EUROSMART
European Smart Card Industry Association

Common Criteria

For Information Technology

Security Evaluation

Protection Profile

Smart Card IC

with Multi-Application Secure Platform

Version 2.0

Issue November 2000

Common Criteria

This version is in compliance with CC V2.1 and ISO/IEC 15408

Registered at the French Certification Body under the number PP/0010

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 – CP8**
  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

- **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
  Telephone : (+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
  Telephone : (+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
  Telephone: (33) 1 30 67 58 00
  Fax: (33)1 30 67 59 37

- **OBERTHUR Card Systems**
  12 bis, rue des Pavillons - BP 133
  92804 PUTEAUX, France
  Telephone : (+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
  Telephone : (+49).8165 930 0
  Fax : (+49) 8165 930 202

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

- **PHILIPS Semiconductors Hamburg**
  UB Philips GmbHD-22502 HAMBURG, Germany
  Telephone : (+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
  Telephone : (+33) 1 47 46 62 01
  Fax : (+33) 1 47 46 55 48 www.slb.com

- **SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE**
  Direction Centrale de la Sécurité des Systèmes d'Information
  Centre de Certification
  51, boulevard de Latour-Maubourg
  75700 PARIS 07 SP
  Telephone: (+33) 1 41 46 37 20
  Fax : (+33) 1 41 46 37 01

- **ST Microelectronics**
  ZI de Rousset BP2
  F- 13106 ROUSSET CEDEX, France
  Telephone : (+33) 4.42.68.88.00
  Fax : (+33) 4.42.68.87.29 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
- http://www.scssi.gouv.fr

This PP is available at the following addresses:

- http://www.eurosmart.com/
- http://www.scssi.gouv.fr,

Table of Content

1 PP INTRODUCTION 6

1.1 PP IDENTIFICATION 6
1.2 PP OVERVIEW 7

2 TOE DESCRIPTION 9

2.1 PRODUCT TYPE 9
2.2 SMART CARD PRODUCT LIFE-CYCLE 12
2.3 LOADED-APPLICATION LIFE CYCLE 15
2.4 TOE ENVIRONMENT 15
2.5 TOE LOGICAL PHASES 16
2.6 TOE INTENDED USAGE 17
2.7 GENERAL IT FEATURES OF THE TOE 18

3 TOE SECURITY ENVIRONMENT 19

3.1 ASSETS 19
3.2 ASSUMPTIONS 20
3.3 THREATS 21
3.4 ORGANIZATIONAL SECURITY POLICIES 28

4 SECURITY OBJECTIVES 29

4.1 SECURITY OBJECTIVES FOR THE TOE 29
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 31

5 TOE SECURITY FUNCTIONAL REQUIREMENTS 34

5.1 SECURITY AUDIT AUTOMATIC RESPONSE (FAU_ARP) 34
5.2 SECURITY AUDIT ANALYSIS (FAU_SAA) 34
5.3 CRYPTOGRAPHIC KEY MANAGEMENT (FCS_CKM) 35
5.4 CRYPTOGRAPHIC OPERATIONS (FCS_COP) 35
5.5 ACCESS CONTROL POLICY (FDP_ACC) 35
5.6 ACCESS CONTROL FUNCTIONS (FDP_ACF) 36
5.7 DATA AUTHENTICATION (FDP_DAU) 36
5.8 EXPORT TO OUTSIDE TSF CONTROL (FDP_ETC) 37
5.9 IMPORT FROM OUTSIDE TSF CONTROL (FDP_ITC) 37
5.10 RESIDUAL INFORMATION PROTECTION(FDP_RIP) 37
5.11 ROLLBACK (FDP_ROL) 38
5.12 STORED DATA INTEGRITY (FDP_SDI) 38
5.13 AUTHENTICATION FAILURES (FIA_AFL) 39
5.14 USER ATTRIBUTE DEFINITION (FIA_ATD) 39
5.15 USER AUTHENTICATION (FIA_UAU) 39
5.16 USER IDENTIFICATION (FIA_UID) 40
5.17 USER-SUBJECT BINDING (FIA_USB) 40
5.18 MANAGEMENT OF FUNCTION IN THE TSF (FMT_MOF) 40
5.19 MANAGEMENT OF SECURITY ATTRIBUTES (FMT_MSA) 41
5.20 MANAGEMENT OF TSF DATA (FMT_MTD) 41
5.21 SECURITY MANAGEMENT ROLES (FMT_SMR) 42
5.22 CLASS FMT : ACTIONS TO BE TAKEN FOR MANAGEMENT : 43
5.23 UNOBSERVABILITY (FPR_UNO) 43
5.24 FAIL SECURE (FPT_FLS) 44

5.25 TSF PHYSICAL PROTECTION (FPT_PHP) 44
5.26 TRUSTED RECOVERY (FPT_RCV) 44
5.27 REFERENCE MEDIATION (FPT_RVM) 44
5.28 DOMAIN SEPARATION (FPT_SEP) 45
5.29 INTER-TSF TSF DATA CONSISTENCY (FPT_TDC) 45
5.30 TSF SELF TEST (FPT_TST) 45
5.31 RESOURCE ALLOCATION (FRU_RSA) 46

6 TOE SECURITY ASSURANCE REQUIREMENTS 47

6.1 ADV_IMP.2 : IMPLEMENTATION OF THE TSF 47
6.2 ALC_DVS.2 : SUFFICIENCY OF SECURITY MEASURES 48
6.3 AVA_VLA.4 HIGHLY RESISTANT 49

7 PP APPLICATION NOTE 50

8 RATIONALE 51

8.1 INTRODUCTION 51
8.2 SECURITY OBJECTIVES RATIONALE 51
8.3 SECURITY REQUIREMENTS RATIONALE 61

1 ANNEX A GLOSSARY 72

2 ANNEX B MAPPING WITH PP/9806 76

1 PP introduction

1.1 PP Identification

Title : Smart Card IC with Multi-Application Secure Platform

Version : V2.0, issue November 2000

Registration : registered at French Certification Body under the number PP/0010

Registration	Version number	Common Criteria
PP/0010	V2.0	version 2.1

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" .

A Security Target compliant with this PP shall claim the compliance to the PP/9806. Indeed, this PP shall not be used independently.

For the sake of clarification, items which are common with PP/9806 will be indicated by a "*" in this PP. In case of discrepancy the component described in this PP/9806 shall be considered as the reference.

A product compliant with this PP may also offer additional security functional requirements, depending on the Native or Loaded-Application types.

1.2 PP overview

Evolution of Smart Cards toward Multi-Application platform as well as multi-layer architecture leads to additional requirements. This PP is upwardly compatible with the PP/9806 and PP/9911 but provides extensions based on the following:

- The dedicated Software acts as an hardware/software secure interface between the IC and the Operating system
- The Loaded-Application System Interface acts as an interface between the Operating system and Loaded-Application Software
- The IC can be designed concurrently with an Operating System and Loaded-Application System Interface.
- The integrated circuit with its Dedicated Software ensures secure exchange of information with the Operating System
- The IC with its Dedicated Software, its Operating System and its Loaded-Application System Interface ensures secure exchange of information with the Loaded-Applications

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
- GEMPLUS
- GIESECKE & DEVRIENT
- HITACHI
- MICROELECTRONICA Española
- MOTOROLA - SPS
- NEC Electronics
- OBERTHUR Card Systems
- ODS
- ORGA
- PHILIPS
- SCHLUMBERGER
- INFINEON Semiconductors
- ST Microelectronics

The intent of this Protection Profile is to specify functional and assurance requirements applicable to a functional Smart Card IC with its embedded software dedicated to multi-application.

The Platform can receive Loaded-Application software at different stages of its life cycle corresponding to different administrators. Loaded-Applications can be either independent or cooperatives. The Platform provide tools for either a total firewalling between Loaded-Applications or to have controlled communications between them

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 Multi-Application Secure Platform built in a Smart integrated circuit. It is considered that the purpose of this platform developed during phase 1 is to control the operation of the Smart Card during phase 4 to 7 (operational phases) and to support several Loaded-Application software .

- 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 operational phases of the card.

- to describe the security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of Loaded-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).

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, independent of the physical interface, the way it is packaged and any other security device supported by the physical card base. The Embedded Software comprises the Multi-Application Platform and eventually integrated applications. 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.

A multi-application Smart Card is composed of hardware and software components, such as:

- IC hardware
- Dedicated Software
- Operating system
- Loaded-Application system Interface
- Loaded-Application layer

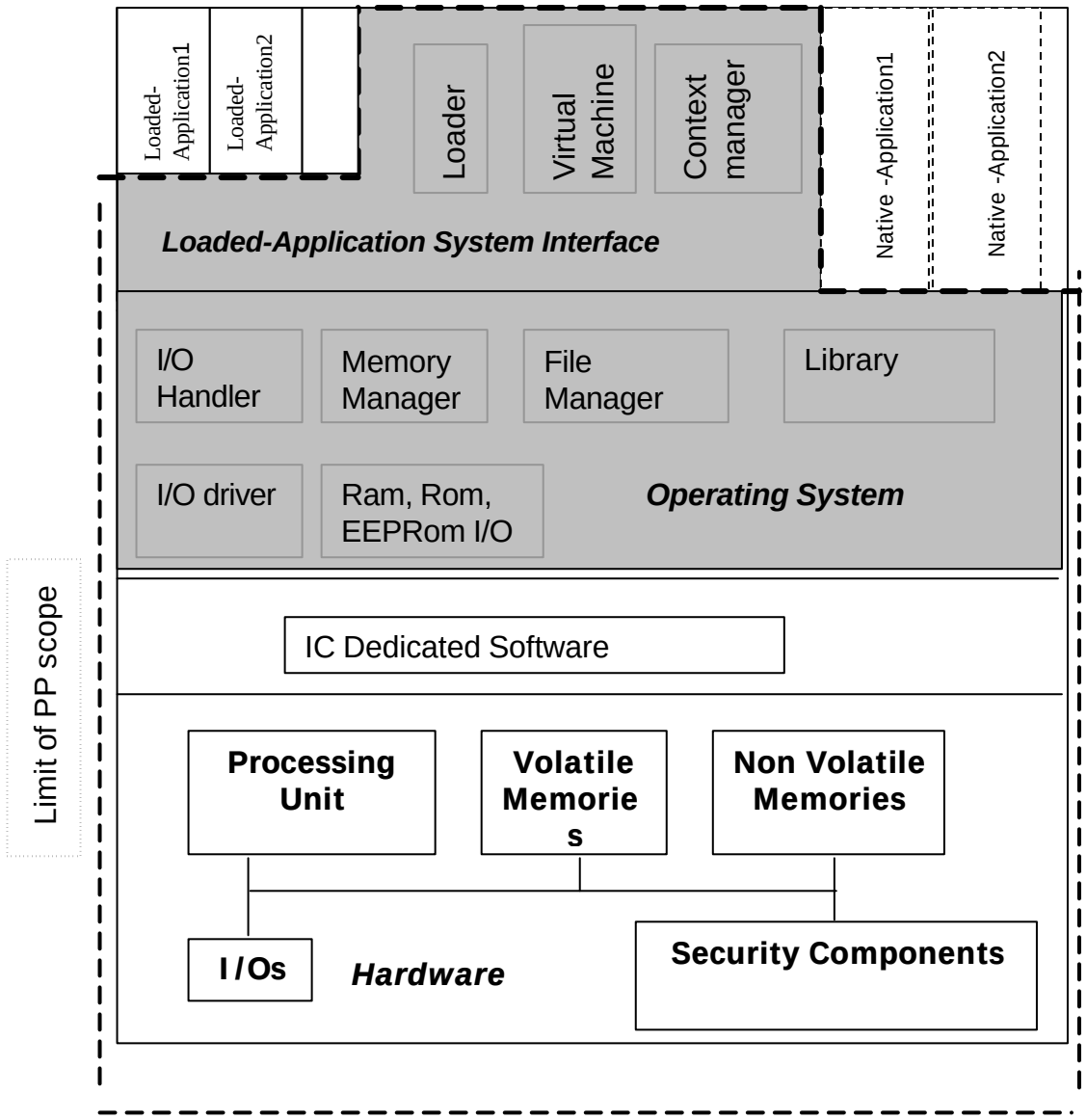

Fig 1 : Typical IC with Multi-Application Platform model

The typical TOE is composed of

- IC hardware layer including a processing unit, volatile and non-volatile memories with the ES, I/O ports and security components.
- IC Dedicated software designed and manufactured by the IC designer/manufacturer. This software (also known as firmware) is often used for testing purpose during IC manufacturing, but may also include additional services.
- Operating System which includes:
  - At a first level: I/O driver, RAM ROM and EEPROM I/O, and hardware drivers.
  - At a second level: I/O handlers and protocols, memory manager, file manager, crypto-server and related services found in a library.

- Native-Applications, if they exist, which access directly to the Operating system. Native applications can be embedded directly by the IC manufacturer (during phase 3), or can be integrated later at the personalisation phase.

- Loaded-Application System Interface which may be composed of the following components:
  - The Loader
  - One or several Virtual Machines
  - Context Manager

Even if this PP does not specifically address Native Applications, the Security Target claiming this PP must include the Native-Applications and at least mandate a demonstration that they do not degrade the security level of the Smart Card IC Multi-Application Secure Platform. If Native-Applications are integrated during the Personalisation phase, the Security Target will have to include this phase.

NOTE: Even if the Native-Applications have no specific security requirements, the assurance requirements must prove that they do not degrade the Integrated Circuit with Multi-Application Platform security. The assurance level of this proof must be at least equal to that required by the PP. Note that this is also required to conform to the Common Criteria.

As a matter of fact, the actual layering depends on the considered TOE and will be precisely described in the ST.

This Protection profile adds (grayed part of fig. 1) to the PP/9806:
- the requirements of the Operating System software embedded in the Smart Card Integrated Circuit, (same as PP/9911)
- necessary requirements to assure the security of the Smart Card IC with Multi-Application Platform and mostly of the Loaded-Application system interface.

NOTE: The term Embedded Software defines the software developed by the smart card software developer and sent to the IC manufacturing for embedding. This software may be in any part of the non-volatile memory.
Embedded software is composed of Operating System and Loaded-Application Interface, but can also include Native-Applications.

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 "

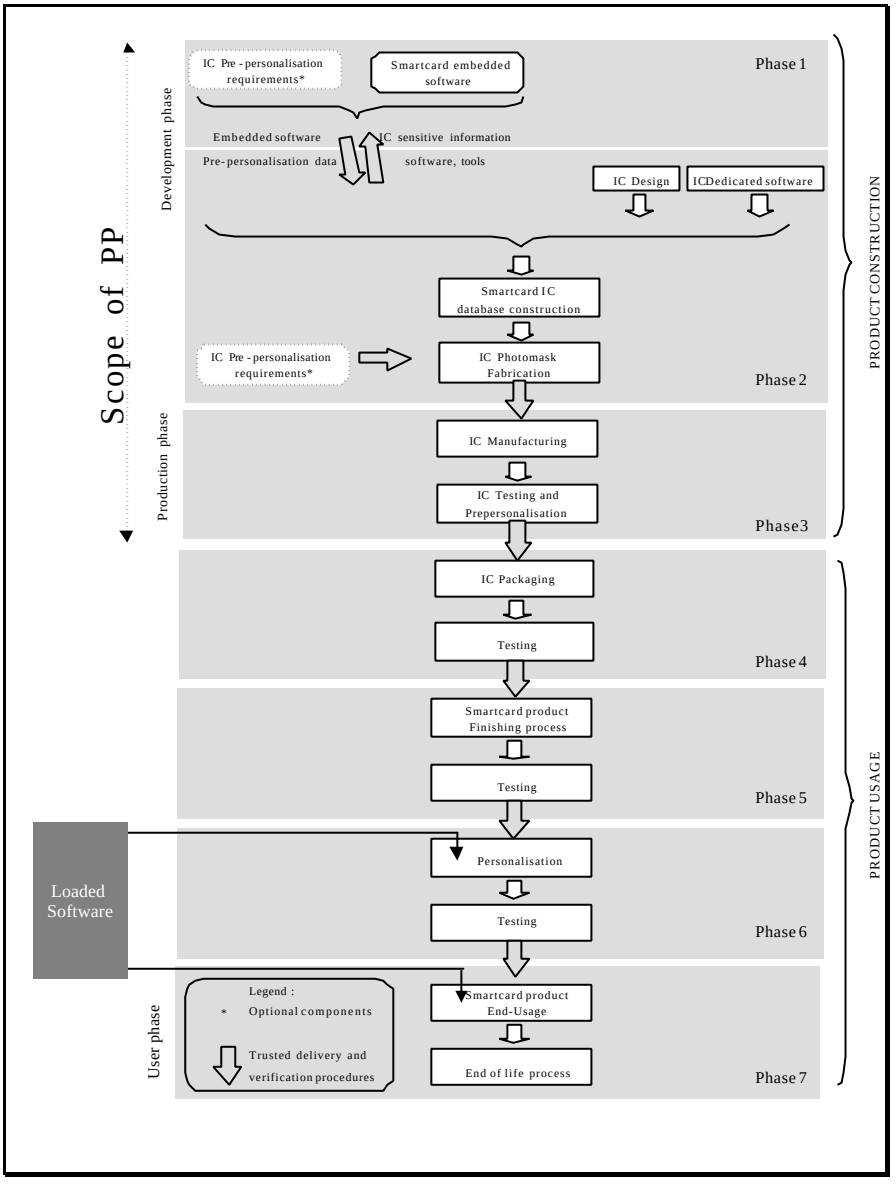

Figure 2: Smart Card IC with Multi-Application Platform life-cycle.

The limits of the protection profile correspond to phases 1, 2 and 3, including the delivery of the TOE to the packaging manufacturer. Procedures concerning phases 4, 5, 6, 7 and Loaded-Application development are outside the scope of this PP.

The purpose of the Platform designed during phase 1 is to control and protect the TOE during phase 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.

Note: The scope of this PP covers phases one to three. The TOE at the end of phase 3 is not a finished product, so it is highly recommended that the ST claiming this PP includes security requirements which cover the assumptions on phases 4, 5 and on phase 6 up to the desabling of the Native-Application integration facility if it exists.

The following table complements the table of paragraph 2.2 Smartcard Product Life-cycle of PP/9806 where it is necessary for Multi-Application Platform.

Phase 1	Smart Card Software Development	The Smart Card software developers are in charge of the Basic Software, the Operating system, the Loaded-Application System Interface development and the specification of Initialization requirements. The developers are also responsible for the development of potential Native-Applications.
Phase 3	IC manufacturing and testing	The IC manufacturer is responsible for producing the IC including the ES. Personalisation keys are loaded. OS, Loaded-Application management system (VM, Loader, Context Manager) may be initialized during this phase
Phase 6	Smart card Personalization	The Personaliser is responsible for the Smart card personalisation and final tests. The Personaliser is also responsible for integrating Native-Applications delivered by the Smart Card Software Developers and which are not part of the ES (embedded during phase 3) and then disabling the integration feature. OS, Loaded-Application system (VM, Loader, Context Manager) is initialized (if not already done) Smart card Loaded-Application Software and data provided by the Loaded-Application Provider may be loaded onto the chip at the personalisation process.
Phase 7	Smart card end-usage	The Loaded-Application Provider is responsible for supplying Loaded-Application data or user data or programs to be remotely or not downloaded into the TOE

Dedicated Software, Operating System and Loaded-Application System Interface 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 Loaded-Application life cycle

Loaded-Applications have a distinct life cycle from that of the platform. The life cycle can also be split into different life phases.

Phase A1	Loaded-Application Development	This phase precedes loading of the Loaded-Application. If this is respected, it can be in parallel with any of the Smart Card IC with Multi-Application Platform life phases.
Phase A2	Loaded-Application loading	Corresponds to phase 6 or to phase 7
Phase A3	Loaded-Application end usage	This is included in 7. It can come to an end before phase 7 does if the Loaded-Application is removed.

2.4 TOE Environment

Considering the TOE, the environment is defined as follows :

- Development environment corresponding to phase 1 and 2
- Production environment corresponding to phase 3 including the integration of the ES in the IC and the test operations
- Packaging of the TOE and finishing operations corresponding to phases 4 and 5.
- Personalisation environment corresponding to personalisation and testing of the Smart Card with the user data (phase 6 or 7). Downloading of Loaded-Application software can occur during this phase. Native-Applications can also be integrated.
- User environment corresponding to downloading of Loaded-Application software and related data (phase 7)

2.4.1 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 be involved to 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 Agreement's.

Design and development of the ES then follow. 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 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)

2.4.2 TOE Production environment

The production environment is defined in Smart card IC PP.

2.4.3 TOE User environment

Phase 4 and 5:

During phases 4 and 5, the TOE is 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 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.

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

During this phase, Loaded-Applications can be loaded on the platform, and Native-Applications integrated.

Phase 7:

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

During this phase, Loaded-Applications can be loaded on the platform in an insecure environment..

2.5 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.

2.6 TOE intended usage

The TOE is a Smart Card IC with Multi-Application platform. Several Loaded-Applications coexist in the same Smart card. Some examples of Loaded-Applications are presented hereafter:

- 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, health cards, driver license etc...).
- multimedia commerce and Intellectual Property Rights protection.

During the phase 1, 2 and 3 the TOE is being developed and produced. The **actors** are the following :

- The IC designer
- The OS developer
- The Loaded-Application System Interface software developer
- the Native-Application Software developer
- The IC manufacturer

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

Phase 4

- IC packaging manufacturer (administrator)

Phase 5:

- The Smart card product manufacturer (administrator)

Phase 6:

- The personaliser (administrator)
- The Smart card Issuer
- The Loaded-Application Provider(s)

Phase 7:

- The Smart card issuer (administrator)
- The Smart card end-user
- The Loaded-Application Provider(s)

2.7 General IT features of the TOE

The TOE security functionality consists in the maintenance of:

- Integrity and confidentiality of Native and or Loaded Applications. This to assure that the applications correspond to their expectations, and that know-how and existing security mechanisms are not revealed.
- Prevention of encroachment of loading and unloading of applications on Loaded-Applications
- Maintaining secure Domain separation of Loaded-Applications
- Integrity and confidentiality of Native and Loaded-Application TSF data.
- Integrity and/or confidentiality of End User Data which have been stored on the TOE when it is required. (For example result of health check-up, audit tracks of financial transactions…),
- Correct operation of arithmetical functions (e.g. incrementing counters in electronic purses, calculating currency conversation in electronic purses...) which are part of the security chain of the system using the TOE.
- Correct operation of application cryptographic functions when required (e.g. electronic signature for legal recognition , e-commerce...) which are part of the security chain of the system using the TOE.
- Contribution to secure data communication,
    - Ciphering and/or stamping of exported data
    - Deciphering and/or origin verification of imported data

3 TOE 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 organizational security policies and the assumptions.

3.1 Assets

Assets are security relevant elements of the TOE that include

Assets linked to the IC with Multi-Application Secure Platform itself

- The IC specifications, design, development tools
- The IC Dedicated software,
- Multi-Application Platform Software
- Multi-Application Platform specifications, implementation, test programs and related documentation,
- The TSF data (such as IC and Multi-Application Platform specific data, Initialization data, IC pre-personalisation requirements and personalisation data,).

Assets linked to the eventual Integrated Applications

- Native-Application software.
- Native-Application TSF data such as keys and identification data.

Assets are also linked to Loaded-Applications on the platform.

- Application provider User Data.:
  - Loaded-Application software loaded on the platform.
  - Loaded-Application SF data. (SF data for the eventual Loaded Application Security Functions)
- The TOE resources
  - Card resources: memory space and computation power made available to a Loaded-Application and its security functions.

Assets are also linked to end user, card holder and application provider.

- End User Data for users of Native Applications
- End User Data for users of Loaded Applications.

NOTE: even if the PP scope does not include the applications, the TOE must provide security mechanisms such that Native or Loaded Applications can protect the Ed User data when required.

Assets have to be protected in terms of confidentiality, authenticity and control of their origin.

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 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.

3.2.2 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).

3.2.3 Assumption on phase 7

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

3.2.4 Assumption on Loaded-Application development (phase A1)

A.APPLI_CONT	Whenever a Loaded-Application is to be loaded on the platform, it is assumed that its development and production follow the Administrator Guidance.

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. This threat addresses User Data and potentially TSF data.

3.3.2 Threats on phase 1

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

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

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 threat 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 Asset Smart Card Embedded Software and any additional *application data* (such as IC pre-personalisation requirements) during the delivery to the IC designer.
NOTE	*application data means TSF data*
T.DIS_ES1 (type a)	Unauthorized disclosure of ES (technical or detailed specifications, implementation code) and/or TSF 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 personalise, 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-personalisation requirements) during the delivery process to the IC designer.
NOTE	*application data means TSF data*
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-personalisation requirements) during the delivery process to the IC designer.
NOTE	application data means TSF data
T.MOD (type a)	Unauthorized modification of ES and/or TSF 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 Personaliser.

These threats are described hereafter:

T.DIS_DEL1	Unauthorized disclosure of Native-Application and ES personnalisation Data during delivery to the IC Packaging manufacturer, the Finishing process manufacturer or the Personaliser
T.DIS_DEL2	Unauthorized disclosure of Native-Application and ES personnalisation Data delivered to the IC Packaging manufacturer, the Finishing process manufacturer or the Personaliser
T.MOD_DEL1	Unauthorized modification of Native-Application and ES personnalisation Data during delivery to the IC Packaging manufacturer, the Finishing process manufacturer or the Personaliser.
T.MOD_DEL2	Unauthorized modification of Native-Application and ES personnalization Data delivered to the IC Packaging manufacturer, the Finishing process manufacturer or the Personaliser.

3.3.4 Threats on phases 4 to 7

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

- Unauthorized disclosure of assets,
- Theft or unauthorized use of assets,
- Unauthorized modification of assets.
- Threats on Native-Applications and on Loaded-Applications

Unauthorized disclosure of assets

This type of threat 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, Native-Application, and Loaded-Application TSF Data (such as data protection system, 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 personalise the product in an unauthorized manner, or try to gain fraudulently access to the Smart Card system

T.T_ES	Unauthorized use of TOE. (e.g. bond 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_TSF	Unauthorized modification or destruction of TOE Security Function Data. (By any mean including probing, electronic perturbation etc.)
T.MOD_LOAD	Unauthorized loading of Native Applications. This includes also illegal modification of eventual Native Applications. As the TOE described in a Security Target claiming this PP must include eventual Native Applications, their loading or modification must be blocked during the usage phase. The threat includes bypassing this blocking.
T.MOD_EXE	Unauthorized execution of Platform or application software.
T.MOD_SHARE	Unauthorized modification of Platform or application behavior by interaction of different programs.
T.MOD_SOFT*	Unauthorized modification of Smart Card Embedded Software and data.

3.3.5 Threats on phases 6 to 7

Threats on assets linked to Loaded-Applications

These threats are specific to the Multi-Application Platform, and thus do not appear in PP/9911. They are centered on threats to loading/unloading of Loaded-Applications and to threats using a Loaded-Application to attack another.

T.LOAD_MAN	Loading an application on the platform bypassing the Administrator. This threat could lead to undue usage of card resources, and for unverified application to attack on other Loaded-Application or Native-Application TSF or User data.
T.LOAD_APP	Loading an application that purports to be another Loaded-Application. This attacks card resources and end user data.

T.LOAD_OTHER	Loading the software representation of a Loaded-Application intended for a specific platform domain onto other platform domains, thus taking from the Loaded-Application representation the security feature of being confined to a specific domain. This is an attack on Loaded-Application User Data.
T.LOAD_MOD	Intercepting application load units and altering code or data without the permission of the Loaded-Application Provider. This attacks application provider user data.
T.APP_DISC	Intercepting application load units and gaining access to confidential code or data This is an attack on application provider user data's confidentiality and know how.
T.APP_CORR	Loading an application that partially or completely overwrites other Loaded-Applications, either corrupting or gaining access to code or data. This is an attack on Application Provider user data.
T.APP_REMOVE	Removing a Loaded -Application without the involvement of the Administrator. This is an attack on Application Provider user data.
T.ERR_REMOVE	Removing a Loaded-Application leaving confidential data and/or code in memory which can be examined This is an attack on Application Provider user data.
T.DEL_REMOVE	Removing a Loaded-Application at the same time deleting part or all of another Loaded-Application. This is an attack on Application Provider user data.
T.APP_READ	Using a loaded application to read confidential data or code belonging to another Loaded-Application. This attacks the confidentiality of User Data.
T.APP_MOD	Using a Loaded-Application to modify data or code belonging to another Loaded-Application without it's authorization. This is an attack on Application Provider user data (and also end user data).
T.RESOURCES	Total or partial destruction of card resources delivered by the platform.

NOTE: T.APP_DISC is also present during phase A1

3.3.6 Threats on phase 7

Unauthorized disclosure of assets

T.DIS_DATA	Unauthorized disclosure of User (application provider and end user) data and TSF data.

Unauthorized modification of assets

T.MOD_DATA	Unauthorized modification or destruction of User ((application provider and end user) Data and TSF 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	Phase 1	Phase A1	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		Class II	Class II	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		Class II	Class II	Class II	
T.MOD_DEL2			Class II	Class II	Class II	
T.MOD	Class II					
T.MOD_TSF			Class I	Class I	Class I	Class I
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 I	Class I	Class I	Class I
T.MOD_SHARE			Class I	Class I	Class I	Class I
T.DIS_DATA						Class I
T.MOD_DATA						Class I
T.LOAD_MAN					Class I	Class I
T.LOAD_APP					Class I	Class I
T.LOAD_OTHER					Class I	Class I
T.LOAD_MOD					Class I/II	Class I/II
T.APP_DISC		Class II			Class I/II	Class I/II
T.APP_CORR					Class I	Class I
T.APP_REMOVE					Class I	Class I
T.ERR_REMOVE					Class I	Class I
T.DEL_REMOVE					Class I	Class I
T.APP_READ					Class I	Class I
T.APP_MOD					Class I	Class I
T.RESOURCES					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

No organizational security policy has been defined in the scope of this PP since such specifications depend essentially on the Loaded-Applications in which the TOE is incorporated.

Nevertheless Organizational Security Policies OSPs may have to be defined, that will depend on the type of smart card IC with multi-application platform to be evaluated, and especially on the security services that it will provide to applications. Indeed, these services can only be evaluated through the platform evaluation, as loaded (or native) applications will rely upon them. The defined OSPs would then possibly introduce new security objectives and new security requirements for the TOE.

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 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.
O.SIDE	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.
NOTE	*sensitive information* means *User Data and TSF data*
O.MOD_MEMORY*	The TOE shall ensure that *sensitive information* stored in memories is protected against any corruption or unauthorized modification.
NOTE	*sensitive information* means *User Data and TSF data*

The following security objectives are necessary to meet the new threats specific to Multi-Application Platforms. This is why these objectives are new and not present in PP/9911.

O.ROLLBACK	The TOE must be in a well-defined valid state before a loading of an application, even in case of failure of the previous loading or removal.. A failure must not hinder the resources that the TOE can deliver. A rollback operation can be achieved either through specific commands or automatically.
O.RESOURCE	The TOE must provide the means of controlling the use of resources by its users and subjects so as to prevent permanent unauthorized denial of service. (for example it must prevent a Loaded-Application from taking control of the whole permanent memory (EEPROM) thus prohibiting other Loaded-Applications from using it)
O.LOAD	Loaded-Applications are only to be loaded on to a platform with the permission of the administrator
O.SECURITY	The application load process must be able to guarantee, when required, the integrity, confidentiality, and to verify the claimed origin of the Loaded-Application code and data;
O.EFFECT_L	Loading an application must have no effect on the code and data of existing Loaded-Applications;
O.REMOVE	Removal of a Loaded-Application and consequent reuse of the Loaded-Application space are only to be performed with the authorization of the administrator. The space must not hold any information relative to data or code linked to the removed Loaded-Application;
O.EFFECT_R	Removal of a Loaded-Application must have no effect on the code and data of the remaining independent Loaded-Applications;
O.SEGREGATE	Loaded-Applications are to be segregated from other Loaded-Applications. A Loaded-Application may not read from or write to another Loaded-Application's code or data without its authorization.

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 Embedded Software must be delivered from the Smart Card software developer (Phase I) 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* : *In this PP it will be always considered applicable.*
NOTE:	
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 Native-Application and ES 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 Personaliser through a trusted delivery and verification procedure that shall be able to maintain the integrity and confidentiality of the Native-Application Data.
(Note: some application data are not required for embedding and are then delivered directly to phases 4 to 6.

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.

4.2.6 Objectives on Loaded-Application development and loading (phase A1 and A2)

This Objective is specific to Loaded-Application development in the Smart Card IC with Multi-Application Platform environment.

O.APPLI_DEV	The Loaded-Application provider must: • follow the Administrator Guidance and • provide trusted delivery channel so that the integrity and origin of the Loaded-Application can be verified and that its confidentiality can be maintained.

5 TOE Security functional requirements

This chapter defines the functional requirements for the TOE using only functional requirement 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.

Functional requirements which are necessary to fulfill the security objectives of this PP are given below.

5.1 Security audit automatic response (FAU_ARP)

5.1.1 FAU_ARP.1 Security Alarms

FAU_ARP.1.1 The TSF shall take [assignment: *list of the least disruptive actions*] upon detection of a potential security violation.

5.2 Security audit analysis (FAU_SAA)

5.2.1 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 event*s] known to indicate a potential security violation;
b) [assignment: *any other rule*s].

5.3 Cryptographic key management (FCS_CKM)

5.3.1 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*].

5.3.2 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*].

5.4 Cryptographic operations (FCS_COP)

5.4.1 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 sizes [assignment *: cryptographic key sizes*] that meet the following [assignment *: list of standards*].

5.5 Access Control Policy (FDP_ACC)

5.5.1 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.

5.6 Access Control Functions (FDP_ACF)

5.6.1 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*].

5.7 Data Authentication (FDP_DAU)

5.7.1 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.

5.8 Export to outside TSF control (FDP_ETC)

5.8.1 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.

5.9 Import from Outside TSF Control (FDP_ITC)

5.9.1 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*].

5.10 Residual Information protection(FDP_RIP)

5.10.1 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]* the following objects :[assignment : *list of objects*].

5.11 Rollback (FDP_ROL)

5.11.1 FDP_ROL.1 Basic rollback

FDP_ROL.1.1 The TSF shall enforce [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to permit the rollback of the [assignment: *list of operations*] on the [assignment: *list of objects*].

FDP_ROL.1.2 The TSF shall permit operations to be rolled back within the [assignment: *boundary limit to which rollback may be performed*]

5.12 Stored data integrity (FDP_SDI)

5.12.1 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*].

5.13 Authentication failures (FIA_AFL)

5.13.1 FIA_AFL.1 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*].

5.14 User attribute definition (FIA_ATD)

5.14.1 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*].

5.15 User Authentication (FIA_UAU)

5.15.1 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.

5.15.2 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)*].

5.16 User identification (FIA_UID)

5.16.1 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated action*s] 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 succesfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.17 User-subject Binding (FIA_USB)

5.17.1 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

.

5.18 Management of function in the TSF (FMT_MOF)

5.18.1 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*]

5.19 Management of security attributes (FMT_MSA)

5.19.1 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*].

5.19.2 FMT_MSA.2 Secure security attributes

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

5.19.3 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.

5.20 Management of TSF data (FMT_MTD)

5.20.1 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*].

5.20.2 FMT_MTD.2 Management of limits on TSF data

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [assignment: *list of TSF data*] to [assignment : *the authorized identified roles*].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed , the indicated limits: [assignment : *actions to be taken*].

5.21 Security management roles (FMT_SMR)

5.21.1 FMT_SMR.1 Security roles

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

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

5.22 Class FMT : Actions to be taken for management :

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

Table 5.1 : Management activity versus functional requirements
legend :
the letter refers to the respective management defined in part 2 of CC V2.1
NM :No Management activity
NA : Not Applicable

5.23 Unobservability (FPR_UNO)

5.23.1 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*].

The functional requirement must be understood in the sense of protection against observation of the mechanisms and TSF data used and of User data manipulated during the operation. The intent is to protect against side channel attacks.

5.24 Fail secure (FPT_FLS)

5.24.1 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*].

5.25 TSF Physical protection (FPT_PHP)

5.25.1 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.

5.26 Trusted recovery (FPT_RCV)

5.26.1 FPT_RCV.4 Function recovery

FPT_RCV.4.1 The TSF shall ensure that [assignment : *list of SFs and failure scenarios*] have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

5.27 Reference mediation (FPT_RVM)

5.27.1 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.28 Domain separation (FPT_SEP)

5.28.1 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.

5.29 Inter-TSF TSF data consistency (FPT_TDC)

5.29.1 FPT_TDC.1 Inter-TSF basic 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.

5.30 TSF self test (FPT_TST)

5.30.1 FPT_TST.1 TSF Testing

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 the authorized user, at the conditions* [assignment : *conditions under which self test should occur*]] to demonstrate the correct operation of the TSF.

5.31 Resource allocation (FRU_RSA)

5.31.1 FRU_RSA.1 Maximum quotas

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [assignment : *controlled resources*] that [selection: *individual user, defined group of users, subjects*] can use [selection: *simultaneously, over a specified period of time*].

6 TOE Security Assurance Requirements

The Assurance requirement 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

7 PP Application Note

This PP application note does not add information but regroups 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") PP/9806. (The Smart card IC with Embedded Software PP also referred as Smart card PP PP/9911 is included in this PP). 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. As a matter of fact, the TOE is the Smart Card IC with Multi-Application Platform able to support one or several Loaded-Applications software possibly loaded during phases 6 or 7.

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

The Smart card Integrated Circuit with Embedded Software PP is an addendum dedicated to software development during phase 1. When the TOE is mentioned, it comprises the Smart Card IC with its Embedded Software.

This PP comprises an addendum, comparable to Smart Card Integrated Circuit with Embedded Software PP, which adds to the Smart card Integrated Circuit the content of PP/9911 and the coverage of the Multi-Application Platform characteristics: loading and removal of Loaded-Application and isolation of private features of Loaded-Applications.

When Assets, Assurance Requirements, Security Objectives are common to the PP/9806, they are mentioned in this PP with an asterisk "*". In this case, the definition of the Smart Card IC PP holds.

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

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 consistent 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 specific security objectives address all security environment aspects identified. Each specific 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 being developed and the pre-personalisation and personalisation requirements are specified for all other phases.

The Target of Evaluation (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 Smart Card during phase 4 to 7(operational phases). The global security requirements of the TOE mandate to consider, during the development phase, the security threats of the other phases. This is why the PP addresses the functions used in phases 4 to 7 but developed during phase 1.Then, the limit of the TOE corresponds to phase 1 including the TOE delivery to the IC manufacturer.

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, TOE participates to countering the threats.

T.DIS_INFO

This threat addresses disclosure of specification, design and development tools concerning the IC and delivered to the software developer (during phase 1) in order to meet with the overall security objectives of the TOE. This threat is countered by development environment.

T.DIS_DEL

This threat addresses disclosure of specifications, test programs, related documents, ES and data which is delivered from phase 1 to phase 2 for software embedding. As the TOE does not yet exist, the threat can only be countered by development environmental procedures.

T.DIS_DEL1

This threat addresses disclosure of software or Native-Application and ES 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 has been 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

The ES and accompanying documents are created and used during phase 1. As during this phase the product does not yet exist, it cannot contribute to countering the threat which must be countered by development environment.

T.DIS_ES2

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

T.DIS_TEST_ES

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

TT_DEL

The threat addresses the theft of software or ES and Native-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 developmental environmental procedures.

T.T_TOOLS

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

T.T_SAMPLE2

TOE samples are used only during phase 1, so this threat can only exist 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 TSF data which is delivered for software embedding, in phase 1. As the TOE does not exist during this phase, the threat must be countered by development procedures.

T.MOD_DEL1

This threat addresses modification of Native-Application Data during delivery from embedded software developer, phase 1, to the IC packaging manufacturer, phase 4, the finishing process manufacturer, phase 5, and for the Personaliser, phase 6. As the data is not yet loaded on the TOE, the threat can only be countered by environmental procedures.

T.MOD_DEL2

This threat addresses modification of Native-Application Data which is delivered to the IC packaging manufacturer, phase 4, the finishing process manufacturer, phase 5, and for the Personaliser, phase 6. As the data is not yet loaded on the TOE, the threat can only be countered by environmental procedures.

T.MOD

Modification of ES and TSF Data can be done during ES design in phase 1. Since the product does not exist, the threat can only be countered by environment procedures.

T.MOD_SOFT

Once present on the TOE, the software and Application data can be modified in an unauthorized way during any phases from 4 to 7. This threat is countered by the TOE.

T.T_ES

This threat covers the unauthorized use of cards during the different phases of the card life cycle as well as the misappropriation of rights of Smart Cards. This threat covers phases 4 to 7 and is countered by the TOE.

T.T_CMD

This threat includes the diversion of the hardware or the software, or both, in order to execute non authorized operations. This threat covers phases 4 to 7 and is countered by the TOE.

T.MOD_LOAD, T.MOD_EXE, T.MOD_SHARE

The loading of Native Applications, execution and modification of software can endanger the security of the TOE, and especially create interference between applications. This threat covers phases 4 to 7 and is countered by the TOE.

New threats not specific to Multi-Application platforms

T.MOD_TSF

Modification of TOE Security function can only appear when the TOE exists, thus only during phases 4 to 7. This threat is countered by the TOE.

T.DIS_DATA

Threats on end user data can only appear after the data has been created, thus in usage phase 7. This threat is countered by the TOE.

T_MOD_DATA

Threats on end user data can only appear after the data has been created, thus in usage phase 7 This threat is countered by the TOE.

New Threats specific to Multi-Application platforms

These threats are present during phases 6 to 7 depending when the Loaded-Applications are loaded. It can be supposed that Loaded-Applications are mostly used during phase 7.

T.LOAD_MAN

This threat comes from illegal loading of Loaded-Applications which can for example clone legal Loaded-Applications on other cards. Loading can be done in phases 6 and 7. This threat is countered by the TOE.

T.LOAD_APP

This threat is a complement to the precedent one. In this case, an illegal Loaded-Application is loaded in place of a legal one. The attacking party can be the same as above. This threat appears during phases 6 and 7 and is countered by the TOE.

T.LOAD_OTHER

This threat addresses loading a Loaded-Application to a domain to which it should not have access. This means that the other Loaded-Application can be attacked. This threat appears during phases 6 and 7 and is countered by the TOE.

T.LOAD_MOD

This threat alters code or data without the permission of the Loaded-Application Provider. This threat appears during phases 6 and 7 and is countered by the TOE and the environment.

T.APP_DISC

This is an attack on the Loaded-Application provider know how, and possibly on confidential data loaded along with the Loaded-Application. This threat appears during phases 6 and 7 and is countered by the TOE and the environment.

T.APP_CORR

This attack destroys partly or completely the other Loaded-Application, or more subtly can divert the Loaded-Application to create a dangerous state. This threat appears during phases 6 and 7 and is countered by the TOE.

T.APP_REMOVE

This threat addresses illegal removal of a legal Loaded-Application. It attacks reliability of services. This threat appears during phases 6 and 7 and is countered by the TOE.

T.ERR_REMOVE

This opportunistic threat takes advantage of a removal operation to attack the confidentiality of Loaded-Application provider know how, or confidential data. This threat appears during phases 6 and 7 and is countered by the TOE.

T.DEL_REMOVE

This threat is on remaining Loaded-Applications which can be damaged during the removal operation. This threat appears during phases 6 and 7 and is countered by the TOE.

T.APP_READ

This threat loads a Trojan horse to illegally access to confidential data belonging to other Loaded-Applications. This threat appears during phases 6 and 7 and is countered by the TOE.

T.APP_MOD

This threat loads a Trojan horse to illegally access to modify data or code belonging to another Loaded-Application. This threat appears during phases 6 and 7 and is countered by the TOE.

T.RESOURCES

This threat is aimed at the reliability of service of the platform or Loaded-Application. This threat appears during phases 6 and 7 and is countered by the TOE.

Threat T.APP_DISC is also present during Loaded-Application development, phase A1 when it is countered by the environment.

8.2.2 Threats addressed by security objectives

8.2.2.1 Security Objectives for the TOE

During phase 1, as 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 specific security objective during the life of the TOE:

Threats/Obj.	TAMPER_ES	SIDE	OPERATE*	FLAW*	DIS_ MECHAN2	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	
T.MOD_EXE	X		X	X		X	X	
T.MOD_SHARE	X		X	X		X	X	
T.MOD_TSF	X		X	X			X	
T.DIS_DATA		X	X	X		X		
T.MOD_DATA	X		X	X			X	

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

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

T.CLON* To realize the threat, it is necessary to have knowledge of the security mechanism, which is prevented by O.DIS_MECHANISM2, and of the TSF data, which is prevented by O.DIS_MEMORY*. The general threat is countered by the dedicated objective O.CLON*.

T.DIS_ES2 Illegal disclosure of ES is countered by O.DIS_MECHANISM2 and disclosure of Application by O.DIS_MEMORY*. More specifically this can be achieved by incorrect operation of the TOE, which is countered by O.OPERATE* and O.FLAW*, or by a direct observation during operation which is countered by O.SIDE

T.T_ES Unauthorized use of TOE can be achieved by a degradation of the security mechanisms which is countered by O.OPERATE* and O.FLAW*, or by modification of the security mechanisms countered by O.TAMPER_ES or by modification of TSF data, countered by O.MOD_MEMORY*.

T.T_CMD	To be able to have an unauthorized use of sequences sent to TOE, it is necessary to achieve a degradation of the security mechanisms which is countered by O.OPERATE* and O.FLAW*, or to modify the security mechanisms countered by O.TAMPER_ES or by modification of TSF data, countered by O.MOD_MEMORY*.
T.MOD_SOFT*	The modification of embedded software of the TOE is countered by a correct operation of security mechanisms O.OPERATE* and O.FLAW*. The threat includes modification of the security mechanisms themselves which is countered by O.TAMPER_ES and modification of TSF data, countered by O.MOD_MEMORY*.
T.MOD_LOAD	To be able to load illegally programs on TOE, it is necessary to achieve a degradation of the security mechanisms which is countered by O.OPERATE* and O.FLAW*, or to modify the security mechanisms countered by O.TAMPER_ES or by modification of TSF data, countered by O.MOD_MEMORY*.
T.MOD_EXE	To be able to illegally execute programs on TOE, it is necessary to bypass or degrade the access security mechanisms. This is countered by O.OPERATE* and O.FLAW*. Modification of the security mechanisms is countered by O.TAMPER_ES. It is also possible to gain access through modification of TSF data, which is countered by O.MOD_MEMORY*, or through disclosure of TSF data which is countered by O.DIS_MEMORY*.
T.MOD_SHARE	To be able to modify programs on TOE, it is necessary to bypass or degrade security mechanisms. This is countered by O.OPERATE* and O.FLAW*. Modification of the security mechanisms is countered by O.TAMPER_ES. Illegal Modification of Application data is countered by O.MOD_MEMORY*. This is also countered by protection of the confidentiality of TSF data: O.DIS_MEMORY*.
T.MOD_TSF	The illegal modification of TSF data of the TOE is countered by O.MOD_MEMORY* which addresses also TSF data. It is also possible to degrade or bypass access mechanisms which is countered by O.TAMPER_ES and O.OPERATE*. Absence of design flaws, O.FLAW*, is necessary to counter the threat.
T.DIS_DATA	The disclosure of application user and TSF data on the TOE is countered by O.DIS_MEMORY*. To fulfill the threat, it can be necessary to degrade or bypass access mechanisms which is countered by O.SIDE and O.OPERATE*. Absence of design flaws, O.FLAW*, is necessary to counter the threat.
T.MOD_DATA	The modification of application user data on the TOE is countered by O.MOD_MEMORY*. To fulfill the threat, it can be necessary to degrade or bypass access mechanisms which is countered by O.TAMPER_ES, O.OPERATE*. Absence of design flaws, O.FLAW*, is necessary to counter the threat.

Threats/Obj.	ROLLBACK	RESOURCE	LOAD	SECURITY	EFFECT_L	REMOVE	EFFECT_R	SEGREGATE
T.LOAD_MAN			X					
T.LOAD_APP			X					
T.LOAD_OTHER					X			
T.LOAD_MOD				X				
T.APP_DISC				X				
T.APP_CORR					X			
T.APP_REMOVE						X		
T.ERR_REMOVE						X		
T.DEL_REMOVE							X	
T.APP_READ								X
T.APP_MOD								X
T.RESOURCES	X	X						

Table 8.1B Mapping of security objectives to threats relative to phase 6 and 7

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

T.LOAD_MAN	O.LOAD imposes that application be loaded only with the permission of the administrator, which counters the threat.
T.LOAD_APP	O.LOAD controls the origin of the Loaded Application before loading, thus if necessary control is made by the administrator, it counters T.LOAD_APP.
T.LOAD_OTHER	Loading an application into an another illegal domain is countered by O.EFFECT_L which prevents applications from having non authorized effects on applications loaded in other domains.
T.LOAD_MOD	Alteration of Loaded Application during loading is prevented by O.SECURITY which guarantees its integrity.
T.APP_DISC	Divulgation of Loaded Application during loading is prevented by O.SECURITY which guarantees its confidentiality.
T.APP_CORR	Loading an application so it corrupts another application is countered by O.EFFECT_L which prevents applications from having non authorized effects on applications loaded in other domains.
T.APP_REMOVE	Removal of application without the consent of the administrator is countered by O.REMOVE which imposes the authorization of the administrator.
T.ERR_REMOVE	Removal of application leaving confidential data is countered by O.REMOVE which imposes that the space left does not hold any information linked to removed application.
T.DEL_REMOVE	Deletion of part of a Loaded Application by removal of another is countered by O.EFFECT_R which ensures that removal has no effect on other Loaded Applications.
T.APP_READ	Use of a Loaded Application to illegally read data contained in another application is countered by O.SEGREGATE which ensure that illegal reading of data of another application is not possible.
T.APP_MOD	Use of a Loaded Application to illegally modify data or code contained

	in another application is countered by O.SEGREGATE which ensure that illegal modification of data or code of another application is not possible.
T.RESOURCES	Destruction or hoarding of card resources is prevented by O.ROLLBACK which guarantees that a failure does not compromise card resources and by O.RESOURCES which controls the use of card resources by Loaded Applications.

8.2.2.2 Security objectives for the environment

The following tables map the security objectives for the environment relative to the various threats in addition to the Smart Card PP.

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

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

T.CLON*	Cloning requires knowledge of : • Development data and access to tools, which is countered by O.DEV_DIS_ES • The software which is countered by O.SOFT_DLV* • Initialization data which is countered by O.INIT_ACS Cloning can also be done by using samples; this is countered by O.SAMPLE_ACS.
T.DIS_INFO*	Disclosure of IC assets is countered by O.DEV_DIS_ES which guarantees the storage of classified information
T.DIS_DEL*	Disclosure of embedded software and corresponding data during delivery is countered by O.SOFT_DLV*.
T.DIS_ES1	Disclosure of ES is countered by O.DEV_DIS_ES which guarantees the storage of classified information and by O.INIT_ACS which guarantees a controlled access to initialization data.
T.DIS_TEST_ES	Disclosure of ES test program is countered by O.DEV_DIS_ES which guarantees the storage of classified information
T.T_DEL*	Theft of software delivered to IC manufacturer is countered by O.SOFT_DLV* which ensures trusted delivery.

T.T_TOOLS	Theft or unauthorized access to development tools is countered by O.DEV_TOOLS* which controls the accesses.
T.T_SAMPLE2	Theft of samples is countered by O.SAMPLE_ACS controlled access.
T.MOD_DEL*	Modification of software and related information is countered by O.SOFT_DLV*.
T.MOD	Unauthorized modifications of software is countered by access control specified by O.DEV_DIS_ES and that of TSF data by O.INIT_ACS

Threats	DLV_DATA	TEST_OPERATE*
T.DIS_DEL1	X	
T.DIS_DEL2		X
T.MOD_DEL1	X	
T.MOD_DEL2		X

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

T.DIS_DEL1 Unauthorized disclosure of Native-Application and ES data during delivery is countered by O.DLV_DATA which specifies a trusted delivery maintaining the confidentiality.

T.DIS_DEL2 Unauthorized disclosure of Native-Application and ES data after delivery is countered by O.TEST_OPERATE* which specifies maintenance of the confidentiality.

T.MOD_DEL1 Unauthorized modification of Native-Application and ES data during delivery is countered by O.DLV_DATA which specifies a trusted delivery maintaining the integrity.

T.MOD_DEL2 Unauthorized modification of Native-Application and ES data after delivery is countered by O.TEST_OPERATE* which specifies maintenance of the integrity and it's test..

Threats	O.APPLI_DEV
T.LOAD_MOD	X
T.APP_DISC	X

Table 8.4 Mapping of security objectives for the environment to threat on phases A1 and A2 (development and delivery for phase A1 to phases 6 and 7

T.LOAD_MOD Modification of Code and data of a Loaded-Application during its transfer and loading is countered by O.APPLI_DEV which ensures the mechanisms to verify their integrity

T.APP_DISC Gaining access to confidential code and data of a Loaded-Application during its transfer and loading is countered by O.APPLI_DEV which ensures the confidentiality.

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 8.5 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 assumption.

Phases		Delivery process for phases 4 to 7			Phases 4 to 6	Phase 7	Phase A1
	Assumptions\Objectives	DLV_ PROTECT*	DLV_ AUDIT*	DLV_ RESP*	TEST_ OPERATE*	USE_ DIAG*	APPLI_DEV
4 to 7	DLV_PROTECT*	X					
4 to 7	DLV_ AUDIT		X				
4 to 7	DLV_ RESP*			X			
4 to 7	USE_TEST*				X		
4 to 7	USE_PROD*				X		
7	USE_DIAG*					X	
A1	APPLI_CONT						X

Table 8.5 demonstrates 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) is suitable to meet the security objectives.

8.3.1 Security functional requirements rationale

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

The table 8.6 demonstrates which security functional requirement contributes to the satisfaction of each TOE security objective. For clarity, the table does not identify indirect dependencies.

Security Functional Requirements	O.TAMPER_ES	O.SIDE	O.OPERATE*	O.DIS_ MECHAN.2	O.DIS MEMORY	O.MOD_ MEMORY	O.FLAW*	O.CLON*
EAL4 Requirements							X	
FAU_ARP.1	X		P	P	X	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	X		P
FDP_ACC.2	X		P	X	X	X		P
FDP_ACF.1	X		P	X	X	X		P
FDP_DAU.1	X		P		X	X		P
FDP_ETC.1					X			
FDP_ITC.1					X	X		
FDP_RIP.1	X				P			
FDP_SDI.2			P			X		
FIA_AFL.1	X		P					P
FIA_ATD.1	X		P					
FIA_UAU.1	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
FPT_FLS.1	X							
FPT_PHP.3	X		X	X	X	X		X
FPT_SEP.1	X			X	X	X		
FPT_TDC.1	X					X		
FPT_TST.1			X		X	X		

Security Requirements	ROLLBACK	RESOURCE	LOAD	SECURITY	EFFECT_L	REMOVE	EFFECT_R	SEGREGATE
FAU_ARP.1.		X						
FAU_SAA.1		X						
FCS_CKM.3				X		X		
FCS_CKM.4				X		X		
FCS_COP.1			X	X		X		
FDP_ACC.2			X			X		X
FDP_ACF.1					X		X	X
FDP_ITC.1			X	X				
FDP_RIP.1						X		
FDP_ROL.1	X							
FIA_UID.1			X			X		
FIA_UAU.1			X			X		
FMT_MSA.1			X			X		
FMT_MSA.2			X			X		
FMT_MSA.3			X			X		
FMT_MTD.1								X
FMT_MTD.2		X	X					
FMT_SMR.1			X			X		
FPT_FLS.1	X				X		X	X
FPT_RCV.4	X				X		X	
FPT_RVM.1			X			X		X
FPT_SEP.1					X		X	X
FRU_RSA.1		X						

Table 8.6 Mapping of security functional requirements and objectives
legend : P :Partial ; X :relevant

This section describes how the security objectives for the TOE are met by the security requirements.

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

O.TAMPER_ES This objective is met through:

- Protection of critical parts from tampering through TSF Security Functional Requirements: SFR: FPT_FLS.1 Failure with preservation of secure state, FPT_PHP.3 Resistance to physical attack, FPT_SEP.1 TSF Domain separation and FPT_TDC.1 Inter-TSF basic TSF data consistency.
- Prevention of unauthorized changes through
  - Identification and authentication SFR (of authorized user): FIA_AFL.1 Authentication failure handling, FIA_ATD.1 User attribute definition, FIA_UAU.1 Timing of authentication, FIA_UAU.4 Single-use Authentication Mechanisms, FIA_UID.1 Timing of identification and FIA_USB.1 User-subject binding.
  - Security management SFR (of authorized roles and rights): FMT_MOF.1

Management of security functions behavior, FMT_MSA.1 Management of security attributes, FMT_MSA.3 Static attribute initialization and FMT_SMR.1 Security roles

- Protection of parameters and keys through:
  - Cryptographic support SFR: FCS_CKM.3 Cryptographic key access, FCS_CKM.4 Cryptographic key destruction and FCS_COP.1 Cryptographic operation
  - User data protection SFR: FDP_ACC.2 Complete Access control, FDP_AC Security attribute based access control, FDP_DAU.1 Basic Data Authenticat and FDP_RIP.1 Subset residual information protection.
  - FAU_SAA.1 Potential violation analysis and FAU_ARP.1 Security alarm support the security functions by allowing analysis of possible attacks.

O.SIDE

Interpretation of side channel information leakage is countered by the SFR:

- FPR_UNO.1 Unobservability ensures that observation of signals cannot reveal information which could allow illegal access and operations.

O.OPERATE*

Correct operation of security functions is assured by the following:

- Security management SFR: FMT_MOF.1 Management of security functions behavior and FMT_SMR.1 Security roles
- Protection of TSF SFR: FPT_PHP.3 Resistance to physical attack and FPT_TE TSF Testing.

On a second level, other SFR are active : FAU_ARP.1, FAU_SAA.1, FCS_CKM.3, FCS_CKM.4 , FDP_ACC.2, FDP_ACF.1, FDP_DAU.1, FDP_SDI.2, FIA_AFL.1, FIA_ATD.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FPR_UNO.1 .

O.DIS_MECHAN2

Protection of security mechanisms against unauthorized disclosure is assured by the following:

- Protection of TSF SFR : FPT_PHP.3 Resistance to physical attack and FPT_SE TSF Domain separation.
- Security management SFR (for authorization to access the functions and their TSF data): FMT_MOF.1 Management of security functions behavior, FMT_MSA.1 Management of security attributes, FMT_MSA.2 Secure security attributes, FMT_MSA.3 Static attribute initialization.
- User data protection SFR (for access control): FDP_ACC.2 Complete Access control and FDP_ACF.1 Security attribute based access control FAU_SAA.1 Potential violation analysis and FAU_ARP.1 Security alarm allow tracking of possible attacks.

O.DIS_MEMORY* Protection of data against unauthorized disclosure is assured by the following:

- User data protection SFR: FDP_ACC.2 Complete Access control, FDP_ACF.1 Security attribute based access control, FDP_DAU.1 Basic Data Authentication , FDP_ETC.1 Export of User Data without Security Attributes, FDP_ITC.1 Import from outside TSF Control, and partially FDP_RIP.1.
- Authentication and identification SFR: FIA_UAU.1 Timing of authentication, FIA_UAU.4 Single-use Authentication Mechanisms, FIA_UID.1 Timing of identification and FIA_USB.1 User-subject binding.
- Cryptographic support SFR can be used for authentication: FCS_COP.1 Cryptographic operation, and this can require FCS_CKM.3 and FCS_CKM.4
- Security management SFR assure the access control: FMT_MTD.1 Management of TSF data, and partially FMT_MOF.1, FMT_MSA.1, FMT_MSA.2and FMT_MSA.3 as support.
- FPR_UNO.1 Unobservability is necessary so that data is not revealed during operations.
- Protection of the above TSF is assured by: FPT_PHP.3 Resistance to physical attack, FPT_SEP.1 TSF Domain separation and FPT_TST.1 TSF Testing
- FAU_ARP.1 Security Alarms and FAU_SAA.1 Potential violation analysis are necessary to monitor possible problems.

O.MOD_MEMORY* Protection of data against unauthorized modification is assured by the following:

- User data protection SFR: FDP_DAU.1 Basic Data Authentication , FDP_ITC.1 Import from Outside TSF Control, FDP_SDI.2 Stored data integrity monitoring and action and partially by FDP_ACC.2 and FDP_ACF.1.
- Authentication and identification SFR: FIA_UAU.1 Timing of authentication, FIA_UAU.4 Single-use Authentication Mechanisms, FIA_UID.1 Timing of identification and FIA_USB.1 User-subject binding, and partially by FIA_AFL.1 and FIA_ATD.1..
- Cryptographic support SFR can be used for authentication: FCS_COP.1 Cryptographic operation, and this can require FCS_CKM.3 and FCS_CKM.4
- Security management SFR which assure the access control: FMT_MTD.1 Management of TSF data, and partially FMT_MOF.1, FMT_MSA.1, FMT_MSA.2and FMT_MSA.3 as support.
- Protection of the above TSF is assured by: FPT_PHP.3 Resistance to physical attack, FPT_TDC.1 Inter-TSF basic TSF data consistency and FPT_TST.1 TSF Testing
- FAU_ARP.1 Security Alarms and FAU_SAA.1 Potential violation analysis are necessary to monitor possible problems.

O.FLAW*	The objective is met by good design and testing as specified by EAL4 augmented conformity requirements.
O.CLON*	The protection against cloning objective is assured by the following: • Good key housekeeping FCS_CKM.4 Cryptographic key destruction • Unobservability of TSF data which are necessary for cloning by FPR_UNO.1 Unobservability • And resistance to attacks FPT_PHP.3 Resistance to physical attack Other SFR participate also to cloning prevention: • Cryptographic support SFR: FCS_CKM.3, FCS_COP.1 • Data protection SFR: FDP_ACC.2, FDP_ACF.1, FDP_DAU.1 • Identification and authentication SFR: FIA_AFL.1, FIA_UAU.1, FIA_UID.1, FIA_UAU.4, FIA_USB.1 • Security management SFR: FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1
O.ROLLBACK	This objective is assured by the following: • FDP_ROL.1 Basic rollback Backed by: FPT_FLS.1 Failure with preservation of secure state and FPT_RCV.4 Function recovery.
O.RESOURCE	Resource preservation objective is assured by the following: • FMT_MTD.2 Management of limits on TSF data • FRU_RSA.1 Maximum quotas Backed by FAU_ARP.1 Security Alarms and FAU_SAA.1 Potential violation analys
O.LOAD	The control of the administrator is assured by the following: • FIA_UAU.1 Timing of authentication and FIA_UID.1 Timing of identification, to have control on the operation • FPT_RVM.1 Non-bypassability of the TSP • Security management SFR: FMT_MSA.1 Management of security attributes, FMT_MSA.2 Secure security attributes, FMT_MSA.3 Static attribute initialization, FMT_MTD.2 Management of limits on TSF data and FMT_SMR.1 Security roles. • User data protection SFR: FDP_ACC.2 Complete access control and FDP_ITC.1 Import of User Data without Security Attributes • FCS_COP.1 Cryptographic operation
O.SECURITY	Loading of applications requirements are assured by the following: • FDP_ITC.1 Import of User Data without Security Attributes Backed by the cryptographic SFR: FCS_COP.1 Cryptographic operation FCS_CKM.3 Cryptographic key access and FCS_CKM.4 Cryptographic key destruction

O.EFFECT_L

Separation of the Loaded-Applications is assured by the following:

- FPT_SEP.1 TSF Domain separation
- FDP_ACF.1 Security attribute based access control

And the following SFR which assure correct operation.

- FPT_FLS.1 Failure with preservation of secure state
- FPT_RCV.4 Function recovery.

O.REMOVE

Safety of the removal process is assured by the following:

Guarantee that only administrator can access is required by

- FIA_UAU.1 Timing of authentication and FIA_UID.1 Timing of identification, to have control on the operation
- FDP_ACC.2 Complete Access control
- Security management SFR so administrator is the sole authorized actor: FMT_MSA.1 Management of security attributes, FMT_MSA.2 Secure security attributes and FMT_MSA.3 Static attribute initialization.
- FMT_SMR.1 Security roles
- FPT_RVM.1 Non-bypassability of the TSP

Supported by cryptographic SFR : FCS_CKM.3 Cryptographic key access, FCS_CKM.4 Cryptographic key destruction and FCS_COP.1 Cryptographic operation.

Guarantee that no information is left is required by

- FDP_RIP.1 Subset residual information protection

O.EFFECT_R

Separation of the unloaded application from the other Loaded-Applications is assured the following:

- FPT_SEP.1 TSF Domain separation
- FDP_ACF.1 Security attribute based access control

And the following SFR which assure correct operation.

- FPT_FLS.1 Failure with preservation of secure state
- FPT_RCV.4 Function recovery.

O.SEGREGATE

Segregation of Loaded-Applications is assured by the following:

- User data protection SFR for access control between subjects: FDP_ACC.2 Complete Access control, and FDP_ACF.1 Security attribute based access control
- Security management SFR: FMT_MTD.1 Management of TSF data.
- FPT_SEP.1 TSF Domain separation

The TSF fulfilling the SFR are protected by

- FPT_FLS.1 Failure with preservation of secure state
- FPT_RVM.1 Non-bypassability of the TSP

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 (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 8.5 list 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**	*
2	FCS_CKM.3 : Cryptographic Key Access	FDP_ITC.1, FCS_CKM.4, FMT_MSA.2	9, 3, 20
3	FCS_CKM.4 : Cryptographic Key Destruction	FDP_ITC.1 , FMT_MSA.2	9, 20
4	FCS_COP.1 : Cryptographic Operation	FDP_ITC.1, FCS_CKM.4, FMT_MSA.2	9, 3, 20
5	FDP_ACC.2 : Complete Access Control	FDP_ACF.1	6
6	FDP_ACF.1 : security attributes based Access Control	FDP_ACC.1, FMT_MSA.3	H(5), 21
7	FDP_DAU.1 : basic Data Authentication	none	
8	FDP_ETC.1 : Export of user data without security attributes	FDP_ACC.1	H(5)
9	FDP_ITC.1 : Import of user data without security attributes	FDP_ACC.1,FMT_MSA.3	H(5), 21
10	FDP_RIP.1 : subset residual information protection	none	
11	FDP_SDI.2 : stored data integrity monitoring and action	none	
12	FIA_AFL.1 : 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	16
15	FIA_UAU.4 : Single-use authentication mechanisms	none	
16	FIA_UID.1 : timing of identification	none	
17	FIA_USB.1 : user-subject binding	FIA_ATD.1	13
18	FMT_MOF.1 : management of security functions behaviour	FMT_SMR.1	23
19	FMT_MSA.1 : management of security attributes	FDP_ACC.1, FMT_SMR.1	H(5), 23
20	FMT_MSA.2 : Secure security attributes	ADV_SPM.1, FSP_ACC.1 FMT_MSA.1, FMT_SMR.1	by EAL4 H(5), 19, 23
21	FMT_MSA.3 : Secure attributes initialization	FMT_MSA.1, FMT_SMR.1	19, 23
22	FMT_MTD.1 : management of TSF data	FMT_SMR.1	23
23	FMT_SMR.1 : security roles	FIA_UID.1	16
24	FPR_UNO.1 : Unobservability	none	
25	FPT_FLS.1 : failure with preservation of secure state	ADV_SPM.1	by EAL4
26	FPT_PHP.3 : Resistance to physical attack	none	
27	FPT_SEP.1 : TSF Domain separation	none	
28	FPT_TDC.1 : inter-TSF basic TSF data consistency	none	
29	FPT_TST.1 : TSF testing	**FPT_AMT.1**	*

* : dependencies are not met for reasons given below

Number	Security functions	Dependencies	Line N°
30	FAU_ARP.1 : Security Alarms	FAU_SAA.1	1
31	FDP_ROL.1 : Basic Rollback	FDP_ACC.1	H(5)
32	FMT_MTD.2: Management of limits on TSF data	FMT_MTD.1, FMT_SMR.1	22, 23
33	FPT_RCV.4 : Function recovery	ADV_SPM.1	By EAL4
34	FPT_RVM.1 : Non-bypassability of the TSP	None	
35	FRU_RSA.1 : Maximum quotas	None	

Table 8.7 *Functional dependencies in Multi-Application environment*

H(5) means that the dependency is satisfied by a higher hierarchical component
Table 8.7 shows that the functional component dependencies are satisfied by all functional components 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 outside world, typically the card reader, the TOE is always the slave. These reasons are why FPT_TST.1 is self consistent and FPT_AMT.1 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	Sufficiency of security measures	Higher hierarchical component
AVA_VLA.4	Highly resistant	Higher hierarchical component

Evaluation Assurance level rationale

An assurance requirement of EAL4 is required because the platform is designed to support Loaded-Applications 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 a high practical level of assurance expected for a future 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.

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.

1 Annex A Glossary

This glossary is a complement of CC Part 1 section 2.3 and Part 3 section 2.4

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.

Context manager
System software in charge of the functional supervision of Loaded-Applications. The Operating System requires services to the Context manager in order to control card and Loaded-Application life cycles.

Disclosure
The Act of revealing confidential information . The information is still In the possession of it's authorized owner.

Embedded Software (ES)
Is defined as the software sent by the software developer during phase1 and sent to the IC manufacturer for embedding during phase 3. 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-personalisation requirements.

Image (of an application)
The representation of an application in the TOE permanent memory.

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-personalisation.

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

Multi-Application Platform
Software platform running on a Smart Card IC and which can provide controlled communication between Loaded Applications.

Loaded Application
Software application which are loaded (during phases 6 or 7) on the Multi-Application Platform using the card loader. These applications communicate through the Multi-Application Platform.
By extension, an application which is integrated (during phase 6 in a controlled environment) is called Loaded Application if it can be proven that its image is identical to the image it would have if it had been loaded through the loader.

Native-Application
Application which are embedded (during phase 3) or integrated (during phase 6) on the Smart Card IC. They are not loaded on the Multi-Application Platform and do not communicate through it.

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

Personalisation data
Specific information in the NVM during personalisation 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)

Sensitive Information
Information such as User Data, TSF Data, development and manufacturing information for which security procedures are required. (typically to guarantee integrity and confidentiality).

Smart Card or Integrated Circuit Card
Medium according to ISO 7810, ISO 7811, ISO 7812 (ID-1) or GSM 11.11 into which has been introduced an Integrated Circuit.

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.

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

Theft
Stealing information or material from it's authorized owner. The authorized owner has no longer access to the information or material.

User data
Data introduced by the user. This can be the Loaded Application itself, the user being the application provider, or data belonging to the card holder (end user).

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

TSFI
TSF Interface

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

2 Annex B Mapping with PP/9806

Security Objective for Environment (mapping from Threats and Assumptions)

		PP/9806																	PP/0010				
	Objectives / Threats	DESIGN_ACS	DEV_DIS	DEV_TOOLS*	DLV_AUDIT*	DLV_PROTECT*	DLV_RESP*	DSOFT_ACS	IC_DLV	MASK_FAB	MECH_ACS	SOFT_ACS	SOFT_DLV*	SOFT_MECH	TEST_OPERATE*	TI_ACS	TOE_PRT	USE_DIAG*	USE_SYS	DEV_DIS_ES	DLV_DATA	INIT_ACS	SAMPLE_ACS	APPLI_DEV
PP/9806	T.CLON*	2	1	1				2	3	2	2	2	1	1		2	3			1		1	1	
	T.DIS_DEL*												1											
	T.DIS_DESIGN	2									2					2	3							
	T.DIS_DSOFT							2									3							
	T.DIS_INFO*		1																	1				
	T.DIS_PHOTOMASK									2							3							
	T.DIS_SOFT											2					3							
	T.DIS_TEST																3							
	T.DIS_TOOLS	2															3							
	T.MOD_DEL*												1											
	T.MOD_DESIGN	2									2					2	3							
	T.MOD_DSOFT							2									3							
	T.MOD_PHOTOMASK									2							3							
	T.MOD_SOFT											2					3							
	T.T_DEL*												1											
	T.T_PHOTOMASK									2							3							
	T.T_PRODUCT								3								3							
	T.T_SAMPLE	2							3								3							
PP/0010	T.DIS_DEL1														1,4-6						1,4-6			
	T.DIS_DEL2														4-6									
	T.DIS_ES1																			1		1		
	T.DIS_TEST_ES																			1				
	T.MOD																			1		1		
	T.MOD_DEL1																				1,4-6			
	T.MOD_DEL2														4-6									
	T.T_SAMPLE2																						1	
	T.T_TOOLS			1																				
	T.LOAD_MOD																							6-7
	T.APP_DISC																							X
	ASSUMPTIONS																							
	A.DLV_ RESP*						4-7																	
	A.DLV_PROTECT*					4-7																		
	A.DLV_AUDIT*				4-7																			
	A.SOFT_ARCHI			1										1										
	A.USE_DIAG*																	7						
	A.USE_PROD*														4-6									
	A.USE_SYS																		7					
	A.USE_TEST*														4-6									
	A.APPLI_CONT																							A1

Figures give the concerned phases

X concerns phases A1, 6 and 7

* Security components common with PP/9806

Security Objective for the TOE
(mapping from Threats)

		PP/9806							Specific to PP/0010										
	Objectives / Threats	CLON*	DIS_MECHANISM	DIS_MEMORY*	FLAW*	MOD_MEMORY*	OPERATE*	TAMPER	DIS_MECHANISM2	TAMPER_ES	SIDE	EFFECT_L	EFFECT_R	LOAD	REMOVE	RESOURCE	ROLLBACK	SECURITY	SEGREGATE
PP/9806	T.CLON*	4-7		3-7					4-7										
	T.DIS_DESIGN		3-7					3-7											
	T.DIS_DSOFT			3-7				3-7											
	T.DIS_SOFT			3-7				3-7											
	T.DIS_TEST			3-6				3-6											
	T.MOD_DESIGN				3-7		3-7	3-7											
	T.MOD_DSOFT				3-7	3-7	3-7	3-7											
	T.MOD_SOFT				3-7	3-7	3-7	3-7		4-7									
	T.T_PRODUCT						3-7												
	T.T_SAMPLE						3-5												
Specific to PP/0010	T.DIS_ES2			4-7	4-7		4-7		4-7		4-7								
	T.MOD_EXE			4-7	4-7	4-7	4-7			4-7									
	T.MOD_LOAD				4-7	4-7	4-7			4-7									
	T.DIS_DATA			7	7		7				7								
	T.MOD_DATA				7	7	7			7									
	T.MOD_SHARE			4-7	4-7	4-7	4-7			4-7									
	T.MOD_TSF				4-7	4-7	4-7			4-7									
	T.T_CMD				4-7	4-7	4-7			4-7									
	T.T_ES				4-7	4-7	4-7			4-7									
	T.APP_CORR											6-7							
	T.APP_DISC																	6-7	
	T.APP_MOD																		6-7
	T.APP_READ																		6-7
	T.APP_REMOVE														6-7				
	T.DEL_REMOVE												6-7						
	T.ERR_REMOVE														6-7				
	T.LOAD_APP													6-7					
	T.LOAD_MAN													6-7					
	T.LOAD_MOD																	6-7	
	T.LOAD_OTHER											6-7							
	T.RESOURCES															6-7	6-7		

Figures give the concerned phases
X concerns phases A1, 6 and 7
* Security components common with PP/9806