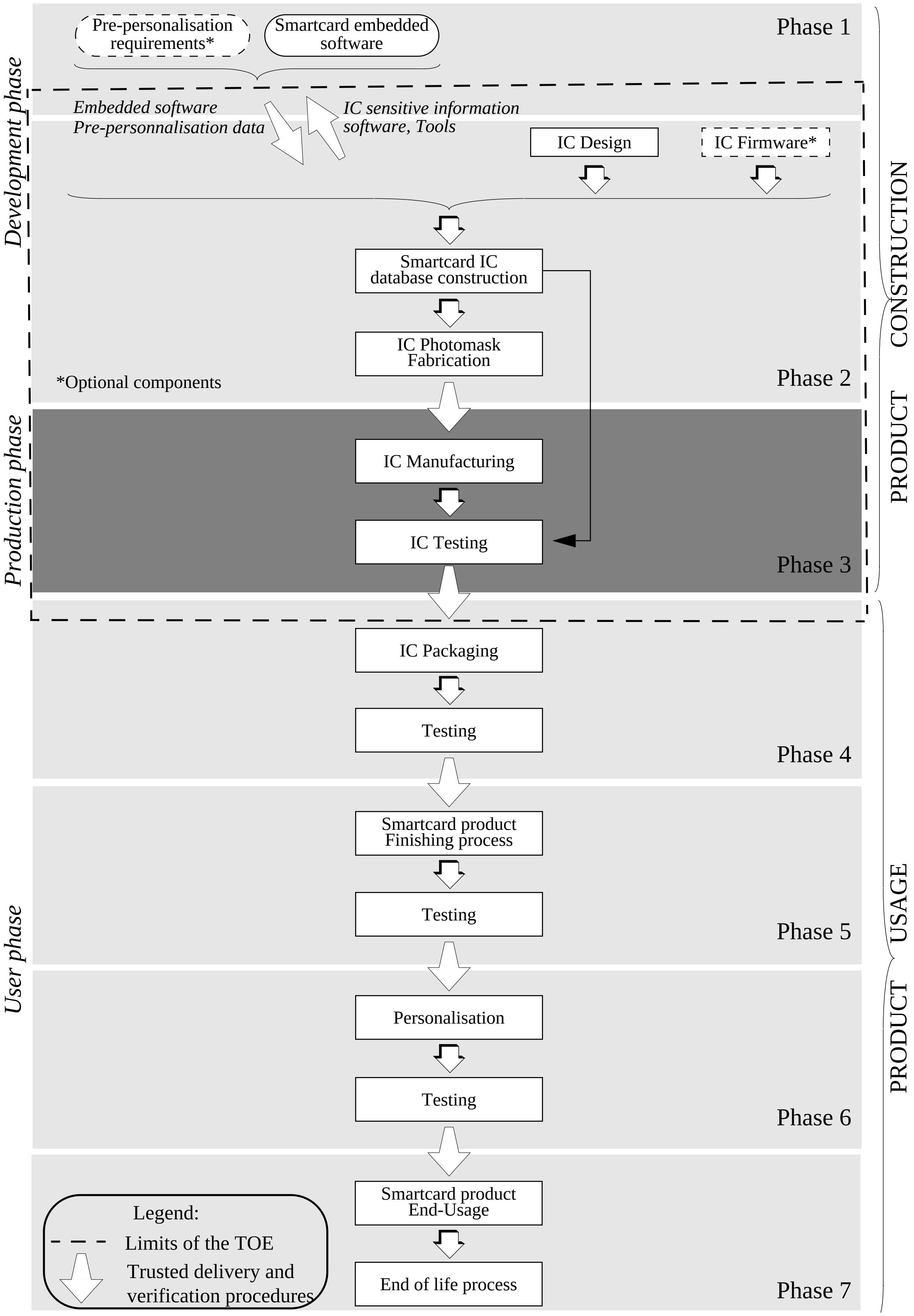

Fig. 2.2 - Smartcard product life-cycle

21 These different phases may be performed at different sites; procedures on the delivery process of the TOE must 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.

22 These procedures must be compliant with the secure usage assumptions [A_DLV] developed in section 3.4.2.

2.3 TOE environment

23 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 Development Environment

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

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

26 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. Storage of sensitive documents, databases on tapes, diskettes, and printed circuit layout information are in appropriately locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

27 Reticles and photomasks are generated from the verified IC databases; the former are used in the silicon Wafer-fab processing. Testing, programming and deliveries of the TOEs then take place. When these are done offsite, they must be transported and worked on in a secure environment with accountability and traceability of all (good and bad) product. During the transfer of sensitive data electronically, procedures must be established to ensure that the data arrives only at the destination

and is not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies).

2.3.2 Production environment

28 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.

29 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.

30 Whether carried out under the control of the IC manufacturer or the packaging manufacturer, wafers must 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. Further testing occurs, followed by smartcard personalisation, retesting then delivery to the smartcard issuer.

2.3.3 User environment

31 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.

32 The 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

33 During its construction usage, the TOE may be under several life logical phases, as described by figure 2.3. These phases are sorted under a logical controlled sequence. The change from one phase to the next is under the TOE control.

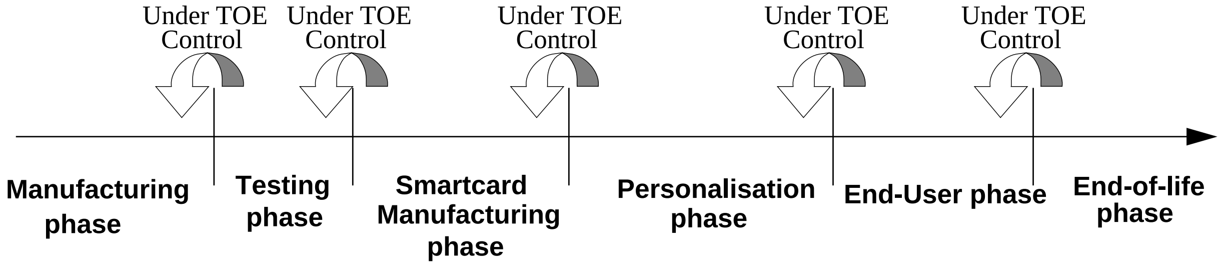

Fig. 2.3 - TOE logical phases

2.5 TOE Intended usage

34 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....).
- multimedia commerce and Intellectual Property Rights protection.

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

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

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

Phase 4	- the packaging manufacturer (**administrator**), - the smartcard embedded software developer, - the system integrators such as the terminal software developer.
Phase 5	- the smartcard product manufacturer **(administrator**), - the smartcard software developer, - the system integrators such as the terminal software developer.
Phase 6	- the personaliser (**administrator**), - the smartcard issuer (**administrator**), - the smartcard embedded software developer, - the system integrators such as the terminal software developer.

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

37 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

Security Environment

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

3.1 Assets

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

- the application data of the TOE (such as prepersonalisation requirements, IC and system specific data),
- the application programs (including operating system programs),
- the IC firmware programs, (optional)
- the IC specification, design, development tools and technology.

39 The TOE itself is therefore an asset.

40 Assets have to be protected in terms of confidentiality, integrity and availability.

3.2 Threats

41 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 or by environmental manipulations, or by specific hardware manipulations or by any other types of attacks...

42 Threats have to be split in:

- threats addressed by the TOE (class I),
- threats addressed by the TOE environment (class II).

3.2.1 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.

3.2.2 Threats on phase 1

43 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 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 software developer to the IC designer.

44 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 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 prepersonalisation 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 prepersonalisation requirements) delivered to the IC designer;

T.T_DEL theft of the smartcard embedded software and any additional application data (such as prepersonalisation requirements) delivered to the IC designer.

3.2.3 Threats on phases 2 to 7

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

- unauthorized disclosure of assets,
- theft of assets,
- unauthorized modification of assets.

46 Unauthorized disclosure of assets

47 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_APROG unauthorized disclosure of application programs and data such as access control, authentication system, data protection system, memory partitioning, cryptographic programs.

T.DIS_FPROG unauthorized disclosure of firmware programs.
This threat covers the unauthorized disclosure of firmware programs including firmware security mechanisms specifications and implementation.

T.DIS_TEST unauthorized disclosure of test information such as test programs, 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 for the silicon process

48 Theft or unauthorized use of assets

49 Potential attackers may gain access to the TOE and perform operations for which they are not authorized. For example, such attackers may personalise the product in an uauthorized 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.

50 Unauthorized modification of assets

51 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_FPROG unauthorized modification of firmware programs, including modification of firmware security mechanisms.

T.MOD_APROG unauthorized modification of application programs and data.

T.MOD_TEST unauthorized modification of test programs.

52 The table 3.1 indicates the relationship 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_APROG		Class II	Class I/II	Class I	Class I	Class I	Class I
T.DIS_FPROG		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_ENV		Class II	Class II				
T.DIS_PHOTOMASK		Class II	Class I/II	Class I	Class I	Class I	Class I
T.DIS_TEST			Class I/II	Class I	Class I		
Theft of assets							
T.T_DEL	Class II						
T.T_SAMPLE		Class II	Class I	Class I	Class I		
T.T_PHOTOMASK		Class II	Class I/II				
T.T_PRODUCT			Class I	Class I	Class I	Class I	Class I
Unauthorized modification threats							
T.MOD_DEL	Class II						
T.MOD_APROG		Class II	Class I/II	Class I	Class I	Class I	Class I
T.MOD_FPROG		Class II	Class I/II	Class I	Class I	Class I	Class I
T.MOD_TEST			Class I/II	Class I	Class I		
T.MOD_DESIGN		Class II	Class I/II	Class I	Class I	Class I	Class I

Tab. 3.1 - Threats and phases

3.3 Organisational Security policies

53 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.

3.4 Secure usage assumptions

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

- due to the definition of the TOE limits, any secure usage assumption for the smartcard 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 trusted delivery procedures.

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

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

3.4.1 Secure usage assumptions on phase 1

A.SOFT_ARCHI the smartcard embedded software shall be designed in a secure manner, that is focusing on integrity of program and data.

A.SOFT_MECH the smartcard embedded software shall use all security features and security mechanisms as required by the IC designer (e.g. cryptography,...).

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.

A.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, Rom-less emulators etc...) that will grant the integrity of program and data.

3.4.2 Secure usage assumptions on the TOE delivery process (phases 4 to 7)

A.DLV_CONTROL procedures must guarantee the control of the TOE delivery and storage process and conformance to its objectives as described in the following secure usage assumptions. Secure storage and handling procedures are applicable for all TOEs (including rejected TOEs).

A.DLV_CONF procedures must also prevent if applicable any non-conformance to the confidentiality convention and must have a corrective action system in case any non-conformance or misprocessed procedures are identified.

A.DLV_PROTECT procedures shall ensure protection of 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.

A.DLV_TRANS procedures shall ensure that material/information is delivered to the correct party.

A.DLV_TRACE procedures shall ensure traceability of delivery including the following parameters:

- origin and shipment details,
- reception, reception acknowledgement,
- location material/information.

A.DLV_AUDIT procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and highlight all non conformance to this process.

A.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.

3.4.3 Secure usage 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).

3.4.4 Secure usage 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 security of sensitive data stored/ handled by the system (terminals, communications ...) is maintained.

A.USE_ISSUE it is assumed that each TOE is used in a smartcard product issued to end-users with a well defined and controlled process.

Chapter 4

Security objectives

56 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 IT Security objectives

57 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 information stored in memories is protected against unauthorized access.

O.MOD_MEMORY The TOE shall ensure that information stored in memories is protected against any corruption or unauthorized modification.

4.2 Non IT Security objectives

4.2.1 Objectives on phase 1

O.DEV_DIS the smartcard 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.

O.SOFT_DLV the embedded software must be delivered from the smartcard 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.

4.2.2 Objectives on phase 2 (development phase)

O.SOFT_ACS embedded software shall be accessible only by authorized personnel (physical, personnel, organisational, technical procedures).

O.DESIGN_ACS IC specifications, detailed design, IC databases, schematics/ layout or any further design information shall be accessible only by authorized personnel (physical, personnel, organisational, technical procedures).

O.FIRM_ACS Any firmware specification, detailed design, source code or any further firmware information shall be accessible only by authorized personnel (physical, personnel, organisational, technical procedures).

O.MASK_FAB physical, personnel, organisational, technical procedures during photomask fabrication shall ensure the integrity and confidentiality of the TOE.

O.MECH_ACS Details of hardware security mechanisms shall be accessible only by authorized personnel.

O.TI_ACS Security relevant technology information shall be accessible only by authorized personnel.

O.MASK_DLV the delivery procedures between the IC designer and the photomasks manufacturer shall maintain the integrity and confidentiality of the TOE.

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.

O.TEST_PRT security procedures shall ensure the confidentiality and integrity of security relevant test programs and databases and specific analysis methods and tools.

O.MANUF_PRT security procedures shall ensure the confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use) during the IC manufacturing and test operations.

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

O.SYSTEM_SEC a procedure shall define a security system applicable during the manufacturing and test operations to maintain confidentiality and integrity of the TOE by control of:

- packing 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 and analysis tools and laboratories,
- access control and audit to test and analysis databases,
- change/modification in the manufacturing equipment, management of rejects.

Chapter 5

TOE IT functional requirements

58 The TOE IT functional requirements define the functional requirements for the TOE using only functional requirements components drawn from the CC part 2.

59 The permitted operations such as assignment, selection, refinement will have to be defined in a Security Target, compliant with this PP. 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.

5.1 Functional requirements applicable to phase 3 (testing phase)

5.1.1 Basic User Authentication (FIA_UAU.1)

60 The TOE Security Functions shall authenticate any user's claimed identity prior to performing any functions for the user.

5.1.2 Basic User Identification (FIA_UID.1)

61 The TOE Security Functions shall identify each user before performing any actions requested by the user.

5.1.3 User Attribute Definition (FIA_ATD.1)

62 The TOE Security Functions shall provide, for each user, a set of security attributes necessary to enforce the TOE security policy.

5.1.4 User Attribute Initialisation (FIA_ATA.1)

63 The TOE Security Functions shall provide the ability to initialise user attributes with provided default values.

5.1.5 User Authentication Data Initialisation (FIA_ADA.1)

64 The TOE Security Functions shall provide functions for initialising user authentication data related to [assignment: identified authentication mechanism].

65 The TOE Security Functions shall restrict the use of these functions to the authorised administrator.

5.1.6 Basic User Authentication Data Protection (FIA_ADP.1)

66 The TOE Security Functions shall protect from unauthorised observation, modification, and destruction authentication data that is stored in the TOE.

5.2 Functional requirements applicable to phases 3 to 7

5.2.1 Imminent Violation Analysis (FAU_SAA.1)

67 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.

68 The set of rules shall be:

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

b) [assignment: any other rules].

5.2.2 Complete Object Access Control (FDP_ACC.2)

69 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.

70 The TOE Security Functions shall ensure that all operations between any subject in the TOE Security Functions Scope of Control and any object within the TOE Security Functions Scope of Control are covered by the Security Functions Policy.

5.2.3 Single Security Attribute Access Control (FDP_ACF.1)

71 The TOE Security Functions shall enforce the [assignment: access control Security Functions Policy] to objects based on [assignment: attribute, named group of attributes].

72 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].

5.2.4 Subset Information Flow Control (FDP_IFC.1)

73 The TOE Security Functions shall enforce the [assignment: information flow control Security Functions Policy] on [assignment: list of subjects, objects and operations among subjects and objects covered by the Security Functions Policy].

74 *Note: this security functional requirement is applicable to the TOE optional firmware.*

5.2.5 Simple Security Attributes (FDP_IFF.1)

75 The TOE Security Functions shall enforce the [assignment: information flow control Security Functions Policy] to enforce at least the following types of subject

and object security attributes [assignment: specification of the minimum number and type of security attributes].

76 The TOE Security Functions shall enforce an information flow between a subject and a controlled object via a controlled operation if the following rules hold [assignment: by operation, the security attribute-based relationship that must hold between subject and object security attributes].

77 The TOE Security Functions shall enforce the [assignment: additional information flow control Security Functions Policy rules].

78 The TOE Security Functions shall enforce the following [assignment: list of additional Security Functions Policy capabilities].

79 *Note: this security functional requirement is applicable to the TOE optional firmware.*

5.2.6 Administrator Defined Attribute Initialisation (FDP_ACI.2)

80 The TOE Security Functions shall enforce the [selection: access control Security Functions Policy, information flow control Security Functions Policy] to provide [selection: restrictive, permissive, other property] default values for object security attributes that are used to enforce the Security Functions Policy.

81 The TOE Security Functions shall allow the specification of alternate initial values to override the default values when an object is created.

82 The TOE Security Functions shall restrict modification of these default values to the authorised administrator.

5.2.7 Administrator Attribute Modification (FDP_SAM.1)

83 The TOE Security Functions shall enforce [selection: access control Security Functions Policy, information flow control Security Functions Policy] to provide authorised administrators with the ability to modify [assignment: list of security attributes].

5.2.8 Administrator Attribute Query (FDP_SAQ.1)

84 The TOE Security Functions shall enforce the [selection: access control Security Functions Policy, information flow control Security Functions Policy] to provide the authorised administrator with the ability to query [assignment: list of security attributes] values.

5.2.9 Stored Data Integrity Monitoring (FDP_SDI.1)

85 The TOE Security Functions shall ensure that upon detection of a data integrity error of [assignment: list of objects], the TOE Security Functions shall [assignment: action to be taken].

86 *Note: the data integrity monitoring can be made by any firmware or software.*

5.2.10 Unobservability (FPR_UNO.1)

87 The TOE Security Functions shall ensure that [assignment: set of users and/or subjects] working together, [selection: including, excluding] authorised administrators, are unable to observe the operation [assignment: list of operations] on [assignment: list of objects] by another user or subject.

5.2.11 Resistance to Physical Attack (FPT_PHP.3)

88 The TOE shall include features that provide unambiguous detection of physical tampering with the TOE Security Functions's physical devices and elements.

89 The TOE Security Functions shall provide the authorised administrator with the capability to determine whether physical tampering with the TOE Security Functions's devices and elements has occurred.

90 For [assignment: list of 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 and elements has occurred.

91 For the following subset of the TOE Security Functions's devices and elements, the TOE shall include features that resist identified physical tampering attacks to the TOE Security Functions's devices and elements:

92 [assignment: list of <devices/elements, physical tampering attack scenarios, work factors> for which resistance to attack is required]

93 For the following identified attack scenarios against the following subset of the TOE Security Functions's device and elements, the TOE shall include features that automatically respond to the attack in such a way as to ensure that the TOE Security Policy is not violated.

94 [assignment: list of <devices/elements, physical tampering attack scenarios> for which automatic response to attack is required].

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

5.2.12 On-Demand TOE Security Functions Testing (FPT_TST.1)

96 The TOE Security Functions shall provide authorised administrators with the capability to demonstrate the correct operation of the TOE Security Functions.

97 The TOE Security Functions shall provide authorised administrators with the capability to verify the integrity of TOE Security Functions data.

5.2.13 Basic Security Administration (FPT_TSA.1)

98 The TOE Security Functions shall distinguish security-relevant administrative functions from other functions.

99 The TOE Security Functions’s set of security-relevant administrative functions shall include all functions necessary to install, configure, and manage the TOE Security Functions; minimally, this set shall include [assignment: list of administrative services to be minimally supplied].

100 The TOE Security Functions shall restrict the ability to perform security-relevant administrative functions to specifically authorised users.

101 The TOE Security Functions shall be capable of distinguishing the set of users authorised for administrative functions from the set of all users of the TOE.

Chapter 6

TOE IT Assurance Requirements

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

103 ADO_DEL.2 "Detection of modification" is an additional component ; the others are hierarchical ones to the components specified in EAL4.

6.1 Additional components

6.1.1 ADO_DEL.2 Detection of modification

Dependencies:

104 ACM_CAP.2 Authorisation controls

Developer actions elements:

105 The developer shall provide documentation about the procedures for delivery of the TOE or parts of it to the user.

106 The developer shall use the delivery procedures.

Content and presentation of evidence elements:

107 The delivery documentation shall describe the procedures to be employed when distributing versions of the TOE to a user’s site.

108 The delivery documentation shall state how the procedures are to be employed to detect modifications.

109 The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer’s master copy and the version received at the user site.

110 The delivery documentation shall describe how the various procedures allow detection of attempted masquerading even in cases in which the developer has sent nothing to the user’s site.

Evaluator action elements:

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

6.2 Hierarchical higher components

6.2.1 ADV_IMP.2 Implementation of the TSF

Dependencies:

112 ADV_LLD.1 Descriptive low-level design

113 ADV_RCR.1 Informal correspondence demonstration

114 ALC_TAT.2 Compliance with implementation standards

Developer actions elements:

115 The developer shall provide the implementation representations for the entire TSF.

Content and presentation of evidence elements:

116 The implementation representations shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

117 The implementation representations shall describe the relationships between all portions of the implementation.

Evaluator action elements:

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

119 The evaluator shall determine if the functional requirements in the ST are addressed by the representation of the TSF.

6.2.2 ALC_DVS.2 Sufficiency of security measures

Dependencies:

120 No dependencies.

Developer actions elements:

121 The developer shall produce development security documentation.

Content and presentation of evidence elements:

122 The development security documentation shall describe the physical, procedural, personnel, and other security measures that are used to protect the confidentiality and integrity of the TOE during its development.

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

124 The evidence shall justify that the security measures are sufficient to protect the confidentiality and integrity of the TOE.

Evaluator action elements:

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

126 The evaluator shall check whether the security measures are being applied.

6.2.3 ATE_DPT.3 Testing - low level design

Dependencies:

127 ADV_FSP.1 TOE and security policy

128 ADV_HLD.1 Descriptive high-level design

129 ADV_LLD.1 Descriptive low-level design

130 ATE_FUN.1 Functional testing

Developer actions elements:

131 The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

132 The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TOE operates in accordance with the functional specification, high level design, and low level design of the TSF.

Evaluator action elements:

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

6.2.4 AVA_VLA.4 Highly resistant

Dependencies:

134 ADV_FSP.1 TOE and security policy

135 ADV_HLD.1 Descriptive high-level design

136 ADV_IMP.1 Subset of the implementation of the TSF

137 ADV_LLD.1 Descriptive low-level design

138 AGD_ADM.1 Administrator guidance

139 AGD_USR.1 User guidance

Developer actions elements:

140 The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

141 The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

142 The evidence shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE.

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

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

Evaluator action elements:

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

146 The evaluator shall conduct penetration testing, based on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

147 The evaluator shall perform an independent vulnerability analysis.

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

149 The evaluator shall determine that the TOE is highly resistant to penetration attacks.

Annex A

Glossary

Integrated Circuit (IC)

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

IC designer

Institution (ot its agent) responsible for the IC developement.

IC manufacturer

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

IC packaging manufacturer

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

Personaliser

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

Smartcard

A credit sized plastic card which has a non volatile memory and a processing unit embedded within it.

Smartcard embedded software developer

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

Smartcard Issuer

Institution (ot its agent) responsible for the smartcard product delivery to the smartcard end-user.

Smartcard product manufacturer

Institution (ot its agent) responsible for the smartcard product finishing process and testing.