Common Security Evaluation &
Certification Consortium
of GBIC and UKF

Common.SECC

Security Evaluation & Certification Consortium

NO-CVM
Point of Interaction
Protection Profile

Date: April 1 2019
Version: 1.0

History table

Version	Comments	Date
0.1	First draft	April 5th, 2017
0.2	Changes after discussion in JTEMS	August 7th, 2017
0.3	First draft for release	December 21st, 2017
0.4	Minor corrections due to further comments from the JTEMS working group	May 9, 2018
1.0	Approved by Common.SECC	April 1, 2019

Table of contents

Table of figures

Table of tables

1 Protection Profile Introduction

1 This document defines the base Protection Profiles dedicated to payment terminals which have only a contactless reader without CVM.

2 The POI-CHIP-ONLY-NO-CVM is applicable to Point of Interaction (POI) devices having a contactless reader without performing CVM related tasks. The second base PP is the POI-COMPREHENSIVE-NO-CVM base PP and is applicable to POI devices having not only a contactless reader but also other readers like contact based and magnetic stripe readers without performing CVM related tasks outside the Chip-Only scheme and can be used in conjunction with the SRED PP Module of this PP which is derived from the SRED PP Module from [POI PP 4.0] in the sense of [PP mod].

1.1 Protection Profile Identification

1.1.1 Identification of POI-CHIP-ONLY-NO-CVM base PP

Title	Point of Interaction Protection Profile – POI-CHIP-ONLY-NO-CVM base PP
Authors	JTEMS Working Group
Version	1.0
Publication Date	April 1, 2019
CC Version	3.1 Revision 5

1.1.2 Identification of POI-COMPREHENSIVE-NO-CVM base PP

Title	Point of Interaction Protection Profile – COMPREHENSIVE-NO-CVM base PP
Authors	JTEMS Working Group
Version	1.0
Publication Date	April 1, 2019
CC Version	3.1 Revision 5

1.1.3 Identification of SRED PP Module (SRED PP-Module), see [POI PP 4.0]

Title	Point of Interaction Protection Profile – SRED PP Module
Identification	ANSSI-CC-PP-POI-SRED-PP-Module
Version	**4.0, Derived from [POI PP 4.0]**
Publication Date	6th March, 2015
Sponsor	ANSSI
CC Version	3.1 Revision 4

Note that the "SRED PP module" cannot be used with the "POI-CHIP-ONLY-NO-CVM" base PP.

Therefore, there are two base PPs and an ST author can claim one of these possible variants.

- POI-CHIP-ONLY-NO-CVM base PP
- POI-COMPREHENSIVE-NO-CVM base PP
- POI-COMPREHENSIVE-NO-CVM base PP + SRED PP Module

1.2 Protection Profile Presentation

3 The products in the scope of this Protection Profile are payment terminals (POI) that manage transaction data and provide external communications capabilities without any Cardholder Verification Method (CVM). Other functionalities than payment, which might be processed by the same device, e.g. fleet card processing or payment with CVM, are out of scope of this PP. These other security functionalities, e.g. secure PIN entry, authentic display functionality, etc is not part of the TOE within this PP and may have to undergo other security assessment based on other PPs or other schemes.

4 The aim of this Protection Profile is to support the business needs of payment schemes which support POI devices without CVM for a predefined CVM limit. Transaction capabilities exceeding the predefined CVM limit which makes use of a CVM will not be in scope of this PP.

5 The usage of this Protection Profile is intended to achieve CC evaluations/certifications, which can be used multiple times for approvals of those payment schemes requiring the conformance with this PP.

6 Ideally, only the security features of the TOE to be used by payment applications 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 TOE. With this approach, the state machine controlling the payment transaction flow is not part of the TOE.

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

8 For the protection of specific assets a modular approach has been chosen. Thus, if the selected base PP given in this document can be extended by the ‘Secure-Read-and-Exchange-Data (SRED) PP-module defined in section 10 which is related to account data protection then the (SRED) PP module has to be chosen by the ST author.

9 This Protection Profile defines two base PPs, each of them with a particular TOE:

- POI-COMPREHENSIVE-NO-CVM base PP: This TOE provides protection for contactless based NO-CVM transactions, payment transaction data management and external communication facilities. This configuration is prepared to be extended by the SRED PP-Module according to [PP Mod] in section 10. If the TOE includes other readers than a contactless only reader or the TOE supports other than NO-CVM transactions then this configuration has to be chosen by the ST author including the (SRED) PP module.
- POI-CHIP-ONLY-NO-CVM base PP: This TOE provides protection for contactless only based NO-CVM transactions, payment transaction data management and external communication facilities. The aim of this Protection Profile variant is the support of the business needs of the payment schemes, which support the chip only environment. Only transactions not exceeding the CVM limit are possible in terminals claiming conformance to this base PP. 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-NO-CVM base PP as a possibility.

10 This Protection Profile defines a specific evaluation package, called EAL POI NO CVM, which is built upon EAL2 and includes some of the most relevant elements from the EAL*4* assurance level, with the aim of ensuring that the POI can be evaluated at the appropriate level. The EAL POI NO CVM balances evaluation effort according to the architecture of the POI, and points out the use of suitably informed penetration testing that reflects the variety of assets.

11 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 with additional functionalities if necessary.

1.3 References

[CC1] Common Criteria Part 1, Version 3.1, Revision 5, CCMB-2017-04-001

[CC2] Common Criteria Part 1, Version 3.1, Revision 5, CCMB-2017-04-002

[CC3] Common Criteria Part 1, Version 3.1, Revision 5, CCMB-2017-04-003

[CEM] Common Criteria Evaluation Methodology, Version 3.1, Revision 5, CCMB-2017-04-004

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

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

[POI AttackPot] Joint Interpretation Library / Application of Attack Potential to POIs, Version 1.92, Date: 11th August 2014. *Note: POI evaluations shall rely on the current version of this document at the moment of the evaluation.*

[POI_PPV4] Point of Interaction Protection Profile Date: March 6, 2015, Version: 4.0.

[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 PP Framework

12 Chapter 1.2 already gives an overview of the PP Framework. However, this chapter gives additional information to understand how a NO-CVM POI evaluation works.

13 The ST author first has to claim the fundamental base PP. There are two fundamental base PPs, the POI-CHIP-ONLY-NO-CVM base PP and the POI-COMPREHENSIVE-NO-CVM base PP. There is no additional description of each base PP in separated chapters of this PP, but each chapter includes information for each base PP.

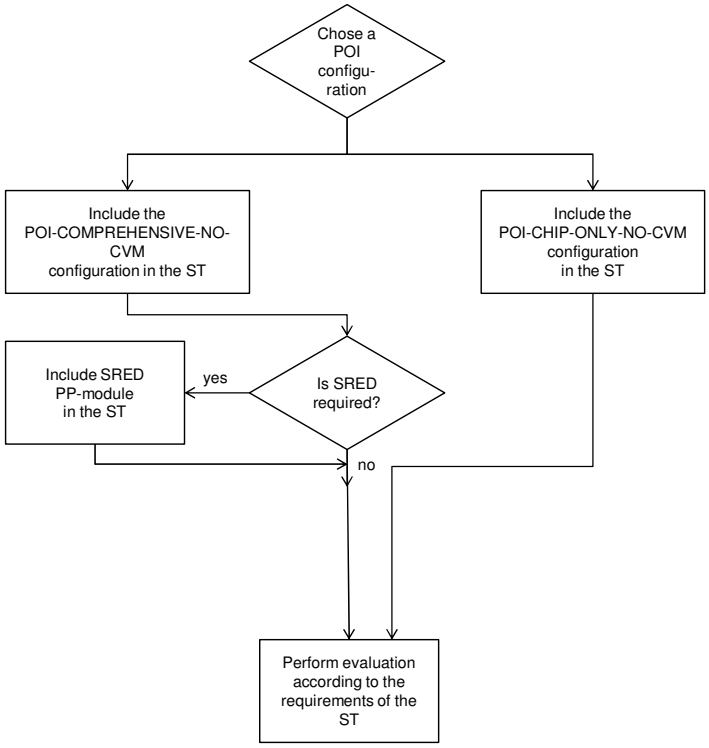


Figure 1: POI Framework – Process Flow

SRED PP-Module

14 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.

15 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, the POI base PP POI-COMPREHENSIVE-NO-CVM has to be selected before (POI-CHIP-ONLY-NO-CVM 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.

16 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 TOE Overview

3.1 TOE Type

17 The TOE is a product of type Point of Interaction (POI) without CVM capability.

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

- POI-COMPREHENSIVE-NO-CVM base PP: This TOE provides protection for contactless based NO-CVM transactions, payment transaction data management and external communication facilities. This configuration is prepared to be extended by the SRED PP-Module according to [PP Mod] in section 10. If the TOE includes other readers than a contactless only reader then this configuration has to be chosen by the ST author.
- POI-CHIP-ONLY-NO-CVM base PP: This TOE provides protection for contactless only based NO-CVM transactions, payment transaction data management and external communication facilities. The aim of this Protection Profile variant is the support of the business needs of the payment schemes, which support the chip only environment. Only transactions not exceeding the CVM limit are possible in devices claiming conformance to this base PP. 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-NO-CVM base PP as a possibility.

3.2 TOE Security Features

19 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.

3.2.1 Generic POI

3.2.1.1 Generic Payment Transaction Process

20 The following figure shows the POI payment transaction process based on contactless communication without CVM.

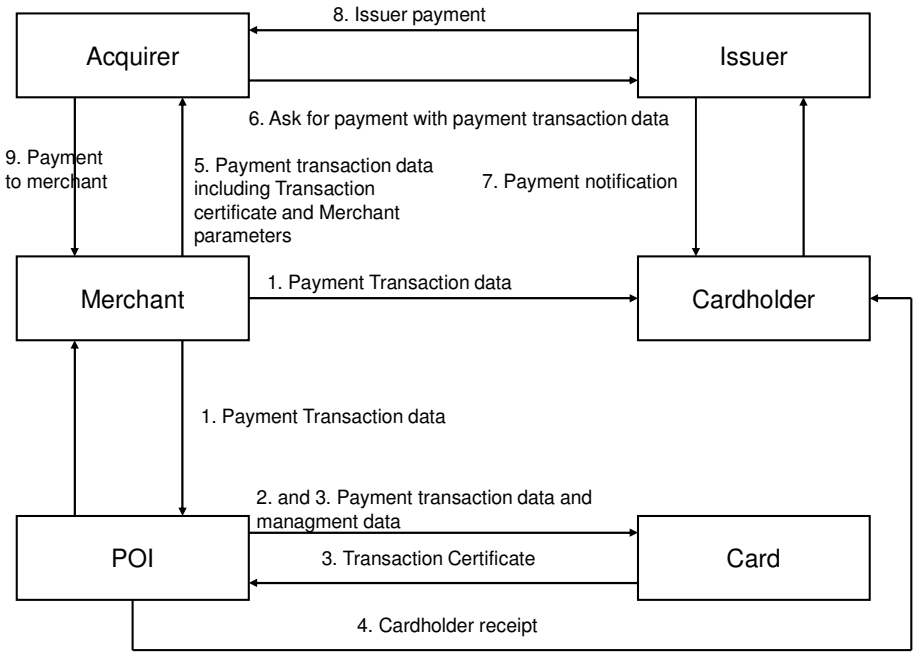


Figure 2: Generic POI Payment Transaction Process

1. The merchant submits payment transaction data (e.g. amount) 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. Upon successful completion of transaction processing, including card risk management on behalf of the Issuer (online), the card issues a transaction certificate.

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

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

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

7. 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).

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

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

3.2.1.2 Generic Terminal Management Process

21 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 Components

22 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/O, 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. **If the POI is capable to accept Magnetic Stripe and contact based then these readers has to be assessed accordingly.**

- **Security Modules** (SM): devices for management of cryptographic keys and cryptographic functions (e.g. a Hardware Security Module (HSM), a security

processor and a Security Application Module (SAM) as an external Security Application Module (SAM) for a purse application (PSAM)).

- **User I/Os:** that may include printer, and audible signals. Different User I/O interfaces may exist for the Attendant and for the Cardholder. Security which has to be provided by a display is not covered by this PP.

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.

- **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.

3.2.2 Security features

23 The security of the TOE payment transactions 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.

24 The goal of the TOE is to enforce, through its security features, part or all of the following properties on the assets, depending on the TOE configuration. These properties on the assets provide an overview of the objectives for the TOE which are precisely described in section 5.7:

- Authenticity and integrity of POI management and transaction data.
- Confidentiality, authenticity and integrity of POI data protection keys.

25 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]. **In this PP only POI-Basic and POI-Moderate are relevant.** 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 3 and Figure 4).

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

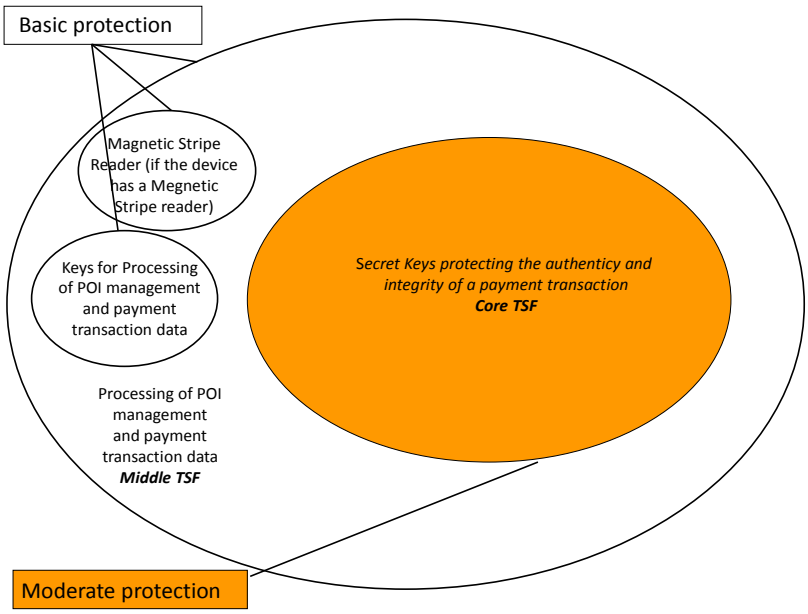


Figure 3: TSF structure in POI-COMPREHENSIVE-NO-CVM configuration

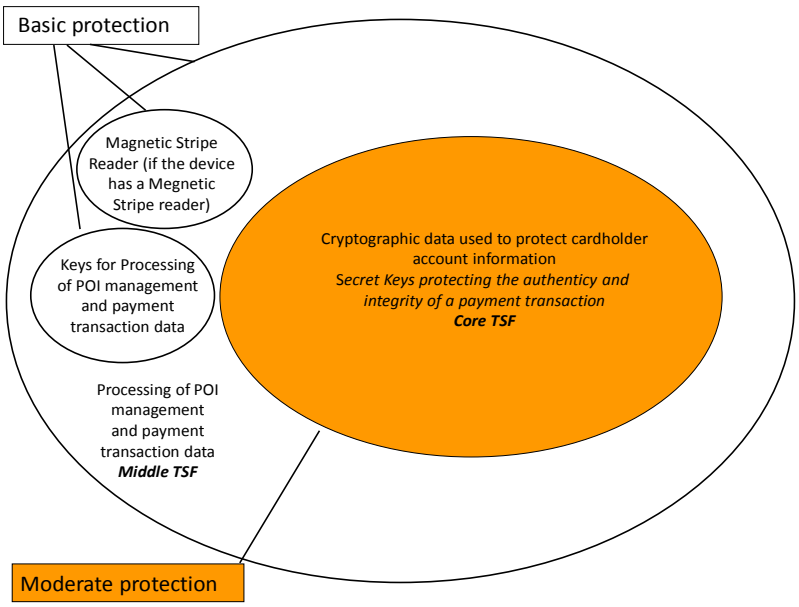


Figure 4: TSF structure in POI-COMPREHENSIVE-NO-CVM configuration with adopted SRED PP-Module

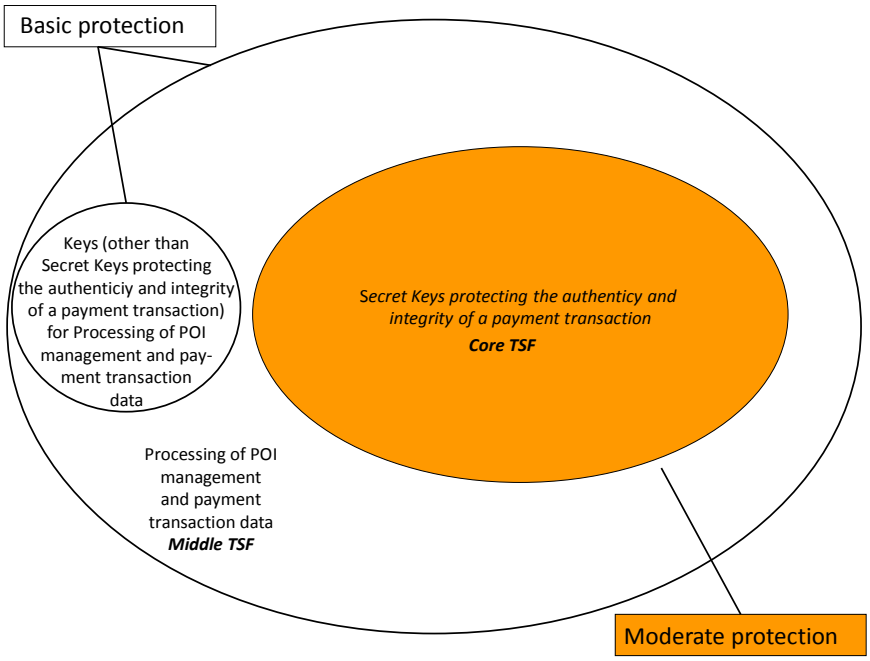


Figure 5: TSF structure in POI-CHIP-ONLY-NO-CVM configuration

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

- CoreTSF contains security features protected at POI-Moderate 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 10 is adopted in a 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 4. For POI-CHIP-ONLY-NO-CVM 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 in the POI-COMPREHENSIVE-NO-CVM configuration **and the MSR TSF has to be adopted appropriately from [POI_PPV4] by the ST Author. Same holds for TOEs with contact based IC readers. Then the ICCR TSF package from [POI_PPV4] has to be appropriately included by the ST Author.** Here, "appropriately" means, that the ST Author includes **all** SFRs from the corresponding package which are needed for the NO-CVM TOE Type, i.e. leaving out SFRs referring to PIN security, which obviously cannot always be fulfilled by a NO-CVM TOE.

27 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.

28 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 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.

29 The physical boundary of each TSF part is defined by the 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.

30 The security features provide a high level view of the security of the terminals. The precise view is given by the SFRs. The complete list of security features in this Protection Profile, consists of:

1. 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.
2. Authenticity and integrity protection of administration (e.g. downloading, update) of POI management and transaction processing software and keys, including appropriate cryptographic means.
3. Tamper-detection/tamper-responsiveness (POI SM, Card Reader SM, Magnetic Stripe Reader).
4. Secure downloading of payment application.
5. 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

31 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	CoreTSF Keys	MiddleTSF	MSR
POI-COMPREHENSIVE-NO-CVM	3 If SRED is adopted 5.	keys for 3	1, 2, 4	3
POI-CHIP-ONLY-NO-	3, 4 (keys and secret Payment		1, 2, 3	

CVM	Transaction Data keys)			

Table 1: TSF decomposition by base PP

32 The components of a POI described in section 3.2.1.3 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 the base PP in terms of components associated to TSF parts.

PP configuration	**CoreTSF**	**MiddleTSF**	**MSR**
POI-COMPREHENSIVE-NO-CVM	SM If SRED is adopted Account Data SM	Other POI components	Magnetic Stripe Reader
POI-CHIP-ONLY-NO-CVM	SM	Other POI components	

Table 2: Physical boundaries of TSF parts by base PP

33 *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 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

34 The TOE can have a display, keypad and other secure chip based card readers than the contactless reader which are non-TOE Hardware and Firmware parts. In this case the POI-COMPREHENSIVE-NO-CVM configuration has to be chosen by the ST author.

3.4 TOE Usage

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

- POI-COMPREHENSIVE-NO-CVM configuration: The TOE is intended to be used in any SEPA payment environment. The TOE may be capable of accepting contact based or contactless chip transaction or supports magnetic stripe transactions without any CVM.

- POI-CHIP-ONLY-NO-CVM: The TOE is intended to be used by chip-only payment schemes like girocard. The TOE supports contactless NO-CVM transactions only.

3.5 TOE Life Cycle

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

37 Developer Phase:

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

38 Operational Phase (User Phase):

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

39 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.

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

41 *Application Note: The ST author shall update this life cycle according to the product specificities, e.g. application loading during Initial Software Loading and/or during use, configuration of applications with TOE specific parameters, etc.*

3.5.1 Developer phase

3.5.1.1 Development and Manufacturing

42 POI development and manufacturing consists of producing

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

43 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

44 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.

45 Initial Cryptographic Keys are loaded into the POI. Additional cryptographic keys can 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.

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

47 *Application note: 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*[1].

3.5.2 User phase

48 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.

49 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.

3.5.2.1 Installation

50 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 POI,
- cabling and connections to external peripherals which may be local, e.g. an Electronic Cash Register, or remote via an external access line,

[1] The initial key is the trust anchor, on which all following cryptographically secure key loading is based and cannot be loaded in the field. The initial key 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 secret, 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 loaded in a potentially insecure environment.

- 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

51 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.

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

53 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.

54 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).

55 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

56 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.

57 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

58 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

59 This Protection Profile is conformant to the Common Criteria version 3.1 revision 5:

60 - CC Part 2 [CC2] extended

61 - CC Part 3 [CC3] extended

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

63 The CC Part 3 is extended with the security assurance components AVA_POI.1 POI vulnerability analysis (cf. section 7.3). By instantiation of AVA_POI.1 this assurance component is applied to TSF parts of different attack potential resistance (cf. 8.2.3). The annex in chapter 11 explains the relationship between AVA_POI and AVA_VAN.2.

4.2 Conformance claim to a package

64 This Protection Profile is conformant to EAL POI NO CVM which is defined in section 8.2.

4.3 Conformance claim of the PP

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

4.4 Conformance claim to the PP

66 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

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

68 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-NO-CVM configuration.

69 **Note: If the ST Author has choosen to add the MSR TSF and the ICCR TSF into the TSF structure of the NO-CVM TOE then it has to be adopted appropriately into the table below.**

Asset	Sensitivity
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
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
POI_SW	A, I
PAYMENT_APP	A, I

Table 3: Assets sensitivity

70 **MAN_DAT (POI management data)**

71 At least POI Management data are the POI Unique Identifier, the Merchant Identifier and the Acquirer risk management data2. The POI_PK is a special kind of MAN_DAT.

72 Sensitivity: Authenticity, Integrity.

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

73 *Application note: MAN_DAT shall be protected inside the TOE and through external communications. PAY_DAT (Payment transaction data)*

74 **PAY_DAT (Data related to the payment transaction.)**

75 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 cryptogram data, the Authorization Reply as well as card script processing and card management data.

76 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.

77 Sensitivity: Authenticity and Integrity.

78 *Application note: The TOE ensures protection of PAY_DAT inside the TOE. Protection of PAY_DAT that are sent outside the TOE 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.*

79 **SRED Account Data**

80 **If the SRED PP-Module is chosen** specific data is addressed to be protected. SRED Account Data can consist of, TOE_CLEAR_PAN, E2E_CIPHER_PAN, TOE_CIPHER_PAN, SURROGATE_PAN and SURROGATE_PAN_SALT see 10, section 10.1.1 Assets.

81 Sensitivity: Confidentiality, Authenticity and Integrity.

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

83 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).

84 Sensitivity: Authenticity and Integrity.

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

86 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).

87 Sensitivity: Confidentiality, Authenticity and Integrity.

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

89 POI_PayDatSK is defined as a subset of POI_SK in order to allow higher protection in case POI-CHIP-ONLY-NO-CVM configuration is claimed. POI_PayDatSK are used to protect the integrity and authenticity of PAY_DAT.

90 Sensitivity: Confidentiality.

91 **CORE_SW**

92 Software (code and data) of the CoreTSF.

93 Sensitivity: Authenticity and Integrity.

94 **CORE_HW**

95 Hardware of the CoreTSF.

96 Sensitivity: Authenticity and Integrity.

97 **POI_SW (POI software)**

98 Software (code and data) of the MiddleTSF.

99 Sensitivity: Authenticity and Integrity.

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

101 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 10.1.1.

102 Sensitivity: Confidentiality, Authenticity and Integrity.

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

104 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 10.1.1**.**

105 **Magnetic Stripe Track Data**

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

107 **PAYMENT_APP**

108 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.)

109 Sensitivity: Integrity and Authenticity

5.1.1 Assets in each base PP

110 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.

111 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. **The ST Author has to derive the MSR TSF package from [POI_PPV4] if the TOE is capable to accept MSR based transactions. Same holds for the ICCR TSF for contact based card readers.**

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

Asset	POI-COMPREHENSIVE-NO-CVM		POI-CHIP-ONLY-NO-CVM	
	CoreTSF	MiddleTSF	CoreTSF	MiddleTSF
POI_SW		x		x
CORE_SW	x		x	
CORE_HW	x		x	
MAN_DAT		x		x
PAY_DAT		x		x
SRED Account Data		x		
POI_PK		x		x
POI_SK		x		x
TOE_PAN_SK	x			
E2E_PAN_SK	x			
PAYMENT_APP		x		x
POI_PayDatSK			x	
Magnetic Stripe Track Data	MSR TSF, see [POI_PPV4]			

Table 4: Assets by base PP

5.2 Users

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

114 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

115 Cardholder

116 The Cardholder interacts with the POI via man-machine interfaces. He places his payment card on the contactless card reader or inserts/swipes his payment card.

117 Attendant

118 The payment application in the POI or in a connected TOE 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.

119 Merchant

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

121 Terminal Administrator

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

5.2.2 External Entities

123 Acquirer System

124 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.

125 Terminal Management System

126 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.

127 IC Card "Cardholder's IC Card"

128 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.

Local Device

130 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.

Payment Application

132 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

134 The Risk Manager is an entity interacting with the IC/NFC Card, the Terminal Management System and the Acquirer System during a payment transaction.

5.2.3 Users in each base PP

135 Table 5 defines the users of each base PP.

User	POI-CHIP-ONLY-NO-CVM	POI-COMPREHENSIVE-NO-CVM
Cardholder	X	X
Attendant	X	X
Merchant	X	X
Terminal Administrator	X	X
Acquirer System	X	X
Terminal Management System	X	X
Card	X (CTLS only)	X
Magnetic Stripe Card		X (If MSR TSF is added)
Local Device	X	X
Payment Application	X	X
Risk Manager	X	X

Table 5: Users by the PP

5.3 Subjects

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

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

Payment Application Logic (PAL)

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.

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.

POI SM

Manages the access and performs all security related cryptographic operations in the POI.

Terminal Management

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.

Card Reader and Card Reader SM (Security Module)

The Card Reader which manages the communications between the Card and the POI.

Core Loader

The loader downloading CORE_SW into the POI.

Middle Loader

The loader downloading POI_SW into the POI.

Magnetic Stripe Reader

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

Payment Application Loader

Loader for downloading and updating payment applications.

5.3.1 Subjects in each base PP

Table 6 defines the subjects of the base PP.

Subject	POI-CHIP-ONLY-NO-CVM	POI-COMPREHENSIVE-NO-CVM
Payment Application Logic	X	X
Terminal Management	X	X
Card Reader	X (CTLS only)	X
Magnetic Stripe Reader		X (If MSR TSF is added)
Core Loader	X	X
Middle Loader	X	X
Payment Application Loader	X	X

Table 6: Subjects by base PP

5.4 Threats

156 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.)

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

158 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.

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

160 *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.*

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

a) Fraudsters use good 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.

b) Fraudsters (including a fraudulent Cardholder) use good 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.

162 **Note** that if the SRED PP-Module is adopted then an additional refinement to this threat applies, as specified in 10.

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

T.FundsAmount (Funds transfer other than correct amount)

a) Fraudulent Merchants manipulate the TOE in order to make the Cardholder issue payment instructions for more than he thinks modifying the amount in payment transaction data PAY_DAT or to make the Cardholder issue several payment instructions instead of one generating several sets of payment transaction data PAY_DAT.
b) Fraudsters use good cards and manipulate TOE to generate transactions based on manipulated payment transaction data PAY_DAT that are rejected by the Acquirer when collected.
c) A fraudulent Cardholder issues valid payment instructions generating valid payment transaction data PAY_DAT but later destroys payment transaction data PAY_DAT before they are collected.
d) Fraudsters modify the interface between TOE and Acquirer; modify payment instructions by modification of payment transaction data PAY_DAT into refunds.

Related assets: POI_SW, PAY_DAT, POI_PK, POI_SK.

T.BadDebt (Account overdraft, bad debt)

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.

Related assets: POI_SW, MAN_DAT.

T.SecureCommunicationLines

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. An attacker may misuse the contactless communication between the NFC chip and NFC capable cards.

Related assets: PAY_DAT, POI_SW, POI_PK, POI_SK.

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).

T.Magstripe

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.

Related assets: Magnetic Stripe Track Data.

T.IllegalCodeInstall

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 man-

agement device or falsely authenticating himself as a trusted authority and thus being able to install untrusted code.

178 Related assets: PAYMENT_APP.

5.4.1 Threats in each base PP

179 Table 7 defines the threats to each base PP.

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

Threat	POI-CHIP-ONLY-NO-CVM	POI-COMPREHENSIVE NO-CVM
T.MerchUsurp	X	X
T.Transaction	X	X
T.FundsAmount	X	X
T.BadDebt	X	X
T.SecureCommunicationLines	X	X
T.Magstripe		X
T.IllegalCodeInstall	X	X

Table 7: Threats by base PP

5.5 Organisational Security Policies

181 OSP.WellFormedPayApp (Well-formed Payment Applications)

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

183 OSP.ApplicationSeparation

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

185 OSP.POISurvey

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

187 OSP.MerchantSurvey

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

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

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

191 OSP.KeyManagement

192 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

193 All the OSP listed above apply to each of the base PPs

5.6 Assumptions

194 **A.UserEducation**

195 It is assumed that Cardholders are informed by their issuing banks about a proper use and about their responsibilities when using the TOE.

196 **A.SecureDevices**

197 It is assumed that the payment application providers have chosen appropriate security measures to protect devices interacting with the TOE e.g. the cards.

5.6.1 Assumptions in each base PP

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

5.7 Security Objectives

199 O.CoreSWHW

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

201 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.

202 Upon failure of any authenticity and integrity check or upon incorrect execution, the TOE shall make any related secret data.

203 O.CardReader

204 The TOE shall ensure that the TOE resists attempts to penetrate the POI to make any additions, substitutions, or modifications to the Card Reader hardware or software.

205 O.PaymentTransaction

206 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.

207 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 signed 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.

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

209 In the POI-CHIP-ONLY-NO-CVM configuration POI_PayDatSK have in addition to be protected by tamper-responsive and tamper-detection means.

210 *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.*

211 **O.POI_SW(Authentic and integer usage of POI software and related hardware)**

212 The TOE shall ensure the authenticity, the integrity and the correct execution of POI_SW processing POI management and payment transaction data.

213 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.

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

215 **O.PaymentApplicationDownload**

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

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

218 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.

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

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

221 If the MSR TSF has been chosen the TOE shall ensure that the TOE resists attempts to penetrate the POI to make any additions, substitutions, or modifications to the Magnetic Stripe Read head and associated hardware or software, in order to determine or modify Magnetic Stripe data.

5.7.1 Security objectives for the TOE in each base PP

222 The table below defines the objectives applicable to each base PP and shows, which TSF parts contribute to each objective.

Objective for the TOE	POI-COMPREHENSIVE-NO-CVM				POI-CHIP-ONLY-NO-CVM			
	CoreTSF	CoreTSF Keys	IC Card Reader	MiddleTSF	CoreTSF	CoreTSF Keys	MiddleTSF	IC Card Reader
O.CoreSWHW	x	x			x			
O.ICCardReader			x					x
O.PaymentTransaction				x			x	
O.POI_SW				x			x	
O.PaymentApplicationDownload				x			x	
O.POIApplicationSeparation				x			x	
O.PromptControl								
O.MSR		MSR TSF (see [POI PP V4])						

Table 8: Objectives for the TOE by base PP

5.8 Security Objectives for the Operational Environment

223 OE.POISurvey

224 Procedural measures like inspections and guidance will prevent manipulations of the TOE enclosure. Procedural measures like inspections and guidance for manipulations of the card interface will prevent attacks based on electronic circuits mounted on the 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.

225 **OE.MerchantSurvey**

226 In case of 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.

227 **OE.SecureDevices**

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

229 **OE.KeyManagement**

230 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.

231 **OE.WellFormedPayApp**

232 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).

233 **OE.LocalDevices**

234 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.

235 *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.FundsAmount and T.BadDebt shall be partially countered in the environment of the TOE. Nevertheless, in those POI architectures where the POI mechanisms are used to protect the connection between Local Devices and other POI components, e.g. the TOE based hardware security mechanisms or cryptographic means, the ST author shall introduce an additional objective for the TOE, with the appropriate associated SFRs.*

5.8.1 Security objectives for the TOE environment by base PP

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

6 Rationale between SPD and security objectives

6.1 Threats

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

238 T.MerchUsurp (Merchant Identity Usurpation)

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

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

241 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).

242 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.

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

244 T.Transaction (Transaction with usurped Cardholder identity)

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

246 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).

247 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.

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

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

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

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

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

T.FundsAmount (Funds transfer other than correct amount)

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

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).

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.

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

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

T.BadDebt (Account overdraft, bad debt)

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.

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).

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.

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

264 T.SecureCommunicationLines

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

266 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).

267 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.

268 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.

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

6.2 OSP

270 OSP.WellFormedPayApp

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

272 OSP.POISurvey

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

274 OSP.MerchantSurvey

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

276 OSP.KeyManagement

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

278 OSP.ApplicationSeparation

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

6.3 Assumptions

280 A.UserEducation

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

282 A.SecureDevices

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

6.4 Rationale applicable to POI-COMPREHENSIVE-NO-CVM configuration

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

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

- T.MerchUsurp (Merchant Identity Usurpation)
- T.PromptControl
- T.Transaction (Transaction with usurped Cardholder identity)

- T.FundsAmount (Funds transfer other than correct amount)
- T.BadDebt (Account overdraft, bad debt)
- T. SecureCommunicationLines
- T.IllegalCodeInstall
- T.Magstripe

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

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

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

- A.UserEducation
- A.SecureDevices

	T.MerchUsurp	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
O.CoreSWHW		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.CardReader		X													
OE.WellFormedPayApp	X	X	X		X	X							X		
OE.POISurvey	X	X	X		X	X				X					
OE.MerchantSurvey	X	X	X								X				
OE.UserEducation														X	
OE.SecureDevices	X	X	X		X	X									X
OE.KeyManagement	X	X	X		X	X						X			
OE.LocalDevices	X	X	X		X	X									

Table 9: SPD coverage by objectives in POI-COMPREHENSIVE-NO-CVM configuration

6.5 Rationale applicable to POI-CHIP-ONLY-NO-CVM configuration

288 This section provides the rationales applicable to the POI-CHIP-ONLY-NO-CVM configuration.

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

- T.MerchUsurp (Merchant Identity Usurpation)
- T.FundsAmount (Funds transfer other than correct amount)
- T.BadDebt (Account overdraft, bad debt)

- T. SecureCommunicationLines
- T.IllegalCodeInstall

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

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

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

- A.UserEducation
- A.SecureDevices

	T.MerchUsurp	T.Transaction	T.FundsAmount	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.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															
O.CardReader															
OE.WellFormedPayApp	X	X	X	X	X							X			
OE.POISurvey	X	X	X	X	X				X						
OE.MerchantSurvey	X	X	X							X					
OE.UserEducation													X		
OE.SecureDevices	X	X	X	X	X									X	
OE.KeyManagement	X	X	X	X	X						X				
OE.LocalDevices	X	X	X	X	X										

Table 10: SPD coverage by objectives in POI-CHIP-ONLY-NO-CVM

7 Extended Requirements

292 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. These are extracted from [POI_PPV4] and modified to suit the need for this NO-CVM-PP. Assignments, selections, refinements or iterations are presented in *italics* and have to be filled by the ST Author. Assignments, selections, refinements or iterations already filled by the PP are **bold**.

7.1 Definition of the Family FCS_RND

293 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.

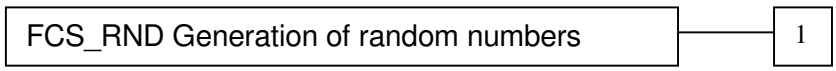
294 The family "Generation of random numbers (FCS_RND)" is specified as follows.

295 FCS_RND Generation of random numbers

296 Family behaviour

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

298 Component levelling:



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

300 Management: FCS_RND.1

301 There are no management activities foreseen.

302 Audit: FCS_RND.1

303 There are no actions defined to be auditable.

FCS_RND.1 Generation of random numbers

304 Hierarchical to: No other components.

305 Dependencies: No dependencies.

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

7.2 Definition of the Family FPT_EMSEC

307 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.

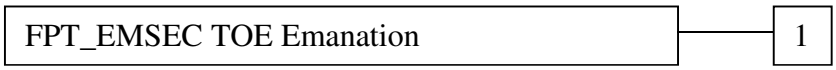
308 The family "TOE Emanation (FPT_EMSEC)" is specified as follows.

309 FPT_EMSEC TOE Emanation

310 Family behaviour:

311 This family defines requirements to mitigate intelligible emanations.

312 Component levelling:



313 FPT_EMSEC.1 TOE emanation

314 Management: FPT_EMSEC.1

315 There are no management activities foreseen.

316 Audit: FPT_EMSEC.1

317 There are no actions defined to be auditable.

FPT_EMSEC.1 TOE emanation

318 Hierarchical to: No other components.

319 Dependencies: No dependencies.

320 **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*].

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

7.3 Definition of the Family AVA_POI

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

323 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 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. Only applicable attacks from [POI AttackPot] have to be considered in this PP.
- AVA_POI has dependencies on ADV_FSP, ADV_TDS and AGD. AVA_POI allows requiring (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.

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

325 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.

326 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.

327 We refer to Section 11 for a detailed explanation of the relationship between AVA_VAN.2 and AVA_POI.

328 AVA_POI Vulnerability analysis of POI

329 Objectives

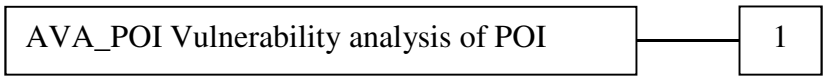
330 POI vulnerability analysis is an assessment to determine whether potential vulnerabilities identified in the POI could allow attackers to violate the SFRs and thus to perform unauthorized access or modification to TOE assets, data or functionality.

331 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.

332 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.

333 Component Levelling

334 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.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

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

336 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*].

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 constraints 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."*

8 Security Requirements

8.1 Security Functional Requirements

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

- POI_DATA Package
- CoreTSF Package
- MiddleTSF Package
- Cryptography Package
- Physical Protection Package

338 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

339 Assignments, selections, refinements or iterations are presented in *italics* and have to be filled by the ST Author. Assignments, selections, refinements or iterations already filled by the PP are **bold**. Assignments, selections, refinements or iterations which are assigned by the PP and have to be filled by the ST Author are presented in ***bold italics***. Both *italic* and ***bold italics*** are mandatory to be filled in by the ST Author.

Policy	Entity	Name	Value (for security attributes)	Definition
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		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, 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
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

Table 11: Entities definition in Security Function Policies

8.1.1 Definition of SFR packages

8.1.1.1 POI_DATA Package

FDP_ACC.1/POI_DATA Subset Access Control

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

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

subjects: POI and its Payment Application Logic

objects: Payment Transaction Data, POI Management Data, POI_SK, Cardholder communication interface, [assignment: *list of payment application internal data*]

operations: send, receive, access.

FDP_ACF.1/POI_DATA Security attribute based access control

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

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

subjects: POI and its Payment Application Logic

objects: Payment Transaction Data, POI Management Data, POI_SK, Cardholder communication interface, [assignment: *list of payment application internal data*]

security attribute of POI_SK: purpose and validity

security attribute of Payment Transaction Data, POI Management Data: access right of Payment Application and authenticity status

[assignment: *list of security attributes*]

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

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).

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).

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 clear text 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:

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

Protection of POI_SK in a POI component against disclosure.

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.

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.

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:

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.

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 device has timed-out waiting from the Cardholder or merchant.

Application note:

This SFR requires that sensitive information shall not be present any longer or used more often than strictly necessary. Buffers shall be cleared immediately 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.

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.

8.1.1.2 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 (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 TOE.

The TOE performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the TOE is in a compromised state. In the event of a failure, the TOE and its functionality fail in a secure manner. The TOE 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 CoreTSF secret data.

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

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 any key type. The operations are any management operation on CoreTSF software and data.

If no list of data exists 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.

[assignment: ***additional importation control rules*****]**

Application note:

If the TOE allows updates of firmware, the TOE 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.

8.1.1.3 MiddleTSF Package

FPT_TST.1/MiddleTSF TSF testing

Dependencies: No dependencies.

FPT_TST.1.1/MiddleTSF 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 MiddleTSF**.

FPT_TST.1.2/MiddleTSF 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/ MiddleTSF 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 MiddleTSF software within the TOE and the Card Reader

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

failure of MiddleTSF self-test

logical anomalies of MiddleTSF

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

Application note:

The "secure state" does not provide access to any other MiddleTSF secret data.

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

The TOE's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong TOE mode and supplying wrong parameters or data which could result in the display outputting sensitive data.

If no list of types of failures exists the assignment shall be filled with none.

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: [assignment: *list of data, in particular cryptographic keys, controlled under this policy*]

operation: download.

Application note:

The "cryptographic keys" stand for any key. The operations are any management operation on MiddleTSF software and data.

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

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

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

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

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

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

The Middle Loader downloads only authentic and 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 are cleared or if the rollback is not possible all MiddleTSF secret data are erased.

[assignment: *additional importation control rules*]

Application note:

The functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong TOE mode and supplying wrong parameters or data which could result in outputting sensitive data.

If the TOE allows updates of firmware, the TOE 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.

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".

The firmware must support the authentication of applications loaded onto the TOE. If the TOE allows software application and/or configuration updates, the TOE cryptographically authenticates updates.

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, the phrase "POI software" is interpreted as ***payment application software***

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

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.

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

FDP_ACC.1/MiddleTSFLoader Subset access control

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

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

subject: Middle Loader

objects: POI_SW, [assignment: ***list of data, in particular cryptographic keys, controlled under this policy*****]**

operation: download.

Application note:

The "cryptographic keys" stand for POI encryption keys (POI_SK). The operations are any management operation on MiddleTSF software and data.

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

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

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

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

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

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

The Middle Loader downloads only authentic and 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:

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

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.

The functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong TOE 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.

FDP_ACC.1/ MiddleTSF Subset access control

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

FDP_ACC.1.1/MiddleTSF The TSF shall enforce the **MiddleTSF SFP** on

subjects: POI components

object: POI_SW, [assignment: *list of data, in particular cryptographic keys, controlled under this policy*]

operations: download.

FDP_ACF.1/MiddleTSF Security attribute based access control

Dependencies:
FDP_ACC.1 Subset access control satisfied by FDP_ACC.1/MiddleTSF
FMT_MSA.3 Static attribute initialisation

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

subjects: POI components

[assignment: ***list of security attributes***]

FDP_ACF.1.2/MiddleTSF The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment:** *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]**.**

FDP_ACF.1.3/MiddleTSF The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment:** *rules, based on security attributes, that explicitly authorise access of subjects to objects*]**.**

FDP_ACF.1.4/MiddleTSF The TSF shall explicitly deny access of subjects to objects based on the **following rules: [assignment:** *rules, based on security attributes, that explicitly deny access of subjects to objects*]**.**

8.1.1.4 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:

If random numbers are generated by the TOE 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 **encipherment/decipherment** in accordance with a specified cryptographic algorithm **[assignment:** *cryptographic algorithm***]** and cryptographic key sizes **[assignment:** *cryptographic key sizes***]** that meet the following: **Standardized specification of cryptographic algorithm**.

Application note:

The author of the Security Target shall iterate this SFR for each TSF part (CoreTSF, MiddleTSF) if necessary.

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_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 (CoreTSF, MiddleTSF) and assign the related SFP (Prompt Control SFP, POI Management and Pay-

ment Transaction Data Information Flow Control SFP), if necessary (i.e. if TDES keys are handled).

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, MiddleTSF.) if necessary.

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.

8.1.1.5 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**

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

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

Penetration of the TOE to disclose the 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:

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 TOE, such that it becomes infeasible to recover the sensitive data.

The TOE makes inaccessible any secret or private keys or other secret information when operational or environmental conditions occurs that are not within the specified 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.

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

This requirement is not applicable in the POI-CHIP-ONLY-NO-CVM configuration. Instead FPT_PHP.3/CHIP-ONLY-NO-CVM holds for the POI-CHIP-ONLY-NO-CVM 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** in excess of **none** enabling access to **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)** to gain access to **encryption keys** and **none**.

Application note:

Recall that CoreTSF shall contain at least the encryption module (device Security Module).

This requirement is not applicable in the POI-CHIP-ONLY-NO-CVM configuration. Instead FPT_EMSEC.1/CHIP-ONLY-NO-CVM holds for the POI-CHIP-ONLY-NO-CVM configuration.

FPT_PHP.3/CardReader Resistance to physical attack

Dependencies: No dependencies.

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

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 TOE components that belong to the.

This requirement is not applicable in the POI-CHIP-ONLY-NO-CVM configuration.

FPT_PHP.3/CHIP-ONLY-NO-CVM Resistance to physical attack

Dependencies: No dependencies.

FPT_PHP.3.1/CHIP-ONLY-NO-CVM The TSF shall resist **the physical tampering scenarios**

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

Penetration of the TOE to disclose POI_PayDatSK and 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-NO-CVM configuration.

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

FPT_EMSEC.1/CHIP-ONLY-NO-CVM TOE Emanation

Dependencies: No dependencies.

FPT_EMSEC.1.1/CHIP-ONLY-NO-CVM The TOE shall not emit **measurable signals including power fluctuations** in excess of **none** enabling access to **POI_PayDatSK** and **none**.

FPT_EMSEC.1.2/CHIP-ONLY-NO-CVM The TSF shall ensure **all users** are unable to use the following interface **emanations (including power fluctuations)** to gain access to **POI_PayDatSK** and **none**.

Application note:

This requirement is only applicable for the POI-CHIP-ONLY-NO-CVM configuration.

8.1.2 Security Functional Requirements in each base PP

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

SFR Package	**TSF part(s)**	**POI-COMPREHENSIVE-NO-CVM**	**POI-CHIP-ONLY-NO-CVM**
POI_DATA	MiddleTSF	X	X
CoreTSF	CoreTSF	X	X
MiddleTSF	MiddleTSF	X	X
Cryptography	CoreTSF	X	X
	MiddleTSF	X	X
Physical Protection			
FPT_PHP.3/CoreTSF	CoreTSF	X	
FPT_EMSEC.1/ CoreTSF	CoreTSF	X	
FPT_PHP.3/ CardReader	ICCR TSF, see [POI_PPV4]	X	
FPT_PHP.3/ CHIP-ONLY-NO-CVM	CoreTSF		X
FPT_EMSEC.1/ CHIP_ONLY-NO-CVM	CoreTSF		X

Table 12: SFR packages included in each base PP

8.1.3 Security Functional Requirements dependencies rationale

341 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.

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

8.2 Security Assurance Requirements

343 The minimum EAL applicable to the products evaluated against this PP is EAL POI defined hereafter. Adopted from [POI_PPV4] and modified to fit this NO-CVM PP and called EAL POI NO CVM here after.

344 Most of the assurance components belonging to EAL POI NO CVM 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-Moderate for CoreTSF, and POI-Basic and for MiddleTSF.

345 The following table lists the Security Assurance Requirements included in EAL POI NO CVM:

- "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.

346 Notice that EAL POI NO CVM 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 11 for details).

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

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

Security Assurance Requirements			EAL POI NO-CVM POI-COMPREHENSIVE-NO-CVM POI-CHIP-ONLY-NO-CVM
EAL2	ADV_ARC.1	REFINED	X X
	ADV_FSP.2	STANDARD	X X
	ADV_TDS.1	STANDARD	X X
	AGD_OPE.1	REFINED	X X
	AGD_PRE.1	REFINED	X X

	ALC_CMC.2	REFINED	X X
	ALC_CMS.2	REFINED	X X
	ALC_DEL.1	REFINED	X X
	ATE_COV.1	STANDARD	X X
	ATE_FUN.1	STANDARD	X X
	ATE_IND.2	REFINED	X X
	AVA_VAN.2		
	ALC_DVS.2	REFINED	X X
	ALC_FLR.1	REFINED	X X
	AVA_POI.1/MiddleTSF	POI-Basic attack potential	X X
	AVA_POI.1/CoreTSF	POI-Moderate attack potential	X X

Table 13: Definition of EAL POI by base PP

8.2.1 Security Assurance Requirements Rationale

349 The EAL POI in [POI_PPV4] 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. Today, CAS is replaced with the Common.SECC (Common Security Evaluation Certification Consortium) as interested user group of this PP.

350 The starting point of EAL POI was CAS risk analysis and its derived security requirements. Indeed, selecting most of the assurance components from EAL2 for EAL POI was sufficient to meet the CAS security. CAS requirements that fall outside standard SAR are addressed by additions (like ALC_DVS.2), by specific refinements stated in section 8.2.2 and by extensions with new assurance components AVA_POI, stated in section 8.2.3. AVA_POI components allow to go beyond EAL2 vulnerability analysis without significant increase of documentation, design and testing effort

351 The above mentioned is adopted in this PP and modified for achieving the EAL POI NO CVM assurance class.

352 For the chosen assurance components all the dependencies are met or exceeded in the EAL POI NO CVM assurance package as shown in section 8.2.4.

8.2.2 Refined security assurance requirements

8.2.2.1 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.

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.

8.2.2.2 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.

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.

8.2.2.3 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.

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,

- Sensitive functions or data are only used in the protected areas(s) of the TOE. This refinement is not applicable for the POI-CHIP-ONLY-NO-CVM configuration.
- 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-NO-CVM configuration. This part of the TSF is assigned to MiddleTSF and thus AVA_POI.1/MiddleTSF has to be applied to this property of the security architecture.
- 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 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.

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:

- Failure of a single security mechanism does not compromise the TOE security. Protection against and 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-NO-CVM configuration.
- For POI-CHIP-ONLY-NO-CVM: Cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts are prevented.

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

8.2.2.4 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:

The vendor must provide adequate documented security guidance for the integration of any secure component into POI Terminal.

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 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 device, 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 TOE is put into maintenance mode, and the vendor's requirements for secure handling of the TOE. 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:

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.

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:

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:

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 TOE. Additionally, cryptographic keys can also be loaded during the user phase. The ST author shall define where the developer phase ends and where the user phase begins in relation to cryptographic key loading.

8.2.2.5 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:

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:

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.

8.2.2.6 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 device in order to comply with the following:

Each device shall have a unique visible identifier affixed to it. The unique identifier applies to the tamper-resistant boundaries (e.g. Secure Module, Card Reader). They must be visible without opening the device.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

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

8.2.2.7 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:

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.

8.2.2.8 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).

8.2.2.9 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 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 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.

The certified[3] 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.

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) in the scope of the evaluation and unauthorized substitutions have not been made.

[3] Certified here means that the Firmware has been checked by the developer. Hence, the Firmware that is part of the configuration items has been checked in integrity.

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

Production software (e.g., firmware) that is loaded to the TOE at the time of manufacture is transported, stored, and used under the principle of dual control, preventing unauthorized modifications and/or substitutions.

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

If the TOE 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.

Security measures are taken during development and maintenance of TOE 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 TOE 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 TOE security-related components.

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.

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

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

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

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 TOE 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:

TOE 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.

The TOE 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 TOE.
Where this is not possible, the TOE 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 TOE 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.

Procedures are in place to transfer accountability for the TOE 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:

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).

8.2.2.10 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:

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 TOE 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.

8.2.2.11 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:

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

For all these TSFI, the evaluator shall assess that:

The TOE 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

The TOE 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.

The TOE 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.

The TOE implements session management.

- a) The TOE 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 TOE sets time limits for sessions and ensures that sessions are not left open for longer than necessary.

8.2.3 Extended security assurance requirements

353 The AVA_POI requirements of the EAL POI NO CVM package consists of:

- AVA_POI.1.

354 AVA_POI.1 is iterated four times and applied to MiddleTSF and CoreTSF.

8.2.3.1 _POI applied to MiddleTSF

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 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.

8.2.3.2 AVA_POI applied to IC Card Reader TSF

355 This requirement holds in POI-COMPREHENSIVE-NO-CVM configurations only if the device accepts contact based IC Card based transactions. This PP does not define a separated IC Card Reader TSF structure for contact based IC card readers. **If the TOE accepts contact based IC card transactions then the contact based IC card reader has to be assessed in accordance with [POI_PPV4].**

8.2.3.3 AVA_POI applied to MSR

356 This requirement holds in POI-COMPREHENSIVE-NO-CVM configurations only if the device accepts magnetic stripe reader based transactions. This PP does not define a separated MSR TSF structure. **If the TOE accepts MSR based transactions then the contact MSR has to be assessed in accordance with [POI_PPV4].**

8.2.3.4 AVA_POI applied to CoreTSF

357 This requirement holds for all configurations.

358 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 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.

8.2.4 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/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/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

Table 14: SAR dependencies

9 Rationale Objectives/SFR

359 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.CoreSWHW	O.PEDMiddleSWHW	O.CardReader	O.PaymentTransaction	O.POI_SW	O.PaymentApplicationDownload	O.POIApplicationSeparation
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						
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	
Cryptography Package							
FCS_RND.1							
FCS_COP.1			X				

	O.CoreSWHW	O.PEDMiddleSWHW	O.CardReader	O.PaymentTransaction	O.POI_SW	O.PaymentApplicationDownload	O.POIApplicationSeparation
FDP_ITC.2			X				
FTP_ITC.1/Crypto			X				
FPT_TDC.1			X				
Physical Protection Package							
FPT_PHP.3/CoreTSF	X		X				
FPT_EMSEC.1/CoreTSF			X				
FPT_PHP.3/CardReader			X				
FPT_PHP.3/CHIP-ONLY-NO-CVM				X			
FPT_EMSEC.1/CHIP-ONLY-NO-CVM				X			

Table 15: Objectives coverage by SFRs

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

361 **O.CoreSWHW**

362 Rationale:

- In POI-CHIP-ONLY-NO-CVM only Card based transactions are accepted. Thus FPT_PHP.3.1/CHIP-ONLY-NO-CVM instead of FPT_PHP.3/CoreTSF applies for POI-CHIP-ONLY-NO-CVM.
- 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.
- FPT_FLS.1/CoreTSF enforces the CoreTSF authenticity and integrity by preserving a secure state in case of self-test failure or logical anomalies.
- 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.

363 **O. CardReader**

364 Rationale:

- FPT_PHP.3/CoreTSF and FPT_EMSEC.1/CoreTSF protect secret cryptographic against disclosure by physical attacks or by emanation (PCIA6).
- FPT_PHP.3/CardReader protect the Card Reader against the physical tampering.
- FDP_RIP.1/CardReader prevents unwanted knowledge of secret data upon the de-allocation of the resources from sensitive objects.
- 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. The cryptographic key import is supported by FTP_ITC.1/Crypto and FPT_TDC.1.

365 **O.PaymentTransaction**

366 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.
- FDP_ITT.1/POI_DATA protects the disclosure of POI_SK when it is transferred between physically separated parts of the POI.
- FDP_UIT.1/POI_DATA protects POI Management Data and Payment Transaction Data at the external lines of the POI against modification.
- FDP_UCT.1/POI_DATA provides means to protect Payment Transaction Data at the external lines of the POI against disclosure.

367 FDP_ACC.1/POI_DATA and FDP_ACF.1/POI_DATA prevents other application to deceive the Cardholder during execution of the payment application.

- 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.
- 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 the POI-CHIP-ONLY-NO-CVM 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-NO-CVM 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.

O.POI_SW

368 Rationale:

- FPT_FLS.1/MiddleTSF enforces the MiddleTSF 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 due to SFRs FDP_ACC.1/MiddleTSFLoader and FDP_ITC.1/MiddleTSFLoader.

369 **O.PaymentApplicationDownload**

370 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.

371 O.POIApplicationSeparation

372 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; that it is not possible for another application to interfere with the execution of the payment application by accessing internal data.
- FDP_RIP.1/POI_DATA ensures that no residual information remains in resources released by the payment application and payment application temporary cryptographic keys.

10 Definition of the SRED PP-Module

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

374 As described in section 2 the SRED module can be added to a base PP including the POI-COMPREHENSIVE-NO-CVM configuration. During the text in this chapter this configuration is sometimes called the **underlying configuration**. This chapter is taken from [POI PP V4] renaming POI-COMPREHENSIVE into POI-COMPREHENSIVE-NO-CVM and removing other configurations defined in [POI PP V4] which are not in the scope in this PP.

10.1 Security Problem Definition

10.1.1 Assets

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

376 PAY_DAT

377 Payment transaction data

378 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 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.

379 Sensitivity: Authenticity and Integrity.

380 Application Note:

381 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.

382 Note: This asset is already contained in the POI-COMPREHENSIVE-NO-CVM configuration; its definition is slightly extended here and may therefore replace the asset of the underlying configuration.

383 PAN

384 Primary account number

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

386 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)

387 It should be noted that even in encrypting mode, the device still has the possibility to transfer a cleartext version of the PAN to an authorized application within the device

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

389 TOE_CLEAR_PAN

390 PAN in clear text.

391 Sensitivity: Confidentiality, Authenticity, and Integrity.

392 TOE_CIPHER_PAN

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

394 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.

395 Sensitivity: Confidentiality, Authenticity, and Integrity.

396 Application Note:

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

398 In that case,

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

399 TOE_PAN_SK

400 Secret/private PAN cryptographic keys for internal TOE transmission

401 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

402 Sensitivity: Confidentiality, Authenticity and Integrity.

403 Application Note:

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

405 **E2E_CIPHER_PAN**

406 Encrypted PAN for end-to-end transmission

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

408 Sensitivity: Confidentiality, Authenticity, and Integrity.

409 **E2E_PAN_PK**

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

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

412 Sensitivity: Authenticity and Integrity.

413 **E2E_PAN_SK**

414 Private cryptographic keys for end-to-end encryption

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

416 Sensitivity: Confidentiality, Authenticity and Integrity.

Application Note:

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

418 **SURROGATE_PAN**

419 Surrogate PAN value

420 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

421 Sensitivity: Authenticity and Integrity.

422 **SURROGATE_PAN_SALT**

423 Salt used to generate a surrogate PAN value

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

425 Sensitivity: Authenticity, Integrity and Confidentiality.

10.1.2 Users / Subjects

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

10.1.3 Threats

427 This threat is already defined by POI-COMPREHENSIVE-NO-CVM but gives here some more examples addressing the PAN.

428 T.Transaction

429 Transaction with usurped Cardholder identity

430 Edition of T.Transaction as defined in PP POI-COMPREHENSIVE-NO-CVM - 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.

10.1.4 Organisational Security Policies

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

10.1.5 Assumptions

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

10.2 Security Objectives

10.2.1 Security Objectives for the TOE

433 The SRED PP-Module includes the objectives **O.PaymentTransaction**, **O.POI_SW**, and **O.POIApplicationSeparation** as defined in section by POI-COMPREHENSIVE-NO-CVM.

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

435 O.PANConfidentiality

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

437 O.PANDeduction

438 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.

439 O.PANOperatingMode

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

441 *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.*

10.2.2 Security objectives for the Operational Environment

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

10.2.3 Security Objectives Rationale

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

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

445 The SRED PP-Module adds the following paragraph to the rationale already given in section 6.1:

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.

10.3 Extended Requirements

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

10.4 Security Requirements

10.4.1 Security Functional Requirements

447 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

448 *Application Notes:*

- *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).*

449 The table hereafter lists the SFR packages in the SRED PP-Module and explains their relation to the PP and their usage in POI-COMPREHENSIVE-NO-CVM.

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.	-
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.	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

Package	SFR	Usage	Comments
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 16: SFR packages in the SRED PP-Module

450 A general note for all of the SRED SFRs:

451 Several of these SFRs are already contained in a very similar form in the underlying configuration from the PP. 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.

10.4.1.1 SRED Basis Package

452 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 in chapter 10.4.3.3.

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 TOE_PAN_SK, E2E_PAN_SK/E2E_PAN_PK*
- *Risk Manager is related to status of E2E_CIPHER_PAN.*
- *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.*
- *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.*

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) 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.*

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.*

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.*
- *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.*

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.**

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:

- **If the TOE 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:

- *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.*

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 TOE is forced to return to its normal mode.**

FPT_PHP.3/SRED Resistance to physical attack

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

- **Penetration of the Card Reader to make any additions, substitutions or modifications to either the Card Reader's hardware or software, in order to determine or modify any sensitive data.**
- **Insertion of both a card and any other foreign object within the card insertion slot.**
- **Replacement of the front and rear casing, which shall be considered as part of any attack scenario.**
- **Operational or environmental conditions that are not within the specified operating range (e.g temperature or operating voltage outside the state operating range).**
- **Penetration of the TOE to disclose the PAN encryption keys.**
- **Unauthorized modification or substitution of public keys stored in the device**
- **[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:

- The TOE uses tamper detection and response mechanisms which cause the TOE to become immediately inoperable and results in the automatic and immediate erasure of any secret information which may be stored in the TOE (PAN, secret cryptographic keys, salt used to generate the surrogate PAN, administration passwords, etc.).
- The TOE makes inaccessible any PAN value, secret or private keys or other TOE secret information when operational or environmental conditions occurs that are not within the specified TOE 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*

FPT_EMSEC.1/SRED TOE Emanation

FPT_EMSEC.1.1/SRED The TOE shall not emit

- **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

- **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:

- *Recall that the scope of this SFR shall contain at least the Card Reader and PAN encryption module (Security Module).*

FMT_MSA.1/SRED Management of security attributes

FMT_MSA.1.1/SRED The TSF shall enforce 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.*
- *Status of operation mode having the value "Encrypting mode" means that the device's encryption of account data functionality is enabled and operational.*
- *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.*
- *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.*

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 of

- **the CoreTSF (CORE_SW and CORE_HW).**
- **the MiddleTSF**.

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**.

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:

The device supports data origin authentication of encrypted messages.

10.4.1.2 SRED Cryptography Package

This package defines cryptography requirements related to:

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

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_PAN_PK/E2E_PAN _SK and TOE_PAN_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 SM.*
- *If remote key distribution is used, the device supports mutual authentication between the sending key distribution host and receiving device.*

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 SM.*

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.*

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 **[assignment:** *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 SM.*

10.4.1.3 SRED Distributed Architecture Package

453 This package addresses the need for protection of the PAN when the TOE is operating as distributed architecture

454 "Distributed architecture" has here to be understood as architectures where the Card Reader are separated from secure module (i.e. not integrated into one single tamper-responsive boundary).

455 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 secure module, which then deciphers it before ciphering it again (E2E_CIPHER_PAN) for the Acquirer.

456 This package is not required if the TOE has an integrated architecture.

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: 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)**.

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: 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:

- **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 Card Reader may send TOE_CIPHER_PAN to the SM**.

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 Card Reader do not send or receive TOE_PAN_SK to/from any subject.**
- **The Card Reader do not send TOE_CLEAR_PAN to any subject.**
- **The Card Reader do not send TOE_CIPHER_PAN to any other subject than the secure module.**
- **The TOE has characteristics that prevent or significantly deter the use of the device for exhaustive PAN determination.**
- **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 and key-encipherment keys have different values.**
- **When operating in encrypting mode, there is no mechanism in the Card Reader 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:

- *When operating in encrypting mode, there is no mechanism in the Card Reader 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.*
- *PAN encryption keys (TOE_PAN_SK) are stored in the Security Module of the component or encrypted.*

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 device or*
- *between the Card Reader (either Card Reade) and device.*

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]**.

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 Card Reader**
- **TOE_CIPHER_PAN immediately after being sent to the secure module by Card Reader**
- **TOE_PAN_SK immediately after being used to cipher TOE_CLEAR_PAN into TOE_CIPHER_PAN by Card Reader [assignment: *sensitive objects with residual information*]**.

Refinement:

- **These deallocations are performed by the Card Reader. Deallocation by the device upon reception is addressed in the End-to-end protection Package.**
- **Deallocation may occur upon completion of the transaction or Card Reader has timed-out waiting from the Cardholder or Merchant.**

Application Note:

- *Account data (in either clear-text or encrypted form) shall not be retained any longer, or used more often, than strictly necessary.*
- *The Card Reader must automatically clear its internal buffers when either: The transaction is completed, or the Card Reader 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.*

10.4.1.4 SRED End-to-end protection Package

457 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.

- *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 device, and the corresponding key.*

458 Note: The cleartext TOE_CLEAR_PAN can also be transmitted by the device, but only to authenticated applications within the device.

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: Device (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.**

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: Device (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 Device: encrypting, non encrypting**
- **information: TOE_CIPHER_PAN, TOE_CLEAR_PAN, TOE_PAN_SK**
- **status of TOE_PAN_SK: validity, purpose**
- **operation mode of the device: 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:

- **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 Device can transfer a cleartext TOE_CLEAR_PAN to an authenticated application within the device.**
- **The device can receive TOE_CIPHER_PAN from the Card Reader. The device deciphers TOE_CIPHER_PAN into TOE_CLEAR_PAN with the appropriate dedicated key immediately after it is is received from Card Reader.**
- **The device can receive TOE_CLEAR_PAN from the Card Reader.**
- **If the operating mode is "encrypting" the device enciphers TOE_CLEAR_PAN with the appropriate dedicated key before 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, which explicitly authorise information flows***]**.

FDP_IFF.1.5/SRED_E2E The TSF shall explicitly deny an information flow based on the following rules:

- **The device does not receive E2E_PAN_SK or E2E_PAN_PK from any other subject than an authenticated key distribution host.**
- **If the operating mode is "encrypting" the device does not send the TOE_CLEAR_PAN to any other subject than an authenticated application within the device**
- **The device does not send E2E_PAN_SK to any subject before being encrypted.**
- **The device does not accept a TOE_CLEAR_PAN or TOE_CIPHER_PAN from any other subject than the Card Reader.**
- **The device has characteristics that prevent or significantly deter the use of the device for exhaustive PAN determination.**
- **Encryption or decryption of any arbitrary data using any account data-encrypting key or key-encrypting key contained in the device is not permitted.**
- **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.*
- *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 the TOE or encrypted.*

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.*

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.*

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 Card Reader has timed-out waiting from the Cardholder or merchant.

Application Note:

- *Account data (in either clear-text or encrypted form) shall not be retained any longer, or used more often, than strictly necessary.*

- ***If the device and 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 device and 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 head) immediately after reception. TOE_CIPHER_PAN is sent to the device, 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.*

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 device.*

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 device 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 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.*

10.4.1.5 SRED Surrogate PAN Package

459 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.

460 SFRs in this package are applicable to MiddleTSF in POI-COMPREHENSIVE-NO-CVM configuration.

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:

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.

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.*
- *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.*
- *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.*

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: device**
- **information: SURROGATE_PAN, SURROGATE_PAN_SALT**
- **operations: send.**

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: device**
- **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 device 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:

- **The device has characteristics that prevent or significantly deter the use of the device for exhaustive PAN determination.**
- **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 and key-encipherment keys have different values.**
- **The device cannot send the SURROGATE_PAN_SALT to any other subject.**

Application Note:

- *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.*
- *the salt used to generate surrogate PAN (SURROGATE_PAN_SALT) is stored by MiddleTSF*

10.4.2 Security Assurance Requirements

461 The SRED PP-Module uses the assurance package of the underlying POI-COMPREHENSIVE-NO-CVM configuration, to which is added. It adds refinements to some of the assurance components. These refinements are defined in this section.

462 With regard to AVA_POI the SRED PP-Module has the following requirements:

- A very specific part of the SRED functionality, namely "5. 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 1. 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.

463 The other SARs are left unchanged from the claimed and defined assurance package of this PP.

10.4.2.1 Refinements for SARs defined for the SRED PP-Module

ADV_ARC.1 Security architecture description

Refinement for **ADV_ARC.1.3C:**

Refinement:

- Initialization includes the logical and physical integration of an approved card reader into a POI terminal. Such integration does not create new attack paths to the account data. The account data is protected from the input component to the secure controller of the device.

Refinement for **ADV_ARC.1.5C**

Refinement:

- 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.
- 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.*
- *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:

- The vendor must provide clear security guidance to ensure that the device 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 device outputting the clear text PAN or other sensitive information.

Refinement for **AGD_OPE.1.6C**

Refinement:

- 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:

- *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.*

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: Secret and private keys that reside within the device to support account data encryption are unique per device.
- If the 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).

ALC_CMS.2 Parts of the TOE CM coverage

Refinement for **ALC_CMS.2.2C**

Refinement:

- The OS/Firmware, and any changes thereafter, has been inspected and re-viewed using a documented and auditable process, and certified as being free from hidden and unauthorized or undocumented functions.

10.4.3 Security Requirements Rationale

10.4.3.1 Objectives

464 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

- 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.

10.4.3.2 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.

Security Objectives	Security Functional Requirements
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 17: Security Objectives and SFRs in SRED- Coverage

10.4.3.3 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	

Requirements	CC Dependencies	Satisfied 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
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

Requirements	CC Dependencies	Satisfied Dependencies
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 18: 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

465 Since all SARs are taken from the POI MO-CVM PP, the same rationale already given there holds (see section 8.2.1).

10.4.3.4 Rationale for the Security Assurance Requirements

466 The assurance requirements are taken from the POI-COMPREHENSIVE-NO-CVM base PP configuration, to which the SRED PP-Module can be 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 MO-CVM PP is given in the next chapter 10.5.

10.5 Rationale of consistency of the SRED PP-Module with the POI-COMPREHENSIVE-NO-CVM base PP

467 As explained in chapter 1 and 2, the POI-COMPREHENSIVE-NO-CVM base PP can be extended by the SRED PP-Module given in 10**.** In order that the SRED PP-Module can be used without checking whether the SRED PP-Module is consistent to the base PP, this chapter gives a rationale for the consistency.

468 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).

469 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 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.

470 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 underlying base PP.

471 User and subjects are the same in the base PP and in the SRED PP-Module.

472 SRED PP-Module does not define additional threats, but refines the existing T.Transaction defined in the PP. The refinement is consistent because it is related to the PAN and this does not contradict other threats.

473 There are no additional assumptions or OSPs.

474 The three objectives O.PaymentTransaction, O.POI_SW, and O.POIApplicationSeparation already included in POI_COMPREHENSIVE-NO-CVM.

475 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 objectives of the base PP. O.PANOperatingMode introduces a new operating mode which does not contradict the base PP objectives.

476 There are no security objectives for the environment.

477 For the SFR part the following holds:

478 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.

479 In addition the table Table 16 in the beginning of chapter 10.4.1 “Security Functional Requirements” of 10 explains and thus gives a rationale for the relation of the SFRs to the base PP.

480 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.

481 The same argument holds for the assurance components.

11 Annex – Relationship between AVA_POI and AVA_VAN.2 families

The following approach is adopted from [POI_PPV4] and modified to suit the need for this NO-CVM-PP.

482 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 of [POI_PPV4] 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]. Remember, EAL POI is from [POI_PPV4] and modified to fit this NO-CVM PP and called EAL POI NO CVM here after.

483 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]).

484 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 which allows requiring 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.

485 In EAL POI NO CVM, each POI component in the scope of the evaluation is addressed by at least one AVA_POI.1 iteration: POI components belong to one of the TSF parts CoreTSF, or MiddleTSF and each of these parts are addressed by at least one iteration of AVA_POI.1. For other TSFs concerning other card readers than the contactless reader, the

[POI_PPV4] has to be consulted. Hence, the set of AVA_POI iterations included in EAL POI NO CVM constitutes a refinement of AVA_VAN.2 applied to the whole TOE.

12 Glossary

486 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.
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).
Common.SECC	Common Security Evaluation Certification Consortium
Enciphered	Enciphered information.
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.

Term	Definition
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
Merchant	A retailer, or any other person, company, or corporation that agrees to accept (bank) cards in the framework of a contract with an Acquirer. In this Protection Profile the Merchant is also responsible for the TOE in order to protect the TOE against manipulations of the enclosure.
Multi-application	A POI that may be used for more than one (card) application.
Offline	Deferred processing without direct communication.
Online	Direct communication between devices with electronic capability (e.g. POI to hosts).
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/Firmware	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, multitasking, 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 func-

Term	Definition
	tions). 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 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.
POI	A POI is an electronic transaction acceptance product. A POI consists of hardware and software and is hosted in an acceptance equipment to enable a Cardholder to perform a card transaction. Thereby the POI may be attended or unattended. POI transactions are IC card based payment transactions as well as any other payment transactions e.g. based on Magnetic Stripe or any non-payment transactions like health, loyalty or government. The TOE is at minimum a POI excluding applications.
POI component	Any physical or logical device involved in a card payment at a POI (e.g. beeper, Card Reader, display, printer).
POI management data	All 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.
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

Term	Definition
	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 display.
Receipt	A hard copy document recording a payment transaction that took place at the POI, with a description that usually includes: date, Merchant name/location, primary account number, amount, and reference number.
Reconciliation	An exchange of messages between two institutions (Acquirer, Issuer or their agents) to reach agreement on financial totals.
Retailer protocol	Protocol used between the sale system (electronic cash register, vending unit, service station infrastructure,..) and the POI.
Reversal	Cancellation of a previous transaction. There might be manual as well as automatic reversals.
Secret (cryptographic) key	A cryptographic key used with symmetric cryptographic techniques and usable only by a set of specified entities.
Sensitive data	Data that must be protected against unauthorized disclosure, alteration or destruction, especially PINs and secret and private cryptographic keys. Depending on the context of the functional requirement sensitive data may be restricted to Plaintext PIN or to Ciphertext PIN and to a subset of cryptographic keys.
Sensitive functions	Sensitive functions are those functions that process sensitive data such as cryptographic keys or PINs.
Sensitive services	Sensitive services provide access to the underlying sensitive functions.
Session key	A key established by a key management protocol, which provides security services to data transferred between the parties. A single protocol execution may establish multiple session keys, e.g., an encryption key and a MAC key.
Settlement	A transfer of funds to complete one or more prior transactions made, subject to final accounting and corresponding to reconciliation advices.
Script	A command or string of commands transmitted by the Issuer to the terminal for the purpose of being sent serially to the IC card.
Secure Application Module (SAM)	See Security Module.
Secure soft-	All software that are involved in the secure handling of IC card payment transaction, i.e. PIN encryption, parameter and software

Term	Definition
ware	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 related to security protection of the payment transaction. E.g. critical parameters, cryptographic keys, etc.
SRED	Secure Read and Exchange – A set of requirements for protection of 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.
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.