Common Approval Scheme
A EUROPEAN INITIATIVE
FOR CARD PAYMENTS IN EUROPE

Point of Interaction Protection Profile

Date: 26th November, 2010
Version: 2.0

This page is intentionally left blank

Table of contents

Table of figures

Table of tables

1 Protection Profile Introduction

1 This document defines three Protection Profiles dedicated to payment terminals, each for a different terminal configuration, namely PED-ONLY applicable to PIN Entry Devices (PED), and POI-COMPREHENSIVE and POI-OPTION applicable to Point of Interaction (POI).

2 In the following, "this Protection Profile" stands for the Protection Profile collection composed of the three Protection Profiles configurations PED-ONLY, POI-COMPREHENSIVE and POI-OPTION.

1.1 Protection Profile Identification

1.1.1 Identification of PED-ONLY configuration

Title	Point of Interaction Protection Profile – PED-ONLY configuration
Identification	ANSSI-CC-PP-POI-PED-ONLY
Authors	Sandro Amendola, SRC Security Research & Consulting GmbH Carolina Lavatelli, Trusted Labs on behalf of CAS (Common Approval Scheme)
Version	2.0
Publication Date	26th November, 2010
Sponsor	ANSSI
CC Version	3.1 Revision 3

1.1.2 Identification of POI-COMPREHENSIVE configuration

Title	Point of Interaction Protection Profile – COMPREHENSIVE configuration
Identification	ANSSI-CC-PP-POI-COMPREHENSIVE
Authors	Sandro Amendola, SRC Security Research & Consulting GmbH Carolina Lavatelli, Trusted Labs on behalf of CAS (Common Approval Scheme)
Version	2.0
Publication Date	26th November, 2010
Sponsor	ANSSI
CC Version	3.1 Revision 3

1.1.3 Identification of POI-OPTION configuration

Title	Point of Interaction Protection Profile – OPTION configuration
Identification	ANSSI-CC-PP-POI-OPTION
Authors	Sandro Amendola, SRC Security Research & Consulting GmbH Carolina Lavatelli, Trusted Labs on behalf of CAS (Common Approval Scheme)
Version	2.0
Publication Date	26th November, 2010
Sponsor	ANSSI
CC Version	3.1 Revision 3

1.2 Protection Profile Presentation

3 This Protection Profile (PP) was developed by the Common Approval Scheme Initiative (CAS) in co-operation with the Joint Interpretation Library Terminal Evaluation Subgroup (JTEMS) to be used for the Common Criteria (CC) evaluation of Point of Interaction. CAS security requirements - which include Payment Card Industry PIN Entry Device (PCI POS PED 2.0) security requirements as well as security requirements on payment transaction data and external communication - have been translated into CC functional and assurance security requirements.

4 The products in the scope of this Protection Profile are payment terminals with Integrated Circuit (IC) Card based online and offline transaction capabilities. Products range from simple PED with PIN keypad, display and IC and Magnetic Stripe Card Readers to complete terminals (POI) that manage transaction data and provide external communications capabilities. Other functionalities than payment, which might be processed by the same device, e.g. fleet card processing, are out of scope of this PP.

5 The usage of this PP is intended to achieve CC evaluations/certifications, which can be used multiple times for approvals of payment schemes participating in the Single Euro Payment Area (SEPA) certification framework.

6 Privacy shielding does not belong to the Target of Evaluation (TOE). Moreover, as the payment applications currently still differ from scheme to scheme the payment applications are also excluded from the TOE in this PP. Ideally, only the security features of the device to be used by payment applications (such as libraries for the use of critical functions like control of the display and the keypad) are in the scope of the TOE whereas the payment applications themselves are assigned to the environment. The TOE includes payment application separation mechanisms, secure software download and update and security features that protect the interfaces of the device. With this approach, the state machine controlling the payment transaction flow is not part of the TOE. Nevertheless, the scope of the TOE can be extended within a specific product

evaluation to cover payment application; in this case, the security target shall address payment application issues.

7 It has to be noted that the security certification is only one input for the approval of a product in a specific payment scheme. Another input is e.g. the functional certification of the device, in which for instance the transaction flow of the payment application is addressed.

8 This Protection Profile defines three PP configurations, each of them with a particular TOE:

- PED-ONLY configuration: The TOE provides protection for both IC and Magnetic Stripe card based transactions. It does not manage transaction data nor provide any external communication facility. The TOE is fully PCI POS PED v2.0 conformant. Note that the TOE of this configuration is the PED part of a POI. This PP configuration has been introduced to acknowledge the current supply chain of POIs, where PEDs are often manufactured separately as components of a broader POI. The aim of this configuration is to support a POI composite evaluation for specific use case scenarios of merchants or other POI vendors. Evaluation against this configuration will not in itself secure common certification across all CAS member markets.
- POI-COMPREHENSIVE configuration: This configuration fully incorporates the PED-ONLY configuration. Therefore the TOE provides protection for both IC and Magnetic Stripe card based transactions and is fully PCI POS PED v2.0 conformant. In addition to the PED-ONLY configuration it provides payment transaction data management and external communication facilities for interaction with the Acquirer defined by CAS. The POI-COMPREHENSIVE configuration covers a harmonized superset of all security requirements which are considered appropriate to defend against current and perceived future threats. The aim of this configuration is to support the concept of the POI as a universal acceptor for SEPA compliant cards. It is the baseline configuration that is intended to secure common approval across all CAS member markets.
- POI-OPTION configuration: This TOE provides protection for IC based transactions, payment transaction data management and external communication facilities. The only difference to the POI-COMPREHENSIVE configuration is the absence of support for the protection of offline plaintext PIN and for the Magnetic Stripe Reader. The POI-OPTION configuration is a subset of the POI-COMPREHENSIVE configuration. Therefore it is not compliant with the POI-COMPREHENSIVE configuration. The aim of this configuration is the support of the business needs of payment schemes, which are migrating to a chip only environment and are using encrypted PIN only. Note that as a consequence, POI-OPTION configuration is not relying on the robustness of the IC Card Reader. This configuration is seen as a major step towards a future POI-CHIP-ONLY configuration. All requirements defined by CAS do apply to POI-OPTION configuration. This configuration is intended to lead to a common security certification of payment schemes being in this migration phase.

9 JTEMS and CAS will collectively review and assess threats to determine the validity or need for any future collection of security requirements.

10 This Protection Profile defines a specific evaluation package, called EAL POI, that is built upon EAL2 and includes some of the most relevant elements from the EAL4 assurance level, with the aim of ensuring that the POI configurations can be evaluated at the appropriate level. The EAL POI balances evaluation effort according to the architecture of the POI, and emphasizes the use of suitably informed penetration testing that reflects the variety of assets. The construction of this package allows the efficient evaluation of PED and POI configurations taking into account the specific attacks observed on PED and POI devices, and the risk management processed for the systems that use them. In critical areas the assurance requirements are augmented to a level significantly greater than EAL2, e.g. with PIN encryption keys evaluated against POI-High attack potential.

11 POI evaluations conformant with this Protection Profile shall rely on the terminals Evaluation Methodology defined in [POI CEM].

12 This Protection Profile requires "strict" conformance. Security Targets or Protection Profiles conformant to this Protection Profile can extend the perimeter of the chosen PED/POI configuration with additional functionalities if necessary.

13 The evaluation of this Protection Profile has been performed by the French ITSEF CEACI Thales. The PP has been certified by French Scheme ANSSI.

1.3 References

[CC1] Common Criteria Part 1, Version 3.1, Revision 3, CCMB-2009-07-001

[CC2] Common Criteria Part 1, Version 3.1, Revision 3, CCMB-2009-07-002

[CC3] Common Criteria Part 1, Version 3.1, Revision 3, CCMB-2009-07-003

[CEM] Common Criteria Evaluation Methodology, Version 3.1, Revision 3, CCMB-2009-07-004

[CASPOI] Framework of POI Security Requirements, CAS Common Approval Scheme, 27th October 2008, Version Draft 1.0 with revisions from a meeting of the EPC Security and Certification Expert group held in Brussels on November 25th 2009 where PLUS requirements were explained to relevant stakeholders.

[EMV] EMV Book 1 to 4, Version 4.2

[EPC Shield] European Payment Council, Towards our Single Payment Area: Privacy shielding of the PIN Entry Device, Implementation Guidelines, Version 1.3, February 2009

[POI AttackPot] Application of Attack Potential to POIs, Draft, Version 0.3, July 2010. *Note: POI evaluations shall rely on the current version of this document at the moment of the evaluation.*

[POI CEM] Terminals Evaluation Methodology – CEM refinement , Version 1.0, January 30th 2010. *Note: POI evaluations shall rely on the current version of this document at the moment of the evaluation.*

[RNGPCI] Payment Card Industry (PCI) POS PIN Entry Device (PED), Version 2.0, Appendix A, Appendix C
Rukhin, Andrew, et al., "A Statistical Test Suite for Random and Pseudo-random Number Generators for Cryptographic Applications", NIST SP800-22, revisions dated May 15, 2001.
Kim, Song-Ju, et al., "Corrections of the NIST Statistical Test Suite for Randomness".
Bassham, Larry (NIST). "Validation Testing and NIST Statistical Test Suite" presentation, dated July 22, 2004.
Hill, Joshua (InfoGard Labs). "ApEn Test Parameter Selection".

2 TOE Overview

2.1 TOE Type

14 The TOE is a product of type PIN Entry Device (PED) or Point of Interaction (POI), either without shielding capabilities or with privacy shielding compliant with EPC guidelines [EPC Shield].

15 The TOE has particular characteristics depending on the PP configuration:

- PED-ONLY configuration: The TOE provides protection for both IC and Magnetic Stripe card based transactions. It does not manage transaction data nor provide any external communication facility.
- POI-COMPREHENSIVE configuration: The TOE provides protection for both IC and Magnetic Stripe card based transactions, provides payment transaction data management and external communication facilities for interaction with the Acquirer.
- POI-OPTION configuration: TOE provides protection for IC Card based transactions, payment transaction data management and external communication facilities. Protection of the offline plaintext PIN authentication and of Magnetic Stripe Reader is out of the scope the TOE.

2.2 TOE Security Features

16 The aim of this section is to provide a high level description of the POI configurations, their logical and physical perimeter, assets, objectives and security features. This section starts with a presentation of a generic POI, then it defines the TOE security features. These features vary from one configuration to another, with a shared kernel around PIN Entry, encrypted PIN authentication and IC Card Reader protection.

2.2.1 Generic POI

2.2.1.1 Generic Payment Transaction Process

17 The following figure shows the POI payment transaction process based on offline PIN verification.

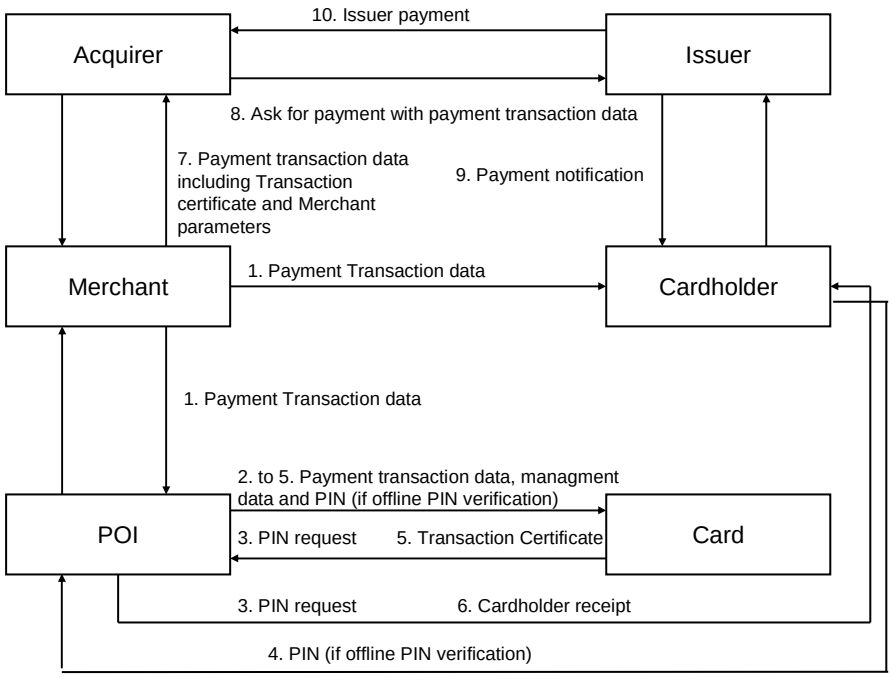


Figure 1: Generic POI Payment Transaction Process

1. The merchant submits payment transaction data (e.g. amount) to the Cardholder through the display and to the POI.

2. The POI submits payment transaction data to the card in order to perform card risk management (and also possibly to the Issuer's authorisation server in case of an online request). This step covers all card/ POI data exchanges until transaction completion.

3. The card requests Cardholder authentication by PIN comparison.

4. The Cardholder provides his PIN to be verified against a reference PIN managed by the IC card (offline) or the remote Issuer via the Acquirer system (online). The POI dispatches the PIN depending on the transaction type: online or offline. Entering the valid PIN implies that the Cardholder accepts the terms of the transaction (i.e. validates transaction data), and enables further transaction processing by granting the card with the rights connected to the Cardholder.

5. Upon successful completion of transaction processing, including card risk management on behalf of the Issuer (online), the card issues a transaction certificate.

6. The POI edits transaction receipts - including transaction data and certificate, as well as Cardholder and merchant identifiers and data - to the Cardholder and merchant.

18 After the POI payment transaction the following process applies. This process is not strongly related to the POI payment transaction.

7. The merchant claims payment by forwarding the transaction data and certificate, plus his own parameters (e.g. merchant identifier) to the Acquirer bank.

8. The Acquirer bank sends this payment request to the Issuer bank detaining the Cardholder's account.

9. The Issuer maps the payment request to one of its Cardholders, debits him and issues a payment notification (to be checked by the Cardholder for consistency).

10. The Issuer pays the Acquirer refund, possibly through global bank-to-bank balance.

11. The Acquirer pays the merchant refund for the goods delivered to the Cardholder.

2.2.1.2 Generic Terminal Management Process

19 The generic Terminal Management process of the POI administration consists of the following steps:

1. A Terminal Management session is established with the Terminal Management System (TMS). The POI executes operations in communication with the TMS and/or asks the TMS for operations to be performed (e.g. the POI asks whether new software is available).

2. The TMS sends POI management data or software to the POI via a data download (e.g. new software is downloaded and authenticity of software is verified by the POI) and/or the POI sends POI management data to the TMS via a data upload.

3. POI configurations are activated or deactivated (e.g. new software is activated). This operation may be performed immediately or deferred in time.

4. The POI reports on its hardware, software and configuration status (e.g. the software status of the POI is reported).

2.2.1.3 Generic POI Architecture

20 The generic POI architecture includes the following components:

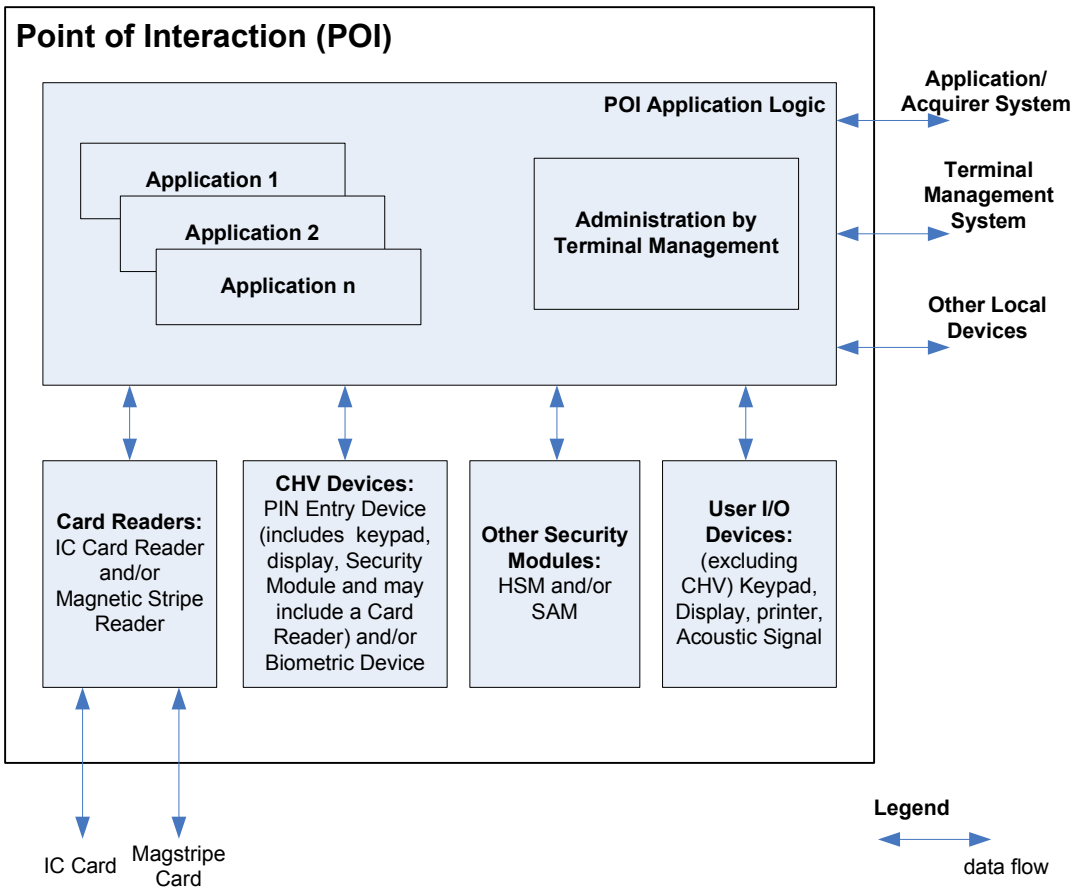


Figure 2: Generic POI Architecture

2.2.1.4 Generic POI Architecture Components

21 POI components may be integrated in the same device as the POI Application Logic. They may also be distributed as independent devices connected to the POI Application Logic by various means such as cables, wireless link, local area network, etc. It is up to the ST author to specify which POI components are inside the TOE and thus, shall be evaluated. For instance, the printer or audible signals, amongst User I/Os, are optional components.

a) **POI Application Logic** (PAL). The POI Application Logic manages the applications running on the POI. At least one of the applications executes payment transactions. The PAL offers security features to the applications and includes the Terminal Management as well as all the related internal interfaces needed to access to the POI peripherals and to the external Terminal Management System.

b) **Applications.** The objective of a POI is to execute applications issued by different application providers (e.g. bank, health, loyalty, government, etc.). A POI may support a multi-application environment.

c) **POI Components.** POI Components are driven by the POI Application Logic. The POI components are:

- **Card Readers**: devices that provide interfaces to cards. The Card Readers may support different types of cards, e.g. IC contact cards, IC contactless cards and Magnetic Stripe cards. POI as per this Protection Profile includes one or more IC Card Readers thus allowing IC based payment transactions. The IC Card Reader may belong to the tamper-responsive enclosure of the PED (CHV devices block in figure 2) or it may be separated (Card Readers block in the figure).

- **Cardholder Verification Devices** (CHV): devices for Cardholder authentication, e.g. a PIN Entry Device (PED). A PED contains a keypad, a display, a Security Module (SM) for PIN encryption and may also include an IC Card Reader. POI as per this Protection Profile includes at least one PED thus allowing Cardholder PIN entry and authentication. As for the PED keypad and PED display, distributed architectures are also accepted provided that the PED keypad security module controls the PED display. The interfaces of the PED keypad security module and the PED display have to be protected.

- **Security Modules** (SM): devices for management of cryptographic keys and cryptographic functions (e.g. a Hardware Security Modules (HSM) or a Security Application Module (SAM) as part of a CHV or an external Security Application Module (SAM) for a purse application (PSAM)). A POI with integrated IC Card Reader may include only one SM (SM for CHV), but in non-integrated cases additional SMs are required (e.g. to provide encryption/decryption of PINs between PED and IC Card Reader if they are not enclosed into one tamper-responsive boundary).

- **User I/Os:** that may include display, keyboard, printer, and audible signals. Different User I/O interfaces may exist for the Attendant and for the Cardholder.

d) **External IT Entities.** POI may provide communication capabilities to interact with external IT entities:

- **IC Card**: The Cardholder's IC Card that interacts with the POI through the IC Card Reader.

- **Magnetic Stripe Card**: The Cardholder's Magnetic Stripe Card that interacts (passively) with the POI through the Magnetic Stripe Reader.

- **Application / Acquirer System:** Entity operated by the Application Provider resp. Acquirer or the Acquirer Processor with whom the POI exchanges transaction data.

- **Terminal Management System:** Entity used to administrate (installation, maintenance) a set of POIs. It is used by the Terminal Administrator.

- **Local Devices:** Any device that is not a peripheral device and that either inputs or outputs payment transaction data. Examples of Local Devices are the Electronic Cash Register (ECR), a Vending Machine Controller or a Pump Controller for Petrol Outdoor configurations. The connections to these external devices may be implemented by various means such as private or public network.

2.2.1.5 POI Example

22 Figure 3, Figure 4 and Figure 5 show the minimum set of components and functions of the TOE in PED-ONLY, POI-COMPREHENSIVE and POI-OPTION configurations respectively, with all components in one device, excluding any payment application.

23 Notice that TOE components may be connected via an open network (in that case the data exchanged on the interfaces between the components are signed or encrypted if required by the Security Functional Requirements or protected by other means).

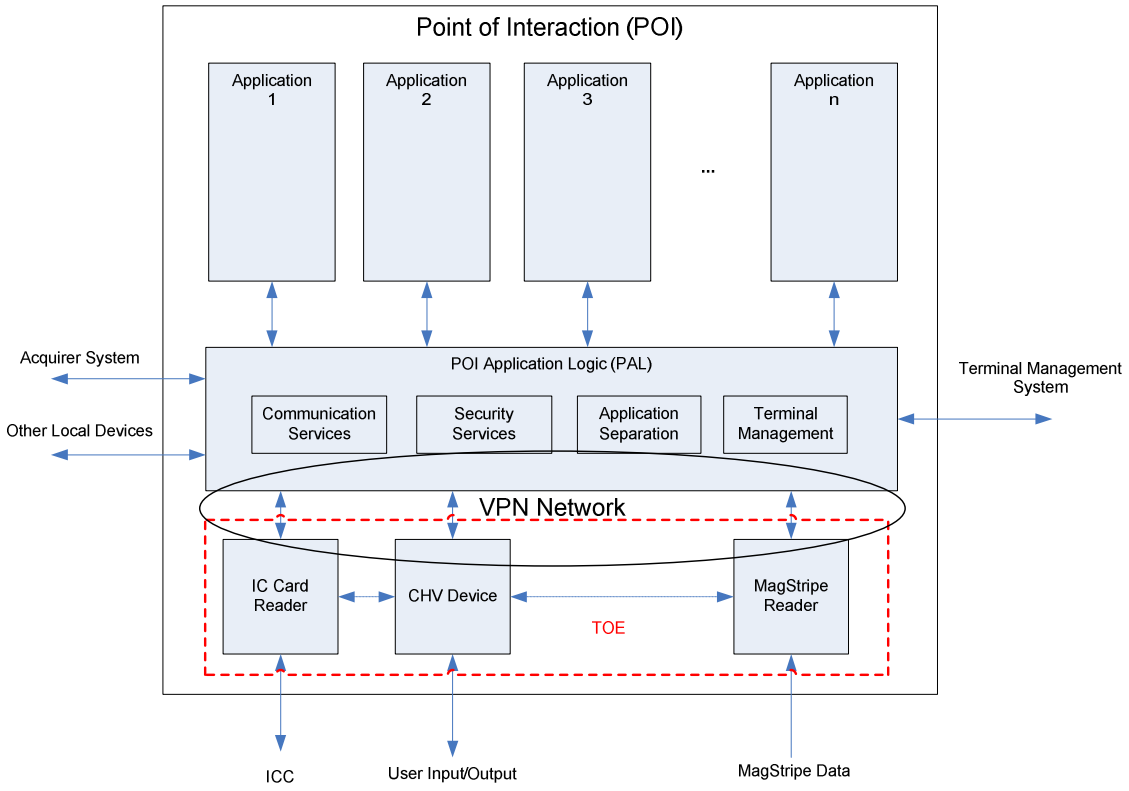


Figure 3: TOE in PED-ONLY configuration

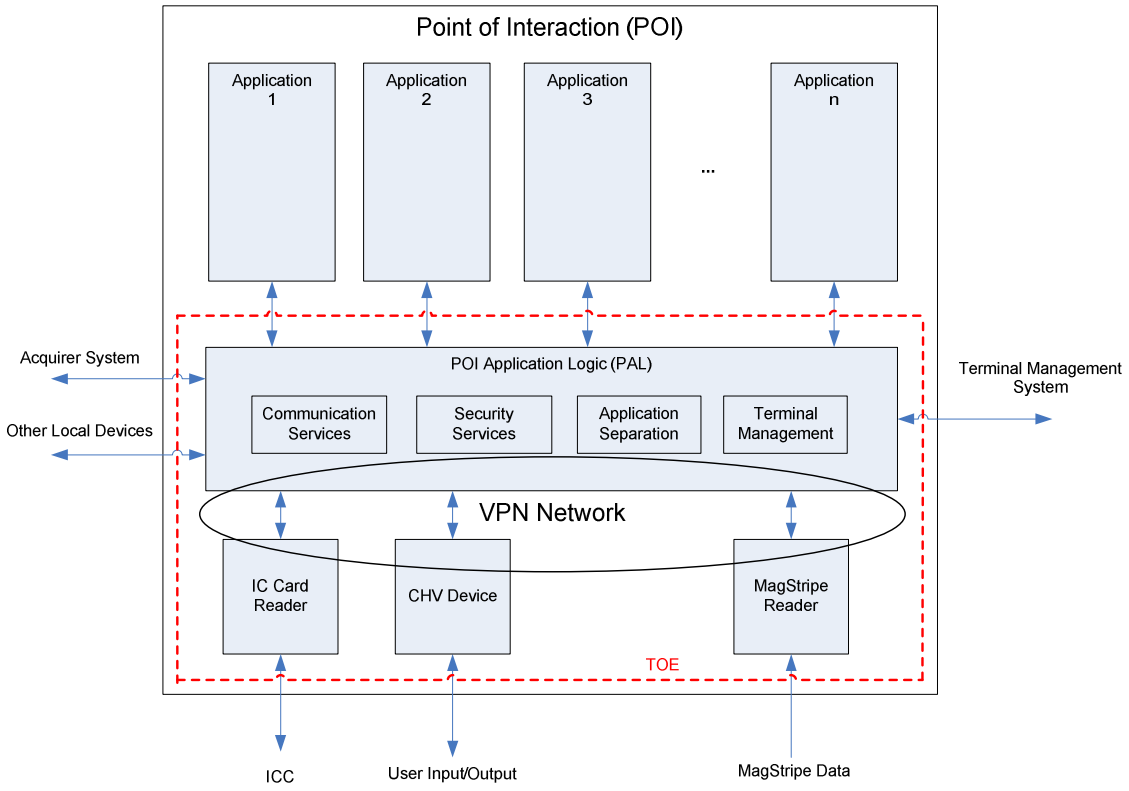


Figure 4: TOE in POI-COMPREHENSIVE configuration

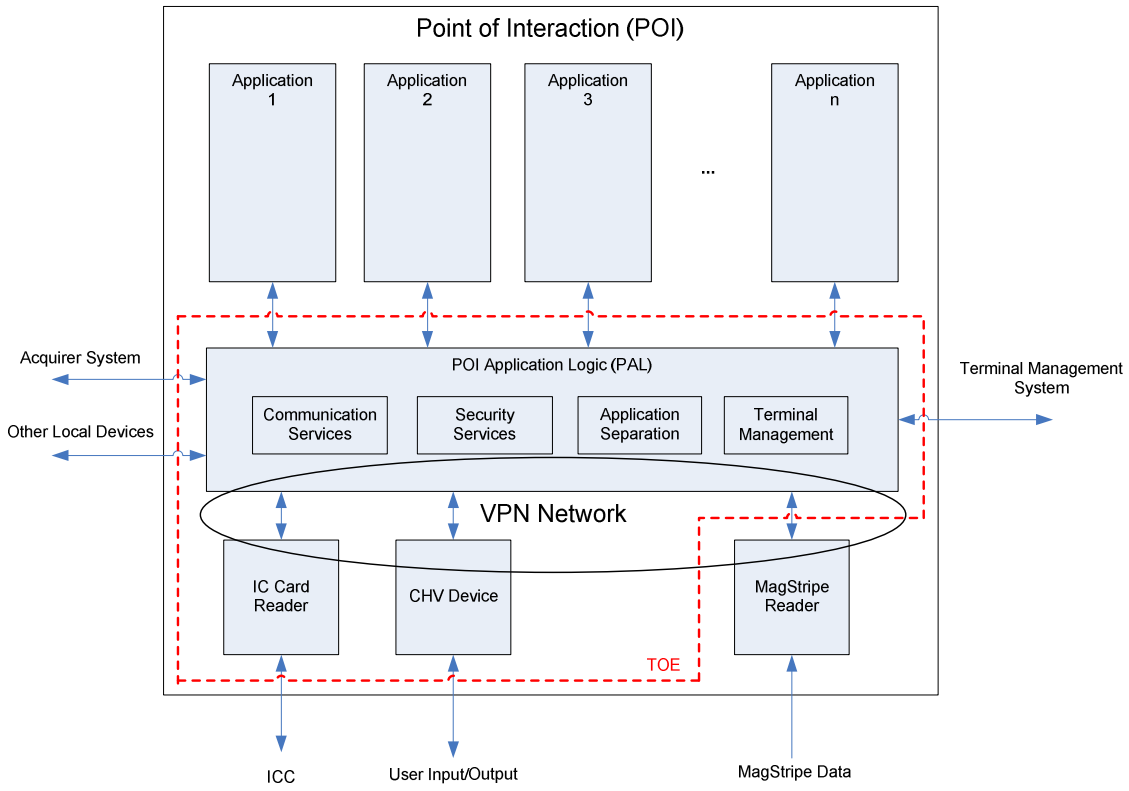


Figure 5: TOE in POI-OPTION configuration

2.2.2 Security features

24 The security of the TOE payment transactions[1] relies on a number of security features provided by the TOE, on the capability of the IC Card as well as on the selected payment application by the IC Card.

25 The goal of the TOE is to enforce, through its security features, part or all of the following properties on the assets, depending on the TOE configuration. These properties on the assets provide an overview of the objectives for the TOE which are precisely described in section 5:

- Confidentiality of PIN (the asset PIN is defined in section 4.1, its definition takes into account the nature of the PIN, e.g. encrypted or plaintext).
- Confidentiality, authenticity and integrity of PIN processing keys.
- Authenticity and integrity of PIN processing software.
- Authenticity and integrity of POI management and transaction data.
- Confidentiality, authenticity and integrity of POI data protection keys.
- Protection of IC Card Reader against tampering
- Protection of Magnetic Stripe Reader against tampering

26 Each TOE configuration provides a specific set of security features that meets the intended usage and the assumptions on the environment. Moreover, each of the security features are protected at a specific level, namely, POI-Basic, POI-Low, POI-Moderate or POI-High, The precise definition of these protection levels in terms of attack potential is given in [POI AttackPot].

27 PED and POI configurations share a common TSF structure made of TSF concentric rings (also called TSF parts), as shown in the following figures.

[1] This Protection Profile addresses security features independently of the standard they comply with, [EMV] or any other legacy, domestic or private IC Card standard.

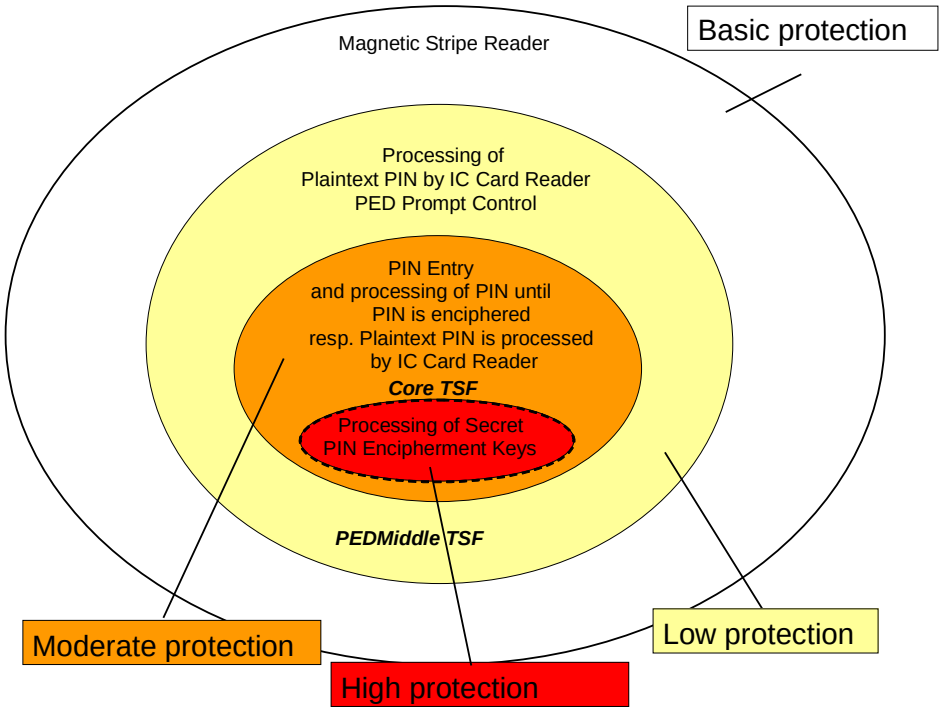


Figure 6: TSF structure in PED-ONLY configuration

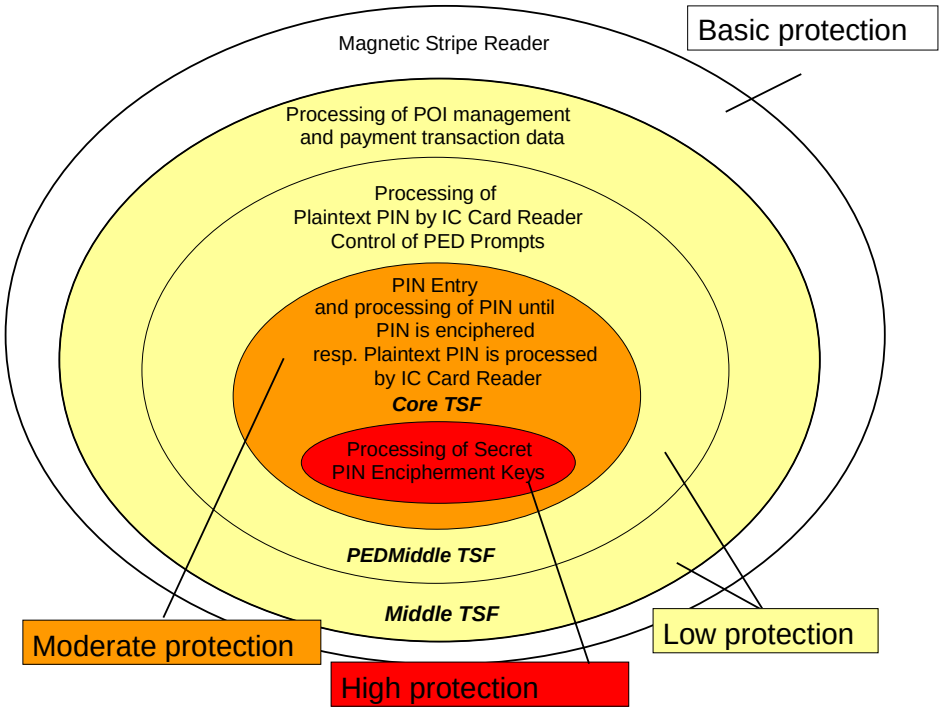


Figure 7: TSF structure in POI-COMPREHENSIVE configuration

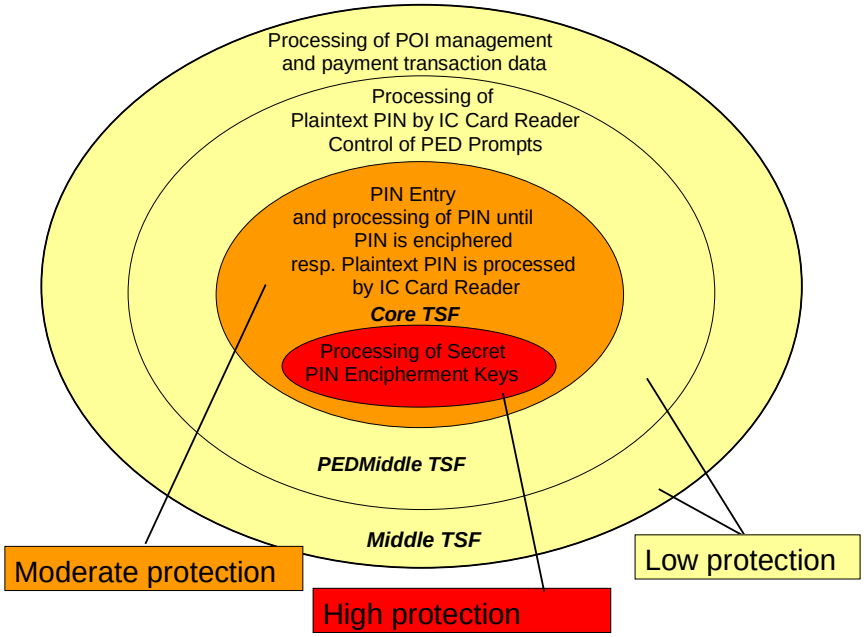


Figure 8: TSF structure in POI-OPTION configuration

28 The TSF parts define the logical and physical TOE boundary of each configuration. Each TSF part is associated to one attack potential level:

- Core TSF Keys (Core TSF PIN encipherment keys) are protected at POI-High level.
- Core TSF contains security features protected at POI-Moderate level.
- PEDMiddle TSF contains security features protected at POI-Low level.
- Middle TSF contains security features protected at POI-Low level.
- MSR is protected at POI-Basic level.

29 Although PEDMiddle TSF and Middle TSF may also contain cryptographic keys and operations, these keys are not used for direct protection of PIN data and thus are protected at POI-Low level, which is consistent with the other assets in these TSF parts. Indeed in the case of PEDMiddle TSF, the PIN data protection is ensured by the IC Card Reader. The PIN in IC Card Reader requires only POI-Low protection level (whereas the PIN in PED requires POI-Moderate protection level). This holds also for PED Prompts.

30 The Magnetic Stripe Reader (MSR), present in PED-ONLY and POI-COMPREHENSIVE configurations, is evaluated at POI-Basic level.

31 The physical boundaries of each TSF part is defined by the PED or POI components involved in the realisation of the TSF part's security features. Note that a component may contribute to more than one TSF part (e.g. a random number generator that is used

for all purposes). In this case, the resistance required from the component is that of the more protected TSF part the component belongs to.

32 There are two different architectures for PEDs and IC Card Readers as components of a POI: in one architecture the PED and the IC Card Reader are integrated into one tamper-responsive boundary. In the other, the PED and the IC Card Reader are not integrated into one tamper-responsive boundary and therefore the Plaintext PIN, addressed by PED-ONLY and POI-COMPREHENSIVE configurations, has to be encrypted on the way to the IC Card Reader.

33 The security features provide a high level view of the security of the terminals. The precise view is given by the SFRs in section 9. The complete list of security features, regardless of the TOE configuration, consists of:

1. PIN Entry without exposure of PIN digits.
2. Encipherment of PIN for offline or online Cardholder encrypted PIN authentication and transfer for further processing (to the IC Card Reader or to the Acquirer).
3. Encipherment of PIN for offline Cardholder plaintext PIN authentication and transmission to the IC Card Reader. Applicable only to distributed architectures where PED and IC Card Reader are not enclosed into one tamper-responsive boundary.
4. Protected transmission of PIN for offline Cardholder authentication of Plaintext PIN to the IC Card Reader. Applicable only to integrated architectures where PED and IC Card Reader are enclosed into one tamper-responsive boundary.
5. Decipherment of PIN by the IC Card Reader and transmission to the IC Card in plaintext. Applicable only to distributed architectures where PED and IC Card Reader are not enclosed into one tamper-responsive boundary.
6. Periodic authentication of PIN processing software.
7. Authenticity and integrity protection of administration (e.g. downloading, update) of PIN processing software and keys, including appropriate cryptographic means.
8. Integrity protection of POI management and payment transaction data and cryptographic means to protect payment transaction data at external communication lines against disclosure and modification.
9. Authenticity and integrity protection of administration (e.g. downloading, update) of POI management and transaction processing software and keys, including appropriate cryptographic means.
10. Control of PED prompts.
11. Tamper-detection/tamper-responsiveness (PED, PED SM, IC Card Reader, IC Card Reader SM, Magnetic Stripe Reader).
12. Secure downloading of payment application.

2.2.2.1 Security features in each PP configuration

34 Table 1 defines the logical boundaries of each PP configuration in terms of TSF parts implementing a particular set of security features. The items in the cells refer to the security features listed in section 2.2.2.

PP configuration	CoreTSF	CoreTSF Keys	PED Middle TSF	Middle TSF	MSR
PED-ONLY	1, 2, 3, 4, 6, 7, 11	PIN encipherment keys for 2, 3, 5, 11	5, 10, 11		11
POI-COMPREHENSIVE	1, 2, 3, 4, 6, 7, 11	PIN encipherment keys for 2, 3, 5, 11	5, 10, 11	8, 9, 12	11
POI-OPTION	1, 2, 6, 7, 11	PIN encipherment keys for (2), 11	10	8, 9, 12	

Table 1: TSF decomposition by PP configuration

35 The components of a POI described in section 2.2.1.4 may be part of the TOE or not. Some of the local devices may be external in strict terms, but sometimes, eg. for a cash register, they may be originators of data to be protected in the TOE. Table 2 defines the default physical boundaries of each PP configuration in terms of components associated to TSF parts.

PP configuration	CoreTSF	CoreTSF Keys	PED Middle TSF	Middle TSF	MSR
PED-ONLY	PED Keypad	IC Card Reader_SM, PED_SM	PED Display PED Keypad IC Card Reader		Magnetic Stripe Reader
POI-COMPREHENSIVE	PED Keypad	IC Card Reader_SM, PED_SM	PED Display PED KeyPad IC Card Reader	Other POI components	Magnetic Stripe Reader
POI-OPTION	PED Keypad	PED_SM	PED Display PED Keypad	Other POI components	

Table 2: Physical boundaries of TSF parts by PP configuration

36 *Application note: The IC Card Reader SM is not required in integrated architectures.*

37 *Application note: The Security Target author shall update the default logical and/or physical boundaries of the TOE regarding TSF parts, according to the product specific properties. The Security Target author is allowed to augment inner rings with components from the outer rings. This means, Core TSF boundary can only be enlarged, with elements from the default PED Middle or Middle TSF, and PED Middle TSF can include components in the default Middle TSF.*

2.3 Non-TOE Hardware/ Software/ Firmware available to the TOE

38 There is no hardware/ software/ firmware available to the TOE.

2.4 TOE Usage

39 The TOE is intended to be used in payment environments. The characteristics required for the environment depend on the PP configuration:

- PED-ONLY configuration: The TOE is intended to be used as a POI component in any payment environment satisfying global PCI requirements.
- POI-COMPREHENSIVE configuration: The TOE is intended to be used in any SEPA payment environment satisfying global PCI requirements.
- POI-OPTION configuration: The TOE is intended to be used by some payment schemes like girocard.

2.5 TOE Life Cycle

40 The main phases of the TOE life cycle are the following:

41 Developer Phase:

1. Development and Manufacturing
2. Initial Software and Cryptographic Key Loading

42 Operational Phase (User Phase):

3. Installation
4. Acquirer Initialisation
5. Use by Merchant and Customer

43 The delivery of the TOE takes place at the end of developer phase. Thus TOE development and manufacturing as well as Initial Software and Cryptographic Key Loading are covered by the evaluation process.

44 The TOE behaviour during the usage phase by the Merchant and Customer is described by the guidance documentation, evaluated with the AGD assurance class.

45 *Application Note: The ST author shall update this life cycle according to the product specificities, e.g. integrated or distributed device, application loading during Initial*

Software Loading and/or during use, configuration of applications with device specific parameters, etc.

2.5.1 Developer phase

46 **Development and Manufacturing**

47 POI development and manufacturing consists of producing

- POI hardware containing embedded software
- Additional software for that POI (when applicable)
- Initial Key Loading and if necessary upload of personalisation cryptographic keys

48 During manufacturing, the POI is assembled, powered on and tested (using the embedded software if present). Pre-personalisation is the manufacturing step when a POI receives the cryptographic keys to be used in the subsequent personalisation phase. In some cases, additional software is added to the embedded software at later phases of the POI life cycle.

49 **Initial Software and Cryptographic Key Loading**

50 Software load agents are installed during initial software loading to allow further remote software installation, if applicable. The installation of a load agent uses the minimum load software present in the embedded software.

51 Initial Cryptographic Keys are loaded into the POI. Additional cryptographic keys can also be loaded during this phase. It is the task of the ST author to describe which cryptographic keys are loaded during the developer phase and which keys are loaded during the operation phase.

52 The TOE is delivered at the end of the Initial Software and Cryptographic Key Loading, which may be performed either by the Terminal Administrator through a Terminal Management System, either by the Terminal Manufacturer.

53 *Application note: Initial Software and Cryptographic Key Loading are post-manufacturing steps, e.g. even if a Terminal Administrator performs it (which should set this step in user phase), it still is subject to evaluation and stays in the SAR perimeter. The ST author shall specify exactly the actors implied in Initial Software and Cryptographic Key Loading.*

2.5.2 User phase

54 During the User phase at the Merchant premises, the POI performs card based payment transactions. POI administration is performed by an Acquirer either through a connection to a Terminal Management System or directly at the POI. Further cryptographic keys may be loaded to personalise the POI.

55 POI installation and POI Acquirer Initialisation are pre-requisites to the use of the POI. These steps are performed at the Merchant site using the user-accessible interfaces of the POI.

56 **Installation**

57 Installation depends on the configuration of the POI, either integrated in one enclosure or distributed. It is up to the ST author to specify the actual installation steps for the evaluated POI. These steps may include:

- physical installation of the different POI components,
- cabling and connections to external peripherals which may be local, e.g. an Electronic Cash Register, or remote via an external access line,
- software downloading,
- configuration with specific parameters,
- mutual recognition of POI components (allowing components to exchange information, for instance in the context of a Large Retail configuration),
- test of the whole POI configuration,
- installation of the address of each Acquirer and Terminal Administrator with whom the Merchant has a contract.

58 **Acquirer Initialisation**

59 Local operation on the POI is needed to start initialisation by the Acquirer. Acquirer initialisation takes place with each Acquirer with whom the Merchant operating the POI has a contract.

60 Further cryptographic keys may be loaded during the Acquirer Initialisation to personalise the POI.

61 The Acquirer downloads parameters configuring how transactions will be processed for each of the acquired brands. A Merchant who does not want to get involved in the administration of his POI would put a Terminal Management System in charge of initialisation. Another Merchant may put his own POI Attendant in charge of initialisation.

62 Sometimes, in preparation for Acquirer address installation (POI installation steps) and for Acquirer application configuration (Acquirer initialisation steps), the POI receives the parameters that are common to the Acquiring environments during the personalisation phase (e.g. list of active Acquirers on the market with their initial host address, list of Application Identifiers and public keys of commonly accepted brands).

63 It is up to the ST author to specify the actual initialisation steps for the evaluated POI. It may also include software downloading.

3 Conformance Claims

3.1 Conformance claim to CC

64 This Protection Profile is conformant to the Common Criteria version 3.1 revision 3:

- CC Part 2 [CC2] extended
- CC Part 3 [CC3] extended

65 The CC Part 2 is extended with the security functional components FCS_RND.1 Quality metric for random numbers, FPT_EMSEC.1 TOE emanation, and FIA_API.1 Authentication Proof of Identity.

66 The CC Part 3 is extended with the security assurance components AVA_POI.1 Basic POI vulnerability analysis, AVA_POI.2 Low POI vulnerability analysis, AVA_POI.3 Moderate POI vulnerability analysis, and AVA_POI.4 High POI vulnerability analysis. Despite the hierarchical relationship between these components (cf. section 7.4) they are all necessary to the definition of the EAL POI package because each of them apply to one TSF part. Annex 12 explains the relationship between AVA_POI and AVA_VAN.2.

3.2 Conformance claim to a package

67 This Protection Profile is conformant to EAL POI which is defined in section 8.2.

3.3 Conformance claim of the PP

68 This PP does not claim conformance to any other PP.

3.4 Conformance claim to the PP

69 The conformance to this PP, required for the Security Targets and Protection Profiles claiming conformance to it, is **strict**, as defined in CC Part 1 [CC1].

4 Security problem definition

4.1 Assets

70 The following table summarises the assets of the TOE and their sensitivity: Confidentiality (C), Authenticity (A) and Integrity (I).

Asset	Sensitivity
PIN	C
ENC_PIN	C
PLAIN_PIN	C
Cleartext PLAIN_PIN	C
Ciphertext PLAIN_PIN	C
MAN_DAT	A, I
PAY_DAT	A, I
Magnetic Stripe Track Data	C, A, I
ENC_PIN_PK	A, I
ENC_PIN_SK	C, A, I
PLAIN_PIN_SK	C, A, I
PED_MIDDLE_PK	A, I
PED_MIDDLE_SK	C, A, I
POI_PK	A, I
POI_SK	C, A, I
CORE_SW	A, I
CORE_HW	A, I
PED_MIDDLE_SW	A, I
PED_MIDDLE_HW	A, I
POI_SW	A, I
PAYMENT_APP	A, I

Table 3: Assets sensitivity

71 **PIN**

72 Cardholder personal identifier, used to authenticate himself against the IC Card or the Issuer. The PIN stands for the digits entered by the Cardholder, before any treatment by the TOE.

73 There are two categories of PIN: ENC_PIN and PLAIN_PIN. ENC_PIN stands for the PIN to be used for online or offline encrypted authentication, while PLAIN_PIN stands for the PIN to be used for offline cleartext authentication. Like PIN, the assets ENC_PIN and PLAIN_PIN stand for the set of digits entered by the Cardholder before any processing.

74 Sensitivity: Confidentiality.

75 **ENC_PIN (PIN digits that have to be received encrypted by the IC Card or the Issuer)**

76 PIN used by the Cardholder to authenticate himself in one of the two following ways (cf. item 2 from the list of security features in section 2.2.2)

- Online authentication: the POI payment application and the IC Card application require sending the PIN encrypted via the online interface of the POI to the Issuer via the Acquirer.
- Offline ciphertext authentication: the POI payment application and the IC Card application require sending the PIN encrypted to the IC Card via the IC Card Reader interface.

77 Sensitivity: Confidentiality.

78 **PLAIN_PIN (PIN digits that have to be received in cleartext by the IC card)**

79 PIN used by the Cardholder to authenticate himself in the following way:

- Offline plaintext authentication: the POI payment application and the IC Card application require sending the PIN in cleartext to the IC Card.

80 There are two categories of PLAIN_PIN, depending on the POI architecture, defined hereafter: Ciphertext PLAIN PIN and Cleartext PLAIN_PIN.

81 Sensitivity: Confidentiality.

82 **Ciphertext PLAIN_PIN (in distributed POI architectures, PIN digits that have to be received in cleartext by the IC Card)**

83 The PLAIN_PIN that has to be encrypted prior to sending it to the IC Card Reader, which then deciphers it before sending it in cleartext to the IC Card. This asset is relevant only for those POI architectures where the PED and the IC Card Reader are separated devices (i.e. not integrated into one single tamper-responsive boundary).

84 Sensitivity: Confidentiality.

85 *Application note: This corresponds to items 3 then 5 from the list of security features (cf. section 2.2.2).*

86 **Cleartext PLAIN_PIN (in integrated POI architectures, PIN digits that have to be received in cleartext by the IC Card)**

87 The PLAIN_PIN that has to be sent to the IC Card Reader in cleartext is called Cleartext PLAIN_PIN. This asset is relevant only for those POI architectures where the PED and the IC Card Reader are included in the same tamper-responsive boundary.

88 Sensitivity: Confidentiality.

89 *Application note: This corresponds to item 4 from the list of security features (cf. section 2.2.2).*

90 **POI_SW (POI software)**

91 Software (code and data) of the MiddleTSF.

92 Sensitivity: Authenticity and Integrity.

93 **PED_MIDDLE_SW**

94 Software (code and data) of the PEDMiddle TSF.

95 Sensitivity: Authenticity and Integrity.

96 **PED_MIDDLE_HW**

97 Hardware of the PEDMiddle TSF.

98 Sensitivity: Authenticity and Integrity.

99 **CORE_SW**

100 Software (code and data) of the Core TSF.

101 Sensitivity: Authenticity and Integrity.

102 **CORE_HW**

103 Hardware of the Core TSF.

104 Sensitivity: Authenticity and Integrity.

105 **MAN_DAT (POI management data)**

106 At least POI Management data are the POI Unique Identifier, the Merchant Identifier and the Acquirer risk management data[2]. The POI_PK is a special kind of MAN_DAT.

107 Sensitivity: Authenticity, Integrity.

108 *Application note: MAN_DAT shall be protected inside the TOE and through external communications.*

109 **PAY_DAT (Payment transaction data)**

110 Data related to the payment transaction. It includes at least the amount, the Primary Account Number (PAN), the personal account number, the currency, the date and time, the encrypted PIN, the transaction identifier of the payment transaction, the cryptogram data, the Authorization Reply and any data which is transferred between the Issuer and the IC Card like card script processing and card management data.

111 Sensitivity: Authenticity and Integrity.

112 *Application note: The TOE ensures protection of PAY_DAT inside the device. Protection of PAY_DAT that are sent outside the device shall be implemented if required by the Acquirer, using TOE security services: The payment application may use the TOE security services to avoid disclosure and modification of PAY_DAT when this data is sent through the online interface.*

113 **ENC_PIN_PK (Public ENC_PIN cryptographic keys)**

114 All public cryptographic keys used to protect the confidentiality of ENC_PIN and the authenticity and integrity of CORE_SW including corresponding Certificate Verification Keys.

115 Sensitivity: Authenticity and Integrity.

116 **ENC_PIN_SK (Secret/private ENC_PIN cryptographic keys)**

117 All secret/private cryptographic keys used to protect the confidentiality of the ENC_PIN and the authenticity and integrity of CORE_SW. Note that private keys are not used to encipher ENC_PIN.

118 Sensitivity: Confidentiality, Authenticity and Integrity.

119 **PED_MIDDLE_PK (Public PEDMiddle cryptographic keys)**

120 PEDMiddle TSF public cryptographic keys used to protect the integrity and authenticity of PED_MIDDLE_SW.

121 Sensitivity: Authenticity and Integrity.

[2] Issuer and Acquirer risk management data are used to decide, together with the card, which kind of authentication and authorisation is necessary.

122 **PED_MIDDLE_SK (Secret/private PEDMiddle cryptographic keys)**

123 PEDMiddle TSF secret/private cryptographic keys used to protect the confidentiality, integrity and authenticity of PED_MIDDLE_SW and Prompt Controls.

124 Sensitivity: Confidentiality, Authenticity and Integrity.

125 **POI_PK (Public POI cryptographic keys)**

126 Middle TSF public cryptographic keys used to protect the integrity and authenticity of POI_SW, PAY_DAT and MAN_DAT (POI transaction and management data respectively).

127 Sensitivity: Authenticity and Integrity.

128 **POI_SK (Secret/private POI cryptographic keys)**

129 Middle TSF secret/private cryptographic keys used to protect the confidentiality, integrity and authenticity of POI_SW, PAY DAT and MAN_DAT (POI transaction and management data respectively).

130 Sensitivity: Confidentiality, Authenticity and Integrity.

131 **PLAIN_PIN_SK (Secret/private PLAIN_PIN cryptographic keys)**

132 All secret cryptographic keys used to protect the confidentiality of Ciphertext PLAIN_PIN.

133 Sensitivity: Confidentiality, Authenticity and Integrity.

134 *Application note: Note that private keys are not used to encipher PLAIN_PIN. This asset is relevant to distributed PED architectures, where the IC Card Reader is not in the same tamper-responsive enclosure as the PED keypad.*

135 **Magnetic Stripe Track Data**

136 The Primary Account Number (PAN) and other data.

137 Sensitivity: Confidentiality, Authenticity and Integrity

138 **PAYMENT_APP**

139 The payment application installed on the POI. It includes the payment application code and any additional data which comes with application code (configuration data, etc.)

140 Sensitivity: Integrity and Authenticity

4.1.1 Assets in each PP configuration

141 Table 4 defines the assets of each PP configuration and the TSF parts they are assigned to. There is no different between PP configurations in the assignments.

142 Note that an asset may be associated to more than one TSF part in a given configuration.

Asset	PED-ONLY				POI-COMPREHENSIVE				POI-OPTION			
	Core TSF	CoreTSF Keys	PEDMiddle TSF	Middle TSF	Core TSF	CoreTSF Keys	PEDMiddle TSF	Middle TSF	Core TSF	CoreTSF Keys	PEDMiddle TSF	Middle TSF
PIN	x				x				x			
ENC_PIN	x	x			x	x			x	x		
PLAIN_PIN	x				x							
Cleartext PLAIN_PIN	x				x							
Ciphertext PLAIN_PIN	x	x	x		x	x	x					
POI_SW								x				x
PED_MIDDLE_SW			x				x				x	
PED_MIDDLE_HW			x				x				x	
CORE_SW	x				x				x			
CORE_HW	x				x				x			
MAN_DAT								x				x
PAY_DAT								x				x
ENC_PIN_PK	x				x				x			
ENC_PIN_SK		x				x				x		
PED_MIDDLE_PK			x				x				x	
PED_MIDDLE_SK			x				x				x	
POI_PK								x				x
POI_SK								x				x
PLAIN_PIN_SK		x	x			x	x					
PAYMENT_APP								x				x
Magnetic Stripe Track Data	MSR TSF				MSR TSF							

Table 4: Assets by PP configuration

4.2 Users

143 Users are humans or IT entities external to the TOE that interact with the TOE.

144 Users are defined sections 4.2.1 and 4.2.2. Users applicable to each PP configuration are defined in section 4.2.3.

4.2.1 Authorised Human Users

145 **Cardholder**

146 The Cardholder interacts with the POI via man-machine interfaces: he reads payment transaction data displayed on the POI, inserts her/his IC card, authenticates her-self/himself with her/his PIN, confirms the payment transaction and takes the receipt.

147 **Attendant**

148 The payment application in the POI or in a connected device may initiate a payment transaction at the request of the Attendant. The Attendant interacts with the TOE via a man-machine interface. The payment transaction is either initiated by the Attendant or by a Local Device. The Merchant himself can be the attendant.

149 **Merchant**

150 A retailer, or any other person, company, or corporation that agrees to accept (bank) cards in the framework of a contract with an Acquirer.

151 **Terminal Administrator**

152 The Terminal Administrator maintains the TOE directly by local operations or re-motely through a Terminal Management System.

4.2.2 External Entities

153 **Acquirer system**

154 The Acquirer System is the entity that exchanges payment transaction data with the POI. Used by the Application Provider resp. Acquirer or the Acquirer Processor.

155 **Terminal Management System**

156 The Terminal Management System is the entity used to administrate (installation, maintenance) a set of POIs: software and parameter download and application activa-tion / deactivation. Used by a Terminal Administrator.

157 **IC Card**

158 The Cardholder's IC Card is an entity interacting with the POI during a payment transaction. The Cardholder's IC Card acts on behalf of the Card Issuer.

159 **Magnetic Stripe Card**

160 The Cardholder's Magnetic Stripe Card is an entity interacting with the POI during a payment transaction. The Cardholder's Magnetic Stripe Card is the Card Issuer’s representative.

161 **Local Device**

162 A payment transaction may be initiated at the request of the Attendant or a Local Device. Examples of Local Devices are the Electronic Cash Register (ECR), a Vending Machine Controller or a Pump Controller for Petrol Outdoor configurations. The connections to these external devices may be implemented by various means such as private or public network etc.

163 **Payment Application**

164 The Payment Application corresponds to the payment application code and data using the Payment Application Logic and the peripheral components of the POI to process a payment transaction. There may be more than one Payment Application in the POI. The Payment Application acts on behalf of the Acquirer.

165 **Risk Manager**

166 The Risk Manager is an entity interacting with the IC Card, the Terminal Management System and the Acquirer System during a payment transaction. The inputs from all three entities helps the Risk Manager determining which type of ENC_PIN (online encrypted or offline encrypted) shall be used.

4.2.3 Users in each PP configuration

167 Table 5 defines the users of each PP configuration.

User	PED-ONLY	POI-COMPREHENSIVE	POI-OPTION
Cardholder	X	X	X
Attendant	X	X	X
Merchant	X	X	X
Terminal Administrator	X	X	X
Acquirer System	X	X	X
Terminal Management System	X	X	X
IC Card	X	X	X
Magnetic Stripe Card	X	X	
Local Device	X	X	X
Payment Application	X	X	X
Risk Manager	X	X	X

Table 5: Users by PP configuration

4.3 Subjects

168 Subjects are active components of the TOE that act on the behalf of users.

169 Subjects applicable to each PP configuration are defined in section 4.3.1.

170 **Payment Application Logic (PAL)**

171 The Payment Application Logic manages the applications running on the POI. The PAL includes software and all the related internal interfaces needed to access to the POI peripherals and external devices. Only part of PAL is SFR-enforcing or SFR-supporting.

172 *Application note: The security components of the POI related to the PAL point at "the security enforcing and supporting part of PAL".*

173 **Terminal Management**

174 The Terminal Management executes POI management commands issued by the Terminal Management System. It may also act of its own, for example when an attack is detected.

175 **IC Card Reader and IC Card Reader SM (Security Module)**

176 The **IC Card Reader** which manages the communications between the IC Card and the POI. The IC Card Reader SM decrypts the Ciphertext PLAIN_PIN to be sent to the IC Card in cleartext.

177 **PED: (PED) keypad, (PED) display, (PED) SM**

178 The **PED** as Cardholder Verification Device and its **(PED) keypad** where the PIN is entered, its **(PED) display** where the Cardholder is asked to enter its PIN and its **(PED) SM** (Security Module) which processes keys or manages them (PIN encryption, MAC verification for CORE_SW).

179 **Core Loader**

180 The loader downloading CORE_SW into the POI.

181 **PED Middle Loader**

182 The loader downloading PED_MIDDLE_SW into the POI.

183 **Middle Loader**

184 The loader downloading POI_SW into the POI.

185 **Payment Application Loader**

186 Loader for downloading and updating payment applications.

187 **Magnetic Stripe Reader**

188 The Magnetic Stripe Reader reads the Magnetic Stripe Track Data of the Magnetic Stripe Card of the Cardholder.

4.3.1 Subjects in each PP configuration

189 Table 6 defines the subjects of each PP configuration.

Subject	PED-ONLY	POI-COMPREHENSIVE	POI-OPTION
Payment Application Logic	X	X	X
Terminal Management	X	X	X
PED	X	X	X
IC Card Reader	X	X	X
Magnetic Stripe Reader	X	X	
Core Loader	X	X	X
PED Middle Loader	X	X	X
Middle Loader		X	X
Payment Application Loader		X	X

Table 6: Subjects by PP configuration

4.4 Threats

190 Any user of the TOE may behave as threat agent. The attack paths that implement the threats may involve physical and/or logical means.

191 **T.MerchUsurp (Merchant Identity Usurpation)**

192 A fraudulent Merchant is credited for transactions that Cardholders intended for another Merchant by manipulating another Merchant's TOE to make the Cardholders issue payment instructions modifying the amount in payment transaction data PAY_DAT to his benefit or stealing and modifying another Merchant's payment transaction data PAY_DAT before they are collected or by modifying risk management data, POI Unique Identifier or the Merchant Identifier in the MAN_DAT.

193 Related assets: MAN_DAT, PAY_DAT, POI_SW, POI_PK, POI_SK.

194 *Application note: The attack on the POI Unique Identifier can be executed by manipulating the Middle TSF or at the external interface to the Acquirer which is also part of the Middle TSF.*

195 **T.CardholderUsurpEPIN (Cardholder Identity Usurpation ENC_PIN)**

196 Fraudsters with POI-moderate attack potential level gain unauthorised access to a Cardholder's account by disclosing the ENC_PIN via any manipulation of the POI.

197 Fraudsters with POI-high attack potential level gain unauthorised access to a Cardholder's account by disclosing the ENC_PIN via penetration of the POI and/or monitoring of the POI emanations (including power fluctuations) that would result in the disclosure of the ENC_PIN_SK.

198 The goal is to steal later the IC Card and to perform a transaction based on payment transaction data PAY_DAT with the captured PIN and the stolen IC Card.

199 Related assets: ENC_PIN, CORE_SW, CORE_HW, ENC_PIN_SK, ENC_PIN_PK.

200 **T.CardholderUsurpCiphPPIN (Cardholder Identity Usurpation Ciphertext PLAIN_PIN)**

201 Fraudsters with POI-moderate attack potential level gain unauthorised access to a Cardholder's account by disclosing the Ciphertext PLAIN_PIN via any manipulation of the POI.

202 Fraudsters with POI-high attack potential level gain unauthorised access to a Cardholder's account by disclosing the Ciphertext PLAIN_PIN via penetration of the POI and/or monitoring the POI emanations (including power fluctuations) that would result in the disclosure of the PLAIN_PIN_SK.

203 Fraudsters with POI-low attack potential level gain unauthorised access to a Cardholder's account by disclosing the Ciphertext PLAIN_PIN via penetrating the IC Card Reader (as part of PED_MIDDLE_SW and PED_MIDDLE_HW) making any additions, substitutions or modifications.

204 The goal is to steal later the IC Card and to perform a transaction based on payment transaction data PAY_DAT with the captured PIN and the stolen IC Card.

205 Related assets: Ciphertext PLAIN_PIN, CORE_SW, CORE_HW, PED_MIDDLE_SW, PED_MIDDLE_HW, PLAIN_PIN_SK, PED_MIDDLE_PK.

206 *Application note: This threat applies to POI with separated PED and IC Card Reader.*

207 **T.CardholderUsurpClearPPIN (Cardholder Identity Usurpation Cleartext PLAIN_PIN)**

208 Fraudsters with POI-moderate attack potential level gain unauthorised access to a Cardholder's account by disclosing the Cleartext PLAIN_PIN via any manipulation of the POI.

209 Fraudsters with POI-low attack potential level gain unauthorised access to a Cardholder's account by disclosing the Cleartext PLAIN_PIN via penetrating the IC Card Reader (as part of PED_MIDDLE_SW and PED_MIDDLE_HW) making any additions, substitutions or modifications.

210 The goal is to steal later the IC Card and to perform a transaction based on payment transaction data PAY_DAT with the captured PIN and the stolen IC Card.

211 Related assets: Cleartext PLAIN_PIN, CORE_SW, CORE_HW, PED_MIDDLE_SW, PED_MIDDLE_HW, PED_MIDDLE_PK.

212 *Application note: This threat applies to POI with integrated PED and IC Card Reader.*

213 **T.PromptControl (Manipulation of Prompt Control)**

214 Fraudsters gain unauthorised access to the Prompt Control (e.g. by corrupting PED_MIDDLE_SW) and use the Prompt Control to ask the Cardholder to enter his/her PIN in order to disclose it (e.g. by processing it in unprotected areas).

215 Related assets: PED_MIDDLE_SW, PED_MIDDLE_HW, PED_MIDDLE_SK, PED_MIDDLE_PK.

216 **T.Transaction (Transaction with usurped Cardholder identity)**

a) Fraudsters perform payment transactions and manipulate TOE hardware or software (POI_SW) to accept counterfeit or stolen IC cards. Before the modification the TOE would detect such cards.

b) Fraudsters use good IC cards and manipulate the TOE hardware or software (POI_SW) to generate payment transactions that debit the wrong account in payment transaction data PAY_DAT.

c) Fraudsters (including a fraudulent Cardholder) use good IC cards and later, during transaction collection, tap the line between TOE and Acquirer and erase their transactions manipulating payment transaction data PAY_DAT stored in the TOE.

217 Related assets: POI_SW, PAY_DAT, POI_PK, POI_SK.

218 **T.FundsAmount (Funds transfer other than correct amount)**

a) Fraudulent Merchants manipulate the TOE in order to make the Cardholder issue payment instructions for more than he thinks modifying the amount in payment transaction data PAY_DAT or to make the Cardholder issue several payment instructions instead of one generating several sets of payment transaction data PAY_DAT.

b) Fraudsters use good cards and manipulate TOE to generate transactions based on manipulated payment transaction data PAY_DAT that are rejected by the Acquirer when collected.

c) A fraudulent Cardholder issues valid payment instructions generating valid payment transaction data PAY_DAT but later destroys payment transaction data PAY_DAT before they are collected.

d) Fraudsters modify the interface between TOE and Acquirer; modify payment instructions by modification of payment transaction data PAY_DAT into refunds.

219 Related assets: POI_SW, PAY_DAT, POI_PK, POI_SK.

220 **T.BadDebt (Account overdraft, bad debt)**

221 A fraudulent Cardholder manipulates the TOE not to go online, thus preventing the Acquirer to collect funds and making the Merchant think the transaction performed correctly whereas no funds have been collected.

222 Related assets: POI_SW, MAN_DAT.

223 **T.SecureCommunicationLines**

224 An attacker manipulates or misuses the POI services underlying the protection of external communication lines in order to disclose or modify the PAY_DAT sent or received on external communication lines.

225 Related assets: PAY_DAT, POI_SW, POI_PK, POI_SK.

226 *Application note: This is a threat against the services provided by the POI. The assets PAY_DAT and POI_SW are indirectly threaten if the services are used to protect them. Note that the protection of PAY_DAT on the external communication lines is a choice of the payment application (cf. definition of PAY_DATA).*

227 **T.Magstripe**

228 An attacker tries to penetrate the POI to make additions, substitutions, or modifications to the Magnetic Stripe Reader head and associated hardware or software, in order to determine or modify Magnetic Stripe data.

229 Related assets: Magnetic Stripe Track Data.

230 **T.IllegalCodeInstall**

231 An attacker may try to violate the integrity and the authenticity of the downloaded application by accessing the communication channel between the POI and the terminal management device or falsely authenticating himself as a trusted authority and thus being able to install untrusted code.

232 Related assets: PAYMENT_APP.

4.4.1 Threats in each PP configuration

233 Table 7 defines the threats to each PP configuration.

234 A threat is associated to the TSF parts that manipulate the threaten assets.

Threat	PED-ONLY	POI-COMPREHENSIVE	POI-OPTION
T.MerchUsurp		X	X
T.CardholderUsurpEPIN	X	X	X

Threat	PED-ONLY	POI-COMPREHENSIVE	POI-OPTION
T.CardholderUsurpCiphPPIN	X	X	
T.CardholderUsurpClearPPIN	X	X	
T.PromptControl	X	X	X
T.Transaction		X	X
T.FundsAmount		X	X
T.BadDebt		X	X
T.SecureCommunicationLines		X	X
T.IllegalCodeInstall		X	X
T.Magstripe	X	X	

Table 7: Threats by PP configuration

4.5 Organisational Security Policies

235 **OSP.WellFormedPayApp (Well-formed Payment Applications)**

236 Payment Applications implemented on the POI shall use the security mechanisms provided by the TOE in a sense that the security of the assets is ensured.

237 **OSP.ApplicationSeparation**

238 The TOE shall implement an application separation mechanism if it provides a multi application environment.

239 **OSP.POISurvey**

240 Procedural measures like inspections and guidance will be implemented preventing manipulations of the TOE enclosure. In particular procedural measures shall reveal manipulations of the IC card interface in order to prevent attacks based on electronic circuits mounted at the IC card interface of the TOE's Card Reader. Those who are responsible for the TOE shall establish and implement procedures for training and vetting administrators of the TOE, or training the supervisors.

241 **OSP.MerchantSurvey**

242 In case of a fraudulent Merchant performing attacks via manipulations of the enclosure or the interfaces of the TOE, especially the IC card interface, the payment schemes shall detect manipulations of a large number of payment transactions at the same merchant with their surveillance systems.

243 The payment schemes implement organisational measures to detect such manipulations.

244 *Application note: The OSP is necessary to counteract the following scenario: A Merchant deploys a faked POI in order to perform payment transactions.*

245 **OSP.KeyManagement**

246 Cryptographic keys have to be securely managed. Especially the generation and installation of cryptographic keys and certificates have to be done in a manner that private or secret cryptographic keys are protected against disclosure and that all cryptographic keys are protected against modification when they are processed outside the POI. Furthermore there are procedures that support and maintain the unique identification of the TOE based on unique cryptographic keys for the protection of the online interface.

4.5.1 OSP in each PP configuration

247 All the OSP listed above apply to each of the PP configurations except the OSP.ApplicationSeparation which does not apply to PED-ONLY configuration.

4.6 Assumptions

248 **A.UserEducation**

249 It is assumed that Cardholders are informed by their issuing banks about a proper use and about their responsibilities when using the TOE. Especially Cardholders shall be asked to keep the PIN secret and not to hand their IC cards to other persons than a trustworthy merchant.

250 **A.SecureDevices**

251 It is assumed that the payment application providers have chosen appropriate security measures to protect devices interacting with the TOE e.g. the IC or Magnetic Stripe cards.

252 **A.PinAndCardManagement**

253 It is assumed that the user PINs as well as the IC Cards are securely managed by the Issuer. Especially it is assumed that the PIN as well as IC Card transfer between Issuer and Cardholder takes place in a manner that the confidentially of the PINs is ensured and the misuse of the cards is prevented by organisational measures.

4.6.1 Assumptions in each PP configuration

254 All the assumptions listed above apply to each of the PP configurations.

5 Security Objectives

5.1 Security Objectives for the TOE

255 **O.PINEntry**

256 The TOE shall provide the functionality to protect the confidentiality of the PIN during PIN entry (e.g. against manipulations of the Cardholder keypad, key presses being seen, key sounds being distinguished or key emanations being distinguished).

257 Upon failure during PIN Entry, if the failure triggers a tamper-responsive mechanism, the TOE shall erase any PIN value and related secret data. Otherwise, the TOE shall make them inaccessible.

258 **O.EncPIN**

259 The TOE shall protect the confidentiality of ENC_PIN until it is enciphered by tamper-responsive and tamper-detection means.

260 The TOE shall immediately delete ENC_PIN after having enciphered it.

261 The TOE shall neither display nor print any ENC_PIN in clear.

262 This objective entails the following derived objectives:

a) The TOE shall protect the confidentiality of ENC_PIN_SK.

b) The TOE shall provide state-of-the-art cryptography for cryptographic means.

263 Upon failure of any authenticity and integrity check or upon incorrect execution, if the failure triggers a tamper-responsive mechanism, the TOE erase any PIN value, ENC_PIN_SK and any other related secret data. Otherwise, the TOE shall make them inaccessible.

264 This objective applies to Online ENC_PIN as well as Offline ENC_PIN.

265 **O.CipherPPIN**

266 The TOE shall protect the confidentiality of Ciphertext PLAIN_PIN until it is enciphered by tamper-responsive and tamper-detection means.

267 The TOE shall immediately delete Ciphertext PLAIN_PIN after having enciphered it.

268 The TOE shall neither display nor print any Ciphertext PLAIN_PIN in clear.

269 This objective entails the following derived objectives:

a) The TOE shall protect the confidentiality of PLAIN_PIN_SK.

b) The TOE shall provide state-of-the-art cryptography for cryptographic means.

270 Upon failure of any authenticity and integrity check or upon incorrect execution, if the failure triggers a tamper-responsive mechanism, the TOE shall erase any PIN value, PLAIN_PIN_SK and any other related secret data. Otherwise, the TOE shall make them inaccessible.

271 *Application note: This objective applies to POI architectures with separated PED and IC Card Reader (e.g. different tamper-responsive boundaries).*

272 **O.ClearPPIN**

273 The TOE shall protect the confidentiality of Cleartext PLAIN_PIN until it is transferred to the IC Card Reader by tamper-responsive and tamper-detection means.

274 The TOE shall immediately delete Cleartext PLAIN_PIN after having transferred it.

275 The TOE shall neither display nor print any Cleartext PLAIN_PIN in clear.

276 Upon failure of any authenticity and integrity check or upon incorrect execution, if the failure triggers a tamper-responsive mechanism, the TOE shall erase any PIN value and related secret data. Otherwise, the TOE shall make them inaccessible.

277 *Application note: This objective applies to POI architectures with integrated PED and IC Card Reader (e.g. one tamper-responsive boundary).*

278 **O.CoreSWHW**

279 The TOE shall ensure the authenticity, the integrity and the correct execution of CORE_SW and CORE_HW (software and related hardware).

280 This objective entails the following derived objectives:

a) The TOE shall check the authenticity and integrity of CORE_SW and Core TSF cryptographic keys upon downloading of new components and updating of existing ones.

b) The TOE shall periodically check the authenticity and integrity of CORE_SW software.

c) The TOE shall periodically check the authenticity and integrity of CORE_ HW related hardware.

281 Upon failure of any authenticity and integrity check or upon incorrect execution, the TOE shall make inaccessible any PIN value, ENC_PIN_SK and any other related secret data.

282 **O.PEDMiddleSWHW**

283 The TOE shall ensure the authenticity, the integrity and the correct execution of PED_MIDDLE_SW and PED_MIDDLE_HW (software and related hardware).

284 This objective entails the following derived objectives:

a) The TOE shall check the authenticity and integrity of PED_MIDDLE_SW and PEDMiddle TSF cryptographic keys upon downloading of new components and updating of existing ones.

b) The TOE shall periodically check the authenticity and integrity of PED_MIDDLE_SW software.

c) The TOE shall periodically check the authenticity and integrity of the PED_MIDDLE_HW hardware.

285 Upon failure of any authenticity and integrity check or upon incorrect execution, the TOE will make inaccessible any PIN value, PED_MIDDLE_SK and any other related secret data.

286 **O.ICCardReader**

287 The TOE shall ensure that the TOE resists attempts to penetrate the POI to make any additions, substitutions, or modifications to the IC Card Reader hardware or software, in order to determine or modify PIN values.

288 **O.PaymentTransaction**

289 The TOE shall protect the authenticity and integrity of POI management and payment transaction data when processed by the TOE. The TOE shall protect the authenticity and integrity of POI management data when sent or received at the interfaces of the TOE. The TOE shall provide security services for protecting PAY_DAT from unauthorized modification and disclosure at the external interface to the Acquirer as well as between physically separated parts of the POI.

290 This objective entails the following derived objectives:

a) The TOE shall protect the confidentiality of POI_SK.

b) The TOE shall ensure the correct execution of POI_SW.

c) The POI calculating Message Authentication Codes (MACs) or Signatures shall be uniquely identifiable if the MAC and the signatures are calculated over software or data related to POI management or a payment transaction which are sent via the external interfaces of the TOE to an external communication party.

d) Any information about the payment transaction shall be displayed, printed or acoustic signalled in an authentic way (controlled by the payment application based on user data) without deceiving neither the Cardholder nor the attendant.

e) The TOE shall provide state-of-the-art cryptography for cryptographic means.

291 Upon failure of any authenticity and integrity check or upon incorrect execution, the TOE erase any Middle TSF secret data.

292 *Application note: Especially the TOE will protect cryptographic keys for Acquirer authentication and Terminal Management System authentication as well as cryptographic keys used to verify the authenticity and integrity of POI management data resp. payment transaction data transferred between TOE and Acquirer resp. TOE and Terminal Management System.*

293 **O.POISW**

294 The TOE shall ensure the authenticity, the integrity and the correct execution of POI_SW processing POI management and payment transaction data and Encrypted ENC_PIN (on-line authentication).

295 This objective entails the following derived objective:

a) The TOE shall check the authenticity and integrity of POI_SW and Middle TSF cryptographic keys upon downloading of new components and updating of existing ones.

296 Upon failure of any authenticity and integrity check the TOE will make inaccessible any Middle TSF secret data.

297 **O.PaymentApplicationDownload**

298 The TOE shall ensure the integrity and authenticity of the payment application during application download or update.

299 **O.POIApplicationSeparation (Application Separation)**

300 The TOE shall support the separation of payment applications from other applications. If applications are simultaneously processed, the security of the payment application shall not be impacted by any other application. Any POI management, payment transaction data, POI_SK, POI_PK owned by an application are only allowed to be accessed by another application if the other application has the necessary access rights.

301 This objective entails the following derived objective: the TOE shall ensure that no residual information remains in resources released by the payment application.

302 **O.PromptControl**

303 If the PED keypad can be used to enter non-PIN data, then prompts demanding for PIN entry at the PED display shall never lead to a PIN disclosure (e.g. by processing the entered PIN data in clear in unprotected areas). The authenticity and proper use of prompts shall be ensured and modification of the prompts or improper use of the prompts shall be prevented.

304 **O.MSR (TOE Protection of Magnetic Stripe Reader)**

305 The TOE shall ensure that the TOE resists attempts to penetrate the POI to make any additions, substitutions, or modifications to the Magnetic Stripe Read head and associated hardware or software, in order to determine or modify Magnetic Stripe data.

5.1.1 Security objectives for the TOE in each PP configuration

306 The table below defines the objectives applicable to each PP configuration.

Objective for the TOE	PED-ONLY				POI-COMPREHENSIVE				POI-OPTION			
	Core TSF	CoreTSF Keys	PEDMiddle TSF	Middle TSF	Core TSF	CoreTSF Keys	PEDMiddle TSF	Middle TSF	Core TSF	CoreTSF Keys	PEDMiddle TSF	Middle TSF
O.PINEntry	x				x				x			
O.EncPIN	x	x			x	x			x	x		
O.CipherPPIN	x	x			x	x						
O.ClearPPIN	x				x							
O.CoreSWHW	x	x			x	x			x	x		
O.PEDMiddleSWHW			x				x				x	
O.ICCardReader			x				x					
O.PaymentTransaction								x				x
O.POISW								x				x
O.PaymentApplicationDownload								x				x
O.POIApplicationSeparation								x				x
O.PromptControl			x				x				x	
O.MSR	MSR TSF				MSR TSF							

Table 8: Objectives for the TOE by PP configuration

5.2 Security Objectives for the Operational Environment

308 **OE.POISurvey**

309 Procedural measures like inspections and guidance will prevent manipulations of the TOE enclosure. Procedural measures like inspections and guidance for manipulations of the IC card interface will prevent attacks based on electronic circuits mounted at the IC card interface of the TOE's Card Reader. Those responsible for the TOE establish and implement procedures for training and vetting administrators of the TOE, or training the supervisors.

310 **OE.MerchantSurvey**

311 In case of a fraudulent Merchant performing attacks via manipulations of the enclosure or the interfaces of the TOE, especially the IC card interface, payment schemes will detect manipulations of a large number of payment transactions at the same merchant with their surveillance systems.

312 **OE.UserEducation**

313 The Cardholder shall be informed by his/her bank to keep the PIN secret.

314 **OE.SecureDevices**

315 The payment application providers have chosen appropriate security measures to protect devices interacting with the TOE e.g. the IC card.

316 **OE.KeyManagement**

317 Cryptographic keys are securely managed. Especially the generation and installation of cryptographic keys and certificates are done in a manner that private or secret cryptographic keys are protected against disclosure and all cryptographic keys are protected against modification when they are processed outside the POI. Furthermore there are procedures that support and maintain the unique identification of the TOE based on unique cryptographic keys for the protection of the online interface.

318 **OE.PinAndCardManagement**

319 User PINs as well as the IC Cards are securely managed by the Issuer. Especially the PIN as well as the IC Card transfer between Issuer and Cardholder takes place in a manner that the confidentially of the PINs is ensured and the misuse of the cards is prevented by organisational measures.

320 **OE.WellFormedPayApp Well-formed Payment Application**

321 Payment Applications implemented on the POI will make use of the security mechanisms provided by the TOE in a sense that the security of the defined assets as specified in this PP cannot be affected. The payment application is especially responsible for the transaction flow of a payment transaction (e.g. performing a payment transaction as result of verification of risk management parameter and other verification results like PIN verification).

322 **OE.LocalDevices**

323 The environment of the TOE shall protect the connection between Local Devices and other POI components via security organisational measures or by using the cryptographic means provided by the POI.

324 *Application note: Due to the broad spectrum of POI architectures, this PP does not require any specific protection mechanism to be used for the connection between local devices and the POI. Hence, the threats T.Transaction, T.MerchUsurp, T.CardholderUsurpCipherPPIN, T.CardholderUsurpClearPPIN, T.FundsAmount and T.BadDebt shall be partially countered in the environment of the TOE. Nevertheless, in those POI architectures where the POI mechanisms are used to protect the connection between Local Devices and other POI components, e.g. the TOE based hardware security mechanisms or cryptographic means, the ST author shall introduce an additional objective for the TOE, with the appropriate associated SFRs.*

5.2.1 Security objectives for the TOE environment by PP configurations

325 All the objectives for the TOE environment listed above apply to each of the PP configurations.

6 Rationale between SPD and security objectives

6.1 Threats

326 This section presents generic rationales between threats and objectives that are independent of the PP configurations.

327 **T.CardholderUsurpEPIN (Cardholder Identity Usurpation ENC_PIN)**

328 Capturing the ENC_PIN when it is entered and processed is countered by O.PINEntry, O.EncPIN and O.CoreSWHW (Authentic and integer usage of CORE_SW and CORE_HW).

329 With OE.UserEducation the user will be educated not to disclose the PIN. PIN disclosure by attacking communication (e.g. during CORE SW update) with the TOE or due to a bad key management are prevented by OE.SecureDevices and OE.KeyManagement.

330 The Security objective for the environment OE.PinAndCardManagement ensures that the Cardholder PIN is secured by organisational measures during transport between issuer and Cardholder.

331 Capturing the ENC_PIN by enclosure manipulation is countered by procedural measures like inspections and guidance due to OE.POISurvey.

332 OE.WellFormedPayApp enforces payment applications performing a payment transaction flow as required by the payment scheme.

333 **T.MerchUsurp (Merchant Identity Usurpation)**

334 Modifying another Merchant's TOE by enclosure manipulation is countered by procedural measures like inspections and guidance due to OE.POISurvey.

335 Furthermore OE.MerchantSurvey ensures that the payment schemes detects fraudulent merchants with their surveillance systems if a large number of manipulated payment transactions are presented by the same merchant.

336 Manipulation of another Merchant's TOE by attacks on the payment transaction data PAY_DAT is countered by O.PaymentTransaction (Authentic and integer payment transaction) and O.POISW (Authentic and integer usage of POI software).

337 Modifying the TOE by attacking devices communicating with the TOE/ TOE components or due to a bad key management is prevented by OE.SecureDevices, OE.LocalDevices (Connection Protection) and OE.KeyManagement.

338 OE.WellFormedPayApp enforces payment applications performing a payment transaction flow as required by the payment scheme.

339 **T.Transaction (Transaction with usurped Cardholder identity)** Manipulating the TOE by enclosure manipulation is countered by procedural measures like inspections and guidance due to OE.POISurvey.

340 Manipulating the TOE by attacks on the payment transaction data PAY_DAT is countered by O.PaymentTransaction (Authentic and integer payment transaction), O.POISW (Authentic and integer usage of POI software and related hardware) and O.POIApplicationSeparation (Application Separation).

341 Modifying the POI by attacking devices communicating with to the TOE or due to a bad key management is prevented by OE.SecureDevices, OE.LocalDevices (Connection Protection) and OE.KeyManagement.

342 The security objective for the TOE environment OE.MerchantSurvey supports the defence of fraudulent transactions.

343 OE.WellFormedPayApp enforces payment applications performing a payment transaction flow as required by the payment scheme.

344 **T.IllegalCodeInstall(Installation of illegal code coming from untrusted authority)**

345 Manipulating the TOE by attacks on the payment application authenticity and integrity is countered by the security objective O.PaymentApplicationDownload.

346 The protection of the Application loader itself is ensured by O.POISW.

347 **T.FundsAmount (Funds transfer other than correct amount)**

348 Manipulating the TOE by enclosure manipulation is countered by procedural measures like inspections and guidance due to OE.POISurvey.

349 Manipulating the TOE by attacks on the payment transaction data PAY_DAT is countered by O.PaymentTransaction (Authentic and integer payment transaction), O.POISW (Authentic and integer usage of POI software and related hardware) and O.POIApplicationSeparation (Application Separation).

350 Manipulating the POI by attacking devices communicating with to the TOE or due to a bad key management is prevented by OE.SecureDevices, OE.LocalDevices (Connection Protection) and OE.KeyManagement.

351 The security objective for the TOE environment OE.MerchantSurvey supports the defence of fraudulent transactions.

352 OE.WellFormedPayApp enforces payment applications performing a payment transaction flow as required by the payment scheme.

353 **T.BadDebt (Account overdraft, bad debt)**

354 Manipulation of the TOE in order that the TOE does not go online by enclosure manipulation is countered by procedural measures like inspections and guidance due to OE.POISurvey.

355 Manipulation of the TOE in order that the TOE does not go online is countered by O.PaymentTransaction (Authentic and integer payment transaction), O.POISW (Authentic and integer usage of POI software and related hardware) and O.POIApplicationSeparation (Application Separation).

356 TOE manipulation or the destruction of payment transaction data PAY_DAT or modification of payment transaction data PAY_DAT into refunds by attacking devices communicating with the TOE or due to a bad key management is prevented by OE.SecureDevices, OE.LocalDevices (Connection Protection) and OE.KeyManagement.

357 OE.WellFormedPayApp enforces payment applications performing a payment transaction flow as required by the payment scheme.

358 **T.SecureCommunicationLines**

359 Manipulation of the TOE enclosure is countered by procedural measures like inspections and guidance due to OE.POISurvey.

360 Manipulating the TOE in order to get personal information of the card holders during the processing of such data within the TOE is prevented by O.POISW (Authentic and integer usage of POI software and related hardware) and O.POIApplicationSeparation (Application Separation).

361 The disclosure of PAY_DAT via the online interfaces of the TOE is secured by O.PaymentTransaction (Authentic and integer payment transaction) protecting data against disclosure by cryptographic means.

362 TOE manipulation in order to spy out personal data by attacking devices communicating with the TOE or due to a bad key management is prevented by OE.SecureDevices, OE.LocalDevices (Connection Protection) and OE.KeyManagement.

363 OE.WellFormedPayApp enforces payment applications performing a payment transaction flow as required by the payment scheme.

364 **T.PromptControl**

365 Unauthorized manipulation of PED_MIDDLE_SW, which manages the prompts, is covered by O.PEDMiddleSWHW.

366 The separation of PIN and non-PIN data entered through the same keypad is ensured by the security objective O.PromptControl.

6.2 OSP

367 **OSP.WellFormedPayApp**

368 The security objective OE.WellFormedPayApp for the environment corresponds to the organisational security policy.

369 **OSP.POISurvey**

370 The security objective OE.POISurvey for the TOE environment corresponds directly to the organisational security policy.

371 **OSP.MerchantSurvey**

372 The security objective OE.MerchantSurvey for the environment of the TOE corresponds directly to this organisational security policy.

373 **OSP.KeyManagement**

374 The security objective OE.KeyManagement for the environment corresponds to the OSP.

375 **OSP.ApplicationSeparation**

376 The TOE security objectives O.POIApplicationSeparation directly implement the organisational security policy OSP.ApplicationSeparation.

6.3 Assumptions

377 **A.UserEducation**

378 The security objective OE.UserEducation for the environment corresponds to the assumption.

379 **A.SecureDevices**

380 The security objective OE.SecureDevices for the environment corresponds to the assumption.

381 **A.PinAndCardManagement**

382 The security objective OE.PinAndCardManagement reflects directly the assumption.

6.4 Rationale applicable to PED-ONLY configuration

383 This section provides the rationales applicable to the PED-ONLY configuration.

384 **T.PromptControl** cf. 6.1

385 **T.CardholderUsurpEPIN (Cardholder Identity Usurpation ENC_PIN)** cf 6.1

386 **T.CardholderUsurpCiphPPIN (Cardholder Identity Usurpation Encrypted PLAIN_PIN)**

387 Capturing the Ciphertext PLAIN_PIN when it is processed is countered by O.CipherPIN (Ciphertext PLAIN_PIN Processing), O.CoreSWHW, O.PEDMiddleSWHW (Authentic and integer usage of PEDMiddle TSF SW and related hardware) and O.ICCardReader.

388 With OE.UserEducation the user will be educated not to disclose the PIN. PIN disclosure by attacking devices communicating with to the TOE or due to a bad key management are prevented by OE.LocalDevices (Connection Protection), OE.SecureDevices and OE.KeyManagement.

389 The Security objective for the environment OE.PinAndCardManagement ensures that the Cardholder PIN is secured by organisational measures during transport between issuer and Cardholder.

390 Capturing the Ciphertext PLAIN_PIN by enclosure manipulation is countered by procedural measures like inspections and guidance due to OE.POISurvey.

391 OE.WellFormedPayApp enforces payment applications performing a payment transaction flow as required by the payment scheme.

392 **T.CardholderUsurpClearPPIN (Cardholder Identity Usurpation Plaintext PLAIN_PIN)**

393 Capturing the Cleartext PLAIN_PIN when it is entered and processed is countered by O.PINEntry, O.ClearPPIN (Cleartext PLAIN_PIN Processing) and O.CoreSWHW, O.PEDMiddleSWHW (Authentic and integer usage of PEDMiddle TSF SW and related hardware) and O.ICCardReader.

394 With OE.UserEducation the user will be educated not to disclose the PIN. PIN disclosure by attacking devices communicating with to the TOE or due to a bad key management are prevented by OE.LocalDevices (Connection Protection), OE.SecureDevices.

395 The Security objective for the environment OE.PinAndCardManagement ensures that the Cardholder PIN is secured by organisational measures during transport between issuer and Cardholder.

396 Capturing the Ciphertext PLAIN_PIN by enclosure manipulation is countered by procedural measures like inspections and guidance due to OE.POISurvey.

397 OE.WellFormedPayApp enforces payment applications performing a payment transaction flow as required by the payment scheme.

398 **T.Magstripe**

399 The security objective O.MSR corresponds to the threat.

400 Rationales for the following OSP are provided in section 6.2:

- OSP.WellFormedPayApp
- OSP.POISurvey
- OSP.MerchantSurvey
- OSP.KeyManagement

401 Rationales for the following assumptions are provided in section 6.3:

- A.UserEducation
- A.SecureDevices
- A.PinAndCardManagement

	T.MerchantUsurp	T.CardholderUsurpCiphPPIN	T.CardholderUsurpClearPPIN	T.CardholderUsurpEPIN	T.Transaction	T.FundsAmount	T.Prompt_Control	T.BadDebt	T.SecureCommunicationLines	T.Magstripe	T.IllegalCodeInstall	OSP.POI_Survey	OSP.MercahntSurvey	OSP.KeyManagement	OSP.WellFormedPayApp	A.UserEducation	A.SecureDevices	A.PinAndCardManagement
O.PINEntry			X	X														
O.EncPin				X														
O.CoreSWHW		X	X	X														
O.ClearPPIN			X															
O.CipherPPIN		X																
O.PEDMiddleSWHW		X	X				X											
O.PaymentTransaction																		
O.POISW																		
O.POIApplicationSeparation																		
O.PromptControl							X											
O.ICCardReader		X	X															
O.MSR										X								
OE.WellFormedPayApp		X	X	X											X			
OE.POISurvey		X	X	X								X						
OE.MerchantSurvey													X					
OE.UserEducation		X	X	X												X		
OE.SecureDevices		X	X	X													X	
OE.KeyManagement		X		X										X				
OE.PinAndCardManagent		X	X	X														X
OE.LocalDevices		X	X															

Table 9: SPD coverage by objectives in PED-ONLY configuration

6.5 Rationale applicable to POI-COMPREHENSIVE configuration

402 This section provides the rationales applicable to the POI-COMPREHENSIVE configuration.

403 Rationales for the following threats are provided in section 6.1:

- T.MerchUsurp (Merchant Identity Usurpation)
- T.PromptControl
- T.Transaction (Transaction with usurped Cardholder identity)
- T.FundsAmount (Funds transfer other than correct amount)
- T.BadDebt (Account overdraft, bad debt)
- T. SecureCommunicationLines
- T.IllegalCodeInstall
- T.CardholderUsurpEPIN (Cardholder Identity Usurpation ENC_PIN)

404 Rationales for the following threats are provided in section 6.4:

- T.CardholderUsurpCiphPPIN (Cardholder Identity Usurpation Encrypted PLAIN_PIN)
- T.CardholderUsurpClearPPIN (Cardholder Identity Usurpation Plaintext PLAIN_PIN)
- T.Magstripe

405 Rationales for the following OSP are provided in section 6.2:

- OSP.WellFormedPayApp
- OSP.POISurvey
- OSP.MerchantSurvey
- OSP.KeyManagement
- OSP.ApplicationSeparation

406 Rationales for the following assumptions are provided in section 6.3:

- A.UserEducation
- A.SecureDevices
- A.PinAndCardManagement

	T.MerchUsurp	T.CardholderUsurpCiphPPIN	T.CardholderUsurpClearPPIN	T.CardholderUsurpEPIN	T.Transaction	T.FundsAmount	T.PromptControl	T.BadDebt	T. SecureCommunicationLines	T.Magstripe	T.IllegalCodeInstall	OSP.ApplicationSeparation	OSP.POISurvey	OSP.MercahntSurvey	OSP.KeyManagement	OSP.WellFormedPayApp	A.UserEducation	A.SecureDevices	A.PinAndCardManagement
O.PINEntry			X	X															
O.EncPin				X															
O.CoreSWHW		X	X	X															
O.ClearPPIN			X																
O.CipherPPIN		X																	
O.PEDMiddleSWHW		X	X				X												
O.PaymentTransaction	X				X	X		X	X										
O.POISW	X				X	X		X	X		X								
O.PaymentApplicationDownload											X								
O.POIApplicationSeparation					X	X		X	X			X							
O.Prompt_Control							X												
O.ICCardReader		X	X																
O.MSR										X									
OE.WellFormedPayApp	X	X	X	X	X	X		X	X							X			
OE.POISurvey	X	X	X	X	X	X		X	X				X						
OE.MerchantSurvey	X				X	X								X					
OE.UserEducation		X	X	X													X		
OE.SecureDevices	X	X	X	X	X	X		X	X									X	
OE.KeyManagement	X	X		X	X	X		X	X						X				
OE.PinAndCardManagent		X	X	X															X
OE.LocalDevices	X	X	X		X	X		X	X										

Table 10: SPD coverage by objectives in POI-COMPREHENSIVE configuration

6.6 Rationale applicable to POI-OPTION configuration

407 This section provides the rationales applicable to the POI-OPTION configuration.

408 Rationales for the following threats are provided in section 6.1:

- T.CardholderUsurpEPIN (Cardholder Identity Usurpation ENC_PIN)
- T.MerchUsurp (Merchant Identity Usurpation)
- T.PromptControl
- T.Transaction (Transaction with usurped Cardholder identity)
- T.FundsAmount (Funds transfer other than correct amount)
- T.BadDebt (Account overdraft, bad debt)
- T. SecureCommunicationLines
- T.IllegalCodeInstall

409 Rationales for the following OSP are provided in section 6.2:

- OSP.WellFormedPayApp
- OSP.POISurvey
- OSP.MerchantSurvey
- OSP.KeyManagement
- OSP.ApplicationSeparation

410 Rationales for the following assumptions are provided in section 6.3:

- A.UserEducation
- A.SecureDevices
- A.PinAndCardManagement

	T.MerchUsurp	T.CardholderUsurpEPIN	T.CardholderUsurpClearPPIN	T.CardholderUsurpCipherPPIN	T.Transaction	T.FundsAmount	T.PromptControl	T.BadDebt	T. SecureCommunicationLines	T.Magstripe	T.IllegalCodeInstall	OSP.ApplicationSeparation	OSP.POISurvey	OSP.MercahntSurvey	OSP.KeyManagement	OSP.WellFormedPayApp	A.UserEducation	A.SecureDevices	A.PinAndCardManagement
O.PINEntry		X																	
O.EncPin		X																	
O.CoreSWHW		X																	
O.ClearPPIN																			
O.CipherPPIN																			
O.PEDMiddleSWHW							X												
O.PaymentTransaction	X				X	X		X	X										
O.POISW	X				X	X		X	X		X								
O.PaymentApplicationDownload											X								
O.POIApplicationSeparation					X	X		X	X			X							
O.PromptControl							X												
O.ICCardReader																			
O.MSR																			
OE.WellFormedPayApp	X	X			X	X		X	X							X			
OE.POISurvey	X	X			X	X		X	X				X						
OE.MerchantSurvey	X				X	X								X					
OE.UserEducation		X															X		
OE.SecureDevices	X	X			X	X		X	X									X	
OE.KeyManagement	X	X			X	X		X	X						X				
OE.PinAndCardManagent		X																	X
OE.LocalDevices	X				X	X		X	X										

Table 11: SPD coverage by objectives in POI-OPTION configuration

7 Extended Requirements

411 This PP extends CC Part 2 with the families of functional requirements FCS_RND, FIA_API and FPT_EMSEC and CC Part 3 with the family of assurance requirements AVA_POI.

7.1 Definition of the Family FCS_RND

412 To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

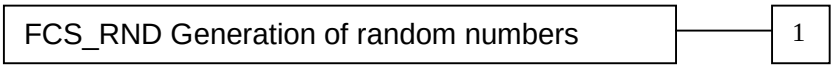
413 The family "Quality metric for random numbers (FCS_RND)" is specified as follows.

FCS_RND Quality metric for random numbers

Family behavior

414 This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

Component levelling:



415 FCS_RND.1 Generation of random numbers, requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

416 There are no management activities foreseen.

Audit: FCS_RND.1

417 There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

7.2 Definition of the Family FIA_API

418 To describe the IT security functional requirements of the TOE, an additional family (FIA_API) of the class FIA (Identification and Authentication) is defined here. This family describes the functional requirements for the proof of a claimed identity for the authentication verification by an external entity where the other families of the class FIA address the verification of the identity of an external entity.

419 The family "Authentication Proof of Identity (FIA_API)" is specified as follows.

FIA_API Authentication Proof of Identity

Family behaviour

420 This family defines functions provided by the TOE to prove its identity and to be verified by an external entity in the TOE IT environment.

Component levelling:

FIA_API Authentication Proof of Identity	1

421 FIA_API.1 Authentication Proof of Identity.

Management: FIA_API.1

422 The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

423 There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorised user or role*].

7.3 Definition of the Family FPT_EMSEC

424 The additional family FPT_EMSEC (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data when the attack is based on external observable physical phenomena of the TOE. This family describes the func-

tional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2.

425 The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

FPT_EMSEC TOE Emanation

Family behaviour:

426 This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMSEC TOE Emanation	1

427 FPT_EMSEC.1 TOE emanation

Management: FPT_EMSEC.1

428 There are no management activities foreseen.

Audit: FPT_EMSEC.1

429 There are no actions defined to be auditable.

FPT_EMSEC.1 TOE emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMSEC.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: specified limits] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

7.4 Definition of the Family AVA_POI

430 The family "Vulnerability analysis of POI (AVA_POI)" defines requirements for evaluator independent vulnerability search and penetration testing of POI.

431 The main characteristics of the new family, compared to AVA_VAN, are the following:

- The scope of the requirements in AVA_POI can be either the whole POI (the TOE) or a consistent set of POI components. Indeed, the AVA_VAN approach that ad-

dresses the TOE as a whole is not suitable for products with heterogeneous security levels.

- It introduces the POI-specific attack potential scale with four levels, namely POI-Basic, POI-Low, POI-Moderate and POI-High, defined in [POI AttackPot]. This document provides the POI attack potential calculation table, the attack potential range (with minimum and maximum values) for each of the four levels and a catalogue of POI-specific attack methods. A minimum time attack criterion exists. The generic AVA_VAN attack potential calculation table defined in CEM and the resulting scale do not meet the POI specificities.
- AVA_POI has dependencies on ADV_FSP, ADV_TDS and AGD. AVA_POI allows to require (partial) implementation representation. The aim is not to evaluate the implementation representation but to use it to make penetration testing more efficient and more effective. The mapping shall allow the evaluator to easily find pieces of hardware drawings and source code that implement the security functionality. In comparison, the evaluation of the TOE implementation representation is required from AVA_VAN.3.
- AVA_POI does not mandate any particular independent vulnerabilities analysis method for the evaluator.

432 As usual, the ST author is allowed to refine AVA_POI if needed, in accordance with [CC1].

433 The actual set of AVA_POI requirements shall cover the whole TOE under evaluation, i.e. all the POI components that contribute to the TSF being evaluated. A mapping between the SFR and the implementation representation shall be required to help the evaluator to understand the relation between the POI components and the TSF parts under evaluation and gain confidence that the set of POI components are well-defined.

434 The family “Vulnerability analysis of POI (AVA_POI)” is defined as follows. Underlined text stands for additions with respect to AVA_VAN.2, thus allowing easy traceability. Bold text shows the differences between two consecutive requirements in the family.

435 We refer to Section 12 for a detailed explanation of the relationship between AVA_VAN.2 and AVA_POI.

436 **AVA_POI Vulnerability analysis of POI**

Objectives

437 POI vulnerability analysis is an assessment to determine whether potential vulnerabilities identified in the POI could allow attackers to violate the SFRs and thus to perform unauthorized access or modification to data or functionality.

438 The vulnerabilities may arise either during the evaluation of the development, manufacturing or assembling environments, during the evaluation of the POI specifications and guidance, during anticipated operation of the POI components or by other methods, for instance statistical methods.

439 Each of the security requirements of the new family AVA_POI applies either to the whole TOE (POI) under evaluation or to a well-defined set of TOE components selected by the developer. A set of POI components can be the target of a requirement provided it defines the physical and logical boundary of a TSF portion, closed by SFR dependencies. Hence, the vulnerabilities identified on a set of POI components could compromise one or more of the SFRs within its boundary.

440 A developer may select different AVA_POI requirements for different sets of POI components. If a POI component is referred to in two or more AVA_POI requirements then the more demanding requirement applies.

441 The search of vulnerabilities and the quotation of the attack methods used in penetration testing shall conform to evaluation guidance in [POI CEM].

Component Levelling

442 Levelling is based on increased levels of attack potential required by an attacker to identify and exploit the potential vulnerabilities.

AVA_POI.1 Basic POI vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.1 Basic design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Objectives

443 A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.

444 The evaluator performs penetration testing on the POI or POI components, to confirm that the potential vulnerabilities cannot be exploited in the operational environment of the POI. Penetration testing is performed by the evaluator assuming an attack potential of POI-Basic.

Developer action elements:

AVA_POI.1.1D The developer shall provide the [selection: POI, [assignment: list of POI components]] for testing.

AVA_POI.1.2D The developer shall provide the implementation representation and a mapping of SFRs to the implementation representation of [selection: POI, [assignment: list of POI components among those in the scope of this requirement], none].

Content and presentation elements:

AVA_POI.1.1C The [selection: POI, [assignment: list of POI components]] shall be suitable for testing.

Evaluator action elements:

AVA_POI.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_POI.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the [selection: POI, [assignment: list of POI components]].

AVA_POI.1.3E The evaluator shall perform an independent vulnerability analysis of the [selection: POI, [assignment: list of POI components]] using the guidance documentation, the functional specification, the design, the security architecture description [selection: as well as the implementation representation and the mapping of SFRs to the implementation representation, none] to identify potential vulnerabilities.

AVA_POI.1.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the [selection: POI, [assignment: list of POI components]] is resistant to attacks performed by an attacker possessing **POI-Basic** attack potential.

AVA_POI.2 Low POI vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.1 Basic design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Objectives

445 A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.

446 The evaluator performs penetration testing on the POI or POI components, to confirm that the potential vulnerabilities cannot be exploited in the operational environment of the POI. Penetration testing is performed by the evaluator assuming an attack potential of POI-Low.

Developer action elements:

AVA_POI.2.1D The developer shall provide the [selection: POI, [assignment: list of POI components]] for testing.

AVA_POI.2.2D The developer shall provide the implementation representation and a mapping of SFRs to the implementation representation of [selection: POI, [assignment: list of POI components among those in the scope of this requirement], none].

Content and presentation elements:

AVA_POI.2.1C The [selection: POI, [assignment: list of POI components]] shall be suitable for testing.

Evaluator action elements:

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

AVA_POI.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the [selection: POI, [assignment: list of POI components]].

AVA_POI.2.3E The evaluator shall perform an independent vulnerability analysis of the [selection: POI, [assignment: list of POI components]] using the guidance documentation, the functional specification, the design, the security architecture description [selection: as well as the implementation representation and the mapping of SFRs to the implementation representation, none] to identify potential vulnerabilities.

AVA_POI.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the [selection: POI, [assignment: list of POI components]] is resistant to attacks performed by an attacker possessing **POI-Low** attack potential.

AVA_POI.3 Moderate POI Vulnerability Analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enfocring functional specification

ADV_TDS.1 Basic design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Objectives

447 A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.

448 The evaluator performs penetration testing on the POI or POI components, to confirm that the potential vulnerabilities cannot be exploited in the operational environment of the POI. Penetration testing is performed by the evaluator assuming an attack potential of POI-Moderate.

Developer action elements:

AVA_POI.3.1D The developer shall provide the [selection: POI, [assignment: list of POI components]] for testing.

AVA_POI.3.2D The developer shall provide the implementation representation and a mapping of SFRs to the implementation representation of [selection: POI, [assignment: list of POI components among those in the scope of this requirement], none].

Content and presentation elements:

AVA_POI.3.1C The [selection: POI, [assignment: list of POI components]] shall be suitable for testing.

Evaluator action elements:

AVA_POI.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_POI.3.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the [selection: POI, [assignment: list of POI components]].

AVA_POI.3.3E The evaluator shall perform an independent vulnerability analysis of the [selection: POI, [assignment: list of POI components]] using the guidance documentation, the functional specification, the design, the security architecture description [selection: as well as

the implementation representation and the mapping of SFRs to the implementation representation, none] to identify potential vulnerabilities.

AVA_POI.3.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the [selection: POI, [assignment: list of POI components]] is resistant to attacks performed by an attacker possessing **POI-Moderate** attack potential.

AVA_POI.4 High POI Vulnerability Analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.1 Basic design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Objectives

449 A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.

450 The evaluator performs penetration testing on the POI or POI components, to confirm that the potential vulnerabilities cannot be exploited in the operational environment of the POI. Penetration testing is performed by the evaluator assuming an attack potential of POI-High.

Developer action elements:

AVA_POI.4.1D The developer shall provide the [selection: POI, [assignment: list of POI components]] for testing.

AVA_POI.4.2D The developer shall provide the implementation representation and a mapping of SFRs to the implementation representation of [selection: POI, [assignment: list of POI components among those in the scope of this requirement], none].

Content and presentation elements:

AVA_POI.4.1C The [selection: POI, [assignment: list of POI components]] shall be suitable for testing.

Evaluator action elements:

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

AVA_POI.4.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the [selection: POI, [assignment: list of POI components]].

AVA_POI.4.3E The evaluator shall perform an independent vulnerability analysis of the [selection: POI, [assignment: list of POI components]] using the guidance documentation, the functional specification, the design, the security architecture description [selection: as well as the implementation representation and the mapping of SFRs to the implementation representation, none] to identify potential vulnerabilities.

AVA_POI.4.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the [selection: POI, [assignment: list of POI components]] is resistant to attacks performed by an attacker possessing **POI-High** attack potential.

8 Security Requirements

8.1 Security Functional Requirements

451 This Protection Profile defines the following packages of SFRs that fulfil one or more objectives for the TOE in each PP configuration:

- PIN Entry Package
- ENC_PIN Package
- PLAIN_PIN Package
- IC Card Reader Package
- POI_DATA Package
- CoreTSF Package
- PEDMiddleTSF Package
- MiddleTSF Package
- PED Prompt Control Package
- Cryptography Package
- Physical Protection Package

452 The main SFR of these packages are mapped to the CAS requirements they implement, either in the text of the SFR or in application notes, or both: CAS requirements that come directly from PCI POS PED 2.0 are referenced with the “PCI” identifier; otherwise, the identifier “CAS” is used. Annex 11.1 recalls the full set of CAS requirements and Annex 11.2 presents the mapping of CAS requirements to SFR in this Protection Profile.

453 Some of PCI A.x and PCI D.x security requirements have been identified not to be security functional ones. These security requirements are introduced as refinements of ADV_ARC (see section 8.2.1.1)

454 In the packages, Security Function Policies (SFP) are described. Each SFP is associated to one package. Cryptography and Physical Protection Packages do not have an associated policy. The definition of the different entities part of the SFPs has been determined in the following manner:

- Subjects are SPD subjects (section 4.3) or SPD users (section 4.2)
- Objects or information are assets (section 4.1)
- Security attributes are assets or subjects properties
- Roles are SPD users (section 4.2)
- Operations are the operations used in CAS requirements

Policy	Entity	Name	Value (for security attributes)	Definition
PIN_ENTRY Information flow control SFP	Subject	Cardholder		4.2.1
		PED keypad		4.3
	Information	PIN		4.1
		non-PIN data		any data that can be entered in the POI via the keypad which is not the PIN
	Operation	PIN entry		PIN digits capture on keypad
		non-PIN data entry		non-PIN digits capture on keypad
ENC_PIN Information Flow Control Policy	Subject	PED		4.3
		IC Card Reader		4.3
	Information	ENC_PIN		4.1
		ENC_PIN_SK		4.1
	Attribute	encrypted (ENC_PIN)	online	4.1
		encrypted (ENC_PIN)	offline	4.1
		validity (ENC_PIN_SK)	boolean	based on expiration time
		purpose (ENC_PIN_SK)	encryption (key, PIN, data) or authentication	key usage: encryption or authentication
	Role	Terminal Management System		4.2.2
		Terminal Administrator		4.2.1
		Risk Manager		4.2.2
	Operation	send		data transfer
PLAIN_PIN Information Flow Control Policy	Subject	PED		4.3
		IC Card Reader		4.3
	Information	PLAIN_PIN		4.1
		PLAIN_PIN_SK		4.1
	Attribute	validity (PLAIN_PIN_SK)	boolean	based on expiration time
		purpose (PLAIN_PIN_SK)	encryption (key, PIN, data) or authentication	key usage: encryption or authentication
	Role	Terminal Management System		4.2.2
		Terminal Administrator		4.2.1
	Operation	send		data transfer
ICCardReader Information Flow Control Policy	Subject	IC Card Reader		4.3
	Information	PLAIN_PIN		4.1

Policy	Entity	Name	Value (for security attributes)	Definition
		PLAIN_PIN_SK		4.1
	Role	Terminal Management System		4.2.2
		Terminal Administrator		4.2.1
	Operation	receive		data reception
POI_DATA Access Control Policy	Subject	POI and its Payment Application Logic		4.3
	Object	Payment Transaction Data		4.1
		POI Management Data		4.1
		POI_SK		4.1
		Cardholder communication interface		display, beeper, printer: any communication interface from the POI or from an external IT entity controlled by the POI communicating to the Cardholder
	Attribute	validity (POI_SK)	boolean	based on expiration time
		purpose (POI_SK)	encryption (key, PIN, data) or authentication	key usage: encryption or authentication
		access right (MAN_DAT, PAY_DAT	boolean	right to access POI Management Data or Payment Transaction Data
		authenticity (MAN_DAT, PAY_DAT)	boolean	authenticity of POI Management Data or Payment Transaction Data
	Role	Acquirer System		4.2.2
	Operation	send		data transfer
		receive		data reception
		access		interface access
CoreTSFLoader Access Control Policy	Subject	Core Loader		4.3
	Object	CORE_SW		4.1
	Operation	download		data or software download
PEDMiddleTSFLoader Access Control Policy	Subject	PED Middle Loader		4.3
	Object	PED_MIDDLE_SW		4.1
	Operation	download		data transfer
ApplicationLoader Access Control Policy	Subject	Payment Application Loader		4.3
	Object	PAYMENT_APP		4.1
	Operation	download		data transfer
MiddleTSFLoader Access Control Policy	Subject	Middle Loader		4.3
	Object	POI_SW		4.1
	Operation	download		data transfer

Policy	Entity	Name	Value (for security attributes)	Definition
PEDPromptControl Access Control Policy	Subject	POI components		2.2.1.4
	Object	PED Display		4.3
		PED Keypad		4.3
		Prompts		cf Glossary
		PIN		4.1
		PED_MIDDLE_PK		4.1
		PED_MIDDLE_SK		4.1
	Operation	entry		digits capture on keypad
		display		data display on screen
	Attribute	usage (PED Display)	PIN display	PED Display usage stands for displaying PIN data
			non-PIN display	PED Display usage stands for displaying non-PIN data
		usage (PED Keypad)	PIN entry	PED Keypad usage stands for entering PIN data
			non-PIN entry	PED Keypad usage stands for entering non-PIN data

Table 12: Entities definition in Security Function Policies

8.1.1 Definition of SFR packages

8.1.1.1 PIN Entry Package

FDP_IFC.1/PIN_ENTRY Subset information flow control

Dependencies: FDP_IFF.1 Subset information flow control not satisfied but justified: there is no rule to specify for PIN_ENTRY SFP in FDP_IFF.1 apart from the one already in FDP_ITC.1/PIN_ENTRY.

FDP_IFC.1.1/PIN_Entry The TSF shall enforce the **PIN ENTRY Information Flow Control SFP** on

- **subjects: Cardholder, PED keypad**
- **information: PIN, non-PIN data**
- **operations: PIN entry, non-PIN data entry**.

FDP_ITC.1/PIN_ENTRY Import of user data without security attributes

Dependencies: FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control; FMT_MSA.3 Static attribute initialisation not satisfied, but justified: The PIN verification value is not stored in the TOE but at the Issuer or in the IC Card inserted in the TOE. Therefore neither access control, nor information flow control, no static attribute initialisation is required.

FDP_ITC.1.1/PIN_ENTRY The TSF shall enforce the **PIN ENTRY Information Flow Control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/PIN_ENTRY The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **PCI B15: PIN is only allowed to be entered at the PED keypad assigned to CoreTSF. The entry of any other data must be separate from the PIN entry process avoiding accidental display of PIN at the PED display. If any other data and PIN are entered at the same keypad, the data entry and the PIN entry shall be clearly separate operations.**
- **[assignment: additional control rules]**.

Application note:

- *If the author of the ST has no additional rules fill it with none.*

FPT_EMSEC.1/PIN_ENTRY	**TOE Emanation**

Dependencies: No dependencies.

FPT_EMSEC.1.1/PIN_ENTRY The TOE shall not emit

- **PCI A5: audible tones during PIN entry, that, if used, could allow to distinguish the entered PIN digits,**
- **PCI A6: sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring,**
- **PCI B5: the entered PIN digits at the display (any array related to PIN entry displays only non-significant symbols, i.e. asterisks)**

in excess of **none** enabling access **to entered and internally transmitted PIN digit** and **none.**

FPT_EMSEC.1.2/PIN_ENTRY The TSF shall ensure **that users** are unable to use the following interface

- **PCI A5: audible tones, if used,**
- **PCI A6: sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring,**
- **PCI B5: the entered PIN digits at the display (any array related to PIN entry displays only non-significant symbols, i.e., asterisks)**

to gain access **to entered and internally transmitted PIN digit** and **none.**

FIA_UAU.2/PIN_ENTRY User authentication before any action

Dependencies: FIA_UID.1 Timing of identification, satisfied by FIA_UID.1/PIN_ENTRY

FIA_UAU.2.1/PIN_ENTRY The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement:

The TSF shall require each user to be successfully authenticated before allowing **access to sensitive services** on behalf of that user.

Application note:

- *Access to sensitive services shall be either via dual control or resulting in the device being unable to use previously existing key data.*
- *PCI B7: Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys*

or PINs. Entering or existing sensitive services shall not reveal or otherwise affect sensitive information.

FIA_UID.1/PIN_ENTRY Timing of identification

Dependencies: No dependencies.

FIA_UID.1.1/PIN_ENTRY The TSF shall allow **access to non sensitive services** on behalf of the user to be performed before the user is identified.

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

FTA_SSL.3/PIN_ENTRY TSF-initiated termination

Dependencies: No dependencies.

FTA_SSL.3.1/PIN_ENTRY The TSF shall terminate an interactive session after a **limited number of actions that can be performed and after an imposed time limit after which the PED is forced to return to its normal mode.**

Application note:

- *PCI B8: To minimize the risks from unauthorized use of sensitive services, limits on the number of actions that can be performed and a time limit shall be imposed, after which the PED is forced to return to its normal mode.*

8.1.1.2 ENC_PIN Package

FDP_IFC.1/ENC_PIN Subset information flow control

Dependencies: FDP_IFF.1 Subset information flow control satisfied by FDP_IFF.1/ENC_PIN

FDP_IFC.1.1/ENC_PIN The TSF shall enforce the **ENC_PIN Information Flow Control SFP** on

- **subjects: PED, IC Card Reader**
- **information: ENC_PIN, ENC_PIN_SK**
- **operations: send**.

FDP_IFF.1/ENC_PIN Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control,
FMT_MSA.3 Static attribute initialisation
satisfied by FDP_IFC.1/ENC_PIN, FMT_MSA.3/ENC_PIN

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

- **subjects: PED, IC Card Reader**
- **information: ENC_PIN, ENC_PIN_SK**
- **status of ENC_PIN: online encrypted, offline encrypted**
- **status of ENC_PIN_SK: validity, purpose [assignment: other ENC_PIN_SK security attributes].**

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

- **The PED sends the ENC_PIN in encrypted form to the IC Card Reader (offline) or to the Acquirer (online).**
- **PCI B6, CAS B6.a: The PED enciphers ENC_PIN with the appropriate dedicated online or offline encryption key immediately after ENC_PIN entry is complete and has been signified as such by the Cardholder.**
- **PCI D4.1: If the PED and IC Card Reader are not integrated into the same tamper-responsive boundary, and the Cardholder verification method (i.e., the IC Card requires) is determined to be Enciphered PIN, then the PIN block shall be enciphered between the PED and the IC Card Reader using either an authenticated encipherment key or the IC Card, or in accordance with ISO 9564.**
- **PCI D4.3: If the PED and the IC Card Reader are integrated in the same tamper-responsive boundary and the Cardholder verification method is determined to be an Enciphered PIN, then the PIN block shall be enciphered using an authenticated encipherment key of the IC Card.**
- **PCI B10, CAS B10.a: The PED uses cryptographic means to prevent the use of the PED for exhaustive PIN determination.**

FDP_IFF.1.3/ENC_PIN The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

FDP_IFF.1.4/ENC_PIN 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/ENC_PIN The TSF shall explicitly deny an information flow based on the following rules:

- **The PED does not send ENC_PIN or ENC_PIN_SK before being encrypted to any other subject outside CoreTSF**.
- **PCI B13: It is not possible to encrypt or decrypt any arbitrary data using any PIN encrypting key or key encrypting key contained in the PED. The PED must enforce that data keys, key encipherment keys, and PIN encryption keys have different values.**
- **PCI B14: There is no mechanism in the PED that would allow the outputting of a private or secret cleartext key or cleartext PIN, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a cleartext key from a component of high security into a component of lesser security.**

Application note:

- *If the author of the ST has no additional information flow control SFP rules ore rules based on security attributes these parts shall be filled with none.*
- *Validity and purpose are security attributes which are only implicitly used in the rules.*
- *PCI B10, CAS B10.a: The intended meaning of "prevent" is to stop an attack; examples (not exhaustive) are the use of unique key per transaction, or the use of ISO PIN block format 1 (random included). By contrast, slowing down an attack is considered as a 'deterrent' that does not meet this requirement.*
- *This SFR forces the immediate encipherment of ENC_PIN. The enciphering must be unique to the transaction, e.g. it is not allowed to produce the same enciphered form for a PIN in different transactions to avoid recognition of PIN values. Additionally, ENC_PIN is only allowed to be enciphered with cryptographic keys only used for PIN encipherment and not used for any other purpose. The SFR enforces that any ENC_PIN_SK is different from any other cryptographic key. However accidental choice of the same value is allowed.*

FMT_MSA.3/ENC_PIN Static attribute initialisation

Dependencies: FMT_MSA.1 Management of security attributes,
FMT_SMR.1 Security roles
satisfied by FMT_MSA.1/ENC_PIN, FMT_SMR.1/ENC_PIN

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

Editorial Refinement:
The TSF shall enforce the **ENC_PIN Information Flow Control SFP** to provide **permissive** default values for **ENC_PIN_SK** security attributes and **restrictive** default values for **ENC_PIN** security attributes, used to enforce the SFP.

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

Editorial Refinement:
The TSF shall allow the **[selection: Terminal Management System and/or POI]** to specify alternative initial values to override the default values of the **ENC_PIN_SK**'s security attributes when an object or information is created. The TSF shall allow **no role** to specify alternative initial values to override the default values of **ENC_PIN** when an object or information is created.

Application note:

- *Subjects or information like ENC_PIN_SK controlled by rules in the SFRs may possess certain attributes that contain information that is used by the TOE for its correct operation. Security attributes may exist specifically for the enforcement of the SFRs. Static attribute initialisation ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. Permissive means that information like ENC_PIN_SK shall explicitly be allowed to be used for a specific cryptographic operation like encryption of PIN, encryption of PIN encrypting keys, etc.*

FMT_MSA.1/ENC_PIN Management of security attributes

Dependencies: FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control satisfied by FDP_IFC.1/ENC_PIN
FMT_SMR.1 Security roles satisfied by FMT_SMR.1/ENC_PIN
FMT_SMF.1 Specification of Management Functions not satisfied but justified. There is no need to specify additional management functions because modification of security attributes is sufficient.

FMT_MSA.1.1/ENC_PIN The TSF shall enforce the **ENC_PIN Information Flow Control SFP** to restrict the ability to **modify** the security attributes **of ENC_PIN resp. of ENC_PIN_SK** to **Risk Manager resp. [selection: Terminal Management System and/or Terminal Administrator]**.

Application note:

- *Status of ENC_PIN may be modified by the Risk Manager. Status of ENC_PIN_SK may be modified by Terminal Management System and/or Terminal Administrator.*

FMT_SMR.1/ENC_PIN Security roles

Dependencies: FIA_UID.1 Timing of identification satisfied by FIA_UID.1.1/ENC_PIN

FMT_SMR.1.1/ENC_PIN The TSF shall maintain the roles **[selection: Terminal Management System and/or Terminal Administrator] and Risk Manager**.

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

Application note:

- *Terminal Management System and/or Terminal Administrator is related to status of ENC_PIN_SK, Risk Manager is related to status of ENC_PIN.*

FIA_UID.1/ENC_PIN Entry Timing of identification

Dependencies: No dependencies.

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

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

Application note:

- *The timing of identification for actions is related to Terminal Management System and/or Terminal Administrator resp. Risk Manager.*

FDP_RIP.1/ENC_PIN Subset residual information protection

Dependencies: No dependencies.

FDP_RIP.1.1/ENC_PIN The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] the following objects: [assignment: sensitive objects with residual information].

Refinement:

FDP_RIP.1.1/ENC_PIN The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **ENC_PIN immediately after being encrypted, temporary cryptographic keys [assignment: sensitive objects with residual information]**.

Deallocation may occur upon completion of the transaction or if the PED has timed-out waiting from the Cardholder or merchant.

Application note:

- *PCI B6: Sensitive information shall not be present any longer or used more often than strictly necessary. Online PINs are encrypted within the PED immediately after PIN entry is complete and has been signified as such by the Cardholder. The PED must automatically clear its internal buffers when either: The transaction is completed, or the PED has timed-out waiting for the response from the Cardholder or merchant.*
- *If no other sensitive objects with residual information exist the assignment shall be filled with none.*

FDP_ITT.1/ENC_PIN Basic internal transfer protection

Dependencies: FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control satisfied by FDP_IFC.1/ENC_PIN

FDP_ITT.1.1 The TSF shall enforce the **[assignment: access control SFP(s) and/or information flow control SFP(s)]** to prevent the **[selection: disclosure, modification, loss of use]** of user data when it is transmitted between physically-separated parts of the TOE.

Refinement:

FDP_ITT.1.1/ENC_PIN The TSF shall enforce the **ENC_PIN Information Flow Control SFP** to prevent the **disclosure** of **ENC_PIN and ENC_PIN_SK [assignment: other secret information, like administration passwords]** when they are transmitted between physically-separated parts of the **CoreTSF and when they are processed by the CoreTSF.**

Application note:

- *The refinement replaces the SFR above, thus the SFR above shall not be considered by the author of the ST. This SFR requires that ENC_PIN and ENC_PIN_SK shall be protected when they are transmitted between physically-separated parts of the PED.*

FTP_TRP.1/ENC_PIN Trusted path

Dependencies: No dependencies.

FTP_TRP.1.1/ENC_PIN The TSF shall provide a communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **unauthorized ENC_PIN_SK replacement and ENC_PIN_SK misuse**.

FTP_TRP.1.2/ENC_PIN The TSF shall permit **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3/ENC_PIN The TSF shall require the use of the trusted path for **ENC_PIN_SK replacement and ENC_PIN_SK usage**.

Application Note:

- *PCI C1: If the PED can hold multiple PIN encryption keys and if the key to be used to encrypt the PIN can be externally selected, then the PED prohibits unauthorised key replacement and key misuse.*
- *If the PED does not hold multiple PIN encryption keys or if the key to be used to encrypt the PIN can not be externally selected, this requirement is not applicable, and is therefore considered to be satisfied.*
- *The term "externally selected" means: selected by an interface function to the PED component that performs the PIN encryption. Both human interfaces and command interfaces are considered, and both direct and indirect. External selection also includes interference with or manipulation of the data by which the PED selects the key to be used. Keys may be selected through the PED keypad, or commands sent from another device such as an electronic cash register. Any commands sent from another device must be cryptographically authenticated to protect against man-in-the-middle and replay attacks, this requirement is not applicable to devices that do not include command for external key selection, or cannot hold multiple key hierarchies related to PIN encryption. If an application can select keys from multiple key hierarchies, the PED must enforce authentication of commands used for external key selection. If the PED only allows an application to select keys from a single hierarchy, then command authentication is not required.*

8.1.1.3 PLAIN_PIN Package

FDP_IFC.1/PLAIN_PIN Subset information flow control

FDP_IFC.1.1/PLAIN_PIN The TSF shall enforce the **PLAIN_PIN Information Flow Control SFP** on

- **subjects: PED, IC Card Reader**
- **information: PLAIN_PIN, PLAIN_PIN_SK**
- **operations: send**.

Dependencies: FDP_IFF.1 Subset information flow control,
satisfied by FDP_IFF.1/PLAIN_PIN

FDP_IFF.1/PLAIN_PIN Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control,
FMT_MSA.3 Static attribute initialisation
satisfied by FDP_IFC.1/PLAIN_PIN, FMT_MSA.3/PLAIN_PIN

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

- **subjects: PED, IC Card Reader**

- **information: PLAIN_PIN, PLAIN_PIN_SK**
- **status of PLAIN_PIN_SK: validity, purpose [assignment: other PLAIN_PIN_SK security attributes]**

FDP_IFF.1.2/PLAIN_PIN The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[selection: PCI_D4.2, PCI_D4.4] where**

- **PCI D4.2 PED and IC Card Reader are not integrated into the one tamper-responsive boundary: If the Cardholder verification method is determined to be PLAIN_PIN, then the PIN shall be encrypted in accordance with ISO 9564 before transmission to the IC Card Reader. In this case PLAIN_PIN is Ciphertext PLAIN_PIN.,**
- **PCI D4.4 PED and IC Card Reader are integrated into one tamper-responsive boundary: If the Cardholder verification method is determined to be PLAIN_PIN, then encryption is not required if the PIN block is transmitted wholly through the tamper-responsive boundary. IC Card Reader gets PLAIN_PIN in clear. In this case PLAIN_PIN is Cleartext PLAIN_PIN**.

FDP_IFF.1.3/PLAIN_PIN The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.4/PLAIN_PIN 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/PLAIN_PIN The TSF shall explicitly deny an information flow based on the following rules:

- **The PED does not send Ciphertext PLAIN_PIN (encrypted or in cleartext) or Cleartext PLAIN_PIN to any other subject than the IC Card Reader.**
- **The PED does not send the Ciphertext PLAIN_PIN to any subject before being encrypted**.
- **The PED does not send PLAIN_PIN_SK (if any) before being encrypted to any other subject before being encrypted**.
- **PCI B14: There is no mechanism in the PED that would allow the outputting of a private or secret cleartext key or cleartext PIN, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a cleartext key from a component of high security into a component of lesser security.**

Application note:

- *If the author of the ST has no additional information flow control SFP rules ore rules based on security attributes these parts shall be filled with none.*
- *Ciphertext PLAIN_PIN holds in POI architectures with physically separated PED and IC Card Reader.*

- *Cleartext PLAIN_PIN holds in POI architectures with PED and IC Card Reader integrated in the same tamper-responsive boundary.*
- *Validity and purpose are security attributes which are only implicitly used in the rules.*
- *This SFR is related to transfer of PLAIN_PIN mandating the implementation of PCI D4.2 or PCI D4.4 depending on the chosen implementation.*

FDP_RIP.1/PLAIN_PIN Subset residual information protection

Dependencies: No dependencies.

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

Refinement

The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects:

- **[selection: Ciphertext PLAIN_PIN immediately after being encrypted, Cleartext PLAIN_PIN immediately after being sent to the IC Card Reader]**
- **temporary cryptographic keys,**
- **[assignment: sensitive objects with residual information]**.

Deallocation may occur upon completion of the transaction or if the PED has timed-out waiting from the Cardholder or merchant.

Application note:

- *PCI B6: Sensitive information shall not be present any longer or used more often than strictly necessary. Online PINs are encrypted within the PED immediately after PIN entry is complete and has been signified as such by the Cardholder. The PED must automatically clear its internal buffers when either: The transaction is completed, or the PED has timed-out waiting for the response from the Cardholder or merchant.*
- *If no other sensitive objects with residual information exist the assignment shall be filled with none.*

FDP_ITT.1/PLAIN_PIN Basic internal transfer protection

Dependencies: FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control satisfied by FDP_IFC.1/PLAIN_PIN

FDP_ITT.1.1/PLAIN_PIN The TSF shall enforce the **[assignment: access control SFP(s) and/or information flow control SFP(s)]** to prevent the **[selection: disclosure, modification, loss of use]** of user data when it is transmitted between physically-separated parts of the TOE.

Refinement:
The TSF shall enforce the **PLAIN_PIN Information Flow Control SFP** to prevent the **disclosure** of **[selection: Cleartext PLAIN_PIN, (Ciphertext PLAIN_PIN, PLAIN_PIN_SK)]** when they are transmitted between physically-separated parts of **PED or to the IC Card Reader.**

Application note:

- *The refinement replaces the SFR above, thus the SFR above shall not be considered by the author of the ST. This SFR requires that PLAIN_PIN and PLAIN_PIN_SK shall be protected when they are transmitted between physically-separated parts of the PED.*

FMT_MSA.3/PLAIN_PIN Static attribute initialisation

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles satisfied by FMT_MSA.1/ PLAIN_PIN, FMT_SMR.1/ PLAIN_PIN

FMT_MSA.3.1/PLAIN_PIN The TSF shall enforce the **PLAIN_PIN Information Flow Control SFP** to provide **permissive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/PLAIN_PIN The TSF shall allow the **[selection: Terminal Management System and/or Terminal Administrator]** to specify alternative initial values to override the default values when an object or information is created.

Application note:

- *This requirement concerns the security attributes of PLAIN_PIN_SK.*
- *Subjects or information like PLAIN_PIN_SK controlled by rules in the SFRs may possess certain attributes that contain information that is used by the TOE for its correct operation. Security attributes may exist specifically for the enforcement of the SFRs. Static attribute initialisation ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. Permissive means that information like PLAIN_PIN_SK shall explicitly be allowed to be used for a specific cryptographic operation like encryption of Ciphertext PLAIN_PIN.*

FMT_MSA.1/PLAIN_PIN Management of security attributes

Dependencies:
FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control satisfied by FDP_IFC.1/PLAIN_PIN
FMT_SMR.1 Security roles satisfied by FMT_SMR.1/PLAIN_PIN
FMT_SMF.1 Specification of Management Functions not satisfied but justified. There is no need to specify additional management functions because modification of security attributes is sufficient.

FMT_MSA.1.1/PLAIN_PIN The TSF shall enforce the **PLAIN_PIN Information Flow Control SFP** to restrict the ability to **modify** the security attributes **status of PLAIN_PIN_SK** to **[selection: Terminal Management System and/or Terminal Administrator].**

FMT_SMR.1/PLAIN_PIN Security roles

Dependencies: FIA_UID.1 Timing of identification satisfied by FIA_UID.1.1/PLAIN_PIN

FMT_SMR.1.1/PLAIN_PIN The TSF shall maintain the roles **[selection: Terminal Management System and/or Terminal Administrator]**.

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

FIA_UID.1/PLAIN_PIN Entry Timing of identification

Dependencies: No dependencies.

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

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

Application note:

- *The timing of identification for actions is related to Terminal Management System and/or Terminal Administrator.*

8.1.1.4 IC Card Reader Package

FDP_IFC.1/ICCardReader Subset information flow control

Dependencies: FDP_IFF.1 Subset information flow control, satisfied by FDP_IFF.1/IC Card Reader

FDP_IFC.1.1/ICCardReader The TSF shall enforce the **IC Card Reader Information Flow Control SFP** on

- **subjects: IC Card Reader**
- **information: PLAIN_PIN, PLAIN_PIN_SK**
- **operations: receive, send**.

FDP_IFF.1/ICCardReader Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control,
FMT_MSA.3 Static attribute initialisation
satisfied by FDP_IFC.1/ICCardReader, FMT_MSA.3/PLAIN_PIN

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

- **subjects: IC Card Reader**
- **information: PLAIN_PIN, PLAIN_PIN_SK**
- **status of PLAIN_PIN_SK: validity, purpose [assignment: other PLAIN_PIN_SK security attributes]**

FDP_IFF.1.2/ICCardReader The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[selection: PCI D4.2, PCI D4.4] where**

- **PCI D4.2 (PED and IC Card Reader are not integrated into the one tamper-responsive boundary): the IC Card Reader receives the Ciphertext PLAIN_PIN, deciphers it and sends it to the IC Card,**
- **PCI D4.4 (PED and IC Card Reader are integrated into one tamper-responsive boundary): the IC Card Reader receives the Cleartext PLAIN_PIN and sends it to the IC Card.**

FDP_IFF.1.3/ICCardReader The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

FDP_IFF.1.4/ICCardReader 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/ICCardReader The TSF shall explicitly deny an information flow based on the following rules:

- **The IC Card Reader does not send PLAIN_PIN (neither Ciphertext PLAIN_PIN nor Cleartext PLAIN_PIN) to any other entity than the IC Card. The IC Card Reader does not send PLAIN_PIN_SK (if any) to any entity.**
- **PCI B14: There is no mechanism in the PED that would allow the outputting of a private or secret cleartext key or cleartext PIN, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a cleartext key from a component of high security into a component of lesser security.**

Application note:

- *Ciphertext PLAIN_PIN holds in POI architectures with physically separated PED and IC Card Reader. Cleartext PLAIN_PIN holds in POI architectures with PED and IC Card Reader integrated in the same tamper-responsive boundary.*
- *If the author of the ST has no additional information flow control SFP rules ore rules based on security attributes these parts shall be filled with none.*
- *This SFR is related to transfer of PLAIN_PIN mandating the implementation of PCI D4.2 or PCI D4.4 depending on the chosen implementation. Both are repeated here (related to the PLAIN_PIN Package) because of the different attack potential.*

FDP_RIP.1/ICCardReader Subset residual information protection

Dependencies: No dependencies.

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

Refinement

The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects:

- **[selection: Ciphertext PLAIN_PIN immediately after being decrypted and sent to the IC Card, Cleartext PLAIN_PIN immediately after being sent to the IC Card]**
- **temporary cryptographic keys,**
- **[assignment: sensitive objects with residual information]**.

Deallocation may occur upon completion of the transaction or if the PED has timed-out waiting from the Cardholder or merchant.

Application note:

- *PCI B6: Sensitive information shall not be present any longer or used more often than strictly necessary. Online PINs are encrypted within the PED immediately after PIN entry is complete and has been signified as such by the Cardholder. The PED must automatically clear its internal buffers when either: The transaction is completed, or the PED has timed-out waiting for the response from the Cardholder or merchant.*
- *If no other sensitive objects with residual information exist the assignment shall be filled with none.*

FDP_ITT.1/ICCardReader Basic internal transfer protection

Dependencies: FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control satisfied by FDP_IFC.1/ICCardReader

FDP_ITT.1.1 The TSF shall enforce the **[assignment: access control SFP(s) and/or information flow control SFP(s)]** to prevent the **[selection: disclosure, modification, loss of use]** of user data when it is transmitted between physically-separated parts of the TOE.

Refinement:

FDP_ITT.1.1/ICCardReader The TSF shall enforce the **IC Card Reader Information Flow Control SFP** to prevent the **disclosure** of **[selection: Cleartext PLAIN_PIN, (Ciphertext PLAIN_PIN, PLAIN_PIN_SK)]** when they are transmitted **to the IC Card or when they are processed by the IC Card Reader.**

Application note:

- *The refinement replaces the SFR above, thus the SFR above shall not be considered by the author of the ST. This SFR requires that PLAIN_PIN and PLAIN_PIN_SK shall be protected when they are transmitted between physically-separated parts of the IC Card Reader.*

8.1.1.5 POI_DATA Package

FDP_ACC.1/POI_DATA Subset Access Control

Dependencies: FDP_ACF.1 Security attribute based access control,
satisfied by FDP_ACF.1/POI_DATA

FDP_ACC.1.1/POI_DATA The TSF shall enforce the **POI Management and Payment Transaction Data Access Control SFP** on

- **subjects: POI and its Payment Application Logic**
- **objects: Payment Transaction Data, POI Management Data, POI_SK, Cardholder communication interface, [assignment: list of payment application internal data]**
- **operations: send, receive, access.**

FDP_ACF.1/POI_DATA Security attribute based access control

Dependencies: FDP_ACC.1 Subset Access Control,
satisfied by FDP_ACC.1/POI_DATA, FMT_MSA.3 Static attribute initialisation not satisfied but justified: no management functions are required for POI_DATA.

FDP_ACF.1.1/POI_DATA The TSF shall enforce the **POI Management and Payment Transaction Data Access Control SFP** based on the following:

- **subjects: POI and its Payment Application Logic**
- **objects: Payment Transaction Data, POI Management Data, POI_SK, Cardholder communication interface, [assignment: list of payment application internal data]**

- **security attribute of POI_SK: purpose and validity**
- **security attribute of Payment Transaction Data, POI Management Data: access right of Payment Application and authenticity status**
- **[assignment: list of security attributes]**

FDP_ACF.1.2/POI_DATA The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **CAS G2.1: The security of payment application in the POI must not be impacted by any other application. Payment application isolation shall be ensured: no other application shall have unauthorized access to application data (Payment Transaction Data, POI Management Data, POI_SK).**
- **CAS G2.2: The security of payment application in the POI must not be impacted by any other application. Payment application isolation shall be ensured: it shall not be possible for another application to interfere with the execution of the payment application, by accessing internal data (such as state machine or internal variables).**
- **CAS G2.3: Payment application isolation shall be ensured: it shall not be possible for another application to deceive the Cardholder during execution of the payment application, by accessing Cardholder communication interface (e.g. display, beeper, printer) used by the payment application.**

FDP_ACF.1.3/POI_DATA The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **POI Management Data and Payment Transaction Data shall be accepted if the data are authentic.**
- **POI Management Data and Payment Transaction Data are allowed to be accessed if Payment Application has access right to the data.**
- **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].**

FDP_ACF.1.4/POI_DATA The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **POI Management Data and Payment Transaction Data shall not be accepted if the data are not authentic.**
- **The POI does not send POI_SK in cleartext to any external IT entity.**
- **[assignment: rules, based on security attributes, that explicitly deny information flows].**

Application note:

- *If the author of the ST has no additional information flow control SFP rules ore rules based on security attributes these parts shall be filled with none.*

FDP_ITT.1/POI_DATA Basic internal transfer protection

Dependencies: FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control satisfied by FDP_ACC.1/POI_DATA

FDP_ITT.1.1 The TSF shall enforce the **[assignment: access control SFP(s) and/or information flow control SFP(s)]** to prevent the **[selection: disclosure, modification, loss of use]** of user data when it is transmitted between physically-separated parts of the TOE.

Refinement:

FDP_ITT.1.1/POI_DATA The TSF shall enforce the **POI Management and Payment Transaction Data Access Control SFP** to prevent the **modification of POI Management Data and Payment Transaction Data and to prevent the disclosure of POI_SK** when it is transmitted between physically-separated parts of the TOE.

Application note:

- *CAS G1.2: Payment Transaction Data shall be handled with authenticity and integrity in the POI.*
- *CAS G1.3: POI Management Data must be protected against unauthorized change in the POI.*
- *CAS G4: Protection of POI_SK in a POI component against disclosure.*

FDP_UIT.1/MAN_DAT Data exchange integrity

Dependencies: FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control, FTP_ITC.1 Inter-TSF Trusted Channel or FTP_TRP.1 Trusted path satisfied by FDP_ACC.1/POI_DATA, FTP_ITC.1/POI_DATA

FDP_UIT.1.1 The TSF shall enforce the **[assignment: access control SFP(s) and/or information flow control SFP(s)]** to **[selection: transmit, receive]** user data in a manner protected from **[selection: modification, deletion, insertion, replay]** errors.

Refinement:

FDP_UIT.1.1/MAN_DAT The TSF shall enforce the **POI Management and Payment Transaction Data Access Control SFP to transmit and receive POI Management Data** in a manner protected from **modification** errors.

FDP_UIT.1.2/MAN_DAT The TSF shall be able to determine on receipt of user data, whether **modification** has occurred.

Application note:

- *The refinement replaces the SFR above, thus the SFR above shall not be considered by the author of the ST.*
- *CAS G1.3: POI Management Data must be provided to the POI in an authentic way and must be protected against unauthorized change.*

- *The POI shall protect in either case POI Management Data sent or received by the POI over external lines against modification by cryptographic mechanisms. Protection against modification includes protection of the authenticity of POI Management Data.*

FDP_UIT.1/PAY_DAT Data exchange integrity

Dependencies: FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control, FTP_ITC.1 Inter-TSF Trusted Channel or FTP_TRP.1 Trusted path satisfied by FDP_ACC.1/POI_DATA, FTP_ITC.1/POI_DATA

FDP_UIT.1.1 The TSF shall enforce the **[assignment: access control SFP(s) and/or information flow control SFP(s)]** to **[selection: transmit, receive]** user data in a manner protected from **[selection: modification, deletion, insertion, replay]** errors.

Refinement:

FDP_UIT.1.1/PAY_DAT The TSF shall enforce the **POI Management and Payment Transaction Data Access Control SFP to be able to transmit and receive Payment Transaction Data** in a manner protected from **modification** errors.

FDP_UIT.1.2/PAY_DAT The TSF shall be able to determine on receipt of user data, whether **modification** has occurred.

Application note:

- *The refinement replaces the SFR above, thus the SFR above shall not be considered by the author of the ST.*
- *CAS G1.1: POI must have the capacity to protect communications over external communication channels, meaning that POI Application Logic must provide cryptographic means: To protect all Payment Transaction Data sent or received by the POI against modification.*
- *The POI shall provide means to protect Payment Transaction Data sent or received by the POI over external lines against modification by cryptographic mechanisms. Whether the means are used or not is controlled by the payment application using that means.*
- *External means 'external to the POI'. Therefore, this requirement addresses communications with local devices (e.g. cash registers, pump controllers), communications with the Acquirer(s) and communications with the Terminal Management System. The object of evaluation for this requirement consists of the security functions that provide those cryptographic means. The security functions should not enforce protection of communications, but the cryptographic means must be available, would the external entity requires protection.*

FDP_UCT.1/POI_DATA Basic data exchange confidentiality

Dependencies: FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path
satisfied by FTP_ITC.1/POI_DATA
FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control
satisfied by FDP_ACC.1/POI_DATA

FDP_UCT.1.1: The TSF shall enforce the **[assignment: access control SFP(s) and/or information flow control SFP(s)]** to **[selection: transmit, receive]** user data in a manner protected from unauthorised disclosure.

Refinement:
FDP_UCT.1.1/POI_DATA The TSF shall enforce the **POI Management and Payment Transaction Data Access Control SFP to transmit and receive POI_SK and to be able to transmit and receive Payment Transaction Data** in a manner protected from unauthorised disclosure.

Application note:

- *The refinement replaces the SFR above, thus the SFR above shall not be considered by the author of the ST.*
- *CAS G1.1: POI must have the capacity to protect communications over external communication channels, meaning that POI Application Logic must provide cryptographic means: To protect all transaction data sent or received by the POI against disclosure.*
- *CAS G4: Protection of POI_SK in a POI component against disclosure.*
- *The POI shall provide means to protect Payment Transaction Data sent or received by the POI over external lines against disclosure by cryptographic mechanisms. Whether the means are used or not is controlled by the payment application using that means.*
- *External means 'external to the POI'. Therefore, this requirement addresses communications with local devices (e.g. cash registers, pump controllers), communications with the acquirer(s) and communications with the terminal manager. The object of evaluation for this requirement consists of the security functions that provide those cryptographic means. The security functions should not enforce protection of communications, but the cryptographic means must be available, would the external entity requires protection.*

FIA_API.1/POI_DATA Authentication Proof of Identity

Dependencies: No dependencies

FIA_API.1.1/POI_DATA The TSF shall provide a **[assignment: authentication mechanism]** to prove the identity of the **POI.**

Application note:

- *CAS G1.1: The POI shall provide means for authentication of its unique identifier by an external IT entity communicates with.*
- *For authentication, uniqueness is only required in a given context: the external entity should be able to distinguish one POI from another. As an example, use of unique key per POI guarantees that POI can be uniquely authenticated.*

FDP_RIP.1/POI_DATA Subset residual information protection

Dependencies: No dependencies.

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

Refinement:
The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **temporary cryptographic keys, [assignment: sensitive objects with residual information, temporary payment transaction data]**.
Deallocation may occur upon completion of the transaction or if the PED has timed-out waiting from the Cardholder or merchant.
Application note:

- *Contribution to CAS G2.1 to CAS G2.3.*
- *This SFR requires that sensitive information shall not be present any longer or user more often than strictly necessary. Buffers shall be cleared immediately after exporting any PIN, upon payment transaction is completed and when MiddleTSF components have time-out waiting for a response.*

FTP_ITC.1/POI_DATA Inter-TSF trusted channel

Dependencies: No dependencies.

FTP_ITC.1.1/POI_DATA The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/POI_DATA The TSF shall permit **[selection: the TSF, another trusted IT product]** to initiate communication via the trusted channel.

Refinement:
The TSF shall permit **Acquirer System** to initiate communication via the trusted channel.

FTP_ITC.1.3/POI_DATA The TSF shall initiate communication via the trusted channel for **transmitting and receiving Payment Transaction Data and POI_SK in a manner protected from unauthorized disclosure, [assignment: list of functions for which a trusted channel is required]**.

Application note:

- *The channel is used to protect the confidentiality of data.*
- *Contribution to CAS G1.1 and CAS G4.*

8.1.1.6 CoreTSF Package

FPT_TST.1/CoreTSF TSF testing

Dependencies: No dependencies.

FPT_TST.1.1/CoreTSF The TSF shall run a suite of self tests **at the conditions**

- **start-up**
- **at least once per day**

to demonstrate the correct operation of **the CoreTSF PED (CORE_SW and CORE_HW)**.

FPT_TST.1.2/CoreTSF The TSF shall provide authorised users with the capability to verify the integrity of **[selection: [assignment: parts of TSF], TSF data]**.

FPT_TST.1.3/CoreTSF The TSF shall provide authorised users with the capability to verify the integrity of **stored TSF executable code**.

Application note:

- *"TSF executable code" stands for CoreTSF software within the PED.*
- *PCI B1: The PED performs a self-test, which includes integrity and authenticity tests as addressed in B4, upon start up and at least once per day to check firmware; security mechanisms for signs of tampering; and whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fails in a secure manner.*
- *If no other parts of TSF exist the assignments shall be filled with none.*

FPT_FLS.1/CoreTSF Failure with preservation of secure state

Dependencies: No dependencies.

FPT_FLS.1.1/CoreTSF The TSF shall preserve a secure state when the following types of failures occur:

- **failure of CoreTSF self-test**
- **logical anomalies of CoreTSF**

- **[assignment: list of types of failures in CoreTSF]**.

Application note:

- *The "secure state" does not provide access to any PIN value, PIN encryption key or any other CoreTSF secret data.*
- *PCI B1: The PED performs a self-test, which includes integrity and authenticity tests as addressed in PCI B4, upon start up and at least once per day to check firmware; security mechanisms for signs of tampering; and whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fails in a secure manner.*
- *PCI B2: The PED's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the PED outputting the clear text PIN or other sensitive information.*
- *If no list of types exist the assignment shall be filled with none.*

FDP_ACC.1/CoreTSFLoader Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control not satisfied but justified: the correspondent access control is satisfied by FDP_ITC.1/CoreTSFLoader

FDP_ACC.1.1/CoreTSFLoader The TSF shall enforce the **Core Loader Access Control SFP** on

- **subject: Core Loader**
- **objects: CORE_SW, [assignment: list of data, in particular cryptographic keys, controlled under this policy]**
- **operation: download**.

Application note:

- *The "cryptographic keys" stand for PIN encryption keys (e.g. ENC_PIN_SK) or for any other key. The operations are any management operation on CoreTSF software and data.*
- *If no list of data exist the assignment shall be filled with "none".*

FDP_ITC.1/CoreTSFLoader Import of user data without security attributes

Dependencies:
FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control satisfied by FDP_ACC.1/CoreTSFLoader
FMT_MSA.3 Static attribute initialisation not satisfied but justified: there are no security attributes to be managed for downloading objects. Terminal Management System decides to update/download them or not.

FDP_ITC.1.1/CoreTSFLoader The TSF shall enforce the **Core Loader Access Control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/CoreTSFLoader The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **The Core Loader downloads only authentic and integer objects coming from the Terminal Management System.**
- **Downloading is an atomic operation. Either it succeeds or the TSF rollbacks to the previous state and all downloaded data is cleared or if the rollback is not possible all CoreTSF secret data are erased.**
- **PIN encryption keys are stored in the Security Module of PED or encrypted**.
- **[assignment: additional importation control rules]**

Application note:

- *PCI B2: The PED's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the PED outputting the clear text PIN or other sensitive information.*
- *PCI B4: If the PED allows updates of firmware, the device cryptographically authenticates the software integrity and if the authenticity is not confirmed, the software update is rejected and deleted.*
- *Update of software or data may be a consequence of the download operation. The assignment of additional importation control rules shall manage the download operations which have an update as a consequence.*

8.1.1.7 PEDMiddleTSF Package

FPT_TST.1/PEDMiddleTSF TSF testing

Dependencies: No dependencies.

FPT_TST.1.1/PEDMiddleTSF The TSF shall run a suite of self tests **at the conditions**

- **start-up**
- **at least once per day**

to demonstrate the correct operation of **the PEDMiddleTSF**.

FPT_TST.1.2/PEDMiddleTSF The TSF shall provide authorised users with the capability to verify the integrity of **[selection: [assignment: parts of TSF], TSF data]**.

FPT_TST.1.3/PEDMiddleTSF The TSF shall provide authorised users with the capability to verify the integrity of **stored TSF executable code**.

Application note:

- *"TSF executable code" stands for PEDMiddleTSF software within the PED and the IC Card Reader.*
- *PCI B1: The PED performs a self-test, which includes integrity and authenticity tests as addressed in PCI B4, upon start up and at least once per day to check firmware; security mechanisms for signs of tampering; and whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fails in a secure manner.*
- *If not other parts of TSF exist the assignments shall be filled with none.*

FPT_FLS.1/PEDMiddleTSF Failure with preservation of secure state

Dependencies: No dependencies.

FPT_FLS.1.1/PEDMiddleTSF The TSF shall preserve a secure state when the following types of failures occur:

- **failure of PEDMiddleTSF self-test**
- **logical anomalies of PEDMiddleTSF**
- **[assignment: list of types of failures in PEDMiddleTSF]**.

Application note:

- *The "secure state" does not provide access to any PIN value, PIN encryption key or any other PEDMiddleTSF secret data.*
- *PCI B1: The PED performs a self-test, which includes integrity and authenticity tests as addressed in PCI B4, upon start up and at least once per day to check firmware; security mechanisms for signs of tampering; and whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fails in a secure manner.*
- *PCI B2: The PED's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the PED outputting the clear text PIN or other sensitive information.*
- *If no list of types of failures exist the assignment shall be filled with none.*

FDP_ACC.1/PEDMiddleTSFLoader Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control not satisfied but justified: the correspondent access control is satisfied by FDP_ITC.1./PEDMiddleTSFLoader

FDP_ACC.1.1/PEDMiddleTSFLoader The TSF shall enforce the **PED Middle Loader Access Control SFP** on

- **subject: PED Middle Loader**
- **objects: PED_MIDDLE_SW, [assignment: list of data, in particular cryptographic keys, controlled under this policy]**
- **operation: download**.

Application note:

- *The "cryptographic keys" stand for PIN encryption keys (PLAIN_PIN_SK) or any other key. The operations are any management operation on PEDMiddleTSF software and data.*
- *If no list of data exist the assignment shall be filled with "none".*

FDP_ITC.1/PEDMiddleTSFLoader Import of user data without security attributes

Dependencies:
FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control satisfied by FDP_ACC.1/PEDMiddleTSFLoader
FMT_MSA.3 Static attribute initialisation not satisfied but justified: there are no security attributes to be managed for downloading objects. Terminal Management System decides to update/download them or not.

FDP_ITC.1.1/PEDMiddleTSFLoader The TSF shall enforce the **PED Middle Loader Access Control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/PEDMiddleTSFLoader The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **The PED Middle Loader downloads only authentic and integer objects coming from the Terminal Management System.**
- **Downloading is an atomic operation. Either it succeeds or the TSF rollbacks to the previous state and all downloaded data is cleared or if the rollback is not possible all PEDMiddleTSF secret data are erased**.
- **[assignment: additional importation control rules]**

Application note:

- *PCI B2: The PED's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the PED outputting the clear text PIN or other sensitive information.*

- *PCI B4: If the PED allows updates of firmware, the device cryptographically authenticates the software integrity and if the authenticity is not confirmed, the software update is rejected and deleted.*
- *Update of software or data may be a consequence of the download operation. The assignment of additional importation control rules shall manage the download operations which have an update as a consequence.*

8.1.1.8 MiddleTSF Package

FDP_ACC.1/ApplicationLoader Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control not satisfied but justified: the correspondent access control is satisfied by FDP_ITC.1./ApplicationLoader

FDP_ACC.1.1/ApplicationLoader The TSF shall enforce the **Payment Application Loader Access Control SFP** on

- **subject: Payment Application Loader**
- **objects: PAYMENT_APP, [assignment: list of data, in particular cryptographic keys, controlled under this policy]**
- **operation: download**.

Application note:

- *The "cryptographic keys" stand for POI encryption keys (POI_SK).*
- *If no list of data exist the assignment shall be filled with "none".*

FDP_ITC.1/ ApplicationLoader import of user data without security attributes

Dependencies: FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control satisfied by FDP_ACC.1/ApplicationLoader FMT_MSA.3 Static attribute initialisation not satisfied but justified: there are no security attributes to be managed for downloading objects. Terminal Management System decides to update/download them or not.

FDP_ITC.1.1/ApplicationLoader The TSF shall enforce the **Payment Application Loader Access Control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/ ApplicationLoader The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **The Payment Application Loader downloads only authentic and integer objects coming from the Terminal Management System.**
- **Payment application downloading is an atomic operation. Either it succeeds or the TSF rollbacks to the previous state and all downloaded** code and **data is cleared or if the rollback is not possible all MiddleTSF secret data are erased**.
- **[assignment: additional importation control rules]**

Application note:
In the following CAS rule, the phrase "POI software" is interpreted as ***payment application software***

- *CAS G3.1: POI software must be provided to the POI in an authentic way and must be protected against unauthorized change.*
- *CAS G3.2: If the POI implements software updates, a PAL security component cryptographically authenticates the software integrity and if the authenticity is not confirmed, the software update is rejected or all secret cryptographic keys are erased.*
- *Update of software or data may be a consequence of the download operation. The assignment of additional importation control rules shall manage the download operations which have an update as a consequence.*

FDP_ACC.1/MiddleTSFLoader Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control not satisfied but justified: the correspondent access control is satisfied by FDP_ITC.1/MiddleTSFLoader.

FDP_ACC.1.1/MiddleTSFLoader The TSF shall enforce the **Middle Loader Access Control SFP** on

- **subject: Middle Loader**
- **objects: POI_SW, [assignment: list of data, in particular cryptographic keys, controlled under this policy]**
- **operation: download**.

Application note:

- *The "cryptographic keys" stand for POI encryption keys (POI_SK). The operations are any management operation on MiddleTSF software and data.*
- *If no list of data exist the assignment shall be filled with "none".*

FDP_ITC.1/MiddleTSFLoader Import of user data without security attributes

Dependencies: FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control satisfied by FDP_ACC.1/MiddleTSFLoader FMT_MSA.3 Static attribute initialisation not satisfied but justified: there are no security attributes to be managed for downloading objects. Terminal Management System decides to update/download them or not.

FDP_ITC.1.1/MiddleTSFLoader The TSF shall enforce the **Middle Loader Access Control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3/MiddleTSFLoader The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

- **The Middle Loader downloads only authentic and integer objects the Terminal Management System.**
- **Downloading is an atomic operation. Either it succeeds or the TSF rollbacks to the previous state and all downloaded data is cleared or if the rollback is not possible all MiddleTSF secret data are erased**.
- **[assignment: additional importation control rules]**

Application note:

- *CAS G3.1: POI software must be provided to the POI in an authentic way and must be protected against unauthorized change.*
- *CAS G3.2: If the POI implements software updates, a PAL security component cryptographically authenticates the software integrity and if the authenticity is not confirmed, the software update is rejected or all secret cryptographic keys are erased.*
- *Update of software or data may be a consequence of the download operation. The assignment of additional importation control rules shall manage the download operations which have an update as a consequence.*

FPT_FLS.1/MiddleTSF Failure with preservation of secure state

Dependencies: No dependencies.

FPT_FLS.1.1/MiddleTSF The TSF shall preserve a secure state when the following types of failures occur:

- **logical anomalies of MiddleTSF**
- **[assignment: list of types of failures in MiddleTSF]**.

Application note:

- *The "secure state" does not provide access to any encryption key or any other MiddleTSF secret data.*
- *CAS G7: The functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in a breach of the security requirements.*
- *If no list of types of failures exist the assignment shall be filled with none.*

8.1.1.9 PED Prompt Control Package

FDP_ACC.1/PEDPromptControl Subset access control

Dependencies: FDP_ACF.1 satisfied by FDP_ACF.1/PEDPromptControl.

FDP_ACC.1.1/PEDPromptControl The TSF shall enforce the **PED Prompt Control SFP** on

- **subjects: POI components**
- **object: PED display, PED keypad, prompts, PIN, PED_MIDDLE_SK, PED_MIDDLE_PK**
- **operations: entry, display**.

Application note:

- *Contribution to A8. See application note of FDP_ACF.1/PEDPromptControl.*

FDP_ACF.1/PEDPromptControl Security attribute based access control

Dependencies: FDP_ACC.1 Subset access control satisfied by FDP_ACF.1/PEDPromptControl FMT_MSA.3 Static attribute initialisation not satisfied but justified: there are no security attributes to be managed for PED Display. Terminal Management System decides to modify prompts for PED Display (as part of the correspondent TSF software) or not.

FDP_ACF.1.1/PEDPromptControl The TSF shall enforce the **PED Prompt Control SFP** to objects based on the following:

- **subjects: POI components**
- **status of PED display usage: PIN display, non-PIN display**
- **status of PED Keypad usage: PIN entry, non-PIN entry**
- **[assignment: list of security attributes]**

FDP_ACF.1.2/PEDPromptControl The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **If the PED key-**

pad can be used to enter non-PIN data, then prompts demanding for PIN entry at the PED display shall never lead to a PIN disclosure (e.g. be processing the entered PIN data in clear in unprotected areas). The authenticity and proper use of prompts and use of the prompts shall be ensured and modification of the prompts or improper use of the prompts shall be prevented.

FDP_ACF.1.3/PEDPromptControl The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/PEDPromptControl The TSF shall explicitly deny access of subjects to objects based on the **following rule: Do not prompt the PIN and do not prompt any secret key in clear to the display**.

Application note:
The SFR can be implemented in different ways which are described in the following.

- *Prompts can be under control of the security module. The security module controls the display. See also refinement ADV_ARC.1.4C. This leads to PCI A8.1: All prompts for non-PIN data entry are under the control of the cryptographic unit of the PED. If the prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts are prevented, or*
- *Access control to prompts may be stored in a lesser secure region than the security module. This implementation requires that the cryptographic unit controls the display. This leads to PCI A8.2: The unauthorized alteration of prompts for non-PIN data entry into the PIN entry key pad such that PINs are compromised, i.e., by prompting for the PIN entry when the output is not encrypted, cannot occur, or*
- *PCI A8.3 For active display devices, cryptographically based controls are utilized to control the PED display and the PED usage such that it is infeasible for an entity not possessing the unlocking mechanism to alter the display and to allow the output of unencrypted PIN data form the PED. The controls provide for unique accountability and utilize key sizes appropriate for the algorithm(s) in question. Key management techniques and other control mechanisms are defined and include appropriate application of the principles of dual control and split knowledge.*

8.1.1.10 Cryptography Package

The SFRs of the Cryptography Package shall be iterated as needed by the ST author. The dependencies shall be adapted consequently.

FCS_RND.1 Quality metric for random numbers

Dependencies: No dependencies.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet **[RNGPCI].**

Application note:

- *PCI B9: If random numbers are generated by the PED in connection with security over sensitive data then, the random number generator has been assessed to ensure it is generating numbers sufficiently unpredictable.*

FCS_COP.1 Cryptographic operation

Dependencies: FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation satisfied by FDP_ITC.2 FCS_CKM.4 Cryptographic key destruction not satisfied but justified. No specific cryptographic key destruction method is enforced. Keys are destroyed by erasing them.

FCS_COP.1.1 The TSF shall perform **PIN encipherment/decipherment** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **ISO 9564**.

Application note:

- *The author of the Security Target shall iterate this SFR for each TSF part (CoreTSF, PEDMiddleTSF, MiddleTSF) if necessary.*
- *Contribution to PCI B10, CAS B10.a, PCI B12, PCI D4.1, PCI D4.2 and PCI D4.4.*

FDP_ITC.2 Import of user data with security attributes

Dependencies: FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control satisfied by FDP_IFC.1/ENC_PIN resp. FDP_IFC.1/PLAIN_PIN resp. FDP_IFC.1/ICCardReader resp. FDP_ACC.1/POI_DATA because the information flow resp. the access control is related to the Cryptographic Key Import FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path satisfied by FTP_ITC.1 FPT_TDC.1 Inter-TSF basic TSF data consistency satisfied by FPT_TDC.1

FDP_ITC.2.1 The TSF shall enforce the **[assignment: access control SFP(s) and/or information flow control SFP(s)]** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **ISO 11568 and/or ANSI X9.24 and ANSI TR-31.**

Application note:

- *The author of the Security Target shall iterate this SFR for each TSF part (Core TSF Keys, CoreTSF, PEDMiddleTSF, MiddleTSF) and assign the related SFP (ENC_PIN Information Flow Control SFP, PLAIN_PIN Information Flow Control SFP, PED Prompt Control SFP, IC Card Reader Information Flow Control SFP, POI Management and Payment Transaction Data Information Flow Control SFP), if necessary.*
- *Contribution to PCI B11, CAS G6.*

FTP_ITC.1 Inter-TSF trusted channel

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **[selection: the TSF, another trusted IT product]** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **importing cryptographic keys, [assignment: list of functions for which a trusted channel is required]**.

Application note:

- *If the author of the ST has no list of functions the assignment shall be filled with none.*
- *The author of the Security Target shall iterate this SFR for each TSF part (CoreTSF, PEDMiddleTSF, MiddleTSF) if necessary.*
- *Contribution to PCI B11, CAS G6.*

FPT_TDC.1 Inter-TSF basic TSF data consistency

Dependencies: No dependencies.

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

FPT_TDC.1.2 The TSF shall use **ISO 11568 and/or ANSI X9.24 and ANSI TR-31 [assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

Application note:

- *If the author of the ST has no list of interpretation rules the assignment shall be filled with none.*
- *In a distributed environment, a TOE may need to exchange TSF data (e.g. the SFP-attributes associated with cryptographic keys) with another trusted IT product, This family defines the requirements for sharing and consistent interpretation of these attributes between the TSF of the TOE and a different trusted IT product. If no such data types and rules exist the ST author shall fill the assignment with none.*
- *Contribution to PCI B11, CAS G6.*

8.1.1.11 Physical Protection Package

FPT_PHP.3/CoreTSF Resistance to physical attack

Dependencies: No dependencies.

FPT_PHP.3.1/CoreTSF The TSF shall resist **the physical tampering scenarios**

- **PCI A1.1:** Replacement of the front and rear casing, that shall be considered as part of any attack scenario.
- **PCI A3:** Operational or environmental conditions that are not within the specified PED operating range (e.g temperature or operating voltage outside the state operating range).
- **PCI A7:** Penetration of the PED to disclose the PIN encryption keys.
- **[assignment: additional physical tampering scenarios]**

to the **physical boundary of the CoreTSF** by responding automatically such that the SFRs are always enforced.

Refinement: The automatic response shall ensure at least the following behaviour:

- PCI A1.1: The PED uses tamper detection and response mechanisms which cause the PED to become immediately inoperable and results in the automatic and immediate erasure of any secret information which may be stored in the PED (PIN, secret cryptographic keys, administration passwords, etc.).
- PCI A3: The PED makes inaccessible any PIN value, secret or private keys or other PED secret information when operational or environmental conditions occurs that are

not within the specified PED operating range (e.g. temperature or operating voltage outside the state operating range)..

Application note:

- *If the author of the ST has no additional physical tampering scenarios fill it with none.*
- *The CoreTSF shall contain at least the PIN keypad and the PIN encryption module of the PED.*

FPT_EMSEC.1/CoreTSF TOE Emanation

Dependencies: No dependencies.

FPT_EMSEC.1.1/CoreTSF The TOE shall not emit **measurable signals including power fluctuations (PCI A7)** in excess of **none** enabling access to **PIN encryption keys** and **none**.

FPT_EMSEC.1.2/CoreTSF The TSF shall ensure **all users** are unable to use the following interface **emanations (including power fluctuations) (PCI A7)** to gain access to **PIN encryption keys** and **none**.

Application note:

- *Supports PCI A7. Recall that CoreTSF shall contain at least the PED keypad and the PIN encryption module (PED Security Module).*

FPT_PHP.3/ICCardReader Resistance to physical attack

Dependencies: No dependencies.

FPT_PHP.3.1/ICCardReader The TSF shall resist **the physical tampering scenarios**

- **PCI D1:** Penetration of the IC Card Reader to make any additions, substitutions or modifications to either the IC Card Reader's hardware or software, in order to determine or modify any sensitive data.
- **[assignment: additional physical tampering scenarios]**

to the **physical boundary of the IC Card Reader** by responding automatically such that the SFRs are always enforced.

Application note:

- *If the author of the ST has no additional physical tampering scenarios the assignment shall be filled with "no additional tamper scenario"..*
- *Apply to the PED components that belong to the PEDMiddleTSF.*

FPT_PHP.3/MSR Resistance to physical attack

Dependencies: No dependencies.

FPT_PHP.3.1/MSR The TSF shall resist **additions, substitutions, or modifications that would allow determination or modification of Magnetic Stripe data** to the **Magnetic Stripe read head and associated hardware and software** by responding automatically such that the SFRs are always enforced.

Application note:

- *Contribution to PCI A11. "Responding automatically" includes the situation where the physical or logical TOE design simply prevents the change from taking place. The TOE should therefore either prevent the attempted changes or respond in a way that leaves the TOE unable to carry out payment transactions or request PINs. Any authorised changes to TOE software are assumed to be approved, and hence not to violate the protection of the Magnetic Stripe data. The TOE is prevented from carrying out payment transactions as a result of any changes, but may be able to carry out administrator functions, subject to the usual requirements for administrator authentication.*

8.1.2 Security Functional Requirements in each PP configuration

455 The table below shows the SFRs included in each PP configuration and the TSF part the individual requirements are associated with.

SFR Package	TSF part(s)	PED-ONLY	POI-COMPRE-HENSIVE	POI-OPTION
PIN Entry	CoreTSF	X	X	X
ENC_PIN	CoreTSF Keys CoreTSF	X	X	X
PLAIN_PIN	Core TSF Keys Core TSF	X	X	
IC Card Reader	Core TSF Keys PEDMiddleTSF	X	X	
POI_DATA	MiddleTSF		X	X
CoreTSF	CoreTSF	X	X	X
PEDMiddleTSF	PEDMiddleTSF	X	X	X
MiddleTSF	MiddleTSF		X	X
PED Prompt Control	PEDMiddleTSF	X	X	X
Cryptography	CoreTSF	X	X	X
	PEDMiddleTSF	X	X	X
	Middle TSF		X	X
Physical Protection				
FPT_PHP.3/CoreTSF	CoreTSF Keys CoreTSF	X	X	X
FPT_EMSEC.1/CoreTSF	CoreTSF Keys	X	X	X
FPT_PHP.3/ICCardReader	PEDMiddleTSF	X	X	
FPT_PHP.3/MSR	MSRTSF	X	X	

Table 13: SFR packages included in each PP configuration

8.1.3 Security Functional Requirements dependencies rationale

456 The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-dissolved dependencies are appropriately explained.

457 The dependency analysis has directly been made within the description of each SFR in section 8.1. All dependencies from CC part 2 and defined by the extended components in section 7 are either fulfilled or their non-fulfilment is justified.

8.2 Security Assurance Requirements

458 The minimum EAL applicable to the products evaluated against this PP is EAL POI defined hereafter.

459 Most of the assurance components belonging to EAL POI come from EAL2 predefined package. The additions to EAL2 concern the evaluation of the development environment through ALC_DVS.2 (including the site inspection of the Initial Key Loading facility) and the vulnerability analysis of the POI's TSF parts to the suitable attack potential through the extended requirement AVA_POI: POI-High for Keys in Core TSF, POI-Moderate for Core TSF, POI-Low for PEDMiddle TSF and Middle TSF, and POI-Basic for MSR.

460 The following table lists the Security Assurance Requirements included in EAL POI:

- "STANDARD" means that the CC requirement applies as is,
- "REFINED" means that the CC requirement has been refined in this PP to meet POI specificities and CAS requirements,
- "EXTENDED" means that the requirement does not belong to CC Part3,
- A greyed cell means that the requirement does not apply to the corresponding TSF part.

461 Notice that EAL POI does not include AVA_VAN.2 since each instance of AVA_POI is a refinement of AVA_VAN.2 restricted to the POI components selected in the instantiation (cf. Annex 12 for details).

462 The "STANDARD" requirements are defined in CC Part3.

463 The "REFINED" and the "EXTENDED" requirements are defined in sections 8.2.2 and 8.2.3 respectively.

Security Assurance Requirements			EAL POI		
			PED-ONLY	POI-COMPREHENSIVE	POI-OPTION
EAL2	ADV_ARC.1	REFINED	X	X	X
	ADV_FSP.2	STANDARD	X	X	X
	ADV_TDS.1	STANDARD	X	X	X
	AGD_OPE.1	REFINED	X	X	X
	AGD_PRE.1	STANDARD	X	X	X
	ALC_CMC.2	REFINED	X	X	X
	ALC_CMS.2	REFINED	X	X	X
	ALC_DEL.1	REFINED	X	X	X
	ATE_COV.1	STANDARD	X	X	X
	ATE_FUN.1	STANDARD	X	X	X
	ATE_IND.2	STANDARD	X	X	X
	AVA_VAN.2				
	ALC_DVS.2	REFINED	X	X	X
Extended Requirements	AVA_POI.1/MSR	POI-Basic attack potential	X	X	
	AVA_POI.2/PEDMiddleTSF	POI-Low attack potential	X	X	X
	AVA_POI.2/MiddleTSF	POI-Low attack potential		X	X
	AVA_POI.3/CoreTSF	POI-Moderate attack potential	X	X	X
	AVA_POI.4/CoreTSFKeys	POI-High attack potential	X	X	X

Table 14: Definition of EAL POI by PP configuration

8.2.1 Security Assurance Requirements Rationale

466 The EAL POI was developed by the Common Approval Scheme Initiative (CAS) in co-operation with the Joint Interpretation Library Terminal Evaluation Subgroup (JTEMS) to be used for CC evaluation of POI. Members of JTEMS are bank associations, payment schemes, certification bodies, POI manufacturers and evaluation laboratories whereas members of CAS are the risk owner of the payment schemes.

467 From JTEMS point of view, the EAL POI package permits a developer to gain sufficient assurance from positive security engineering based on good commercial development practices which do not require substantial specialist knowledge, skills, and

other resources. Moreover, the EAL POI provides the required assurance in economically feasible way.

468 The starting point of EAL POI was CAS risk analysis and its derived security requirements (see Annex 11.1). Indeed, selecting most of the assurance components from EAL2 for EAL POI was sufficient to meet the CAS security requirements as shown in Annex 11.2 “Mapping from CAS to SFRs and SARs”. CAS requirements that fall outside standard SAR are addressed by additions (like ALC_DVS.2), by specific refinements stated in section 8.2.2 and by extensions with new assurance components AVA_POI, stated in section 8.2.3. AVA_POI components allow to go beyond EAL2 vulnerability analysis without significant increase of documentation, design and testing effort. Moreover, this new family fully meets CAS security requirements regarding the attack potential levels. The relationship between the family AVA_POI and the assurance component AVA_VAN.2 is shown in Annex 12.

469 For the chosen assurance components all the dependencies are met or exceeded in the EAL POI assurance package as shown in section 8.2.4.

8.2.2 Refined security assurance requirements

8.2.2.1 ADV_ARC Security Architecture

ADV_ARC.1 Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

Refinement:
If the POI_DATA package is included in the set of evaluated SFR, the security architecture description shall describe the security domains that result from the application separation principle (requirement CAS G2), specified in FDP_ACC.1/POI_DATA, FDP_ACF.1/POI_DATA and FDP_RIP.1/POI_DATA. It shall describe how isolation of payment application data is achieved, how the correct execution of the payment application is

enforced as well as the management of Cardholder communication interface during payment application execution and how interference from other applications is avoided.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

Refinement:

In particular, the security architecture description shall demonstrate that,

- PCI A2: If the PED or ICC reader permits access to internal areas (e.g., for service or maintenance), then it is not possible using this access area to insert a pin disclosing bug. Immediate access to sensitive data such as PIN or cryptographic data is either prevented by the design of the internal areas (e.g., by enclosing components with sensitive data into tamper resistant/responsive enclosures) or it has a mechanism so that access to internal areas causes the immediate erasure of sensitive data.
- PCI A4: Sensitive functions or information are only used in the protected areas(s) of the PED
- PCI D1: It is not feasible to penetrate the IC Card Reader to make any additions, substitutions, or modifications to either the IC Card Reader's hardware or software, in order to determine or modify any sensitive data.
- PCI A10: The design of the PED or ICC reader is such that it is not practical to construct a duplicate PED or ICC reader from commercially available components. For example, the casing used to house the device's electronic components is not commonly available.
- PCI D2.1 : The slot of the ICC reader into which the IC card is inserted does not have sufficient space to hold a PIN-disclosing “bug” when a card is inserted, nor can it feasibly be enlarged to provide space for a PIN-disclosing “bug.” It is not possible for both an IC card and any other foreign object to reside within the card insertion slot.
- PCI D2.2 : The opening for the insertion of the IC card is in full view of the Cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.
- PCI D3 : The ICC reader is constructed so that wires running out of the slot of the IC Card Reader to a recorder or a transmitter (an external bug) can be observed by the Cardholder.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Refinement:

In particular, the security architecture description shall demonstrate that,

- PCI A1.2: Failure of a single security mechanism does not compromise PED security. Protection against a threat is based on a combination of at least two independent security mechanisms.

- PCI A8.1: All prompts for non-PIN data entry are under the control of the cryptographic unit of the PED. If the prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts are prevented.

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.2.2 AGD_OPE Operational user guidance

AGD_OPE.1 Operational user guidance

AGD_OPE.1.1D The developer shall provide operational user guidance.

Refinement:

In particular, the user guidance shall address the following topics:

- PCI D2.2: The opening for the insertion of the IC card is in full view of the Cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.
- CAS F5: The user guidance shall provide instructions for the operational management of the TOE. This includes instructions for recording the whole life cycle of the TOE components and of the way those components are integrated into a single device, e.g.:
  - data on production and personalisation,
  - physical/chronological whereabouts,
  - repair and maintenance,
  - removal from operation,
  - loss or theft.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application note:
Developing and manufacturing of the TOE are part of the developer phase. During the developer phase the initial cryptographic keys are loaded and if required also other cryptographic keys are loaded into the POI. Additionally, cryptographic keys can also be loaded during the user phase. The ST author shall define where the developer phase ends and where the user phase begins in relation to cryptographic key loading.

8.2.2.3 ALC_CMC CM capabilities

ALC_CMC.2 Use of a CM system

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

ALC_CMC.2.1C The TOE shall be labelled with its unique reference.

Refinement:
The unique identification shall also apply to the PED in order to comply with the following CAS requirement:

- CAS F4: Each POI security-related component shall have a unique visible identifier affixed to it.

The unique identifier applies to the tamper-resistant boundaries (eg. PED, IC Card Reader). They must be visible without opening the terminal.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

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

8.2.2.4 ALC_CMS CM Scope

ALC_CMS.2 Parts of the TOE CM coverage

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

Refinement:

- PCI B3: The Firmware, and any changes thereafter, has been inspected and reviewed using a documented and auditable process, and certified as being free from hidden and unauthorized or undocumented functions.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

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

8.2.2.5 ALC_DEL Delivery

ALC_DEL.1 Delivery procedures

ALC_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinement:
The evaluator shall confirm the use of the delivery procedures by examination of the developer's documentation and evidences. The delivery procedures involving the Initial Key Loading Facility, shall be also checked during a site visit (cf. ALC_DVS.2).

8.2.2.6 ALC_DVS Development Security

ALC_DVS.2 Sufficiency of security measures

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

Refinement:
The development environment stands for the design, manufacturing, assembling and maintenance environments of TOE components, including the final assembly and the Initial Key Loading facilities. The Initial Key Loading is defined as the point where responsibility for the TOE security-related components falls to the acquirers.

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.

Refinement:
The development security documentation shall meet the following requirements:

- PCI E2, CAS E2.a: The certified[3] firmware is protected and stored in such a manner as to preclude unauthorized modification, e.g. using dual control or standardized cryptographic authentication procedures. This requirement addresses the firmware of the PED and the PAL security enforcing components.
- PCI E3, CAS E3.a: The device is assembled in a manner that the PED and PAL security enforcing components used in the manufacturing process are those in the scope of the evaluation and unauthorized substitutions have not been made. These components belong to the TOE configuration list.
- PCI E4, CAS E4.a: Production software that is loaded to devices at the time of manufacture is transported, stored, and used under the principle of dual control, preventing unauthorized modifications and/or substitutions.
- PCI E5, CAS E5. a: Subsequent to production but prior to shipment from the manufacturer's facility, the PED and any PAL security enforcing component are stored in protected, access-controlled area or sealed within tamper-evident packaging to prevent undetected unauthorized access to the device or its components.
- PCI E6, CAS E6.a: If the PED and any PAL security enforcing component will be authenticated at the Key Loading Facility by means of secret information placed in the device during manufacturing, then this secret information is unique to each

[3] Certified here means that the Firmware has been checked by the developer. Hence the Firmware that is part of the configuration items has been checked in integrity.

PED or PAL security enforcing component, unknown and unpredictable to any person, and installed in the PED or PAL security enforcing component under dual control to ensure that it is not disclosed during installation.

- CAS E7.1: If the manufacturer is in charge of initial-key-loading himself he must verify the authenticity of the PAL security enforcing components for himself.
- CAS E7.2: If the manufacturer is not in charge of Initial Key Loading he must provide means to the initial-key-loading facility to assure the verification of the authenticity of the PAL security enforcing components.
- CAS E8: Security measures during development and maintenance of PAL security enforcing components. The manufacturer must write a development security documentation, which describes all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity of the design and implementation of the PAL security enforcing components in their development environment. The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the PAL security enforcing components. The evidence shall justify that the security measures provide the necessary level of protection to maintain the integrity of the PAL security enforcing components.
- PCI F3, CAS F3.a: While in transit from the manufacturer's facility to external facilities, the PED and PAL security enforcing components are:
  - Shipped and stored in tamper-evident packaging; and/or,
  - Shipped and stored containing a secret that is immediately and automatically erased if any physical or functional alteration to the device is attempted, that can be verified by the Initial Key Loading facility, but that cannot feasibly be determined by unauthorized personnel."

The development security documentation shall describe all the delivery procedures necessary to maintain the security of the TOE components before assembling, subsequent to production and prior to shipment and on the way to the Initial Key Loading Facility. The delivery procedures shall contribute enforcing the following requirements:

- PCI E4, CAS E4.a: Production software that is loaded to devices at the time of manufacture is transported, stored, and used under the principle of dual control, preventing unauthorized modifications and/or substitutions.
- PCI F1, CAS F1.a: The PED and PAL security enforcing components are shipped from the manufacturer's facility to the initial-key-loading facility, and stored en route, under auditable controls that can account for the location of every components at every point.

PCI F2, CAS F2.a: Procedures are in place to transfer accountability for the device from the manufacturer to the initial-key-loading facility.

ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

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.

Refinement:

- CAS E9: The evaluator shall confirm that the security measures are being applied by examination of the developer's documentation and evidences. The security measures involving the final assembly and the Initial Key Loading facilities shall be checked during a site visit.

8.2.3 Extended security assurance requirements

470 The AVA_POI requirements of the EAL POI package consists of:

- AVA_POI.1 applied to MSR
- Two iterations of AVA_POI.2, applied to PEDMiddle TSF and to MiddleTSF
- AVA_POI.3 applied to CoreTSF
- AVA_POI.4 applied to Core TSF keys

8.2.3.1 AVA_POI applied to MSR

471 This requirement holds in PED-ONLY and POI-COMPREHENSIVE configurations only.

AVA_POI.1/MSR "Basic POI vulnerability analysis"

Dependencies:

ADV_ARC.1 Security architecture description
ADV_FSP.2 Security-enforcing functional specification
ADV_TDS.1 Basic modular design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures Objectives

Developer action elements:

AVA_POI.1.1D/MSR The developer shall provide the **MSR components** for testing.

AVA_POI.1.2D/MSR The developer shall provide the implementation representation and a mapping of SFRs to the implementation representation of **the Magnetic Stripe Reader hardware.**

Content and presentation elements:

AVA_POI.1.1C/MSR The POI shall be suitable for testing.

Evaluator action elements:

AVA_POI.1.1E/MSR The evaluator ***shall confirm*** that the information provided meets all requirements for content and presentation of evidence.

AVA_POI.1.2E/MSR The evaluator ***shall perform*** a search of public domain sources to identify potential vulnerabilities in the **Magnetic Stripe Reader component of the POI**.

AVA_POI.1.3E/MSR The evaluator ***shall perform*** an independent vulnerability analysis of **the Magnetic Stripe Reader component of the POI** using the guidance documentation, functional specification, design, the security architecture description **as well as the available implementation representation and the mapping of SFRs to the implementation representation** to identify potential vulnerabilities.

AVA_POI.1.4E/MSR The evaluator ***shall conduct*** penetration testing, based on the identified potential vulnerabilities, to determine that the **Magnetic Stripe Reader component of the POI** is resistant to attacks performed by an attacker possessing **POI-Basic** attack potential.

Application note:

- *Inputs for MSR vulnerability analysis do not need to be separate documents – they may be included in other TOE deliverables. Important aspects to be shown in the inputs is the design and layout of any relevant tamper-resistance aspects of the MSR, the interfaces between these and the processor responsible for detection and responding to tampering with the MSR, and the nature of the responses.*
- *The vulnerabilities examined shall include penetration of the TOE to make any additions, substitutions, or modifications to the Magnetic Stripe read head and associated hardware or software, in order to determine or modify Magnetic Stripe data.*

8.2.3.2 AVA_POI applied to MiddleTSF

AVA_POI.2/MiddleTSF "Low POI vulnerability analysis"

Dependencies:

ADV_ARC.1 Security architecture description
ADV_FSP.2 Security-enforcing functional specification
ADV_TDS.1 Basic modular design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures Objectives

Developer action elements:

AVA_POI.2.1D/MiddleTSF The developer shall provide the **MiddleTSF's components** for testing.

AVA_POI.2.2D/MiddleTSF The developer shall provide the implementation representation and a mapping of SFRs to the implementation representation of **'none'**.

Content and presentation elements:

AVA_POI.2.1C/MiddleTSF The **MiddleTSF's components** shall be suitable for testing.

Evaluator action elements:

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

AVA_POI.2.2E/MiddleTSF The evaluator ***shall perform*** a search of public domain sources to identify potential vulnerabilities in the **MiddleTSF's components.**

AVA_POI.2.3E/MiddleTSF The evaluator shall perform an independent vulnerability analysis of the **MiddleTSF's components** using the guidance documentation, the functional specification, the design, the security architecture description to identify potential vulnerabilities.

AVA_POI.2.4E/MiddleTSF The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the **MiddleTSF's components** are resistant to attacks performed by an attacker possessing **POI-Low** attack potential.

8.2.3.3 AVA_POI applied to PEDMiddle TSF

AVA_POI.2/PEDMiddleTSF "Low POI vulnerability analysis"

Dependencies:

ADV_ARC.1 Security architecture description
ADV_FSP.2 Security-enforcing functional specification
ADV_TDS.1 Basic modular design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures Objectives

Developer action elements:

AVA_POI.2.1D/PEDMiddleTSF The developer shall provide the **PEDMiddleTSF's components** for testing.

AVA_POI.2.2D/PEDMiddleTSF The developer shall provide the implementation representation and a mapping of SFRs to the implementation representation of the hardware and software **PEDMiddleTSF's components**.

Content and presentation elements:

AVA_POI.2.1C/PEDMiddleTSF The **PEDMiddleTSF's components** shall be suitable for testing.

Evaluator action elements:

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

AVA_POI.2.2E/PEDMiddleTSF The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the **PEDMiddleTSF's components.**

AVA_POI.2.3E/ PEDMiddleTSF The evaluator shall perform an independent vulnerability analysis of the **PEDMiddleTSF's components** using the guidance documentation, functional specification, design, security architecture description **as well as the available implementation representation and the mapping of SFRs to the implementation representation** to identify potential vulnerabilities.

AVA_POI.2.4E/PEDMiddleTSF The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the **PEDMiddleTSF's components** are resistant to attacks performed by an attacker possessing **POI-Low** attack potential.

8.2.3.4 AVA_POI applied to CoreTSF

AVA_POI.3/CoreTSF "Moderate POI Vulnerability Analysis"

Dependencies:

ADV_ARC.1 Security architecture description
ADV_FSP.2 Security-enforcing functional specification
ADV_TDS.1 Basic modular design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures Objectives

Developer action elements:

AVA_POI.3.1D/CoreTSF The developer shall provide the **CoreTSF's components** for testing.

AVA_POI.3.2D/CoreTSF The developer shall provide the implementation representation and a mapping of SFRs to the implementation representation of **the hardware and software CoreTSF's components**.

Content and presentation elements:

AVA_POI.3.1C/CoreTSF The **CoreTSF's components** shall be suitable for testing.

Evaluator action elements:

AVA_POI.3.1E/CoreTSF The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_POI.3.2E/CoreTSF The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the **CoreTSF's components**.

AVA_POI.3.3E/CoreTSF The evaluator shall perform an independent vulnerability analysis of the **CoreTSF's components** using the guidance documentation, functional specification, design, security architecture description **as well as the available implementation representation and the mapping of SFRs to the implementation representation** to identify potential vulnerabilities.

AVA_POI.3.4E/CoreTSF The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the **CoreTSF's components** are resistant to attacks performed by an attacker possessing **POI-Moderate** attack potential.

8.2.3.5 AVA_POI applied to the Core TSF Keys

472 AVA_POI.4 is applied to the part of CoreTSF which stores and processes secret PIN Encryption Keys. Note that AVA_POI.4/CoreTSFKeys supersedes AVA_POI.3/CoreTSF regarding secret PIN Encryption Keys (Core TSF Keys).

AVA_POI.4/CoreTSFKeys "High POI vulnerability analysis"

Dependencies:

ADV_ARC.1 Security architecture description
ADV_FSP.2 Security-enforcing functional specification
ADV_TDS.1 Basic modular design
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures Objectives

Developer action elements:

AVA_POI.4.1D/CoreTSFKeys The developer shall provide the **CoreTSFKeys components** for testing.

AVA_POI.4.2D/CoreTSFKeys The developer shall provide the implementation representation and a mapping of SFRs to implementation representation of **the hardware and software CoreTSFKeys components**.

Content and presentation elements:

AVA_POI.4.1C/CoreTSFKeys The **CoreTSFKeys components** shall be suitable for testing.

Evaluator action elements:

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

AVA_POI.4.2E/CoreTSFKeys The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the **CoreTSFKeys components**.

AVA_POI.4.3E/CoreTSFKeys The evaluator shall perform an independent vulnerability analysis of the **CoreTSFKeys components** using the guidance documentation, functional specification, design, security architecture description **as well as the available implementation representation and the mapping of SFRs to implementation representation** to identify potential vulnerabilities.

AVA_POI.4.4E/CoreTSFKeys The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the **CoreTSFKeys components** is resistant to attacks performed by an attacker possessing **POI-High** attack potential.

8.2.4 Security Assurance Requirements Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.2, ADV_TDS.1
ADV_FSP.2	(ADV_TDS.1)	ADV_TDS.1
ADV_TDS.1	(ADV_FSP.2)	ADV_FSP.2
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.2
AGD_PRE.1	No dependencies	
ALC_CMC.2	(ALC_CMS.1)	ALC_CMS.2
ALC_CMS.2	No dependencies	
ALC_DEL.1	No dependencies	
ATE_COV.1	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.2, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.1
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and	ADV_FSP.2, AGD_OPE.1,

	(AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	AGD_PRE.1, ATE_COV.1, ATE_FUN.1
ALC_DVS.2	No dependencies	
AVA_POI.1/MSR	(ADV_ARC.1) and (ADV_FSP.1) and (ADV_TDS.1) and (AGD_OPE.1) and (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1
AVA_POI.2/PEDMiddleTSF	(ADV_ARC.1) and (ADV_FSP.1) and (ADV_TDS.1) and (AGD_OPE.1) and (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1
AVA_POI.2/MiddleTSF	(ADV_ARC.1) and (ADV_FSP.1) and (ADV_TDS.1) and (AGD_OPE.1) and (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1
AVA_POI.3/CoreTSF	(ADV_ARC.1) and (ADV_FSP.1) and (ADV_TDS.1) and (AGD_OPE.1) and (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1
AVA_POI.4/CoreTSFKeys	(ADV_ARC.1) and (ADV_FSP.1) and (ADV_TDS.1) and (AGD_OPE.1) and (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1

Table 15: SAR dependencies

9 Rationale Objectives/SFR

473 The following table provides an overview of the coverage of security objectives by security functional requirements and constitutes evidence for sufficiency and necessity of the selected SFRs.

	O.PINEntry	O.EncPIN	O.CipherPPIN	O.ClearPPIN	O.CoreSWHW	O.PEDMiddleSWHW	O.ICCardReader	O.PaymentTransaction	O.POISW	O.PaymentApplicationDownload	O.POIApplicationSeparation	O.PromptControl	O.MSR
PIN Entry Package													
FDP_IFC.1/PIN_ENTRY	X												
FDP_ITC.1/PIN_ENTRY	X												
FPT_EMSEC.1/PIN_ENTRY	X												
FIA_UAU.2/PIN_ENTRY	X	X	X	X	X	X	X						
FIA_UID.1/PIN_ENTRY	X	X	X	X	X	X	X						
FTA_SSL.3/PIN_ENTRY	X												
ENC_PIN Package													
FDP_IFC.1/ENC_PIN		X											
FDP_IFF.1/ENC_PIN		X											
FMT_MSA.3/ENC_PIN		X											
FMT_MSA.1/ENC_PIN		X											
FMT_SMR.1/ENC_PIN		X											
FIA_UID.1/ENC_PIN		X											
FDP_RIP.1/ENC_PIN		X											
FDP_ITT.1/ENC_PIN		X											
FTP_TRP.1/ENC_PIN		X											
PLAIN_PIN Package													
FDP_IFC.1/PLAIN_PIN			X	X									
FDP_IFF.1/PLAIN_PIN			X	X									
FDP_RIP.1/PLAIN_PIN			X	X									
FDP_ITT.1/PLAIN_PIN			X	X									
FMT_MSA.3/PLAIN_PIN			X				X						
FMT_MSA.1/PLAIN_PIN			X				X						
FMT_SMR.1/PLAIN_PIN			X				X						
FIA_UID.1/PLAIN_PIN			X				X						
IC Card Reader Package													
FDP_IFC.1/ICCardReader							X						
FDP_IFF.1/ICCardReader							X						
FDP_RIP.1/ICCardReader							X						
FDP_ITT.1/ICCardReader							X						
POI_DATA Package													
FDP_ACC.1/POI_DATA								X			X		

	O.PINEntry	O.EncPIN	O.CipherPPIN	O.ClearPPIN	O.CoreSWHW	O.PEDMiddleSWHW	O.ICCardReader	O.PaymentTransaction	O.POISW	O.PaymentApplicationDownload	O.POIApplicationSeparation	O.PromptControl	O.MSR
FDP_ACF.1/POI_DATA								X			X		
FDP_ITT.1/POI_DATA								X					
FDP_UIT.1/MAN_DAT								X					
FDP_UIT.1/PAY_DAT								X					
FDP_UCT.1/POI_DATA								X					
FDP_RIP.1/POI_DATA								X			X		
FTP_ITC.1/POI_DATA								X					
FIA_API.1/POI_DATA								X					
CoreTSF Package													
FPT_TST.1/CoreTSF					X								
FPT_FLS.1/CoreTSF					X								
FDP_ACC.1/CoreTSFLoader					X								
FDP_ITC.1/CoreTSFLoader					X								
PEDMiddleTSF Package													
FPT_TST.1/PEDMiddleTSF						X							
FPT_FLS.1/PEDMiddleTSF						X							
FDP_ACC.1/PEDMiddleTSFLoader						X							
FDP_ITC.1/PEDMiddleTSFLoader						X							
MiddleTSF Package													
FDP_ACC.1/MiddleTSFLoader									X				
FDP_ITC.1/MiddleTSFLoader									X				
FPT_FLS.1/MiddleTSF									X				
FDP_ACC.1/ApplicationLoader										X			
FDP_ITC.1/ApplicationLoader										X			
PED Prompt Control Package													
FDP_ACC.1/PEDPromptControl												X	
FDP_ACF.1/PEDPromptControl												X	
Cryptography Package													
FCS_RND.1		X	X										
FCS_COP.1		X	X				X						
FDP_ITC.2		X	X				X						
FTP_ITC.1		X	X				X						
FPT_TDC.1		X	X				X						
Physical Protection Package													
FPT_PHP.3/CoreTSF	X	X	X	X	X		X						
FPT_EMSEC.1/CoreTSF		X	X				X						
FPT_PHP.3/ICCardReader							X						
FPT_PHP.3/MSR													X

Table 16: Objectives coverage by SFRs

474 A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given below.

475 **O.PINEntry**

476 Rationale:

- With FPT_EMSEC.1/PIN_ENTRY the PED only emits indistinguishable audible tones, if any (PCI A5); the PED does not emit sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring (PCI A6); not emit the entered PIN digits at the display (PCI B5)
- With FPT_PHP.3/CoreTSF the PED resists physical manipulation and manipulation of the CoreTSF hardware to protect the confidentiality of any PIN (PCI A1.1) including changing environmental conditions (PCI A3).
- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).
- According to FDP_IFC.1/PIN_ENTRY and FDP_ITC.1/PIN_ENTRY PIN Entry is only allowed to be entered at the PED keypad assigned to CoreTSF (PCI B15).
- According to FTA_SSL.3/PIN_ENTRY limits on the number of actions that can be performed and a time limit shall be imposed, after which the PED is forced to return to its normal mode (PCI B8).

477 **O.EncPIN**

478 Rationale:

- With FPT_PHP.3/CoreTSF the PED resists physical manipulation and manipulation of the CoreTSF hardware to protect the confidentiality of any ENC_PIN and ENC_PIN_SK (PCI A1.1, PCI A7) including changing environmental conditions (PCI A3).
- FPT_EMSEC.1/CoreTSF protects ENC_PIN_SK against emanation (PCI A7).
- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).
- Due to FDP_IFC.1/ENC_PIN and FDP_IFF.1/ENC_PIN the PED enciphers ENC_PIN with the appropriate dedicated online or offline encryption key immediately after ENC_PIN entry is complete and has been signified as such by the Cardholder (PCI B6, CAS B6.a).
- The PED sends the ENC_PIN in encrypted form to the IC Card Reader (offline) or to the Acquirer (online). In case of offline encryption FDP_IFC.1/ENC_PIN and FDP_IFF.1/ENC_PIN mandate encryption of the PIN (PCI D4.1, PCI D4.3).
- According to FDP_IFC.1/ENC_PIN and FDP_IFF.1/ENC_PIN the PED uses cryptographic means to prevent the use of the PED for exhaustive PIN determination (PCI B10, CAS B10.a, PCI D4.1, PCI D4.3).

- According to FDP_IFC.1/ENC_PIN and FDP_IFF.1/ENC_PIN it is not possible to encrypt or decrypt any arbitrary data using any PIN related key and PIN related keys have different values (PCI B13). Additionally, output of cleartext cryptographic keys or moving from one component of higher security to a component of less security is prevented (PCI B14).
- FDP_ITT.1/ENC_PIN prevents the disclosure of ENC_PIN and ENC_PIN_SK when they are transmitted between physically-separated parts of the PED or to the IC Card Reader
- FDP_RIP.1/ENC_PIN prevents unwanted knowledge of secret data upon the de-allocation of the resources from sensitive objects. Especially ENC_PIN is deleted immediately after being enciphered (PCI B6).
- Because of FTP_TRP.1/ENC_PIN the following holds: If the PED can hold multiple PIN encryption keys and if the key to be used to encrypt the PIN can be externally selected, then the PED prohibits unauthorised key replacement and key misuse (PCI C1).
- According to FCS_RND.1 mechanisms are provided to generate random numbers that meet a defined quality metric for cryptographic means (PCI B9).
- According to FCS_COP.1, PIN encipherment is performed following ISO 9564 (PCI B10, CAS B10a, PCI B12, PCI D4.1, PCI D4.2, PCI D4.4).
- According to FDP_ITC.2 also the import of cryptographic keys is according to ISO 11568 and/or ANSI X9.24 and ANSI TR-31. Therefore state-of-the-art cryptography for cryptographic means is provided (PCI B11). The cryptographic key import is supported by FTP_ITC.1 and FPT_TDC.1.
- With FMT_MSA.3/ENC_PIN, FMT_MSA.1/ENC_PIN, FMT_SMR.1/ENC_PIN and FIA_UID.1/ENC_PIN security attributes are managed and roles are assigned.

479 **O.CipherPPIN**

480 Rationale:

- With FPT_PHP.3/CoreTSF the PED resists physical manipulation and manipulation of the CoreTSF hardware to protect the confidentiality of Ciphertext PLAIN_PIN and PLAIN_PIN_SK (PCI A1.1, PCI A7) including changing environmental conditions (PCI A3).
- FPT_EMSEC.1/CoreTSF protects PLAIN_PIN_SK against emanation (PCI A7).
- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).
- Due to FDP_IFC.1/PLAIN_PIN and FDP_IFF.1/PLAIN_PIN the PED enciphers Ciphertext PLAIN_PIN if PED and IC Card Reader are not integrated into the same tamper-responsive boundary (PCI D4.2).
- FDP_ITT.1/PLAIN_PIN prevents the disclosure of Ciphertext PLAIN_PIN and PLAIN_PIN_SK when they are transmitted between physically-separated parts of the PED or to the IC Card Reader.

- FDP_RIP.1/PLAIN_PIN prevents unwanted knowledge of secret data upon the de-allocation of the resources from sensitive objects. Especially PLAIN_PIN is deleted immediately after being enciphered (PCI B6).
- According to FCS_RND.1 mechanisms are provided to generate random numbers that meet a defined quality metric for cryptographic means (PCI B9).
- According to FCS_COP.1, PIN encipherment is performed following ISO 9564 (PCI B10, CAS B10a, PCI B12, PCI D4.1, PCI D4.2, PCI D4.4).
- According to FDP_ITC.2 also the import of cryptographic keys is according to ISO 11568 and/or ANSI X9.24 and ANSI TR-31. Therefore state-of-the-arte cryptography for cryptographic means is provided (PCI B11). The cryptographic key import is supported by FTP_ITC.1 and FPT_TDC.1.
- With FMT_MSA.3/PLAIN_PIN, FMT_MSA.1/PLAIN_PIN, FMT_SMR.1/PLAIN_PIN and FIA_UID.1/PLAIN_PIN security attributes are managed and roles are assigned.

481 **O.ClearPPIN**

482 Rationale:

- With FPT_PHP.3/CoreTSF the PED resists physical manipulation and manipulation of the CoreTSF hardware to protect the confidentiality of Plaintext PLAIN_PIN and (PCI A1.1) including changing environmental conditions (PCI A3).
- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).
- Due to FDP_IFC.1/PLAIN_PIN and FDP_IFF.1/PLAIN_PIN the PED transmits the PIN block wholly through the tamper-responsive boundary if PED and IC Card Reader are integrated into the same tamper-responsive boundary (PCI D4.4).
- FDP_ITT.1/PLAIN_PIN prevents the disclosure of Cleartext PLAIN_PIN when it is transmitted between physically-separated parts of the PED or to the IC Card Reader.
- FDP_RIP.1/PLAIN_PIN prevents unwanted knowledge of secret data upon the de-allocation of the resources from sensitive objects. Especially PLAIN_PIN is deleted immediately after being sent to the IC Card Reader (PCI B6).

483 **O.CoreSWHW**

484 Rationale:

- With FPT_PHP.3/CoreTSF the PED resists physical manipulation and manipulation of the CoreTSF hardware (PCI A1.1) or software, including changing environmental conditions (PCI A3).
- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).

- FPT_TST.1/CoreTSF implements the periodically checking of the authenticity and integrity of CoreTSF by running a suite of tests during initial start-up, periodically during normal operation and at the request of an authorised user (PCI B1).
- FPT_FLS.1/CoreTSF enforces the Core TSF authenticity and integrity by preserving a secure state in case of self-test failure or logical anomalies (PCI B1, PCI B2).
- The protection of the authenticity and integrity of CORE_SW and cryptographic keys upon downloading of new components and updating of existing ones is protected due to FDP_ACC.1.1/CoreTSFLoader and FDP_ITC.1/CoreTSFLoader (PCI B2, PCI B4).

485 **O.PEDMiddleSWHW**

486 Rationale:

- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).
- FPT_TST.1/PEDMiddleTSF implements the periodically checking of the authenticity and integrity of PEDMiddleTSF by running a suite of tests during initial start-up, periodically during normal operation and at the request of an authorised user (PCI B1).
- FPT_FLS.1/PEDMiddleTSF enforces the PEDMiddleTSF authenticity and integrity by preserving a secure state in case of self-test failure or logical anomalies (PCI B1, PCI B2).
- The protection of the authenticity and integrity of PED_MIDDLE_SW and cryptographic keys upon downloading of new components and updating of existing ones is protected due to FDP_ACC.1/PEDMiddleTSFLoader and FDP_ITC.1/PEDMiddleTSFLoader (PCI B2, PCI B4).

487 **O.ICCardReader**

488 Rationale:

- FPT_PHP.3/CoreTSF and FPT_EMSEC.1/CoreTSF protect secret cryptographic keys processed in the IC Card Reader against disclosure by physical attacks or by emanation (PCI A7).
- FPT_PHP.3/ICCardReader (PCI D1) protect the IC Card Reader against the physical tampering.
- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).
- FDP_IFC.1/ICCardReader and FDP_IFF.1/ICCardReader enforce that the IC Card Reader receives the Ciphertext PLAIN_PIN, deciphers it and sends it to the IC Card if PED and IC Card Reader are not integrated into the one tamper-responsive boundary (PCI D4.2). FDP_IFC.1/IC Card Reader and FDP_IFF.1/ICCardReader enforce that

the IC Card Reader receives the Cleartext PLAIN_PIN and sends it to the IC Card if PED and IC Card Reader are integrated into one tamper-responsive boundary (PCI D4.4). The IC Card Reader does not send PLAIN_PIN to any other entity than the IC Card. The IC Card Reader does not send PLAIN_PIN_SK (if any) to any entity (PCI B14).

- FDP_RIP.1/ICCardReader prevents unwanted knowledge of secret data upon the de-allocation of the resources from sensitive objects. Especially PLAIN_PIN is deleted immediately after being sent to the IC Card Reader and temporary cryptographic keys (PCI B6).
- FDP_ITT.1/ICCardReader prevents the disclosure of PLAIN_PIN and PLAIN_PIN_SK in the IC Card Reader.
- With FMT_MSA.3/PLAIN_PIN, FMT_MSA.1/PLAIN_PIN, FMT_SMR.1/PLAIN_PIN and FIA_UID.1/PLAIN_PIN security attributes are managed and roles are assigned.
- According to FCS_COP.1, PIN decipherment is performed following ISO 9564 (PCI B10, CAS B10a, PCI B12, PCI D4.1, PCI D4.2, PCI D4.4).
- According to FDP_ITC.2 also the import of cryptographic keys is according to ISO 11568 and/or ANSI X9.24 and ANSI TR-31. Therefore state-of-the-art cryptography for cryptographic means is provided (PCI B11). The cryptographic key import is supported by FTP_ITC.1 and FPT_TDC.1.

489 **O.PaymentTransaction**

490 Rationale:

- FDP_ITT.1/POI_DATA protects Payment Transaction Data and POI Management Data when it is transferred between physically separated parts of the POI (CAS G1.2 and CAS G1.3).
- FDP_ITT.1/POI_DATA protects the disclosure of POI_SK when it is transferred between physically separated parts of the POI (CAS G4).
- FDP_UIT.1/MAN_DAT protects POI Management Data at the external lines of the POI against modification (CAS G1.3).
- FDP_UIT.1/PAY_DAT provides means to protect Payment Transaction Data at the external lines of the POI against modification (CAS G1.1).
- FDP_UCT.1/POI_DATA provides means to protect Payment Transaction Data at the external lines of the POI against disclosure (CAS G1.1).
- FIA_API.1/POI_DATA provides means to prove the identity of the POI (CAS G1.1).
- FDP_ACC.1/POI_DATA and FDP_ACF.1/POI_DATA prevents other application to deceive the Cardholder during execution of the payment application (CAS G2.3).
- FTP_ITC.1/POI_DATA provides the communication channel to protect data at the external lines against disclosure.

- FDP_RIP.1/POI_DATA ensures that Middle TSF secret data is no longer accessible once used.

491 **O.POISW**

492 Rationale:

- FPT_FLS.1/MiddleTSF enforces the MiddleTSF authenticity and integrity by preserving a secure state in case of logical anomalies (CAS G7).
- The protection of the authenticity and integrity of POI_SW and cryptographic keys upon downloading of new components and updating of existing ones is protected due to SFRs FDP_ACC.1/MiddleTSFLoader and FDP_ITC.1/MiddleTSFLoader (CAS G3.1 and CAS G3.2).

493 **O.PaymentApplicationDownload**

494 Rationale:

- The protection of the integrity and authenticity of the payment application code is guaranteed by SFRs FDP_ACC.1/ApplicationLoader and FDP_ITC.1/ApplicationLoader (CAS G3.1 and CAS G3.2).

495 **O.POIApplicationSeparation**

496 Rationale:

- FDP_ACC.1/POI_DATA and FDP_ACF.1/POI_DATA ensures that no other application has unauthorized access to application data of a payment application (CAS G2.1); that it is not possible for another application to interfere with the execution of the payment application by accessing internal data (CAS G2.2) and that it is not be possible for another application to deceive the Cardholder during execution of the payment application (CAS G2.3).
- FDP_RIP.1/POI_DATA ensures that no residual information remains in resources released by the payment application and payment application temporary cryptographic keys (CAS G2.1 to CAS G2.3).

497 **O.PromptControl**

498 Rationale:

- FDP_ACC.1/PEDPromptControl and FDP_ACF.1/PEDPromptControl enforces the protection of PIN prompts and the control of PED display specifying different kinds of implementation (PCI A8.1 to A8.3).

499 **O.MSR**

500 Rationale:

- FPT_PHP.3/MSR leads to resistance against additions, substitutions, or modifications that would allow determination or modification of Magnetic Stripe data to the to the Magnetic Stripe read head and associated hardware and software.

10 Glossary

501 For the Common Criteria oriented sections it is assumed the reader is familiar with the language used. If not, please refer to [CC1]. Those definitions are not repeated here.

Term	Definition
Acquirer	A body acquiring card related transactions from Merchants or other parties, and transmitting these transactions to an Issuer. Usually, an Acquirer is represented by a bank or a financial institution. It can also be any body entitled to acquire card related transactions. It is responsible for the Merchant's compliance to the security rules.
Acquirer Processor	An entity acting for or on behalf of an Acquirer in acquiring card related transactions.
Application	The objective of a POI is to execute applications issued by different application providers (e.g. bank, health, loyalty, government, etc.). A POI may support a multi application environment where several applications are executed simultaneously. The applications use functions provided by the core software of the POI. Applications may consist of data and software. The applications are excluded from the TOE.
Attended	In an attended POI, the Merchant typically provides a member of staff who processes purchased items and provides assistance to the Cardholder in using different payment applications.
(Bank) card	A card issued by a bank (or by a similar institution) to perform payment transactions.
Cardholder	A person using a (bank) card linked to an account to perform payment transactions.
Card payment	Any payment transaction originating from a (bank) card.
CHV	Cardholder Verification Devices (CHV): devices for Cardholder authentication, e.g. a PIN Entry Device (PED). A PED contains a keypad, a display, a Security Module (SM) for PIN encryption and may also include an IC Card Reader. POI as per this Protection Profile includes at least one PED thus allowing Cardholder PIN authentication.
Device	In contrast to distributed architectures an enclosed IT product with external communication interfaces.
Enciphered	Enciphered information.
Enciphered	PIN that is only allowed to leave the POI in enciphered form when

Term	Definition
PIN	it has to be verified by the IC Card or by the Issuer.
Encrypted	Synonym for enciphered.
Firmware	All the software present in the POI at the delivery point.
Hardware Security Module (HSM)	Hardware Security Module. A physically and logically protected hardware device that provides a secure set of cryptographic services.
Issuer	A body issuing cards to Cardholders and authentic transactions initiated by this cards. Usually, an Issuer is represented by a bank or a financial institution. It can also be any body entitled to issue cards.
JIL	Joint Interpretation Library
JTEMS	JIL Terminal Evaluation Methodology Subgroup
Magnetic Stripe	Stripe containing magnetically encoded information.
Merchant	A retailer, or any other person, company, or corporation that agrees to accept (bank) cards in the framework of a contract with an Acquirer. In this Protection Profile the Merchant is also responsible for the TOE in order to protect the TOE against manipulations of the enclosure.
Multi application	A POI that may be used for more than one (card) application.
Offline	Deferred processing without direct communication.
Online	Direct communication between devices with electronic capability (e.g. POI to hosts).
Payment system	Any system processing payment transaction data.
Payment transaction	The act between a Cardholder and a Merchant or Acquirer that results in the exchange of goods or services against payment. For the purpose of this PP also the process performing all steps of a card payment related to the POI.
Payment transaction data	Data that are involved in a payment transaction. Examples for payment transaction data are the amount, the currency, the date of the payment transaction, cryptogram data, the data used to perform Dynamic Data Authentication and stored in the POI, any data which is transferred between Issuer and IC card as card script processing and card management, the Transaction Counter and any other payment transaction data processed by the POI. The Acquirer, the Cardholder and the attended performs operations

Term	Definition
	on the payment transaction data.
PCI	Payment Card Industry. Issuer of security requirements. Jointly formed by MasterCard, Visa and other card payment schemes.
PIN Entry Device (PED)	A device for secure PIN entry and processing. The PED typically consists of a keypad for PIN entry, laid out in a prescribed format, a display for user interaction, a Security Module consisting of a processor and memory performing cryptographic operations with cryptographic keys on PINs and firmware. A PED has a clearly defined physical and logical boundary, and a tamper resistant or tamper evident shell. The PED is a CHV.
Plaintext PIN	PIN which is allowed to be sent to the IC card as plaintext in order to be verified by the IC card.
POI	A POI is an electronic transaction acceptance product. A POI consists of hardware and software and is hosted in an acceptance equipment to enable a Cardholder to perform a card transaction. Thereby the POI may be attended or unattended. POI transactions are IC card based payment transactions as well as any other payment transactions e.g. based on Magnetic Stripe or any non-payment transactions like health, loyalty or government. The TOE is at minimum a POI excluding applications.
POI component	Any physical or logical device involved in a card payment at a POI (e.g. beeper, Card Reader, display, printer, PED).
POI management data	All PIN related or security related data used to manage and administer the POI. Examples for POI Management data are the risk management data, POI Unique Identifier or the Merchant Identifier. The Terminal Administrator performs operations on POI management data.
PIN related data	All items related to the processing of a PIN, i.e. the PIN itself, the PIN encryption keys, etc.
Private key	That key of an entity's asymmetric key pair that should only be used by that entity. In the case of a digital signature scheme, the private key defines the signature function.
Public key	That key of an entity's asymmetric key pair that can be made public. In the case of a digital signature scheme, the public key defines the verification function.
Public key certificate	The public key and identity of an entity together with some other information, rendered unforgeable by signing with the private key of the certification authority that issued that certificate.
Processor	Any organisation or system processing card payment transactions. An entity operating a data or host processing centre as agent of an

Term	Definition
	Acquirer, Issuer or Merchant to process card payment transactions.
Prompts	Prompts are the text shown on the PED display.
Receipt	A hard copy document recording a payment transaction that took place at the POI, with a description that usually includes: date, Merchant name/location, primary account number, amount, and reference number.
Reconciliation	An exchange of messages between two institutions (Acquirer, Issuer or their agents) to reach agreement on financial totals.
Retailer protocol	Protocol used between the sale system (electronic cash register, vending unit, service station infrastructure,..) and the POI.
Reversal	Cancellation of a previous transaction. There might be manual as well as automatic reversals.
Secret (cryptographic) key	A cryptographic key used with symmetric cryptographic techniques and usable only by a set of specified entities.
Sensitive data	Data that must be protected against unauthorized disclosure, alteration or destruction, especially PINs and secret and private cryptographic keys. Depending on the context of the functional requirement sensitive data may be restricted to Plaintext PIN or to Ciphertext PIN and to a subset of cryptographic keys.
Sensitive functions	Sensitive functions are those functions that process sensitive data such as cryptographic keys or PINs.
Sensitive services	Sensitive services provide access to the underlying sensitive functions.
Session key	A key established by a key management protocol, which provides security services to data transferred between the parties. A single protocol execution may establish multiple session keys, e.g., an encryption key and a MAC key.
Settlement	A transfer of funds to complete one or more prior transactions made, subject to final accounting and corresponding to reconciliation advices.
Script	A command or string of commands transmitted by the Issuer to the terminal for the purpose of being sent serially to the IC card.
Secure Application Module (SAM)	See Security Module.
Secure software	All software that are involved in the secure handling of IC card payment transaction, i.e. PIN encryption, parameter and software authentication, card and transaction data protection, etc.
Security Mod-	Any (physical or logical) device that manages secret cryptographic

Term	Definition
ule (SM)	keys and cryptographic functions and performs cryptographic operations using keys that have a justified level of protection (e.g. a Hardware Security Modules (HSM) or an external Security Application Module (SAM) for a purse application (PSAM)).
Security related data	All items, other than PIN related data, related to security protection of the payment transaction. E.g. critical parameters, cryptographic keys, etc.
Tamper-resistant	A characteristic that provides passive physical protection against an attack.
Tamper-Responsive	A characteristic that provides an active response to the detection of an attack, thereby preventing a success.
Terminal	A POI is a terminal providing a man-machine to a human via display and keypad.
Terminal Management System (TMS)	A system used to administrate (installation, maintenance) a set of POIs. Used by a terminal manager.

11 Annex – CAS to Common Criteria

11.1 CAS Security Requirements

Class	CAS Security Requirements	Number
CORE	The PED uses tamper detection and response mechanisms which cause the PED to become immediately inoperable and results in the automatic and immediate erasure of any secret information which may be stored in the PED. These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams) and using ventilation openings and there is not any demonstrable way to disable or defeat the mechanisms and insert a pin disclosing bug or gain access to secret information without requiring an attack potential of at least 25 per PED, exclusive of the IC Card Reader, for identification and initial exploitation as defined in Appendix B of the PCI POS PED DTRs. and (Note: The replacement of both the front and rear casing shall be considered as part of any attack scenario).	PCI A1.1
CORE	Failure of a single security mechanism does not compromise PED security. Protection against a threat is based on a combination of at least two independent security mechanisms.	PCI A1.2
CORE	If the PED or ICC reader[4] permits access to internal areas (e.g., for service or maintenance), then it is not possible using this access area to insert a pin disclosing bug. Immediate access to sensitive data such as PIN or cryptographic data is either prevented by the design of the internal areas (e.g., by enclosing components with sensitive data into tamper resistant/responsive enclosures), or it has a mechanism so that access to internal areas causes the immediate erasure of sensitive data.	PCI A2
CORE	The security of the PED is not compromised by altering: - Environmental conditions. - Operational conditions (An example includes subjecting the PED to temperatures	PCI A3

[4] The "**or**" in the term "PED **or** ICC reader" in this requirement and the following ones is a logical or. If the security property mentioned depends on design properties of the PED and the IC Card Reader, either independently or together, the requirement must be met by each of the two devices.

Class	CAS Security Requirements	Number
	or operating voltages outside the stated operating ranges).	
CORE	Sensitive functions or information are only used in the protected area(s) of the PED. Sensitive information and functions dealing with sensitive information are protected from modification without requiring an attack potential of at least 25 per PED, excluding the IC Card Reader, for identification and first exploitation as defined in Appendix B of PCI PED Derived Test Requirements.	PCI A4
CORE	If PIN entry is accompanied by audible tones, then the tone for each entered PIN digit is indistinguishable from the tone for any other entered PIN digit.	PCI A5
CORE	There is no feasible way to determine any entered and internally transmitted PIN digit by monitoring sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring, even with the cooperation of the terminal operator or sales clerk without the requiring an attack potential of at least 25 per PED to defeat or circumvent as defined in Appendix B of PCI PED Derived Test Requirements.	PCI A6
CORE	To determine any PIN-security-related cryptographic key resident in the PED or ICC reader, by penetration of the PED or ICC reader and/or by monitoring emanations from the PED or ICC reader (including power fluctuations) requires an attack potential of at least 35 for identification and first exploitation as defined in Appendix B of PCI PED Derived Test Requirements.	PCI A7 (high protection of IC Card Reader optional within "CAS only"
CORE	If the PED has a keypad that can be used to enter non-PIN data, then at least <u>one</u> of the following statements A8.x must be true. (S*tatements A8.1 and A8.2 are intended to be met by the vendor controlling the means of authorizing prompt changes. A8.3 is the option that is intended to allow third parties to control the means of authorization.)*	PCI A8
	All prompts for non-PIN data entry are under the control of the cryptographic unit of the PED and requiring an attack potential of at least 16 per PED to circumvent for identification and first exploitation as defined in Appendix B of PCI PED Derived Test Requirements. If the prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of	PCI A8.1

Class	CAS Security Requirements	Number
	the prompts or improper use of the prompts are prevented, or	
	The unauthorized alteration of prompts for non-PIN data entry into the PIN entry key pad such that PINs are compromised, i.e., by prompting for the PIN entry when the output is not encrypted, cannot occur without requiring an attack potential of at least 16 per PED for identification and first exploitation as defined in Appendix B of PCI PED Derived Test Requirements, or	PCI A8.2
	For active display devices, cryptographically based controls are utilized to control the PED display and PED usage such that it is infeasible for an entity not possessing the unlocking mechanism to alter the display and to allow the output of unencrypted PIN data from the PED. The controls provide for unique accountability and utilize key sizes appropriate for the algorithm(s) in question. Key management techniques and other control mechanisms are defined and include appropriate application of the principles of dual control and split knowledge.	PCI A8.3
CORE	The PED provides a means to deter visual observation of PIN values as they are being entered by the Cardholder.	PCI A9
PLUS	The PED must provide privacy shielding according to [EPC Shield]. Note: The acquirer is the responsible party to assure, that the installation of the PED is according to the requirements defined in [EPC Shield].	CAS A9.a
CORE	The design of the PED or ICC reader is such that it is not practical to construct a duplicate PED or ICC reader from commercially available components. For example, the casing used to house the device's electronic components is not commonly available.	PCI A10
CORE	It is not feasible to penetrate the PED to make any additions, substitutions, or modifications to the Magnetic Stripe Read head and associated hardware or software, in order to determine or modify Magnetic Stripe track data, without requiring an attack potential of at least 14 (Optional requirement).	PCI A11 (an option within "CAS only")
CORE	The PED performs a self-test, which includes integrity and authenticity tests as addressed in PCI B4, upon start up and at least once per day to check firmware, security	PCI B1

Class	CAS Security Requirements	Number
	mechanisms for signs of tampering, and whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fail in a secure manner.	
CORE	The PED's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the PED outputting the clear text PIN or other sensitive information.	PCI B2
CORE	The Firmware, and any changes thereafter, has been inspected and reviewed using a documented and auditable process, and certified as being free from hidden and unauthorized or undocumented functions.	PCI B3
PLUS	The review of the PED firmware must be performed by a testing laboratory.	CAS B3.a
CORE	If the PED allows updates of firmware, the device cryptographically authenticates the software integrity and if the authenticity is not confirmed, the software update is rejected and deleted.	PCI B4
CORE	The PED never displays the entered PIN digits. Any array related to PIN entry displays only non-significant symbols, i.e., asterisks.	PCI B5
CORE	Sensitive information shall not be present any longer or used more often than strictly necessary. Online PINs are encrypted within the PED immediately after PIN entry is complete and has been signified as such by the Cardholder. The PED must automatically clear its internal buffers when either: - The transaction is completed, or - The PED has timed-out waiting for the response from the Cardholder or merchant.	PCI B6
PLUS	If the PIN (offline or online) needs to be encrypted, it shall be encrypted immediately.	CAS B6.a
CORE	Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as Cryptographic Keys, Pins and Passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive information.	PCI B7
CORE	To minimize the risks from unauthorized use of sensitive services, limits on the number of actions that can be per-	PCI B8

Class	CAS Security Requirements	Number
	formed and a time limit shall be imposed, after which the PED is forced to return to its normal mode.	
CORE	If random numbers are generated by the PED in connection with security over sensitive data then, the random number generator has been assessed to ensure it is generating numbers sufficiently unpredictable.	PCI B9
PCI	The PED has characteristics that prevent or significantly deter the use of a device for exhaustive PIN determination.	PCI B10
CAS	The PED has characteristics that prevent the use of a device for exhaustive PIN determination.	CAS B10.a
CORE	The key-management techniques implemented in the PED conform to ISO 11568 and/or ANSI X9.24. Key management techniques must support ANSI TR-31 or an equivalent methodology for maintaining the TDEA key bundle.	PCI B11
PCI	The PIN encryption technique implemented in the PED is a technique included in ISO 9564.	PCI B12
CORE	It is not possible to encrypt or decrypt any arbitrary data using any PIN encrypting key or key encrypting key contained in the PED. The PED must enforce that data keys, key encipherment keys, and PIN encryption keys, have different values.	PCI B13
CORE	There is no mechanism in the PED that would allow the outputting of a private or secret clear-text key or cleartext PIN, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a clear-text key from a component of high security into a component of lesser security.	PCI B14
CORE	The entry of any other transaction data must be separate from the PIN entry process, avoiding the accidental display of a Cardholder PIN on the PED display. If other data and the PIN are entered on the same keypad, then the data entry and the PIN entry shall be clearly separate operations.	PCI B15
CORE	If the PED can hold multiple PIN encryption keys and if the key to be used to encrypt the PIN can be externally selected, then the PED prohibits unauthorized key replacement and key misuse.	PCI C1
CORE	It is not feasible to penetrate the IC Card Reader to make any additions, substitutions, or modifications to either the IC Card Reader's hardware or software, in order to determine or modify any sensitive data, without requiring an at-	PCI D1

Class	CAS Security Requirements	Number
	tack potential of at least 16. Note: The IC Card Reader may consist of areas of different protection levels, e.g. the areas of the IC card interface itself, and the area holding retraced cards.	
CORE	The slot of the ICC reader into which the IC card is inserted does not have sufficient space to hold a PIN-disclosing "bug" when a card is inserted, nor can it feasibly be enlarged to provide space for a PIN-disclosing "bug." It is not possible for both an IC card and any other foreign object to reside within the card insertion slot.	PCI D2.1
CORE	The opening for the insertion of the IC card is in full view of the Cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.	PCI D2.2
CORE	The ICC reader is constructed so that wires running out of the slot of the IC Card Reader to a recorder or a transmitter (an external bug) can be observed by the Cardholder.	PCI D3
CORE	PIN protection during transmission within the PED (at least must comply):	PCI D4
	If the PED and IC Card Reader are not integrated into the same secure module, and the Cardholder verification method (i.e., the IC card requires) is determined to be enciphered PIN, then the PIN block shall be enciphered between the PED and the IC Card Reader using either an authenticated encipherment key or the IC card, or in accordance with ISO 9564.	PCI D4.1
	If the PED and the IC Card Reader are not integrated into the same secure module, and the Cardholder verification method is determined to be a plaintext PIN, then the PIN block shall be enciphered from the PED to the IC Card Reader (the IC Card Reader will the decipher the PIN for transmission in plaintext to the IC card) in accordance with ISO 9564.	PCI D4.2
	If the PED and the IC Card Reader are integrated and the Cardholder verification method is determined to be an enciphered PIN, then the PIN block shall be enciphered using an authenticated encipherment key of the IC card.	PCI D4.3
	If the PED and the IC Card Reader are integrated and the Cardholder verification method is determined to be a plaintext PIN, then the encipherment is not required if the PIN block is transmitted wholly through a protected	PCI D4.4

Class	CAS Security Requirements	Number
	environment (as defined in ISO 9564). If the plaintext PIN is transmitted to the IC Card Reader through an unprotected environment, then the PIN block shall be enciphered in accordance with ISO 9564.	
CORE	Change-control procedures are in place so that any intended security-relevant change to the physical or logical capabilities of the POI causes a re-certification of the device under the Physical Security Requirements or the Logical Security Requirements of this document. The detailed evaluation and change procedures are described in a additional document.	PCI E1
PLUS	Requirement PCI E1, whose scope is the PED, is extended to cover all POI security-related components. More precisely, the subject of this requirement is any security-related changes to the physical or logical capabilities of the POI; a change is security-related if it affects the security protections needed to comply with al PCI plus security CAS requirements.	CAS E1.a
CORE	The certified POI firmware is protected and stored in such a manner as to preclude unauthorized modification, e.g., using dual control or standardized cryptographic authentication procedures.	PCI E2
PLUS	Requirement PCI E2, whose scope is the PED, is extended to cover all POI security-related components. More precisely, the subject of this requirement is the protection and storage of the software in the POI security-related components.	CAS E2.a
CORE	The POI is assembled in a manner that the components used in the authenticating process are those components that were certified by the Physical Security Requirements evaluation, and that unauthorized substitutions have not been made. The vendor shall confirm this by giving an integration statement.	PCI E3
PLUS	Requirement E3, whose scope is the PED, is extended to cover all POI security-related components.	CAS E3.a
CORE	Production software that is loaded to devices at the time of manufacture is transported, stored, and used under the principle of dual control, preventing unauthorized modifications and/or substitutions.	PCI E4
PLUS	Requirement E4, whose scope is the PED, is extended to cover all POI security-related components.	CAS E4.a

Class	CAS Security Requirements	Number
CORE	Subsequent to production but prior to shipment from the manufacturer's facility, the PED and any of its components are stored in protected, access-controlled area or sealed within tamper-evident packaging to prevent undetected unauthorized access to the device or its components.	PCI E5
PLUS	Requirement E5, whose scope is the PED, is extended to cover all POI security-related components.	CAS E5.a
CORE	If the PED will be authenticated at the Key Loading Facility by means of secret information placed in the device during manufacturing, then this secret information is unique to each PED, unknown and unpredictable to any person, and installed in the PED under dual control to ensure that it is not disclosed during installation.	PCI E6
PLUS	Requirement E6, whose scope is the PED, is extended to cover all POI security-related components.	CAS E6.a
PLUS	Authentication at the initial Key Loading Facility. Vendors must comply with all requirements of PCI E7.	CAS E7
PLUS	If the manufacturer is not in charge of initial-key-loading he must provide means to the initial-key-loading facility to assure the authenticity of the POI security-related components for himself.	CAS E7.1
PLUS	If the manufacturer is not in charge of initial-key-loading he must provide means to the initial-key-loading facility to assure the verification of the authenticity of the POI security-related components.	CAS E7.2
PLUS	Security measures during development and maintenance of POI security related components. The manufacturer must write a development security documentation, which describes all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity of the design and implementation of the POI security-related components in their development environment. The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the POI security-related components. The evidence shall justify that the security measures provide the necessary level of protection to maintain the integrity of the POI security-related components.	CAS E8
PLUS	All PCI and CAS E requirements must be checked via a site visit.	CAS E9

Class	CAS Security Requirements	Number
CORE	The PED is shipped from the manufacturer's facility to the initial-key-loading facility, and stored en route, under auditable controls that can account for the location of every PED at every point.	PCI F1
PLUS	Requirement F1, whose scope is the PED, is extended to cover all POI security-related components.	CAS F1.a
CORE	Procedures are in place to transfer accountability for the device from the manufacturer to the initial-key-loading facility.	PCI F2
PLUS	Requirement F2, whose scope is the PED, is extended to cover all POI security-related components.	CAS F2.a
CORE	While in transit from the manufacturer's facility to external facilities, the device is: - Shipped and stored in tamper-evident packaging; and/or, - Shipped and stored containing a secret that is immediately and automatically erased if any physical or functional alteration to the device is attempted, that can be verified by the initial-key-loading facility, but that cannot feasibly be determined by unauthorized personnel.	PCI F3
PLUS	Requirement F3, whose scope is the PED, is extended to cover all POI security-related components.	CAS F3.a
PLUS	Each POI security-related component shall have a unique visible identifier affixed to it.	CAS F4
PLUS	The vendor must provide a manual, which provides instructions for the operational management of the POI. This includes instructions for recording the whole life cycle of the POI security-related components and of the way those components are integrated into a single POI, e.g.: - data on production and personalisation, - physical/chronological whereabouts, - repair and maintenance, - removal from operation, - loss or theft.	CAS F5
PLUS	Authenticity and integrity of payment transactions. Vendors must comply with all requirements of G1.	CAS G1
PLUS	The POI must have the capacity to protect communications over external communication channels, meaning that POI security components must provide cryptographic means: - To protect all transactions data sent or received by the POI against modification	CAS G1.1

Class	CAS Security Requirements	Number
	- To protect all transaction data sent or received by the POI against disclosure - For the POI to be uniquely authenticated by the external entity it communicates with.	
PLUS	The transaction/accounting data shall be handled with authenticity and integrity in the POI.	CAS G1.2
PLUS	POI management data must be provided to the POI in an authentic way and must be protected against unauthorized change.	CAS G1.3
PLUS	Application integrity via application separation. Vendors must comply with all requirements of CAS G2.	CAS G2
PLUS	The security of payment application in the POI must not be impacted by any other application. Payment application isolation shall be ensured: no other application shall have unauthorized access to payment application data (any data: transaction data, management data, non-PIN keys, encrypted PIN)	CAS G2.1
PLUS	The security of payment application in the POI must not be impacted by any other application. Payment application isolation shall be ensured: it shall not be possible for another application to interfere with the execution of the payment application, by accessing internal data (such as state machine or internal variables).	CAS G2.2
PLUS	Payment application isolation shall be ensured: it shall not be possible for another application to deceive the Cardholder during execution of the payment application, by accessing Cardholder communication interface (e.g. display, beeper, printer) used by the payment application.	CAS G2.3
PLUS	Authenticity and integrity of POI software. Vendors must comply with all requirements of G3.	CAS G3
PLUS	POI software must be provided to the POI in an authentic way and must be protected against unauthorized change.	CAS G.3.1
PLUS	If the POI implements software updates, a POI security-related component cryptographically authenticates the software integrity and it the authenticity is not confirmed, the software update is rejected or all secret cryptographic keys are erased.	CAS G3.2
PLUS	To determine any non-PIN secret key in a POI security-related components, by any means, including penetration and including crypto-analysis, requires an attack potential of at least 16 for identification and initial exploitation as	CAS G4

Class	CAS Security Requirements	Number
	defined in Appendix B of the PCI POS DTRs.	
PLUS	To defeat a mechanism (hardware or software) in a POI security-related component, by any means, including modification of public keys, requires an attack potential of at least 16 for identification and initial exploitation as defined in Appendix B of the PCI POS DTRs.	CAS G5
PLUS	The key management techniques implemented in a POI security-related component conform to ISO 11568 and/or ANSI X9.24 Note: This requirement does not supplement PCI B11 whose scope is the PED.	CAS G6
PLUS	The functionality of a POI security-related component shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in a breach of the security requirements.	CAS G7

11.2 Mapping from CAS to SFRs and SARs

502 The following table shows the mapping between CAS requirements from [CASPOI] and security requirements in this PP. All links except links to AVA_POI can be traced back to the statement of the requirements in this PP. Links to AVA_POI are addressed in [POI CEM].

CAS-requirement	SFR	SAR
PCI A1.1	FPT_PHP.3/CoreTSF	
PCI A1.2		ADV_ARC.1
PCI A2		ADV_ARC.1
PCI A3	FPT_PHP.3/CoreTSF	
PCI A4		ADV_ARC.1
PCI A5	FPT_EMSEC.1/PIN_ENTRY	
PCI A6	FPT_EMSEC.1/PIN_ENTRY	
PCI A7	FPT_PHP.3/CoreTSF, FPT_EMSEC.1/CoreTSF	
PCI A8.1	FDP_ACC.1/PEDPromptControl, FDP_ACF.1/PEDPromptControl,	ADV_ARC.1
PCI A8.2	FDP_ACC.1/PEDPromptControl, FDP_ACF.1/PEDPromptControl	
PCI A8.3	FDP_ACC.1/PEDPromptControl, FDP_ACF.1/PEDPromptControl	
PCI A9	Outside the CC evaluation (objective for the environment)	
CAS A9.a		
PCI A10		ADV_ARC.1
PCI A11	FPT_PHP.3/MSR	
PCI B1	FPT_TST.1/ PEDMiddleTSF, FPT_FLS.1/ PEDMiddleTSF, FPT_TST.1/CoreTSF, FPT_FLS.1/CoreTSF	
PCI B2	FDP_ITC.1/PEDMiddleTSFLoader, FPT_FLS.1/ PEDMiddleTSF, FPT_FLS.1/CoreTSF, FDP_ITC.1/CoreTSFLoader	

CAS-requirement	SFR	SAR
PCI B3		ALC_CMS.2
CAS B3.a	Covered by the CC evaluation	
PCI B4	FDP_ITC.1/CoreTSFLoader, FDP_ITC.1/PEDMiddleTSFLoader	
PCI B5	FPT_EMSEC.1/PIN_ENTRY	
PCI B6	FDP_IFF.1/ENC_PIN, FDP_RIP.1/ENC_PIN, FDP_RIP.1/PLAIN_PIN, FDP_RIP.1/ICCardReader	
CAS B6.a	FDP_IFF.1/ENC_PIN	
PCI B7	FIA_UAU.2/PIN_ENTRY	
PCI B8	FTA_SSL.3/PIN_ENTRY	
PCI B9	FCS_RND.1	
PCI B10	FDP_IFF.1/ENC_PIN, FCS_COP.1	
CAS B10.a	FDP_IFF.1/ENC_PIN, FCS_COP.1	
PCI B11	FDP_ITC.2, FTP_ITC.1, FPT_TDC.1	
PCI B12	FCS_COP.1	
PCI B13	FDP_IFF.1/ENC_PIN	
PCI B14	FDP_IFF.1/ENC_PIN, FDP_IFF.1/PLAIN_PIN, FDP_IFF.1/ICCardReader	
PCI B15	FDP_ITC.1/PIN_ENTRY	
PCI C1	FTP_TRP.1/ENC_PIN	
PCI D1	FPT_PHP.3/ICCardReader	ADV_ARC.1
PCI D2.1		ADV_ARC.1
PCI D2.2		ADV, ARC.1 AGD_OPE.1
PCI D3		ADV_ARC.1
PCI D4.1	FDP_IFF.1/ENC_PIN, FCS_COP.1	
PCI D4.2	FDP_IFF.1/PLAIN_PIN,	

CAS-requirement	SFR	SAR
	FDP_IFF.1/ICCardReader, FCS_COP.1	
PCI D4.3	FDP_IFF.1/ENC_PIN	
PCI D4.4	FDP_IFF.1/PLAIN_PIN, FDP_IFF.1/ICCard Reader, FCS_COP.1	
PCI E1		Re-evaluation issues are out of scope. The PP stands by CC maintenance process.
CAS E1.a		
PCI E2		ALC_DVS.2
CAS E2.a		
PCI E3		ALC_DVS.2
CAS E3.a		
PCI E4		ALC_DVS.2
CAS E4.a		
PCI E5		ALC_DVS.2
CAS E5.a		
PCI E6		ALC_DVS.2
CAS E6.a		
CAS E7		ALC_DVS.2
CAS E7.1		
CAS E7.2		
CAS E8		ALC_DVS.2
CAS E9		ALC_DVS.2
PCI F1		ALC_DVS.2
CAS F1.a		
PCI F2		ALC_DVS.2
CAS F2.a		
PCI F3		ALC_DVS.2
CAS F3.a		
CAS F4		ALC_CMC.2
CAS F5		AGD_OPE.1

CAS-requirement	SFR	SAR
CAS G1.1	FDP_UIT.1/PAY_DAT, FDP_UCT.1/POI_DATA, FIA_API.1/POI_DATA, FTP_ITC.1/POI_DATA	
CAS G1.2	FDP_ITT.1/POI_DATA	
CAS G1.3	FDP_ITT.1/POI_DATA , FDP_UIT.1/MAN_DAT	
CAS G2.1	FDP_RIP.1/POI_DATA, FDP_ACF.1/POI_DATA	ADV_ARC.1
CAS G2.2	FDP_RIP.1/POI_DATA, FDP_ACF.1/POI_DATA	ADV_ARC.1
CAS G2.3	FDP_RIP.1/POI_DATA, FDP_ACF.1/POI_DATA	ADV_ARC.1
CAS G3.1	FDP_ITC.1/MiddleTSFLoader FDP_ITC.1/ApplicationLoader	
CAS G3.2	FDP_ITC.1/MiddleTSFLoader FDP_ITC.1/ApplicationLoader	
CAS G4	FDP_ITT.1/POI_DATA, FDP_UCT.1/POI_DATA, FTP_ITC.1/POI_DATA	
CAS G5	Covered by the CC evaluation	
CAS G6	FDP_ITC.2, FTP_ITC.1, FPT_TDC.1	
CAS G7	FPT_FLS.1/MiddleTSF	

12 Annex – Relationship between AVA_POI and AVA_VAN.2 families

The relationship between AVA_VAN.2 and the requirements of the extended AVA_POI family relies on the interpretation of CC "Basic" attack potential as within the limits of "POI-Basic", defined in [POI AttackPot] , and on the nature of the additions introduced in the extended family.

We assume that the points needed to reach Basic level in the context of POI evaluation are lower or equal than the points needed to reach the POI-Basic level. This assumption does not affect the generality of the argumentation since both Basic and POI-Basic are the lowest levels in the attack potential scales.

Let us show that each AVA_POI requirement is a refinement of AVA_VAN.2 for the POI components selected in the instantiation of AVA_POI.1.1D. Note that AVA_POI.1, AVA_POI.2, AVA_POI.3 and AVA_POI.4 differ only in the attack potential level assumed for an attacker, POI-Basic, POI-Low, POI-Moderate and POI-High, which are strictly increasing. Hence it is enough to show that AVA_POI.1 refines AVA_VAN.2 for the selected POI components:

- AVA_POI.1.1D: This is the same as AVA_VAN.2.1D, restricted to the selected POI components.
- AVA_POI.1.2D: This is an additional element, without counterpart in AVA_VAN.2, that allows to require implementation representation information and the mapping to SFRs to be used by the evaluator during the vulnerability analysis (cf. AVA_POI.1.3E). Formally, this element is a refinement of AVA_VAN.2.1D.
- AVA_POI.1.1C: This is the same as AVA_VAN.2.1C, restricted to the selected POI components
- AVA_POI.1.1E: This is the same as AVA_VAN.2.1E.
- AVA_POI.1.2E: This is the same as AVA_VAN.2.2E, restricted to the selected POI components.
- AVA_POI.1.3E: This is a refinement of AVA_VAN.2.3E, restricted to the selected POI components, that introduces the use of the available implementation representation and mapping to SFRs during the vulnerabilities analysis.
- AVA_POI.1.4E: This is a refinement of AVA_VAN.2.4E, restricted to the selected POI components, where POI-Basic attack potential replaces Basic attack potential. By assumption Basic attack potential is weaker or equal than POI-Basic attack potential level, hence the new requirement is stronger than the original one.

In EAL POI, each POI component in the scope of the evaluation is addressed by at least one AVA_POI instance: POI components belong to one of the TSF parts Core TSF Keys, Core TSF, PED Middle TSF, Middle TSF or MSR and each of these parts are addressed by at least one instance of AVA_POI. Hence, the set of AVA_POI instances included in EAL POI constitutes a refinement of AVA_VAN.2 applied to the whole POI.