Point of Interaction
Protection Profile

Date: 6th March 2015
Version: 4.0

History table

Version	Comments
4.0	Update from last published version 2.0. Includes new security requirements from [EPC B4], in particular addition of the “Open Protocols package” and the “SRED module”

Table of contents

Table of figures

Table of tables

1 Protection Profile Introduction

1 This document defines six base Protection Profiles dedicated to payment terminals, each for a different terminal variant. The first three of these are PED-ONLY applicable to PIN Entry Devices (PED), and POI-COMPREHENSIVE and POI-CHIP-ONLY applicable to Point of Interaction (POI). The second set of three base PPs consists of the same three variants, but in each case enhanced by a package called "Open protocol package". How this enhancement is done, is explained in section 2.1 later on.

2 In the following, "this Protection Profile" stands for the Protection Profile collection composed of these six base Protection Profiles. In the later text of this PP, many definitions are only described for the first three of these base PPs, since these definitions are not changed by the addition of the "Open protocol package".

3 In addition to these six base PPs a module in the sense of [PP Mod] the SRED PP-Module is defined, which may be added to four of the six base PPs listed above. How this is done, is explained in section 2.1 later on.

1.1 Protection Profile Identification

1.1.1 Identification of PED-ONLY base PP

Title	Point of Interaction Protection Profile – PED-ONLY base PP
Identification	ANSSI-CC-PP-POI-PED-ONLY
Authors	Sandro Amendola, SRC Security Research & Consulting GmbH Carolina Lavatelli, Trusted Labs Tony Boswell, SiVenture on behalf of OSeC (Open Standards for Security and Certification)
Version	4.0
Publication Date	6th March, 2015
Sponsor	ANSSI
CC Version	3.1 Revision 4

1.1.2 Identification of POI-COMPREHENSIVE base PP

Title	Point of Interaction Protection Profile – COMPREHENSIVE base PP
Identification	ANSSI-CC-PP-POI-COMPREHENSIVE
Authors	Sandro Amendola, SRC Security Research & Consulting GmbH Carolina Lavatelli, Trusted Labs Tony Boswell, SiVenture on behalf of OSeC (Open Standards for Security and Certification)
Version	4.0
Publication Date	6th March, 2015
Sponsor	ANSSI
CC Version	3.1 Revision 4

1.1.3 Identification of POI-CHIP-ONLY base PP

Title	Point of Interaction Protection Profile – POI-CHIP-ONLY base PP
Identification	ANSSI-CC-PP-POI-CHIP-ONLY
Authors	Sandro Amendola, SRC Security Research & Consulting GmbH Carolina Lavatelli, Trusted Labs Tony Boswell, SiVenture on behalf of OSeC (Open Standards for Security and Certification)
Version	4.0
Publication Date	6th March, 2015
Sponsor	ANSSI
CC Version	3.1 Revision 4

1.1.4 Identification of SRED PP Module (SRED PP-Module)

Title	Point of Interaction Protection Profile – SRED PP Module
Identification	ANSSI-CC-PP-POI-SRED-PP-Module
Authors	Carolina Lavatelli, Guillaume Tétu, Trusted Labs on behalf of OSeC (Open Standards for Security and Certification)
Version	4.0
Publication Date	6th March, 2015
Sponsor	ANSSI
CC Version	3.1 Revision 4

1.1.5 Identification of the Package SFR-supporting features related to Open Protocols

Title	Point of Interaction Protection Profile – Package of SFR-supporting features related to Open Protocols
Identification	ANSSI-CC-PP-POI-Open-Protocols
Authors	Sandro Amendola, SRC Security Research & Consulting GmbH Carolina Lavatelli, Trusted Labs Tony Boswell, SiVenture on behalf of OSeC (Open Standards for Security and Certification)
Version	4.0
Publication Date	6th March, 2015
Sponsor	ANSSI
CC Version	3.1 Revision 4

Note that the three base PPs derived from the three base PPs already defined in sections 1.1.1, 1.1.2 and 1.1.3 by adding this "Open protocol package" can now be identified uniquely as follows:

- ANSSI-CC-PP-POI-PED-ONLY + ANSSI-CC-PP-POI-Open-Protocols,
- ANSSI-CC-PP-POI-COMPREHENSIVE + ANSSI-CC-PP-POI-Open-Protocols,
- ANSSI-CC-PP-POI-CHIP-ONLY + ANSSI-CC-PP-POI-Open-Protocols.

Note also that the four configurations derived from the base PPs by adding the "SRED PP module" can be identified uniquely as follows:

- ANSSI-CC-PP-POI-PED-ONLY + ANSSI-CC-PP-POI-SRED-PP-Module,
- ANSSI-CC-PP-POI-COMPREHENSIVE + ANSSI-CC-PP-POI-SRED-PP-Module,
- ANSSI-CC-PP-POI-PED-ONLY + ANSSI-CC-PP-POI-Open-Protocols + ANSSI-CC-PP-POI-SRED-PP-Module,
- ANSSI-CC-PP-POI-COMPREHENSIVE + ANSSI-CC-PP-POI-Open-Protocols + ANSSI-CC-PP-POI-SRED-PP-Module.,

Note that the "SRED PP module" can neither be used with the "ANSSI-CC-PP-POI-CHIP-ONLY" base PP nor with the "ANSSI-CC-PP-POI-CHIP-ONLY + ANSSI-CC-PP-POI-Open-Protocols" base PP.

Since there are six base PPs and four configurations using the "SRED PP module", an ST author can claim one of ten possible variants.

1.2 Protection Profile Presentation

4 This Protection Profile (PP) was developed by the Open Standards for Security and Certification (OSeC) body 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. European Payment Council (EPC) security requirements [EPC B4], chap. 2.6 - which include Payment Card Industry Payment Transaction Security (PCI POS PTS v4.0) requirements as well as security requirements on payment transaction data and external communication - have been translated into CC functional and assurance security requirements.

5 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.

6 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.

7 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.

8 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.

9 For the optional protection of specific assets a modular approach has been chosen. Thus a selected base PP given in this document can be extended by the 'Secure-Read-and-Exchange-Data (SRED) PP-module defined in section 12. This PP-module covers the set of PCI PTS requirements K which are related to account data protection. Depending on the addressed security problem the vendor may choose this option or not.

10 In addition optional SFR-supporting features related to Open Protocols[1] are provided in the assurance part of this document. The SFR-supporting features are refinements of the assurance components. A base PP can claim the fulfilment of these SFR-supporting fea-

[1] A set of requirements that ensures POI using open security protocols and open communication protocols to access public networks and services do not have public domain vulnerabilities.

tures. Therefore the SFR-supporting features are seen as a package. These SFR-supporting assurance refinements cover the set of PCI PTS requirements F-J. If Open Protocols are used in the TOE then the vendor may chose this option or not.

11 This Protection Profile defines six base PPs, each of them with a particular TOE:

- PED-ONLY base PP: The TOE provides protection for both IC and Magnetic Stripe card based transactions. It does not manage transaction data nor provide any on-line communication facility to an acquirer. The TOE is fully conformant to the set of PCI POS PTS v4.0 requirements A-D, L and M. Note that the TOE of this base PP is the PED part of a POI. This base PP 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 base PP is to support a POI composite evaluation for specific use case scenarios of merchants or other POI vendors. Evaluation against this base PP will not in itself secure common approval across all OSeC member markets[2]. The PED-ONLY base PP is suitable to be extended by the SRED PP-Module according to [PP Mod] in section 12 covering the set of PCI PTS requirements K.
- PED-ONLY and Open protocol base PP: This fully incorporates the PED-ONLY base PP and corresponds to a compliance with the sets of PCI PTS requirements A-D, F-J, L and M. The PED-ONLY and Open protocol base PP extended by the SRED PP-Module in section 12 corresponds to a compliance with the sets of PCI PTS requirements A-D, F-J, K, L and M.
- POI-COMPREHENSIVE base PP: This base PP fully incorporates the PED-ONLY base PP. Therefore the TOE provides protection for both IC and Magnetic Stripe card based transactions and is fully conformant to the set of PCI PTS requirements A-D, L and M. In addition to the PED-ONLY capabilities it provides payment transaction data management and external communication facilities for interaction with the Acquirer defined by OSeC. POI-COMPREHENSIVE is prepared to be extended by the SRED PP-Module according to [PP Mod] in section 12 covering the set of PCI PTS requirements K. The POI-COMPREHENSIVE base PP extended by the SRED PP-Module in section 12 and the Open Protocol SFR-supporting features (if Open Protocols are supported) corresponds to a compliance with PCI PTS requirements A-D, K, L and M and compliance with additional security requirements of other OSeC members.
- The POI-COMPREHENSIVE and Open protocol base PP: This fully incorporates the POI-COMPREHENSIVE base PP. If this base PP is extended by the SRED PP-Module in section 12, it corresponds to a compliance with PCI PTS requirements A-D, F-J, K, L and M and compliance with additional security requirements of other OSeC members. The POI-COMPREHENSIVE and Open Protocol base PP extended by the SRED PP-Module in section 12 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

[2] In other words: The PED-ONLY configuration is meant to support a model, where a PED is used in several different POIs without the need to re-evaluate the PED each time. Approval for a payment system is given only for complete POIs in most cases; therefore the PED may not get an approval of its own, but its CC-certificate may be re-used in the approval process for several POIs.

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-CHIP-ONLY base PP: This TOE provides protection for IC based transactions, payment transaction data management and external communication facilities. The only differences to the POI-COMPREHENSIVE base PP are the absence of hardware security requirements for the protection of the PIN as well as the absence of support for the protection of offline plaintext PIN and for the Magnetic Stripe Reader. The POI-CHIP-ONLY base PP is a subset of the POI-COMPREHENSIVE base PP. Therefore it is not compliant with the POI-COMPREHENSIVE base PP. The aim of this variant is the support of the business needs of payment schemes, which support a chip only environment and are using encrypted PIN only. Note that as a consequence, the POI-CHIP-ONLY base PP does not rely on the robustness of the IC Card Reader. This configuration is intended to lead to a common security certification of payment schemes being in this migration phase. SRED is not expected to be used in combination with the chip-only approach and its definition therefore does not assume the POI-CHIP-ONLY base PP as a possibility.
- POI-CHIP-ONLY and Open protocol base PP: This fully incorporates the POI-CHIP-ONLY base PP and additionally covers the set of PCI PTS requirements F-J. SRED is not expected to be used in combination with the chip-only approach and its definition therefore does not assume the POI-CHIP-ONLY and Open protocol base PP as a possibility.

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

13 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 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.

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

15 This Protection Profile and the packages defined in this document require “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.

16 The evaluation of this Protection Profile has been performed by the French ITSEF Serma Technologies ITSEF. The PP has been certified by French Scheme ANSSI.

1.3 References

[CC1] Common Criteria Part **1**, Version 3.1, Revision 4, CCMB-2012-09-001

[CC2] Common Criteria Part **1**, Version 3.1, Revision 4, CCMB-2012-09-002

[CC3] Common Criteria Part **1**, Version 3.1, Revision 4, CCMB-2012-09-003

[CEM] Common Criteria Evaluation Methodology, Version 3.1, Revision 4, CCMB-2012-09-004

[EPC B4] SEPA CARDS STANDARDISATION (SCS) "VOLUME" 1, Book 4, "Security", Version 6.4.0.40

[PP Mod] CC and CEM addenda / Modular PP, Date: March 2014, Version 1.0, CCDB-2014-03-001

[EMV] EMV Book 1 to 4, Version 4.3

[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] Joint Interpretation Library / Application of Attack Potential to POIs, Version 1.0 (for trial use), Date: 9th June 2011. *Note: POI evaluations shall rely on the current version of this document at the moment of the evaluation.*

[POI PP 2.0] Common Approval Scheme (CAS) / Point of Interaction Protection Profile Date: 26 th November, 2010, Version: 2.0. *Note: This is the preceding version of this PP.*

[POI CEM] Joint Interpretation Library – CEM Refinements for POI Evaluation, Version 1.0, 27th May 2011. *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 Pseudorandom 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 POI PP Framework

17 Chapter 1.2 already gives an overview of the POI PP Framework. However, this chapter gives additional information to understand how a POI evaluation works.

18 The ST author first has to choose one of the three fundamental base PPs, i.e. the PED-ONLY, the POI-COPMREHENSIVE or the POI-CHIP-ONLY one. There is no description of each POI base PPs in separated chapters of the PP, but each chapter includes information for each POI base PPs. This is the same approach as in Version 2.0 of this document.

2.1 "Open Protocol Package"

19 For the SFR-enforcing features related to "Open Protocols" (see foot note 1) the following approach has been chosen: These features are all realised as refinements of the SARs. The refinements are given in chapter 9.2.2 "Refined security assurance requirements" of this document and are clearly marked as "Open Protocol" refinements. These SAR refinements can be seen as a package.

20 In order to include the "Open protocol package", the ST author has to choose one of the base PPs "PED-ONLY and Open protocols", "POI-COPMREHENSIVE and Open protocols" or "POI-CHIP-ONLY and Open protocols". There is no formal method applied in the definition of the "Open Protocol" package. This is simply done by refining corresponding SARs. However, the ST has to claim conformance to the "Open Protocol" package if the package is going to be used. If the ST claims conformance to a base PP including the "Open Protocol" package, the conformance must be strict. The version of the package is given in this document.

21 There is no new assurance component for the evaluation of a Security Target compliant with a POI configuration extended by the SFR-enforcing features. Each of the components in ASE_CCL.1 that apply to a standard PP also applies to the POI configuration extended by the SFR-enforcing features. Indeed, in order to assess the conformity of a Security Target to a POI base PP extended by the SFR-enforcing features, the POI base PP extended by the SFR-enforcing features have to be interpreted as a base PP. Beside the conformance claim the evaluator has to check that all refinements of the SARs are also part of the ST.

2.2 SRED PP-Module

22 The SRED requirements set is defined according to the module approach described in [PP Mod] and the security problem, the SFRs and the SARs are described separately from the chapters describing the POI base PPs. However, the assignment of the protection levels is not described separately but part of the chapters describing the POI base PPs. Thus the chapters describing the POI base PPs have links to the SRED PP-Module.

23 If the SRED requirement set is going to be used the SRED PP-Module must be claimed in the ST. If the SRED PP-Module is to be used, a POI base PP i.e. either POI-COMPREHENSIVE or PED-ONLY, possibly enhanced by the Open protocol package, has to be selected before (POI-CHIP-ONLY is not feasible with SRED). If the ST claims conformance to the chosen POI base PP and the SRED PP-Module the conformance claim shall be strict. See also [PP Mod] for detailed rules on how to use a PP Module.

24 There is no new assurance component for the evaluation of a Security Target compliant with a POI base PP extended by the SRED PP-Module. Each of the components in ASE_CCL.1 that apply to a base PP also applies to the base PP extended by the SRED PP-Module. Indeed, in order to assess the conformity of a Security Target to a base PP extended by the SRED PP-Module, the POI configuration extended by the SRED PP-Module has to be interpreted as a standard PP, following guidance given in chap. 2.6 of [PP Mod].[3]

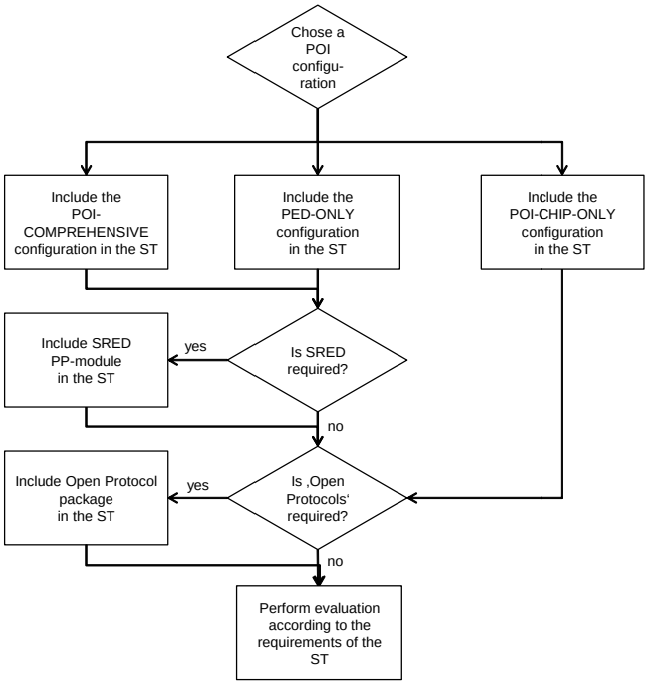


Figure 1: POI Framework – Process Flow

[3] Please note: According to [PP Mod] a configuration is always the result of the inclusion of a module. However, for readability in the following chapters of this document sometimes all possible TOE-variants including the base PPs are called “configuration” in a general sense.

3 TOE Overview

3.1 TOE Type

25 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].

26 The TOE has particular characteristics depending on the base PP:

- PED-ONLY base PP: 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. PED-ONLY is suitable to be extended by the SRED PP-Module in section 12 and/or the Open Protocol SFR-supporting features.
- POI-COMPREHENSIVE base PP: 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-COMPREHENSIVE is suitable to be extended by the SRED PP-Module in section 12 and/or the Open Protocol SFR-supporting features.
- POI-CHIP-ONLY base PP: TOE provides protection for IC Card based transactions, payment transaction data management and external communication facilities. There are no hardware security requirements for the protection of the PIN. Protection of the offline plaintext PIN authentication and of the Magnetic Stripe Reader is out of the scope of the TOE. POI-CHIP-ONLY is suitable to be extended by the Open Protocol SFR-supporting features.

Since the existence of these variants makes this PP harder to read than a PP for a simple TOE type, the reader may want to use the following picture to understand the relation between various definitions and chapters in this PP:

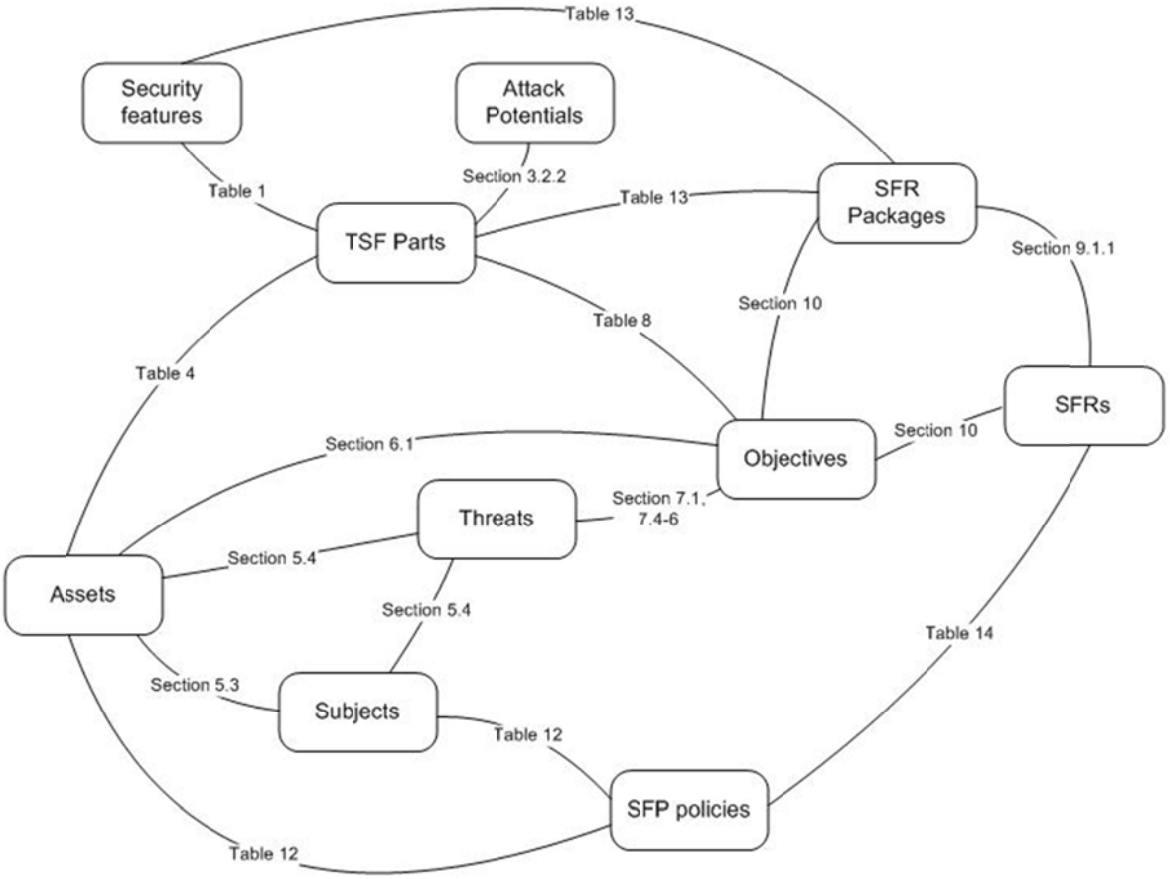


Figure 2: Relations between various definitions and chapters in this PP.

3.2 TOE Security Features

27 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, and 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.

3.2.1 Generic POI

3.2.1.1 Generic Payment Transaction Process

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

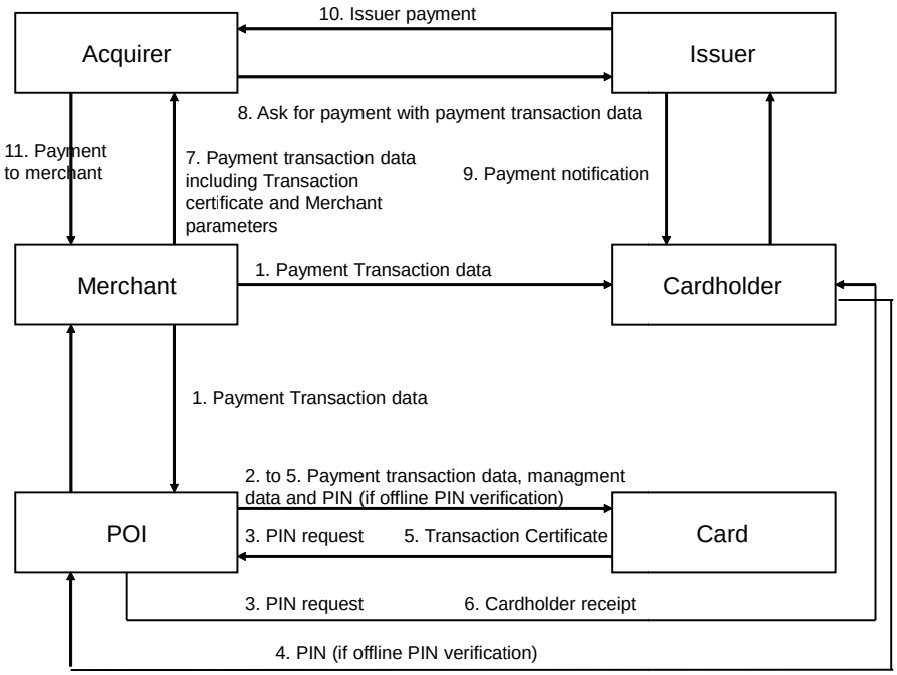


Figure 3: Generic POI Payment Transaction Process

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.

29 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.

3.2.1.2 Generic Terminal Management Process

30 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. The internal state of the POI is changed appropriately (e.g. new parameters are applied or new software is activated). This operation may be performed immediately or deferred in time.

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

3.2.1.3 Generic POI Architecture

31 The generic POI architecture includes the following components:

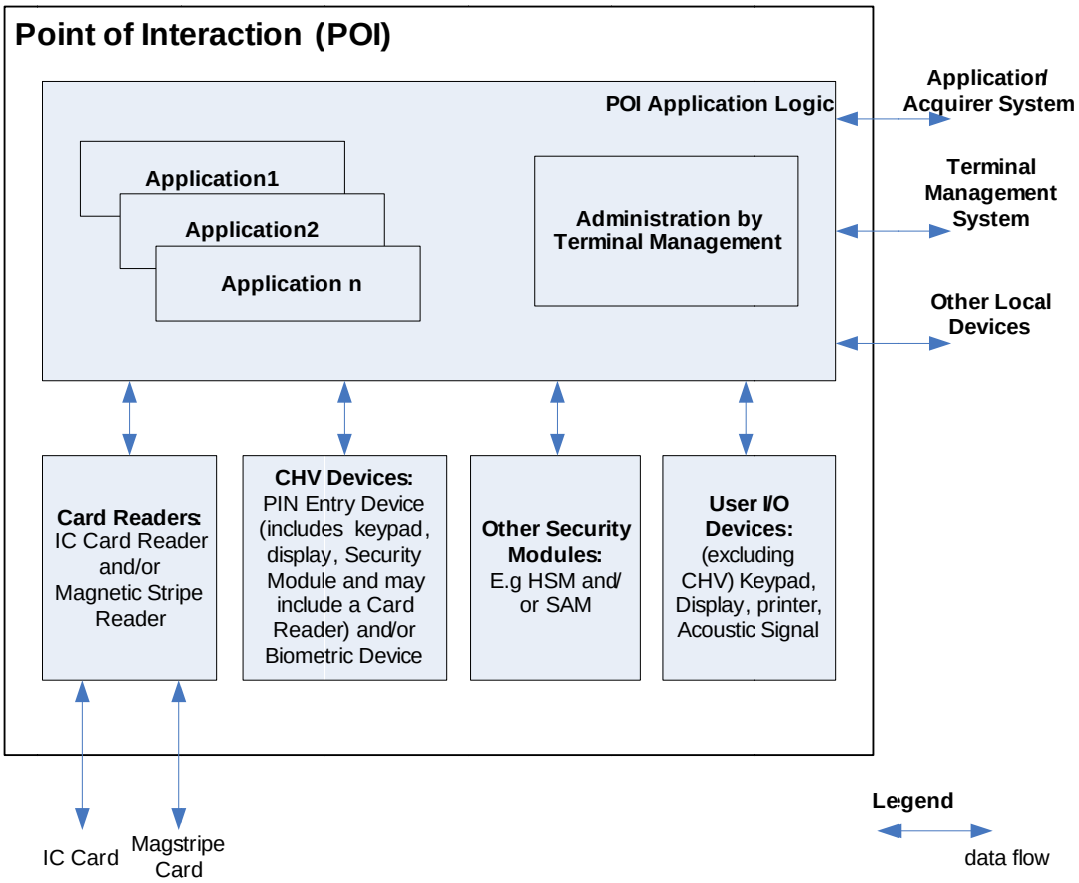


Figure 4: Generic POI Architecture

3.2.1.4 Generic POI Architecture Components

32 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 4) or it may be separated (Card Readers block in the same 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 (PED 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 Module (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; in this case an IC Card Reader SM is needed in addition to the PED SM).

- **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, the 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.

3.2.1.5 POI Example

33 Figure 5, Figure 6 and Figure 7 show the minimum set of components and functions of the TOE in PED-ONLY, POI-COMPREHENSIVE and POI-CHIP-ONLY configurations respectively, with all components in one device, excluding any payment application.

34 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 5: TOE in PED-ONLY configuration

Figure 6: TOE in POI-COMPREHENSIVE configuration

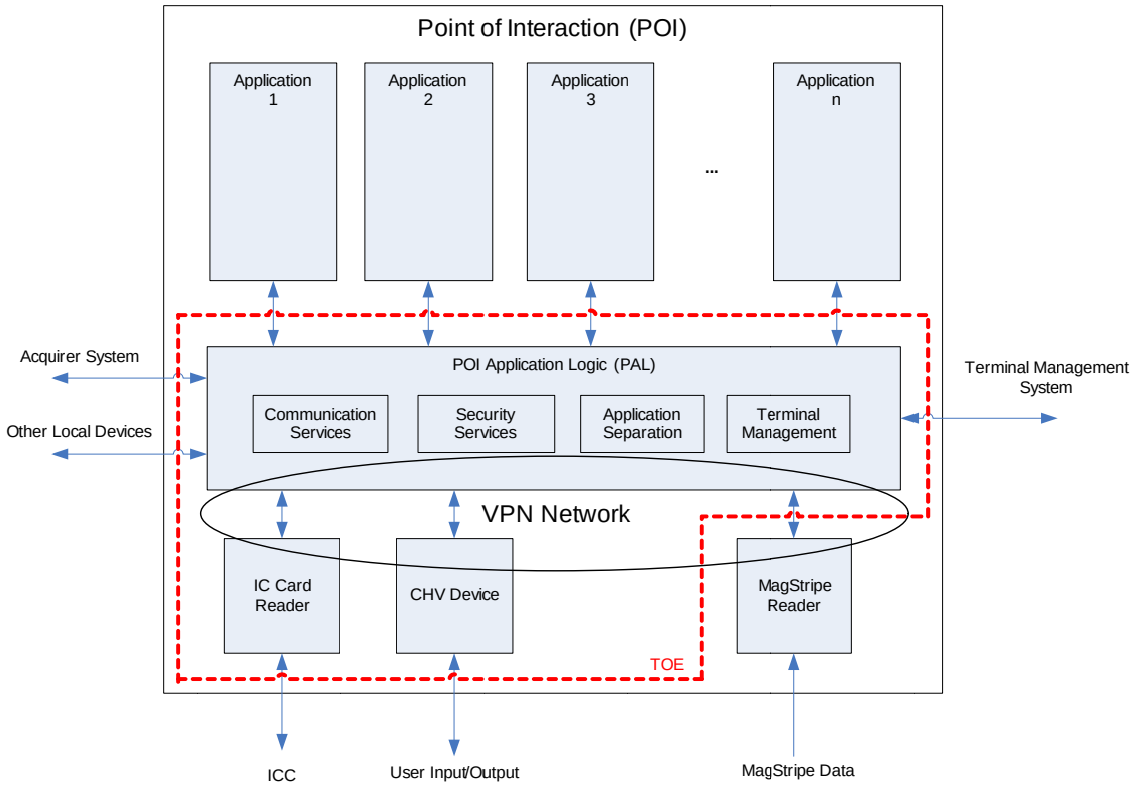


Figure 7: TOE in POI-CHIP-ONLY configuration

3.2.2 Security features

35 The security of the TOE payment transactions[4] 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.

36 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 6:

- Confidentiality of PIN (the asset PIN is defined in section 5.1, 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

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

- Protection of Magnetic Stripe Reader against tampering

37 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-EnhancedLow, POI-Moderate, or POI-High, The precise definition of these protection levels in terms of attack potential is given in [POI AttackPot]. Note that the protection for keys and other cryptographic data (e.g. salt values) used to protect cardholder account data may be set at different levels according to whether the SRED PP-Module is included or not (cf. Figure 9 and Figure 10).

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

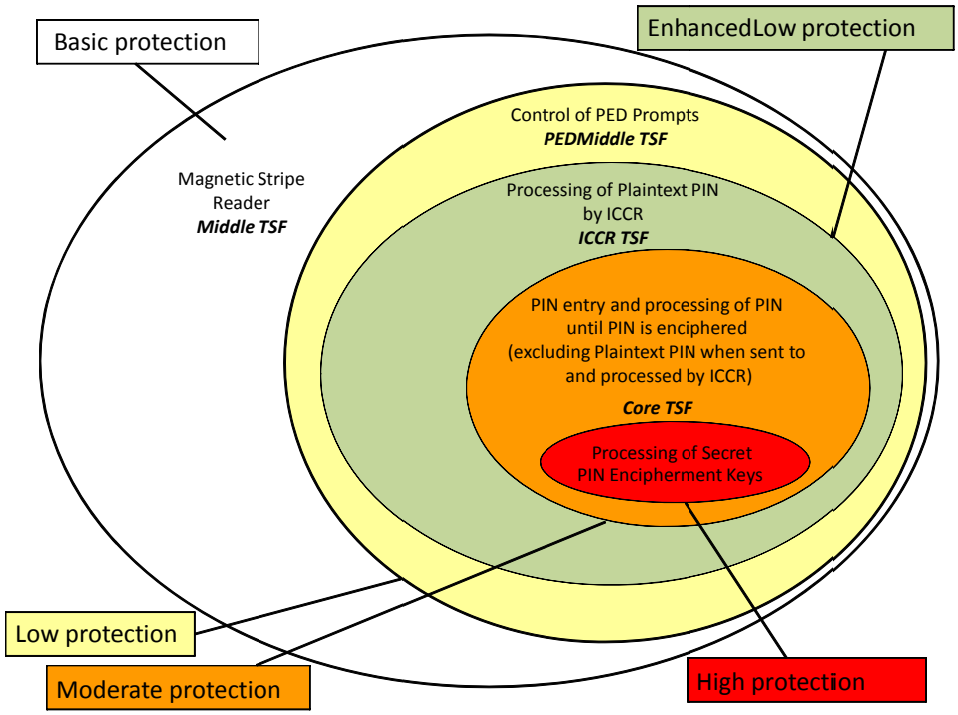


Figure 8: TSF structure in PED-ONLY configuration

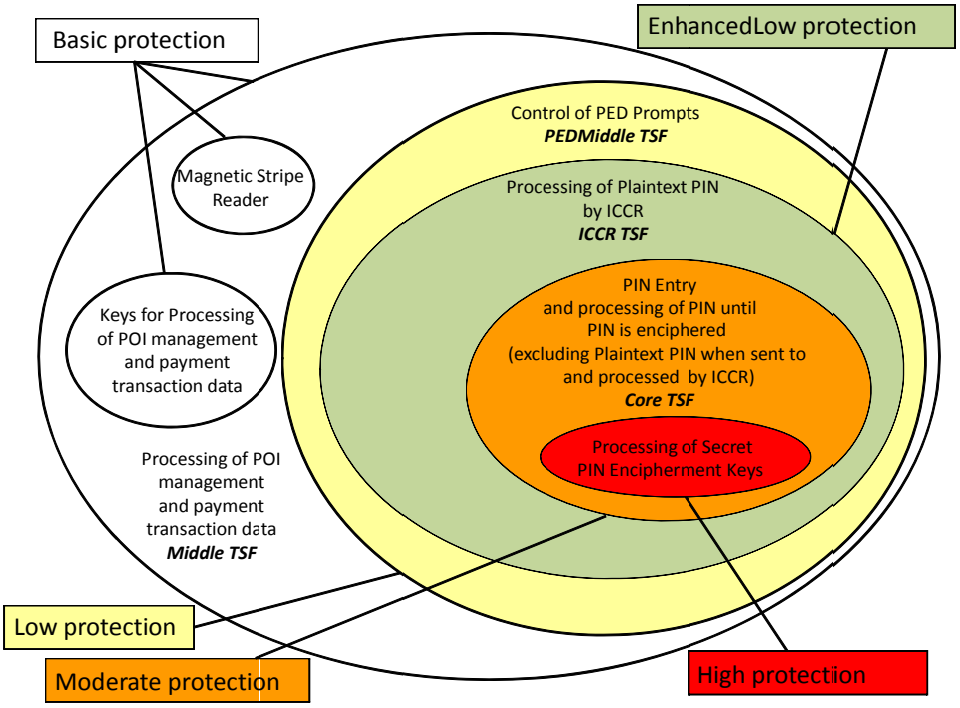


Figure 9: TSF structure in POI-COMPREHENSIVE configuration

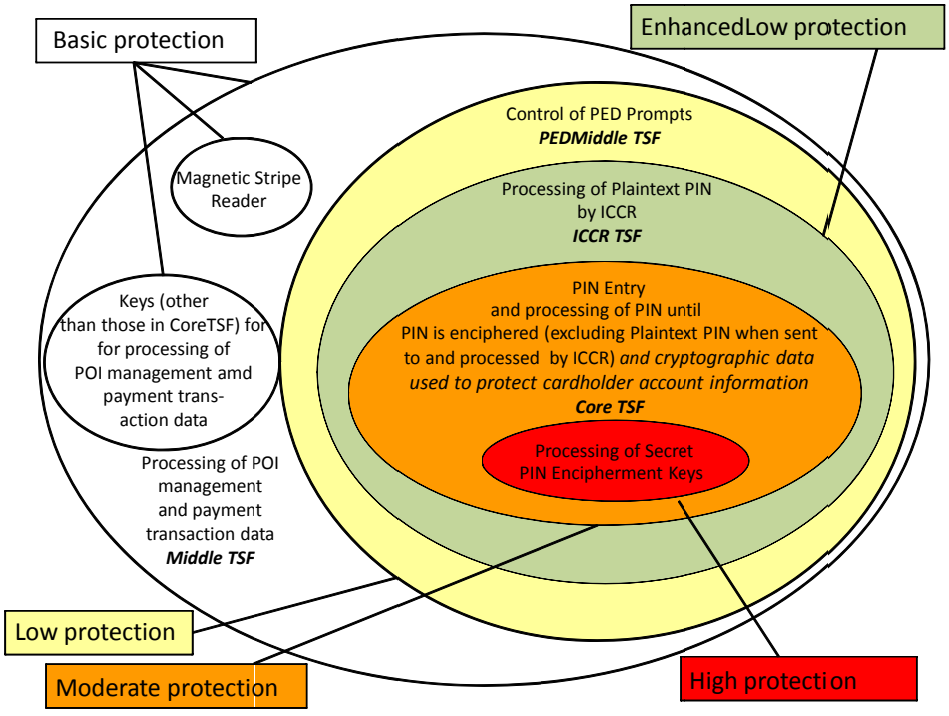


Figure 10: TSF structure in POI-COMPREHENSIVE configuration with adopted SRED PP-Module

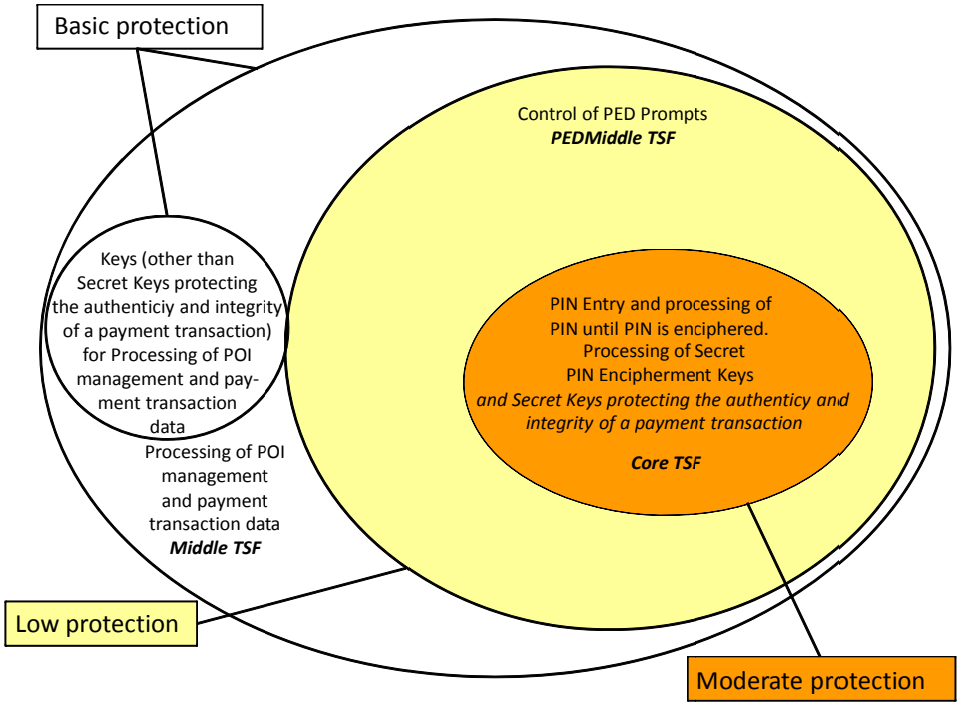


Figure 11: TSF structure in POI-CHIP-ONLY configuration

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

- CoreTSFKeys (CoreTSF PIN encipherment keys) are protected at POI-High level for the PED-ONLY and POI-COMPREHENSIVE configurations.
- CoreTSF contains security features protected at POI-Moderate level. Only for POI-CHIP-ONLY configuration the following holds: PIN encipherment keys are assigned to CoreTSF and thus are protected at POI-Moderate level (instead of POI-High level in PED-ONLY and POI-COMPREHENSIVE configurations).
- Plaintext PIN processing by the IC Card Reader (ICCR) is protected at POI-EnhancedLow level for the PED-ONLY and POI-COMPREHENSIVE configurations. Plaintext PIN processing is not applicable for the POI-CHIP-ONLY configuration.
- PEDMiddleTSF contains security features protected at POI-Low level.
- MiddleTSF (including keys for processing POI management and payment transaction data) contains security features protected at POI-Basic level. If the optional SRED PP-Module in section 12 is adopted in an ST or a conforming PP, then this will result in cryptographic data used to protect cardholder account information (e.g. keys and any salt values used for a surrogate PAN) being protected at POI-Moderate level instead of POI-Basic level, see Figure 10. For POI-CHIP-ONLY configuration only secret keys protecting Payment Transaction Data are protected at POI-Moderate level

against disclosure and thus assigned to CoreTSF, superseding POI-Basic level.

- The Magnetic Stripe Reader (MSR) is protected at POI-Basic level.

40 The definition of the TSF parts takes into account that keys may be protected at higher levels than the individual instances of data that they protect, and that keys for different purposes are protected to different levels.

41 The highest level of protection is given to keys that protect PIN data (with the above described exception for protecting these keys at POI-Moderate in POI-CHIP-ONLY). Although PEDMiddleTSF and MiddleTSF may also contain cryptographic keys and operations, these keys are not used for direct protection of PIN data and thus are protected at a variety of lower levels (as shown in the figures above) according to the type/use of the key, the configuration, and whether the SRED PP-Module is adopted or not.

42 The ICCR TSF, present in PED-ONLY and in POI-COMPREHENSIVE, includes processing of the PIN in plaintext by the IC Card Reader, and this requires POI-EnhancedLow protection (whereas the PIN processed in the PED requires POI-Moderate protection level).

43 The PEDMiddleTSF controls the protection of PED prompts at POI-Low level for all configurations.

44 The MiddleTSF provides processing of POI management and payment transaction data. This is protected at POI-Basic level. Keys used to process POI management and payment transaction data are separately identified (mainly so that they can be distinguished from keys used to protect PINs) but are protected at POI-Basic as for the rest of the MiddleTSF. As pointed out above, certain specific keys related to cardholder account data protection are protected at POI-Moderate level if the SRED PP-Module is chosen.

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

46 The physical boundary 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. Also note that data may be protected at different levels according to the different components in which it is situated.

47 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.

48 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.
13. Tamper-detection/tamper-responsiveness (PED SM in case of CHIP_ONLY).
14. Confidentiality, authenticity and integrity protection of keys (including authenticity and integrity of public keys) used to protect account data in payment transactions.

3.2.2.1 Security features in each base PP

49 Table 1 defines the logical boundaries of each base PP 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 3.2.2.

PP configuration	CoreTSF	CoreTSFKeys	IC Card Reader	PED MiddleTSF	MiddleTSF	MSR
PED-ONLY	1, 2, 3, 4, 6, 7, 11 If SRED is adopted also 14.	Secret PIN encipherment keys for 2, 3, 5, 11	5	10, 11 If SRED is adopted, also 8.		11
POI-COMPREHENSIVE	1, 2, 3, 4, 6, 7, 11 If SRED is adopted 14.	Secret PIN encipherment keys for 2, 3, 5, 11	5	10, 11	8, 9, 12	11
POI-CHIP-ONLY	1, 2, 6, 7, 13 (including secret PIN encipherment keys and secret Payment Transaction Data keys)			10	8, 9, 12	

Table 1: TSF decomposition by base PP

50 The components of a POI described in section 3.2.1.4 may be part of the TOE or not. Some of the local devices may be external in strict terms, but sometimes, e.g. 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 base PP in terms of components associated to TSF parts.

PP configuration	CoreTSF	CoreTSF-Keys	IC Card Reader	PED MiddleTSF	MiddleTSF	MSR
PED-ONLY	PED Keypad If SRED is adopted Account Data SM	IC Card Reader SM, PED SM	IC Card Reader	PED Display PED Keypad	If SRED is adopted: Other POI components handling POI management and payment transaction data.	Magnetic Stripe Reader
POI-COMPREHENSIVE	PED Keypad If SRED is adopted Account Data SM	IC Card Reader SM, PED SM	IC Card Reader	PED Display PED KeyPad	Other POI components	Magnetic Stripe Reader
POI-CHIP-ONLY	PED Keypad, PED SM			PED Display PED Keypad	Other POI components	

Table 2: Physical boundaries of TSF parts by base PP

51 *Application note: The IC Card Reader SM is not required in integrated architectures, where the PIN does not travel outside a logically and physically secure boundary.*

52 *Application note: The POI SM may not exist as a separate component in some POI – it might, for example, be a role fulfilled by the PED SM.*

53 *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, CoreTSF boundary can only be enlarged, with elements from the default PED Middle or MiddleTSF, and PED MiddleTSF can include components in the default MiddleTSF. In any such enlargement, the attack potential levels for an element can only be increased.*

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

54 There is no non-TOE hardware/ software/ firmware available to the TOE.

3.4 TOE Usage

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

- 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-CHIP-ONLY configuration: The TOE is intended to be used by chip-only payment schemes like girocard.

3.5 TOE Life Cycle

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

57 Developer Phase:

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

58 Operational Phase (User Phase):

3. Installation
4. Acquirer Initialisation
5. Use by Merchant and Customer
6. End of life

59 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.

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

61 *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.*

3.5.1 Developer phase

3.5.1.1 Development and Manufacturing

62 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

63 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.

3.5.1.2 Initial Software and Cryptographic Key Loading

64 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.

65 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.

66 The TOE is delivered after the Initial Software and Cryptographic Key Loading.

67 *Application note:*

68 *The ST author shall specify exactly, which software parts and which keys are covered by the Initial Software and Cryptographic Key Loading. While Initial Software loading is optional (if all necessary software and/or firmware is already introduced during hardware production), there will always be an Initial Key Loading procedure*[5].

3.5.2 User phase

69 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.

70 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.

[5] The initial key is the trust anchor, on which all following cryptographically secure key loading is based and cannot be loaded in the field. Note also that the OSeC steering committee has defined the initial key by "The initial key in no cases is the acquirer key, but is the key, which assures the authentication of the hardware device independent of the purpose it is used for later on. " While this statement is about authenticity of the POI, the common property between this and the preceding sentence is the need for an initial secrect, which is needed for the secure implementation of further steps. This initial secret can only be imported in clear text (otherwise its encryption would require another secret, which would then be the initial key). Therefore it cannot be imported in a potentially insecure environment.

3.5.2.1 Installation

71 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.

3.5.2.2 Acquirer Initialisation

72 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.

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

74 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.

75 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).

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

3.5.2.3 Use by merchant and customer

77 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.

78 All security relevant guidance for secure use of the TOE in this phase needs to be addressed in the guidance documentation.

3.5.2.4 End of life

79 The handling of the TOE after its usage may depend on the individual product and is not described in this PP. All security requirements defined in this PP have to be upheld during this phase. If, for example, a TOE can be re-loaded with new software and date to be used in a new context, the ST-author will have to describe, how this is done in a way, which upholds the security of cryptographic keys and other data from the former usage phase (e.g. by securely deleting them).

4 Conformance Claims

4.1 Conformance claim to CC

80 This Protection Profile is conformant to the Common Criteria version 3.1 revision 4:

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

81 The CC Part 2 is extended with the security functional components FCS_RND.1 Generation of random numbers, and FPT_EMSEC.1 TOE emanation.

82 The CC Part 3 is extended with the security assurance components AVA_POI.1 POI vulnerability analysis (cf. section 8.3). By instantiation of AVA_POI.1 this assurance component is applied to TSF parts of different attack potential resistance (cf. 9.2.3). The annex in chapter 14 explains the relationship between AVA_POI and AVA_VAN.2.

83 Note: The definition of AVA_POI has changed compared Version 2.0 of this document although the same name for the family is kept. This could be confusing between devices certified under different versions of the PP. Therefore, if readers of evaluation documentation for a product (for example the according certificate) encounter difficulties in interpreting the AVA-level, they are asked to check what version of the PP applies (so e.g. certifications under this PP will only use AVA_POI.1, whereas those under Version 2.0 of this document used up to AVA_POI.4).

4.2 Conformance claim to a package

84 This Protection Profile is conformant to EAL POI which is defined in section 9.2.

4.3 Conformance claim of the PP

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

4.4 Conformance claim to the PP

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

5 Security problem definition

5.1 Assets

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

88 Some assets only need to be separately identified if a particular configuration is used, or if the SRED PP-Module is adopted – in other cases these assets would either not be present or else would be included as part of another asset. For example, PAN and other SRED Account Data are only distinguished as separate assets if SRED is adopted, otherwise they are considered as part of PAY_DAT. Similarly, POI_PayDatSK is only separated from the rest of POI_SK in the POI-CHIP-ONLY configuration.

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
SRED Account Data partly subset of PAY_DAT (if SRED PP-Module is chosen)	C, 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
E2E_PAN_PK (if SRED PP-Module is chosen)	A, I
TOE_PAN_SK, E2E_PAN_SK (if SRED PP-Module is chosen)	C, A, I
POI_PayDatSK subset of POI_SK	C
CORE_SW	A, I
CORE_HW	A, I
PED_MIDDLE_SW	A, I

Asset	Sensitivity
PED_MIDDLE_HW	A, I
ICCR_SW	A, I
ICCR_HW	A, I
POI_SW	A, I
PAYMENT_APP	A, I

Table 3: Assets sensitivity

89 **PIN**

90 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.

91 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.

92 Sensitivity: Confidentiality.

93 **ENC_PIN[6] (PIN digits that have to be received encrypted by the IC Card or the Issuer) { XE "ENC_PIN (Enciphered PIN)" }**

94 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 3.2.2)

- 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.

95 Sensitivity: Confidentiality.

96 **PLAIN_PIN (PIN digits that have to be received in cleartext by the IC Card) { XE "PLAIN_PIN (Plaintext PIN)" }**

97 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.

[6] A more descriptive name fort this asset would be something like "PIN_TO_BE_ENCRYPTED", because it stands for the plain text PIN, which needs to be encrypted later on. To keep the name short we stay with ENC_PIN.

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

99 Sensitivity: Confidentiality.

100 Ciphertext PLAIN_PIN[7] (in distributed POI architectures, PIN digits that have to be received in cleartext by the IC Card){ XE "Enciphered PLAIN_PIN" }

101 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).

102 Sensitivity: Confidentiality.

103 Application note: This corresponds to items 3 then 5 from the list of security features (cf. section 3.2.2).

104 Cleartext PLAIN_PIN (in integrated POI architectures, PIN digits that have to be received in cleartext by the IC Card){ XE "Plaintext PLAIN_PIN" }

105 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.

106 Sensitivity: Confidentiality.

107 Application note: This corresponds to item 4 from the list of security features (cf. section 3.2.2).

108 **POI_SW (POI software) {** XE "POI_SW (POI software)" **}**

109 Software (code and data) of the MiddleTSF.

110 Sensitivity: Authenticity and Integrity.

111 ICCR_SW

112 Software (code and data) of the ICCR TSF.

113 Sensitivity: Authenticity and Integrity.

114 ICCR_HW

115 Hardware of the ICCR TSF.

116 Sensitivity: Authenticity and Integrity.

[7] In a similar way to the name ENC_PIN (as discussed in footnote 6) the name "Ciphertext PLAIN_PIN" is an abbreviation of its role. This name does not stand for an already encrypted value but for a plain text value that needs to be encrypted for internal transfer in the distributed TOE.

117 **PED_MIDDLE_SW**

118 Software (code and data) of the PEDMiddleTSF.

119 Sensitivity: Authenticity and Integrity.

120 **PED_MIDDLE_HW**

121 Hardware of the PEDMiddleTSF.

122 Sensitivity: Authenticity and Integrity.

123 **CORE_SW { XE "CORE_SW (Core software and hardware)" }**

124 Software (code and data) of the CoreTSF.

125 Sensitivity: Authenticity and Integrity.

126 **CORE_HW**

127 Hardware of the CoreTSF.

128 Sensitivity: Authenticity and Integrity.

129 **MAN_DAT (POI management data) {** XE "MAN_DAT (POI management data)" **}**

130 At least POI Management data are the POI Unique Identifier, the Merchant Identifier and the Acquirer risk management data[8]. The POI_PK is a special kind of MAN_DAT.

131 Sensitivity: Authenticity, Integrity.

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

133 **PAY_DAT (Payment transaction data) {** XE "PAY_DAT (Payment transaction data)" **}**

134 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, and the transaction identifier of the payment transaction. Other data are considered part of PAY_DAT if they are transferred between the Issuer and the IC Card during a payment transaction, for example the encrypted PIN, the cryptogram data, the Authorization Reply as well as card script processing and card management data.

135 The Account Data subset of PAY_DAT includes the full PAN and (if present) any elements of sensitive authentication data associated with the account. The following are also considered to be account data if sent in conjunction with the PAN: cardholder name, expiration date, or service code. Where a surrogate PAN is used and is calculated by a hash of the original PAN combined with a salt, then the value of the salt is also treated as Account Data.

136 Sensitivity: Authenticity and Integrity.

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

137 *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.*

138 **SRED Account Data**

139 If the SRED PP-Module is chosen specific data is addressed to be protected. SRED Account Data consist of PAN, TOE_CLEAR_PAN, TOE_CIPHER_PAN, SURROGATE_PAN and SURROGATE_PAN_SALT see 12, section 12.1.1 Assets**.**

140 Sensitivity: Confidentiality, Authenticity and Integrity.

141 **ENC_PIN_PK (Public ENC_PIN cryptographic keys) {** XE "ENC_PIN_PK (Public ENC_PIN cryptographic keys)" **}**

142 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.

143 Sensitivity: Authenticity and Integrity.

144 **ENC_PIN_SK (Secret/private ENC_PIN cryptographic keys) {** XE "ENC_PIN_SK (Secret/private ENC_PIN cryptographic keys)" **}**

145 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 only needed for decryption, not for encryption of ENC_PIN.

146 Sensitivity: Confidentiality, Authenticity and Integrity.

147 **PED_MIDDLE_PK (Public PEDMiddle cryptographic keys) { XE "POI_PK (Public POI cryptographic keys)" }**

148 PEDMiddleTSF public cryptographic keys used to protect the integrity and authenticity of PED_MIDDLE_SW.

149 Sensitivity: Authenticity and Integrity.

150 **PED_MIDDLE_SK (Secret/private PEDMiddle cryptographic keys) { XE "POI_SK (Secret/private POI cryptographic keys)" }**

151 PEDMiddleTSF secret/private cryptographic keys used to protect the confidentiality, integrity and authenticity of PED_MIDDLE_SW and Prompt Controls.

152 Sensitivity: Confidentiality, Authenticity and Integrity.

153 **POI_PK (Public POI cryptographic keys) {** XE "POI_PK (Public POI cryptographic keys)" **}**

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

155 Sensitivity: Authenticity and Integrity.

156 **E2E_PAN_PK (part of SRED Account Data keys)**

157 If SRED PP-Module is chosen specific public cryptographic keys are addressed to be protected. If SRED PP-Module is chosen for E2E_PAN_PK, see section 12.1.1.

158 Sensitivity: Authenticity and Integrity.

159 **POI_SK (Secret/private POI cryptographic keys) {** XE "POI_SK (Secret/private POI cryptographic keys)" **}**

160 MiddleTSF 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).

161 Sensitivity: Confidentiality, Authenticity and Integrity.

162 **TOE_PAN_SK, E2E_PAN_SK (part of SRED Account Data keys)**

163 If SRED PP-Module is chosen specific secret cryptographic keys are addressed to be protected. If SRED PP-Module is chosen for TOE_PAN_SK and E2E_PAN_SK, see section 12.1.1.

164 Sensitivity: Confidentiality, Authenticity and Integrity.

165 **POI_PayDatSK (Secret/ private POI PAY_DAT Protection Keys)**

166 POI_PayDatSK is defined as a subset of POI_SK in order to allow higher protection in case POI-CHIP-ONLY configuration is claimed. POI_PayDatSK are used to protect the integrity and authenticity of PAY_DAT.

167 Sensitivity: Confidentiality.

168 **PLAIN_PIN_SK (Secret/private PLAIN_PIN cryptographic keys) { XE "POI_SK (Secret/private POI cryptographic keys)" }**

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

170 Sensitivity: Confidentiality, Authenticity and Integrity.

171 *Application note: Note that private keys only needed for decryption, not for encryption of 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.*

172 **Magnetic Stripe Track Data**

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

174 Sensitivity: Confidentiality, Authenticity and Integrity

175 **PAYMENT_APP**

176 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.)

177 Sensitivity: Integrity and Authenticity

5.1.1 Assets in each base PP

178 Table 4 defines the assets of each base PP and the TSF parts they are assigned to. The columns for TSF parts, which do not exist in a given configuration, are marked by a grey background colour. In addition there is no PLAIN_PIN in the POI-CHIP-ONLY configuration, so the corresponding cells also marked with grey background colour.

179 There is no column for the TSF part "MSR TSF", since this is exclusively dedicated to protect the asset "Magnetic stripe track data". This is indicated by including the text "MSR TSF" in the corresponding cell.

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

Asset	PED-ONLY					POI-COMPREHENSIVE					POI-CHIP-ONLY				
	CoreTSF	CoreTSF Keys	IC Card Reader TSF	PEDMiddleTSF	MiddleTSF	CoreTSF	CoreTSFKeys	IC Card Reader TSF	PEDMiddleTSF	MiddleTSF	CoreTSF	CoreTSFKeys	IC Card Reader TSF[9]	PEDMiddleTSF	MiddleTSF
PIN	x					x					x				
ENC_PIN	x	x				x	x				x				
PLAIN_PIN	x		x			x		x							
Cleartext PLAIN_PIN	x					x									
Ciphertext PLAIN_PIN	x	x		x		x	x		x						
POI_SW										x					x
ICCR_SW			x					x							
ICCR_HW			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
SRED Account Data										x					

[9] Note that although an implementation of the POI-CHIP-ONLY configuration will clearly include an IC Card Reader, the configuration does not rely on the security of this component of the TOE, as explained in section 1.2.

Asset	PED-ONLY					POI-COMPREHENSIVE					POI-CHIP-ONLY				
	CoreTSF	CoreTSF Keys	IC Card Reader TSF	PEDMiddleTSF	MiddleTSF	CoreTSF	CoreTSFKeys	IC Card Reader TSF	PEDMiddleTSF	MiddleTSF	CoreTSF	CoreTSFKeys	IC Card Reader TSF[9]	PEDMiddleTSF	MiddleTSF
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
E2E_PAN_PK	x					x									
POI_SK										x					x
TOE_PAN_SK,	x					x									
E2E_PAN_SK	x					x									
PLAIN_PIN_SK		x	x	x			x	x	x						
PAYMENT_APP										x					x
POI_PayDatSK											x				
Magnetic Stripe Track Data	**MSR TSF**					**MSR TSF**									

Table 4: Assets by base PP

5.2 Users

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

182 Users are defined in sections 5.2.1 and 5.2.2. Users applicable to each base PP are defined in section 5.2.3.

5.2.1 Authorised Human Users

183 Cardholder { XE "Cardholder" }

184 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 herself/himself with her/his PIN, confirms the payment transaction and takes the receipt.

185 Attendant { XE "Attendant" }

186 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.

187 **Merchant { XE "Merchant" }**

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

189 **Terminal Administrator { XE "Terminal Administrator" }**

190 The Terminal Administrator maintains the TOE directly by local operations or remotely through a Terminal Management System.

5.2.2 External Entities

191 **Acquirer System { XE "Acquirer system" }**

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

193 **Terminal Management System {** XE "Terminal Management System" **}**

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

195 **IC Card { XE "**Cardholder's IC Card**" }**

196 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.

197 **Magnetic Stripe Card { XE "Cardholder's IC Card" }**

198 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.

199 **Local Device { XE "Local Device" }**

200 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 a private or public network.

201 **Payment Application { XE "Payment Application " }**

202 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.

Risk Manager

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.

5.2.3 Users in each base PP

Table 5 defines the users of each base PP.

User	PED-ONLY	POI-COMPREHENSIVE	POI-CHIP-ONLY
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 base PP

5.3 Subjects

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

Subjects applicable to each base PP are defined in section 5.3.1.

Payment Application Logic (PAL) { XE "Payment Application " }

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.

210 *Application note: The PAL is responsible for providing access to the POI SM (Security Module) that performs cryptographic operations on account data using POI_SK and POI_PK (or the relevant subset assets defined in section 5.1), although as noted in section 3.2.2.1, the POI SM may not be a separate component in all cases.*

211 **Terminal Management**

212 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.

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

214 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.

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

216 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).

217 **Core Loader**

218 The loader downloading CORE_SW into the POI.

219 **PED Middle Loader**

220 The loader downloading PED_MIDDLE_SW into the POI.

221 **Middle Loader**

222 The loader downloading POI_SW into the POI.

223 **ICCR Loader**

224 The loader downloading ICCR_SW into the POI.

225 **Payment Application Loader**

226 Loader for downloading and updating payment applications.

227 **Magnetic Stripe Reader**

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

5.3.1 Subjects in each base PP

229 Table 6 defines the subjects of each base PP.

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

Table 6: Subjects by base PP

5.4 Threats

230 Any user of the TOE may behave as threat agent. The attack paths that implement the threats may involve physical and/or logical means. (Where assets are identified for each threat then these are stated at the highest level: subset assets, such as PAN (a subset of PAY_DAT), are not separately identified.)

231 **T.MerchUsurp (Merchant Identity Usurpation) { XE "T.MerchUsurp (Merchant Identity Usurpation)" }**

232 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.

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

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

235 **T.CardholderUsurpEPIN (Cardholder Identity Usurpation ENC_PIN) { XE "T.CardholderUsurpEPIN (Cardholder Identity Usurpation Encrypted-PIN)" }**

236 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.

237 Fraudsters with POI-High attack potential (for POI-CHIP-ONLY POI-Moderate because only IC card based transactions are accepted) 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.

238 The goal of the attacker is

- either to steal also the IC Card and to perform a transaction based on payment transaction data PAY_DAT with the captured PIN and the stolen IC Card
- or to get a copy of the magnetic stripe data and to perform a transaction with the captured PN and a fake card using the magnetic stripe data.

239 For the POI-CHIP-ONLY configuration hardware attacks on the PINs are not seen as a threat because the combined effort of attacking the hardware of the TOE and to steal the IC Card is considered to be too unlikely in this case (note that there is no magnetic stripe in this case).

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

241 **T.CardholderUsurpCiphPPIN (Cardholder Identity Usurpation Ciphertext PLAIN_PIN){ XE "T.CardholderUsurpEncPPIN (Cardholder Identity Usurpation Encrypted PLAIN_PIN)" }**

242 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.

243 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.

244 Fraudsters with POI-EnhancedLow attack potential level gain unauthorised access to a Cardholder's account by disclosing the Ciphertext PLAIN_PIN via penetrating the IC Card Reader (ICCR_SW, ICCR_HW) making any additions, substitutions or modifications.

245 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.

246 Related assets: Ciphertext PLAIN_PIN, CORE_SW, CORE_HW, ICCR_SW, ICCR_HW, PED_MIDDLE_SW, PED_MIDDLE_HW, PLAIN_PIN_SK, PED_MIDDLE_PK.

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

248 **T.CardholderUsurpClearPPIN (Cardholder Identity Usurpation Cleartext PLAIN_PIN){ XE "T.CardholderUsurpPlainPPIN (Cardholder Identity Usurpation Plaintext PLAIN_PIN)" }**

249 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.

250 Fraudsters with POI-EnhancedLow attack potential level gain unauthorised access to a Cardholder's account by disclosing the Cleartext PLAIN_PIN via penetrating the IC Card Reader (ICCR_SW and ICCR_HW) making any additions, substitutions or modifications.

251 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.

252 Related assets: Cleartext PLAIN_PIN, CORE_SW, CORE_HW, ICCR_SW, ICCR_HW, PED_MIDDLE_SW, PED_MIDDLE_HW, PED_MIDDLE_PK.

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

254 **T.PromptControl (Manipulation of Prompt Control){ XE "T.CardholderUsurpEncPPIN (Cardholder Identity Usurpation Encrypted PLAIN_PIN)" }**

255 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).

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

257 **T.Transaction (Transaction with usurped Cardholder identity) { XE "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.

258 Note that if the SRED PP-Module is adopted then an additional refinement to this threat applies, as specified in 12.

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

260 **T.FundsAmount (Funds transfer other than correct amount) { XE "T.TransAmount (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.

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

262 **T.BadDebt (Account overdraft, bad debt) { XE "T.BadDebt (Account overdraft, bad debt)" }**

263 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.

264 Related assets: POI_SW, MAN_DAT.

265 **T.SecureCommunicationLines{ XE "T.DisclosurePersonalData" }**

266 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.

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

268 *Application note: This is a threat against the services provided by the POI. The assets PAY_DAT and POI_SW are indirectly threatened 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).

269 **T.Magstripe**

270 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.**{ XE "T.DisclosurePersonalData" }**

271 Related assets: Magnetic Stripe Track Data.

272 **T.IllegalCodeInstall**

273 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.

274 Related assets: PAYMENT_APP.

5.4.1 Threats in each base PP

275 Table 7 defines the threats to each base PP.

276 A threat is relevant only for those configurations containing the threatened assets.

Threat	PED-ONLY	POI-COMPREHENSIVE	POI-CHIP-ONLY
T.MerchUsurp		X	X
T.CardholderUsurpEPIN	X	X	X
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 base PP

5.5 Organisational Security Policies

277 **OSP.WellFormedPayApp (Well-formed Payment Applications) { XE "OSP.WellFormedPayApp (Well-formed Payment Applications)" }**

278 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.

279 **OSP.ApplicationSeparation { XE "OSP.AppSeparation" }**

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

281 **OSP.POISurvey**

282 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.

283 **OSP.MerchantSurvey { XE "OSP.MerchantSurvey" }**

284 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.

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

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

287 **OSP.KeyManagement {** XE "OSP.KeyManagement" **}**

288 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.

5.5.1 OSP in each base PP

289 All the OSP listed above apply to each of the base PPs except the OSP.ApplicationSeparation which does not apply to PED-ONLY configuration.

5.6 Assumptions

290 **A.UserEducation { XE "A.UserEducation" }**

291 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.

292 **A.SecureDevices**

293 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.

294 **A.PinAndCardManagement{** XE "A.PinAndCardManagement" **}**

295 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.

5.6.1 Assumptions in each base PP

296 All the assumptions listed above apply to each of the base PPs.

6 Security Objectives

6.1 Security Objectives for the TOE

A1.1 { XE "A1.1" }

A1.2 { XE "A1.2" }

A4 { XE "A4" }

A5 { XE "A5" }

A6 { XE "A6" }

A7 { XE "A7" }

A8 { XE "A8" }

A9 { XE "A9" }

A10 { XE "A10" }

B1 { XE "B1" }

B2 { XE "B2" }

B3 { XE "B3" }

B4 { XE "B4" }

B5 { XE "B5" }

B6 { XE "B6" }

B7 { XE "B7" }

B8 { XE "B8" }

B9 { XE "B9" }

B10 { XE "B10" }

C1 { XE "C1" }

C2 { XE "C2" }

C3 { XE "C3" }

C4 { XE "C4" }

C5 { XE "C5" }

C6 { XE "C6" }

C7 { XE "C7" }

C8 { XE "C8" }

D2 { XE "D2" }

D3 { XE "D3" }

D4.1 { XE "D4.1" }

D4.2 { XE "D4.2" }

D4.3 { XE "D4.3" }

D4.4 { XE "D4.4" }

D5 { XE "D5" }

E1 { XE "E1" }

E2 { XE "E2" }

E3 { XE "E3" }

E4 { XE "E4" }

E4.1 { XE "E4.1" }

E4.2 { XE "E4.2" }

E4.3 { XE "E4.3" }

E5 { XE "E5" }

E6 { XE "E6" }

F1 { XE "F1" }

F1.1 { XE "F1.1" }

F1.2 { XE "F1.2" }

F1.3 { XE "F1.3" }

F1.4 { XE "F1.4" }

F2 { XE "F2" }

G1 { XE "G1" }

G2 { XE "G2" }

G3 { XE "G3" }

G3.1 { XE "G3.1" }

G3.2 { XE "G3.2" }

G3.3 { XE "G3.3" }

G3.4 { XE "G3.4" }

G4 { XE "G4" }

G5 { XE "G5" }

G { XE "G" }

297 **O.PINEntry**

298 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).

299 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.

300 For the POI-CHIP-ONLY configuration PIN entry is only protected by software means, since T.CardholderUsurpEPIN makes an explicit exception for this case.

301 **O.EncPIN**

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

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

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

305 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.

306 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.

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

308 For the POI-CHIP-ONLY configuration tamper-responsive and tamper-detection protection mechanisms do not apply for the protection of ENC_PIN, since T.CardholderUsurpEPIN makes an explicit exception for this case. For same reason, in the POI-CHIP-ONLY configuration described above, tamper-responsive and tamper-detection means apply for ENC_PIN_SK but at a lower level.

309 O.CipherPPIN

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

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

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

313 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.

314 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.

315 *Application note: This objective applies to POI architectures with separated PED and IC Card Reader (e.g. different tamper-responsive boundaries). Other aspects of the separate IC Card Reader are addressed under O.ICCardReader.*

316 O.ClearPPIN

317 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.

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

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

320 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.

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

322 **O.CoreSWHW**

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

324 This objective entails the following derived objectives:

a) The TOE shall check the authenticity and integrity of CORE_SW and CoreTSF 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.

325 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.

326 **O.PEDMiddleSWHW**

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

328 This objective entails the following derived objectives:

a) The TOE shall check the authenticity and integrity of PED_MIDDLE_SW and PEDMiddleTSF 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.

329 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.

330 **O.ICCardReader**

331 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.

332 **O.PaymentTransaction**

333 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.

334 This objective entails the following derived objectives:

a) The TOE shall protect the confidentiality of POI_SK.

b) The TOE shall protect the authenticity and integrity of POI_PK.

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

d) 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.

e) 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 either the Cardholder or the attendant.

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

335 Upon failure of any authenticity and integrity check or upon incorrect execution, the TOE erases any MiddleTSF secret data.

336 In the POI-CHIP-ONLY configuration POI_PayDatSK have in addition to be protected by tamper-responsive and tamper-detection means.

337 *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 and payment transaction data transferred between TOE and Acquirer or TOE and Terminal Management System.*

338 **O.POI_SW{ XE "O.POI_SW_HW (Authentic and integer usage of POI software and related hardware)" }**

339 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 (online authentication).

340 This objective entails the following derived objective:

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

341 Upon failure of any authenticity and integrity check the TOE will make inaccessible any MiddleTSF secret data.

342 **O.PaymentApplicationDownload**

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

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

345 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.

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

347 **O.PromptControl**

348 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.

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

350 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.

6.1.1 Security objectives for the TOE in each base PP

351 The table below defines the objectives applicable to each base PP and shows, which TSF parts contribute to each objective. Note that the TSF part "MSR TSF" has no column of its own, since it only contributes to O.MSR as indicated in the relevant cells.

	PED-ONLY	POI-COMPREHENSIVE	POI-CHIP-ONLY

Objective for the TOE	CoreTSF	CoreTSF Keys	IC Card Reader	PEDMiddleTSF	MiddleTSF	CoreTSF	CoreTSF Keys	IC Card Reader	PEDMiddleTSF	MiddleTSF	CoreTSF	CoreTSF Keys	PEDMiddleTSF	MiddleTSF
O.PINEntry	x					x					x			
O.EncPIN	x	x				x	x				x			
O.CipherPPIN	x	x	x			x	x	x						
O.ClearPPIN	x		x			x		x						
O.CoreSWHW	x	x				x	x				x			
O.PEDMiddleSWHW				x					x				x	
O.ICCardReader			x	x				x						
O.PaymentTransaction										x				x
O.POI_SW										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 base PP

6.2 Security Objectives for the Operational Environment

352 **OE.POISurvey { XE "OE.POI_Survey" }**

353 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.

354 **OE.MerchantSurvey { XE "OE.MerchantSurvey" }**

355 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.

356 **OE.UserEducation { XE "OE.UserEducation" }**

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

358 **OE.SecureDevices { XE "OE.SecureDevices" }**

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

360 **OE.KeyManagement { XE "OE.KeyManagement" }**

361 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.

362 **OE.PinAndCardManagement { XE "OE.PinAndCardManagement" }**

363 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.

364 **OE.WellFormedPayApp { XE "OE.EMV_other (Well-formed Payment Application)" }**

365 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).

366 **OE.LocalDevices { XE "OE.Local_Devices" }**

367 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.

368 *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.

6.2.1 Security objectives for the TOE environment by base PPs

369 All the objectives for the TOE environment listed above apply to each of the base PPs.

7 Rationale between SPD and security objectives

7.1 Threats

370 This section presents generic rationales between threats and objectives that are independent of the base PPs.

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

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

373 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.

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

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

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

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

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

379 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.

380 Manipulation of another Merchant's TOE by attacks on the payment transaction data PAY_DAT is countered by O.PaymentTransaction (Authentic and integrity-protected payment transaction) and O.POI_SW (Authentic and integrity-protected usage of POI software).

381 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.

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

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

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

385 Manipulating the TOE by attacks on the payment transaction data PAY_DAT is countered by O.PaymentTransaction (Authentic and integrity-protected payment transaction), O.POI_SW (Authentic and integrity-protected usage of POI software and related hardware) and O.POIApplicationSeparation (Application Separation).

386 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.

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

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

389 Note that if the SRED PP-Module is adopted then the mapping of T.Transaction to security objectives is extended as described in 12.

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

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

392 The protection of the TOE software already in the TOE is ensured by O.POI_SW.

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

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

395 Manipulating the TOE by attacks on the payment transaction data PAY_DAT is countered by O.PaymentTransaction (Authentic and integrity-protected payment transaction), O.POI_SW (Authentic and integrity-protected usage of POI software and related hardware) and O.POIApplicationSeparation (Application Separation).

396 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.

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

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

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

400 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.

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

402 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.

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

404 **T.SecureCommunicationLines**

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

406 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.POI_SW (Authentic and integrity-protected usage of POI software and related hardware) and O.POIApplicationSeparation (Application Separation).

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

408 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.

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

410 **T.PromptControl**

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

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

7.2 OSP

413 **OSP.WellFormedPayApp**

414 The security objective OE.WellFormedPayApp corresponds to the organisational security policy.

415 **OSP.POISurvey**

416 The security objective OE.POISurvey corresponds directly to the organisational security policy.

417 **OSP.MerchantSurvey**

418 The security objective OE.MerchantSurvey rresponds directly to this organisational security policy.

419 **OSP.KeyManagement**

420 The security objective OE.KeyManagement corresponds to the OSP.

421 **OSP.ApplicationSeparation**

422 The TOE security objective O.POIApplicationSeparation directly implements the organisational security policy OSP.ApplicationSeparation.

7.3 Assumptions

423 **A.UserEducation**

424 The security objective OE.UserEducation corresponds to the assumption.

425 **A.SecureDevices**

426 The security objective OE.SecureDevices corresponds to the assumption.

427 **A.PinAndCardManagement**

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

7.4 Rationale applicable to PED-ONLY configuration

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

430 **T.PromptControl** cf. 7.1

431 **T.CardholderUsurpEPIN** (Cardholder Identity Usurpation ENC_PIN) cf 7.1

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

433 Capturing the Ciphertext PLAIN_PIN when it is processed is countered by O.CipherPPIN (Ciphertext PLAIN_PIN Processing), O.CoreSWHW, O.PEDMiddleSWHW (Authentic and integrity-protected usage of PEDMiddleTSF SW and related hardware) and O.ICCardReader.

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

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

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

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

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

439 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 integrity-protected usage of PEDMiddleTSF SW and related hardware) and O.ICCardReader.

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

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

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

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

444 **T.Magstripe**

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

446 Rationales for the following OSP are provided in section 7.2:

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

447 Rationales for the following assumptions are provided in section 7.3:

- 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.ApplicationSeparation	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.POI_SW																			
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

7.5 Rationale applicable to POI-COMPREHENSIVE configuration

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

449 Rationales for the following threats are provided in section 7.1:

- 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)

450 Rationales for the following threats are provided in section 7.4:

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

451 Rationales for the following OSP are provided in section 7.2:

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

452 Rationales for the following assumptions are provided in section 7.3:

- 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.POI_SW	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

7.6 Rationale applicable to POI-CHIP-ONLY configuration

453 This section provides the rationales applicable to the POI-CHIP-ONLY configuration.

454 Rationales for the following threats are provided in section 7.1:

- 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

455 Rationales for the following OSP are provided in section 7.2:

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

456 Rationales for the following assumptions are provided in section 7.3:

- 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.POI_SW	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-CHIP-ONLY configuration

8 Extended Requirements

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

8.1 Definition of the Family FCS_RND

458 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.

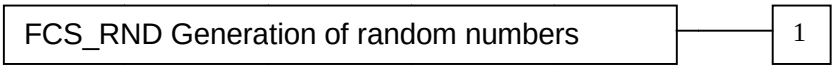
459 The family "Generation of random numbers (FCS_RND)" is specified as follows.

460 FCS_RND Generation of random numbers

461 Family behaviour

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

463 Component levelling:



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

465 Management: FCS_RND.1

466 There are no management activities foreseen.

467 Audit: FCS_RND.1

468 There are no actions defined to be auditable.

FCS_RND.1 Generation of random numbers

469 Hierarchical to: No other components.

470 Dependencies: No dependencies.

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

8.2 Definition of the Family FPT_EMSEC

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

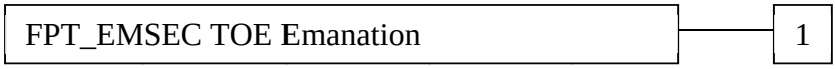
473 The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

474 FPT_EMSEC TOE Emanation

475 Family behaviour:

476 This family defines requirements to mitigate intelligible emanations.

477 Component levelling:



478 FPT_EMSEC.1 TOE emanation

479 Management: FPT_EMSEC.1

480 There are no management activities foreseen.

481 Audit: FPT_EMSEC.1

482 There are no actions defined to be auditable.

FPT_EMSEC.1 TOE emanation

483 Hierarchical to: No other components.

484 Dependencies: No dependencies.

485 **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*].

486 **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*].

8.3 Definition of the Family AVA_POI

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

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

- In contrast to AVA_VAN, the assurance activities for vulnerability assessment do not vary depending on the attack potential.
- Consequently, AVA_POI[10] only includes a single component AVA_POI.1, which is based on AVA_VAN.2 with addition of POI-related specificities.
- The attack potential is not fixed in the definition of the component. The PP/ST author shall directly assign the attack potential that corresponds to the POI or POI components to which the component applies.
- The attack potential calculation table and the admissible attack potentials are defined in [POI AttackPot] which provides also a catalogue of POI-specific attack methods. The minimum attack potential is POI-Basic. 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 and the mapping of SFR into the implementation. 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 vulnerability analysis method for the evaluator.

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

490 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.

491 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.

492 We refer to Section 14 for a detailed explanation of the relationship between AVA_VAN.2 and AVA_POI. **{** XE "AVA_VAN.2/POI_1" **}**

493 **AVA_POI Vulnerability analysis of POI**

494 Objectives

[10] Please note that the definition of AVA_POI has changed compared to Version 2.0 of this document although the same name for the family is kept. In the old version of AVA_POI, a specific attack potential was included in each hierarchic level from AVA_POI.1 to AVA_POI.4; but in the new version there is only a single level (AVA_POI.1) with the attack potential completed as a selection for each iteration. This change might be confusing between devices certified under different versions of the PP. Therefore, if a readers of the evaluation documentation (for example the according certificate) encounter difficulties in interpreting the VAN-level, they are asked to check what version of the PP applies (e.g. certifications under this PP will only use AVA_POI.1, whereas those under Version 2.0 of this document used up to AVA_POI.4).

495 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 TOE assets, data or functionality.

496 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.

497 When more than one instantiation of AVA_POI.1 is used in a PP or ST, to apply to different sets of abstract components, then it may be that the separate instantiations map to the same concrete physical or logical components in a particular TOE (i.e. more than one of the abstract components maps to one of the concrete components). In this case the more demanding requirement applies to the concrete component.

498 Component Levelling

499 AVA_POI includes a single component; the attack potential required by an attacker to identify and exploit the potential vulnerabilities has to be assigned by the PP or ST author within the SAR definition.

AVA_POI Vulnerability analysis of POI	1

AVA_POI.1 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

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

501 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 the attack potential assigned within the requirement definition.

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 [assignment: attack potential equal to or higher than **POI-Basic** attack potential] [selection: with a minimum attack potential for the [assignment: identification phase, exploitation phase, attack potential factor and phase names] of [assignment: value and (where applicable) units], empty].

{ XE "AVA_VAN.2/POI_1" **}**

Application note:

- *The 'empty' value in the selection at the end of AVA_POI.1.4E indicates that if there are no additional constraints on minimum attack potential in either identification or exploitation phase then no text need be added at the end of the element.*
- *If more than one constraint is required at the end of AVA_POI.1.4E, then these may be concatenated with the word "and" between instances of the constaint assignment, e.g. "…with a minimum attack potential of 10 for the exploitation phase and a minimum elapsed time attack potential factor of 8 hours in the exploitation phase."*

9 Security Requirements

9.1 Security Functional Requirements

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

- 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

503 The main SFRs of these packages are mapped to the EPC requirements they implement, either in the text of the SFR or in application notes, or both: EPC requirements that come directly from PCI PTS V4 are referenced with the "PCI" identifier; otherwise, the identifier "EPC PLUS" or "EPC-CHIP-ONLY" is used. The annex in chapter 13.1 recalls the full set of EPC requirements and the annex in chapter 13.2 presents the mapping of EPC requirements to SFR in this Protection Profile.

504 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 9.2.2.31)

505 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 5.3) or SPD users (section 5.2)
- Objects or information are assets (section 5.1)
- Security attributes are assets or subjects properties
- Roles are SPD users (section 4.2)
- Operations are the operations used in EPC requirements

Policy	Entity	Name	Value (for security attributes)	Definition
PIN_ENTRY Information flow control SFP	Subject	Cardholder		5.2.1
		keypad		5.3
	Information	PIN		5.1
		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 SFP	Subject	PED		5.3
		IC Card Reader		5.3
	Information	ENC_PIN		5.1
		ENC_PIN_SK		5.1
	Attribute	encrypted (ENC_PIN)	online	5.1
		encrypted (ENC_PIN)	offline	5.1
		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		5.2.2
		Terminal Administrator		5.2.1
		Risk Manager		5.2.2
	Operation	send		data transfer
PLAIN_PIN Information Flow Control SFP	Subject	PED		5.3
		IC Card Reader		5.3
	Information	PLAIN_PIN		5.1
		PLAIN_PIN_SK		5.1
	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		5.2.2
		Terminal Administrator		5.2.1
	Operation	send		data transfer
ICCardReader Information Flow Control SFP	Subject	IC Card Reader		5.3
	Information	PLAIN_PIN		5.1
		PLAIN_PIN_SK		5.1

Policy	Entity	Name	Value (for security attributes)	Definition
	Role	Terminal Management System		5.2.2
		Terminal Administrator		5.2.1
	Operation	receive, send		data reception and transfer
POI Management and Payment Transaction Data Access Control SFP	Subject	POI and its Payment Application Logic		5.3
	Object	Payment Transaction Data		5.1
		POI Management Data		5.1
		POI_SK		5.1
		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		5.2.2
	Operation	send		data transfer
		receive		data reception
		access		interface access
Core Loader Access Control SFP	Subject	Core Loader		5.3
	Object	CORE_SW		5.1
	Operation	download		data or software download
PED Middle Loader Access Control SFP	Subject	PED Middle Loader		5.3
	Object	PED_MIDDLE_SW		5.1
	Operation	download		data transfer
Payment Application Loader Access Control SFP	Subject	Payment Application Loader		5.3
	Object	PAYMENT_APP		5.1
	Operation	download		data transfer
Middle Loader Access Control SFP	Subject	Middle Loader		5.3
	Object	POI_SW		5.1
	Operation	download		data transfer

Policy	Entity	Name	Value (for security attributes)	Definition
ICCR Loader Access Control SFP	Subject	ICCR Loader		5.3
	Object	ICCR_SW		5.1
	Operation	download		data transfer
PED Prompt Control SFP	Subject	POI components		3.2.1.4
	Object	PED Display		5.3
		PED Keypad		5.3
		Prompts		cf Glossary
		PIN		5.1
		PED_MIDDLE_PK		5.1
		PED_MIDDLE_SK		5.1
	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

9.1.1 Definition of SFR packages

9.1.1.1 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 satisfied by FDP_IFC.1/PIN_ENTRY; 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:

PCIB15: PIN is only allowed to be entered at the 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 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

PCIA11: audible tones during PIN entry, that, if used, could allow to distinguish the entered PIN digits,

PCIA5: sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring,

PCIB5: the entered PIN digits at the display (any array related to PIN entry displays only non-significant symbols, e.g. 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

PCIA11: audible tones, if used,

PCIA5: sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring,

PCIB5: the entered PIN digits at the display (any array related to PIN entry displays only non-significant symbols, e.g., asterisks)

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

Application note:

PCIA5 does not apply in the POI-CHIP-ONLY configuration.

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.

PCIB7: 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 data.

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 also after an imposed time limit. In both cases the PED is forced to return to its normal mode.**

Application note:

PCIB8: To minimize the risks from unauthorized use of sensitive services, limits on the number of actions that can be performed and a time limit imposed, after which the PED is forced to return to its normal mode[11].

9.1.1.2 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.

{ XE "FDP_IFF.1/ENC_PIN" **}**

FDP_IFF.1/ENC_PIN Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control satisfied by FDP_IFC.1/ENC_PIN, FMT_MSA.3 Static attribute initialisation not formally satisfied however justified as follows: The management of the attributes is defined by FMT_MSA.1/ENC_PIN, where certain roles are allowed to manage them. These roles are also responsible for initial values, where applicable.

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).

[11] "Normal mode" means a mode, where use of sensitive functions or services is not possible without new authentication of the user.

PCIB6: 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.

PCID4.1: If the PED encrypting the PIN and the ICC reader are not integrated into the same secure module, and the cardholder verification method is determined to be: Enciphered PIN, the PIN block shall be enciphered between the PED and the ICC reader using either an authenticated encipherment key of the IC card, or in accordance with ISO 9564.

PCID4.3: If the PED encrypting the PIN and the ICC reader are integrated into the same secure module, and the cardholder verification method is determined to be: Enciphered PIN, the PIN block shall be enciphered using an authenticated encipherment key of the IC card.

PCIB10, EPCPlusB10.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.

PCIB13: 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.

PCIB14: 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 or rules based on security attributes the corresponding assignments shall be filled with none.

Validity and purpose are security attributes which are only implicitly used in the rules.

PCIB10, EPCPlusB10.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.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 and of ENC_PIN_SK** to **Risk Manager and [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/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 the Terminal Management System and/or the Terminal Administrator and/or the 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:

PCIB6: Sensitive data shall not be retained 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, e.g., via pressing the enter button. 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/ENC_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:
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 POI.

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 **f**rom **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:
PCIC1: 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.

Note that this is relevant for the online PIN case, usually not for the offline PIN case.

If the PED does not hold multiple PIN encryption keys or if the key to be used to encrypt the PIN cannot 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 in-

terference 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.

9.1.1.3 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 satisfied by FDP_IFC.1/PLAIN_PIN, FMT_MSA.3 Static attribute initialisation not formally satisfied however justified as follows: The management of the attributes is defined by FMT_MSA.1/PLAIN_PIN, where certain roles are allowed to manage them. These roles are also responsible for initial values, where applicable.

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: PCID4.2, PCID4.4] where**

PCID4.2: If the PED and the ICC reader are not integrated into the same secure module, and the cardholder verification method is determined to be: A

Plaintext PIN, the PIN block shall be enciphered from the PED to the ICC reader (the ICC reader will then decipher the PIN for transmission in plaintext to the IC card) in accordance with ISO 9564.

PCID4.4: If the PED and the ICC reader are integrated into the same secure module, and the cardholder verification method is determined to be: A Plaintext PIN, then encipherment is not required if the PIN block is transmitted wholly through a protected environment (as defined in ISO 9564). If the plaintext PIN is transmitted to the ICC reader through an unprotected environment, the PIN block shall be enciphered in accordance with ISO 9564.

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.

PCIB14: 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 or rules based on security attributes the corresponding assignments 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 PCID4.2 or PCID4.4 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:

PCIB6: Sensitive data shall not be retained 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, e.g., via pressing the enter button. 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 **the 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 POI.

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/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/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].**

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.

9.1.1.4 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 satisfied by FDP_IFC.1/ICCardReader,
FMT_MSA.3 Static attribute initialisation not formally satisfied however justified as follows: The management of the attributes is defined by FMT_MSA.1/PLAIN_PIN, where certain roles are allowed to manage them. These roles are also responsible for initial values, where applicable.

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: PCID4.2, PCID4.4] where**

PCID4.2 (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,

PCID4.4 (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.

PCIB14: 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" or "rules based on security attributes" the corresponding assignments shall be filled with "none".

This SFR is related to transfer of PLAIN_PIN mandating the implementation of PCID4.2 or PCID4.4 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:

PCIB6: Sensitive data shall not be retained 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, e.g., via pressing the enter button. 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 corresponding 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.

FDP_ACC.1/ICCRLoader 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/ICCRLoader

FDP_ACC.1.1/ICCRLoader The TSF shall enforce the **ICCR Loader Access Control SFP** on

subject: ICCR Loader

objects: ICCR_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. PLAIN_PIN_SK) or for any other key. The operations are any management operation on IC Card Reader software and data.

If no list of data exist the assignment shall be filled with "none".

FDP_ITC.1/ICCRLoader 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/ICCRLoader
FMT_MSA.3 Static attribute initialisation not satisfied but justified: there are no security at-

tributes to be managed for downloading objects. Terminal Management System decides to update/download them or not.

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

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

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

The ICCR Loader downloads only authentic and integrity-protected 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 ICCR TSF secret data are erased.

PIN encryption keys are only stored in the Security Module of the device or encrypted.

[assignment: additional importation control rules]

Application note:

PCIB2: The functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a the clear-text PIN or other sensitive data.

PCIB4: If cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware 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.

9.1.1.5 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.

{ XE "FDP_IFF.1/POI_DATA" **}**

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:

EPCN2.1: 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).

EPCN2.2: 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).

EPCN2.3: 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.

PCIB17: If the POI supports multiple applications, it must enforce the separation between applications. It must not be possible that one application interferes with or tampers with another application or the OS of the POI including, but not limited to, modifying data objects belonging to another application or the OS.

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.

A Payment Application will be allowed to access POI Management Data and Payment Transaction Data if the Payment Application has access rights 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 or 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.

This is replaced by the following 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 one of these data items is transmitted between physically-separated parts of the TOE.

Application note:

EPCN1.2: Payment Transaction Data shall be handled with authenticity and integrity in the POI (this includes preventing modification of the transaction amount in the TOE after it has been acknowledged by entry of the carcholder's PIN).

EPCN1.3: POI Management Data must be protected against unauthorized change in the POI.

EPCN4: Protection of POI_SK in a POI component against disclosure.

{ XE "FDP_UIT.1/POI_DATA" **}**

FDP_UIT.1/POI_DATA 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.

This is replaced by the following refinement:
FDP_UIT.1.1/POI_DATA The TSF shall enforce the **POI Management and Payment Transaction Data Access Control SFP to transmit and receive POI Management Data and Payment Transaction Data** in a manner protected from **modification** errors.

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

Application note:

The refinements FDP_UIT.1.1 and .1.2 replaces the original FDP_UIT.1.1 above, thus the original element shall not be considered by the author of the ST.

EPCN1.3: 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.

EPCN1.1: 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.

This is replaced by the following 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:

EPCN1.1: 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.

EPCN4: 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.

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 EPCN2.1 to EPCN2.3.

This SFR requires that sensitive information shall not be present any longer or used 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, [assignment: list of functions for which a trusted channel is required]**.

Application note:

The channel is used to protect the confidentiality and authenticity of data.

Contribution to EPCN1.1 and EPCN4.

EPCN1.1: The POI shall provide means for authentication of its unique identifier by an external IT entity that it communicates with.

For unique identification, 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.

9.1.1.6 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 data], 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.

PCIB1: The PED performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fail in a secure manner. The PED must reinitialize memory at least every 24 hours.

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.

PCIB1: The PED performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fail in a secure manner. The PED must reinitialize memory at least every 24 hours.

PCIB2: 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 data.

If no list of additional failure 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 integrity-protected 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 only stored in the Security Module of PED or encrypted.

[assignment: additional importation control rules]

Application note:

PCIB2: 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 data.

PCIB4: If the PED allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware 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.

9.1.1.7 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 data], 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.

PCIB1: The PED performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fail in a secure manner. The PED must reinitialize memory at least every 24 hours.

If no 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.

PCIB1: The PED performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fail in a secure manner. The PED must reinitialize memory at least every 24 hours.

PCIB2: 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 data.

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".

{ XE "FDP_ITC.1/PlainPinMiddleTSFLoader" **}**

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 integrity-protected 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:

PCIB2: 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 data.

PCIB4: If the PED allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware 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.

9.1.1.8 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".

PCIB4.1: The firmware must support the authentication of applications loaded onto the terminal consistent with PCIB4. If the device allows software application and/or configuration updates, the device cryptographically authenticates updates consistent with PCIB4.

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 integrity-protected 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 EPC rule, the phrase "POI software" is interpreted as ***payment application software***

EPCN3.1: POI software must be provided to the POI in an authentic way and must be protected against unauthorized change.

EPCN3.2: 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.

PCIB4.1: The firmware must support the authentication of applications loaded onto the terminal consistent with PCIB4. If the device allows software application and/or configuration updates, the device cryptographically authenticates updates consistent with PCIB4.

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".

{ XE "FDP_ITC.1/MiddleTSFLoader" **}**

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 integrity-protected 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:

EPCN3.1: POI software must be provided to the POI in an authentic way and must be protected against unauthorized change.

EPCN3.2: 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.

EPCN7: 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.

9.1.1.9 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_ACC.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 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. 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: unauthorised modification access to the text of prompts shall always be prevented**.

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

If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: PCIA7, PCIB16, or EPC-CHIP-ONLYB16.

PCIA7 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit.

PCIB16 applies to PEDs that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer.

EPC-CHIP-ONLYB16 only applies for the POI-CHIP-ONLY configuration.

Prompts can be under control of the security module. The security module controls the display. This leads to PCIB16: All prompts for non-PIN data entry are under the control of the cryptographic unit of the device. 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.

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 PCIA7: 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.

Appropriate requirement for POI-CHIP-ONLY is necessary. This leads to EPC-CHIP-ONLYB16: 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.

9.1.1.10 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 Generation of random numbers

Dependencies: No dependencies.

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

Application note:

PCIB9: If random numbers are generated by the PED in connection with security over sensitive data, 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, ICCR TSF) if necessary.

Contribution to PCIB10, EPCPlusB10.a, PCIB12, PCID4.1, PCID4.2 and PCID4.4.

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 (according to the data concerned) by FDP_IFC.1/ENC_PIN or FDP_IFC.1/PLAIN_PIN or FDP_IFC.1/ICCardReader or FDP_ACC.1/POI_DATA because the relevant information flow or 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/Crypto 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, supporting the ANSI TR-31 key derivation methodology or an equivalent methodology for maintaining the TDEA Key Bundle.**

Application note:

Note that this SFR is specifically meant for TDES-keys and their handling. So "User data" in the SFR is to read as "TDES-keys".

The author of the Security Target shall iterate this SFR for each TSF part (CoreTSFKeys, CoreTSF, PEDMiddleTSF, MiddleTSF, ICCR TSF) 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 (i.e. if TDES keys are handled).

Contribution to PCIB11, EPCN6.

FTP_ITC.1/Crypto Inter-TSF trusted channel

Dependencies: No dependencies.

FTP_ITC.1.1/Crypto 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/Crypto The TSF shall permit **[selection: the TSF, another trusted IT product]** to initiate communication via the trusted channel.

FTP_ITC.1.3/Crypto 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. ICCR TSF) if necessary.

Contribution to PCIB11, EPCN6.

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, supporting the ANSI TR-31 key derivation methodology or an equivalent methodology for maintaining the TDEA Key Bundle, and [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 PCIB11, EPCN6.

9.1.1.11 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**

PCIA1: Replacement of the front and rear casing, that shall be considered as part of any attack scenario.

PCIA3: Operational or environmental conditions that are not within the specified PED operating range (e.g temperature or operating voltage outside the state operating range).

PCIA6: 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:

PCIA1: The PED uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the PED, such that it becomes infeasible to recover the sensitive data.

PCIA3: 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.

Where the attack scenario considered requires the installation of a bug (for collecting, storing, processing, and/or transmitting PIN or key data) then this installation is included in the attack potential calculation.

This requirement is not applicable in the POI-CHIP-ONLY configuration. Instead FPT_PHP.3/CHIP-ONLY holds for the POI-CHIP-ONLY configuration.

FPT_EMSEC.1/CoreTSF TOE Emanation

Dependencies: No dependencies.

FPT_EMSEC.1.1/CoreTSF The TOE shall not emit **measurable signals including power fluctuations (PCIA6)** 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) (PCIA6)** to gain access to **PIN encryption keys** and **none**.

Application note:

Supports PCIA6. Recall that CoreTSF shall contain at least the PED keypad and the PIN encryption module (PED Security Module).

This requirement is not applicable in the POI-CHIP-ONLY configuration. Instead FPT_EMSEC.1/CHIP-ONLY holds for the POI-CHIP-ONLY configuration. This holds because of the difference risk analysis where POI-CHIP-ONLY only supports IC card based transcations.

FPT_PHP.3/ICCardReader Resistance to physical attack

Dependencies: No dependencies.

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

PCID1: 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 ICCR TSF.

This requirement is not applicable in the POI-CHIP-ONLY configuration.

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 PCIA9. "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 pro-

tection 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.

This requirement is not applicable in the POI-CHIP-ONLY configuration.

FPT_PHP.3/CHIP-ONLY Resistance to physical attack

Dependencies: No dependencies.

FPT_PHP.3.1/CHIP-ONLY The TSF shall resist **the physical tampering scenarios**

PCIA3: Operational or environmental conditions that are not within the specified PED operating range (e.g temperature or operating voltage outside the state operating range).

EPC-CHIP-ONLYA6: Penetration of the PED to disclose POI_PayDatSK and 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.

Application note:

This requirement is only applicable for the POI_CHIP-ONLY configuration.

Where the attack scenario considered requires the installation of a bug (for collecting, storing, processing, and/or transmitting PIN or key data) then this installation is included in the attack potential calculation.

FPT_EMSEC.1/CHIP-ONLY TOE Emanation

Dependencies: No dependencies.

FPT_EMSEC.1.1/CHIP-ONLY The TOE shall not emit **measurable signals including power fluctuations** in excess of **none** enabling access to **POI_PayDatSK and PIN Encryption Keys** and **none**.

FPT_EMSEC.1.2/CHIP-ONLY The TSF shall ensure **all users** are unable to use the following interface **emanations (including power fluctuations)** to gain access to **POI_PayDatSK and PIN Encryption Keys** and **none**.

Application note:

This requirement is only applicable for the POI-CHIP-ONLY configuration.

9.1.2 Security Functional Requirements in each base PP

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

SFR Package	Security features (see section 3.2.2)	TSF part(s)	PED-ONLY	POI-COMPREHENSIVE	POI-CHIP-ONLY
PIN Entry	1	CoreTSF	X	X	X
ENC_PIN	2	CoreTSFKeys CoreTSF	X	X	X (CoreTSF only)
PLAIN_PIN	3, 4	CoreTSFKeys CoreTSF	X	X	
IC Card Reader	5	CoreTSFKeys IC Card Reader	X	X	
POI_DATA	8, 12	MiddleTSF		X	X
CoreTSF	6, 7(if SRED, also 14)	CoreTSF	X	X	X
PEDMiddleTSF	11 (if SRED also 8)	PEDMiddleTSF	X	X	X
MiddleTSF	9, 12	MiddleTSF		X	X
PED Prompt Control	10	PEDMiddleTSF	X	X	X
Cryptography	(support various features)	CoreTSF	X	X	X
		PEDMiddleTSF	X	X	X
		MiddleTSF		X	X
Physical Protection					
FPT_PHP.3/CoreTSF	11	CoreTSFKeys CoreTSF	X	X	
FPT_EMSEC.1/ CoreTSF	11	CoreTSFKeys	X	X	
FPT_PHP.3/ ICCardReader	11	ICCR TSF	X	X	
FPT_PHP.3/MSR	11	MSR	X	X	
FPT_PHP.3/ CHIP-ONLY	11, 13	CoreTSF			X
FPT_EMSEC.1/ CHIP_ONLY	11	CoreTSF			X

Table 13: SFR packages included in each base PP

9.1.3 Security Functional Requirements dependencies rationale

507 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.

508 The dependency analysis has directly been made within the description of each SFR in section 9.1. All dependencies from CC part 2 and defined by the extended components in section 8 are either fulfilled or their non-fulfilment is justified.

9.2 Security Assurance Requirements

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

510 Most of the assurance components belonging to EAL POI come from EAL2 pre-defined 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 CoreTSF (except for POI-CHIP-ONLY, where these keys are POI-Moderate), POI-Moderate for CoreTSF, POI-EnhancedLow for Plaintext PIN processing by the IC Card Reader, POI-Low for PED-MiddleTSF, and POI-Basic for MiddleTSF and MSR.

511 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 EPC 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.

512 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. the annex in chapter 14 for details).

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

514 The "REFINED" and the "EXTENDED" requirements are defined in sections 9.2.2 and 9.2.3 respectively.

Security Assurance Requirements			EAL POI		
			PED-ONLY	POI-COMPREHENSIVE	POI-CHIP-ONLY
EAL2	ADV_ARC.1	REFINED	X	X	X
	ADV_FSP.2	REFINED	X	X	X
	ADV_TDS.1	REFINED	X	X	X
	AGD_OPE.1	REFINED	X	X	X
	AGD_PRE.1	REFINED	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	REFINED	X	X	X
	AVA_VAN.2				
	ALC_DVS.2	REFINED	X	X	X
	ALC_FLR.1	REFINED	X	X	X
Extended Requirements	AVA_POI.1/MSR	POI-Basic attack potential	X	X	
	AVA_POI.1/PEDMiddleTSF	POI-Low attack potential	X	X	X
	AVA_POI.1/MiddleTSF	POI-Basic attack potential		X	X
	AVA_POI.1/IC Card Reader	POI-EnhancedLow attack potential	X	X	
	AVA_POI.1/CoreTSF	POI-Moderate attack potential	X	X	X
	AVA_POI.1/CoreTSFKeys	POI-High attack potential	X	X	

Table 14: Definition of EAL POI by base PP

9.2.1 Security Assurance Requirements Rationale

515 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.

- 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.
- The starting point of EAL POI was CAS risk analysis and its derived security requirements (see the annex in chapter 13.1). Indeed, selecting most of the assurance components from EAL2 for EAL POI was sufficient to meet the CAS security requirements as shown in Annex 13.2 “Mapping from EPC Book 4 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 9.2.2 and by extensions with new assurance components AVA_POI, stated in section 9.2.3. 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 at-

tack potential levels. The relationship between the family AVA_POI and the assurance component AVA_VAN.2 is shown in the annex in chapter 14.

- For the chosen assurance components all the dependencies are met or exceeded in the EAL POI assurance package as shown in section 9.2.4.

9.2.2 Refined security assurance requirements

9.2.2.1 ADV_FSP Functional Specification

ADV_FSP.2 Security-enforcing functional specification

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

Refinement:
If the TOE claims conformance to package "SFR-supporting features related to Open Protocols", the following holds.

PCIF1: The TSFIs consisting in protocols or services shall be considered at least SFR-supporting and shall define the following parameters:

- Protocol name
- Protocol type:
  - Link Layer Protocols
  - IP Protocols
  - Security Protocols
  - IP Services
  - Other
- Protocol number (for IP protocols)
- Port number (for IP services)

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

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

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.**{** XE "ADV_ARC.1/PCI__ONLY" **}**

9.2.2.2 ADV_TDS Basic design

ADV_TDS.1 Basic design

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

Refinement:

In particular, for SFR-supporting features related to Open Protocols, the following holds: The design shall describe the behaviour of each SFR-supporting or SFR non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing. For all SFR-supporting TSF subsystem implementing a security protocol, the design shall describe

PCII2: how the device provides confidentiality of data sent over a network connection, including

a) Encryption mechanism with key sizes appropriate for the algorithm(s) in question.

b) Encryption provided by using keys that are established in a secure manner using appropriate key-management procedures, such as those listed in NIST SP800-21, Guidelines for Implementing Cryptography

PCII3: how the device is able to provide the integrity of data that is sent over a network connection, including

a) Integrity provided by a MAC as defined in ISO 16609, or by a digital signature.

b) Hashing provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512.

PCII4: how the device uses a declared security protocol to authenticate the server.

a) Server authentication with key sizes appropriate for the algorithm(s) in question.

b) Hashing provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512.

c) verification of the validity of public keys received by the platform.

d) verification of the authenticity of public keys received by the platform.

PCII6: How the platform implements session management.

a) Tracking of all connections and restriction of the number of sessions that can remain active on the platform to the minimum necessary number.

b) Time limits for sessions and insurance that sessions are not left open for longer than necessary.

ADV_TDS.1.4C The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

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

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

9.2.2.3 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 SFRs, the security architecture description shall describe the security domains that result from the application separation principle (requirement EPCN2), specified in FDP_ACC.1/POI_DATA, FDP_ACF.1/POI_DATA and FDP_RIP.1/POI_DATA. This design information shall explain the mechanisms used to achieve application separation. 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.

Refinement:

In particular, for SFR-supporting features related to Open Protocols, the following holds:

PCIH2: In particular, the security architecture shall demonstrate how the defaut configuration is secure for each TSFI of the following types : Link Layer Protocols, IP Protocols, Security Protocols, IP Services.

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,

PCIA4: Sensitive functions or data are only used in the protected areas(s) of the PED. This refinement is not applicable for the POI-CHIP-ONLY configuration.

PCIA10: Secure components intended for unattended devices contain an anti-removal mechanism to protect against unauthorized removal and/or unauthorized re-installation. This refinement is not applicable for the POI-CHIP-ONLY configuration. This part of the TSF is assigned to PEDMiddleTSF and thus AVA_POI.1/PEDMiddleTSF has to be applied to this property of the security architecture.

PCIB18: The operating system of the device must contain only the software (components and services) necessary for the intended operation. The operating system must be configured securely and run with least privilege.

PCIB20: The POI is capable of performing only its designed functions - i.e., there is no hidden functionality. The only approved functions performed by the POI are those allowed by the policy.[12]

PCID1: It is neither 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, nor is it possible for both an IC card and any other foreign object to reside within the card insertion slot. This refinement is not applicable for the POI-CHIP-ONLY configuration.

PCID2 : 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. This refinement is not applicable for the POI-CHIP-ONLY configuration.

PCID3 : 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. This refinement is not applicable for the POI-CHIP-ONLY configuration.

Refinement:

[12] This is a part of the PCIB20 requirement: the remainder is addressed as a refinement of AGD_OPE.1.

In particular, for SFR-supporting features related to Open Protocols, the following holds:

PCIH3: In particular the security architecture shall demonstrate how the TSF protects an unauthorized tampering of keys or certificates

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:

PCIA2: 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 (these mechanisms may be based on the same principles or technology, such as sensors, as long as their operation is independent – e.g. multiple switches activated on opening of the device casing are not independent). This refinement is not applicable in the POI-CHIP-ONLY configuration.

PCIB16: All prompts for non-PIN data entry are under the control of the cryptographic unit of the device. 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.

EPC-CHIP-ONLYB16: 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.

Refinement:

In particular, for SFR-supporting features related to Open Protocols, the following holds:

PCIG2: The security architecture shall demonstrate:

- How the TSF protects itself from the exploitation of a public-knowledge vulnerability on a TSFI of the following types : Link Layer Protocols, IP Protocols, Security Protocols, IP Services, including
  a) exploitation of replay of messages (PCII5),
  b) exploitation of insecure exception handling (PCII5).

PCIH3: The security architecture shall demonstrate:

- How the TSF protects itself from bypass of the SFR-enforcing functionality via an unexpected usage of keys or certificates.

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

{ XE "ADV_ARC.1/PCI__ONLY" **}**

9.2.2.4 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:

PCIB19: The vendor must provide adequate documented security guidance for the integration of any secure component into a PIN entry POI Terminal.

PCIB20: A user-available security policy from the vendor addresses the proper use of the POI in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements. The security policy must define the roles supported by the POI and indicate the services available for each role in a deterministic tabular format.[13]

PCID2: 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. This refinement is not applicable for the POI-CHIP-ONLY configuration.

PCIM8: The user guidance shall provide instructions for the operational management of the TOE. This includes instructions for recording the entire life cycle of the TOE components and of the manner in which 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.

The user guidance shall include guidance for how the POI is put into maintenance mode, and the vendor's requirements for secure handling of the POI. The vendor guidance is required in addition to any guidance that may be issued by the Acquirer or Merchant.

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.

Application Note:
In particular, for SFR-supporting features related to Open Protocols, the following holds:

DTR H1: The device has security guidance that describes how protocols and services must be used for each TSFI of the following types: Link Layer Protocols, IP Protocols, Security Protocols, IP Services. The operational user guidance shall also describe how to use the available protocol or service interfaces provided by the TOE in a secure manner. The operational guidance not only describes human interactions with the TOE but also the secure integration with other systems, devices or applications.

[13] This is a part of the PCIB20 requirement: the remainder is addressed as a refinement of ADV_ARC.1.

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.

Application Note:
In particular, for SFR-supporting features related to Open Protocols, the following holds:

PCIH3: The device has guidance for key management describing how keys and certificates must be used.

a) The key-management guidance is at the disposal of internal users, and/or of application developers, system integrators, and end-users of the platform.

b) Key-management security guidance describes the properties of all keys and certificates that can be used by the platform.

c) Key-management security guidance describes the responsibilities of the platform vendor, application developers, system integrators, and end-users of the platform.

d) Key-management security guidance ensures secure use of keys and certificates.

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:
In particular, for SFR-supporting features related to Open Protocols, the following holds:

DTR H1: The evaluator shall not limit to the human users of the TOE. The evaluator shall ensure that the mapping between all SFR-supporting TSFIs and guidance is complete and consistent.

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.

9.2.2.5 AGD_PRE Preparative procedure

AGD_PRE.1 Preparative procedures

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Application Note:
In particular, for SFR-supporting features related to Open Protocols, the following holds:

DTR H2: The device has guidance that describes the default configuration for each TSFI of the following types: Link Layer Protocols, IP Protocols, Security Protocols, IP Services. The evaluator shall ensure that the mapping between all SFR-supporting TSFIs and preparative procedures is complete and consistent.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

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

Application Note:
In particular, for SFR-supporting features related to Open Protocols, the following holds:

DTR H2 The device has guidance that describes the default configuration for each TSFI of the following types: Link Layer Protocols, IP Protocols, Security Protocols, IP Services. The evaluator shall ensure that the mapping between all SFR-supporting TSFIs and preparative procedures is complete and consistent.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

9.2.2.6 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:

PCIM7: Each device shall have a unique visible identifier affixed to it.

The unique identifier applies to the tamper-resistant boundaries (e.g. 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.

9.2.2.7 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:

PCIB3: The firmware, and any changes thereafter, have 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.

9.2.2.8 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).

9.2.2.9 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 (here and in the following text "security-related" is used in the sense of "SFR-enforcing".) falls to the acquirers. The initial key here is *not* the Acquirer key, but is the key that assures the authentication of the hardware device independent of the its ultimate purpose and destination.

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:
In the following requirements 'device' reflects the PED and the POI security-related components. In terms of Common Criteria security-related means SFR-enforcing.
The development security documentation shall meet the following requirements:

The development security documentation shall describe the entire device manufacturing lifecycle, up to and including Initial Key Loading, and shall identify the sites involved in each lifecycle stage.

PCIL2: The certified[14] firmware is protected and stored in such a manner as to preclude unauthorized modification during its entire manufacturing life-cycle e.g., by using dual control or standardized cryptographic authentication procedures. This requirement addresses the firmware of the device.

PCIL3: The device is assembled in a manner that the components of the device used in the manufacturing process are those components that were certified by the requirements of this PP (not to be applied for SRED and SFR-supporting features for Open Protocols) in the scope of the evaluation and unauthorized substitutions have not been made.

Application Note: These components belong to the TOE configuration list.

PCIL4: Production software (e.g., firmware) 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.

[14] 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.

PCIL5: Subsequent to production but prior to shipment from the manufacturer's or reseller's facility, the device 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.

PCIL6: If the device will be authenticated at the key-loading facility of initial deployment by means of secret information placed in the device during manufacturing, then this secret information is unique to each device, unknown and unpredictable to any person, and installed in the device under dual control to ensure that it is not disclosed during installation.

PCIL7: Security measures are taken during development and maintenance of POI security-related components. The manufacturer must maintain a development security documentation describing 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.

PCIL8: Controls exist over the repair process and the inspection/testing process subsequent to repair to ensure that the device has not been subject to unauthorized modification.

PCIM3: While in transit from the manufacturer's facility to the initial key-loading facility, 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.

PCIM4: The device's development security documentation must provide means to the initial key-loading facility to assure the authenticity of the TOE's security relevant components.

PCIM5: If the manufacturer is in charge of initial key-loading, then the manufacturer must verify the authenticity of the POI security-related components.

PCIM6: If the manufacturer is not in charge of initial key-loading, the manufacturer must provide the means to the initial key-loading facility to assure the verification of the authenticity of the POI security-related components.

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:

PCIL4: Production software (e.g., firmware) 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.

PCIM1: The POI should be protected from unauthorized modification with tamper-evident security features, and customers shall be provided with documentation

(both shipped with the product and available securely online) that provides instruction on validating the authenticity and integrity of the POI.
Where this is not possible, the POI is shipped from the manufacturer's facility to the initial key-loading facility or to the facility of initial deployment and stored en route under auditable controls that can account for the location of every POI at every point in time.
Where multiple parties are involved in organizing the shipping, it is the responsibility of each party to ensure that the shipping and storage they are managing is compliant with this requirement.

PCIM2: 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:

EPC PlusL0: 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 to each relevant site (as determined by the lifecycle description for ALC_DVS.2.1C).

9.2.2.10 ALC_FLR Flaw Remediation

ALC_FLR.1 Basic flaw remediation

ALC_FLR.1.1D The developer shall document and provide flaw remediation procedures addressed to TOE developers.

Refinement:

In particular, for SFR-supporting features related to Open Protocols, the following holds:

PCIG3: The notion of "reports of security flaws" includes all public-knowledge vulnerabilities found on SFR-supporting TSFIs of the following types: Link Layer Protocols, IP Protocols, Security Protocols, IP Services.

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

Refinement:

The flaw remediation procedures shall ensure a timely distribution of information about newly found vulnerabilities and mitigations for the vulnerabilities; this information includes identification, description, and assessment of the vulnerabilities. The procedures shall ensure timely creation of mitigation measures for newly found vulnerabilities that may impact POI security.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

Refinement:
The flaw remediation procedures shall ensure timely detection of vulnerabilities that apply to the device by periodical execution of a vulnerability assessment that includes activities such as: analysis, survey of information available in the public domain, and testing.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

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

9.2.2.11 ATE_IND Independent testing - sample

ALC_IND.2 Independent testing - sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

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

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

Refinement:
In particular, for SFR-supporting features related to Open Protocols, the following holds:

PCII1: The evaluator shall verify that all security protocols present on the device are described as SFR-supporting TSFIs in the functional specification.

For all these TSFI, the evaluator shall assess that:

PCII2: The device is able to provide confidentiality of data sent over a network connection.

- a) Encryption mechanism utilizes key sizes appropriate for the algorithm(s) in question.

- b) Encryption is provided by using keys that are established in a secure manner using appropriate key-management procedures, such as those listed in NIST SP800-21, Guidelines for Implementing Cryptography

PCII3: The device is able to provide the integrity of data that is sent over a network connection.

- a) Integrity is provided by a MAC as defined in ISO 16609, or by a digital signature.
- b) Hashing can be provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512.

PCII4: The device uses a declared security protocol to authenticate the server.

- a) Server authentication utilizes key sizes appropriate for the algorithm(s) in question.
- b) Hashing can be provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512.
- c) The platform is able to verify the validity of the public keys it receives.
- d) The platform is able to verify the authenticity of the public keys it receives.

PCII6: The platform implements session management.

- a) The platform keeps track of all connections and restricts the number of sessions that can remain active on the platform to the minimum necessary number.
- b) The platform sets time limits for sessions and ensures that sessions are not left open for longer than necessary.

9.2.3 Extended security assurance requirements

516 The AVA_POI requirements of the EAL POI package consists of:

- AVA_POI.1.

517 AVA_POI.1 is iterated five times and applied to MSR, PEDMiddleTSF, MiddleTSF, IC Card Reader, CoreTSF and CoreTSFKeys.

9.2.3.1 AVA_POI applied to MSR

518 This requirement holds in PED-ONLY and POI-COMPREHENSIVE configurations only.

AVA_POI.1/MSR "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 **Magnetic Stripe Reader component of the POI** 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 component of the POI**.

Content and presentation elements:

AVA_POI.1.1C/MSR The **Magnetic Stripe Reader component of 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 **attack potential equal or higher than POI-Basic attack potential with a minimum attack potential for the exploitation phase of a value defined in [POI AttackPot].**

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.*

9.2.3.2 AVA_POI applied to MiddleTSF

519 This requirement holds in the POI-COMPREHENSIVE and in the POI-CHIP-ONLY configurations only.

AVA_POI.1/MiddleTSF "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/MiddleTSF The developer shall provide the **MiddleTSF's components** for testing.

AVA_POI.1.2D/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.1.1C/MiddleTSF The **MiddleTSF's components** shall be suitable for testing.

Evaluator action elements:

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

AVA_POI.1.2E/MiddleTSF The evaluator ***shall perform*** a search of public domain sources to identify potential vulnerabilities in the **MiddleTSF's components.**

AVA_POI.1.3E/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 as well as **none** to identify potential vulnerabilities.

AVA_POI.1.4E/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-Basic attack potential with a minimum attack potential for the exploitation phase of a value defined in [POI AttackPot].**

Refinement:
In particular, for SFR-supporting features related to Open Protocols, the following holds:

PCIG2: In particular the evaluator shall exploit public-knowledge vulnerabilities on all SFR-supporting TSFIs of the following types: Link Layer Protocols, IP Protocols, Security Protocols, IP Services. Exploitation methods shall include at least replay of messages and exploitation of insecure exception handling.

9.2.3.3 AVA_POI applied to PEDMiddleTSF

520 This requirement holds in all configurations.

AVA_POI.1/PEDMiddleTSF "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/PEDMiddleTSF The developer shall provide the **PEDMiddleTSF's components** for testing.

AVA_POI.1.2D/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.1.1C/PEDMiddleTSF The **PEDMiddleTSF's components** shall be suitable for testing.

Evaluator action elements:

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

AVA_POI.1.2E/PEDMiddleTSF The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the **PEDMiddleTSF's components.**

AVA_POI.1.3E/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.1.4E/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 with a minimum attack potential for the exploitation phase of a value defined in [POI AttackPot].**

Refinement:
In particular, for SFR-supporting features related to Open Protocols, the following holds:

PCIG2: In particular the evaluator shall exploit public-knowledge vulnerabilities on all SFR-supporting TSFIs of the following types: Link Layer Protocols, IP Protocols, Security Protocols, IP Services. Exploitation methods shall include at least replay of messages and exploitation of insecure exception handling.

9.2.3.4 AVA_POI applied to IC Card Reader TSF

521 This requirement holds in PED-ONLY and POI-COMPREHENSIVE configurations only.

AVA_POI.1/IC Card Reader "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/IC Card Reader The developer shall provide the **IC Card Reader components** for testing.

AVA_POI.1.2D/IC Card Reader The developer shall provide the implementation representation and a mapping of SFRs to implementation representation of **the hardware and software IC Card Reader components**.

Content and presentation elements:

AVA_POI.1.1C/IC Card Reader The **IC Card Reader components** shall be suitable for testing.

Evaluator action elements:

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

AVA_POI.1.2E/IC Card Reader The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the **IC Card Reader components**.

AVA_POI.1.3E/IC Card Reader The evaluator shall perform an independent vulnerability analysis of the **IC Card Reader 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.1.4E/IC Card Reader The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the **IC Card Reader components**

are resistant to attacks performed by an attacker possessing **POI-EnhancedLow attack potential with a minimum attack potential for the exploitation phase of a value defined in [POI AttackPot].**

Refinement:
In particular, for SFR-supporting features related to Open Protocols, the following holds:

PCIG2: In particular the evaluator shall exploit public-knowledge vulnerabilities on all SFR-supporting TSFIs of the following types: Link Layer Protocols, IP Protocols, Security Protocols, IP Services. Exploitation methods shall include at least replay of messages and exploitation of insecure exception handling.

9.2.3.5 AVA_POI applied to CoreTSF

522 This requirement holds for all configurations. In addition, for the POI-CHIP-ONLY configuration the following holds: For the POI-CHIP-ONLY configuration CoreTSF covers in addition secret Payment Transaction Keys.

523 If the SRED PP-Module is selected AVA_POI.1/CoreTSF is applied also to the part of MiddleTSF which stores and processes cryptographic data to protect account data.

AVA_POI.1/CoreTSF "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/CoreTSF The developer shall provide the **CoreTSF's components** for testing.

AVA_POI.1.2D/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.1.1C/CoreTSF The **CoreTSF's components** shall be suitable for testing.

Evaluator action elements:

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

AVA_POI.1.2E/CoreTSF The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the **CoreTSF's components**.

AVA_POI.1.3E/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.1.4E/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 with a minimum attack potential for the exploitation phase of a value defined in [POI AttackPot].**

Refinement:
In particular, for SFR-supporting features related to Open Protocols, the following holds:

PCIG2: In particular the evaluator shall exploit public-knowledge vulnerabilities on all SFR-supporting TSFIs of the following types: Link Layer Protocols, IP Protocols, Security Protocols, IP Services. Exploitation methods shall include at least replay of messages and exploitation of insecure exception handling.

9.2.3.6 AVA_POI applied to the CoreTSFKeys

524 This requirement holds in PED-ONLY and POI-COMPREHENSIVE configurations only.

525 AVA_POI.1/CoreTSFKeys is applied to the part of CoreTSF which stores and processes secret PIN Encryption Keys in PED-ONLY and POI-COMPREHENSIVE configurations only.

526 Note that AVA_POI.1/CoreTSFKeys supersedes AVA_POI.1/CoreTSF regarding secret PIN Encryption Keys (CoreTSFKeys) in PED-ONLY and POI-COMPREHENSIVE configuration only.

AVA_POI.1/CoreTSFKeys "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/CoreTSFKeys The developer shall provide the **CoreTSFKeys components** for testing.

AVA_POI.1.2D/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.1.1C/CoreTSFKeys The **CoreTSFKeys components** shall be suitable for testing.

Evaluator action elements:

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

AVA_POI.1.2E/CoreTSFKeys The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the **CoreTSFKeys components**.

AVA_POI.1.3E/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.1.4E/CoreTSFKeys The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the **CoreTSFKeys components** are resistant to attacks performed by an attacker possessing **POI-High attack potential with a minimum attack potential for the exploitation phase of a value defined in [POI AttackPot].**

Refinement:
In particular, for SFR-supporting features related to Open Protocols, the following holds:

PCIG2: In particular the evaluator shall exploit public-knowledge vulnerabilities on all SFR-supporting TSFIs of the following types: Link Layer Protocols, IP Protocols, Security Protocols, IP Services. Exploitation methods shall include at least replay of messages and exploitation of insecure exception handling.

9.2.4 Security Assurance Requirements Dependencies

Requirements	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 (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.2, AGD_OPE.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.2) 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.1/PEDMiddleTSF	(ADV_ARC.1) and (ADV_FSP.2) 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.1/MiddleTSF	(ADV_ARC.1) and (ADV_FSP.2) 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.1/IC Card Reader	(ADV_ARC.1) and (ADV_FSP.2) 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.1/CoreTSF	(ADV_ARC.1) and (ADV_FSP.2) 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.1/CoreTSFKeys	(ADV_ARC.1) and (ADV_FSP.2) 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

10 Rationale Objectives/SFR

527 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.POI_SW{XE	O.PaymentApplication Download	O.POIApplicationSeparatio	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.1/ENC_PIN		X											
FMT_SMR.1/ENC_PIN		X	X				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									

	O.PINEntry	O.EncPIN	O.CipherPPIN	O.ClearPPIN	O.CoreSWHW	O.PEDMiddleSWHW	O.ICCardReader	O.PaymentTransaction	O.POI_SWE	O.PaymentApplication Download	O.POIApplicationSeparatio	O.PromptControl	O.MSR
FDP_ITT.1/PLAIN_PIN			X	X									
FMT_MSA.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						
FDP_ACC.1/ICCRLoader							X						
FDP_ITC.1/ICCRLoader							X						
POI_DATA Package													
FDP_ACC.1/POI_DATA								X			X		
FDP_ACF.1/POI_DATA								X			X		
FDP_ITT.1/POI_DATA								X					
FDP_UIT.1/POI_DAT								X					
FDP_UCT.1/POI_DATA								X					
FDP_RIP.1/POI_DATA								X			X		
FTP_ITC.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							

	O.PINEntry	O.EncPIN	O.CipherPPIN	O.ClearPPIN	O.CoreSWHW	O.PEDMiddleSWHW	O.ICCardReader	O.PaymentTransaction	O.POI_SWE	O.PaymentApplication Download	O.POIApplicationSeparatio	O.PromptControl	O.MSR
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/Crypto		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
FPT_PHP.3/CHIP-ONLY		X						X					

	O.PINEntry	O.EncPIN	O.CipherPPIN	O.ClearPPIN	O.CoreSWHW	O.PEDMiddleSWHW	O.ICCardReader	O.PaymentTransaction	O.POI_SWE	O.PaymentApplication Download	O.POIApplicationSeparatio	O.PromptControl	O.MSR
FPT_EMSEC.1/CHIP-ONLY								X					

Table 16: Objectives coverage by SFRs

528 A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given below.

529 **O.PINEntry**

530 Rationale:

- With FPT_EMSEC.1/PIN_ENTRY the PED only emits indistinguishable audible tones, if any (PCIA11); the PED does not emit sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring (PCIA5); not emit the entered PIN digits at the display (PCIB5). Because of the reduced risks in a the POI-CHIP-ONLY configuration PCIA5 is not applicable and does not contribute to the objective in that configuration. This is caused in the different risk analysis between POI-CHIP-ONLY and other configurations where in POI-CHIP-ONLY only IC Card based transactions are accepted.
- With FPT_PHP.3/CoreTSF the PED resists physical manipulation and manipulation of the CoreTSF hardware to protect the confidentiality of any PIN (PCIA1) including changing environmental conditions (PCIA3). Because of the reduced risks in a the POI-CHIP-ONLY configuration there is no need to protect the PIN by hardware means and PCIA1 is not applicabe. Thus FPT_PHP.3/CHIP-ONLY insteat of FPT_PHP.3/CoreTSF contributes to that objective for the POI-CHIP-ONLY configuration (PCIA3).
- 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 (PCIB7).
- 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 (PCIB8).

531 **O.EncPIN**

532 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 (PCIA1, PCIA6) including changing environmental conditions (PCIA3). Because of the reduced risks in a the POI-CHIP-ONLY configuration there is no need to protect the PIN by hardware means. Thus PCIA1 is not applicable and does not contribute to the security objective. Only penetration of the PED to disclose the PIN encryption keys is contributing to that objective (at a lower level) by hardware means (EPC-CHIP-ONLYA6). Thus for POI-CHIP-ONLY configurations FPT_PHP.3/CHIP-ONLY instead of FPT_PHP.3/CoreTSF applies.
- FPT_EMSEC.1/CoreTSF protects ENC_PIN_SK against emanation (PCIA6). FPT_EMSEC.1/CHIP-ONLY contribute for POI-CHIP-ONLY instead of FPT_EMSEC.1/CoreTSF (EPC-CHIP-ONLYA6).
- 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 (PCIB7).
- 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 (PCIB6,).
- 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 (PCID4.1, PCID4.3).
- 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 (PCIB10, EPCPlusB10.a, PCID4.1, PCID4.3).
- 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 (PCIB13). Additionally, output of cleartext cryptographic keys or moving from one component of higher security to a component of less security is prevented (PCIB14).
- 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 deallocation of the resources from sensitive objects. Especially ENC_PIN is deleted immediately after being enciphered (PCIB6).
- 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 (PCIC1).
- According to FCS_RND.1 mechanisms are provided to generate random numbers that meet a defined quality metric for cryptographic means (PCIB9).
- According to FCS_COP.1, PIN encipherment is performed following ISO 9564 (PCIB10, EPCPlusB10a, PCIB12, PCID4.1, PCID4.2, PCID4.4).

- 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 (or equivalent). Therefore state-of-the-art cryptography for cryptographic means is provided (PCIB11). The cryptographic key import is supported by FTP_ITC.1/Crypto and FPT_TDC.1.
- With FMT_MSA.1/ENC_PIN, FMT_SMR.1/ENC_PIN and FIA_UID.1/ENC_PIN security attributes are managed and roles are assigned.

533 **O.CipherPPIN**

534 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 (PCIA1, PCIA6) including changing environmental conditions (PCIA3).
- FPT_EMSEC.1/CoreTSF protects PLAIN_PIN_SK against emanation (PCIA6).
- 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 (PCIB7).
- 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 (PCID4.2).
- 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 deallocation of the resources from sensitive objects. Especially PLAIN_PIN is deleted immediately after being enciphered (PCIB6).
- According to FCS_RND.1 mechanisms are provided to generate random numbers that meet a defined quality metric for cryptographic means (PCIB9).
- According to FCS_COP.1, PIN encipherment is performed following ISO 9564 (PCIB10, EPCPlusB10a, PCIB12, PCID4.1, PCID4.2, PCID4.4).
- 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 (or equivalent). Therefore state-of-the-arte cryptography for cryptographic means is provided (PCIB11). The cryptographic key import is supported by FTP_ITC.1/Crypto and FPT_TDC.1.
- With FMT_MSA.1/PLAIN_PIN, FMT_SMR.1/ENC_PIN and FIA_UID.1/PLAIN_PIN security attributes are managed and roles are assigned.

535 **O.ClearPPIN**

536 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 NewA1) including changing environmental conditions (PCIA3).
- 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 (PCIB7).
- 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 (PCID4.4).
- 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 deallocation of the resources from sensitive objects. Especially PLAIN_PIN is deleted immediately after being sent to the IC Card Reader (PCIB6).

537 **O.CoreSWHW**

538 Rationale:

- With FPT_PHP.3/CoreTSF the PED resists physical manipulation and manipulation of the CoreTSF hardware (PCIA1) or software, including changing environmental conditions (PCIA3). These requirements are not applicable for the POI-CHIP-ONLY configuration and thus do not contribute to the security objective for the POI-CHIP-ONLY configuration. This is caused in the different risk analysis between POI-CHIP-ONLY and other configurations where in POI-CHIP-ONLY only IC Card based transactions are accepted. Thus FPT_PHP.3.1/CHIP-ONLY instead of FPT_PHP.3/CoreTSF applies for POI-CHIP-ONLY (PCIA3).
- 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 (PCIB7).
- 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 (PCIB1).
- FPT_FLS.1/CoreTSF enforces the CoreTSF authenticity and integrity by preserving a secure state in case of self-test failure or logical anomalies (PCIB1, PCIB2).
- 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 (PCIB2, PCIB4).

539 **O.PEDMiddleSWHW**

540 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 (PCIB7).

- 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 (PCIB1).
- FPT_FLS.1/PEDMiddleTSF enforces the PEDMiddleTSF authenticity and integrity by preserving a secure state in case of self-test failure or logical anomalies (PCIB1, PCIB2).
- 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 (PCIB2, PCIB4).

541 **O.ICCardReader**

542 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 (PCIA6).
- FPT_PHP.3/ICCardReader (PCID1) 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 (PCIB7).
- 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 (PCID4.2). 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 (PCID4.4). 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 NewB14).
- FDP_RIP.1/ICCardReader prevents unwanted knowledge of secret data upon the deallocation of the resources from sensitive objects. Especially PLAIN_PIN is deleted immediately after being sent to the IC Card Reader and temporary cryptographic keys (PCIB6).
- FDP_ITT.1/ICCardReader prevents the disclosure of PLAIN_PIN and PLAIN_PIN_SK in the IC Card Reader.
- With FMT_MSA.1/PLAIN_PIN, FMT_SMR.1/ENC_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 (PCIB10, EPCPlusB10a, PCIB12, PCID4.1, PCID4.2, PCID4.4).
- 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 (or equivalent). Therefore state-of-the-art

cryptography for cryptographic means is provided (PCIB11). The cryptographic key import is supported by FTP_ITC.1/Crypto and FPT_TDC.1.

- The protection of the authenticity and integrity of ICCR_SW and cryptographic keys upon downloading of new components and updating of existing ones is protected due to FDP_ACC.1.1/ICCRLoader and FDP_ITC.1/ICCRLoader (PCIB2, PCIB4).

543 **O.PaymentTransaction**

544 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 (EPCN1.2 and EPCN1.3).
- FDP_ITT.1/POI_DATA protects the disclosure of POI_SK when it is transferred between physically separated parts of the POI (EPCN4).
- FDP_UIT.1/POI_DATA protects POI Management Data and Payment Transaction Data at the external lines of the POI against modification (EPCN1.3 and EPCN1.1).
- FDP_UCT.1/POI_DATA provides means to protect Payment Transaction Data at the external lines of the POI against disclosure (EPCN1.1).

545 FDP_ACC.1/POI_DATA and FDP_ACF.1/POI_DATA prevents other application to deceive the Cardholder during execution of the payment application (EPCN2.3).

- FTP_ITC.1/POI_DATA provides the communication channel to protect data at the external lines against disclosure. This includes means to prove the identity of the POI (EPCN1.1).
- FDP_RIP.1/POI_DATA ensures that MiddleTSF secret data is no longer accessible once used.
- Because of the specific properties – no hardware protection – of a the POI-CHIP-ONLY configuration the Acquirer needs to know which POI is communicating with the Acquirer during an online payment transaction. Therefore FPT_PHP.3/CHIP-ONLY and FPT_EMSEC.1/CHIP-ONLY ensure that secret keys protecting the authenticy and integrity of Payment Transaction Data are protected against disclosure and thus these SFRs are contributing to that objective.

546 **O.POI_SW{ XE "O.POI_SW_HW (Authentic and integer usage of POI software and related hardware)" }**

547 Rationale:

- FPT_FLS.1/MiddleTSF enforces the MiddleTSF authenticity and integrity by preserving a secure state in case of logical anomalies (EPCN7).
- 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 (EPCN3.1 and EPCN3.2).

548 O.PaymentApplicationDownload

549 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 (EPCN3.1 and EPCN3.2).

550 **O.POIApplicationSeparation**

551 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 (EPCN2.1); that it is not possible for another application to interfere with the execution of the payment application by accessing internal data (EPCN2.2) and that it is not be possible for another application to deceive the Cardholder during execution of the payment application (EPCN2.3).
- FDP_RIP.1/POI_DATA ensures that no residual information remains in resources released by the payment application and payment application temporary cryptographic keys (EPCN2.1 to EPCN2.3).

552 **O.PromptControl**

553 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 (PCIA7, PCIB16, EPC-CHIP-ONLYB16 for POI-CHIP-ONLY).

554 **O.MSR**

555 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.

11 Glossary

556 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.
Distributed architecture	POI architectures where (at least) two security relevant parts of the POI (usually the PED and the Card Reader) are separated devices (i.e. not integrated into one single tamper-responsive boundary).
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.
IC	Integrated Circuit
ICC	Integrated Circuit Card
ICCR	Integrated Circuit Card Reader
Integrated Architecture	POI architectures where all security relevant parts of the POI are integrated into one single tamper-responsive boundary.
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.
MSR	Magnetic Stripe Reader
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).
Open Protocol (OP)	A set of requirements that ensures PIN entry devices using open security protocols and open communication protocols to access public networks and services do not have public domain vulnerabilities.
OS	In the scope of this PP, any underlying software providing services for code running in the device is considered part of the operating system. Examples of such services include: system initialization and boot, hardware abstraction layers, memory management, mul-

Term	Definition
	titasking, synchronization primitives, file systems, device drivers and networking stacks. Services that provide security or may impact security are, in addition, considered firmware. Operating systems may range from hardware abstraction layer libraries and embedded micro-kernels, to complex multi-user operating systems.
OSeC	Open Standards for Security and certification
PAN	Primary Account Number
Payment Application	A payment application is a particular type of Application, which uses functions provided by the core software of the POI to carry out payment transactions (and possibly card management functions). The Payment Application is excluded from the TOE.
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 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.

Term	Definition
	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.
PP-Module	See [PP Mod] for the definition.
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 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.

Term	Definition
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 Module (SM)	Any (physical or logical) device that manages secret cryptographic 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.
SRED	Secure Read and Exchange – A set of requirements protection account data and account data related cryptographic data.
surrogate PAN	A value derived from the PAN, that can be exported outside the device, e.g. to update a loyalty application. Such surrogate PAN can be obtained by different methods: encryption, cryptographic hash (with salt), mask, or truncation.
Tamper-resistant	A characteristic that provides passive physical protection against an attack.

Term	Definition
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.

12 Definition of the SRED PP-Module

557 This chapter contains the definition of the SRED PP-Module.

558 As described in section 2.1 the SRED module can be added to a base PP including either the PED-ONLY configuration or to the POI-COMPREHENSIVE configuration. During the text in this chapter this configuration is sometimes called the **underlying configuration**.

559 Note: The security properties of the SRED PP-Module overlap with those of the POI-COMPREHENSIVE configuration. For example, the security objective O.PaymentTransaction is needed for the SRED PP-Module and also included in POI-COMPREHENSIVE, but not in PED-ONLY. Therefore this objective needs to be added, if the underlying configuration is PED-ONLY, but does not need to be added, if the underlying configuration is POI-COMPREHENSIVE. We try to explicitly mention similar effects in the following chapters.

12.1 Security Problem Definition

12.1.1 Assets

560 The following assets are defined for the SRED PP-Module in addition to the assets for the underlying configuration.

561 **PAY_DAT {** XE "PAY_DAT" **}**

562 Payment transaction data

563 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 (if transferred online during the payment transaction), 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.

564 Sensitivity: Authenticity and Integrity.

565 *Application Note:*

566 *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.*

567 Note: This asset is added, if the underlying configuration is PED-only. While this asset is already contained in the POI-COMPREHENSIVE configuration, its definition is slightly extended here and may therefore replace the asset of the underlying configuration.

568 **PAN {** XE "PAN" **}**

569 Primary account number

570 The primary account number is a part of Payment transaction data (PAY_DATA). PAN is obtained from IC Card or magnetic card, and then has to be transmitted to the acquirer.

571 PAN has three possible forms in the TOE:

- TOE_CLEAR_PAN (cleartext PAN). cleartext PAN is either encrypted immediately upon entry or entered in clear-text into the device and processed within the secure controller of the device.
- TOE_CIPHER_PAN (when operating in encrypting mode and when the TOE includes several physically separate parts, PAN is ciphered by TSF for internal transfer)
- E2E_CIPHER_PAN (when operating in encrypting mode, the TSF ciphers the PAN for end-to-end protection)

572 It should be noted that even in encrypting mode, the PED still has the possibility to transfer a cleartext version of the PAN to an authorized application within the device (see PCI K15.1)

573 Sensitivity: Authenticity and Integrity (as any other part of PAY_DATA) and Confidentiality.

574 **TOE_CLEAR_PAN {** XE "TOE_CLEAR_PAN" **}**

575 PAN in clear text.

576 Sensitivity: Confidentiality, Authenticity, and Integrity.

577 **TOE_CIPHER_PAN {** XE "TOE_CIPHER_PAN" **}**

578 In distributed POI architectures, PAN ciphered for internal TOE transmission

579 In distributed architectures and when operating encrypting mode, the PAN has to be encrypted by the Card Reader prior to sending it to the PED, which then deciphers it before ciphering it for the Acquirer.

580 Sensitivity: Confidentiality, Authenticity, and Integrity.

581 Application Note:

582 "Distributed architecture" has to be understood as POI architectures where the PED and the Card Reader are separated devices (i.e. not integrated into one single tamper-responsive boundary).

583 In that case,

- the card reader transforms TOE_CLEAR_PAN into TOE_CIPHER_PAN, and transmits it to the PED
- the PED transforms TOE_CIPHER_PAN into TOE_CLEAR_PAN
- the PED transforms TOE_CLEAR_PAN into E2E_CIPHER_PAN

584 **TOE_PAN_SK {** XE "TOE_PAN_SK" **}**

585 Secret/private PAN cryptographic keys for internal TOE transmission

586 All secret cryptographic keys used to protect the confidentiality of PAN, while transmitted between physically-separate parts of the TOE. Application of TOE_PAN_SK "transforms" TOE_CLEAR_PAN into TOE_CIPHER_PAN

587 Sensitivity: Confidentiality, Authenticity and Integrity.

588 *Application Note:*

589 *Note that private keys only needed for decryption, not for encryption of PAN. This asset is relevant to distributed PED architectures, where the Card Reader is not in the same tamper-responsive enclosure as the PED keypad.*

590 **E2E_CIPHER_PAN {** XE "E2E_CIPHER_PAN" **}**

591 Encrypted PAN for end-to-end transmission

592 In encrypting mode, the POI payment application requires sending the encrypted PAN to the Acquirer via the online interface of the POI.

593 Sensitivity: Confidentiality, Authenticity, and Integrity.

594 **E2E_PAN_PK {** XE "E2E_PAN_PK" **}**

595 Public PAN cryptographic keys for end-to-end encryption

596 All public cryptographic keys used to protect the confidentiality of PAN.

597 Sensitivity: Authenticity and Integrity.

598 **E2E_PAN_SK {** XE "E2E_PAN_SK" **}**

599 Private cryptographic keys for end-to-end encryption

600 All private cryptographic keys used to protect the confidentiality of the E2E_CIPHER_PAN.

601 Sensitivity: Confidentiality, Authenticity and Integrity.

602 *Application Note:*

603 *Note that private keys only needed for decryption, not for encryption of E2E_CIPHER_PAN.*

604 **SURROGATE_PAN {** XE "SURROGATE_PAN" **}**

605 Surrogate PAN value

606 The TSF can generate a surrogate PAN, that can be exported outside the device, e.g. to update a loyalty application. Such surrogate PAN can be obtained by different methods:

- encryption
- cryptographic hash (with salt)
- mask
- truncation

607 Sensitivity: Authenticity and Integrity.

608 **SURROGATE_PAN_SALT {** XE "SURROGATE_PAN_SALT" **}**

609 Salt used to generate a surrogate PAN value

610 When a cryptographic hash is used to generate a surrogate PAN, TSF must take a salt as input for the cryptographic hash.

611 Sensitivity: Authenticity, Integrity and Confidentiality.

12.1.2 Users / Subjects

612 The SRED PP-Module does not define additional users or subjects.

12.1.3 Threats

613 The SRED PP-Module defines the threat T-Transaction. If the underlying configuration is PED-ONLY, this is an additional threat, if it is POI-COMPREHENSIVE, this is an extended version of an existing threat.

614 **T.Transaction {** XE "T.Transaction" **}**

615 Transaction with usurped Cardholder identity

616 Edition of T.Transaction as defined in PP POI - addition of the following examples:

d) Fraudsters obtain knowledge of a legitimate user's Primary Account Number during transaction, in order to impersonate the user in another transaction.

e) Fraudsters deduce a legitimate user's Primary Account Number from the surrogate PAN stored by an application (such as loyalty application), in order to impersonate the user in another transaction.

12.1.4 Organisational Security Policies

617 The SRED PP-Module does not define additional Organisational Security Policies.

12.1.5 Assumptions

618 The SRED PP-Module does not define additional assumptions.

12.2 Security Objectives

12.2.1 Security Objectives for the TOE

619 The SRED PP-Module includes the objectives **O.PaymentTransaction**, **O.POI_SW**, and **O.POIApplicationSeparation** as defined in section 6.1.

620 Note: If the underlying configuration is PED-ONLY, these objectives are added by claiming the SRED PP-Module. In the case of POI-COMPREHENSIVE, these objectives are already included and do not need to be added.

621 In addition, the SRED PP-Module defines the following new objectives.

622 O.PANConfidentiality **{** XE "O.PANConfidentiality" **}**

623 The TOE shall protect the confidentiality of PAN when operating in encrypting mode.

624 O.PANDeduction **{** XE "O.PANDeduction" **}**

625 If the TOE enables surrogate PAN values to be outputted outside of the device, such values shall resist the deduction of the original PAN knowing only the surrogate value.

626 O.PANOperatingMode **{** XE "O.PANOperatingMode" **}**

627 The TSF shall allow the selection and update of the operating mode to authenticated users only.

628 *Application Note:*

- *operating mode defines whether SRED functionality is activated or not*
- *operating mode will be hereafter described by the two values "encrypting mode" and "non-encrypting mode"*
- *if the operating mode cannot be changed at all (SRED functionality is always active), this objective is considered trivially fulfilled.*

12.2.2 Security objectives for the Operational Environment

629 The SRED PP-Module does not define additional Security objectives for the Operational Environment.

12.2.3 Security Objectives Rationale

630

631 All objectives defined in this module are mapped to T.Transaction and the rationale is as follows:

632 **T.Transaction** Transaction with usurped Cardholder identity

633 The SRED PP-Module adds the following paragraph to the rationale already given in section 7.1:

O.PANConfidentiality and O.PANDeduction prevent attacks using knowledge of the PAN, whether it is obtained during the transaction or by deduction from a surrogate value stored by an external application.

O.PANOperatingMode prevents attacks consisting in deactivating the protection by the TOE.

12.3 Extended Requirements

634 The SRED PP-Module does not define additional extended requirements.

12.4 Security Requirements

12.4.1 Security Functional Requirements

635 The SRED PP-Module defines the following packages of SFRs:

- Protection of the PAN for end-to-end encryption is addressed by the 'SRED End-to-end protection package'.
- The 'SRED Distributed Architecture Package' addresses the protection of the PAN when transmitted within the TOE.
- Both packages rely on the 'SRED Cryptography package' to ensure encipherment and decipherment operations.
- Protection of the surrogate values generated from the PAN is addressed by the 'SRED Surrogate PAN Package'.
- The 'SRED Basis Package' provides the common protection requirements such as physical resistance

636 *Application Notes:*

- *Mapping between SFRs and PCI requirements: the SFRs in these packages are mapped to the PCI SRED requirements they implement, either in the text of the SFR or in application notes, or both: they are referenced with the "PCI" identifier.*
- *Mapping between SARs and PCI requirements: some PCI security requirements have been identified not to be security functional ones. These security requirements are introduced as refinements of ADV_ARC, AGD_OPE, AGD_PRE and ALC_CMC.*
- *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.*
- *As in the PP POI, the definition of the different entities part of the SFPs has been determined in the following manner:*
  - *Subjects are SPD subjects (section 5.3) or SPD users (section 5.2).*
  - *Objects or information are assets (section 5.1).*
  - *Security attributes are properties of assets or subjects.*
  - *Roles are SPD users (section 5.2).*

637 The table hereafter lists the SFR packages in the SRED PP-Module and explains their relation to PP POI and their usage in POI-COMPREHENSIVE or PED-ONLY configuration.

Package	SFR	Usage	Comments
SRED Basis Package	FIA_UID.1 FTA_SSL.3 FIA_UAU.2 FMT_MSA.1 FTP_ITC.1 FPT_FLS.1 FPT_TST.1 FMT_SMR.1 FDP_ACF.1 FDP_ACC.1 FDP_ITC.1 FPT_EMSEC.1 FPT_PHP.3	This package is always needed in the SRED PP-Module.	Some of these SFRs were built on the model of their PIN_ENTRY counterpart in PP POI, but covering a different objective (PAN protection).
SRED Cryptography Package	FTP_ITC.1, FPT_TDC.1, FDP_ITC.2, FCS_COP.1	This package defines cryptographic primitives needed for cryptographic functions in the other packages and its functionality is therefore always needed.	These SFRs have only been defined to cover explicitly the PCI SRED requirements, but usually the PP POI functionality already covers the security needs. If the cryptographic primitives used for SRED are the same as for the POI functions in the underlying configuration, these SFRs may be good candidates to remove them (only adding their refinements and application notes to the corresponding SFRs in the underlying package, where applicable).
SRED Distributed Architecture Package	FDP_IFC.1, FDP_IFF.1, FDP_ITT.1, FMT_MSA.1, FDP_RIP.1	This package has to be added **if the TOE consists of several physically-separated parts**.	Definition of INTERNAL_PROTECTION Information Flow Control SFP : protection of the PAN when transmitted between separate parts of the TOE
SRED End-to-end protection Package	FDP_IFC.1, FDP_IFF.1, FMT_MSA.1, FMT_SMR.1, FIA_UID.1, FDP_RIP.1, FDP_ITT.1, FTP_TRP.1	This package has to be added in any configuration	Definition of END_TO_END Information Flow Control SFP : protection of the PAN for end-to-end transmission
SRED Surrogate PAN Package	FCS_COP.1, FDP_IFC.1, FDP_IFF.1	This package has to be added **if the TOE enables the creation of surrogate values for the PAN**	Definition of SURROGATE_PAN Information Flow Control SFP : protection of the surrogate values of PAN

Table 17: SFR packages in the SRED PP-Module

638 A general note for all of the SRED SFRs:

Several of these SFRs are already contained in a very similar form in the underlying configuration from the POI PP, in particular if the underlying configuration is POI-COMPREHENSIVE. This may lead to some redundancies. Note that such redundancies are "removed" automatically during later evaluation steps when mapping SFRs to TSFI during ADV_FSP activities, because identical functionality will be mapped on the same TSFI. Therefore these redundancies should have no impact on the TOE design and testing documentation, except for some mapping tables, which are longer in this case.

12.4.1.1 SRED Basis Package

Note: The "dependencies"-part of each SFR is omitted in this chapter for brevity. All dependencies are as defined in CC, Part 2, and the rationale for the dependencies are contained in chapter 12.4.3.3.

FMT_SMR.1/SRED Security roles

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

FMT_SMR.1.2/SRED 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, TOE_PAN_SK, E2E_PAN_SK/E2E_PAN_PK*
- *Risk Manager is related to status of ENC_PIN, E2E_CIPHER_PAN.*
- *PCI K9: If the device may be accessed remotely for the purposes of administration, all access attempts must be cryptographically authenticated. If the authenticity of the access request cannot be confirmed, the access request is denied.*

FIA_UID.1/SRED Timing of identification

FIA_UID.1.1/SRED 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/SRED 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 in particular related to the Terminal Management System and/or Terminal Administrator and to the Risk Manager.*

- *PCI K9: If the device may be accessed remotely for the purposes of administration, all access attempts must be cryptographically authenticated. If the authenticity of the access request cannot be confirmed, the access request is denied.*

{ XE "FDP_ITC.1/SRED" }

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

FDP_ITC.1.1/SRED The TSF shall enforce the **Application Separation SFP** when importing user data, controlled under the SFP, from outside of the TOE.

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

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

- **PAN encryption keys (TOE_PAN_SK, E2E_PAN_SK/E2E_PAN_SK) are stored in the CoreTSF (Security Module of PED) or encrypted.**
- **the salt used to generate surrogate PAN (SURROGATE_PAN_SALT) is stored by MiddleTSF**
- **[assignment: additional importation control rules]**.

Application Note:

- *Note that the subjects, objects and operations for the Application Separation SFP are defined in FDP_ACC.1/SRED.*
- *Contribution to PCI K11.1, PCI K12 as defined in [EPC B4].*

{ XE "FPT_FLS.1/SRED" }

FPT_FLS.1/SRED Failure with preservation of secure state

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

failure of TSF self-test

logical anomalies of TSF

[assignment: list of types of failures in TSF].

Application Note:

- *The "secure state" does not provide access to any PAN value, PAN encryption key or any other TSF secret data.*
- *Contribution to PCI K11.1, PCI K13 as defined in [EPC B4].*

{ XE "FIA_UAU.2/SRED" }

FIA_UAU.2/SRED User authentication before any action

FIA_UAU.2.1/SRED 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 K22: 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, account data, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.*
- *Loading of Firmware, Application software and updates of these two are considered sensitive. Therefore this SFR implies that they require authentication. More particular updates need to provide authenticity of the updated code using cryptographical means (see PCI K11.1, K12 as defined in [EPC B4]).*

{ XE "FDP_ACC.1/SRED" **}**

FDP_ACC.1/SRED Subset access control

FDP_ACC.1.1/SRED The TSF shall enforce the **Application Separation SFP** on

- **subjects: POI and its Payment Application Logic**
- **objects:**
  - **Payment Transaction Data, POI Management Data, POI_SK, Cardholder communication interface**
  - **TOE_CLEAR_PAN**
  - **TOE_CIPHER_PAN and TOE_PAN_SK**
  - **E2E_CIPHER_PAN and E2E_PAN_SK/E2E_PAN_PK**
  - **SURROGATE_PAN and SURROGATE_PAN_SALT**
  - **[assignment: list of payment application internal data]**
- **operations: send, receive, access.**

{ XE "FDP_ACF.1/SRED" **}**

FDP_ACF.1/SRED Security attribute based access control

FDP_ACF.1.1/SRED The TSF shall enforce the **Application Separation SFP** to objects based on the following:

- **subjects: POI and its Payment Application Logic**
- **objects:**

  - **Payment Transaction Data, POI Management Data, POI_SK, Card-holder communication interface**
  - **TOE_CLEAR_PAN**
  - **TOE_CIPHER_PAN and TOE_PAN_SK**
  - **E2E_CIPHER_PAN and E2E_PAN_SK/E2E_PAN_PK**
  - **SURROGATE_PAN and SURROGATE_PAN_SALT**
  - **[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**
- **security attribute of TOE_PAN_SK, E2E_PAN_SK, E2E_PAN_PK: purpose and validity**
- **security attribute of TOE_CLEAR_PAN, TOE_CIPHER_PAN, E2E_CIPHER_PAN, SURROGATE_PAN, SURROGATE_PAN_SALT: access right of Payment Application**
- **[assignment: list of security attributes]**.

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

- **PCI K20: If the device supports multiple applications, it must enforce the separation between applications. It must not be possible that one application interferes with or tampers with another application or the firmware of the device including, but not limited to, modifying data objects belonging to another application or the firmware.**

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

- **POI Management Data and Payment Transaction Data shall only be accepted if the data are authentic.**
- **POI Management Data and Payment Transaction Data are only 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/SRED 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:

- *PCI K20 requirement can also be covered by extending the original PP POI FDP_ACC.1 and FDP_ACF.1 requirement to the new sensitive assets defined by SRED PP-Module*
- *If the author of the ST has no additional information flow control SFP rules or rules based on security attributes these parts shall be filled with none.*

{ XE "FTA_SSL.3/SRED" **}**

FTA_SSL.3/SRED TSF-initiated termination

FTA_SSL.3.1/SRED 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**[15].

Application Note:

- *PCI K23: 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.*

{ XE "FPT_PHP.3/SRED" **}**

FPT_PHP.3/SRED Resistance to physical attack

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

- **PCI K1.1: 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.**
- **PCI K1.1: Insertion of both an IC card and any other foreign object within the card insertion slot.**
- **PCI K1.1: 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 K3: Penetration of the PED to disclose the PAN encryption keys.**
- **PCI K3.1: Unauthorized modification or substitution of public keys stored in the device**
- **PCI K1.1: Additions, substitutions, or modifications on MSR that would allow determination or modification of Magnetic Stripe data**
- **PCI K1.1: If the MSR is part of an unattended devices, TSF shall contain an anti-removal mechanism to protect against unauthorized removal and/or unauthorized re-installation.**
- **[assignment: additional physical tampering scenarios]**

[15] "Normal mode" means a mode, where use of sensitive functions or services is not possible without new authentication of the user.

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:

- 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 (PAN, secret cryptographic keys, salt used to generate the surrogate PAN, administration passwords, etc.).
- The PED makes inaccessible any PAN 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 the assignment with none*
- *Contribution to PCI K19*

{ XE "FPT_EMSEC.1/SRED" **}**

FPT_EMSEC.1/SRED TOE Emanation

FPT_EMSEC.1.1/SRED The TOE shall not emit

- **PCI K3: sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring,**

in excess of **none** enabling access to **to PAN encryption keys** and **none**.

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

- **PCI K3: sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring,**

to gain access to **PAN encryption keys** and **none**.

Application Note:

- *Supports PCI K3. Recall that the scope of this SFR shall contain at least the MSR, IC Card Reader and PAN encryption module (PED Security Module).*

{ XE "FMT_MSA.1/SRED" **}**

FMT_MSA.1/SRED Management of security attributes

FMT_MSA.1.1/SRED The TSF shall **e**nforce the **ENCRYPTING_MODE Information Flow Control SFP** to restrict the ability to **modify** the security attributes **operation mode** to **Risk Manager**.

Application Note:

- *operation mode (encrypting / non-encrypting mode) may be modified by the Risk Manager.*
- *PCI K15: Status of operation mode having the value "Encrypting mode" means that the device's encryption of account data functionality is enabled and operational.*
- *PCI K15: For devices that allow the modification of Status of operation mode, the change to "encrypting mode" must result in the firmware revision number changing and the device providing visual indication of SRED enablement. The change to "non encrypting mode" must result in the firmware revision number reverting and the device no longer providing visual indication of SRED enablement.*
- *PCI K15: If whitelist(s) are utilized to exclude card data from mandatory encryption, the whitelist shall be cryptographically authenticated either prior to being instantiated in the device or before being utilized.*
- *Note: enablement/disablement of "encrypting mode" could have been formalized via a FMT_SMF requirement instead of FMT_MSA; current FMT_MSA wording has been retained because it enables to define more clearly the role of the "encrypting mode" security attribute in the corresponding flow control policies.*

{ XE "FPT_TST.1/SRED" **}**

FPT_TST.1/SRED TSF testing

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

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

to demonstrate the correct operation o**f**

- **the CoreTSF PED (CORE_SW and CORE_HW).**
- **the PEDMiddleTSF**.

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

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

Application Note:

Contribution to PCI K11.1, PCI K12.

{ XE "FTP_ITC.1/SRED" }

FTP_ITC.1/SRED Inter-TSF trusted channel

FTP_ITC.1.1/SRED 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/SRED The TSF shall permit **[selection: the TSF, another trusted IT product]** to initiate communication via the trusted channel.

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

Application Note:

PCI K6: The device supports data origin authentication of encrypted messages.

12.4.1.2 SRED Cryptography Package

This package defines cryptography requirements related to PCI K4, PCI K5, PCI K17 and PCI K18requirements. They are built on their counterparts in PP POI:

FTP_ITC.1 Inter-TSF trusted channel

FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2 Import of user data with security attributes

FCS_COP.1 Cryptographic operation

{ XE "FTP_ITC.1/SRED_CRYPTO" }

FTP_ITC.1/SRED_CRYPTO Inter-TSF trusted channel

FTP_ITC.1.1/SRED_CRYPTO 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/SRED_CRYPTO The TSF shall permit **[selection: the TSF, another trusted IT product]** to initiate communication via the trusted channel.

FTP_ITC.1.3/SRED_CRYPTO The TSF shall initiate communication via the trusted channel for **importing cryptographic keys including E2E_CIPHER_PK/E2E_CIPHER_SK and TOE_CIPHER_SK, [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.*
- *this SFR is related to the import of keys for the encipherment of E2E_CIPHER_PAN (in order to be transmitted to the acquirer) as well as encipherment of TOE_CIPHER_PAN (in order to be transmitted between parts of the TOE) and decipherment of TOE_CIPHER_PAN by the PED SM.*
- *PCI K5: If remote key distribution is used, the device supports mutual authentication between the sending key distribution host and receiving device.*
- *Contribution to PCI K4 and K17.*

{ XE "FPT_TDC.1/SRED_CRYPTO" **}**

FPT_TDC.1/SRED_CRYPTO Inter-TSF basic TSF data consistency

FPT_TDC.1.1/SRED_CRYPTO The TSF shall provide the capability to consistently interpret **cryptographic keys including E2E_CIPHER_PK/E2E_CIPHER_SK and TOE_CIPHER_SK key derivation methodology or an equivalent methodology for maintaining the TDEA Key Bundle, and [assignment: list of TSF data types]** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/SRED_CRYPTO The TSF shall use **ISO 11568 and/or ANSI X9.24 and ANSI TR-31 or an equivalent methodology [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.

- *this SFR is related to the import of keys for the encipherment of TOE_CLEAR_PAN into TOE_CIPHER_PAN as well as E2E_CIPHER_PAN, and decipherment of TOE_CIPHER_PAN by the PED SM.*
- *Contribution to PCI K4 and K17.*

{ XE "FDP_ITC.2/SRED_CRYPTO" **}**

FDP_ITC.2/SRED_CRYPTO Import of user data with security attributes

FDP_ITC.2.1/SRED_CRYPTO 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/SRED_CRYPTO The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/SRED_CRYPTO 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/SRED_CRYPTO 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/SRED_CRYPTO 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, supporting the ANSI TR-31 key derivation methodology or an equivalent methodology for maintaining the TDEA Key Bundle**.

Application Note:

- *This SFR is related to the import of keys for the encipherment of E2E_CIPHER_PAN (in order to be transmitted to the acquirer) as well as encipherment of TOE_CIPHER_PAN (in order to be transmitted between parts of the TOE) and decipherment of TOE_CIPHER_PAN into TOE_CLEAR_PAN by the PED SM.*
- *The author of the Security Target shall iterate this SFR for each TSF part, which needs FCS_COP.1/SRED_CRYPTO (see the application notes for that SFR) in the context of one of the SRED-Packages. In FDP_ITC.2.1/SRED_CRYPTO the ST author shall assign the SFP related to that SRED package.*
- *Contribution to PCI K4 and K17.*

{ XE "FCS_COP.1/SRED_CRYPTO" **}**

FCS_COP.1/SRED_CRYPTO Cryptographic operation

FCS_COP.1.1/SRED_CRYPTO The TSF shall perform **encipherment/decipherment of PAN** in accordance with a specified cryptographic algorithm **[selection: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **ANSI X9 or ISO-approved encryption algorithms (e.g., AES, TDES)**.

Application Note:

- *The author of the Security Target shall iterate this SFR for each TSF part if necessary.*
- *This SFR is related to the encipherment of TOE_CLEAR_PAN into E2E_CIPHER_PAN (in order to be transmitted to the acquirer) as well as TOE_CIPHER_PAN (in order to be transmitted between parts of the TOE) and decipherment of TOE_CIPHER_PAN by the PED SM.*
- *PCI K18: The following are examples of techniques that may be used to prevent an exhaustive PAN determination attack, such as one producing random transactions through the device until the ciphertext produced equals the ciphertext recorded when the device was in operational use:*
  - *Use of a unique key per transaction technique. (Prevents the attack.)*
  - *Limiting the rate at which the device will encrypt PANs. (Deters the attack.) For example, the function would be a maximum of the throughput that could be achieved through the physical interface during intended usage.*
- *Contribution to K4*

12.4.1.3 SRED Distributed Architecture Package

639 This package addresses the need for protection of the PAN when the TOE is operating as distributed architecture

640 "Distributed architecture" has here to be understood as POI architectures where the PED and the Card Reader are separated devices (i.e. not integrated into one single tamper-responsive boundary).

641 If the TOE is operating in encrypting mode, the cleartext PAN (TOE_CLEAR_PAN) has to be ciphered (TOE_CIPHER_PAN) by the Card Reader prior to sending it to the PED, which then deciphers it before ciphering it again (E2E_CIPHER_PAN) for the Acquirer.

642 This package is not required if the TOE has an integrated architecture.

{ XE "FDP_IFC.1/SRED_INT" **}**

FDP_IFC.1/SRED_INT Subset information flow control

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

- **subjects: MSR, IC Card Reader**
- **information: TOE_CLEAR_PAN, TOE_CIPHER_PAN, TOE_PAN_SK**
- **operations: send (TOE_CLEAR_PAN, TOE_CIPHER_PAN), send/receive (TOE_PAN_SK)**.

{ XE "FDP_IFF.1/SRED_INT" **}**

FDP_IFF.1/SRED_INT Simple security attributes

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

- **subjects: MSR, IC Card Reader**
- **information: TOE_CLEAR_PAN, TOE_CIPHER_PAN, TOE_PAN_SK**
- **status of TOE_PAN_SK: validity, purpose**
- **operation mode of the PED: encrypting, non encrypting [assignment: other TOE_PAN_SK security attributes]**.

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

- **PCI K1: TOE_CLEAR_PAN is either encrypted immediately upon entry or entered in clear-text into the device and processed within the secure controller of the device.**
- **The IC Card Reader and MSR may send TOE_CIPHER_PAN to the PED**.

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

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

- **The IC Card Reader and MSR do not send or receive TOE_PAN_SK to/from any subject.**
- **The IC Card Reader and MSR do not send TOE_CLEAR_PAN to any subject.**
- **The IC Card Reader and MSR do not send TOE_CIPHER_PAN to any other subject than the PED.**
- **PCI K18: The device has characteristics that prevent or significantly deter the use of the device for exhaustive PAN determination.**
- **PCI K8: Encryption or decryption of any arbitrary data using any account data-encrypting key or key-encrypting key contained in the device is not permitted. The device must enforce that account data keys, key-encipherment keys, and PIN-encryption keys have different values.**
- **PCI K15: When operating in encrypting mode, there is no mechanism in the IC Card Reader, MSR or PED that would allow the outputting of a private or secret cleartext key or cleartext PAN, the encryption of a key or PAN 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:

- *Contribution to PCI K15: When operating in encrypting mode, there is no mechanism in the IC Card Reader, MSR or PED that would allow the outputting of a private or secret cleartext key or cleartext PAN, the encryption of a key or PAN 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.*
- *If the author of the ST has no additional information flow control SFP rules or 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 K8: this PCI requirement is processed the same manner as PCI B13 in the PP POI.*
- *PCI K18: this PCI requirement is processed the same manner as PCI B10 in the PP POI.*
- *PAN encryption keys (TOE_PAN_SK) are stored in the Security Module of the component or encrypted.*

{ XE "FDP_ITT.1/SRED_INT" **}**

FDP_ITT.1/SRED_INT Basic internal transfer protection

FDP_ITT.1.1/SRED_INT The TSF shall enforce the **INTERNAL_PROTECTION Information Flow Control SFP** to prevent the **disclosure and modification** of user data when it is transmitted between physically-separated parts of the TOE.

Application Note:

The physical separation of components has to be understood in terms of

- *physically-separated parts of the PED or*
- *between the Card Reader (either IC Card Reader or MSR) and PED.*

{** XE "FMT_MSA.3/SRED_INT" **}{** XE "FMT_MSA.1/SRED_INT" **}

FMT_MSA.1/SRED_INT Management of security attributes

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

{ XE "FDP_RIP.1/SRED_INT" **}**

FDP_RIP.1/SRED_INT Subset residual information protection

FDP_RIP.1.1/SRED_INT 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:

- **TOE_CLEAR_PAN immediately after being ciphered into TOE_CIPHER_PAN by IC Card Reader or MSR**

- **TOE_CIPHER_PAN immediately after being sent to the PED by IC Card Reader or MSR**
- **TOE_PAN_SK immediately after being used to cipher TOE_CLEAR_PAN into TOE_CIPHER_PAN by IC Card Reader or MSR [assignment: sensitive objects with residual information]**.

Refinement:

- **These deallocations are performed by the Card Reader (either IC Card Reader or encrypting MSR). Deallocation by the PED upon reception is addressed in the End-to-end protection Package.**
- **Deallocation may occur upon completion of the transaction or if the MSR or IC Card Reader has timed-out waiting from the Cardholder or Merchant.**

Application Note:

- *Contribution to PCI K15.2: Account data (in either clear-text or encrypted form) shall not be retained any longer, or used more often, than strictly necessary.*
- *The IC Card Reader or MSR must automatically clear its internal buffers when either: The transaction is completed, or the IC Card Reader or MSR 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.*

12.4.1.4 SRED End-to-end protection Package

643 This package addresses the supplementary need for protection of the PAN in the context of end-to-end encryption between the POI and the Acquirer, also called "encrypting mode" in PCI SRED requirements. It introduces

- *the assets E2E_CIPHER_PAN, E2E_PAN_SK and E2E_PAN_PK, which are the PAN encrypted for transmission to the acquirer, and the corresponding keys*
- *the assets Ciphertext TOE_CLEAR_PAN, TOE_CIPHER_PAN, TOE_PAN_SK, which are the PAN in cleartext or ciphertext received by the PED, and the corresponding key.*

644 Note: The cleartext TOE_CLEAR_PAN can also be transmitted by the PED, but only to authenticated applications within the device.

{ XE "FDP_IFC.1/SRED_E2E" **}**

FDP_IFC.1/SRED_E2E Subset information flow control

FDP_IFC.1.1/SRED_E2E The TSF shall enforce the **END_TO_END Information Flow Control SFP** on

- **subjects: PED (in the sense of the tamper responsive TOE part responsible for protection of the PAN)**
- **information: E2E_PAN_SK, E2E_PAN_PK**
- **operations: receive**
- **information: E2E_CIPHER_PAN**
- **operations: send.**
- **information: TOE_CIPHER_PAN, TOE_CLEAR_PAN, TOE_PAN_SK**
- **operations: receive.**

{ XE "FDP_IFF.1/SRED_E2E" }

FDP_IFF.1/SRED_E2E Simple security attributes

FDP_IFF.1.1/SRED_E2E The TSF shall enforce the **END_TO_END Information Flow Control SFP** based on the following types of subject and information security attributes:

- **subjects: PED (in the sense of the tamper responsive TOE part responsible for protection of the PAN)**
- **information: E2E_CIPHER_PAN, E2E_PAN_SK/E2E_PAN_PK**
- **status of E2E_PAN_SK/E2E_PAN_PK: validity, purpose**
- **operation mode of the PED: encrypting, non encrypting**
- **information: TOE_CIPHER_PAN, TOE_CLEAR_PAN, TOE_PAN_SK**
- **status of TOE_PAN_SK: validity, purpose**
- **operation mode of the PED: encrypting, non encrypting**
- **[assignment: other E2E_PAN_SK/E2E_PAN_PK security attributes].**

FDP_IFF.1.2/SRED_E2E The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **PCI K1: TOE_CLEAR_PAN is either encrypted immediately upon entry or entered in clear-text into the device and processed within the secure controller of the device.**
- **PCI K15.1: The PED can transfer a cleartext TOE_CLEAR_PAN to an authenticated application within the device.**
- **The PED can receive TOE_CIPHER_PAN from the Card Reader. The PED deciphers TOE_CIPHER_PAN into TOE_CLEAR_PAN with the appropriate dedicated key immediately after it is is received from Card Reader (either IC Card Reader or MSR).**
- **The PED can receive TOE_CLEAR_PAN from the Card Reader.**
- **If the operating mode is "encrypting" the PED enciphers TOE_CLEAR_PAN with the appropriate dedicated keybefore it is sent to external entities.**
- **FDP_IFF.1.3/SRED_E2E The TSF shall enforce the [assignment: additional information flow control SFP rules]**.

FDP_IFF.1.4/SRED_E2E 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/SRED_E2E The TSF shall explicitly deny an information flow based on the following rules:

- **PCI K5: The PED do not receive E2E_PAN_SK or E2E_PAN_PK from any other subject than an authenticated key distribution host.**
- **PCI K15.1: If the operating mode is "encrypting" the PED does not send the TOE_CLEAR_PAN to any other subject than an authenticated application within the device**
- **The PED does not send E2E_PAN_SK to any subject before being encrypted.**
- **The PED does not accept a TOE_CLEAR_PAN or TOE_CIPHER_PAN from any other subject than the Card Reader (either IC Card Reader or MSR).**

- **PCI K18: The device has characteristics that prevent or significantly deter the use of the device for exhaustive PAN determination.**
- **PCI K8: Encryption or decryption of any arbitrary data using any account data-encrypting key or key-encrypting key contained in the device is not permitted. The device must enforce that account data keys, key-encipherment keys, and PIN-encryption keys have different values.**
- **PCI K15: there is no mechanism in the device that would allow the outputting of clear-text account data, which has been entered in operating mode "encrypting". Changing between an encrypting and non-encrypting mode of operation requires explicit authentication.**

Application Note:

- *If the author of the ST has no additional information flow control SFP rules or 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.*
- *This SFR forces the encipherment of TOE_CLEAR_PAN. The enciphering must be unique to the transaction, e.g. it is not allowed to produce the same enciphered form for a PAN in different transactions to avoid recognition of PAN values. Additionally, TOE_CLEAR_PAN is only allowed to be enciphered with cryptographic keys only used for PAN encipherment and not used for any other purpose. The SFR enforces that any ENC_PAN_PK is different from any other cryptographic key. However accidental choice of the same value is allowed.*
- *PCI K8: this PCI requirement is processed the same manner as PCI B13 in the PP POI.*
- *PCI K18: this PCI requirement is processed the same manner as PCI B10 in the PP POI.*
- *PCI K15: Within the frame of END_TO_END Information Flow Control SFP (i.e. when operating in encrypting mode), there is no mechanism in the device that would allow the outputting of clear-text account data.*
- *secret parts of the PAN encryption keys (E2E_PAN_SK) are only stored in the Security Module of PED or encrypted.*

{ XE "FMT_MSA.3/SRED_E2E" **}{** XE "FMT_MSA.1/SRED_E2E" **}**

FMT_MSA.1/SRED_E2E Management of security attributes

FMT_MSA.1.1/SRED_E2E The TSF shall enforce the **END_TO_END Information Flow Control SFP** to restrict the ability to **modify** the security attributes **of E2E_CIPHER_PAN -** and **of E2E_PAN_SK/E2E_PAN_PK**

to **Risk Manager -** and **[selection: Terminal Management System and/or Terminal Administrator]**.

Application Note:

- *Status of E2E_CIPHER_PAN may be modified by the Risk Manager.*
- *Status of E2E_PAN_SK/E2E_PAN_PK may be modified by Terminal Management System and/or Terminal Administrator.*

{ XE "FIA_UID.1/SRED_E2E" **}**

FIA_UID.1/SRED_E2E Timing of identification

FIA_UID.1.1/SRED_E2E 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/SRED_E2E 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 and to the Risk Manager.*

{ XE "FDP_RIP.1/SRED_E2E" **}**

FDP_RIP.1/SRED_E2E Subset residual information protection

FDP_RIP.1.1/SRED_E2E 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:

- **TOE_CIPHER_PAN immediately after being deciphered into TOE_CLEAR_PAN,**
- **TOE_CLEAR_PAN immediately after being enciphered into E2E_CIPHER_PAN,**
- **temporary cryptographic keys**
- **[assignment: sensitive objects with residual information].**

Deallocation may occur upon completion of the transaction or if the IC Card Reader or MSR has timed-out waiting from the Cardholder or merchant.

Application Note:

- *PCI K15.2: Account data (in either clear-text or encrypted form) shall not be retained any longer, or used more often, than strictly necessary.*
- ***If the PED and Card Reader (either MSR or IC Card Reader) are integrated into the same tamper-responsive boundary**, TOE_CLEAR_PAN is enciphered into E2E_CIPHER_PAN by the SM of the PED immediately after their reception.*
- ***If the PED and Card Reader (either encrypting MSR or IC Card Reader) are not integrated into the same tamper-responsive boundary**, then the TOE_CLEAR_PAN is enciphered within the SM of the Card Reader (either IC Card Reader or encrypting MSR head) immediately after reception. TOE_CIPHER_PAN is sent to the PED, which shall decipher it prior to encipher it as E2E_CIPHER_PAN. Between decipherment and encipherment, TOE_CLEAR_PAN shall not be retained any longer, or used more often, than strictly necessary.*

- *In any case, The TSF must automatically clear its internal buffers when either: The transaction is completed, or the TSF 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.*

{ XE "FDP_ITT.1/SRED_E2E" **}**

FDP_ITT.1/SRED_E2E Basic internal transfer protection

FDP_ITT.1.1/SRED_E2E 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 **END_TO_END Information Flow Control SFP** to prevent the **disclosure** of **E2E_CIPHER_PAN and E2E_PAN_SK/E2E_PAN_PK [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 E2E_CIPHER_PAN and E2E_PAN_SK/E2E_PAN_PK shall be protected when they are transmitted between physically-separated parts of the PED.*

{ XE "FTP_TRP.1/SRED_E2E" **}**

FTP_TRP.1/SRED_E2E Trusted path

FTP_TRP.1.1/SRED_E2E 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 E2E_PAN_SK/E2E_PAN_PK replacement and E2E_PAN_SK/E2E_PAN_PK misuse**.

FTP_TRP.1.2/SRED_E2E The TSF shall permit **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3/SRED_E2E The TSF shall require the use of the trusted path for **E2E_PAN_SK/E2E_PAN_PK replacement and E2E_PAN_SK/E2E_PAN_PK usage**.

Application Note:

- *If the TSF can hold multiple PAN encryption keys and if the key to be used to encrypt the PAN can be externally selected, then the PED prohibits unauthorised key replacement and key misuse.*

- *If the TSF does not hold multiple PAN encryption keys or if the key to be used to encrypt the PAN cannot 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 TSF component that performs the PAN 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 TSF 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 PAN encryption. If an application can select keys from multiple key hierarchies, the TSF must enforce authentication of commands used for external key selection. If the TSF only allows an application to select keys from a single hierarchy, then command authentication is not required.*

12.4.1.5 SRED Surrogate PAN Package

645 This package is intended for devices using hash functions to generate surrogate PAN values, e.g. in order to exploit a client database outside the device without having to disclose the PAN value.

646 SFRs in this package are applicable to MiddleTSF in POI-COMPREHENSIVE configuration.

{ XE "FCS_COP.1/SRED_SURROGATE_PAN" **}**

FCS_COP.1/SRED_SURROGATE_PAN Cryptographic operation

FCS_COP.1.1/SRED_SURROGATE_PAN The TSF shall perform **Generation of SURROGATE_PAN** in accordance with a specified cryptographic algorithm **[selection: hash, other method]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Refinement:

PCI K16: If the device is capable of generating surrogate PAN values to be outputted outside of the device, it is not possible to determine the original PAN knowing only the surrogate value.

PCI K16.1: If using a hash function to generate surrogate PAN values, hash shall use an input salt of a minimum length of 64 bits.

Application Note:

- *The author of the Security Target shall iterate this SFR for each TSF part if necessary.*
- *Contribution to PCI K16: If the device is capable of generating SURROGATE_PAN to be outputted outside of the device, it is not possible to determine the original TOE_CLEAR_PAN knowing only the surrogate value.*

- *Contribution to PCI K16.1: If using a hash function to generate SURROGATE_PAN, input to the hash function must use a SURROGATE_PAN_SALT with minimum length of 64-bits.*

{ XE "FDP_IFC.1/SRED_SURROGATE_PAN" **}**

FDP_IFC.1/SRED_SURROGATE_PAN Subset information flow control

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

- **subjects: PED**
- **information: SURROGATE_PAN, SURROGATE_PAN_SALT**
- **operations: send.**

{ XE "FDP_IFF.1/SRED_SURROGATE_PAN" **}**

FDP_IFF.1/SRED_SURROGATE_PAN Simple security attributes

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

- **subjects: PED**
- **information: SURROGATE_PAN, SURROGATE_PAN_SALT**
- **no security attribute.**

FDP_IFF.1.2/SRED_SURROGATE_PAN 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 can transfer a SURROGATE_PAN outside the device.

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

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

- **PCI K18: The device has characteristics that prevent or significantly deter the use of the device for exhaustive PAN determination.**
- **PCI K8: Encryption or decryption of any arbitrary data using any account data-encrypting key or key-encrypting key contained in the device is not permitted. The device must enforce that account data keys, key-encipherment keys, and PIN-encryption keys have different values.**
- **PCI K16.2: The PED cannot send the SURROGATE_PAN_SALT to any other subject.**

Application Note:

- *PCI K15: PAN data that is encrypted, hashed (with salt), masked or truncated PANs may be outputted from the device. Truncated PANs are typically defined as a maximum of the first six and the last four digits. However, due to differing PAN lengths, the determination must be made if the truncated digits offer sufficient protection against attacks designed to predict valid, full PANs (with longer BIN ranges). This would partially depend on the potential universe of PANs that could be included and if the vendor wishes to output more than first six and last four digits of PAN data (for greater than 16 digit PANs) they must demonstrate that the probability of PAN recovery for the larger PAN values are equivalent to the first six, last four determination for 16 digit PANs. If using truncation, any removed segment cannot be replaced with a hashed version of any component of the original PAN. Truncated and hashed versions of the same PAN must not be transmitted together unless encrypted.*
- *If the author of the ST has no additional information flow control SFP rules or 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 K8: this PCI requirement is processed the same manner as PCI B13 in the PP POI.*
- *PCI K18: this PCI requirement is processed the same manner as PCI B10 in the PP POI.*
- *the salt used to generate surrogate PAN (SURROGATE_PAN_SALT) is stored by MiddleTSF*

12.4.2 Security Assurance Requirements

647 The SRED PP-Module uses the assurance package of the underlying POI configuration, to which is added. It adds refinements to some of the assurance components. These refinements are defined in this section.

648 With regard to AVA_POI the SRED PP-Module has the following requirements:

- A very specific part of the SRED functionality, namely "14. Confidentiality, authenticity and integrity protection of keys (including authenticity and integrity of public keys) used to protect account data in payment transactions.", as listed in section 3.2.2 is considered part of the CoreTSF and therefore requires AVA_POI.1/CoreTSF (which uses POI-Moderate attack potential).
  Note:AVA_POI.1/CoreTSF is already defined in the underlying configuration. Evaluation under this component supports PCI K3.
- All other SRED functionality is part of feature 8. as listed in section 3.2.2. Therefore, according to Table 1 in section 3.2.2.1, it belongs to the "MiddleTSF" and requires AVA_POI.1/MiddleTSF, which uses POI-Basic attack potential. For an underlying PED-ONLY configuration AVA_POI.1/MiddleTSF has to be added to the assurance package.
  Notes: AVA_POI.1/MiddleTSF is already contained in the underlying package in the case of POI-COMPREHENSIVE. Evaluation under this component supports PCI K1.1.

649 Some PCI security requirements have been identified not to be security functional ones. These security requirements are introduced as refinements of ADV_ARC, AGD_OPE, AGD_PRE and ALC_CMC.

650 The other SARs are left unchanged from EAL2.

12.4.2.1 Refinements for SARs defined for the SRED PP-Module

{ XE "ADV_ARC.1/SRED" **}**

ADV_ARC.1 Security architecture description

Refinement for **ADV_ARC.1.3C:**

Refinement:

- PCI K2: Initialization includes the logical and physical integration of an approved card reader into a PIN entry POI terminal. Such integration does not create new attack paths to the account data. The account data is protected (consistent with PCI A2) from the input component to the secure controller of the device.

Refinement for **ADV_ARC.1.5C**

Refinement:

- PCI K1.2: Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms.
- PCI K21: The security architecture shall demonstrate how following features of the device's operating system are configured:
    - The operating system of the device must contain only the software (components and services) necessary for the intended operation.
    - The operating system must be configured securely and run with least privilege.
    - The security policy enforced by the device must not allow unauthorized or unnecessary functions.
    - API functionality and commands that are not required to support specific functionality must be disabled (and where possible, removed).

Application note for **ADV_ARC.1.1E**

Application Note:

- *Regarding ADV_ARC.1.3C refinement on integration: The objective of this requirement is to assess those terminals where the card reader is integrated into the final solution and to ensure that as an integrated device it does not create any new weaknesses or permit new attack methods to be used against the data. The ICC reader may consist of areas of different protection levels: the areas of the IC card itself, and the area holding retracted cards.*

- *Regarding ADV_ARC.1.5C refinement: In general, techniques may include any combination of tamper-detection methods. Security mechanisms must not rely on insecure services or characteristics provided by the device such as (but not limited to) its power supply and unprotected wires. Tamper-evident labels and similar methods involving tamper evidence are not considered a security mechanism. This requirement does not imply the need for redundant security mechanisms, but rather separate mechanisms of a different nature.*

AGD_OPE.1 Operational user guidance

Refinement for **AGD_OPE.1.2C**

Refinement:

- K11.2: The vendor must provide clear security guidance to ensure that the PED's functionality will 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 PAN or other sensitive information.

Refinement for **AGD_OPE.1.6C**

Refinement:

- K11.2: The vendor must provide clear security guidance to ensure that account data is not retained any longer, or used more often, than strictly necessary

Application note for **AGD_OPE.1.1E**

Application Note:

- *PCI K15: For devices that allow the modification of Status of operation mode, the change to "encrypting mode" must result in the firmware revision number changing and the device providing visual indication of SRED enablement. The change to "non encrypting mode" must result in the firmware revision number reverting and the device no longer providing visual indication of SRED enablement. The visual indication must not be transient. This must be documented in information provided by the vendor to the entities deploying these devices.*

{ XE "AGD_PRE.1/SRED" **}**

AGD_PRE.1 Preparative procedures

Refinement for **AGD_PRE.1.2C**

Refinement:

- The preparative procedures must define clearly, that during initialisation and key management procedures for the device, the following must be met: PCI K7: Secret and

private keys that reside within the device to support account data encryption are unique per device.

- PCI K21: If TOE user participation is required, the preparative procedures shall describe clearly how the TOE user can configure the device's operating system as follows:
  - The operating system of the device must contain only the software (components and services) necessary for the intended operation.
  - The operating system must be configured securely and run with least privilege.
  - The security policy enforced by the device must not allow unauthorized or unnecessary functions.
  - API functionality and commands that are not required to support specific functionality must be disabled (and where possible, removed).

{ XE "ALC_CMS.2/SRED" }

ALC_CMS.2 Parts of the TOE CM coverage

Refinement for **ALC_CMS.2.2C**

Refinement:

- PCI K10: 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.

12.4.3 Security Requirements Rationale

12.4.3.1 Objectives

651 This section justifies, how the security objectives for the TOE, which were newly defined for the SRED PP-Module, are supported by the SFRs in the SRED PP-Module.

O.PaymentTransaction

652 If the underlying configuration is POI-COMPREHENSIVE, this objective is already upheld by the SFRs in that configuration as shown in the corresponding rationale in section 10. In this case the following rationale can be considered as additional support. In the case of PED-ONLY, the following rationale covers the objective completely.

- The SRED Distributed Architecture Package protects payment data during internal transfer if the TOE is based on a distributed architecture.
- The SRED basis package defines access control rules, which make sure that only authentic management data can be used for TOE management and that only authorised applications can process payment data according to clearly defined rules ensuring authenticity and (where applicable) confidentiality.

O.POI_SW

- The SRED basis package, in particular FPT_FLS.1/SRED enforces the TSF authenticity and integrity by preserving a secure state in case of logical anomalies).
- 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 by the SRED basis package, in particular due to SFRs FDP_ACC.1/SRED, FDP_ACF.1/SRED and FDP_ITC.1/SRED.

O.POIApplicationSeparation

- The SRED basis package, in particular FDP_ACC.1/SRED and FDP_ACF.1/SRED ensure that no other application can interfere with security functions of a payment application.
- FDP_RIP.1/SRED ensures that no residual information remains in resources released by the payment application and payment application temporary cryptographic keys.

O.PANConfidentiality

- Confidentiality of the PAN for end-to-end encryption is addressed by SFRs from the SRED End-to-end protection Package.
- Confidentiality of the PAN when transmitted within the TOE is addressed by SFRs from the SRED Distributed Architecture Package
- Both packages rely on the SRED Cryptography package to ensure encipherment and decipherment operations.
- SRED Basis Package provides the common protection requirements such as physical resistance

O.PANDeduction

- Protection of the surrogate values generated from the PAN is addressed by SRED Surrogate PAN Package.

O. PANOperatingMode

- This is enforced by the SRED end-to-end protection package, in particular by the SFR FMT_MSA.1/SRED.

12.4.3.2 Rationale table of Security Objectives and SFRs

Security Objectives	Security Functional Requirements
O.PaymentTransaction	All SFRs from the SRED basis package. In case of a distributed architecture also all SFRs of the SRED distributed architecture package.
O.POI_SW	All SFRs from the SRED basis package, in particular FDP_ACC.1/SRED, FDP_ACF.1/SRED and FDP_ITC.1/SRED
O.POIApplicationSeparation	All SFRs from the SRED basis package, in particular FDP_ACC.1/SRED, FDP_ACF.1/SRED and FDP_RIP.1/SRED
O.PANConfidentiality	All SFRs from the packages SRED basis, SRED End-to-End protection and SRED cryptography. In case of a distributed architecture also all SFRs from the SRED Distributed architecture packages.
O.PANDeduction	All SFRs from the SRED Surrogate PAN Package
O.PANOperatingMode	All SFRs from the SRED base package, in particular FMT_MSA.1/SRED

Table 18: Security Objectives and SFRs in SRED- Coverage

12.4.3.3 Dependencies

SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FMT_SMR.1/SRED	(FIA_UID.1)	FIA_UID.1/SRED
FIA_UID.1/SRED	No Dependencies	
FDP_ITC.1/SRED	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FDP_ACF.1/SRED and (see below)
FPT_FLS.1/SRED	No Dependencies	
FIA_UAU.2/SRED	(FIA_UID.1)	FIA_UID.1/SRED
FDP_ACF.1/SRED	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SRED and (see below).
FDP_ACC.1/SRED	(FDP_ACF.1)	FDP_ACF.1/SRED
FTA_SSL.3/SRED	No Dependencies	
FPT_PHP.3/SRED	No Dependencies	
FPT_EMSEC.1/SRED	No Dependencies	
FMT_MSA.1/SRED	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/SRED_E2E, FMT_SMR.1/SRED see below for omitting FMT_SMF.1
FPT_TST.1/SRED	No Dependencies	
FTP_ITC.1/SRED	No Dependencies	
FTP_ITC.1/SRED_CRYPTO	No Dependencies	
FPT_TDC.1/SRED_CRYPTO	No Dependencies	
FDP_ITC.2/SRED_CRYPTO	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FTP_ITC.1/SRED_CRYPTO, FPT_TDC.1/SRED_CRYPTO, FDP_IFC.1/SRED_INT, FDP_IFC.1/SRED_E2E
FCS_COP.1/SRED_CRYPTO	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/SRED_CRYPTO and (see below)
FDP_IFC.1/SRED_INT	(FDP_IFF.1)	FDP_IFF.1/SRED_INT
FDP_IFF.1/SRED_INT	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/SRED_INT, and (see below)
FDP_ITT.1/SRED_INT	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/SRED_INT

Requirements	CC Dependencies	Satisfied Dependencies
FMT_MSA.1/SRED_INT	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1/SRED, FDP_IFC.1/SRED_INT see below for FMT_SMF.1
FDP_RIP.1/SRED_INT	No Dependencies	
FDP_IFC.1/SRED_E2E	(FDP_IFF.1)	FDP_IFF.1/SRED_E2E
FDP_IFF.1/SRED_E2E	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/SRED_E2E, and (see below)
FMT_MSA.1/SRED_E2E	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/SRED_E2E, FMT_SMR.1/SRED, see below for FMT_SMF.1
FIA_UID.1/SRED_E2E	No Dependencies	
FDP_RIP.1/SRED_E2E	No Dependencies	
FDP_ITT.1/SRED_E2E	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/SRED_E2E
FTP_TRP.1/SRED_E2E	No Dependencies	
FCS_COP.1/ SRED_SURROGATE_PAN	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	see below
FDP_IFC.1/ SRED_SURROGATE_PAN	(FDP_IFF.1)	FDP_IFF.1/SRED_E2E
FDP_IFF.1/ SRED_SURROGATE_PAN	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/SRED_SURROGATE_PAN and (see below)

Table 19: SFRs Dependencies in the SRED PP-Module

Rationale for the exclusion of Dependencies

- **The dependency FMT_MSA.3 of FDP_ITC.1/SRED is discarded.** There are no security attributes to be managed for downloading objects. Terminal Management System decides to update/download them or not.
- **The dependency FMT_MSA.3 of FDP_ACF.1/SRED is discarded.** No management functions are required for the considered assets.
- **The dependency FMT_SMF.1 of FMT_MSA.1/SRED is discarded.** There is no need to specify additional management functions because modification of security attributes is sufficient.
- **The dependency FCS_CKM.4 of FCS_COP.1/SRED_CRYPTO is discarded.** No specific cryptographic key destruction method is enforced. Keys are destroyed by erasing them.
- **The dependency FMT_MSA.3 of FDP_IFC.1/SRED_INT is discarded.** The roles responsible for managing the security attributes are defined in FMT_MSA.1/SRED_INT. These roles are also responsible for making sure that initial values of the attributes are set properly.
- **The dependency FMT_SMF.1 of FMT_MSA.1/SRED_INT is discarded.** There is no need to specify additional management functions because modification of security attributes is sufficient.
- **The dependency FMT_MSA.3 of FDP_IFC.1/SRED_E2E is discarded.** The roles responsible for managing the security attributes are defined in FMT_MSA.1/SRED_E2E. These roles are also responsible for making sure that initial values of the attributes are set properly.
- **The dependency FMT_SMF.1 of FMT_MSA.1/SRED_E2E is discarded.** There is no need to specify additional management functions because modification of security attributes is sufficient.
- **The dependency FCS_CKM.4 of FCS_COP.1/SRED_SURROGATE_PAN is discarded.** If a hash function is used, the following holds: A hash function does not use any cryptographic key; hence, a respective key destruction cannot be expected here. If a cryptographic algorithm with secret keys is used, the following holds: No specific cryptographic key destruction method is enforced. Keys are destroyed by erasing them.
- **The dependency FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 of FCS_COP.1/SRED_SURROGATE_PAN is discarded.** If a hash function is used, the following holds: A hash function does not use any cryptographic key; hence, neither a respective key import nor key generation can be expected here. If a different cryptographic function is used by a specific TOE, the ST author may need to add one of the SFRs required by the dependency or give a specific rationale for not needing the dependency otherwise.
- **The dependency FMT_MSA.3 of FDP_IFF.1/SRED_SURROGATE_PAN is discarded.** There are no security attribute to consider for this function

SARs Dependencies

653 Since all SARs are taken from the POI PP, the same rationale already given there holds (see section 9.2.1).

12.4.3.4 Rationale for the Security Assurance Requirements

654 The assurance requirements are taken from the POI configuration, to which the SRED PP-Module is added, and suitable refinements were added for some of them. A general rationale for the fact that the SRED PP-Module is consistent to the underlying configurations from the POI PP is given in chapter 12.5.

12.5 Rationale of consistency of the SRED PP-Module with the base PPs

655 As explained in chapter 1 and 2, the POI-COMPREHENSIVE base PP and the PED-ONLY base PP, possibly enhanced by the Open protocols package, are the four base PPs which can be extended by the SRED PP-Module given in 12**.** In order that the SRED PP-Module can be used without checking whether the SRED PP-Module is consistent to the chosen base PP, this chapter gives a rationale for the consistency.

656 As can be seen from the asset chapter in the SRED PP-Module, the assets addressed by the SRED PP-Module are consistent with the assets addressed by the base PP: The PAN in the SRED PP-Module is an element of PAY_DAT in the base PP and in the SRED PP-Module specific forms of the PAN are addressed (TOE_CLEAR_PAN, TOE_CIPHER_PAN and E2E_CIPHER_PAN).

657 In addition TOE_PAN_SK is defined which is a key used to protect the PAN during internal transmission. E2E_PAN_PK and E2E_PAN_SK are keys to used to protect the PAN when transferred end-to-end. These keys can be seen as instantiations of POI_SK and POI_PK. This is not a contradiction in the asset definition because all assets are clearly defined.

658 Finally SURROGATE_PAN and SURROGATE_PAN_SALT are assets introduced by the SRED PP-Module and clearly defined and therefore there is no contradiction to the assets of the base PP.

659 User and subjects are the same in the base PP and in the SRED PP-Module.

660 SRED PP-Module does not define additional threats, but refines the existing T.Transaction defined in PP POI. The refinement is consistent because it is related to the PAN and this does not contradict other threats.

661 There are no additional assumptions or OSPs.

662 The three objectives O.PaymentTransaction, O.POI_SW, and O.POIApplicationSeparation are added to the base PP in the case of PED-ONLY. That they are compatible with the base PP can be seen from the fact that they are already included in POI_COMPREHENSIVE, which is also an extension of POI_PED.

663 All other objectives of the SRED-Module add additional protection requirements for the PAN and related data: The objective of PAN confidentiality protection is added as a separate objective (O.PANConfidentiality), the objective of a surrogate PAN resisting to deduction is added as a separate objective (O.PANDeduction) and the objective of protection of SRED activation functions is added as a separate objective (O.PANOperatingMode). O.PANConfidentiality is a refinement of the base PP objectives addressing PAY_DAT and therefore does not contradict those. Surrogate PANs are introduced by the SRED PP-Module and thus O.PANDeduction does not contradict to any ob-

jectives of the base PP. O.PANOperatingMode introduces a new operating mode which does not contradict the base PP objectives.

664 There are no security objectives for the environment.

665 For the SFR part the following holds:

666 The PAN related SFRs of the SRED PP-Module do not contradict the PAY_DAT related SFRs because the base PP requires the POI to be able to protect all PAY_DAT sent or received by the POI against modification and PAY_DAT sent or received by the POI against disclosure. This is not a contradiction because the SFRs of the SRED PP-Module refine the SFRs of the base PP. The same holds for the keys of the SRED PP-Module. If a key of the SRED PP-Module is seen as an instantiation of POI_SK or POI_PK there is no contradiction for the same reason, i.e. a refinement of the usage of these keys when used to protect PAY_DAT.

667 In addition the table Table 17 in the beginning of chapter 12.4.1 “Security Functional Requirements” of 12 explains and thus gives a rationale for the relation of the SFRs to the base PP.

668 The SRED PP-Module does not assign attack potentials. This is done in the base PP. However, it has to be proven that the “linking pin” between the SRED PP-Module and the base PP is consistent. First the asset definition of the base PP and the SRED PP-Module is consistent because of the reference to the SRED PP-Module in the related chapter. In addition, the base PP introduces Account Data as the non-key assets of the SRED PP-Module and Account Data related keys as the key assets of the SRED PP-Module. The base PP requires the Account Data to be protected at a Basic level and the keys related to the account data to be protected at a Moderate level. Thus the asset link is consistent. The base PP assigns the assets and operations on them to TSFs, i.e. Account Data to MiddleTSF and Account Data related keys to CoreTSF. Assigning the protection level to the assets this clearly defines at which level the TSFs are to be protected. Considering the protection level of Account Data and PAY_DAT this is consistent because both are Low. Considering the protection level of POI_SK, POI_PK and the Account Data related keys, there is a difference because Account Data related keys are to be protected at a higher level. This is not an inconsistency because increasing the protection level is an allowed approach when the asset definition is clear.

669 The same argument holds for the assurance components.

13 Annex – EPC Book 4 to Common Criteria

13.1 EPC Book 4 Security Requirements

Note: EPCN requirements are not all explicitly included in [EPC B4] but derived from chap. 2.7 especially considering the applicability of requirements. SRED is not covered in this chapter, cf. section 12**.** SFR-supporting features due to Open Protocols are also not covered in this chapter.

Class	EPC Book 4 Security Requirements	Number
Core Physical Security Requirements		
PCI (N/A for the POI-CHIP-ONLY configuration according to [EPC B4], chap. 2.6.2)	The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data. 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 mechanism and insert a PIN-disclosing bug or gain access to secret information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader; and Note: The replacement of both the front and rear casings shall be considered as part of any attack scenario. All attacks shall include a minimum of ten hours' attack time for exploitation.	PCIA1
PCI (N/A for the POI-CHIP-ONLY configuration according to [EPC B4], chap. 2.6.2)	Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms.	PCIA2
PCI	The security of the device is not compromised by altering: - Environmental conditions. - Operational conditions (An example includes subjecting the device to tempera-	PCIA3

Class	EPC Book 4 Security Requirements	Number
Core Physical Security Requirements		
	tures or operating voltages outside the stated operating ranges).	
PCI (N/A for the POI-CHIP-ONLY configuration according to [EPC B4], chap. 2.6.2)	Sensitive functions or data are only used in the protected area(s) of the device. Sensitive data and functions dealing with sensitive data are protected from modification without requiring an attack potential of at least 26 for identification and initial exploitation	PCIA4
PCI (N/A for the POI-CHIP-ONLY configuration according to [EPC B4], chap. 2.6.2)	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 device operator or sales clerk—without requiring an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation.	PCIA5
PCI POI-CHIP-ONLY configuration according to [EPC B4], chap. 2.6.2)	Determination of any PIN-security-related cryptographic key resident in the device, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 35 for identification and initial exploitation with a minimum of 15 for exploitation. For POI in the POI-CHIP-ONLY configuration the attack potential is reduced. "…,requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation." In addition the requirement holds for secret keys protecting the authenticity and integrity of payment transaction data.	PCIA6 EPC-CHIP-ONLYA6
PCI	Note: If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: A7, B16.	

Class	EPC Book 4 Security Requirements	Number
Core Physical Security Requirements		
	- A7 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit. - B16 applies to devices that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer.	
PCI (N/A for the POI-CHIP-ONLY configuration according to [EPC B4], chap. 2.6.2)	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 without requiring an attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation.	PCIA7
PCI	The device provides a means to deter the visual observation of PIN values as they are being entered by the cardholder.	PCIA8
EPC PLUS	It is optional to have a privacy shield on a PED. However if a privacy shield is in place then it shall be according to EPC Guidelines on Privacy Shields.	EPC PlusA8.a
PCI (N/A for the POI-CHIP-ONLY configuration according to [EPC B4], chap. 2.6.2)	It is not feasible to penetrate the device to make any additions, substitutions, or modifications to the magnetic-stripe reader and associated hardware or software, in order to determine or modify magnetic-stripe track data, without requiring an attack potential of at least 16 per device, for identification and initial exploitation, with a minimum of 8 for exploitation.	PCIA9
PCI (N/A for the POI-CHIP-ONLY configura-	Secure components intended for unattended devices contain an anti-removal mechanism to protect against unauthorized removal and/or unauthorized re-installation. Defeating or circumventing this mechanism must require an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for exploita-	PCIA10

Class	EPC Book 4 Security Requirements	Number
Core Physical Security Requirements		
tion according to [EPC B4], chap. 2.6.2)	tion.	
PCI	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.	PCIA11
Core Logical Security Requirements		
PCI	The device performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the device is in a compromised state. In the event of a failure, the device and its functionality fail in a secure manner. The device must reinitialize memory at least every 24 hours.	PCIB1
PCI	The device'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 device outputting the clear-text PIN or other sensitive data.	PCIB2
PCI	The firmware, and any changes thereafter, have been inspected and reviewed using a documented and auditable process, and certified as being free from hidden and unauthorized or undocumented functions.	PCIB3
EPC PLUS	The initial review of the PED firmware must be performed by a testing laboratory.	EPC PlusB3.a
PCI	If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.	PCIB4
PCI	The firmware must support the authentication of applications loaded onto the terminal consistent with B4. If the device allows software application and/or configuration updates, the device cryptographically authenticates updates consistent with B4.	PCIB4.1
PCI	The device never displays the entered PIN digits. Any array related to PIN entry displays only non-significant symbols, e.g., asterisks.	PCIB5
PCI	Sensitive data shall not be retained any longer, or used more often, than strictly necessary. Online PINs are encrypted within the device immediately after PIN entry is	PCIB6

Class	EPC Book 4 Security Requirements	Number
Core Physical Security Requirements		
	complete and has been signified as such by the cardholder, e.g., via pressing the enter button. The device must automatically clear its internal buffers when either: The transaction is completed, or The device has timed out waiting for the response from the cardholder or merchant.	
PCI	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 data.	PCIB7
PCI	To minimize the risks from unauthorized use of sensitive services, limits on the number of actions that can be performed and a time limit imposed, after which the device is forced to return to its normal mode.	PCIB8
PCI	If random numbers are generated by the device in connection with security over sensitive data, the random number generator has been assessed to ensure it is generating numbers sufficiently unpredictable.	PCIB9
PCI	The device has characteristics that prevent or significantly deter the use of the device for exhaustive PIN determination.	PCIB10
EPC PLUS	The POI has characteristics that prevent the use of the device for exhaustive PIN determination.	EPC PlusB10.a
PCI	The key-management techniques implemented in the device conform to ISO 11568 and/or ANSI X9.24. Key management techniques must support the ANSI TR-31 key derivation methodology or an equivalent methodology for maintaining the TDEA key bundle.	PCIB11
PCI	The PIN encryption technique implemented in the device is a technique included in ISO 9564.	PCIB12
PCI	It is not possible to encrypt or decrypt any arbitrary data using any PIN encrypting key or key encrypting key contained in the device. The device must enforce that data keys, key-encipherment keys, and PIN-encryption keys, have different values.	PCIB13
PCI	There is no mechanism in the device 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	PCIB14

Class	EPC Book 4 Security Requirements	Number
Core Physical Security Requirements		
	itself be disclosed, or the transfer of a clear-text key from a component of high security into a component of lesser security.	
PCI	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 device display. If other data and the PIN are entered on the same keypad, the other data entry and the PIN entry shall be clearly separate operations.	PCIB15
PCI	Note: If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: A7, B16. - A7 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit. - B16 applies to devices that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer.	
PCI	All prompts for non-PIN data entry are under the control of the cryptographic unit of the device and requiring an attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation to circumvent. 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.	PCIB16
POI-CHIP-ONLY configuration according to [EPC B4], chap. 2.6.2)	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.	EPC-CHIP-ONLYB16
PCI	If the device supports multiple applications, it must enforce the separation between applications. It must not be possible that one application interferes with or tampers	PCIB17

Class	EPC Book 4 Security Requirements	Number
Core Physical Security Requirements		
	with another application or the OS of the device including, but not limited to, modifying data objects belonging to another application or the OS.	
PCI	The operating system of the device must contain only the software (components and services) necessary for the intended operation. The operating system must be configured securely and run with least privilege.	PCIB18
PCI	The vendor must provide adequate documented security guidance for the integration of any secure component into a PIN entry POI Terminal.	PCIB19
PCI	A user-available security policy from the vendor addresses the proper use of the POI in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements. The security policy must define the roles supported by the POI and indicate the services available for each role in a deterministic tabular format. The POI is capable of performing only its designed functions - i.e., there is no hidden functionality. The only approved functions performed by the POI are those allowed by the policy.	PCIB20
Online PIN Security Requirements		
PCI	If the device can hold multiple PIN-encryption keys and if the key to be used to encrypt the PIN can be externally selected, then the device prohibits unauthorized key replacement and key misuse.	PCIC1
Offline PIN Security Requirements		
PCI	It is neither feasible to penetrate the ICC reader to make any additions, substitutions, or modifications to either the ICC reader's hardware or software, in order to determine or modify any sensitive data, without requiring an attack potential of at least 20 for identification and initial exploitation, with a minimum of 10 for exploitation, nor is it possible for both an IC card and any other foreign object to reside within the card insertion slot. Note: All attacks shall include a minimum of ten hours' attack time for exploitation.	PCID1
PCI	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.	PCID2

Class	EPC Book 4 Security Requirements	Number
Core Physical Security Requirements		
PCI	The ICC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder.	PCID3
PCI	PIN protection during transmission within the PED (at least must comply):	PCID4
	If the device encrypting the PIN and the ICC reader are not integrated into the same secure module, and the cardholder verification method is determined to be:	
	- An enciphered PIN, the PIN block shall be enciphered between the device encrypting the PIN and the ICC reader using either an authenticated encipherment key of the IC card, or in accordance with ISO 9564.	PCID4.1
	- A plaintext PIN, the PIN block shall be enciphered from the device encrypting the PIN to the ICC reader (the ICC reader will then decipher the PIN for transmission in plaintext to the IC card) in accordance with ISO 9564.	PCID4.2
	If the device encrypting the PIN and the ICC reader are integrated into the same secure module, and the cardholder verification method is determined to be:	
	- An enciphered PIN, the PIN block shall be enciphered using an authenticated encipherment key of the IC card.	PCID4.3
	- - A plaintext PIN, then encipherment is not required if the PIN block is transmitted wholly through a protected environment (as defined in ISO 9564). If the plaintext PIN is transmitted to the ICC reader through an unprotected environment, the PIN block shall be enciphered in accordance with ISO 9564.	PCID4.4
POS Terminal Integration - Configuration Management		
EPC PLUS	L requirements must be checked by the testing lab. This includes a periodic site visit regarding critical steps in the manufacturing process (e.g. initial key loading).	EPCPlusL0
PCI	Change-control procedures are in place so that any intended security-relevant change to the physical or functional capabilities of the device causes a re-certification of the device under the Core PIN Entry and/or POS Terminal Integration Security Requirements of this document.	PCIL1

Class	EPC Book 4 Security Requirements	Number
Core Physical Security Requirements		
PCI	The certified firmware is protected and stored in such a manner as to preclude unauthorized modification during its entire manufacturing life cycle–e.g., by using dual control or standardized cryptographic authentication procedures.	PCIL2
PCI	The device is assembled in a manner that the components used in the manufacturing process are those components that were certified by the Core PIN Entry and/or POS Terminal Integration Security Requirements evaluation, and that unauthorized substitutions have not been made.	PCIL3
PCI	Production software (e.g., firmware) 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.	PCIL4
PCI	Subsequent to production but prior to shipment from the manufacturer's or reseller's facility, the device and any of its components are stored in a protected, access-controlled area or sealed within tamper-evident packaging to prevent undetected unauthorized access to the device or its components.	PCIL5
PCI	If the device will be authenticated at the key-loading facility or the facility of initial deployment by means of secret information placed in the device during manufacturing, then this secret information is unique to each device, unknown and unpredictable to any person, and installed in the device under dual control to ensure that it is not disclosed during installation.	PCIL6
PCI	Security measures are taken during the development and maintenance of POI security related components. The manufacturer must maintain development security documentation describing 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.	PCIL7
PCI	Controls exist over the repair process and the inspec-	PCIL8

Class	EPC Book 4 Security Requirements	Number
Core Physical Security Requirements		
	tion/testing process subsequent to repair to ensure that the device has not been subject to unauthorized modification.	
EPC PLUS	M requirements must be checked by the testing lab. This includes a periodic site visit regarding critical steps in the manufacturing process (e.g. initial key-loading).	EPC PlusM0
PCI	The POI should be protected from unauthorized modification with tamper-evident security features, and customers shall be provided with documentation (both shipped with the product and available securely online) that provides instruction on validating the authenticity and integrity of the POI. Where this is not possible, the POI is shipped from the manufacturer's facility to the initial key-loading facility or to the facility of initial deployment and stored en route under auditable controls that can account for the location of every POI at every point in time. Where multiple parties are involved in organizing the shipping, it is the responsibility of each party to ensure that the shipping and storage they are managing is compliant with this requirement.	PCIM1
PCI	Procedures are in place to transfer accountability for the device from the manufacturer to the facility.	PCIM2
PCI	While in transit from the manufacturer's facility to the initial key-loading facility, 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.	PCIM3
PCI	The device's development security documentation must provide means to the initial key-loading facility to assure the authenticity of the TOE's security relevant components.	PCIM4
PCI	If the manufacturer is in charge of initial key-loading, then the manufacturer must verify the authenticity of the POI security-related components.	PCIM5
PCI	If the manufacturer is not in charge of initial key-loading, the manufacturer must provide the means to the initial key-loading facility to assure the verification of the authenticity of the POI security-related components.	PCIM6

Class	EPC Book 4 Security Requirements	Number
Core Physical Security Requirements		
PCI	Each device shall have a unique visible identifier affixed to it.	PCIM7
PCI	The vendor must maintain a manual that provides instructions for the operational management of the POI. This includes instructions for recording the entire life cycle of the POI security-related components and of the manner in which those components are integrated into a single POI, e.g.: - Data on production and personalization - Physical/chronological whereabouts - Repair and maintenance - Removal from operation - Loss or theft	PCIM8
PLUS	Authenticity and integrity of payment transactions. Vendors must comply with all requirements of G1.	EPCN1
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 - 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.	EPCN1.1
PLUS	The transaction/accounting data shall be handled with authenticity and integrity in the POI.	EPCN1.2
PLUS	POI management data must be provided to the POI in an authentic way and must be protected against unauthorized change.	EPCN1.3
PLUS	Application integrity via application separation. Vendors must comply with all requirements of EPCN2.	EPCN2
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)	EPCN2.1
PLUS	The security of payment application in the POI must not be impacted by any other application. Payment application	EPCN2.2

Class	EPC Book 4 Security Requirements	Number
Core Physical Security Requirements		
	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).	
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.	EPCN2.3
PLUS	Authenticity and integrity of POI software. Vendors must comply with all requirements of G3.	EPCN3
PLUS	POI software must be provided to the POI in an authentic way and must be protected against unauthorized change.	EPCN.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.	EPCN3.2
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 defined in Appendix B of the PCI POS DTRs.	EPCN4
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.	EPCN5
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 PCIB11 whose scope is the PED.	EPCN6
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.	EPCN7

13.2 Mapping from EPC Book 4 to SFRs and SARs

670 The following table shows the mapping between EPC requirements from [EPC B4] and security requirements in this PP. EPCN requirements are not all explicitly included in [EPC B4] but derived from chap. 2.7 especially considering the applicability of requirements. All links except links to AVA_POI can be traced back to the statement of the requirements in this PP. SRED is not covered in this chapter, cf. section 12. SFR-supporting features due to Open Protocols are also not covered in this chapter.

CAS-requirement	**SFR**	**SAR**
PCIA1	FPT_PHP.3/CoreTSF	
PCIA2		ADV_ARC.1
PCIA3	FPT_PHP.3/CoreTSF	
PCIA4		ADV_ARC.1
PCIA5	FPT_EMSEC.1/PIN_ENTRY	
PCIA6	FPT_PHP.3/CoreTSF, FPT_EMSEC.1/CoreTSF	
EPC-CHIP-ONLYA6	FPT_PHP.3/CHIP-ONLY FPT_EMSEC.1/CHIP-ONLY	
PCIA7	FDP_ACC.1/PEDPromptControl, FDP_ACF.1/PEDPromptControl	
PCI NewA8	Outside the CC evaluation (objective for the environment)	
EPCA8.a		
PCIA9	FPT_PHP.3/MSR	
PCIA10		ADV_ARC.1
PCIA11	FPT_EMSEC.1/PIN_ENTRY	
PCIB1	FPT_TST.1/ PEDMiddleTSF, FPT_FLS.1/ PEDMiddleTSF, FPT_TST.1/CoreTSF, FPT_FLS.1/CoreTSF	
PCIB2	FDP_ITC.1/PEDMiddleTSFLoader, FPT_FLS.1/ PEDMiddleTSF, FPT_FLS.1/CoreTSF, FDP_ITC.1/CoreTSFLoader	
PCIB3		ALC_CMS.2
EPC PlusB3.a	Covered by the CC evaluation	

CAS-requirement	SFR	SAR
PCIB4	FDP_ITC.1/CoreTSFLoader, FDP_ITC.1/PEDMiddleTSFLoader	
PCIB4.1	FDP_ACC.1/ ApplicationLoader, FDP_ITC.1/ ApplicationLoader	
PCIB5	FPT_EMSEC.1/PIN_ENTRY	
PCIB6	FDP_IFF.1/ENC_PIN, FDP_RIP.1/ENC_PIN, FDP_RIP.1/PLAIN_PIN, FDP_RIP.1/ICCardReader	
PCIB7	FIA_UAU.2/PIN_ENTRY	
PCIB8	FTA_SSL.3/PIN_ENTRY	
PCIB9	FCS_RND.1	
PCIB10	FDP_IFF.1/ENC_PIN, FCS_COP.1	
EPC PlusB10.a	FDP_IFF.1/ENC_PIN, FCS_COP.1	
PCIB11	FDP_ITC.2, FTP_ITC.1/Crypto, FPT_TDC.1	
PCIB12	FCS_COP.1	
PCIB13	FDP_IFF.1/ENC_PIN	
PCIB14	FDP_IFF.1/ENC_PIN, FDP_IFF.1/PLAIN_PIN, FDP_IFF.1/ICCardReader	
PCIB15	FDP_ITC.1/PIN_ENTRY	
PCIB16	FDP_ACC.1/PEDPromptControl, FDP_ACF.1/PEDPromptControl	ADV_ARC.1
EPC-CHIP-ONLYB16	FDP_ACC.1/PEDPromptControl, FDP_ACF.1/PEDPromptControl	ADV_ARC.1
PCIB17	FDP_ACF.1/POI_DATA	
PCIB18		ADV_ARC.1
PCIB19		AGD_OPE.1
PCIB20		ADV_ARC.1 AGD_OPE.1
PCIC1	FTP_TRP.1/ENC_PIN	
PCID1	FPT_PHP.3/ICCardReader (not cover-	ADV_ARC.1

CAS-requirement	SFR	SAR
	ing insertion slot requirement)	
PCID2		ADV, ARC.1 AGD_OPE.1
PCID3		ADV_ARC.1
PCID4.1	FDP_IFF.1/ENC_PIN, FCS_COP.1	
PCID4.2	FDP_IFF.1/PLAIN_PIN, FDP_IFF.1/ICCardReader, FCS_COP.1	
PCID4.3	FDP_IFF.1/ENC_PIN	
PCID4.4	FDP_IFF.1/PLAIN_PIN, FDP_IFF.1/ICCardReader, FCS_COP.1	
In the following requirements 'device' reflects the PED and the POI security-related com-po-nents. In terms of Common Criteria security-related means SFR-enforcing.		
EPC PlusL0		ALC_DVS.2
PCIL1		Re-evaluation issues are out of scope. The PP stands by CC maintenance process.
EPC PLUS L1.a		
PCIL2		ALC_DVS.2
PCIL3		ALC_DVS.2
PCIL4a		ALC_DVS.2
PCIL5		ALC_DVS.2
PCIL6		ALC_DVS.2
PCIL7		ALC_DVS.2
PCIL8		ALC_DVS.2
PCIM1		ALC_DVS.2
PCIM2		ALC_DVS.2
PCIM3		ALC_DVS.2
PCIM4		ALC_DVS.2
PCIM5		ALC_DVS.2
PCIM6		ALC_DVS.2
PCIM7		ALC_CMC.2

CAS-requirement	SFR	SAR
PCIM8		AGD_OPE.1
EPCN1.1	FDP_UIT.1/POI_DAT, FDP_UCT.1/POI_DATA, FTP_ITC.1/POI_DATA	
EPCN1.2	FDP_ITT.1/POI_DATA	
EPCN1.3	FDP_ITT.1/POI_DATA , FDP_UIT.1/POI_DAT	
EPCN2.1	FDP_RIP.1/POI_DATA, FDP_ACF.1/POI_DATA	ADV_ARC.1
EPCN2.2	FDP_RIP.1/POI_DATA, FDP_ACF.1/POI_DATA	ADV_ARC.1
EPCN2.3	FDP_RIP.1/POI_DATA, FDP_ACF.1/POI_DATA	ADV_ARC.1
EPCN3.1	FDP_ITC.1/MiddleTSFLoader FDP_ITC.1/ApplicationLoader	
EPCN3.2	FDP_ITC.1/MiddleTSFLoader FDP_ITC.1/ApplicationLoader	
EPCN4	FDP_ITT.1/POI_DATA, FDP_UCT.1/POI_DATA, FTP_ITC.1/POI_DATA	
EPCN5	Covered by the CC evaluation	
EPCN6	FDP_ITC.2, FTP_ITC.1/Crypto, FPT_TDC.1	
EPCN7	FPT_FLS.1/MiddleTSF	

14 Annex – Relationship between AVA_POI and AVA_VAN.2 families

671 The relationship between AVA_VAN.2 and the requirements of the extended AVA_POI family is essentially one of refinement, as demonstrated in the discussion below. However, the suitability of AVA_POI.1 as a substitution in EAL POI for AVA_VAN.2 in EAL2 also relies on the interpretation of CC "Basic" attack potential (which is required in AVA_VAN.2) as within the limits of "POI-Basic", defined in [POI AttackPot].

672 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 can be confirmed by consulting [POI AttackPot]). 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.

673 Let us show that AVA_POI.1 is a refinement of AVA_VAN.2 for the POI components selected in the instantiation of AVA_POI.1.1D:

- 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, and allowing any of the POI attack potential thresholds to be assigned. In addition, it allows (optionally) certain more specific requirements to be stated on parts of the attack potential calculation, to enable an author to set minimum thresholds for exploitation aspects, for example. The minimum attack potential that can be specified in this element is POI-Basic which replaces standard CC Basic attack potential. By assumption Basic attack potential is weaker than or equal to POI-Basic attack potential level, hence the new requirement is stronger than the original one.

674 In EAL POI, each POI component in the scope of the evaluation is addressed by at least one AVA_POI.1 iteraton: POI components belong to one of the TSF parts CoreTSFKeys, CoreTSF, PED MiddleTSF, MiddleTSF or MSR and each of these parts are addressed by at least one iteration of AVA_POI.1. Hence, the set of AVA_POI iterations included in EAL POI constitutes a refinement of AVA_VAN.2 applied to the whole POI.