EUROSMART
European Smart Card Industry Association

Common Criteria

For Information Technology

Security Evaluation

Protection Profile

Smart Card Integrated Circuit

With Embedded Software

Version 2.0

Issue June 99

Registered by the French Certification Body under the reference PP/9911

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

- **ATMEL Smart Card ICs**
  The Maxwell Building
  Scottish Enterprise Technology Park
  East Kilbride
  Glasgow G75 OQF
  Scotland
  Tel: (+44) 1355 35 5308
  Fax: (+44) 1355 24 2743 www.tics11@email.sps.mot.com

- **BULL - SC&T**
  68 route de Versailles - BP 45
  78431 LOUVECIENNES, France
  Tel : (+33) 1.39.66.44.90
  Fax : (+33) 1.39.66.44.02 www.CP8.Bull.net

- **DE LA RUE - Card Systems**
  3 à 5, Avenue Galliéni
  94250 - GENTILLY CEDEX, France
  Tel : (+33) 1.49.69.24.00
  Fax : (+33) 1.49.69.25.02 www.delarue.com

- **EUROSMART**
  Rue Montoyer, 47
  B - 1000 BRUXELLES
  Tel : (+32-2) 506.88.68
  Fax : (+32-2) 506.88.68 www.eurosmart.com

- **GEMPLUS**
  Z.E. de la Plaine de Jouques - BP 100
  13881 GEMENOS CEDEX, France
  Tel : (+33) 04.42.36.55.77
  Fax : (+33) 04.42.36.57.92 www.gemplus.com

- **GIESECKE & DEVRIENT GmbH**
  Prinzregentenstrasse 159
  D-81677 Munich, Germany
  P.O.Box 80 07 29
  D-81607 Munich, Germany
  Tel : (+49.89) 4119 0
  Fax : (+49.89) 4119 1535 www.gdm.de

- **HITACHI Europe Ltd**
  Whitebrook Park
  Lower Cookham Road
  Maidenhead
  SL6 8YA United Kingdom
  Tel: (+44) 1628 585 000
  Fax: (+44) 1628 585 972 www.hitachi-eu.com

- **INFINEON Technologies (formerly SIEMENS)**
  CC M - PO Box 80 17 60
  D-81617 MUNCHEN, Germany
  Tel: (+49) 89 234 48964
  Fax: (+49) 89 234 22214 www.infineon.com

- **MICROELECTRONICA Española**
  Concha Espina 65
  28016 MADRID, Spain
  Tel: (+34) 91 563 6847
  Fax: (+34) 91 561 2080

- **MOTOROLA - SPS**
  18, rue Grange Dame Rose
  BP95
  78143 Velizy, France
  Tel: (+33) 1 34 63 59 66
  Fax: (+33) 1 34 63 58 61 www.mot.com

- **NEC Electronics**
  9, rue Paul Dautier
  BP 52
  78142 VELIZY-VILLACOUBLAY CEDEX
  Tel: (33) 1 30 67 58 00
  Fax: (33)1 30 67 59 37

- **OBERTHUR Smart Card**
  12 bis, rue des Pavillons - BP 133
  92804 PUTEAUX, France
  Tel: (+33) 1.41.25.28.28
  Fax: (+33) 1.40.90.99.70 www.oberthur.com

- **ODS**
  Ludwig-Erhard Strasse., 16
  D-85375 - Neufahrn, Germany
  Tel: (+49).8165 930 0
  Fax: (+49) 8165 930 202

- **ORGA**
  An Der Kapelle 2
  D-33104 PADERBORN, Germany
  Tel: (+49) 52.54.991.0
  Fax: (+49) 52.54.991.199 www.orga.com

- **PHILIPS Semiconductors Hamburg**
  UB Philips GmbH
  D-22502 HAMBURG, Germany
  Tel: (+49) 40.5613.2624
  Fax: (+49) 40.5613.3045 www.semiconductors.philips.com

- **SCHLUMBERGER Cards Division**
  50, Avenue Jean Jaures, BP 620-12
  92542 - MONTROUGE, France
  Tel: (+33) 1 47 46 62 01
  Fax: (+33) 1 47 46 55 48 www.slb.com

- **Service Central de la Securité des Systèmes d'Information**
  Information Technology Security Certification Center
  18, rue du Docteur Zamenhof
  92131 ISSY-LES-MOULINEAUX, France
  Tel: (+33) 1 41 46 37 84
  Fax: (+33) 1 41 46 37 01

- **ST Microelectronics**
  ZI de Rousset BP2
  F- 13106 ROUSSET CEDEX, France
  Telephone : (+33) 4.42.25.89.44
  Fax : (+33) 4.42.25.87.29 www.st.com

For information or comments, please e-mail ssi20@calva.net

Common Criteria are available at the following address : http://www.crsc.nist.gov/cc
This PP is available at the following addresses:
http://www.eurosmart.com
http://www.scssi.gouv.fr,

TABLE OF CONTENTS

Chapter 1. PP introduction

1.1. PP Identification

Title : Smart Card Integrated Circuit with Embedded Software Protection Profile

Version : V2.0, issue June 1999

Registration : Registered at French Certification Body under the number PP/9911.

This PP supersedes PP/9809.

Registration	**Version number**	**Common Criteria**
PP/9911	V2.0	version 2.0

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

The Smart Card is considered as a functional object made of hardware and software designed to run on a specific hardware platform compliant with the “ Smart Card Integrated Circuit Protection Profile Ref : PP/9806 Version 2.0”, also referred to in the text as Smart Card IC PP.

A Security Target compliant with this PP shall claim the compliance to the Smart Card IC PP. Indeed, this PP should not be used independently. For the sake of clarification, items which are common with Smart Card IC PP will be indicated by a “*” in this PP. In case of discrepancy the component described in Smart Card IC PP shall be considered as the reference.

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

1.2. PP overview

This Protection Profile results from the work of the Eurosmart Security Working group and advice's from IT Security Evaluation and Certification Bodies. This group was composed of the following participants :

- ATMEL Smart Card ICs
- BULL
- DE LA RUE - Card Systems
- GEMPLUS
- GIESECKE & DEVRIENT
- HITACHI
- INFINEON Technologies (formerly SIEMENS)
- MICROELECTRONICA Española
- MOTOROLA - SPS
- NEC Electronics
- OBERTHUR Smart Card
- ODS
- ORGA
- PHILIPS
- SCHLUMBERGER
- ST Microelectronics

The intent of this Protection Profile is to specify functional and assurance security requirements applicable to a functional Smart Card Integrated Circuit containing its Embedded Software (ES) in operation.

A Smart Card 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 Smart Cards whatever the interface and communication protocol with the intended usage environment (contact or contact-less Smart Cards or a combination of both).

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

- the development stage : Integrated Circuit (hereafter IC) design, Smart Card Embedded Software development, integration and photomask fabrication,

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

- the Smart Card production stage : Smart Card IC packaging (and testing), Smart Card product finishing process, printing (and testing), Smart Card preparation and shipping to the personalization line.

In addition, two important stages are to be considered in the Smart Card life cycle :

- the Smart Card personalization and testing stage where the end-user data is loaded into the Smart Card's memory,

- the Smart Card usage by its issuers and end-user.

The increase in the number and complexity of applications in the Smart Card market is reflected in the increase of the level of data and program security required. The security needs for a Smart Card can be summarized as being able to counter those who want to defraud, gain unauthorized access to data or control a system using a Smart Card (which is considered to be inseparable pair of hardware and software). Therefore it is mandatory to :

- maintain the integrity and the confidentiality of the content of the Smart Card non volatile memory (program and data memories),
- maintain the integrity and the confidentiality necessary to enforce and ensure security, in addition to the relevant architectural components (security mechanisms and associated functions) embedded into the integrated circuit.

Protected information is in general secret data, such 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 the use of the Smart Card.

The intended environment is widespread and generally once issued the Smart Card can be stored and used anywhere in the world at any time, with no particular controls being applied to either the Smart Card or the end-user (with the exception of those controls which ensure that the use of the Smart Card in a given application is in accordance with the application system's specifications).

Presently the major Smart Card 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.),
- multimedia commerce and Intellectual Property Rights protection.

One of the key market drivers for Smart Cards 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.

The main objectives of this Protection Profile are :

- to describe the Target of Evaluation (TOE) as a functional product. This PP focuses on the development and use of the Embedded Software in the integrated circuit, considering that the only purpose of the Embedded Software developed during the first part of the Smart Card's life cycle is to control its operation during its product usage,

- 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 environment during the development and the product usage,

- 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 phase,

- to specify the security requirements which includes the TOE security functional requirements and the TOE security assurance requirements.

The assurance level for this PP is EAL4 augmented. The minimum strength level for the TOE security functions is “ SOF-high ”(Strength of Functions High).

Chapter 2. TOE Description

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

2.1. Product type

The Target of Evaluation (TOE) is the Smart Card Integrated Circuit with Embedded Software in operation and in accordance with the functional specifications, independent of the physical interface, the way it is packaged and any other security device supported by the physical card base. Generally, a Smart Card product may include other elements (such as specific hardware components, batteries, capacitors, antennae, holograms, magnetic stripes, security printing...) but these are not in the scope of this Protection Profile.

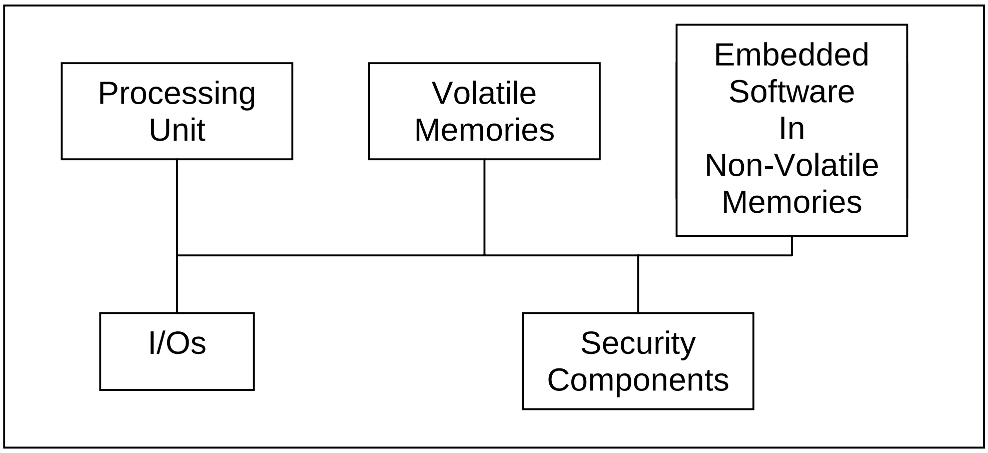

Fig 2.1 Typical Smart Card IC with ES

The typical TOE is composed of a processing unit, security components, I/Os and volatile and non-volatile memories including the ES. The TOE includes any IC designer/manufacturer proprietary IC Dedicated Software, Basic Software, Application Software and/or Initialization data and process.

This PP addresses the requirements of the Basic Software (BS) and the Application Software (AS) embedded in the Smart Card Integrated Circuit, since BS and AS are part of ES.

2.2. Smart Card Product Life-cycle

The Smart Card product life-cycle is decomposed into 7 phases, according to the “ Smart Card Integrated Circuit Protection Profile ” and is described in figure 2.2

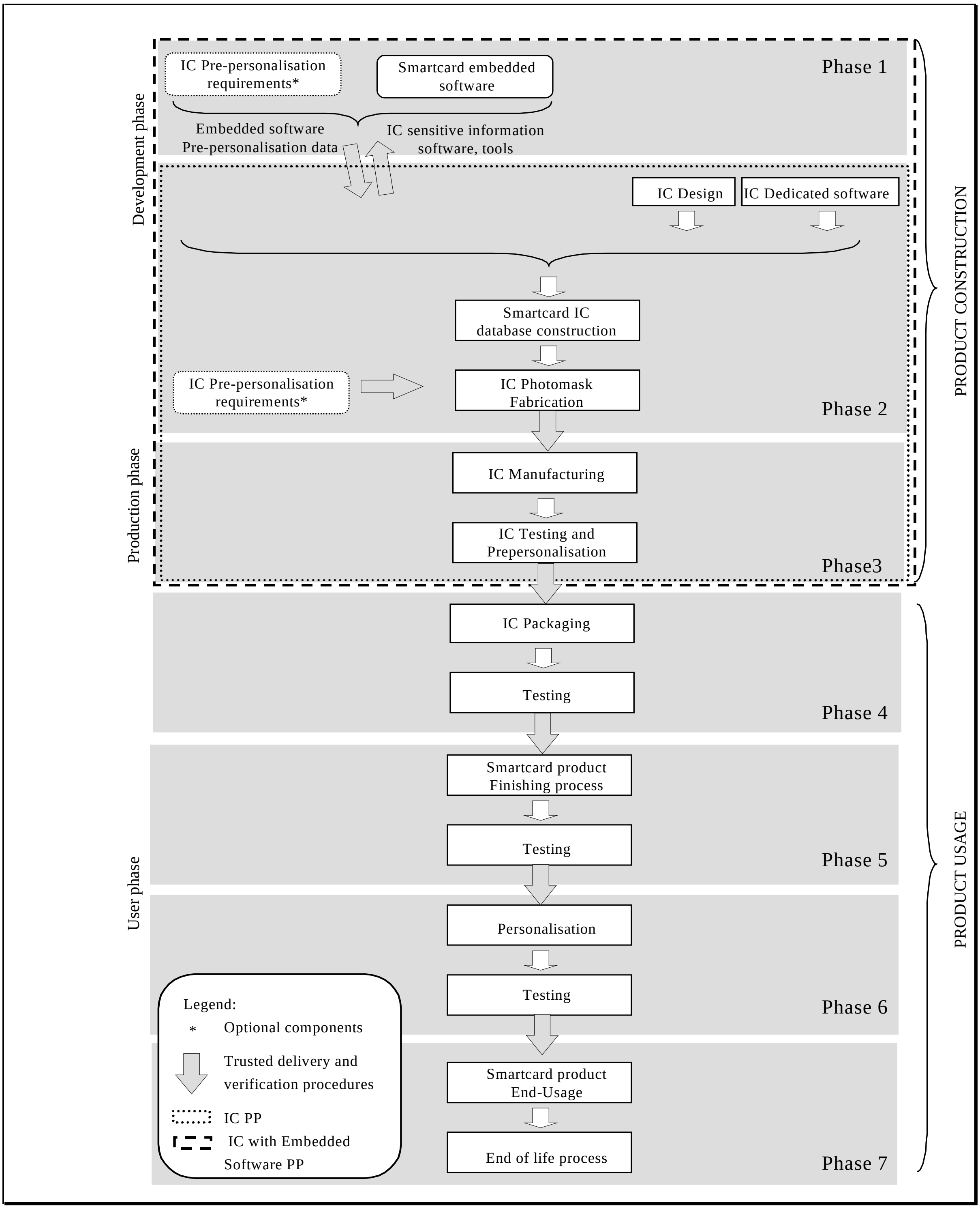
Phase 1
IC Pre-personalisation requirements*
Smartcard embedded software
Embedded software Pre-personalisation data
IC sensitive information software, tools
Development phase
IC Design
IC Dedicated software
Smartcard IC database construction
IC Pre-personalisation requirements*
IC Photomask Fabrication
Phase 2
Production phase
IC Manufacturing
IC Testing and Prepersonalisation
Phase3
PRODUCT CONSTRUCTION
IC Packaging
Testing
Phase 4
Smartcard product Finishing process
Testing
Phase 5
User phase
Personalisation
Testing
Phase 6
Smartcard product End-Usage
End of life process
Phase 7
PRODUCT USAGE
Legend:
* Optional components
Trusted delivery and verification procedures
IC PP
IC with Embedded Software PP

Figure 2.2 Smart Card Product life-cycle

The purpose of the Embedded Software designed during phase 1 is to control and protect the TOE during phases 4 to 7 (product usage).The global security requirements of the TOE are such that it is mandatory during the development phase, to anticipate the security threats of the other phases. This is why this PP addresses the functions used in phases 4 to 7 but developed during phase 1.

Phase 1 is part of this product life cycle where the following authorities are involved

Phase 1	Smart Card Software Development	The Smart Card software developers are in charge of the Basic Software and Application Software development and the specification of Initialization requirements.

BS and AS may be designed at different sites ; procedures on the delivery process of the TOE must exist and be applied for every delivery within this phase or between phases. This includes any kind of delivery performed from phase 1 to 6, 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.

2.3. TOE Environment

The TOE environment is defined as follow :

- Development environment corresponding to phase 1 and 2,
- Development and IC Photomask Fabrication environment corresponding to phases 2 addressed by the Smart Card IC PP,
- IC manufacturing environment corresponding to phase 3, including the integration of the ES in the IC and the test operations,
- IC Packaging, Smart Card Finishing process environment corresponding to phases 4 and 5, including test operations,
- Personalization environment corresponding to personalization and testing of the Smart Card with the user data (phase 6),
- End-User environment (phase 7).

2.3.1. TOE Development Environment

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

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

Design and development of the ES then follows. The engineer uses a secure computer system (preventing unauthorized access) to make his design, implementation and test performances.

Sensitive documents, databases on tapes, disks and diskettes are stored in an appropriately locked cupboard/safe. Also of paramount importance is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

Testing, programming and deliveries of the TOEs then take place. When these are done off-site, they must be transported and worked in a secure environment with accountability and traceability of all (good and bad) products.

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. TOE Production Environment

This production environment is defined in Smart Card IC PP.

2.3.3. TOE User Environment

Phases 4 and 5:

During phases 4 and 5 of production, the TOE are used in the IC Packaging, Smart Card Finishing process and the test environments. Everyone involved in such operations shall fully understand the importance of security procedures.

Moreover the environment in which these operations take place must be secured. Sensitive information (tapes, disks or diskettes) are stored in an appropriately locked cupboard/safe. Also of paramount importance is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

Phase 6:

Since it is commonplace to produce high volumes of Smart Cards, adequate control procedures are necessary to account for all products at all stages.

These must be transported and manipulated in a secure environment with accountability and traceability of all (good and bad) products.

Phase 7:

This End-User environment is defined in Smart Card IC PP.

2.4. TOE logical phases

During its construction usage, the TOE may be under several 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

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 a 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 protection of Intellectual Property Rights.

During phase 1, while the TOE is being developed, the **administrators** are as the following :

- the Basic Software developer
- the Application Software developer

2.6. General IT features of the TOE

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

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

Chapter 3. TOE Security Environment

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

3.1. Assets

Assets are security relevant elements of the TOE that include :

- the IC specifications, design, development tools and technology,
- the IC Dedicated software,
- the Smart Card Embedded Software including specifications, implementation and related documentation,
- the application data of the TOE (such as IC and system specific data, Initialization data, IC pre-personalization requirements and personalization data,)

The TOE itself is therefore an asset.

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

3.2. Assumptions

Security always concerns 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 Smart Card products :

3.2.1. Assumptions on phase 1

A.DEV_ORG* Procedures dealing with physical, personnel, organizational, technical measures for the confidentiality and integrity, of Smart Card 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)

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 TOE 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. Assumption on phase 7

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

3.3. Threats

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 manipulation, by specific hardware manipulation, by a combination of hardware and software manipulations or by any other type of attacks.

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 all phases of the TOE life-cycle, from phase 1 to phase 7, but only phases 1 and 4 to 7 are considered here, since functional cloning in phases 2 and 3 are purely in the scope of Smart Card IC PP. 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

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

a) threats on the Smart Cards Embedded Software and its development environment, such as unauthorized disclosure, modification or theft of the Smart Card Embedded Software and/or initialization data at phase 1.

b) threats on the assets transmitted from the IC designer to the Smart Card software developer during the Smart Card ES development ;

c) threats on the Smart Card Embedded Software and initialization data transmitted during the delivery process from the Smart Card software developer to the IC designer.

Unauthorized disclosure of assets

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_INFO*
(type b)
Unauthorized disclosure of the assets delivered by the IC designer to the Smart Card Embedded Software developer, such as sensitive information on IC specification, design and technology, software and tools if applicable.

T.DIS_DEL*
(type c)
Unauthorized disclosure of the Smart Card Embedded Software and any additional application data (such as IC pre-personalization requirements) during the delivery to the IC designer.

T.DIS_ES1
(type a)
Unauthorized disclosure of ES (technical or detailed specifications, implementation code) and/or Application Data(such as secrets, or control parameters for protection system, specification and implementation for security mechanisms).

T.DIS_TEST_ES
(type a and c)
Unauthorized disclosure of the Smart Card ES test programs or any related information.

Theft or unauthorized use of assets

Potential attackers may gain access to the TOE and perform operations for which they are not authorized. For example, such an attacker may personalize, modify or influence the product in order to gain access to the Smart Card application system.

T.T_DEL* (type c)
Theft of the Smart Card Embedded Software and any additional application data (such as pre-personalization requirements) during the delivery process to the IC designer.

T.T_TOOLS (type a and b)
Theft or unauthorized use of the Smart Card ES development tools (such as PC, development software, data bases).

T.T_SAMPLE2 : (type a)
Theft or unauthorized use of TOE samples (e.g. bond-out chips with the Embedded Software).

Unauthorized modification of assets

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 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_DEL* (type c)
Unauthorized modification of the Smart Card Embedded Software and any additional application data (such as IC pre-personalization requirements) during the delivery process to the IC designer.

T.MOD (type a)
Unauthorized modification of ES and/or Application Data or any related information (technical specifications).

3.3.3. Threats on delivery for/from phase 1 to phases 4 to 6

Threats on data transmitted during the delivery process from the Smart Card developer to the IC packaging manufacturer, the Finishing process manufacturer or the Personalizer.

These threats are described hereafter :

T.DIS_DEL1
Unauthorized disclosure of Application Data during delivery to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.

T.DIS_DEL2
Unauthorized disclosure of Application Data delivered to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.

T.MOD_DEL1
Unauthorized modification of Application Data during delivery to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.

T.MOD_DEL2 Unauthorized modification of Application Data delivered to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.

3.3.4. Threats on phases 4 to 7

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

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

Unauthorized disclosure of assets

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_ES2 Unauthorized disclosure of ES and Application Data (such as data protection systems, memory partitioning, cryptographic programs and keys).

Theft or unauthorized use of assets

Potential attackers may gain access to the TOE and perform operation for which they are not allowed. For example, such attackers may personalize the product in an unauthorized manner, or try to gain fraudulently access to the Smart Card system

T.T_ES Theft or unauthorized use of TOE. (e.g. bound out chips with embedded software).

T.T_CMD Unauthorized use of instructions or commands or sequence of commands sent to the TOE.

Unauthorized modification of assets

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 threat includes the implementation of malicious Trojan horses, Trapdoors, downloading of viruses or unauthorized programs.

T.MOD_LOAD Unauthorized loading of programs.

T.MOD_EXE Unauthorized execution of programs.

T.MOD_SHARE	Unauthorized modification of program behavior by interaction of different programs.
T.MOD_SOFT*	Unauthorized modification of Smart Card Embedded Software and Application Data.

The table 3.1 given below indicates the relationship between the phases of the Smart Card life cycle, the threats and the type of the threats :

Threats	**Phase1**	**Phase 4**	**Phase 5**	**Phase 6**	**Phase 7**
T.CLON*	Class II	Class I	Class I	Class I	Class I
T.DIS_INFO*	Class II				
T.DIS_DEL*	Class II				
T.DIS_DEL1	Class II				
T.DIS_DEL2		Class II	Class II	Class II	
T.DIS_ES1	Class II				
T.DIS_TEST_ES	Class II				
T.DIS_ES2		Class I	Class I	Class I	Class I
T.T_DEL*	Class II				
T.T_TOOLS	Class II				
T.T_SAMPLE2	Class II				
T.T_ES		Class I	Class I	Class I	Class I
T.T_CMD		Class I	Class I	Class I	Class I
T.MOD_DEL*	Class II				
T.MOD_DEL1	Class II				
T.MOD_DEL2		Class II	Class II	Class II	
T.MOD	Class II				
T.MOD_SOFT*		Class I	Class I	Class I	Class I
T.MOD_LOAD		Class I	Class I	Class I	Class I
T.MOD_EXE		Class 1	Class I	Class I	Class I
T.MOD_SHARE		Class I	Class I	Class I	Class I

Table 3.1: relationship between phases and threats

Note: Phases 2 and 3 are covered in the scope of Smart Card IC PP.

3.4. Organizational Security policies

An organizational security policy is mandatory for the Smart Card product usage and its end-destination. Nevertheless, no organizational security policy has been defined in the scope of this PP since such specifications depend essentially on the applications in which the TOE is incorporated.

Chapter 4. Security objectives

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

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

4.1. Security Objectives for the TOE

The TOE shall use state of art technology to achieve the following IT security objectives, and for that purpose, when IC physical security features are used, the specification of those IC physical security features shall be respected. When IC physical security features are not used, the Security Objectives shall be achieved in other ways :

O.TAMPER_ES The TOE must prevent tampering with its security critical parts. Security mechanisms have especially to prevent the unauthorized change of functional parameters, security attributes and secrets such as the life cycle sequence flags and cryptographic keys.
The ES must be designed to avoid interpretations of electrical signals from the hardware part of the TOE.

O.CLON* The TOE functionality must be protected from cloning.

O.OPERATE* The TOE must ensure continued correct operation of its security functions.

O.FLAW* The TOE must not contain flaws in design, implementation or operation.

O.DIS_MECHANISM2 The TOE shall ensure that the ES 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_TOOLS*

The Smart Card ES 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 result in the integrity of program and data.

O.DEV_DIS_ES

The Embedded Software developer shall use established procedures to control storage and usage of the classified development tools and documentation, suitable to maintain the integrity and the confidentiality of the assets of the TOE.

It must be ensured that tools are only delivered and accessible to the parties authorized personnel.
It must be ensured that confidential information on defined assets are only delivered to the parties authorized personnel on a need to know basis.

O.SOFT_DLV*

The Smart Card embedded software must be delivered from the Smart Card 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.INIT_ACS

Initialization Data shall be accessible only by authorized personnel (physical, personnel, organizational, technical procedures).

O.SAMPLE_ACS

Samples used to run tests shall be accessible only by authorized personnel.

4.2.2. 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 element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage
- secure storage and handling procedures (including rejected

TOE's)

- 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 be able to act fully in accordance with the above expectations.

4.2.3. Objectives on delivery from phase 1 to phases 4, 5 and 6

O.DLV_DATA The Application Data must be delivered from the Smart Card embedded software developer (phase 1) either to the IC Packaging manufacturer, the Finishing Process manufacturer or the Personalizer through a trusted delivery and verification procedure that shall be able to maintain the integrity and confidentiality of the Application Data.

4.2.4. Objectives on phases 4 to 6

O.TEST_OPERATE* Appropriate functionality testing of the TOE shall be used in phases 4 to 6.
During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

4.2.5. Objectives on phase 7

O.USE_DIAG* Secure communication protocols and procedures shall be used between the Smart Card and the terminal.

Chapter 5. TOE Security functional requirements

This chapter defines the functional requirements for the TOE using only functional requirements components drawn from the CC part 2.

The assurance level for this PP is EAL4 augmented. The minimum strength level for the TOE security functions is “ SOF-high ”(Strength of Functions High).

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

5.1. Security audit analysis (FAU_SAA)

5.1.1. FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF 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 TSP.

FAU_SAA.1.2 The TSF 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;
[assignment: *any other rules*].

5.2. Cryptographic key management (FCS_CKM)

5.2.1. FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform [assignment : *type of cryptographic key access*] in accordance with a specified cryptographic key access method, [assignment *: cryptographic key access method*] that meets the following : [assignment *: list of standards*].

5.2.2. FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method, [assignment : *cryptographic key destruction method*] that meets the following : [assignment : *list of standards*].

5.3. Cryptographic operations (FCS_COP)

5.3.1. FCS_COP.1 Cryptographic operations

FCS_COP.1.1 The TSF shall perform [assignment : *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment *: cryptographic algorithm*] and cryptographic key size [assignment *: cryptographic key size*] that meet the following [assignment *: list of standards*].

5.4. Access Control Policy (FDP_ACC)

5.4.1. FDP_ACC.2 Complete Access control

FDP_ACC.2.1 The TSF shall enforce the [assignment : *access control SFP*] on [assignment : *list of subjects and objects*], and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.5. Access Control Functions (FDP_ACF)

5.5.1. FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment *: access control SFP*] to objects based on [assignment : *security attributes, named groups of security attributes*].

FDP_ACF.1.2 The TSF 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*].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules : [assignment : *rules, based on security attributes, that explicitly authorize access of subjects to objects*].

FDP_ACF.1.4 The TSF 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*].

5.6. Data Authentication (FDP_DAU)

5.6.1. FDP_DAU.1 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment : *list of objects or information types]*.

FDP_DAU.1.2 The TSF shall provide [assignment : *list of subjects]* with the ability to verify evidence of the validity of the indicated information.

5.7. Export to outside TSF control (FDP_ETC)

5.7.1. FDP_ETC.1 Export of User Data without Security Attributes

FDP_ETC.1.1 The TSF shall enforce the [assignment : *access control SFP(s) and/or information flow control SFP(s)*] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

5.8. Import from Outside TSF Control (FDP_ITC)

5.8.1. FDP_ITC.1 Import of User Data without Security Attributes

FDP_ITC.1.1 The TSF shall enforce the [assignment : *access control SFP and/or information flow control SFP]* when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC : [assignment : *additional importation control rules]*.

5.9. Residual Information protection(FDP_RIP)

5.9.1. FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection : *allocation of the resource to, de-allocation of the resource from]* and the following objects :[assignment : *list of objects*].

5.10. Stored data integrity (FDP_SDI)

5.10.1. FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for [assignment : *integrity errors*] on all objects, based on the following attributes :[assignment : *user data attributes*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment : *action to be taken*].

5.11. Authentication failures (FIA_AFL)

5.11.1. FIA_AFL.1 Basic authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [assignment : *number*] unsuccessful authentication attempts occur related to [assignment :*list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment : *list of actions*].

5.12. User attribute definition (FIA_ATD)

5.12.1. FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users : [assignment : *list of security attributes*].

5.13. User Authentication (FIA_UAU)

5.13.1. FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [assignment : *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.13.2. FIA_UAU.3 Unforgeable authentication

FIA_UAU.3.1 The TSF shall [selection : *detect, prevent*] use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall [selection :*detect, prevent*] use of authentication data that has been copied from any other user of the TSF.

5.13.3. FIA_UAU.4 Single-use Authentication Mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment : *identified authentication mechanism(s)*].

5.14. User identification (FIA_UID)

5.14.1. FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [assignment : *list of TSF mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.15. User-subject Binding (FIA_USB)

5.15.1. FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

5.16. Management of function in the TSF (FMT_MOF)

5.16.1. FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [selection : *determine the behavior of, disable, enable, modify the behavior of*] the functions [assignment : *list of functions*] to [assignment : *the authorized identified roles*]

5.17. Management of security attributes (FMT_MSA)

5.17.1. FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [assignment : *access control SFP, information flow control SFP*] 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 authorized identified roles*].

5.17.2. FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.17.3. FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [assignment *: access control SFP, information flow control SFP*] to provide [selection : *restrictive, permissive, other property*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment : *the authorized identified roles]* to specify alternative initial values to override the default values when an object or information is created.

5.18. Management of TSF data (FMT_MTD)

5.18.1. FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [selection : *change_default, query, modify, delete, clear* [assignment : *other operations*]] the [assignment : *list of TSF data*] to [assignment : *the authorized identified roles*].

5.19. Security management roles (FMT_SMR)

5.19.1. FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [assignments : *the authorized identified roles*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.20. Class FMT : Actions to be taken for management :

Function	Actions	Function	Actions	Function	Actions
FAU_SAA.1	NA	FIA_AFL.1	a)	FMT_MTD.1	a)
FCS_CKM.3	a)	FIA_ATD.1	a)	FMT_SMR.1	NA
FCS_CKM.4	a)	FIA_UAU.1	a)	FPR_UNO.1	NA
FCS_COP.1	NM	FIA_UAU.3	NM	FPT_FLS.1	NM
FDP_ACC.2	NM	FIA_UAU.4	NM	FPT_PHP.3	NA
FDP_ACF.1	a)	FIA_UID.1	NA	FPT_SEP.1	NM
FDP_DAU.1	a)	FIA_USB.1	a)	FPT_TDC.1	NM
FDP_ETC.1	NM	FMT_MOF.1	a)	FPT_TST.1	NA
FDP_ITC.1	a)	FMT_MSA.1	a)		
FDP_RIP.1	NA	FMT_MSA.2	NM		
FDP_SDI.2	NA	FMT_MSA.3	a)		

Table 5.1 : Management activity versus functional requirements

legend :

the letter refers to the respective management defined in part 2 of CC V2.0
NM :No Management activity
NA : Not Applicable

5.21. Unobservability (FPR_UNO)

5.21.1. FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF 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*].

5.22. Fail secure (FPT_FLS)

5.22.1. FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur :[assignment : *list of types of failures in the TSF*].

5.23. TSF Physical protection (FPT_PHP)

5.23.1. FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist [assignment : *physical tampering scenarios*] to the [assignment : *list of TSF devices/elements*] by responding automatically such that the TSP is not violated.

5.24. Domain separation (FPT_SEP)

5.24.1. FPT_SEP.1 TSF Domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.25. Inter-TSF basic data consistency (FPT_TDC)

5.25.1. FPT_TDC.1 Inter-TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment : *list of TSF data types*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [assignment : *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.

5.26. TSF self test (FPT_TST)

5.26.1. TSF Testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests [selection : *during initial start-up, periodically during normal operation, at the request of authorized user, at the conditions* [assignment : *conditions under which self test should occur*]] to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of the stored TSF executable code.

Chapter 6. TOE Security Assurance Requirements

The Assurance requirements is EAL 4 augmented with additional assurance components listed in the following section.
These components are hierarchical ones to the components specified in EAL4.

6.1. ADV_IMP.2 : Implementation of the TSF

Developer action elements:

ADV_IMP.2.1D The developer shall provide the implementation representation for **the entire TSF**.

Content and presentation of evidence elements:

ADV_IMP.2.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.2.2C The implementation representation shall be internally consistent.

ADV_IMP.2.3C The implementation representation shall describe the relationships between all portions of the implementation.

Evaluator action elements:

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

ADV_IMP.2.2E The evaluator shall determine that the **implementation representation** is an accurate and complete instantiation of the TOE security functional requirements.

*Dependencies***:**

ADV_LLD.1 Descriptive low-level design

ADV_RCR.1 Informal correspondence demonstration

ALC_TAT.1 Well defined development tools

6.2. ALC_DVS.2 : Sufficiency of security measures

Developer action elements:

ALC_DVS.2.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.2.3C The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

Evaluator action elements:

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

ALC_DVS.2.2E The evaluator shall confirm that the security measures are being applied.

Dependencies:

No dependencies.

6.3. AVA_VLA.4 Highly resistant

Developer action elements:

AVA_VLA.4.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.4.2D The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.4.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.4.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.4.3C The evidence shall show that the search for vulnerabilities is systematic.

AVA_VLA.4.4C The analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

Evaluator action elements:

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

AVA_VLA.4.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.4.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.4.4E 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.

AVA_VLA.4.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a high attack potential.

Dependencies:

ADV_FSP.1	Informal functional specification
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1	Subset of the implementation of the TSF
ADV_LLD.1	Descriptive low-level design
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance

Chapter 7. PP Application Note

This PP Application Note does not add information but regroup important statements for the comprehension of the document.

An ST claiming this PP shall also claim the Smart Card IC PP (“Smart Card Integrated Circuit Protection Profile”).

The TOE is then the Smart Card Integrated Circuit with Embedded Software in operation, and the scope of the evaluation comprises at least phases 1 to 3 of the Smart Card life cycle.

The Smart Card IC PP is dedicated to phases 2 and 3, and to IC design and realization including software manipulation and embedding.

This PP is dedicated to software development during phase 1. When the TOE is mentioned, it comprises the Smart Card IC with its Embedded Software.

When Assets, Assurance Requirements, Security Objectives are common to the two PP's, they are mentioned in this PP with an asterisk “*”. In this case, the definition of the Smart Card IC PP holds.

This PP does not mention threats and objectives during phases 2 and 3 as they are covered by Smart Card IC PP.

Since the TOE only exists after the end of phase 3, the security objectives for the TOE can only come into play to at this stage to counteract the threats.

Chapter 8. Rationale

8.1. Introduction

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.

8.2. Security objectives rationale

This section demonstrates that the stated security objectives address all the security environment aspects identified. Each security objective being correlated to at least one threat or one assumption.

8.2.1. Threats and security objectives

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

During phase 1, the Smart Card ES is developed and Application Data are specified for all other phases.

The TOE is a functional product designed during phase 1, considering that the only purpose of the Embedded Software is to control and protect the operation of the TOE during phases 4 to 7 (product usage). The global security requirements to consider in the TOE, during the development phase, are the security threats of the other phases. Such threats are identified in chapter 3 of this PP. This is why the PP addresses the functions used in phases 4 to 7 but developed during phase 1.

T.CLON*

The TOE being constructed can be cloned, but also the construction tools and document can help clone it. During phase 1, Since the product does not exist, it cannot contribute to countering the threat. For the remaining phases 4 to 7, the TOE participates in countering the threats.

T.DIS_INFO*

This threat addresses disclosure of sensitive information concerning security mechanisms implemented in the IC and/or in the ES and known by the software developer, in order to meet the overall security objectives of the TOE. Sensitive information are transmitted by the IC designer to the Smart Card Software developer during phase 1.

T.DIS_DEL*

This threat addresses disclosure of software or Application Data which is delivered, from phase 1 to phase 2 for software embedding. As the data is not yet implemented in the TOE, the threat can only be countered by environmental procedures.

T.DIS_DEL1

This threat addresses disclosure of software or data during delivery from phase 1 to phases 4 to 6. As the data is not yet implemented in the TOE, the threat can only be countered by environmental procedures.

T.DIS_DEL2

This threat addresses disclosure of software or data which is delivered from phase 1 to phases 4 to 6. As the data is not yet implemented in the TOE, the threat can only be countered by environmental procedures.

T.DIS_ES1

Although the ES is created in phase 1, it is active throughout the life of the Smart Card, and therefore this threat can be carried out during any and all of phases 1 through 7.
During phases 1 and 2, as the product does not yet exist, so it cannot contribute to countering the threat.

T.DIS_TEST_ES

Tests concerning the embedded software or software to be embedded are carried out in phase 1. This threat is countered by environmental procedures, of which the tests themselves are part.

T.T_DEL*

This threat addresses the theft of software or Application Data which is delivered for software embedding, from phase 1 to phase 2. As the data is not yet implemented in the TOE, the threat can only be countered by environmental procedures.

T.T_TOOLS

TOE development tools are only used during phase 1, so this threat can exist only during phase 1. As the TOE does not yet exist, these threats are countered by environmental procedures.

T.T_SAMPLE2

TOE samples are used only during phase 1, so this threat can exist only during phase 1. The theft or unauthorized use of samples are countered by environmental procedures.

T.MOD_DEL*

This threat addresses modification of software or data which is delivered for software embedding, in phase 2.

T.MOD_DEL1

This threat addresses modification of Application Data during delivery to the IC packaging manufacturer, phase 4, the Finishing process manufacturer, phase 5, and for the Personalizer, phase 6.

T.MOD_DEL2

This threat addresses modification of Application Data which is delivered to the IC packaging manufacturer, phase 4, the Finishing process manufacturer, phase 5, and for the Personalizer, phase 6.

T.MOD

Modification of software and Application Data can be done during ES design in phase 1. Since the product does not exist, the threat can only be countered by environmental objectives.

T.MOD_SOFT*

Once developed, the ES and the Application Data can be modified during any of the phases 4 to 7.

T.DIS_ES2

Disclosure of ES and sensitive data can compromise security. During phases 4 to 7, the TOE must counter the unauthorized disclosure of the ES and the Application Data.

T.T_ES

This threat covers the unauthorized use of stolen cards during the different phases of the Smart Card life cycle as well as the misappropriation of rights of the Smart Cards.

T.T_CMD

This threat includes the diversion of the hardware or the software, or both, in order to execute non authorized operations.

T.MOD_LOAD, T.MOD_EXE, T.MOD_SHARE

The loading, execution and modification of programs shall not endanger the security of the TOE, especially to avoid interference between applications.

8.2.2. Threats addressed by security objectives

8.2.2.1. Security Objectives for the TOE

During phase 1, the TOE does not yet exist, there is no threat on the TOE itself.
For the phases 4 to 7, the following table indicates that each threat is mapped to at least one security objective during the life of the TOE:

Threats/Obj.	TAMPER_ ES	OPERATE*	FLAW*	DIS_ MECHANISM2 .	DIS MEMORY*	MOD_ MEMORY*	CLON*
T.CLON*				X	X		X
T.DIS_ES2	X	X	X	X	X		
T.T_ES	X	X	X			X	
T.T_CMD	X	X	X			X	
T.MOD_SOFT*	X	X	X			X	
T.MOD_LOAD	X	X	X			X	X
T.MOD_EXE	X	X	X			X	X
T.MOD_SHARE	X	X	X			X	X

Table 8.1 Mapping of security objectives to threats relative to phase 4 to 7

The TOE shall use state of the art technology to achieve the following IT security objectives ; for that purpose, when Smart Card IC physical security features are used, the specification of these physical security features shall be respected :

O.TAMPER_ES addresses the protection of the security critical parts of the TOE and protects them from any disclosure, either directly by bypassing protections or indirectly by interpretation of physical or logical behavior. This feature addresses disclosure centered threat T.DIS_ES2.
Security mechanisms must especially prevent the unauthorized modification of security attributes and functional parameters such as the life cycle sequence flags. This feature addresses the modification oriented threats T.MOD_SHARE and T.MOD_SOFT*.
The ES must be designed to avoid interpretations of electrical signals from the hardware part of the TOE. These characteristics cover either the currents, voltages, power consumption, radiation, or timing of signals during the processing activity of the TOE.
The TOE has to provide physical and logical security mechanisms to avoid fraudulent access to any sensitive data, such as passwords, cryptographic keys or authentication data. This covers illegal use or duplication of TOE: T.T_ES, T.T_CMD, T.MOD_LOAD and T.MOD_EXE.

O.CLON* addresses the threat of cloning the TOE, T.CLON*. This objective limits the possibility to access any sensitive security relevant information of the TOE, and thus covers T.MOD_LOAD, T.MOD_EXE and T.MOD_SHARE.

O.OPERATE* The TOE must ensure the correct continuation of operation of its security functions. Security mechanisms have to be implemented to avoid fraudulent usage of an interruption or change in sequence in the normal process order to avoid the security protection. These interruptions or changes may be carried out either by physical or by logical actions(statically or dynamically).
This objective covers the unauthorized change of security attributes managing the access to sensitive information which materialize T.DIS_ES2, T.MOD_SHARE and T._MOD_SOFT*, as well as actions of skipping internal protections of the TOE, which result in threats T.T_ES, T.T_CMD, T.MOD_LOAD and T.MOD_EXE.

O.FLAW* Addresses the threats T.DIS_ES2, T.T_ES, T.T_CMD, T.MOD_LOAD, T.MOD_EXE, T.MOD_SHARE and T._MOD_SOFT* by preventing any unauthorized modification of the TOE which could lead to malfunctions in security mechanisms during its design, production or operation.

O.DIS_MECHANISM2 The TOE shall ensure that the security mechanisms are protected against unauthorized disclosure, to combat the threats T.DIS_ES2 and T.CLON*.
The security mechanism can use either the hardware or the software or both. Such mechanisms must be kept confidential, especially the way to use them in order to counter threats.

O.DIS_MEMORY* The TOE shall ensure that sensitive information stored in memories is protected against unauthorized access. Such disclosure realizes the threats T.DIS_ES2, and can lead to T.CLON*.
This is obvious for secret information, but also applies to access controlled information.

O.MOD_MEMORY* The TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorized modification, which covers T.MOD_SOFT* and modification by unauthorized loading which covers T.MOD_LOAD.
The TOE shall also ensure that any loss of integrity cannot endanger the security, especially in case of modification of system flags or security attributes. It helps to combat T.MOD_EXE and T.MOD_SHARE threats.
The TOE shall prevent the fraudulent modification of such information as indicators or flags in order to go backwards,

through the card life cycle sequence to gain access to prohibited information. Such modifications are a first step to realize T.T_ES or T.T_CMD.

8.2.2.2. Security objectives for the environment

The following tables map the security objectives for the environment relative to the various threats.
Tables 8.2 and 8.3 address phase1 and phases 4 to 6 respectively :

Threats/Obj	DEV_TOOLS*	DEV_DIS_ES	SOFT_DLV*	INIT_ACS	SAMPLE_ACS
T.CLON*	X	X	X	X	X
T.DIS_INFO*		X			
T.DIS_DEL*	X	X	X	X	
T.DIS_ES1	X	X		X	
T.DIS_TEST_ES	X	X	X		
T.T_DEL*			X		
T.T_TOOLS	X				
T.T_SAMPLE2					X
T.MOD_DEL*		X	X	X	
T.MOD		X		X	

Table 8.2 Mapping of security objectives for the environment to threats relative to phase 1

O.DEV.TOOLS* The development tools shall provide for the integrity, availability and reliability of both programs and data. This specificity will protect against cloning, T.CLON*.
Information Technology equipment are used to develop, to test, debug, modify, load the ES and personalize the TOE. Therefore, these equipment shall be accessible only by authorized personnel. This is to cover threats based on illegal access to equipment or development information: T.DIS_ES1,T.DIS_TEST_ES, T.T_TOOLS.

O.DEV_DIS_ES The ES shall be designed in a secure manner, in order to focus on the integrity availability and confidentiality of programs and data.

It must be ensured that confidential information (such as user manuals and general information on defined assets) are only delivered to the parties authorized personnel. This covers the disclosure based threats: T.DIS_INFO*, T.DIS_DEL*, T.DIS_ES1 and T.DIS_TEST_ES, and thus helps to combat T.MOD, T.MOD_DEL* and T.CLON*.

O.SOFT_DLV* O.SOFT_DLV addresses all the threats applicable to the delivery of the Smart Card 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* , T.MOD) and the confidentiality of the software if applicable (T.DIS_DEL*). and of initialization data (T.DIS_ES1) and test information (T.DIS_TEST_ES). This contributes to combat the threat T.CLON*.

O.INIT_ACS It must be ensured that Initialization Data are only delivered to the parties authorized personnel and that Initialization Data integrity is achieved. This covers disclosure based threats: T.DIS_DEL* and T.DIS_ES1. It also covers the theft based threats: illegal modification T.MOD_DEL* and T.MOD. All of this contributes to combat T.CLON*.

O.SAMPLE_ACS Samples used to run tests shall be accessible only by authorized personnel in order to avoid illicit use of such samples. These sample must be considered as sensitive parts, especially because they can be used (with the relevant parameters) in the place of trusted TOEs. This covers T.T_SAMPLE2 and T.CLON*.

Threats	DLV_ DATA	TEST_OPERATE*
T.DIS_DEL1	X	
T.DIS_DEL2		X
T.MOD_DEL1	X	
T.MOD_DEL.2		X

Table 8.3 Mapping of security objectives for the environment to threats on delivery for phase 1 to phases 4 to 6

O.DLV_DATA Protects against disclosure or modification of Application Data during the delivery to other manufacturers, and thus covers : T.DIS_DEL1 and, T.MOD_DEL1.

O.TEST_OPERATE Protects against disclosure or modification of Application Data delivered to other manufacturers and thus covers T.DIS_DEL2 and T.MOD_DEL2.

8.2.3. Assumptions and security objectives for the environment

This section demonstrates that the combination of the security objectives is suitable to satisfy the identified assumptions for the environment.
Each of the assumptions for the environment is addressed by objectives.
Table 8.4 demonstrates which objectives contribute to the satisfaction of each assumption. For clarity, the table does not identify indirect dependencies.
This section describes why the security objectives are suitable to provide each of the assumptions.

Phases		Phase 1			Delivery process for phases 4 to 7			Phases 4 to 6	Phase 7
	Assumptions	DEV_ DIS_ES	DEV_ TOOLS*	SOFT_ DLV*	DLV_ PROTECT*	DLV_ AUDIT*	DLV_ RESP*	TEST_ OPERATE*	USE_ DIAG*
1	DEV_ORG*	X	X	X					
4 to 7	DLV_PROTECT*				X				
4 to 7	DLV_AUDIT*					X			
4 to 7	DLV_RESP*						X		
4 to 6	USE_TEST*							X	
4 to 6	USE_PROD*							X	
7	USE_DIAG*								X

Table 8.4.mapping of security objectives for the environment to assumptions

8.3. Security requirements rationale

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

8.3.1. Security functional requirements rationale

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

The table 8.5 demonstrates which security functional requirements contributes to the satisfaction of each TOE security objective. For clarity, the table does not identify indirect dependencies.

Security Requirements	TAMPER_ ES	OPERATE*	DIS_ MECHANISM2	DIS_ MEMORY*	MOD_ MEMORY*	FLAW*	CLON*
EAL4 requirements						X	
FAU_SAA.1	X	P	P	X	X		
FCS_CKM.3	X	P		P	P		P
FCS_CKM.4	X	P		P	P		X
FCS_COP.1	X			X			P
FDP_ACC.2	X	P	X	X	P		P
FDP_ACF.1	X	P	X	X	P		P
FDP_DAU.1	X	P			X		P
FDP_ETC.1				X	P		
FDP_ITC.1				X			
FDP_RIP.1	X			P			
FDP_SDI.2		P			X		
FIA_AFL.1	X	P			P		P
FIA_ATD.1	X	P			P		
FIA_UAU.1	X			X	X		P
FIA_UAU.3	X			X	X		P
FIA_UAU.4	X			X	X		P
FIA_UID.1	X			X	X		P
FIA_USB.1	X			X	X		P
FMT_MOF.1	X	X	X	P	P		P
FMT_MSA.1	X	P	X	P	P		P
FMT_MSA.2	X	P	X	P	P		P
FMT_MSA.3	X	P	X	P	P		P
FMT_MTD.1				X	X		P
FMT_SMR.1	X	X					
FPR_UNO.1	X	P		X	X		X
FPT_FLS.1	X						
FPT_PHP.3	X	X	X	X	X		X
FPT_SEP.1	X		X	X			
FPT_TDC.1	X				X		
FPT_TST.1		P			X		

Table 8.5 Mapping of security functional requirements and objectives
legend : P :Partial ; X :relevant

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

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

As the TOE is able to detect potential physical violation via sensors and related circuitry, and logical violation through TSF enforcing functions, FAU_SAA.1 meets the security objectives O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY* and partially O.OPERATE* and O.DIS_MECHANISM2 in order to monitor events and indicate a potential violation of the TSP.

Cryptographic support functional requirements : FCS_CKM.3 and FCS_CKM.4 support the access control to the assets by key management and key destruction in the case of illicit access, or any attempt to steal sensitive information. These functions combine to meet the security objectives of O.TAMPER_ES, and participate in meeting O.OPERATE*, O.DIS_MEMORY*, O.MOD_MEMORY* and O.CLON* requirements. FCS_COP.1 which support data encryption or electronic signature controls the assets by authentication mechanisms and encryption. This function combine to meet the security objectives of O.TAMPER_ES, O.DIS_MEMORY* and also contributes to O.CLON*.

Access control functional requirements , FDP_ACC.2 and FDP_ACF.1 control the access conditions. This fulfills the security objectives, O.TAMPER_ES, O.DIS_MECHANISM2, O.DIS_MEMORY* and partially O.OPERATE* and O.MOD_MEMORY*. They participate in the fulfillment of O.CLON*.

The Data authentication functional requirement FDP.DAU.1 assures the objectives O.TAMPER_ES and O.MOD_MEMORY*. It contributes to the correct operation of TOE, O.OPERATE, and O .CLON*.

The export to outside TSF control functions FDP_ETC.1, contribute to realization of O.DIS_MEMORY*. They contribute to the correct operation of the TOE, O.MOD_MEMORY*.

Sensitive information can be securely imported from outside in order to be processed or stored inside the TOE. The TSF control functions FDP_ITC.1, contribute to the realization of O.DIS_MEMORY*.

FDP_RIP.1 prevents to access to residual sensitive information which was temporarily stored in memories during previous states of processing. This functional requirement meets O.TAMPER_ES objectives and partially O.DIS_MEMORY*.

The FDP_SDI.2 functional requirement meets O.MOD_MEMORY* objectives. It also contributes to the correct operation of TOE which covers O.OPERATE* .

Identification and authentication functional requirements FIA_AFL.1 and FIA_ATD.1 which manage illicit authentication attempts and related security attributes meet O.TAMPER_ES objectives and partially O.OPERATE* and O.MOD MEMORY*. FIA_AFL1 also contributes to the correct operation of the TOE, O.CLON*.

Identification and authentication functional requirements FIA_UAU.1, FIA_UAU.3, FIA_UAU.4, FIA_UID.1 and FIA_USB.1 prevent unauthorized access to stored memory, and thus contributes to security objectives O.TAMPER_ES, O.DIS_MEMORY* and O.MOD_MEMORY*. They also partially contributes to the correct operation of the TOE, O.CLON*.

FMT_MOF.1 restricts the ability to modify the access conditions or the user rights This functional requirement meets O.TAMPER_ES, O.OPERATE*, O.DIS_MECHANISM2 and partially O.DIS_MEMORY*, O.MOD_MEMORY*, O.CLON* objectives.

Management of TSF data functional requirements FMT_MSA.1, FMT_MSA.2 and FMT_MSA.3 which control the usage, modification and deletion of the security attributes meet the O.TAMPER_ES, and O.DIS_MECHANISM2 objective and contribute to the correct operation of the TOE, O.OPERATE*, O.DIS_MEMORY*, O.MOD_MEMORY and O.CLON*.

The FMT_MTD.1 controls the authorization to access or modify sensitive information. This functional requirement meets O.DIS_MEMORY* and O.MOD_MEMORY* objectives and partially O.CLON*.

FMT_SMR.1 functional requirement meets O.TAMPER_ES and O.OPERATE* objectives.

The FPR_UNO.1 functional requirement meets O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY*, and O.CLON* especially to protect against the observation of internal processes of the TOE. It provides protection against unauthorized disclosure of sensitive information during operation of the TOE under control of the Embedded Software. Thus, it also contributes to O.OPERATE*.

The FPT_FLS.1 functional requirement meets O.TAMPER_ES objectives.

FPT_PHP.3 (Resistance to physical attack) functional requirement meets O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY* and O.CLON*. FPT_PHP.3 also meets O.OPERATE* and O.DIS_MECHANISM2. It should be noted that FPT_PHP.1 (Passive detection of physical attack) is not relevant for Smart Cards because it is always more secure not to give information on the origin of physical attacks to the outside world, since this could help an attacker to counter a security mechanism.

The FPT_SEP.1 functional requirement meets O.TAMPER_ES, O.DIS_MECHANISM2 and O.DIS_MEMORY* objectives.

The FPT_TDC.1 functional requirement meets O.MOD_MEMORY* and O.TAMPER_ES objectives. The TOE shall interpret consistently the information coming from trusted IT products.

FPT_TST .1 functional requirement meets O.MOD_MEMORY* and partially O.OPERATE*. The suite of self tests may run only during initial start-up of the TOE, aiming at the integrity of executable code and/or sensitive memory content. Each test yields a global answer depending of the result of the test. This test has to be defined, but it is clear that a correct authentication process or a correct cryptographic operation demonstrate the correct operation of the TSF during execution of commands.

8.3.2. Security functional requirements dependencies.

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

The assurance requirements specified by this PP are precisely as defined in EAL4 with several higher hierarchical components (ADV_IMP.2, ALC_DVS.2 and AVA_VLA.4). This is asserted to be a known set of assurance components for which all dependencies are satisfied.

The table 8.6 lists all functional components including security requirements in the IT environment. For each component, the dependencies specified in Common Criteria are listed, and a reference to the component number is given.

Number	Security functions	Dependencies	line N°
1	FAU_SAA.1 : Potential Violation Analysis	**FAU_GEN.1**	**a**
2	FCS_CKM.3 : Cryptographic Key Access	FDP_ITC.1, FCS_CKM.4, FMT_MSA.2	9, 3, 21
3	FCS_CKM.4 : Cryptographic Key Destruction	FDP_ITC.1 , FMT_MSA.2	9, 21
4	FCS_COP.1 : Cryptographic Operation	FDP_ITC.1, FCS_CKM.4, FMT_MSA.2	9, 3, 21
5	FDP_ACC.2 : Complete Access Control	FDP_ACF.1	6
6	FDP_ACF.1 : security attributes based Access Control Functions	FDP_ACC.1, FMT_MSA.3	H(5)[b], 22
7	FDP_DAU.1 : basic Data Authentication	none	
8	FDP_ETC.1 : Export of user data without security attributes	none	
9	FDP_ITC.1 : Import of user data without security attributes	FMT_MSA.3	22
10	FDP_RIP.1 : subset residual information protection	none	
11	FDP_SDI.2 : stored data integrity monitoring and action	none	
12	FIA_AFL.1 : basic authentication failure handling	FIA_UAU.1	14
13	FIA_ATD.1 : user attribute definition	none	
14	FIA_UAU.1 : timing of authentication	FIA_UID.1	17
15	FIA_UAU.3 : unforgeable authentication	none	
16	FIA_UAU.4 : Single-use authentication mechanisms	none	
17	FIA_UID.1 : timing of identification	none	
18	FIA_USB.1 : user-subject binding	FIA_ATD.1	13
19	FMT_MOF.1 : management of security functions behavior	FMT_SMR.1	24
20	FMT_MSA.1 : management of security attributes	FMT_SMR.1	24
21	FMT_MSA.2 : safe security attributes	ADV_SPM.1, FMT_MSA.1, FMT_SMR.1	by EAL4 20, 24
22	FMT_MSA.3 : safe attributes initialization	FMT_MSA.1, FMT_SMR.1	20, 24,
23	FMT_MTD.1 : management of TSF data	FMT_SMR.1	24
24	FMT_SMR.1 : security roles	FIA_UID.1	17
25	FPR_UNO.1 : Unobservability	none	
26	FPT_FLS.1 : failure with preservation of secure state	ADV_SPM.1	by EAL4
27	FPT_PHP.3 : Resistance to physical attacks	none	
28	FPT_SEP.1 : TSF Domain separation	none	
29	FPT_TDC.1 : inter-TSF basic TSF data consistency	none	
30	FPT_TST.1 : TSF testing	**FPT_AMT.1**	**a**

a : dependencies are not met for reasons given below

b: H(5) means that the dependency is satisfied by a higher hierarchical component

Table 8.6 : Functional dependencies

Table 8.6 shows that the functional component dependencies are satisfied by any functional component of the PP except for the components stated in bold characters, as explained as follows:
The dependency of FAU_SAA.1 with FAU_GEN.1 is not applicable to the TOE ; the FAU_GEN.1 component forces many security relevant events to be recorded (due to dependencies with other functional security components) and this is not achievable in a Smart Card since many of these events result in card being in an insecure state where recording of the event itself could cause a security breach. 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.

The dependency of FPT_TST.1 with FPT_AMT.1 is not clearly relevant for a Smart Card ; FPT_TST.1 is self-consistent for the TOE (hardware and software) and does not require the FPT_AMT.1 function (Abstract Machine Testing). The TOE software is not tested inside the scope of FPT_TST.1. In its relations with external devices, typically the card reader, the TOE is always the slave. This is why FPT_TST.1 is self consistent, and FPT_AMT.1 is not applicable.

8.3.3. Strength of function level rationale

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

8.3.4. Security assurance requirements rationale

The assurance requirements of this Protection Profile are summarized in the following table :

Requirements	**Name**	**Type**
EAL4	Methodically Designed, Tested and Reviewed	Assurance level
ADV_IMP.2	Implementation of the TSF	Higher hierarchical component
ALC_DVS.2	Development Security Measures	Higher hierarchical component
AVA_VLA.4	Highly resistant	Higher hierarchical component

table 8.7 -PP assurance requirements

Evaluation Assurance level rationale

An assurance requirement 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 defense against such attacks, the evaluators should have access to the low level design and source code. The lowest for which such access is required is EAL4.
The assurance level EAL4 is achievable, since it requires no specialist techniques on the part of the developer.

Assurance augmentations rationale

Additional assurance requirements are also required due to the definition of the TOE and to the conformance to the ITSEC evaluation level E3 with a strength of mechanism high.

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. ES source code is an example of implementation representation.
This assurance component is a higher hierarchical component to EAL4 (only ADV_IMP.1 is found in EAL4.) It is important for a Smart Card that the evaluator evaluates the implementation representation of the entire TSF to 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 components are included in EAL4, and so these dependencies are satisfied.

ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE.
This assurance component is a higher hierarchical component to EAL4 (only ALC_DVS.1 is found in EAL4). Due to the nature of the TOE, there is a need to justify the sufficiency of these procedures to protect the confidentiality and the integrity of the TOE.
ALC_DVS.2 has no dependencies.

AVA_VLA .4 Highly resistant

Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks. This is due to the fact that a Smart Card can be placed in a hostile environment, such as electronic laboratories.

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.

8.3.5. Security requirements are mutually supportive and internally consistent.

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

No detailed analysis is given in respect to the assurance requirement because :

- EAL4 is an established set of mutually supportive and internally consistent assurance requirements,
- 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).
- The dependencies analysis for the functional requirements described above demonstrate mutual support and internal consistency between the functional requirements.
- Inconsistency between functional and assurance requirements can only arise if there are functional-assurance dependencies which are not met, a possibility which has been shown not to arise in the above section "Security functional requirements dependencies".

Therefore, the dependencies analysis described above demonstrates mutual support and internal consistency between the functional requirements.

Annex A

Glossary

Application Software (AS)

Is the part of ES in charge of the Application of the Smart Card IC.

Application Data

IC and system specific data, Initialization data, IC pre-personalization requirements and personalization data

Basic Software (BS)

Is the part of ES in charge of the generic functions of the Smart Card IC such as Operating System, general routines and Interpretors.

DAC

Discretionary Access Control

Embedded Software (ES)

Is defined as the software embedded in the Smart Card Integrated Circuit. The ES may be in any part of the non-volatile memories of the Smart Card IC.

Embedded software developer

Institution (or its agent) responsible for the Smart Card embedded software development and the specification of pre-personalization requirements.

Initialization

Is the process of writing specific information in the NVM during IC manufacturing and testing (phase 3) as well as executing security protection procedures by the IC manufacturer. The information could contain protection codes or cryptographic keys.

Initialization Data

Specific information written during manufacturing or testing of the TOE

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 purposes; it may either be IC embedded software(also known as IC firmware) or test programs 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-personalization.

IC packaging manufacturer

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

Personalizer

Institution (or its agent) responsible for the Smart Card personalization and final testing.

Personalization data
Specific information in the NVM during personalization phase

Role

A predefined set of rules establishing the allowed interactions between a user and the TOE

Security Information

Secret data, initialization data or control parameters for protection systems)

Smart Card

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

Smart Card Issuer

Institution (or its agent) responsible for the Smart Card product delivery to the Smart Card end-user.

Smart Card product manufacturer

Institution (or its agent) responsible for the Smart Card product Finishing process and testing.

Smart Card Application Software (AS)

Is the part of ES dedicated to the applications

Abbreviations

CC
Common Criteria

EAL

Evaluation Assurance Level. A package consisting of assurance components that represents a point on the CC predefined assurance scale

IT

Information Technology

NVM

Non Volatile Memory

PP

Protection Profile. An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
SF

Security function. A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP

SOF

Strength of Function

ST

Security Target. A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE

TOE

Target of Evaluation

TSC

TSF Scope of Control. The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

TSF

TOE Security functions

TSF data

Data created by and for the TOE, that might affect the operation of the TOE, especially specific data managed by the ES.

TSFI

TSF Interface

TSP

TOE Security Policy. A set of rules that regulate how assets are managed, protected and distributed within a TOE.

User data

Application Data introduced during User phase.