XIRING

gemalto
security to be free

Common Criteria for IT Security Evaluation
Protection Profile

Secure Smartcard Reader with Human Interface
Protection Profile

Profil de Protection
Lecteur Sécurisé de Carte avec Interface Homme-Machine

Summary

1) PP INTRODUCTION (APE_INT) 5

PP REFERENCE 5
CONTEXT 5
PP OBJECTIVES 5
GENERAL OVERVIEW OF THE TOE 6
TOE type 8
Security features of the TOE 8
Specific conditions and security specificities of the TOE 8
Hardware and software environment 8
Lifecycle environment 9

2) CONFORMANCE CLAIMS (APE_CCL) 9

CONFORMANCE OF THIS PROTECTION PROFILE 9
Conformance with the Common Criteria 9
Conformance with an assurance package 10
Conformance with a Protection Profile 10
CONFORMANCE OF SECURITY TARGETS AND PROTECTION PROFILES 10

3) SECURITY PROBLEM DEFINITION (APE_SPD) 10

ASSETS 11
Assets in the operational environment 11
THREATS 12
Threat agents 12
Attack potential 13
Threats 13
OSP 13
ASSUMPTIONS 13

4) SECURITY OBJECTIVES (APE_OBJ) 14

SECURITY OBJECTIVES FOR THE TOE 14
SECURITY OBJECTIVES FOR THE ENVIRONMENT 14
RATIONALE 15
Coverage of threats in the operational environment. 15

5) EXTENDED COMPONENTS DEFINITION (APE_ECD) 16

6) SECURITY REQUIREMENTS (APE_REQ) 16

SECURITY FUNCTIONAL REQUIREMENTS 16
SECURITY ASSURANCE REQUIREMENTS 19
RATIONALE 20
Security requirements / Security objectives 21
Conformity with a PP 21
Extended components 21

7) ACRONYMS 22

8) BIBLIOGRAPHY 23

9) GLOSSARY 24

FIGURES

Figure 1 : architecture of the TOE 7

Figure 2 Lifecycle of the TOE 9

Figure 3: The environment of the TOE 11

TABLES

Table 1 : Threats, assumptions and Security objectives **16**
Table2: Dependencies of functional requirements **19**
Table3: Security Assurance requirements **20**
Table4:Security objectives and security functional requirements **21**

1) PP Introduction (APE_INT)

PP reference

Title : Secure Smartcard Reader with Human Interface Protection Profile Version : 1.6
Authors :

XIRING, 25 quai Gallieni, 92158 SURESNES CEDEX.
GEMALTO, 6 rue de la Verrerie, 92197 MEUDON Cedex, FRANCE

Evaluation Assurance Level : EAL3 augmented.
Registration : xxxxxx given by the French certification body at the protection profile registration, as certified.
Conformant to Version 3.1, release 3 of Common Criteria [9].
Key words : Smartcard, smartcard reader, keypad, electronic signature, electronic commerce, pinpad, secure pin entry, display.
A glossary of terms used in the PP is given in Glossary.

A product compliant with this PP may also offer additional security functional requirements.
This Protection Profile elaborated in conformance with the French IT Security Evaluation and Certification Scheme is the work of the following organisations :

XIRING, 25 quai Gallieni, 92158 SURESNES CEDEX, FRANCE

GEMALTO, 6, rue de la Verrerie, 92197 MEUDON CEDEX, FRANCE

SCM Microsystems Gmbh, Oskar-Messter-Str. 13, 85737 Ismaning, GERMANY

Context

This PP has been drawn up under the aegis of the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).
The intent of this Protection Profile is to specify functional and assurance requirements applicable to a generic « secure pin entry device ».
Hereafter in this document the expression « secure pin entry device » will be replaced by « the Device ».
The aim is to provide an administration framework for the certification of secure pin entry devices to meet the requirements of the public and private sectors with a view to their qualification.

PP Objectives

The main objectives of this Protection Profile are:

- to describe the Target of Evaluation (TOE) as a product and position it in its life cycle ;
- to describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by the operational environment during the user phase ;
- to describe the security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of application data and programs;
- to specify the IT security requirements which includes the TOE functional requirements and the TOE IT Assurance requirements.

General overview of the TOE

A smartcard is a piece of plastic, with an electronic component embedded in it. The electronic component is a micro-computer with internal memory, able to perform controls and calculations. One or several software applications, in the micro-computer, can activate those functions to use the smartcard as a token in a card scheme, providing to the card scheme security functions such as authentication, electronic signature generation or control.

Usually the smartcard is « personalized ». It means that before the use stage of the smartcard, it is given a unique identification number, and this unique identification number can be checked without any doubt by the card scheme. The Device is to be used with personalized smartcards, by the legitimate users of those smartcards. The security of the smartcard is out of scope of the TOE. Many applications in the smartcard require a user authentication. The authentication is done by providing the application in the smartcard with a personal data, which is frequently a numeric password, called the “PIN” (personal identification number). Once verified successfully by the smartcard, the PIN allows the user to fully access the application.

The smartcard has no human interface. It has only a physical connector (ISO 7816 type) to link to a smartcard reader, and the smartcard reader has normally a serial type connector, to link to a Personal Computer (PC), or Workstation. The PC may be a Microsoft Windows, Mac or Linux OS powered. The security of the PC is out of scope of the TOE.

As a PIN (personal data) is required for some smartcard applications, this PIN is usually keyed on the PC keyboard and forwarded to the smartcard through PC/SC [3] and ISO 7816 / EMV commands [4, 10]. As the security of the PC cannot be guaranteed, a malware (virus, Trojan, worm, key logger…) could intercept the PIN, record it to replay it or forward it to a remote attacker. Such a malware can also use the security mechanisms of the smartcard to block the smartcard application (denial of service attack type), by providing the smartcard with a modified (and false) personal data (example: PIN).

As the smartcard may be used to sign some critical information, the display of the Device may be used to provide the user with a mean to check this information, even partially, or to approve explicitly the operation before signing it.

The purpose of the Device is to avoid compromising the PIN or modifying the critical information to be signed by such a malware: the PIN is never keyed on the PC keyboard, but on the Device keypad, and forwarded directly to the smartcard and never transmitted to the PC. There is no way for a malware to ask for a PIN to the Device and to receive this PIN.

There is also no way for a malware to ask for a PIN on the PC keyboard and forward it to the smartcard.

The Device is supposed to be used in a private environment. That is to say that the Device is to be used by an individual, or a small group of persons (limited to a well defined group persons), in a place under control of this individual, or group of persons, so it can be used at home, or at the office. The Device is not intended to be used in a public area.

The Device has a « smartcard reader ». It means that it equipped with an integrated smartcard reader and is able to interact with the smartcard [8].

The Device is intended to be linked to a PC (Personal Computer). It means that it is linked to a personal computer through a serial interface
The Device is a pin entry device. It has a keypad (numeric or alphanumeric) and a display. The Device could be considered as a device gathering the capacity to interact with smartcard, to securely capture an authentication information and transaction data in order to pass it to the application software in the smartcard to generate secured transactions (in the general sense, not restricted to bank transaction). Hereafter in this document, the personal data to be passed securely to the smartcard application is called PIN, because in most cases, this authentication information is a numeric code (Personal Identification Number).

The display of the Device may be used by an application in the smartcard to securely interact with the user and display some data to be signed by this application or provided by this application.

The device includes a specific embedded software (called hereafter the "firmware"), whose functionalities will be described by the ST writer.

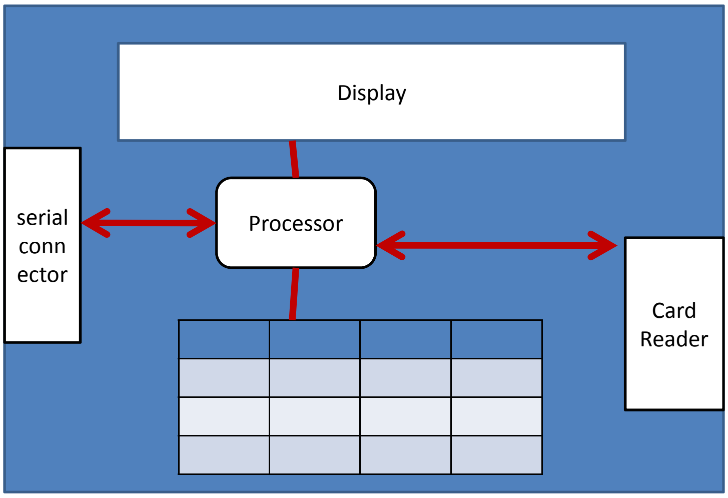

Figure 1 : architecture of the TOE

To summarize:

The TOE ("the Device") is a device with an internal electronic board, a smartcard reader, a keypad, a display and a serial connector, included in a monolithic physical casing.

The TOE is to be used linked to an external PC (via the serial connector).
The TOE is to be used with a smartcard, which must be inserted in the internal smartcard reader of the TOE

TOE type

The TOE is a hardware device connected to a PC station for the purpose of securely entering a personal data (example: pin code) and forwarding it uniquely to a smartcard (the smartcard reader is included in the physical enclosure of the device). If the secure pin entry device is used to sign specific information, this information (or a part of it) can be displayed on the display, to be verified by the user.
The TOE is a low cost product, and does not need any permanent internal secret for the use stage. The TOE does not provide any cryptographic services, except if needed for the firmware insertion.

Security features of the TOE

2) Protect the confidentiality of personal data from any potential malware on the workstation: the personal data is never keyed in on the workstation keyboard, and transmitted only to the smartcard, without passing by the workstation.
3) Protect the integrity of data to be transmitted to the smartcard: the data can be shown on the display before transmission to the smartcard and may be checked (and eventually validated) by the user.

The ST writer will describe the detailed specifications of those processings by the ST.

Specific conditions and security specificities of the TOE

This secure pin entry device is intended to be installed and used on a fixed or portable workstation in a controlled environment. The workstation may be used at home or in company premises. The workstation can be multi-user.

Hardware and software environment

In order to operate, the TOE depends greatly on the operating system used at the workstation. The workstation must have at least one serial interface and associated software. . The ST writer will define the Operating Systems it will work with, the type of serial interface, and if necessary, the adequate drivers will be provided.

The TOE is intended to provide a smartcard with a dedicated human interface. The security of the smartcard and its applications is out of scope of the TOE.

Lifecycle environment

The hardware development and fabrication stages should require just state of the art quality controls and restricted documentation, normally provided by the manufacturer. They are out of scope of the TOE. The ST writer will describe the security measures taken to ensure hardware conformance.

The firmware is part of the TOE. Depending on the fabrication process, it can be integrated in the TOE during the hardware fabrication (if it is a ROM component, for example), or at the end of the fabrication process (by flashing a EEPROM, for example). The ST writer will describe the security measures taken to ensure firmware integrity.

In the two examples of TOE lifecycles given in the following figure, the hatched blocks are in the scope of the TOE.

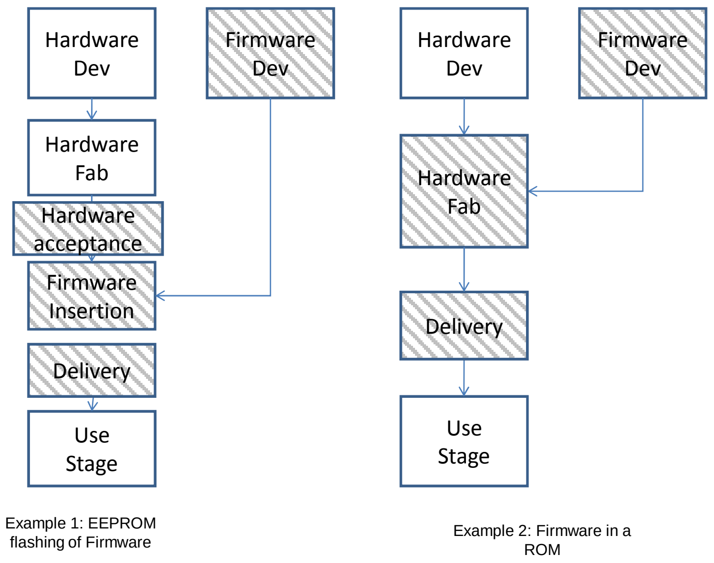

Figure 2 : Lifecycle of the TOE

2) Conformance claims (APE_CCL)

Conformance of this Protection Profile

Conformance with the Common Criteria

This protection profile conforms to the Common Criteria, Version 3.1, Release 3, dated July 2009.

- This protection profile is conformant to Part 2 of the Common Criteria, Version 3.1, Release 3, dated July 2009 (see [6])
- This protection profile is conformant to Part 3 of the Common Criteria, Version 3.1, Release 3, dated July 2009 (see [7])

Conformance with an assurance package

The level of assurance targeted by this protection profile is EAL3+ (EAL3 augmented with AVA.VAN.3, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1,ALC_FLR.3).

Conformance with a Protection Profile

This protection profile is not dependent on any other protection profile.

Conformance of security targets and protection profiles

This PP requires "**demonstrable"** conformance of the PP or ST claiming conformance to this PP.
The "demonstrable" conformity level allows:

- conformity with several protection profiles to be announced
- the specification of a higher assurance package
- the specification of alternative security functional requirements
- a security objective for the operational environment to be transformed into a security objective for the TOE
- PP operations to be modified provided that they are more restrictive

3) Security problem definition (APE_SPD)

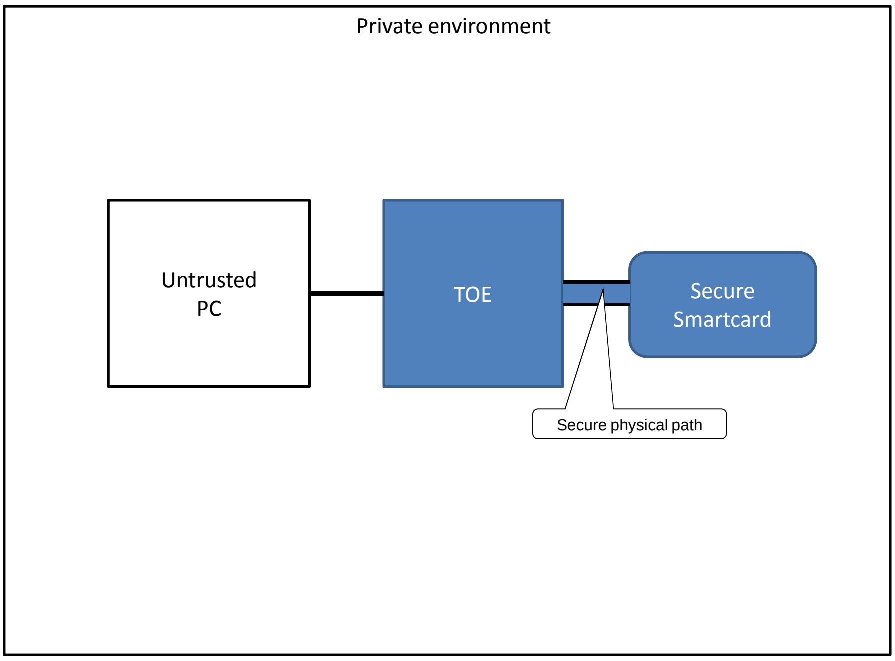

Figure 3: The environment of the TOE

Assets

Assets in the operational environment

Sensitive assets protected by the TOE

The assets that have to be protected are identification data (B.PIN) of the user and critical information to be displayed before signing (B.DIS).

B.PIN

The identification data (B.PIN) is an external asset which passes through the Device. The Device has been designed to protect this external asset, in confidentiality (this data must be passed uniquely to the smartcard), and in integrity (a modified identification data can block the smartcard application) .

Sensitivity: confidentiality, integrity

B.DIS

The critical information to be approved (B.DIS) is an internal (message in the firmware for example) or external asset. The Device has been designed to protect this asset against modification inside the TOE.

Examples of external assets:

An external asset may be a piece of data received from the PC in a command, displayed on the display of the device and checked by the user before validating the command. An external asset may be also a piece of data received from the smartcard, displayed on the display of the device and checked by the user before validating the command.

Sensitivity: integrity

Sensitive assets of the TOE

The assets of the TOE which can be attacked are:

B.FIRM	The Firmware of the TOE
B.HARD	The Hardware of the TOE

B.FIRM The firmware .This sensitive asset corresponds to all TOE programs. These programs are held in memory of the TOE.

Sensitivity: integrity.

B.HARD The hardware. This sensitive asset corresponds to the hardware casing of the TOE, in the use stage, just after firmware download.

Sensitivity: integrity.

Threats

Threat agents

A threat agent to the TOE can be :

During the use stage:
U_agressor: **an aggressor:** this is a person who has not received a product in an authorised way or otherwise gains illicit access to the TOE. The aggressor may gain access to the TOE through the PC, or have temporary access to the TOE when not in use, and modify it.

As the TOE is to be used in a private environment, the legitimate user is not considered hostile.

Attack potential

Individuals performing attacks have an **Enhanced Basic** attack potential. They correspond to malicious persons possessing the computing skills of a well-informed user having gained access to some restricted information about the TOE.

Threats

The threats to the TOE by an attacker are:

T.PIN_DISCLOSE: An attacker can try to access the pin B.PIN, and transmit it out of the TOE , by modifying the firmware B.FIRM or the hardware B.HARD of the TOE.

T.PIN_MODIFY: An attacker can try to modify the pin B.PIN in the TOE and block the smartcard application (false Pin counter), by modifying the firmware B.FIRM or inserting a hardware bug in the hardware B.HARD.

T.DIS: An attacker malware modifies the information to be displayed and signed by the Device (B.DIS). Or an attacker can try to modify the critical information to be approved (B.DIS), by modifying the firmware B.FIRM or inserting a bug in the hardware B.HARD.

OSP

OSP.USER: The user is provided with information on usage of the device, checking its integrity and replacing it if tampered with,

Assumptions

The TOE is suitable both for the office and for private use.

The end user is informed about his or her responsibility during the use of the TOE:

A.USER.UNOBSERV:

The user must enter his or her identification data unobserved.

A.USER.PIN:

It is assumed that the user stores his or her identification data using recommendations of the smartcard provider.

A.USER.KEYPAD:

It is assumed that the user enters his or her identification data using the keypad of the TOE.

A.USER.DIS:

It is assumed that the user verifies the information displayed on the display before approving it.

A.USER.USAGE:

The TOE is designed for use in private environments or office environments. That means that only a limited number of persons have access to the TOE.

4) Security objectives (APE_OBJ)

The Device is used to get the identification data (B.PIN) from the User, and transfer it only to the smartcard. The Device has been designed to protect the critical information to be approved (B.DIS) against modification inside the TOE.

The basic security objectives for the TOE are:

Security objectives for the TOE

O.REVEAL: The TOE does not reveal any identification data. An identification data, as a personal identification code (B.PIN) is not externalized from the TOE, except to the smartcard.

O.HARD_EVIDENT: The hardware casing cannot be opened easily and this opening shall be visible to the user (tamper evidence). The integrity of the hardware B.HARD can be checked by the user.

Security objectives for the environment

OE.PRIVATE: The TOE is to be used in private environments. In an office environment, the TOE should be managed to prevent access to unauthorized users. That means that the smart card reader is linked to a PC which is usable by a limited number of persons only.

OE.MANUAL: The user is provided with a user manual explaining the rules or refer to smartcard provider information for storing securely his PIN, verifying the data displayed before entering his PIN, keying his PIN unobserved on the keypad of the TOE . The manual also explains how to check TOE's integrity , stop using it if tampered with and how to replace it .

Rationale

Coverage of threats in the operational environment.

T.PIN_DISCLOSE: is countered by O.REVEAL .(Protection).

Detection: O.HARD_EVIDENT should warn the user that T.PIN_DISCLOSE is possible.

Response: The user does not use the TOE anymore (replace it with a new one).

T.PIN_MODIFY: is countered by O.HARD_EVIDENT.(Protection)

Detection: O.HARD_EVIDENT should warn the user that T.PIN_MODIFY is possible.

Response: The user does not use the TOE anymore (replace it with a new one).

T.DIS: is countered by: O.HARD_EVIDENT (should warn the user that T.DIS is possible).

Response: The user does not use the TOE anymore (replace it with a new one).

A.USER_UNOBSERVED , A.USER_KEYPAD , A.USER_DIS, A.USER_PIN are fulfilled by OE.MANUAL

A.USER_USAGE is fulfilled by OE.PRIVATE

OSP.USER is fulfilled by O.HARD_EVIDENT and OE.MANUAL

	T.PIN_DISCLOSEE	T.DIS	T.PIN_MODIFY	A.USER_UNOBSERVED	A.USER_KEYPAD	A.USER_DIS	A.USER_USAGE	A.USER_PIN	OSP.USER
O.REVEAL	X								
O.HARD_EVIDENT	X	X	X						X
OE.PRIVATE							X		
OE.MANUAL	X			X	X	X		X	X

Table 1 : Threats, assumptions and Security objectives

5) Extended components definition (APE_ECD)

Not applicable.

6) Security requirements (APE_REQ)

Security functional requirements

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **Information Flow Control SFP** on **subjects:**

- **S.INTERFACE:**

Informations:

- **OB.PIN: Identification data**

and the operations covered by the SFP:

- **OP.P_ENTRY: PIN entry**

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **Information Flow Control SFP** based on the following types of subject and information security attributes:
subjects:

- **S.INTERFACE:**

Attribute values:

USER through the keypad interface,

PC through the serial interface,

ICC Smart card through the card reader interface,

informations:

- **OB.PIN: Identification data,**

Attribute values:

USER through the keypad interface,

PC through the serial interface,

ICC Smart card through the card reader interface,

and the operations covered by the SFP:

- **OP.P_ENTRY: PIN entry**

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **OP.P_ENTRY receives OB.PIN only from S.INTERFACE attribute USER, and tranmits it only to S.INTERFACE attribute ICC**

FDP_IFF.1.3 The TSF shall enforce the [assignment: none].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows]**.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

- **OB.PIN is not transmitted to S.INTERFACE attribute PC**

FDP_RIP.2: Full residual information protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon **the deallocation of the resource from** all objects.

Note: A memory erasure of the buffer for the transmission of the PIN from the keypad to the smart card must be realized immediately after:

- extracting the card,
- abort by the user,
- timeout during the PIN input
- timeout or counter completed in a signature session.(The ST writer shall describe precisely the conditions of a session).

FPT_TOE material protection

FPT_PHP.1: Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

Note: the detection can be done by non IT means. For example, modification of the visual aspect of the TOE.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

Note: the user can be involved in the detection, for example by checking the visual aspect of the TOE.

Security requirement	Dependencies	Comments
FDP_IFC.1	FDP_IFF.1	This component is a selected component
FDP_IFF.1	FDP_IFC.1,	This components is a selected component
	FMT_MSA.3	N/A (there are no initial values)
FDP_RIP.2	No	
FDP_PHP.1	No	

Table2: Dependencies of functional requirements

Security assurance requirements

The requirements for the aimed evaluation assurance level 3 are listed in table 4 Common Criteria part 3 as follows .The augmentation AVA.VAN.3 and its dependencies are required for this type of product in regard of potential attackers (enhanced basic) considering that the usage is in private environment. ALC_FLR.3 with dependencies are listed in red. ALC_FLR3 is required to provide TOE users with confidence in the product they are using. The ADV components shall be refined to cope with the hardware acceptance process. The ST writer shall specify the procedures to be applied by the TOE developer to check the integrity of the hardware.

Assurance class	Assurance component
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete Functional Specification
	ADV_TDS.3 Basic modular design
	ADV_IMP.1 Implementation representation of the TSF
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative Procedures
ALC: Life cycle support	ALC_CMC3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life cycle model
	ALC_FLR.3 Systematic flaw remediation

	ALC_TAT.1 Well-defined development tools
ASE: security target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing: sample
AVA: Vulnerability assessment	AVA.VAN.3 Focused vulnerability analysis

Table3: Security Assurance requirements

Rationale

O.REVEAL is covered by FDP_IFC.1.1 and FDP_IFF.1.1, FDP_IFF.1.4 , FDP_IFF.1.5 as the flow control is managed inside the TOE.
O.REVEAL is covered also by FDP_RIP.2.1, as the critical information OB.PIN is not stored.
O.HARD_EVIDENT is covered by FDP_PHP.1.1 and FDP_PHP.1.2, which give the user the ability to detect tampering of the TOE .

Security requirements / Security objectives

	O.REVEAL	O.HARD_EVIDENT
FDP_IFC.1.1	X	
FDP_IFF.1.1	X	
FDP_IFF.1.2	X	
FDP_IFF.1.4	X	
FDP_IFF.1.5	X	
FDP_RIP.2.1	X	
FDP_PHP.1.1		X
FDP_PHP.1.2		X

Table4:Security objectives and security functional requirements

Conformity with a PP

Not applicable

Extended components

Not applicable

7) Acronyms

CC	Common Criteria
CCID	Integrated Circuit Cards Interface Devices
CT-API	Card terminal Application Programming Interface
EAL	Evaluation Assurance Level
EMV	Eurocard Mastercard Visa
EEPROM	Electrically Erasable Read Only Memory
ICC	Integrated Circuit Card
ID	Identifier
ISO	International Standards Organisation
IT	Information Technology
OS	Operating System
OSP	Organisational Security Policy
PC	Personal Computer
PC/SC	Personal Computer / Smart Card
PIN	Personal Identification Number
PP	Protection Profile
ROM	Read Only Memory
ST	Security Target
TOE	Target of Evaluation
USB	Universal Serial Bus

8) Bibliography

[3] PC-SC V 2.0	Interoperability Specification for ICCs and Personal Computer Systems, Revision 2.02.6, April 2009 http://www.pcscworkgroup.com/specifications/files/pcsc10_v2.02.06.pdf
[4] ISO/IEC 7816	Integrated circuit(s) cards with contacts http://www.iso.org/iso/catalogue_detail.htm?csnumber=29257
[5] QUA-STD	RGS Qualification Standard, verion 1-2 http://www.ssi.gouv.fr/IMG/pdf/RGS_qualif_standard_version_1-2.pdf
[6] CC2	Common Criteria V3-1 Révision 3 Part 2 http://www.ssi.gouv.fr/IMG/pdf/CCPART2V3-1R3.pdf
[7] CC3	Common Criteria V3-1 Révision 3 Part 3 http://www.ssi.gouv.fr/IMG/pdf/CCPART3V3-1R3.pdf
[8] CCID	Chip/Smart Card Interface Devices, Revision 1.1, April 22rd 2005 http://www.usb.org/developers/devclass_docs/DWG_Smart-Card_CCID_Rev110.pdf
[9] Common Criteria	Common Criteria for Information Technology Security Evaluation http://www.ssi.gouv.fr/site_article135.html
[10] EMV 2004	Integrated Circuit Card Terminal Specifications for Payment Systems, version 4.1

9) Glossary

Keypad	An alphanumeric or numeric keyboard
Display	An alphanumerical display of one (or more) lines of characters.
Legitimate user	The legitimate user of the device is the legitimate user of the smartcard.
PIN	The personal data to be passed securely to the smartcard application which is called PIN in the document, because in most cases, this personal data is a numeric code (Personal Identification Number).
Private environment	A place under control of this individual, or group of persons, so it can be used at home, or at the office. The Device is not intended to be used in a public area.
Serial interface	An USB or RS 232 interface, with appropriate connectors, cables and drivers.