ingenico
Healthcare
e-ID

# Security Target lite - CC EAL 3+ - Leo V3

**XRD-2015-3119**
**Public**

**Damien FRANQUET**

12/07/2016

Version 1.0

**www.ingenico.com**

28/32, boulevard de Grenelle, 75015 Paris - France / (T) +33 (0)1 58 01 80 00 / (F) +33 (0)1 58 01 91 35

Ingenico – S.A. au capital de 53 086 309 € / 317 218 758 RCS PARIS

# Table of content

**1 ST introduction ..... 5**
**1_1** ST reference ..... 5
**1_2** TOE reference ..... 5
**1_3** TOE introduction ..... 5
**1_4** TOE overview ..... 6
**1_5** TOE description ..... 6
**2 Lifecycle ..... 8**
**3 Conformance Claims ..... 9**
**4 Security problem definition ..... 10**
**4_1** Subjects ..... 10
**4_2** Assets ..... 10
**4_2_1** Sensitive assets protected by the TOE ..... 10
**4_2_2** Sensitive assets of the TOE ..... 11
**4_3** Threats ..... 11
**4_3_1** Threat agents ..... 11
**4_3_2** Attack potential ..... 11
**4_3_3** The threats to the TOE by an attacker are: ..... 11
**4_4** Organisational security policies ..... 12
**4_5** Assumptions ..... 12
**5 Security Objectives ..... 13**
**5_1** Security objectives for the TOE ..... 13
**5_2** Security objectives for the environment ..... 13
**5_3** Security objectives rationale ..... 13
**6 Extended components definition ..... 15**
**7 Security Requirements ..... 16**
**7_1** Security functional requirements ..... 16

**7_2** Functional requirement dependencies ..... 19
**7_3** Security assurance requirements ..... 19
**7_4** Security requirements rationale ..... 20
**8 Acronyms ..... 21**
**9 Bibliography ..... 22**

# Document approval

| | Name | Function | Date |
|---|---|---|---|
| **Written by** | Damien FRANQUET | HSO/SSO | 2016/07/11 |
| **Verified by** | Damien FRANQUET<br>Claude MEGGLE | HSO/SSO<br>Consultant | 2016/07/11<br>2016/07/11 |
| **Approved by** | | | |

# Document history

| Revision | Author | Date | Modification |
|---|---|---|---|
| **0.9** | D. FRANQUET | 2016/07/11 | First draft based on version XRD-2014-2626 version 1.5 |
| **1.0** | D. FRANQUET | 2016/07/12 | First release |

# 1 ST introduction

This security target describes the functional and organisational security requirements and procedures for the TOE, a “secure pin entry device” (also known as “the Device”), and its operational environment.

The target of evaluation is the Leo V3 smart card reader.

## 1_1 ST reference

| Title of the Security Target | Smartcard reader Leo V3 Security Target<br>Common Criteria EAL3+ |
|---|---|
| **Version** | 1.0 |
| **Issue date** | 12/07/2016 |
| **Document ID** | XRD-2015-3119 |
| **Author** | Damien FRANQUET, Claude MEGGLÉ |
| **Evaluation level** | EAL3 + |

## 1_2 TOE reference

| Target of evaluation | Leo V3 |
|---|---|
| **Version** | PPD002-vwx-Axy* |
| **Firmware version** | PA01.02 |
| **Issue date** | 2015/03/18 |

* Where vwx are customer personalisation (color, lens logo) and xy are minor revisions numbers. vwx and xy are not related to the security features of the TOE.

## 1_3 TOE introduction

A smartcard is a piece of plastic, with an electronic component embedded in it. It has no human interface but 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 Personal Identification Number (also known and referred as ‘PIN’) 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 of 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 embeds a « smartcard reader ».

## 1_4 TOE overview

The Leo V3 smart card reader is a secure PIN entry device, a universal smart card reader with keypad, display and a connecting cable with USB connector. The Leo V3 smart card reader cannot be used in standalone mode. It must be plugged in a Personal Computer USB plug to offer capability for secure PIN entry. The Personal Computer can be a PC with a Windows OS, Linux or Mac OS. The secure PIN entry functionality can be activated from a software application loaded in the PC (not provided and out of scope of this TOE), and used in conjunction with a secure smartcard (not provided and out of scope of this TOE).

## 1_5 TOE description

The Leo V3 smart card reader is a universal smart card reader device, which can communicate with ISO 7816 and EMV2004 compliant processor cards through the PC/SC [3] application interface. The device work with any smart card transmission protocol compliant with ISO 7816 [4] (T=0, T=1).

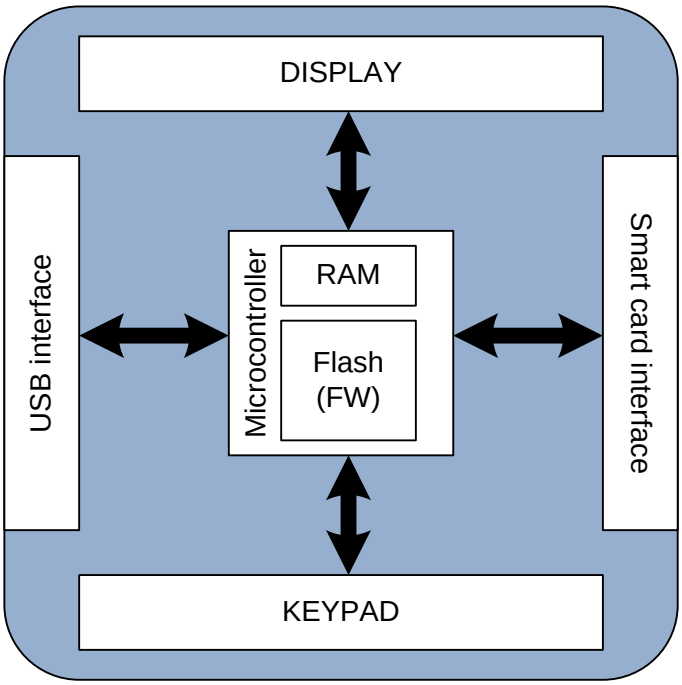
Leo V3 reader has a keypad with silicone keys, to enter a digital PIN. The numeric keys “0” to “9” as well as the keys “Clear” (yellow), “OK” (green) and “Cancel” (red) are present. The reader complies with PC/SC part 10 [3] and CCID secure command specifications [8]. Therefore, within the frame of a Secure Pin Entry session, the device inserts the digits keyed on the keypad as a PIN in the PIN field of the command to the smart card. The PIN is formatted according to external parameters transmitted through the accurate CCID PC_RDR_Secure commands as described in [8]. The firmware in the TOE manages the security functions.

In addition to standard SPE command, Leo V3 reader has a specific function of “multi-signing application”: the legitimate user can sign several documents entering only once the PIN on the smart card reader, for a limited number of documents.

It is possible to memorize the PIN for a maximum of 999 SPE.

The reader can be connected to all USB equipped host systems, like PC computers, running Microsoft Windows, Linux or Mac OS.
It is used as peripherals in the PC surrounding field. The reader is provided with power supply through the USB interface. It cannot be used in standalone mode.

PC applications communicate with the reader through PC/SC [3] interfaces. The reader is declared and recognized as a PC/SC [3] device by its PC host driver. All functions at the interfaces are illustrated for PC/SC in accordance with [3].




Details on available host software such as drivers are available in the user manual of the Leo V3.
The driver software is not included in this evaluation. The TOE ends at the USB interface to the host computer. Installation software including drivers, manual and tools can be downloaded from:
http://healthcare-eid.ingenico.com/support_leo.aspx
The Leo V3 reader is able to enter identification data (PIN) and convey it securely to a smart card, for instance a secure signature creation device. It can be used also to allow authorise access to some applications or to the computer itself, if the appropriate software has been installed.

It is possible to activate TOE multi-signing application through proprietary commands.

The firmware is filtering the commands sent to the reader for secure PIN input, and allows only PC/SC commands which involved data identification (PIN). Therefore there is no way to address directly the pinpad or the display.

The housing is sealed by means of falsification secure security stickers, which will be destroyed when someone attempt to open it. Stickers can be used only once.

# 2 Lifecycle

The firmware is part of the TOE. It is integrated in the TOE at the end of the fabrication process by flashing an EEPROM memory (and destroying a fuse thus disabling the possibility of flashing another firmware). Security stickers are put in place at the end of the fabrication process.
The fabrication process is outsourced to a partner factory/manufacturer. Security policies, defined by Ingenico Healthcare/e-ID, enforcing confidence in firmware integrity management from delivery through flashing operation on the production chain have been transmitted to the manufacturer. A specific policy for security sticker management at the factory site was also defined for the manufacturer.

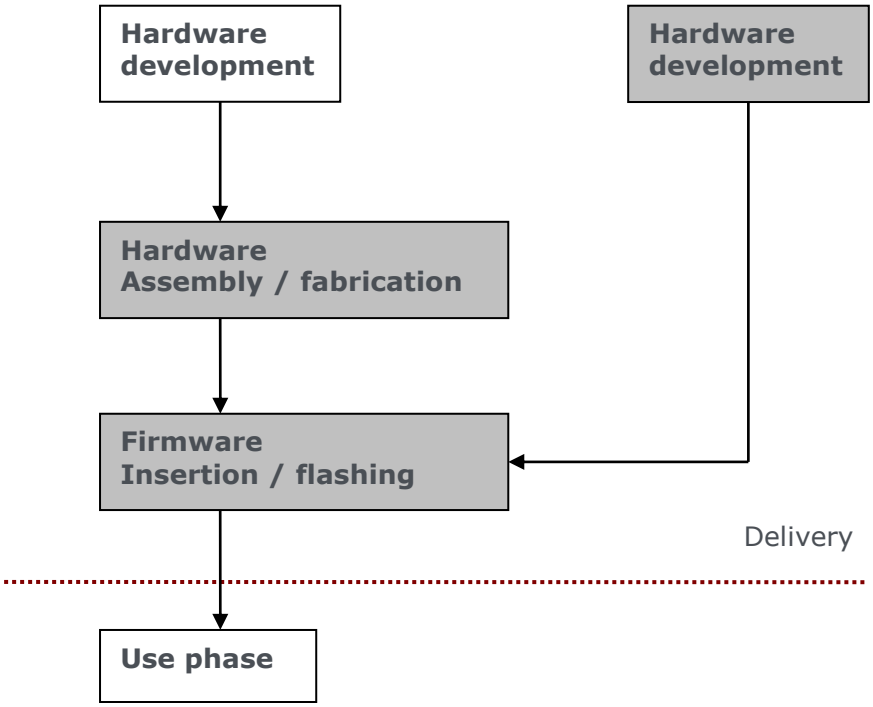



**Figure 1: Lifecycle of the TOE.**

Grey blocks are in the scope of the TOE. The delivery point is located at the Ingenico Healthcare/e-ID partner factory where goods are passed to a forwarder for delivery.

# 3 Conformance Claims

This security target is conformant to the Common Criteria, Version 3.1, Release 3, dated July 2009 as follow:

- Part 2 of the Common Criteria, Version 3.1, Release 3, dated July 2009,
- Part 3 of the Common Criteria, Version 3.1, Release 3, dated July 2009

The claimed assurance level is EAL3 augmented with ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ALC_TAT.1 and ALC_FLR.3.

# 4 Security problem definition

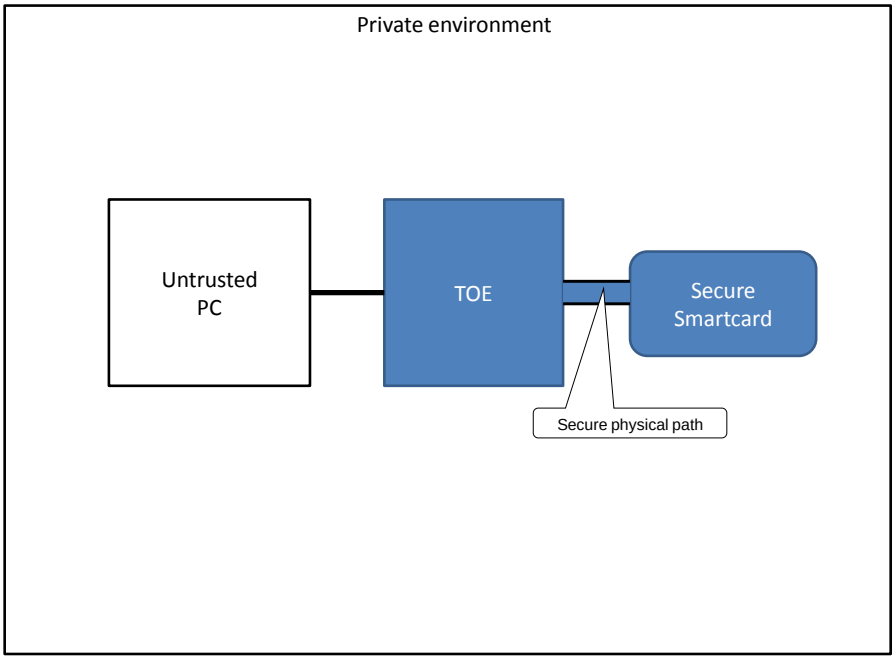



**Figure 2: The TOE and its environment.**

## 4_1 Subjects

S.PC: A personal computer that can communicate with the pinpad via a USB connection.

S.INTERFACE: represents a logical or physical communication interface that can be used by any type of users.

S.USER: A user of the TOE.

S.ICC: A smartcard that can be used with the TOE.

## 4_2 Assets

### 4_2_1 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

### 4_2_2 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.

## 4_3 Threats

### 4_3_1 Threat agents

During the use stage, a threat agent can be:
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.

### 4_3_2 Attack potential

Individuals performing attacks have an **Basic** attack potential. They correspond to persons possessing some computing skills.

### 4_3_3 The threats to the TOE by an attacker are:

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) as well as the firmware (B.FIRM) and hardware (B.HARD) of the smart card reader itself. The reader itself has no secret.

**T.PIN_DISCLOSE**: An attacker can try to access the pin B.PIN, and transmit it out of the TOE, by gaining access to 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 modifies the information to be displayed and/or signed by the Device (B.DIS), before sending it to the Device. 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.

## 4_4 Organisational security policies

**OSP.USER**: A written procedure or manual is given to the user by the smartcard provider, (or by the company if the TOE is to be used in company premises) to inform the user how to use the reader, how to store securely his smartcard (or smartcards), how to use securely his or one of his smartcards with the reader, and how to store and use securely his PIN, and how to check that the reader has not been tampered.

## 4_5 Assumptions

LEO V3 smart card readers are suitable both for the office and for private use.
Readers can support additional uses beyond those described in the Security Target. 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.

# 5 Security Objectives

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.

## 5_1 Security objectives for the TOE

The Leo V3 smart card reader is used to get the identification data (B.PIN) from the user. The basic security objectives for the TOE are:

**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 should be visible to the user (tamper evidence). The integrity of the hardware B.HARD can be checked by the user.

**O.SIGNAL**: The TOE guarantees that the secure PIN entry mode is clearly signified to the user.

## 5_2 Security objectives for the environment

The security objectives for the environment correspond in a general manner to those under 4.1 specified:

**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 people only.

**OE.MANUAL**: The user is provided with a user manual explaining the rules or, refers to the smartcard provider information for storing securely his PIN, verifies the data displayed before entering his PIN, keys 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.

## 5_3 Security objectives rationale

**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) and O.SIGNAL.
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 |
| **O.SIGNAL** | | X | | X | X | X | X | | |
| **OE.PRIVATE** | | | | | | | X | | |
| **OE.MANUAL** | X | | | X | X | X | | X | X |

# 6 Extended components definition

This security target does not contain any extended components.

# 7 Security Requirements

## 7_1 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:**
- **B.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:**
- **B.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 transmits it only to S.INTERFACE attribute ICC**

**FDP_IFF.1.3:** The TSF shall enforce **the following rules to determine if an operation among controlled subjects and controlled objects is allowed:**

**The PC (S.PC) sends commands on behalf of the application to the reader, which causes the TOE to then only cause the display (OB.DIS) to display the secure PIN entry mode message "ENTRER CODE" (OP.D_CONTROL) and to pass the entered PIN (OB.PIN) to the smart card (S_ICC), if both following conditions are met :**

**1.) The command sent is a CCID PC_To_RDR_Secure [8] command**

**2.) This PC_To_RDR_Secure command requests one of the following Secure Entry command:**

- Verify PIN.
- Change PIN.

**The PIN (OB.PIN) must be entered by the user (S.USER) at the keypad of the TOE (OP.P_ENTRY).**
**The PIN (OB.PIN) may be sent only over the card reader interface to the smart card (S.ICC) for verification of the PIN (OP.P_VERIFY).**

**FDP_IFF.1.4:** The TSF shall explicitly authorise an information flow based on the following rules:
**The TOE must rejects the command coming from the PC (S.PC) if the command sent is a CCID PC_To_RDR_Xfr_Block and if this command carry an identification data (PIN).**
**It also rejects commands coming from the PC (S.PC) if the command sent is a CCID PC_to RDR_Secure and this PC_to_RDR_Secure does not involve data identification.**
**It also accepts multi-signing command from the PC (S.PC) in order to activate the multi-signing application on the TOE. Those commands are sent through CCID PC_to_RDR_Escape.**
**The reader informs the application running on the PC (S.PC) that the command has been rejected by the appropriate return code.**

**FDP_IFF.1.5:** The TSF shall explicitly deny an information flow based on the following rules:
**B.PIN is not transmitted to S.INTERFACE attribute PC**

**SFR.FDP_RIP.2: Full residual information protection**
**SFR.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.
**A memory rework of the buffer where the PIN is stored from the keypad to the smart card is realized immediately after:**

- **extracting the card,**
- **abort by the user,**
- **timeout during the PIN input,**
- **timeout or counter completed in multi-signing application.**
- **Invalid session ID.**

The maximum value for the multi-signing application counter is 999.

**TOE access**

**SFR.FTA_TAB.1:** Default TOE access banners
**SFR.FTA_TAB.1.1:** Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

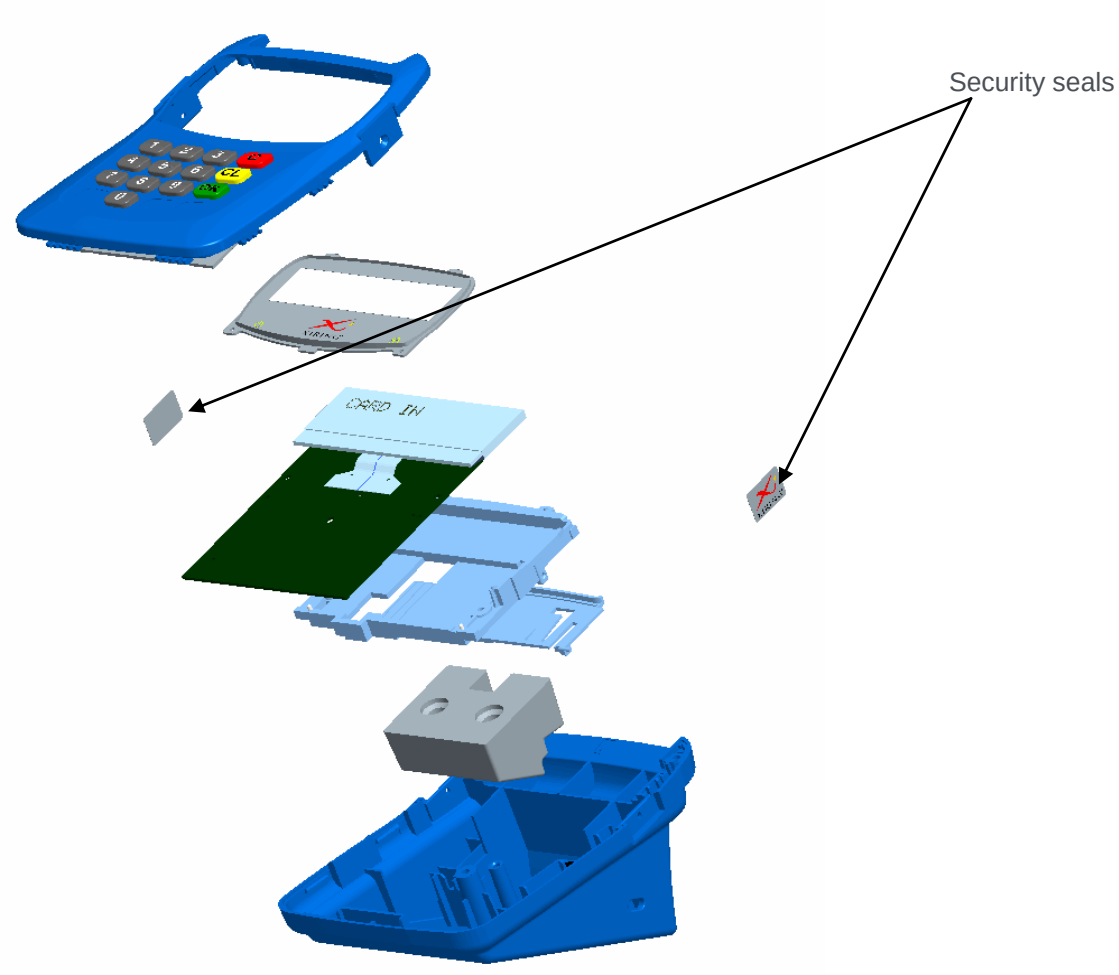
Note: During execution of the function “Secure PIN entry” a green lock icon must be lit. The message “ENTRER CODE” (French translation of “Enter PIN” ) is displayed before the entry.
After transmission of the PIN to the signature component (smart card) and confirmation by the smart card with the status byte SW1=0x90 the display shows “CODE CORRECT” (French translation of “PIN OK”).
If the entered PIN is not correct, the message “CODE INCORRECT” (French translation of “Wrong PIN” ) is displayed. The green lock icon is not lit anymore.
A disturbance of the card reader caused intentionally or due to a technical failure is indicated to the user by displaying “ERREUR” (French translation of “ERROR).
Invalid data are rejected. An error message is transferred to the host.

**TOE physical 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.
**The casing is sealed by means of falsification secure security stickers, which will be destroyed during removal and thus can be used only once.**

**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.
**The casing is sealed by means of falsification secure security stickers, which will be destroyed during removal and thus can be used only once. Thus the user can recognize by the condition of the safety seal that no manipulations at the hardware were made. If the safety seal has been tampered, then the user is at risk that his PIN can be compromised, by an electronic bug inserted in the device, or a logical bug inserted in the firmware.**



## 7_2 Functional requirement dependencies

| Security requirement | Dependencies | Comments |
|---|---|---|
| **FDP_IFC.1** | FDP_IFF.1 | This component is a selected component |
| **FDP_IFF.1** | FDP_IFC.1,<br>FMT_MSA.3 | This components is a selected component<br>N/A (there are no initial values) |
| **FTA_TAB.1.1** | None | |
| **FDP_RIP.2** | None | |
| **FDP_PHP.1** | None | |

## 7_3 Security assurance requirements

The requirements for the aimed evaluation assurance level 3 are listed in table 4 Common Criteria part 3 as follows. 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 Security enforcing 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_CMC.3 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.2 vulnerability analysis |

## 7_4 Security requirements rationale

Security requirements / Security objectives:

| | O.REVEAL | O.HARD_EVIDENT | O.SIGNAL |
|---|---|---|---|
| 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** | | |
| FTA_TAB.1.1 | | | **X** |
| FDP_RIP.2.1 | **X** | | |
| FDP_PHP.1.1 | | **X** | |
| FDP_PHP.1.2 | | **X** | |

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 B.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.

# 8 Acronyms

| Acronyms | Definition |
|---|---|
| **CC** | Common Criteria |
| **CCID** | Integrated Circuit Cards Interface Devices |
| **CT-API** | Card terminal Application Programming Interface |
| **EMV** | Eurocard Mastercard Visa |
| **ID** | Identifier |
| **PC** | Personal Computer |
| **PC/SC** | Personal Computer / Smart Card |
| **PIN** | Personal Identification Number |
| **SPR** | Secure Pin Pad Reader |
| **USB** | Universal Serial Bus |

# 9 Bibliography


| Reference | Description |
|---|---|
| **[1] Decret 2001-272** | Decret du 30/03/2001 chapitre 1 : Des dispositifs sécurisés de création de signature électronique |
| **[2] 1999/99/CE** | European Community Directive on electronic signature |
| **[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 |
| **[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 Part 1-3, September 2006 |
| **[10] EMV 2004** | Integrated Circuit Card Terminal Specifications for Payment Systems, version 4.1 |
| **[11] CC 1316-4** | Article 1316-4 du Code Civil relatif à la signature électronique |