DPS SKP200 / SCR200
Common Criteria Security Target

Version 0.2
17 November 2013

paymentexpress®

Table of contents

Table of figures

Table of tables

1 SECURITY TARGET INTRODUCTION

1 This document provides the security target (ST) for the SKP200 and SCR200 PED, designed and manufactured by Direct payment Solutions of 98 Anzac Avenue, Auckland, New Zealand.. It is provided in accordance with Common Criteria version 3.1 Revision 4, and claims conformance to the POI-COMPREHENSIVE configuration of version 2.0 Point of Interaction Protection Profile (26th November 2010), [POI PP]. The product within the scope of this protection profile is a payment terminal with Integrated Circuit (IC) Card based online and offline transaction capabilities, with optional privacy shielding compliant with EPC guidelines.

2 The POI-COMPREHENSIVE configuration requires that the TOE provide protection for both IC and Magnetic Stripe card based transactions and is fully PCI POS PED v2.0 conformant. It provides payment transaction data management and external communication facilities for interaction with the Acquirer defined by CAS. The POI-COMPREHENSIVE configuration covers a harmonized superset of all security requirements that are considered appropriate to defend against current and perceived future threats. The aim of this configuration is to support the concept of the POI as a universal acceptor for SEPA compliant cards. It is the baseline configuration that is intended to secure common approval across all CAS member markets.

1.1 SECURITY TARGET IDENTIFICATION

Title	SKP200 / SCR200 Common Criteria Security Target
Author	Primasec Ltd
Version	0.01
Date	17 November 2013
CC Version	3.1 Revision 4

Table 1 – ST identification

1.2 TOE IDENTIFICATION

1.2.1 TOE component versions

SCR200	
Hardware version	SCR200

AT91SO application firmware	DPSSCR200 v1.2
MSP tamper firmware	GridMonitor_SCR200 v1.0
MSR firmware	MagHead_SCR200 v1.0
DPS secure boot firmware	SBOOT v2.2
SKP200	
Hardware version	SKP200
AT91SO application firmware	DPSSKP200 v1.0
MSP tamper firmware	GridMonitor_SKP200 v1.0

Table 2 – TOE identification

1.2.2 Non-TOE hardware

3 A system controller is connected via a serial link to the SCR200 unit to support an external communications link. The system controller does not form part of the TOE.

1.3 REFERENCES

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

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

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

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

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

[EMV] EMV Book 1 to 4, Version 4.2

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

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

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

[POI PP] Point of Interaction Protection Profile – POI-COMPREHENSIVE configuration, Identification: ANSSI-CC-PP-2010/10 Level EAL_POI, Authors: Sandro Amendola, SRC Security Research & Consulting GmbH Carolina Lavatelli, Trusted Labs on behalf of CAS (Common Approval Scheme), version 2.0, Publication Date: 26th November, 2010, Sponsor: ANSSI, CC: Version 3.1 Revision 3

[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 TOE OVERVIEW

2.1 TOE TYPE

4 The TOE is a product of type Point of Interaction (POI), with optional privacy shielding compliant with EPC guidelines [EPC Shield].

5 The TOE is to be evaluated against the POI-COMPREHENSIVE configuration, providing protection for both IC and Magnetic Stripe card based transactions. It provides payment transaction data management and external communication facilities for interaction with the Acquirer.

2.2 SCOPE OF EVALUATION

6 The TOE provides a physical keypad, Magnetic Stripe Reader (MSR), Integrated Circuit Reader (ICCR), LCD display, and serial communications. The TOE includes two separate devices, a PINpad with integrated display (SKP200), and a secure card reader with both magnetic and IC card readers (SCR200). The devices are connected together with a single serial cable, and the card reader is connected to a 'system controller' with a separate serial cable. The system controller is outside the scope of the evaluation.

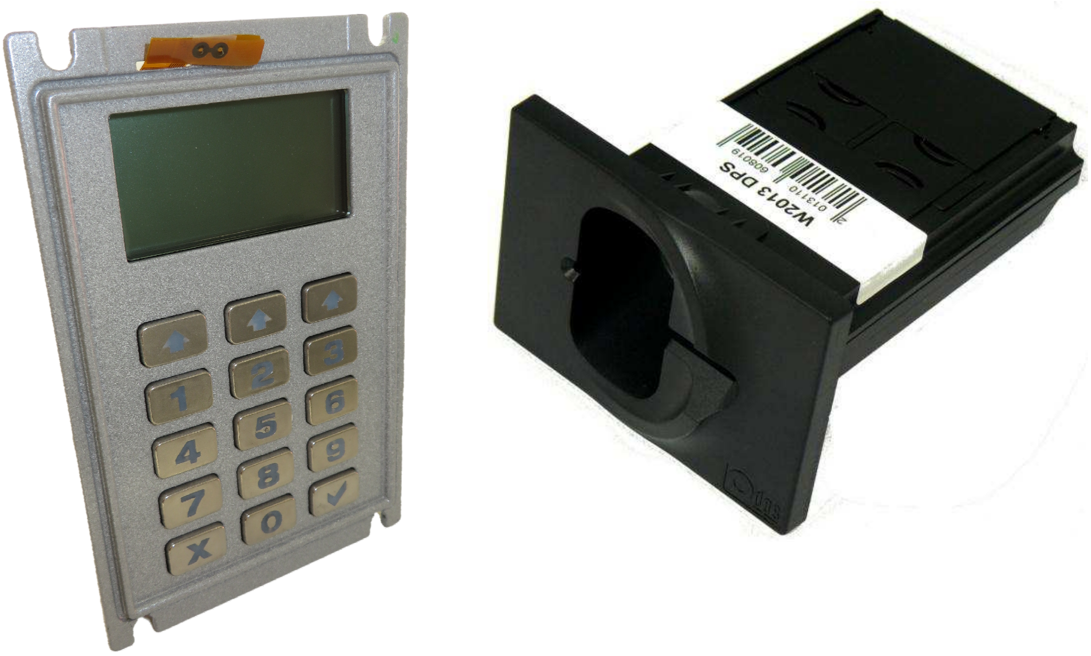

Figure 1 –SKP200 and SCR200

7 Figure 2 below shows the connections between the TOE components, the system controller and the host.

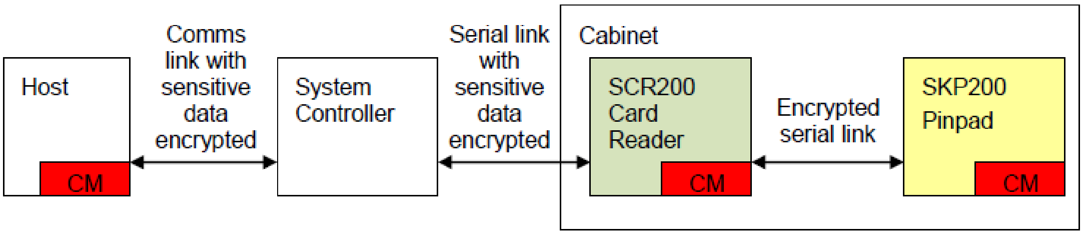

Figure 2 –TOE physical connections

8 The functionality of the PED is determined by the configuration carried out at DPS. The standard configuration would include:

a) Magnetic stripe capability with optional online PIN authentication;

b) Contact EMV capability with offline PIN authentication;

c) Contact EMV capability with online PIN authentication;

d) Contact EMV capability with no card holder verification.

2.3 TOE SECURITY FEATURES

9 The aim of this section is to provide a high level description of the POI configuration, its logical and physical perimeter, assets, objectives and security features.

2.3.1 Payment Transaction Process

10 The terminal supports both online and offline PIN verification. The following figure from [POI PP] shows the POI payment transaction process based on offline PIN verification.

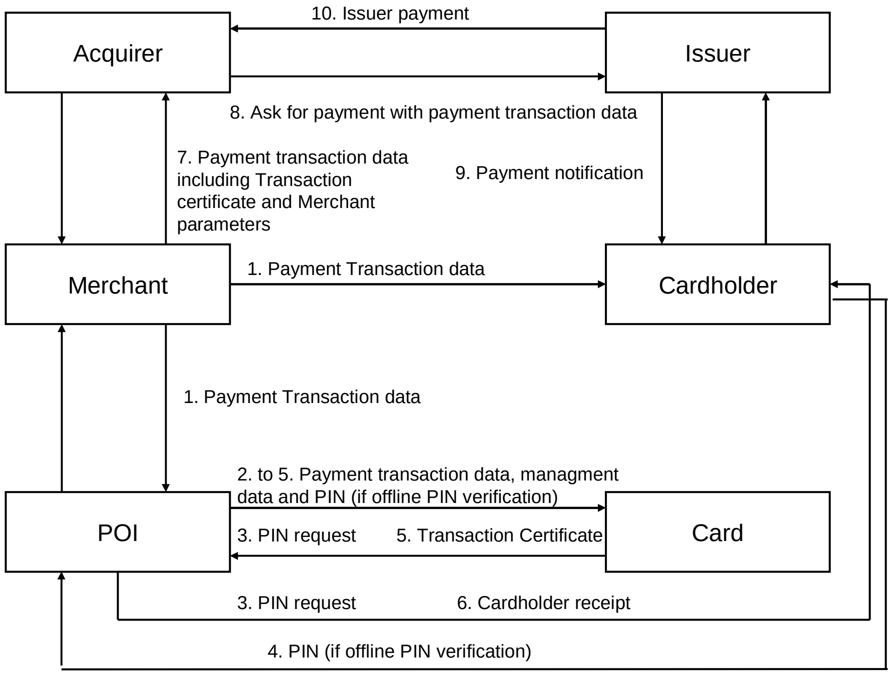
10. Issuer payment
Acquirer
Issuer
8. Ask for payment with payment transaction data
7. Payment transaction data including Transaction certificate and Merchant parameters
9. Payment notification
Merchant
1. Payment Transaction data
Cardholder
1. Payment Transaction data
2. to 5. Payment transaction data, managment data and PIN (if offline PIN verification)
POI
3. PIN request
5. Transaction Certificate
Card
3. PIN request
6. Cardholder receipt
4. PIN (if offline PIN verification)

Figure 3 - POI Payment Transaction Process

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

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

3. The card requests Cardholder authentication by PIN comparison.

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

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

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

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

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

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

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

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

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

2.3.2 Terminal Management Process

12 The 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/or the POI sends POI management data to the TMS via a data upload.

3. POI configurations are activated or deactivated (e.g. new software is activated).

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

2.3.3 POI Architecture

13 The generic POI architecture in [POI PP] includes the following components:

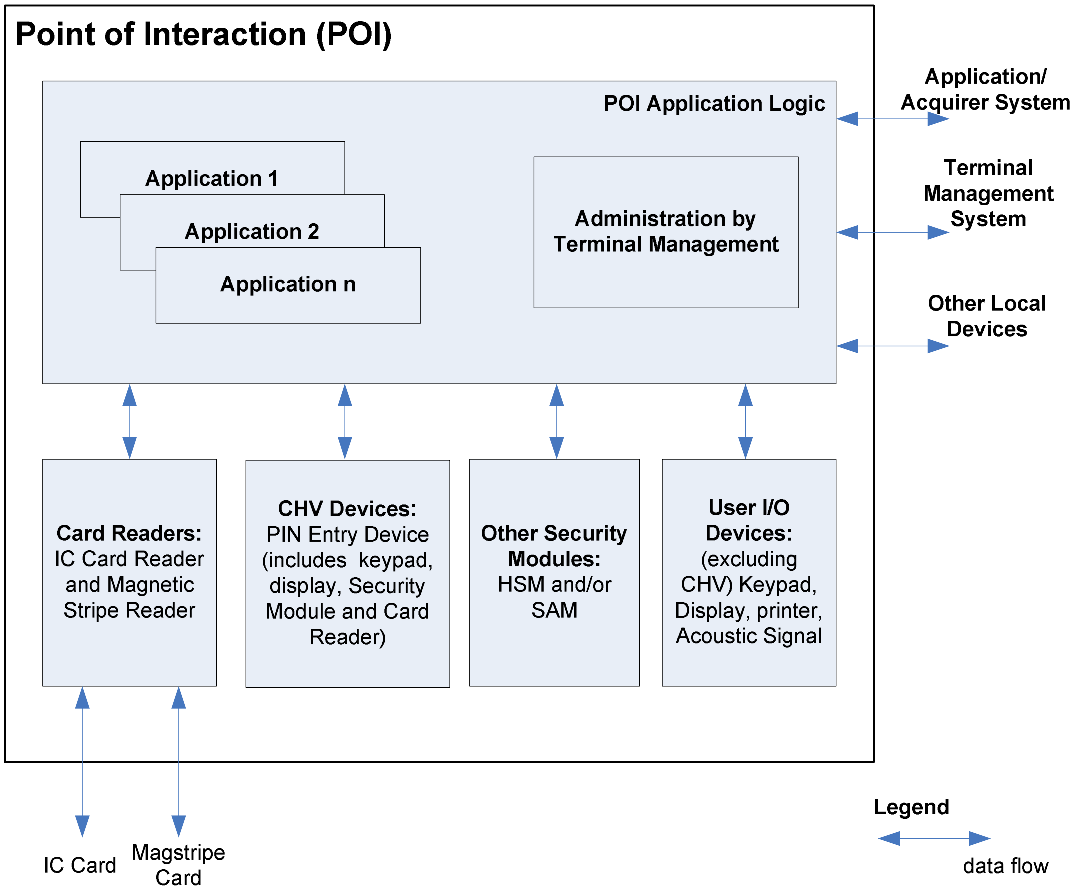
Point of Interaction (POI)
POI Application Logic
Application 1
Application 2
Application n
Administration by Terminal Management
Application/ Acquirer System
Terminal Management System
Other Local Devices
Card Readers: IC Card Reader and Magnetic Stripe Reader
CHV Devices: PIN Entry Device (includes keypad, display, Security Module and Card Reader)
Other Security Modules: HSM and/or SAM
User I/O Devices: (excluding CHV) Keypad, Display, printer, Acoustic Signal
IC Card
Magstripe Card
Legend
data flow

Figure 4 - POI Architecture

2.3.4 POI Architecture Components

14 All POI components are integrated in the same device as the POI Application Logic. The following are the principal architectural 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.). The POI supports a multi-application environment. For this TOE there is only a single application.

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 TOE supports IC contact cards, IC contactless cards and Magnetic Stripe cards. The IC Card Readers are contained within a tamper-responsive enclosure (CHV devices block in figure 2).

- **Cardholder Verification Devices** (CHV): devices for Cardholder authentication, e.g. a PIN Entry Device (PED). This TOE includes a keypad, a display and a security module (SM) for PIN encryption, thus allowing Cardholder PIN entry and authentication. The interfaces of the PED keypad security module and the PED display are protected.

- **Security Module** (SM): devices for management of cryptographic keys and cryptographic functions (e.g. a Hardware Security Modules (HSM) or a Security Application Module (SAM) as part of a CHV).

- **User I/Os:** that include display, keyboard, printer, and audible signals.

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

- **IC Card**: The Cardholder's IC Card interacts with the POI through the IC Card Reader (contact based).

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

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

- **Terminal Management System:** Entity used to administer (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.

15 Figure 5 shows the set of components and functions of the TOE in POI-COMPREHENSIVE configuration, showing all components in one device, excluding any payment application.

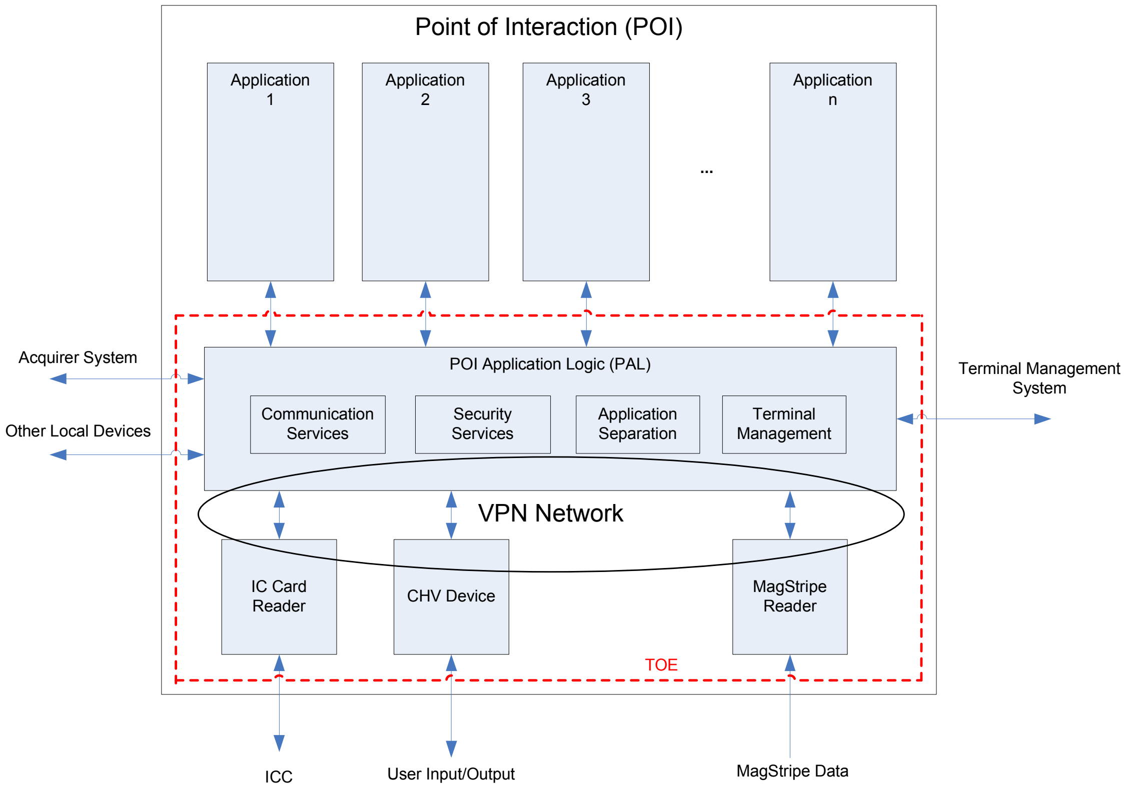

Figure 5 - TOE in POI-COMPREHENSIVE configuration

2.3.5 TOE specific architecture

2.3.5.1 SCR200 secure card reader

16 The SCR200 secure card reader contains an ICC reader, magnetic stripe reader, secure processor and integrated communications. These parts are contained within a tamper detecting box and plastic external casing.

17 The front bezel is constructed with either plastic or zinc. The front bezel is attached with bolts inserted from the behind the front. The front is designed to be easily removed for installation of the Card Reader into a cabinet. Three communications ports are located on the rear of the device; one is for connection to the pin pad, a second for connection to a system controller and the third reserved for future use.

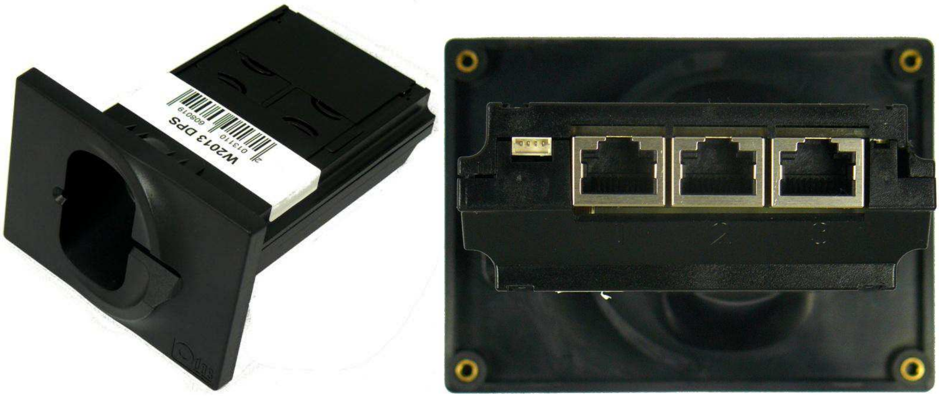

Figure 6 - SCR200

2.3.5.2 SKP200 secure PIN entry device

18 The keypad and display are integrated into a single tamper detecting module. The front of the device is constructed from zinc. A Perspex cover protects the Liquid Crystal Display and is located near the top end of the device. 15 metallic keys are used to enter numeric data into the device.

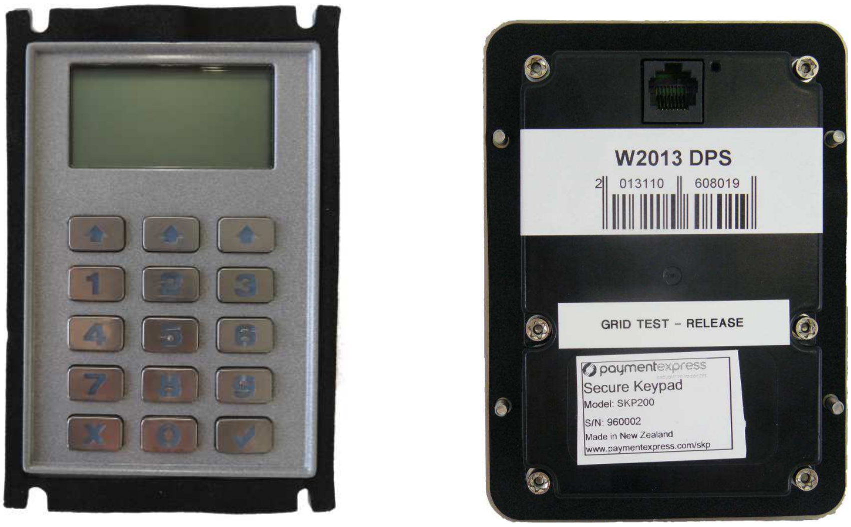

Figure 7 - SKP200

2.3.5.3 Communication services

19 A POS / System Controller is integrated via a serial link connected to the SCR200 unit. The System Controller will communicate to the PED using the proprietary *DPS SCR200 Serial Message Specification*. This specification provides a set of basic commands to a POS / Sys-

tem Controller to allow a transaction to be started, and allows the SCR200 push commands back to the DPS HOST. This communication channel is opened when the controller sends the TXEN (Transmit Enable) command to the SCR200. From there the SCR200 will send unsolicited TX messages to the POS, which it will forward to DPS HOST for decryption using Thales HSM. No financial messages can be initiated until the SCR200 has successfully sent and received all required messages to PXHOST. These may be logon messages or for configuring downloads.

20 The unit must be initialized before a transaction can take place. In some circumstances this will require the device to logon to the DPS HOST and re-download the configuration.

21 The most basic transaction is initiated using an AUTH message, where the system controller will specify the amount of the transaction. The SCR200 unit will take over once a transaction request has been initiated. It will control the processing of the MSR, IC Card Reader, and SKP200 until the transaction has completed. It will then return the result to the system controller. During the transaction the SCR200 may communicate back to the DPS HOST in order to submit the transaction result or perform and online authorization. The communication from the SCR to the DPS HOST is protected using DUKPT message encryption as defined in ANSI X9.24-1:2009. In the case of a failed transmission the SCR200 will respond according and may queue an advice in which case must be transmitted to the DPS HOST.

22 The system controller is outside the scope of the evaluation.

2.3.6 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, the following properties on the assets. These properties on the assets provide an overview of the objectives for the TOE which are precisely described in section 5:

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

25 The TOE provides a set of security features that meets the intended usage and the assumptions on the environment. [POI PP] provides for each of the security features to be protected at a specific level, namely, POI-Basic, POI-Low, POI-Moderate or POI-High. The precise definition of these protection levels in terms of attack potential is given in [POI AttackPot]. The TSF for this TOE is implemented as a single application, and as such all security features are protected at POI-High.

26 [POI PP] uses a logical TSF structure that may be viewed as TSF concentric rings (also called TSF parts), as shown as coloured rings in the following figure, with the colours indicating the protection level. For this TOE the colours should be disregarded, since the TOE provides the highest level of protection for all rings.

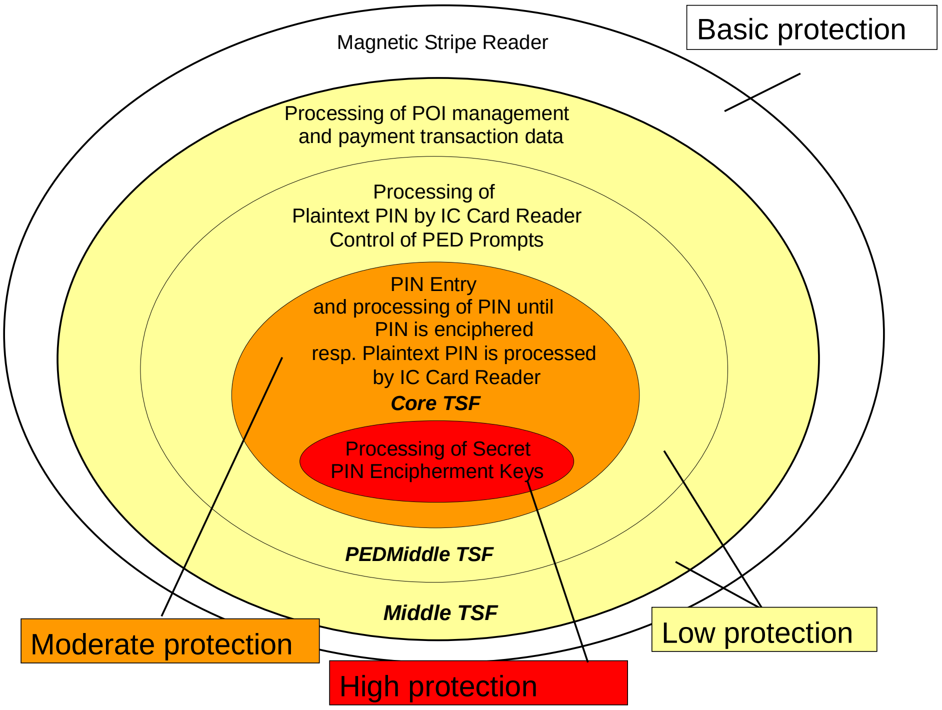

Figure 8 - TSF structure in POI-COMPREHENSIVE configuration

27 The [POI PP] TSF parts define the logical and physical TOE boundary of the TOE configuration.

- Core TSF Keys
- Core TSF
- PEDMiddle TSF
- Middle TSF
- MSR

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

1. PIN Entry without exposure of PIN digits.
2. Encipherment of PIN for offline or online Cardholder encrypted PIN authentication and transfer for further processing (to the IC Card Reader or to the Acquirer).
3. Protected transmission of PIN for offline Cardholder authentication of Plaintext PIN to the IC Card Reader.
4. Periodic authentication of PIN processing software.
5. Authenticity and integrity protection of administration (e.g. downloading, update) of PIN processing software and keys, including appropriate cryptographic means.
6. 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.
7. Authenticity and integrity protection of administration (e.g. downloading, update) of POI management and transaction processing software and keys, including appropriate cryptographic means.
8. Control of PED prompts.
9. Tamper-detection/tamper-responsiveness (PED, PED SM, IC Card Reader, IC Card Reader SM, Magnetic Stripe Reader).
10. Secure downloading of payment application.

29 Table 3 - TSF decomposition defines the logical boundaries of the TOE in terms of TSF parts implementing a particular set of security features. The items in the cells refer to the security features listed in section 2.3.5.

		CoreTSF	**PED**		
PP configuration	**CoreTSF**	**Keys**	**Middle TSF**	**Middle TSF**	**MSR**
POI-COMPREHENSIVE	1, 2, 3, 4, 5, 9	PIN encipherment keys for 2, 9	8, 9	6, 7, 10	9

Table 3 - TSF decomposition

30 Table 4 - Physical boundaries of TSF parts

31 defines the default physical boundaries of the TOE in terms of components associated to TSF parts.

		CoreTSF	**PED**		
PP configuration	**CoreTSF**	**Keys**	**Middle TSF**	**Middle TSF**	**MSR**

POI-COMPREHENSIVE	PED Keypad	PED_SM	PED Display PED KeyPad IC Card Reader	Other POI components	Magnetic Stripe Reader

Table 4 - Physical boundaries of TSF parts

2.4 TOE DOCUMENTATION

32 The following documentation is available to support use of the TOE:

SCR200/SKP200 Hardware Installation Guide

2.5 NON-TOE HARDWARE/ SOFTWARE/ FIRMWARE AVAILABLE TO THE TOE

33 The following are outside the scope of the TOE:

a) System controller

b) DPS host

2.6 TOE USAGE

34 The TOE is intended to be used in attended and unattended payment environments, within a secure cabinet enclosure. In the POI-COMPREHENSIVE configuration the TOE is intended to be used in any SEPA payment environment satisfying global PCI requirements.

2.7 TOE LIFE CYCLE

2.7.1 Overview

35 An overview of the TOE lifecycle is shown in Figure 9. Note that in the figure, two main blocks are clearly differentiated:

- The Developer Phase, which comprises all tasks to be performed prior to the delivery of the product. This phase includes manufacturing and initial SW and initial key loading processes;
- The Operational (User) Phase: which covers all that happens to a terminal once it has been delivered.

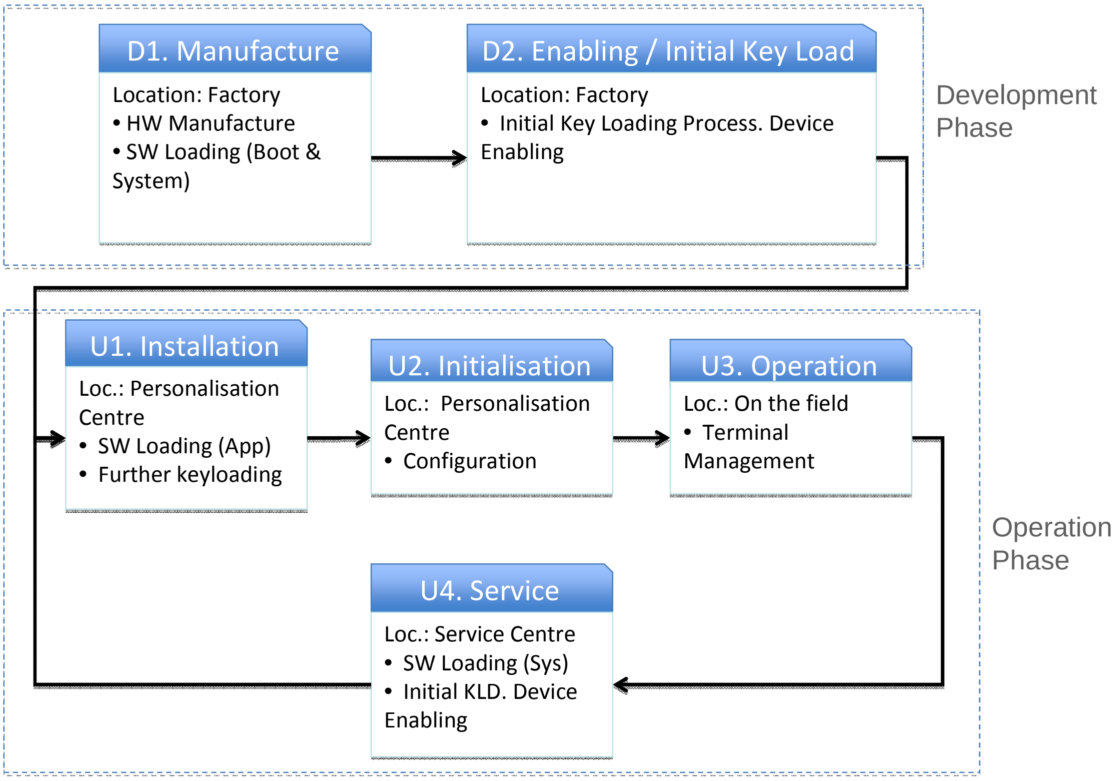

Figure 9 - Security Product Life Cycle

2.7.2 Developer Phase

36 In this phase two major tasks are fulfilled.

1. The terminal is manufactured and some initial software is loaded into it. This initial software includes the bootloader of the device, and all other firmware and System software and system applications.
2. The terminal undergoes its initial key loading session, which also acts as its enabling process.

37 Note that these two processes take place at the same physical location, the DPS manufacturing site, with the key loading process executed in a secure environment.

2.7.2.1 D1. Manufacturing

38 Manufacturing includes all processes and tasks leading to a fully built and operational device, lacking only Application software and cryptographic keys. At the end of the process the output is a disabled terminal with all firmware and system software loaded.

39 Both the SCR200 and SKP200 use a security microprocessor manufactured by ATMEL, which has been designed specifically for high security systems such as payment terminals and pin entry devices. It provides secure application loading between the ATMEL factory

and the recipient of the chip. ATMEL injects a unique derived key per microprocessor, and also loads the ATMEL SBOOT bootloader.

40 DSP manufactures the SCR and SKP units. As part of quality assurance a test application is downloaded to the device allowing certain test functions to be performed. This test application is pre-signed by the DPS and is downloaded via the HSM onto the device using the ATMEL SBOOT. This ensures that only DPS test firmware can be loaded during time of manufacturing.

41 A report is generated after a batch has been manufactured, this is loaded into the asset management system by a member of the logistics team. The process of entering the batch involves scanning the barcode of each device and inspecting the device for damage or signs of tamper. The batch is then secured into a tamper evident box for transport and moved into a secured storeroom. The status of the batch is then updated in the asset management system as 'ready for loading'.

2.7.2.2 D2. Firmware and Key Loading / Device Enabling

42 The outcome of this process is an enabled terminal, with its initial keys loaded and ready for delivery.

43 The firmware is built using the DPS build server environment. A SHA-256 hash of the firmware is generated under dual control, and encrypted with the DPS private key. The signed firmware is then copied to the download server, along with the signature.

44 The firmware and key loading process is done as a single step at the Key Injection Facility (KIF) at 98 Anzac Ave, Auckland New Zealand.

45 The loading process requires two activations staff member to activate the loading batch. The key injection batch activation process involves the staff members logging on to the DPS Payment Management Interface, the first member selects the batch and pre-configured firmware profile and selects activate, the other member refreshes the page and selected confirm. The batch is then activated on the KIF software for loading.

46 The two staff members then enter the KIF using dual access cards and panels, and load the batch. The firmware and key loading process overwrites the ATMEL SBOOT software with the DPS SBOOT 2.2. The KIF facility provides a key injector, a bar-code reader and step by step process to follow. It allows loading of only the serial numbers in the batch, in any order and any exceptions (faulty loads) are recorded. The DUKPT keys and RSA keys necessary for communication and pairing between the SCR and SKP are injected during this process.

47 When the loading process has been completed the devices are placed back into the storage container and re-sealed. The staff members exit the KIF using dual access panels and transport the devices back into the secured storeroom. The asset manager status is then updated to 'Ready to ship'.

48 The procedure is designed such that two people must be present and participate in the loading process.

2.7.3 Operation Phase

49 The operation phase covers all tasks from delivery to the personalisation centre to use of the product for payment processing, and the repair work a product may undergo.

2.7.3.1 U1. Installation/Personalisation

50 The outcome of this process is an enabled terminal ready for shipment to a customer.

51 The DPS activations staff are responsible for provisioning the configurations before a terminal is shipped to a customer.

52 The DPS TMS has pre-configured configurations that have been certified with an acquirer, these include card prefix tables, kernel configurations and terminal configurations.

53 The staff member will configure a 'Port' which assigns a virtual terminal configuration bound to a SCR device. The Port defines the terminal id and merchant id that is used against the acquirer, this can only be changed at DPS. Additional details such as card acceptor name location and other merchant details are also loaded into the port.

54 The SCR is assigned a 'Card Acceptor Device Profile', this then relates to what kernel configurations are enabled and what card prefix tables are downloaded. Any customization required for the customer must be performed through the DPS TMS by authorized personnel. The DPS TMS is accessible by the Payment Management Interface, which enforces permissions to select personnel and audits all changes to the system.

55 Functional tests are performed on the device once the configuration is complete. This includes verifying basic functions, i.e. mag-stripe reads, EMV reads, SCR+SKP pairing.

56 The devices are then packaged and the status is updated to 'Shipped'.

2.7.3.2 U2. Initialisation

57 The outcome of this process is a fully functional terminal, ready to process financial transactions.

58 Upon receiving hardware the customer will install the device using a POS certified by DPS. The unit must be properly mounted into the enclosure to ensure all removal sensors are closed. When the device has been installed the controller software MUST perform a logon before first use, this is enforced by the SCR. The initial logon will report a removal, which is then corrected by DPS support staff in the DPS TMS. Confirmation of identity is perform on the merchant as per standard DPS security checks.

59 A subsequent logon will cause the SCR to verify local configuration with the configuration loaded into the DPS TMS. This will mismatch on first use, and a configuration download will be initiated. Once all configuration has been downloaded the unit will be functional.

2.7.3.3 U3. Operation

60 The terminal will be in normal use by the end user, processing financial transactions. Depending on the acquirer application and the device communication capabilities, the terminal may connect to a Terminal Management System put in place by the acquirer or the merchant. The connection and functionalities of the Terminal Management System are acquirer/merchant and application dependent. and hence their definition is out of the scope of this document. Note that, in any case, the Terminal Management System will make use of the security features of the TOE, such as software authentication.

61 If the device ever suffers a malfunction, it will be returned to DPS for repair.

2.7.3.4 U4. Service

62 The outcome of this process is a serviced / repaired and enabled terminal, with its initial keys loaded and ready for redelivery. Apart from the servicing tasks, the process and security requirements are the same as that described above for process D2.

3 CONFORMANCE CLAIMS

3.1 CONFORMANCE CLAIM TO CC

63 This ST is conformant to the Common Criteria version 3.1 revision 4:

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

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

65 CC Part 3 is extended with the security assurance components AVA_POI.1 Basic POI vulnerability analysis, AVA_POI.2 Low POI vulnerability analysis, AVA_POI.3 Moderate POI vulnerability analysis, and AVA_POI.4 High POI vulnerability analysis.

3.2 CONFORMANCE CLAIM OF THE ST TO [POI PP]

66 This ST claims strict conformance, as defined in CC Part 1 [CC1], to [POI PP] POI-COMPREHENSIVE configuration.

67 This ST claims conformance to the EAL_POI assurance package, as defined in [POI PP].

68 The ST includes all of the assets, users, subjects, threats, organisational security policies, assumptions, objectives, security functional requirements and security assurance requirements contained in [POI PP] that are applicable to the TOE. Items that are not applicable to this TOE are marked using ~~strikethrough text~~. The exclusion of all such non-applicable items is permitted by [POI PP].

4 SECURITY PROBLEM DEFINITION

4.1 ASSETS

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

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

Table 5 - Assets sensitivity

PIN

70 Cardholder personal identifier, used to authenticate against the IC Card or the Issuer. The PIN represents the digits entered by the Cardholder, before any treatment by the TOE.

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

Sensitivity: Confidentiality.

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

72 PIN used by the Cardholder to authenticate in one of the two following ways (cf. item 2 from the list of security features in section 2.3.6)

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

74 Offline ciphertext authentication: the POI payment application and the IC Card application require sending the PIN encrypted to the IC Card via the IC Card Reader interface.

Sensitivity: Confidentiality.

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

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

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

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

Sensitivity: Confidentiality.

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

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

Sensitivity: Confidentiality.

Application note: This corresponds to items 3 and 5 from the list of security features (cf. section 2.3.6).

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

79 The PLAIN_PIN that has to be sent to the IC Card Reader in cleartext is called Cleartext PLAIN_PIN.

Sensitivity: Confidentiality.

Application note: This corresponds to item 4 from the list of security features (cf. section 2.3.6).

POI_SW (POI software)

80 Software (code and data) of the MiddleTSF.

Sensitivity: Authenticity and Integrity.

PED_MIDDLE_SW

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

Sensitivity: Authenticity and Integrity.

PED_MIDDLE_HW

82 Hardware of the PEDMiddle TSF.

83 Within this TOE this corresponds to the ICC reader.

Sensitivity: Authenticity and Integrity.

CORE_SW

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

85 Within the TOE this corresponds to the bootloader and firmware.

Sensitivity: Authenticity and Integrity.

CORE_HW

86 Hardware of the Core TSF.

87 Within the TOE this corresponds to the security island, the keypad and the enclosure.

Sensitivity: Authenticity and Integrity.

MAN_DAT (POI management data)

88 POI Management data are the POI Unique Identifier, the Merchant Identifier and the Acquirer risk management data[1]. The POI_PK is a special kind of MAN_DAT.

Sensitivity: Authenticity, Integrity.

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

PAY_DAT (Payment transaction data)

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

Sensitivity: Authenticity and Integrity.

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

ENC_PIN_PK (Public ENC_PIN cryptographic keys)

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

Sensitivity: Authenticity and Integrity.

ENC_PIN_SK (Secret/private ENC_PIN cryptographic keys)

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

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

Sensitivity: Confidentiality, Authenticity and Integrity.

PED_MIDDLE_PK (Public PEDMiddle cryptographic keys)

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

Sensitivity: Authenticity and Integrity.

PED_MIDDLE_SK (Secret/private PEDMiddle cryptographic keys)

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

Sensitivity: Confidentiality, Authenticity and Integrity.

POI_PK (Public POI cryptographic keys)

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

Sensitivity: Authenticity and Integrity.

POI_SK (Secret/private POI cryptographic keys)

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

Sensitivity: Confidentiality, Authenticity and Integrity.

PLAIN_PIN_SK (Secret/private PLAIN_PIN cryptographic keys)

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

Sensitivity: Confidentiality, Authenticity and Integrity.

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

Magnetic Stripe Track Data

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

Sensitivity: Confidentiality, Authenticity and Integrity

PAYMENT_APP

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

102 The payment application is out of scope for this TOE.

Sensitivity: Integrity and Authenticity

4.1.1 Assets and TSF parts

103 Table 6 - Assets mapped to TSF components

104 defines the assets and the TSF parts to which they are assigned. Note that an asset may be associated with more than one TSF part.

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

Table 6 - Assets mapped to TSF components

4.2 USERS

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

106 Users are defined sections 4.2.1 and 4.2.2.

4.2.1 Authorised Human Users

Cardholder

107 The Cardholder interacts with the POI via man-machine interfaces: reads payment transaction data displayed on the POI, inserts IC card, authenticates with a PIN, confirms the payment transaction and takes the receipt.

Attendant

108 The payment application in the POI may initiate a payment transaction at the request of the Attendant. The Attendant interacts with the TOE via a man-machine interface. The Merchant himself can be the attendant.

Merchant

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

Terminal Administrator

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

4.2.2 External Entities

Acquirer system

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

Terminal Management System

112 The Terminal Management System is the entity used to administer (install, maintain) a set of POIs: software and parameter download and application activation / deactivation. Used by a Terminal Administrator.

IC Card

113 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.

Magnetic Stripe Card

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

Local Device

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

Payment Application

116 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

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

4.3 SUBJECTS

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

Payment Application Logic (PAL)

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

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

Terminal Management

121 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.

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

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

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

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

Core Loader

124 The loader downloading CORE_SW into the POI.

PED Middle Loader

125 The loader downloading PED_MIDDLE_SW into the POI.

Middle Loader

126 The loader downloading POI_SW into the POI.

Payment Application Loader

127 Loader for downloading and updating payment applications.

Magnetic Stripe Reader

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

4.4 THREATS

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

T.MerchUsurp (Merchant Identity Usurpation)

130 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.

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

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

T.CardholderUsurpEPIN (Cardholder Identity Usurpation ENC_PIN)

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

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

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

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

T.CardholderUsurpCiphPPIN (Cardholder Identity Usurpation Ciphertext PLAIN_PIN)

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

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

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

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

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

142 *Application note: This threat applies only to a POI with separated PED and IC Card Reader, and so is not applicable for this TOE.*

T.CardholderUsurpClearPPIN (Cardholder Identity Usurpation Cleartext PLAIN_PIN)

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

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

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

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

T.PromptControl (Manipulation of Prompt Control)

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

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

T.Transaction (Transaction with usurped Cardholder identity)

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

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

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

149 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.

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

T.BadDebt (Account overdraft, bad debt)

151 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.

152 Related assets: POI_SW, MAN_DAT.

T.SecureCommunicationLines

153 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.

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

155 *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

156 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.

157 Related assets: Magnetic Stripe Track Data.

T.IllegalCodeInstall

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

159 Related assets: PAYMENT_APP.

4.5 ORGANISATIONAL SECURITY POLICIES

OSP.WellFormedPayApp (Well-formed Payment Applications)

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

OSP.ApplicationSeparation

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

OSP.POISurvey

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

OSP.MerchantSurvey

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

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

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

OSP.KeyManagement

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

4.6 ASSUMPTIONS

A.UserEducation

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

A.SecureDevices

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

A.PinAndCardManagement

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

5 SECURITY OBJECTIVES

5.1 SECURITY OBJECTIVES FOR THE TOE

O.PINEntry

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

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

O.EncPIN

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

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

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

176 This objective entails the following derived objectives:

a) The TOE shall protect the confidentiality of ENC_PIN_SK.

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

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

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

O.CipherPPIN

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

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

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

182 This objective entails the following derived objectives:

a) The TOE shall protect the confidentiality of PLAIN_PIN_SK.

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

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

184 *Application note: This objective applies to POI architectures with separated PED and IC Card Reader (e.g. different tamper-responsive boundaries), and so is not applicable to this TOE.*

O.ClearPPIN

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

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

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

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

O.CoreSWHW

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

190 This objective entails the following derived objectives:

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

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

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

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

O.PEDMiddleSWHW

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

193 This objective entails the following derived objectives:

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

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

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

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

O.ICCardReader

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

O.PaymentTransaction

196 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.

197 This objective entails the following derived objectives:

a) The TOE shall protect the confidentiality of POI_SK.

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

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

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

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

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

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

O.POISW

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

201 This objective entails the following derived objective:

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

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

O.PaymentApplicationDownload

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

O.POIApplicationSeparation (Application Separation)

204 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.

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

O.PromptControl

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

O.MSR (TOE Protection of Magnetic Stripe Reader)

207 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.

208 The table below maps the objectives applicable to the POI-COMPREHENSIVE configuration to specific areas of the TSF.

	POI-COMPREHENSIVE			
Objective for the TOE	**Core TSF**	**CoreTSF Keys**	**PEDMiddle TSF**	**Middle TSF**
O.PINEntry	x			
O.EncPIN	x	x		
O.CipherPPIN	x	x		
O.ClearPPIN	x			
O.CoreSWHW	x	x		
O.PEDMiddleSWHW			x	
O.ICCardReader			x	
O.PaymentTransaction				x
O.POISW				x
O.PaymentApplicationDownload				x

Objective for the TOE	POI-COMPREHENSIVE			
	Core TSF	CoreTSF Keys	PEDMiddle TSF	Middle TSF
O.POIApplicationSeparation				x
O.PromptControl			x	
O.MSR	MSR TSF			

Table 7 - Objectives for the TOE

5.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

OE.POISurvey

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

OE.MerchantSurvey

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

OE.UserEducation

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

OE.SecureDevices

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

OE.KeyManagement

213 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.

OE.PinAndCardManagement

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

OE.WellFormedPayApp Well-formed Payment Application

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

OE.LocalDevices

216 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.

6 RATIONALE BETWEEN SPD AND SECURITY OBJECTIVES

6.1 THREATS

217 This section presents generic rationales between threats and objectives.

T.MerchUsurp (Merchant Identity Usurpation)

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

219 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.

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

221 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.

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

T.CardholderUsurpEPIN (Cardholder Identity Usurpation ENC_PIN)

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

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

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

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

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

T.CardholderUsurpClearPPIN (Cardholder Identity Usurpation Plaintext PLAIN_PIN)

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

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

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

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

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

T.PromptControl

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

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

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

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

236 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.

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

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

T.FundsAmount (Funds transfer other than correct amount)

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

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

241 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.

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

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

T.BadDebt (Account overdraft, bad debt)

244 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.

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

246 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.

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

T.SecureCommunicationLines

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

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

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

251 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.

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

T.Magstripe

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

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

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

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

6.2 OSP

OSP.WellFormedPayApp

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

OSP.ApplicationSeparation

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

OSP.POISurvey

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

OSP.MerchantSurvey

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

OSP.KeyManagement

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

6.3 ASSUMPTIONS

A.UserEducation

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

A.SecureDevices

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

A.PinAndCardManagement

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

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

Table 8 - SPD coverage by objectives in POI-COMPREHENSIVE configuration

7 EXTENDED REQUIREMENTS

264 The text for this section is unchanged from that in [POI PP], and has therefore not been repeated here.

8 SECURITY REQUIREMENTS

8.1 SECURITY FUNCTIONAL REQUIREMENTS

265 This security target defines the following packages of SFRs that fulfil one or more objectives for the TOE for the POI-COMPREHENSIVE configuration:

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

266 The main SFRs of these packages are mapped to the CAS requirements they implement, either in the text of the SFR or in application notes, or both: CAS requirements that come directly from PCI POS PED 2.0 are referenced with the “PCI” identifier; otherwise, the identifier “CAS” is used.

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

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

- Subjects are SPD subjects (section 4.3) or SPD users (section 4.2).
- Objects or information are assets (section 4.1).
- Security attributes are assets or subjects properties.
- Roles are SPD users (section 4.2).
- Operations are the operations used in CAS requirements.
- Operations completed in the PP are shown in **bold**. Operations completed in this ST are shown in **bold underline**.

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

Policy	Entity	Name	Value (for security attributes)	Definition
	Attribute	validity (PLAIN_PIN_SK)	boolean	based on expiration time
		purpose (PLAIN_PIN_SK)	encryption (key, PIN, data) or authentication	key usage: encryption or authentication
	Role	Terminal Management System		4.2.2
		Terminal Administrator		4.2.1
	Operation	send		data transfer
ICCardReader Information Flow Control Policy	Subject	IC Card Reader		4.3
	Information	PLAIN_PIN		4.1
		PLAIN_PIN_SK		4.1
	Role	Terminal Management System		4.2.2
		Terminal Administrator		4.2.1
	Operation	receive		data reception
POI Management and Payment Transaction Data Access Control Policy	Subject	POI and its Payment Application Logic		4.3
	Object	Payment Transaction Data		4.1
		POI Management Data		4.1
		POI_SK		4.1
		Cardholder communication interface		display, beeper, printer: any communication interface from the POI or from an external IT entity controlled by the POI communicating to the Cardholder
	Attribute	validity (POI_SK)	boolean	based on expiration time
		purpose (POI_SK)	encryption (key, PIN, data) or authentication	key usage: encryption or authentication
		access right (MAN_DAT, PAY_DAT	boolean	right to access POI Management Data or Payment Transaction Data

Policy	Entity	Name	Value (for security attributes)	Definition
		authenticity (MAN_DAT, PAY_DAT)	boolean	authenticity of POI Management Data or Payment Transaction Data
	Role	Acquirer System		4.2.2
	Operation	send		data transfer
		receive		data reception
		access		interface access
Core Loader Access Control Policy	Subject	Core Loader		4.3
	Object	CORE_SW		4.1
	Operation	download		data or software download
PED Middle Loader Access Control Policy	Subject	PED Middle Loader		4.3
	Object	PED_MIDDLE_SW		4.1
	Operation	download		data transfer
Payment Application Loader Access Control Policy	Subject	Payment Application Loader		4.3
	Object	PAYMENT_APP		4.1
	Operation	download		data transfer
Middle Loader Access Control Policy	Subject	Middle Loader		4.3
	Object	POI_SW		4.1
	Operation	download		data transfer
PED Prompt Control Policy	Subject	POI components		2.3.4
	Object	PED Display		4.3
		PED Keypad		4.3
		Prompts		cf Glossary
		PIN		4.1
		PED_MIDDLE_PK		4.1
		PED_MIDDLE_SK		4.1
	Operation	entry		digits capture on keypad
		display		data display on screen

Policy	Entity	Name	Value (for security attributes)	Definition
	Attribute	usage (PED Display)	PIN display	PED Display usage stands for displaying PIN data
			non-PIN display	PED Display usage stands for displaying non-PIN data
		usage (PED Keypad)	PIN entry	PED Keypad usage stands for entering PIN data
			non-PIN entry	PED Keypad usage stands for entering non-PIN data

Table 9 - Entities definition in Security Function Policies

8.1.1 Definition of SFR packages

8.1.1.1 PIN Entry Package

FDP_IFC.1/PIN_ENTRY Subset information flow control

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

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

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

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

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

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

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

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

- **PCI B15: PIN is only allowed to be entered at the PED keypad assigned to CoreTSF. The entry of any other data must be separate from the PIN entry process avoiding accidental display of PIN at the PED display. If any other data and PIN are entered at the same keypad, the data entry and the PIN entry shall be clearly separate operations.**
- **[No additional control rules]**.

FPT_EMSEC.1/PIN_ENTRY	**TOE Emanation**

Dependencies: No dependencies.

FPT_EMSEC.1.1/PIN_ENTRY The TOE shall not emit

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

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

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

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

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

FIA_UAU.2/PIN_ENTRY User authentication before any action

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

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

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

Application note:

- *Access to sensitive services shall be either via dual control or resulting in the device being unable to use previously existing key data.*
- *PCI B7: Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys or PINs. Entering or existing sensitive services shall not reveal or otherwise affect sensitive information.*

FIA_UID.1/PIN_ENTRY Timing of identification

Dependencies: No dependencies.

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

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

FTA_SSL.3/PIN_ENTRY TSF-initiated termination

Dependencies: No dependencies.

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

Application note:

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

8.1.1.2 ENC_PIN Package

FDP_IFC.1/ENC_PIN Subset information flow control

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

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

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

FDP_IFF.1/ENC_PIN Simple security attributes

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

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

- **subjects: PED, IC Card Reader**
- **information: ENC_PIN, ENC_PIN_SK**
- **status of ENC_PIN: online encrypted, offline encrypted**
- **status of ENC_PIN_SK: validity, purpose [no other ENC_PIN_SK security attributes].**

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

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

- ~~**PCI D4.3: If the PED and the IC Card Reader are integrated in the same tamper-responsive boundary and the Cardholder verification method is determined to be an Enciphered PIN, then the PIN block shall be enciphered using an authenticated encipherment key of the IC Card.**~~
- **PCI B10, CAS B10.a: The PED uses cryptographic means to prevent the use of the PED for exhaustive PIN determination.**

FDP_IFF.1.3/ENC_PIN The TSF shall enforce the **[No additional information flow control SFP rules]**.

FDP_IFF.1.4/ENC_PIN The TSF shall explicitly authorise an information flow based on the following rules: **[No rules]**.

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

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

Application note:

- *Validity and purpose are security attributes which are only implicitly used in the rules.*
- *PCI B10, CAS B10.a: The intended meaning of "prevent" is to stop an attack; examples (not exhaustive) are the use of unique key per transaction, or the use of ISO PIN block format 1 (random included). By contrast, slowing down an attack is considered as a 'deterrent' that does not meet this requirement.*
- *This SFR forces the immediate encipherment of ENC_PIN. The enciphering must be unique to the transaction, e.g. it is not allowed to produce the same enciphered form for a PIN in different transactions to avoid recognition of PIN values. Additionally, ENC_PIN is only allowed to be enciphered with cryptographic keys only used for PIN encipherment and not used for any other purpose. The SFR enforces that any ENC_PIN_SK is different from any other cryptographic key. However accidental choice of the same value is allowed.*

FMT_MSA.3/ENC_PIN Static attribute initialisation

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

FMT_MSA.3.1/ENC_PIN The TSF shall enforce the **ENC_PIN Information Flow Control SFP** to provide **permissive** default values for **ENC_PIN_SK** security attributes and **restrictive** default values for **ENC_PIN** security attributes, used to enforce the SFP.

FMT_MSA.3.2/ENC_PIN The TSF shall allow the **[Terminal Management System]** to specify alternative initial values to override the default values of the **ENC_PIN_SK**'s security attributes when an object or information is created. The TSF shall allow **no role** to specify alternative initial values to override the default values of **ENC_PIN** when an object or information is created.

Application note:

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

FMT_MSA.1/ENC_PIN Management of security attributes

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

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

Application note:

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

FMT_SMR.1/ENC_PIN Security roles

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

FMT_SMR.1.1/ENC_PIN The TSF shall maintain the roles **[<u>Terminal Management System</u>] and Risk Manager**.

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

Application note:

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

FIA_UID.1/ENC_PIN Entry Timing of identification

Dependencies: No dependencies.

FIA_UID.1.1/ENC_PIN The TSF shall allow **[<u>no TSF-mediated actions</u>]** on behalf of the user to be performed before the user is identified.

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

Application note:

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

FDP_RIP.1/ENC_PIN Subset residual information protection

Dependencies: No dependencies.

Refinement:

FDP_RIP.1.1/ENC_PIN The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **ENC_PIN immediately after being encrypted, temporary cryptographic keys [<u>no other objects</u>]**.

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

Application note:

- *PCI B6: Sensitive information shall not be present any longer or used more often than strictly necessary. Online PINs are encrypted within the PED immediately after PIN entry is complete and has been signified as such by the Cardholder. The PED must automatically clear its internal* *buffers when either: The transaction is completed, or the PED has timed-out waiting for the response from the Cardholder or merchant.*

FDP_ITT.1/ENC_PIN Basic internal transfer protection

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

Refinement:

FDP_ITT.1.1/ENC_PIN The TSF shall enforce the **ENC_PIN Information Flow Control SFP** to prevent the **disclosure** of **ENC_PIN and ENC_PIN_SK [no other information]** when they are transmitted between physically-separated parts of the **CoreTSF and when they are processed by the CoreTSF.**

Application note:

- *This SFR requires that ENC_PIN and ENC_PIN_SK shall be protected when they are transmitted between physically-separated parts of the PED.*

FTP_TRP.1/ENC_PIN Trusted path

Dependencies: No dependencies.

Application Note:

- *PCI C1: If the PED can hold multiple PIN encryption keys and if the key to be used to encrypt the PIN can be externally selected, then the PED prohibits unauthorised key replacement and key misuse.*
- *The key to be used to encrypt the PIN can not be externally selected, this requirement is not applicable, and is therefore considered to be satisfied.*

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

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

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

8.1.1.3 PLAIN_PIN Package

FDP_IFC.1/PLAIN_PIN Subset information flow control

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

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

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

FDP_IFF.1/PLAIN_PIN Simple security attributes

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

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

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

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

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

FDP_IFF.1.3/PLAIN_PIN The TSF shall enforce the **[no additional information flow control SFP rules]**.

FDP_IFF.1.4/PLAIN_PIN The TSF shall explicitly authorise an information flow based on the following rules: **[no other rules that explicitly authorise information flows]**.

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

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

Application note:

- *Validity and purpose are security attributes which are only implicitly used in the rules.*
- *This SFR is related to transfer of PLAIN_PIN mandating the implementation of PCI D4.4.*

FDP_RIP.1/PLAIN_PIN Subset residual information protection

Dependencies: No dependencies.

FDP_RIP.1.1/PLAIN_PIN The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects:

- **[Ciphertext PLAIN_PIN immediately after being encrypted],**
- **temporary cryptographic keys,**
- **[no other sensitive objects]**.

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

Application note:

- *PCI B6: Sensitive information shall not be present any longer or used more often than strictly necessary. Online PINs are encrypted within the PED immediately after PIN entry is complete and has been signified as such by the Cardholder. The PED must automatically clear its internal buffers when either: The transaction is completed, or the PED has timed-out waiting for the response from the Cardholder or merchant.*
- *Note that the TOE does not encrypt the PIN if PLAIN_PIN is used, as the PED and card reader are integrated into the same device. Therefore the second bullet “temporary cryptographic keys” is not applicable to this TOE.*

FDP_ITT.1/PLAIN_PIN Basic internal transfer protection

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

FDP_ITT.1.1/PLAIN_PIN
The TSF shall enforce the **PLAIN_PIN Information Flow Control SFP** to prevent the **disclosure** of **[Ciphertext PLAIN_PIN, PLAIN_PIN_SK]** when they are transmitted between physically-separated parts of **PED or to the IC Card Reader.**

FMT_MSA.3/PLAIN_PIN Static attribute initialisation

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

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

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

FMT_MSA.1/PLAIN_PIN Management of security attributes

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

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

FMT_SMR.1/PLAIN_PIN Security roles

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

FMT_SMR.1.1/PLAIN_PIN The TSF shall maintain the roles **[Terminal Management System]**.

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

FIA_UID.1/PLAIN_PIN Entry Timing of identification

Dependencies: No dependencies.

FIA_UID.1.1/PLAIN_PIN The TSF shall allow **[no TSF-mediated actions]** on behalf of the user to be performed before the user is identified.

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

8.1.1.4 IC Card Reader Package

FDP_IFC.1/ICCardReader Subset information flow control

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

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

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

FDP_IFF.1/ICCardReader Simple security attributes

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

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

- **subjects: IC Card Reader**
- **information: PLAIN_PIN~~,~~ PLAIN_PIN_SK**

- **status of PLAIN_PIN_SK: validity, purpose [no other PLAIN_PIN_SK security attributes]**

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

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

FDP_IFF.1.3/ICCardReader The TSF shall enforce the **[no additional information flow control SFP rules]**.

FDP_IFF.1.4/ICCardReader The TSF shall explicitly authorise an information flow based on the following rules: **[no rules that explicitly authorise information flows]**.

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

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

Application note:

- *Ciphertext PLAIN_PIN holds in POI architectures with physically separated PED and IC Card Reader. Cleartext PLAIN_PIN holds in POI architectures with PED and IC Card Reader integrated in the same tamper-responsive boundary.*
- *This SFR is related to transfer of PLAIN_PIN mandating the implementation of PCI D4.2.*

FDP_RIP.1/ICCardReader Subset residual information protection

Dependencies: No dependencies.

FDP_RIP.1.1/ICCardReader The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects:

- **[Ciphertext PLAIN_PIN immediately after being decrypted and sent to the IC Card]**
- **temporary cryptographic keys,**
- **[no other sensitive objects]**.

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

Application note:

- *PCI B6: Sensitive information shall not be present any longer or used more often than strictly necessary. Online PINs are encrypted within the PED immediately after PIN entry is complete and has been signified as such by the Cardholder. The PED must automatically clear its internal buffers when either: The transaction is completed, or the PED has timed-out waiting for the response from the Cardholder or merchant.*

FDP_ITT.1/ICCardReader Basic internal transfer protection

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

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

8.1.1.5 POI_DATA Package

FDP_ACC.1/POI_DATA Subset Access Control

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

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

- **subjects: POI and its Payment Application Logic**
- **objects: Payment Transaction Data, POI Management Data, POI_SK, Cardholder communication interface, [no 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, [none]**
- **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**
- **[no other security attributes]**

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

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

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

- **POI Management Data and Payment Transaction Data shall be accepted if the data are authentic.**
- **POI Management Data and Payment Transaction Data are allowed to be accessed if Payment Application has access right to the data.**
- **[no other rules].**

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

- **POI Management Data and Payment Transaction Data shall not be accepted if the data are not authentic.**
- **The POI does not send POI_SK in cleartext to any external IT entity.**
- **[no other rules].**

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

Application note:

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

FDP_UIT.1/MAN_DAT Data exchange integrity

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

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

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

Application note:

- *CAS G1.3: POI Management Data must be provided to the POI in an authentic way and must be protected against unauthorized change.*

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

FDP_UIT.1/PAY_DAT Data exchange integrity

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

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

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

Application note:

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

FDP_UCT.1/POI_DATA Basic data exchange confidentiality

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

FDP_UCT.1.1/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:

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

FIA_API.1/POI_DATA Authentication Proof of Identity

Dependencies: No dependencies

FIA_API.1.1/POI_DATA The TSF shall provide a [**unique key**] to prove the identity of the **POI.**

Application note:

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

FDP_RIP.1/POI_DATA Subset residual information protection

Dependencies: No dependencies.

FDP_RIP.1.1/POI_DATA The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **temporary cryptographic keys, [no other objects]**.
Deallocation may occur upon completion of the transaction or if the PED has timed-out waiting from the Cardholder or merchant.

Application note:

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

FTP_ITC.1/POI_DATA Inter-TSF trusted channel

Dependencies: No dependencies.

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

FTP_ITC.1.2/POI_DATA The TSF shall permit **Acquirer System** to initiate communication via the trusted channel.

FTP_ITC.1.3/POI_DATA The TSF shall initiate communication via the trusted channel for **transmitting and receiving Payment Transaction Data and POI_SK in a manner protected from unauthorized disclosure, [transmitting and receiving Payment Transaction Data and POI_SK in a manner protected from unauthorized modification]**.

Application note:

- *Contribution to CAS G1.1 and CAS G4.*

8.1.1.6 CoreTSF Package

FPT_TST.1/CoreTSF TSF testing

Dependencies: No dependencies.

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

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

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

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

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

Application note:

- *"TSF executable code" stands for CoreTSF software within the PED.*
- *PCI B1: The PED performs a self-test, which includes integrity and authenticity tests as addressed in B4, upon start up and at least once per day to check firmware; security mechanisms for signs of tampering; and whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fails in a secure manner.*

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**
- **[no other types of failure]**.

Application note:

- *The "secure state" does not provide access to any PIN value, PIN encryption key or any other CoreTSF secret data.*
- *PCI B1: The PED performs a self-test, which includes integrity and authenticity tests as addressed in PCI B4, upon start up and at least once per day to check firmware; security mechanisms for signs of tampering; and whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fails in a secure manner.*
- *PCI B2: The PED's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device*

mode and supplying wrong parameters or data which could result in the PED outputting the clear text PIN or other sensitive information.

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, [none]**
- **operation: download**.

Application note:

- *The "cryptographic keys" stand for PIN encryption keys (e.g. ENC_PIN_SK) or for any other key. The operations are any management operation on CoreTSF software and data.*

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

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

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

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

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

- **The Core Loader downloads only authentic and integer objects coming from the Terminal Management System.**
- **Downloading is an atomic operation. Either it succeeds or the TSF rollbacks to the previous state and all downloaded data is cleared or if the rollback is not possible all CoreTSF secret data are erased.**

- **PIN encryption keys are stored in the Security Module of PED or encrypted**.
- **[no other importation control rules]**.

Application note:

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

8.1.1.7 PEDMiddleTSF Package

FPT_TST.1/PEDMiddleTSF TSF testing

Dependencies: No dependencies.

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

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

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

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

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

Application note:

- *"TSF executable code" stands for PEDMiddleTSF software within the PED and the IC Card Reader.*
- *PCI B1: The PED performs a self-test, which includes integrity and authenticity tests as addressed in PCI B4, upon start up and at least once per day to check firmware; security mechanisms for signs of tampering; and whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fails in a secure manner.*

FPT_FLS.1/PEDMiddleTSF Failure with preservation of secure state

Dependencies: No dependencies.

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

- **failure of PEDMiddleTSF self-test**
- **logical anomalies of PEDMiddleTSF**
- **[<u>no other types of failure</u>]**.

Application note:

- *The "secure state" does not provide access to any PIN value, PIN encryption key or any other PEDMiddleTSF secret data.*
- *PCI B1: The PED performs a self-test, which includes integrity and authenticity tests as addressed in PCI B4, upon start up and at least once per day to check firmware; security mechanisms for signs of tampering; and whether the PED is in a compromised state. In the event of a failure, the PED and its functionality fails in a secure manner.*
- *PCI B2: The PED's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the PED outputting the clear text PIN or other sensitive information.*

FDP_ACC.1/PEDMiddleTSFLoader Subset access control

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

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

- **subject: PED Middle Loader**
- **objects: PED_MIDDLE_SW, [<u>none</u>]**
- **operation: download**.

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

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

FDP_ACC.1/PEDMiddleTSFLoader
FMT_MSA.3 Static attribute initialisation not satisfied but justified: there are no security attributes to be managed for downloading objects. Terminal Management System decides to update/download them or not.

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

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

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

- **The PED Middle Loader downloads only authentic and integer objects coming from the Terminal Management System.**
- **Downloading is an atomic operation. Either it succeeds or the TSF rollbacks to the previous state and all downloaded data is cleared or if the rollback is not possible all PED-MiddleTSF secret data are erased**.
- **[no additional importation control rules]**

Application note:

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

8.1.1.8 MiddleTSF Package

FDP_ACC.1/ApplicationLoader Subset access control

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

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

- **subject: Payment Application Loader**

- **objects: PAYMENT_APP, [none]**
- **operation: download**.

Application note:

- *The "cryptographic keys" stand for POI encryption keys (POI_SK).*

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

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

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

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

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

- **The Payment Application Loader downloads only authentic and integer objects coming from the Terminal Management System.**
- **Payment application downloading is an atomic operation. Either it succeeds or the TSF rollbacks to the previous state and all downloaded** code and **data is cleared or if the rollback is not possible all MiddleTSF secret data are erased**.
- **[no additional importation control rules]**

Application note:

*In the following CAS rule, the phrase “POI software” is interpreted as **payment application software***

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

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, [none]**
- **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.*

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

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

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

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

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

- **The Middle Loader downloads only authentic and integer objects the Terminal Management System.**
- **Downloading is an atomic operation. Either it succeeds or the TSF rollbacks to the previous state and all downloaded data is cleared or if the rollback is not possible all MiddleTSF secret data are erased**.
- **[no additional importation control rules]**

Application note:

- *CAS G3.1: POI software must be provided to the POI in an authentic way and must be protected against unauthorized change.*
- *CAS G3.2: If the POI implements software updates, a PAL security component cryptographically authenticates the software integrity and if the authenticity is not confirmed, the software update is rejected or all secret cryptographic keys are erased.*

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**
- **[no other types of failures in MiddleTSF]**.

Application note:

- *The "secure state" does not provide access to any encryption key or any other MiddleTSF secret data.*
- *CAS G7: The functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in a breach of the security requirements.*

8.1.1.9 PED Prompt Control Package

FDP_ACC.1/PEDPromptControl Subset access control

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

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

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

Application note:

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

FDP_ACF.1/PEDPromptControl Security attribute based access control

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

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

- **subjects: POI components**
- **status of PED display usage: PIN display, non-PIN display**
- **status of PED Keypad usage: PIN entry, non-PIN entry**
- **[no other security attributes]**

FDP_ACF.1.2/PEDPromptControl The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **If the PED keypad can be used to enter non-PIN data, then prompts demanding for PIN entry at the PED display shall never lead to a PIN disclosure (e.g. by processing the entered PIN data in clear in unprotected areas). The authenticity and proper use of the prompts shall be ensured and modification of the prompts or improper use of the prompts shall be prevented**.

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

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

- *PCI A8.3 For active display devices, cryptographically based controls are utilized to control the PED display and the PED usage such that it is infeasible for an entity not possessing the unlocking mechanism to alter the display and to allow the output of unencrypted PIN data from the PED. The controls provide for unique accountability and utilize key sizes appropriate for the algorithm(s) in question. Key management techniques and other control mechanisms are defined and include appropriate application of the principles of dual control and split knowledge.*

8.1.1.10 Cryptography Package

FCS_RND.1 Quality metric for random numbers

Dependencies: No dependencies.

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

Application note:

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

FCS_COP.1 Cryptographic operation

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

FCS_COP.1(1) Cryptographic operation (TDES)

FCS_COP.1.1(1) The TSF shall perform **PIN encipherment/decipherment, encipherment/decipherment of cryptographic keys, encipherment/decipherment of DUKPT key values, encipherment/decipherment of user data and message authentication** in accordance with a specified cryptographic algorithm **[TDES]** and cryptographic key sizes **[112 bit]** that meet the following: **ISO 9564, NIST SP 800-67 and ANSI X9.24**.

FCS_COP.1(2) Cryptographic operation (HMAC)

FCS_COP.1.1(2) The TSF shall perform **firmware integrity checking** in accordance with a specified cryptographic algorithm **[HMAC-SHA256]** and cryptographic key sizes **[256 bit]** that meet the following: **FIPS 198**.

FCS_COP.1(3) Cryptographic operation (RSA)

FCS_COP.1.1(3) The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **[RSA]** and cryptographic key sizes **[2048 bit]** that meet the following: **PKCS#1 v2.1**.

FCS_COP.1(4) Cryptographic operation (SHA)

FCS_COP.1.1(4) The TSF shall perform **cryptographic hashing** in accordance with a specified cryptographic algorithm **[SHA-256]** and cryptographic key sizes **[N/A]** that meet the following: **FIPS 180-4**.

Application note:

- *Contribution to PCI B10, CAS B10.a, PCI B12, PCI D4.1, PCI D4.2 and PCI D4.4.*

FDP_ITC.2 Import of user data with security attributes

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

FDP_ITC.2.1 The TSF shall enforce the **[ENC_PIN information control SFP and POI Management and Payment Transaction Data Information Flow Control SFP]** when importing user data, controlled under the SFP, from outside of the TOE.

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

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

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

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

Application note:

- *Contribution to PCI B11, CAS G6.*

FTP_ITC.1 Inter-TSF trusted channel

Dependencies: No dependencies.

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

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **importing cryptographic keys, [no other functions]**.

Application note:

- *Contribution to PCI B11, CAS G6.*

FPT_TDC.1 Inter-TSF basic TSF data consistency

Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **cryptographic keys, [no other TSF data types]** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use **ISO 11568 and/or ANSI X9.24 and ANSI TR-31 [no interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

Application note:

- *Contribution to PCI B11, CAS G6.*

8.1.1.11 Physical Protection Package

FPT_PHP.3/CoreTSF Resistance to physical attack

Dependencies: No dependencies.

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

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

- **[no additional physical tampering scenarios]**

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

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

- PCI A1.1: The PED uses tamper detection and response mechanisms which cause the PED to become immediately inoperable and results in the automatic and immediate erasure of any secret information which may be stored in the PED (PIN, secret cryptographic keys, administration passwords, etc.).
- PCI A3: The PED makes inaccessible any PIN value, secret or private keys or other PED secret information when operational or environmental conditions occurs that are not within the specified PED operating range (e.g. temperature or operating voltage outside the state operating range).

Application note:

- *The CoreTSF shall contain at least the PIN keypad and the PIN encryption module of the PED.*

FPT_EMSEC.1/CoreTSF TOE Emanation

Dependencies: No dependencies.

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

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

Application note:

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

FPT_PHP.3/ICCardReader Resistance to physical attack

Dependencies: No dependencies.

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

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

- **[no 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:

- *Apply to the PED components that belong to the PEDMiddleTSF.*

FPT_PHP.3/MSR Resistance to physical attack

Dependencies: No dependencies.

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

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

8.1.2 Security Functional Requirements and TSF parts

269 The table below shows the SFR packages and the TSF part the requirements are associated with.

SFR Package	TSF part(s)
PIN Entry	CoreTSF
ENC_PIN	CoreTSF Keys CoreTSF
PLAIN_PIN	Core TSF Keys Core TSF
IC Card Reader	Core TSF Keys PEDMiddleTSF
POI_DATA	MiddleTSF
CoreTSF	CoreTSF

PEDMiddleTSF	PEDMiddleTSF
MiddleTSF	MiddleTSF
PED Prompt Control	PEDMiddleTSF
Cryptography	CoreTSF
	PEDMiddleTSF
	Middle TSF
Physical Protection	
FPT_PHP.3/CoreTSF	CoreTSF Keys CoreTSF
FPT_EMSEC.1/CoreTSF	CoreTSF Keys
FPT_PHP.3/ICCardReader	PEDMiddleTSF
FPT_PHP.3/MSR	MSRTSF

Table 10 - SFR packages and TSF parts

8.1.3 Security Functional Requirements dependencies rationale

270 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.

271 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 of [POI PP] are either fulfilled or their non-fulfilment is justified.

8.2 SECURITY ASSURANCE REQUIREMENTS

272 The assurance package applicable to the TOE is EAL POI as defined in [POI PP].

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

274 Table 11 lists the Security Assurance Requirements included in EAL POI.

275 “STANDARD” means that the CC requirement applies as is,

276 “REFINED” means that the CC requirement has been refined in this PP to meet POI specificities and CAS requirements,

277 “EXTENDED” means that the requirement does not belong to CC Part3,

278 A greyed cell means that the requirement does not apply to the corresponding TSF part.

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

280 The “STANDARD” requirements are defined in CC Part 3.

281 The “REFINED” and the “EXTENDED” requirements are defined in [POI PP].

Security Assurance Requirements		
EAL2	ADV_ARC.1	REFINED
	ADV_FSP.2	STANDARD
	ADV_TDS.1	STANDARD
	AGD_OPE.1	REFINED
	AGD_PRE.1	STANDARD
	ALC_CMC.2	REFINED
	ALC_CMS.2	REFINED
	ALC_DEL.1	REFINED
	ATE_COV.1	STANDARD
	ATE_FUN.1	STANDARD
	ATE_IND.2	STANDARD
	AVA_VAN.2	
	ALC_DVS.2	REFINED
Extended Requirements	AVA_POI.1/MSR	POI-Basic attack potential
	AVA_POI.2/PEDMiddleTSF	POI-Low attack potential
	AVA_POI.2/MiddleTSF	POI-Low attack potential

	AVA_POI.3/CoreTSF	POI-Moderate attack potential
	AVA_POI.4/CoreTSFKeys	POI-High attack potential

Table 11 - Definition of EAL POI

9 RATIONALE OBJECTIVES/SFR

282 The following table provides an overview of the coverage of security objectives by security functional requirements and constitutes evidence for sufficiency and necessity of the selected SFRs.

	O.PINEntry	O.EncPIN	O.CipherPPIN	O.ClearPPIN	O.CoreSWHW	O.PEDMiddleSWHW	O.ICCardReader	O.PaymentTransaction	O.POISW	O.PaymentApplicationDownload	O.POIApplicationSeparation	O.PromptControl	O.MSR
PIN Entry Package													
FDP_IFC.1/PIN_ENTRY	X												
FDP_ITC.1/PIN_ENTRY	X												
FPT_EMSEC.1/PIN_ENTRY	X												
FIA_UAU.2/PIN_ENTRY	X	X	X	X	X	X	X						
FIA_UID.1/PIN_ENTRY	X	X	X	X	X	X	X						
FTA_SSL.3/PIN_ENTRY	X												
ENC_PIN Package													
FDP_IFC.1/ENC_PIN		X											
FDP_IFF.1/ENC_PIN		X											
FMT_MSA.3/ENC_PIN		X											
FMT_MSA.1/ENC_PIN		X											
FMT_SMR.1/ENC_PIN		X											
FIA_UID.1/ENC_PIN		X											
FDP_RIP.1/ENC_PIN		X											
FDP_ITT.1/ENC_PIN		X											
~~FTP_TRP.1/ENC_PIN~~													
PLAIN_PIN Package													
FDP_IFC.1/PLAIN_PIN			X	X									
FDP_IFF.1/PLAIN_PIN			X	X									
FDP_RIP.1/PLAIN_PIN			X	X									
FDP_ITT.1/PLAIN_PIN			X	X									
FMT_MSA.3/PLAIN_PIN			X				X						
FMT_MSA.1/PLAIN_PIN			X				X						

	O.PINEntry	O.EncPIN	O.CipherPPIN	O.ClearPPIN	O.CoreSWHW	O.PEDMiddleSWHW	O.ICCardReader	O.PaymentTransaction	O.POISW	O.PaymentApplicationDownload	O.POIApplicationSeparation	O.PromptControl	O.MSR
FMT_SMR.1/PLAIN_PIN			X				X						
FIA_UID.1/PLAIN_PIN			X				X						
IC Card Reader Package													
FDP_IFC.1/ICCardReader							X						
FDP_IFF.1/ICCardReader							X						
FDP_RIP.1/ICCardReader							X						
FDP_ITT.1/ICCardReader							X						
POI_DATA Package													
FDP_ACC.1/POI_DATA								X			X		
FDP_ACF.1/POI_DATA								X			X		
FDP_ITT.1/POI_DATA								X					
FDP_UIT.1/MAN_DAT								X					
FDP_UIT.1/PAY_DAT								X					
FDP_UCT.1/POI_DATA								X					
FDP_RIP.1/POI_DATA								X			X		
FTP_ITC.1/POI_DATA								X					
FIA_API.1/POI_DATA								X					
CoreTSF Package													
FPT_TST.1/CoreTSF					X								
FPT_FLS.1/CoreTSF					X								
FDP_ACC.1/CoreTSFLoader					X								
FDP_ITC.1/CoreTSFLoader					X								
PEDMiddleTSF Package													
FPT_TST.1/PEDMiddleTSF						X							
FPT_FLS.1/PEDMiddleTSF						X							
FDP_ACC.1/PEDMiddleTSFLoader						X							
FDP_ITC.1/PEDMiddleTSFLoader						X							
MiddleTSF Package													
FDP_ACC.1/MiddleTSFLoader									X				
FDP_ITC.1/MiddleTSFLoader									X				
FPT_FLS.1/MiddleTSF									X				
FDP_ACC.1/ApplicationLoader										X			
FDP_ITC.1/ApplicationLoader										X			
PED Prompt Control Package													

	O.PINEntry	O.EncPIN	O.CipherPPIN	O.ClearPPIN	O.CoreSWHW	O.PEDMiddleSWHW	O.ICCardReader	O.PaymentTransaction	O.POISW	O.PaymentApplicationDownload	O.POIApplicationSeparation	O.PromptControl	O.MSR
FDP_ACC.1/PEDPromptControl												X	
FDP_ACF.1/PEDPromptControl												X	
Cryptography Package													
FCS_RND.1		X	X										
FCS_COP.1(1 TDES)		X	X				X	X	X	X			
FCS_COP.1(4 HMAC)					X	X			X				
FCS_COP.1(5 RSA)		X	X										
FCS_COP.1(6 SHA)					X	X			X				
FDP_ITC.2		X	X				X						
FTP_ITC.1		X	X				X						
FPT_TDC.1		X	X				X						
Physical Protection Package													
FPT_PHP.3/CoreTSF	X	X	X	X	X		X						
FPT_EMSEC.1/CoreTSF		X	X				X						
FPT_PHP.3/ICCardReader							X						
FPT_PHP.3/MSR													X

Table 12 - Objectives coverage by SFRs

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

O.PINEntry

284 Rationale:

- With FPT_EMSEC.1/PIN_ENTRY the PED only emits indistinguishable audible tones, if any (PCI A5); the PED does not emit sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring (PCI A6); not emit the entered PIN digits at the display (PCI B5)
- With FPT_PHP.3/CoreTSF the PED resists physical manipulation and manipulation of the CoreTSF hardware to protect the confidentiality of any PIN (PCI A1.1) including changing environmental conditions (PCI A3).

- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).
- According to FDP_IFC.1/PIN_ENTRY and FDP_ITC.1/PIN_ENTRY PIN Entry is only allowed to be entered at the PED keypad assigned to CoreTSF (PCI B15).
- According to FTA_SSL.3/PIN_ENTRY limits on the number of actions that can be performed and a time limit shall be imposed, after which the PED is forced to return to its normal mode (PCI B8).

O.EncPIN

285 Rationale:

- With FPT_PHP.3/CoreTSF the PED resists physical manipulation and manipulation of the CoreTSF hardware to protect the confidentiality of any ENC_PIN and ENC_PIN_SK (PCI A1.1, PCI A7) including changing environmental conditions (PCI A3).
- FPT_EMSEC.1/CoreTSF protects ENC_PIN_SK against emanation (PCI A7).
- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).
- Due to FDP_IFC.1/ENC_PIN and FDP_IFF.1/ENC_PIN the PED enciphers ENC_PIN with the appropriate dedicated online or offline encryption key immediately after ENC_PIN entry is complete and has been signified as such by the Cardholder (PCI B6, CAS B6.a).
- The PED sends the ENC_PIN in encrypted form to the IC Card Reader (offline) or to the Acquirer (online). In case of offline encryption FDP_IFC.1/ENC_PIN and FDP_IFF.1/ENC_PIN mandate encryption of the PIN (PCI D4.1, PCI D4.3).
- According to FDP_IFC.1/ENC_PIN and FDP_IFF.1/ENC_PIN the PED uses cryptographic means to prevent the use of the PED for exhaustive PIN determination (PCI B10, CAS B10.a, PCI D4.1, PCI D4.3).
- According to FDP_IFC.1/ENC_PIN and FDP_IFF.1/ENC_PIN it is not possible to encrypt or decrypt any arbitrary data using any PIN related key and PIN related keys have different values (PCI B13). Additionally, output of cleartext cryptographic keys or moving from one component of higher security to a component of less security is prevented (PCI B14).
- FDP_ITT.1/ENC_PIN prevents the disclosure of ENC_PIN and ENC_PIN_SK when they are transmitted between physically-separated parts of the PED or to the IC Card Reader
- FDP_RIP.1/ENC_PIN prevents unwanted knowledge of secret data upon the de-allocation of the resources from sensitive objects. Especially ENC_PIN is deleted immediately after being enciphered (PCI B6).
- According to FCS_RND.1 mechanisms are provided to generate random numbers that meet a defined quality metric for cryptographic means (PCI B9).

- According to FCS_COP.1(1 TDES) and FCS_COP.1(3 RSA)), PIN encipherment is performed following ISO 9564. FCS_COP.1(1 TDES) provides protection for stored key values. (PCI B10, CAS B10a, PCI B12, PCI D4.1, PCI D4.2, PCI D4.4).
- According to FDP_ITC.2 also the import of cryptographic keys is according to ISO 11568 and/or ANSI X9.24 and ANSI TR-31. Therefore state-of-the-art cryptography for cryptographic means is provided (PCI B11). The cryptographic key import is supported by FTP_ITC.1 and FPT_TDC.1.
- With FMT_MSA.3/ENC_PIN, FMT_MSA.1/ENC_PIN, FMT_SMR.1/ENC_PIN and FIA_UID.1/ENC_PIN security attributes are managed and roles are assigned.

O.CipherPPIN

286 Rationale:

- With FPT_PHP.3/CoreTSF the PED resists physical manipulation and manipulation of the CoreTSF hardware to protect the confidentiality of Ciphertext PLAIN_PIN and PLAIN_PIN_SK (PCI A1.1, PCI A7) including changing environmental conditions (PCI A3).
- FPT_EMSEC.1/CoreTSF protects PLAIN_PIN_SK against emanation (PCI A7).
- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).
- Due to FDP_IFC.1/PLAIN_PIN and FDP_IFF.1/PLAIN_PIN the PED enciphers Ciphertext PLAIN_PIN if PED and IC Card Reader are not integrated into the same tamper-responsive boundary (PCI D4.2).
- FDP_ITT.1/PLAIN_PIN prevents the disclosure of Ciphertext PLAIN_PIN and PLAIN_PIN_SK when they are transmitted between physically-separated parts of the PED or to the IC Card Reader.
- FDP_RIP.1/PLAIN_PIN prevents unwanted knowledge of secret data upon the de-allocation of the resources from sensitive objects. Especially PLAIN_PIN is deleted immediately after being enciphered (PCI B6).
- According to FCS_RND.1 mechanisms are provided to generate random numbers that meet a defined quality metric for cryptographic means (PCI B9).
- According to FCS_COP.1(1 TDES) and (FCS_COP.1(3 RSA) PIN encipherment is performed following ISO 9564. FCS_COP.1(1 TDES) provides protection for stored key values. (PCI B10, CAS B10a, PCI B12, PCI D4.1, PCI D4.2, PCI D4.4).
- According to FDP_ITC.2 also the import of cryptographic keys is according to ISO 11568 and/or ANSI X9.24 and ANSI TR-31. Therefore state-of-the-art cryptography for cryptographic means is provided (PCI B11). The cryptographic key import is supported by FTP_ITC.1 and FPT_TDC.1.
- With FMT_MSA.1/PLAIN_PIN, FMT_MSA.3/PLAIN_PIN, FMT_SMR.1/PLAIN_PIN and FIA_UID.1/PLAIN_PIN security roles are managed and assigned.

O.ClearPPIN

287 Rationale:

- With FPT_PHP.3/CoreTSF the PED resists physical manipulation and manipulation of the CoreTSF hardware to protect the confidentiality of Plaintext PLAIN_PIN and (PCI A1.1) including changing environmental conditions (PCI A3).
- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).
- Due to FDP_IFC.1/PLAIN_PIN and FDP_IFF.1/PLAIN_PIN the PED transmits the PIN block wholly through the tamper-responsive boundary if PED and IC Card Reader are integrated into the same tamper-responsive boundary (PCI D4.4).
- FDP_ITT.1/PLAIN_PIN prevents the disclosure of Cleartext PLAIN_PIN when it is transmitted between physically-separated parts of the PED or to the IC Card Reader.
- FDP_RIP.1/PLAIN_PIN prevents unwanted knowledge of secret data upon the de-allocation of the resources from sensitive objects. Especially PLAIN_PIN is deleted immediately after being sent to the IC Card Reader (PCI B6).

O.CoreSWHW

288 Rationale:

- With FPT_PHP.3/CoreTSF the PED resists physical manipulation and manipulation of the CoreTSF hardware (PCI A1.1) or software, including changing environmental conditions (PCI A3).
- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).
- FPT_TST.1/CoreTSF implements the periodically checking of the authenticity and integrity of CoreTSF by running a suite of tests during initial start-up, periodically during normal operation and at the request of an authorised user (PCI B1).
- FPT_FLS.1/CoreTSF enforces the Core TSF authenticity and integrity by preserving a secure state in case of self-test failure or logical anomalies (PCI B1, PCI B2).
- The protection of the authenticity and integrity of CORE_SW and cryptographic keys upon downloading of new components and updating of existing ones is protected due to FDP_ACC.1.1/CoreTSFLoader, FDP_ITC.1/CoreTSFLoader, FCS_COP.1(2 HMAC) and FCS_COP.1(4 SHA) (PCI B2, PCI B4).

O.PEDMiddleSWHW

289 Rationale:

- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).

- FPT_TST.1/PEDMiddleTSF implements the periodically checking of the authenticity and integrity of PEDMiddleTSF by running a suite of tests during initial start-up, periodically during normal operation and at the request of an authorised user (PCI B1).
- FPT_FLS.1/PEDMiddleTSF enforces the PEDMiddleTSF authenticity and integrity by preserving a secure state in case of self-test failure or logical anomalies (PCI B1, PCI B2).
- The protection of the authenticity and integrity of PED_MIDDLE_SW and cryptographic keys upon downloading of new components and updating of existing ones is protected due to FDP_ACC.1/PEDMiddleTSFLoader, FDP_ITC.1/PEDMiddleTSFLoader, FCS_COP.1(2 HMAC) and FCS_COP.1(4 SHA) (PCI B2, PCI B4).

O.ICCardReader

290 Rationale:

- FPT_PHP.3/CoreTSF and FPT_EMSEC.1/CoreTSF protect secret cryptographic keys processed in the IC Card Reader against disclosure by physical attacks or by emanation (PCI A7).
- FPT_PHP.3/ICCardReader (PCI D1) protect the IC Card Reader against the physical tampering.
- Due to FIA_UAU.2/PIN_ENTRY and FIA_UID.1/PIN_ENTRY Sensitive services entering or existing sensitive services shall not reveal or otherwise affect sensitive information like PINs or cryptographic keys (PCI B7).
- FDP_IFC.1/ICCardReader and FDP_IFF.1/ICCardReader enforce that the IC Card Reader receives the Ciphertext PLAIN_PIN, deciphers it and sends it to the IC Card if PED and IC Card Reader are not integrated into the one tamper-responsive boundary (PCI D4.2). FDP_IFC.1/IC Card Reader and FDP_IFF.1/ICCardReader enforce that the IC Card Reader receives the Cleartext PLAIN_PIN and sends it to the IC Card if PED and IC Card Reader are integrated into one tamper-responsive boundary (PCI D4.4). The IC Card Reader does not send PLAIN_PIN to any other entity than the IC Card. The IC Card Reader does not send PLAIN_PIN_SK (if any) to any entity (PCI B14).
- FDP_RIP.1/ICCardReader prevents unwanted knowledge of secret data upon the de-allocation of the resources from sensitive objects. Especially PLAIN_PIN is deleted immediately after being sent to the IC Card Reader and temporary cryptographic keys (PCI B6).
- FDP_ITT.1/ICCardReader prevents the disclosure of PLAIN_PIN and PLAIN_PIN_SK in the IC Card Reader.
- With FMT_MSA.1/PLAIN_PIN, FMT_MSA.3?PLAIN_PIN, FMT_SMR.1/PLAIN_PIN and FIA_UID.1/PLAIN_PIN security roles are managed and assigned.
- According to FCS_COP.1(1 TDES) and FCS_COP.1(3 RSA), PIN decipherment is performed following ISO 9564 (PCI B10, CAS B10a, PCI B12, PCI D4.1, PCI D4.2, PCI D4.4).
- According to FDP_ITC.2 also the import of cryptographic keys is according to ISO 11568 and/or ANSI X9.24 and ANSI TR-31. Therefore state-of-the-art cryptography for crypto-

graphic means is provided (PCI B11). The cryptographic key import is supported by FTP_ITC.1 and FPT_TDC.1.

O.PaymentTransaction

291 Rationale:

- FDP_ITT.1/POI_DATA protects Payment Transaction Data and POI Management Data when it is transferred between physically separated parts of the POI (CAS G1.2 and CAS G1.3).
- FDP_ITT.1/POI_DATA protects the disclosure of POI_SK when it is transferred between physically separated parts of the POI (CAS G4).
- FDP_UIT.1/MAN_DAT, FCS_COP.1(1 TDES) protects POI Management Data at the external lines of the POI against modification (CAS G1.3).
- FDP_UIT.1/PAY_DAT and FCS_COP.1(1 TDES) provide means to protect Payment Transaction Data at the external lines of the POI against modification (CAS G1.1).
- FDP_UCT.1/POI_DATA, FCS_COP.1(1 TDES) provides means to protect Payment Transaction Data at the external lines of the POI against disclosure (CAS G1.1).
- FIA_API.1/POI_DATA provides means to prove the identity of the POI (CAS G1.1).
- FDP_ACC.1/POI_DATA and FDP_ACF.1/POI_DATA prevents other application to deceive the Cardholder during execution of the payment application (CAS G2.3).
- FTP_ITC.1/POI_DATA provides the communication channel to protect data at the external lines against disclosure.
- FDP_RIP.1/POI_DATA ensures that Middle TSF secret data is no longer accessible once used.

O.POISW

292 Rationale:

- FPT_FLS.1/MiddleTSF enforces the MiddleTSF authenticity and integrity by preserving a secure state in case of logical anomalies (CAS G7).
- The protection of the authenticity and integrity of POI_SW and cryptographic keys upon downloading of new components and updating of existing ones is protected due to SFRs FDP_ACC.1/MiddleTSFLoader, FDP_ITC.1/MiddleTSFLoader, FCS_COP.1(1 TDES), FCS_COP.1(2 HMAC) and FCS_COP.1(4 SHA) (CAS G3.1 and CAS G3.2).

O.PaymentApplicationDownload

293 Rationale:

- The protection of the integrity and authenticity of the payment application code is guaranteed by SFRs FDP_ACC.1/ApplicationLoader, FDP_ITC.1/ApplicationLoader FCS_COP.1(1 TDES), FCS_COP.1(2 HMAC) and FCS_COP.1(4 SHA) (CAS G3.1 and CAS G3.2).

O.POIApplicationSeparation

294 Rationale:

- FDP_ACC.1/POI_DATA and FDP_ACF.1/POI_DATA ensures that no other application has unauthorized access to application data of a payment application (CAS G2.1); that it is not possible for another application to interfere with the execution of the payment application by accessing internal data (CAS G2.2) and that it is not be possible for another application to deceive the Cardholder during execution of the payment application (CAS G2.3).
- FDP_RIP.1/POI_DATA ensures that no residual information remains in resources released by the payment application and payment application temporary cryptographic keys (CAS G2.1 to CAS G2.3).

O.PromptControl

295 Rationale:

- FDP_ACC.1/PEDPromptControl and FDP_ACF.1/PEDPromptControl enforces the protection of PIN prompts and the control of PED display specifying different kinds of implementation (PCI A8.3).

O.MSR

296 Rationale:

- FPT_PHP.3/MSR leads to resistance against additions, substitutions, or modifications that would allow determination or modification of Magnetic Stripe data to the to the Magnetic Stripe read head and associated hardware and software.

10 TOE SUMMARY SPECIFICATION

297 The table below provides information on how each of the SFRs is implemented.

SFR	Implementation
PIN Entry Package	
FDP_IFC.1/PIN_ENTRY	The subjects, information and operations of the PIN Entry Information Flow Control SFP are defined in this requirement. It does not mandate any specific TOE features.
FDP_ITC.1/PIN_ENTRY	The PIN can only be entered using the SKP200 keypad. No data can be entered using the keypad other than the PIN. The PIN digits are not displayed
FPT_EMSEC.1/PIN_ENTRY	There are no audible tones emitted during PIN entry. No data can be detected from electro-magnetic emissions or changes in power consumption Asterisks are used to indicate the entry of digits.
FIA_UAU.2/PIN_ENTRY FIA_UID.1/PIN_ENTRY FTA_SSL.3/PIN_ENTRY	There is only one sensitive service on the device (key and firmware loading). This is conducted at the DPS KIF under two person control. The device has no non-sensitive services at this point in its lifecycle. At this stage in the lifecycle the TOE is not fully configured, and there is no normal mode of operation.
ENC_PIN Package	
FDP_IFC.1/ENC_PIN FDP_IFF.1/ENC_PIN	The subjects, information and operations of the ENC_PIN Information Flow Control SFP are defined in FDP_IFC.1/ENC_PIN. Communication of any PIN block entering into a SKP 200 is encrypted using a KPE session established when the SCR pairs with SKP. This pairing is done by mutual authentication. PIN blocks between the SCR and SKP are encrypted using ISO Format 1 and may be transformed on the SCR if used for offline PIN authentication.
FMT_MSA.3/ENC_PIN	The ENC_PIN_SK is generated specifically for the purpose of protecting the PIN during internal transfer between distributed parts of the TOE, and is explicitly allocated for this purpose. Its validity and purpose are defined by the device, and are not subject to change by any external entity.
FMT_MSA.1/ENC_PIN	The ENC_PIN_SK used to protect the PIN during transmission between the SCR and SKP is internally generated and is not subject to change by an external entity.
FMT_SMR.1/ENC_PIN	The TSF is able to identify the Terminal Management System (Key Loader) by cryptographic means, and thereby to support its role.
FIA_UID.1/ENC_PIN	No actions can be performed (most commonly payment processing) before the user (understood here to be the cardholder) is identified by means of a valid PIN.

SFR	Implementation
FDP_RIP.1/ENC_PIN	The plain PIN is cleared from memory immediately after encryption. All temporary cryptographic keys are erased from memory when no longer required.
FDP_ITT.1/ENC_PIN	The session keys used to protect internal transfers between the SCR and SKP are internally generated by the TOE and established using the method outlined under FDP_ITT.1/POI_DATA below. When the SCR needs to get a PIN, it sends a "Get input string" message. When the SKP receives the "Get PIN" request, it gathers the clear PIN digits, and formats the PIN digits into a ISO 9564 format 1 clear-text PIN block, encrypts the PIN block under current KPE using TDES CBC mode and null IV, then sends back to SCR. SCR decrypts the PIN block and re-encrypts it using the current uplink PIN encryption key.
FTP_TRP.1/ENC_PIN	The key to be used to encrypt the PIN cannot be externally selected, this requirement is not applicable, and is therefore considered to be satisfied.
PLAIN_PIN Package	
FDP_IFC.1/PLAIN_PIN FDP_IFF.1/PLAIN_PIN	The subjects, information and operations of the PLAIN_PIN Information Flow Control SFP are defined in this requirement. FDP_IFC.1/PLAIN_PIN does not mandate any specific TOE features. The PIN is always protected using TDES when transmitted between the SKP and SCR. The SKP does not send the PIN anywhere other than the SCR. There is no mechanism in the SKP that would allow secret keys or PIN to be output other than in encrypted form to the SCR.
FDP_RIP.1/PLAIN_PIN	The plain PIN is cleared from memory immediately after encryption. All temporary cryptographic keys are erased from memory when no longer required.
FDP_ITT.1/PLAIN_PIN	The session keys used to protect internal transfers between the SCR and SKP are internally generated by the TOE and established using the method outlined under FDP_ITT.1/POI_DATA below. When the SCR needs to get a PIN, it sends a "Get input string" message. When the SKP receives the "Get PIN" request, it gathers the clear PIN digits, and formats the PIN digits into a ISO 9564 format 1 clear-text PIN block, encrypts the PIN block under current KPE using TDES CBC mode and null IV, then sends back to SCR. SCR decrypts the PIN block and re-encrypts it using the current uplink PIN encryption key.
FMT_MSA.3/PLAIN_PIN	The PLAIN_PIN_SK is generated specifically for the purpose of protecting the PIN during internal transfer between distributed parts of the TOE, and is explicitly allocated for this purpose. Its validity and purpose are defined by the device, and are not subject to change by any external entity.
FMT_MSA.1/PLAIN_PIN	The PLAIN_PIN_SK used to protect the PIN during transmission between the SCR and SKP is internally generated and is not subject to change by an external entity.

SFR	Implementation
FMT_SMR.1/PLAIN_PIN	The TSF is able to identify the Terminal Management System (Key Loader) by cryptographic means, and thereby to support its role.
FIA_UID.1/PLAIN_PIN	No actions can be performed (most commonly payment processing) before the user (understood here to be the cardholder) is identified by means of a valid PIN.
IC Card Reader Package	
FDP_IFC.1/ICCardReader FDP_IFF.1/ICCardReader	The subjects, information and operations of the IC Card Reader Information Flow Control SFP are defined in this requirement. FDP_IFC.1/ICCardReader does not mandate any specific TOE features. The IC Card Reader receives the Ciphertext PLAIN_PIN, deciphers it and sends it only to the IC Card. There is no method for outputting a cleartext key or PIN from the devices.
FDP_RIP.1/ICCardReader	The plain PIN is cleared from memory immediately after being sent to the card.
FDP_ITT.1/ICCardReader	The PLAIN_PIN is protected during transfer between the SCR and the SKP using TDES. Other than this transfer the PIN does not pass outside the protected security area of the devices.
POI_DATA Package	
FDP_ACC.1/POI_DATA FDP_ACF.1/POI_DATA	The subjects, objects and operations of the POI Management and Payment Transaction Data Access Control SFP are defined in this requirement. FDP_ACC.1/POI_DATA does not mandate any specific TOE features. There is only one application in the TOE, and therefore no requirement for application separation. Integrity and authenticity of management and payment transaction data is ensured through use of TDES encryption and MAC keys under the DUKPT key management scheme. If MAC checks do not succeed or a non-matching key has been used the data will be rejected.
FDP_ITT.1/POI_DATA	The key management for SCR-SKP Inter-communication is designed to provide a way to establish a secured channel between SCR and SKP, and to allow SCR and SKP not to depend on each other, i.e., a SCR can detect the SKP hardware change automatically and work with any SKP without any change. Three RSA key pairs are used for establishing secure channel between SCR and SKP: • SKmfg/PKmfg: DPS key pair used to sign PKcr and PKpp • SKcr/PKcr: SCR key pair for symmetric key exchange • SKpp/PKpp: SKP key pair for symmetric key exchange During the key loading process, the following keys are injected to SCR: • PKmfg: Public key of DPS key • sSKmfg(PKcr): The SCR public key signed by DPS secret key

SFR	Implementation
	- SKcr: Secrete key of SCR The following keys are injected to SKP: - PKmfg: Public key of DPS key - sSKmfg(PKpp): The SKP public key signed by DPS secret key - SKpp: Secrete key of SKP After power on, the SCR sends “Hello” message to SKP periodically. When SKP is connected, SKP sends a response contains it serial number, Key verification code of message encryption key (KME), Key verification code of message authentication key (KMAC), Key verification code of PIN encryption key (KPE) and other information. SCR checks the SKP serial number, KVC of KME , KVC of KMAC and KVC of KPE against the stored values. If they match, the KME, KMAC and KPE (session keys) have already established successfully, both parties can proceed to normal message exchange. If they do not match, a key initialization procedure then takes place. After session keys (KME, KMAC and KPE) are established, they will be expired after 24 hours. The SCR is responsible for starting the key initialization procedure when the session keys are expired, and MUST not send any message to SKP except the “Hello” message and “Key Initialization” message. SKP should also discard its current session keys once the key initialization procedure is in progress, and should not respond to any message from SCR other than the “Hello” message and “Key Initialization” message. Messages other than the “Hello” message and “Key Initialization” message are encrypted under KME using 3DES CBC mode. After encryption, a message authentication block is calculated on the entire message including the message type field. The first 4 bytes of the message authentication block is then appended to the message. The entire message is encoded into STX/ETX/LRC format and eventually sent over serial port.
FDP_UIT.1/MAN_DAT FDP_UIT.1/PAY_DAT	Management and payment transaction data is protected against modification during transmission over external lines using TDES and the DUKPT key management scheme. A separate DUKPT MAC key is used.
FDP_UCT.1/POI_DATA	Management and payment transaction data is protected against disclosure during transmission over external lines using TDES and the DUKPT key management scheme.
FDP_RIP.1/POI_DATA	All temporary cryptographic keys are erased from memory when no longer required.
FTP_ITC.1/POI_DATA	The SCR200 does not have its own communication channel to DPS host. It requires the POS application to provide a channel. When the SCR200 wants to send a message to DPS host, it sends the message to the POS application and the POS application forwards it to DPS host. When a response is received from DPS host by the POS application, the POS application forwards the response to SCR200. The actual message exchanged between SCR200 and DPS host is embedded in the SCR200 serial protocol message. The host interface message is en-

SFR	Implementation
	crypted and MAC'ed using the DUKPT key management scheme. The DUKPT key management is described in ANSI X9.24-1 specification.
FIA_API.1/POI_DATA	The TOE uses a unique per-chip identification which can be used to determine the proper key associated with the device and/or used for logging purposes. SBOOT provides a default challenge key which is associated with all devices that have not had their key changed. However, once the challenge key has been changed then the acquirer must have a mechanism for "remembering" which keys are associated with which ID's. If the correct challenge key for a given device is not provided, then no application code can be loaded into the device. The challenge is comprised of a 64 bit random number that has been encrypted using the device's challenge key. The correct response is formed by doing a triple-DES decrypt operation on the 64 bit challenge. The 128 bit challenge key associated with the device is used. If no challenge key has been entered into the device, then a constant default key is used. The 64 bit response is encoded in hex digits and sent to the device terminated with an end-of-line sequence as described above. If the response is correct, the device responds, otherwise if the response is incorrect the device repeats the process with a new challenge.
CoreTSF Package	
FPT_TST.1/CoreTSF	A firmware self-test will be performed upon each startup of the TOE, and after each subsequent 24 hours. Upon discovery of any anomaly, all sensitive data will be erased. All sensitive services will be disabled except firmware updating. All operations on the keypad, magnetic card and IC card will be disabled.
FPT_FLS.1/CoreTSF	Upon discovery of any anomaly during a self-test, all services will be disabled except firmware updating via the serial interface. All operations on the keypad, magnetic card and IC card will be disabled. Once a successful challenge/response is received on this interface all firmware apart from the boot loader is erased, together with the on-chip user key area. The device is programmed to handle unexpected inputs and buffer overflow attacks. Upon discovery of any anomaly that cannot be handled, all sensitive data will be erased. All sensitive services will be disabled except firmware updating. All operations on the keypad, magnetic card and IC card will be disabled.
FDP_ACC.1/CoreTSFLoader FDP_ITC.1/CoreTSFLoader	The subjects, objects and operations of the Core Loader Access Control SFP are defined in this requirement. FDP_ACC.1/CoreTSFLoader does not mandate any specific TOE features. Initial firmware loading is carried out within a secure facility, following completion of a challenge/response sequence to load the boot loader. The firmware is loaded into RAM, and a CRC check is used to ensure the firmware is loaded correctly before it is copied to EEPROM.

SFR	Implementation
	Field updates rely on the DUKPT mechanism to protect the integrity of the firmware. The host will also verify the firmware signature before transmission to the device. The CRC check is used to ensure the firmware is loaded correctly before it is copied to EEPROM.
PEDMiddleTSF Package	
FPT_TST.1/PEDMiddleTSF	The application needs to be signed after loading. The signing is done by generating HMAC-SHA256 over the application range. The HMAC value is stored in the application header information area inside the SBOOT boot loader. SBOOT uses the signature to verify the integrity and authenticity of the application. The application itself can also use this information for authenticity and integrity test as required by PCI PTS specification. The HMAC key is randomly generated the first time the SBOOT runs. A firmware self-test will be performed upon each startup of the TOE, and after each subsequent 24 hours.
FPT_FLS.1/PEDMiddleTSF	Upon discovery of any anomaly during a self-test, all services will be disabled except firmware updating via the serial interface. All operations on the keypad, magnetic card and IC card will be disabled. Once a successful challenge/response is received on this interface all firmware apart from the boot loader is erased, together with the on-chip user key area. The device is programmed to handle unexpected inputs and buffer overflow attacks. Upon discovery of any anomaly that cannot be handled, all sensitive data will be erased. All sensitive services will be disabled except firmware updating. All operations on the keypad, magnetic card and IC card will be disabled.
FDP_ACC.1/PEDMiddleTSFLoader FDP_ITC.1/PEDMiddleTSFLoader	The subjects, objects and operations of the PED Middle Loader Access Control SFP are defined in this requirement. FDP_ACC.1/PEDMiddleTSFLoader does not mandate any specific TOE features. Initial firmware loading is carried out within a secure facility, following completion of a challenge/response sequence to load the boot loader. The firmware is loaded into RAM, and a CRC check is used to ensure the firmware is loaded correctly before it is copied to EEPROM. Field updates rely on the DUKPT mechanism to protect the integrity of the firmware. The host will also verify the firmware signature before transmission to the device. The CRC check is used to ensure the firmware is loaded correctly before it is copied to EEPROM.
MiddleTSF Package	

SFR	Implementation
FDP_ACC.1/MiddleTSFLoader FDP_ITC.1/MiddleTSFLoader	The subjects, objects and operations of the Middle Loader Access Control SFP are defined in this requirement. FDP_ACC.1/MiddleTSFLoader does not mandate any specific TOE features. Initial firmware loading is carried out within a secure facility, following completion of a challenge/response sequence to load the boot loader. The firmware is loaded into RAM, and a CRC check is used to ensure the firmware is loaded correctly before it is copied to EEPROM. Field updates rely on the DUKPT mechanism to protect the integrity of the firmware. The host will also verify the firmware signature before transmission to the device. The CRC check is used to ensure the firmware is loaded correctly before it is copied to EEPROM.
FPT_FLS.1/MiddleTSF	The device is programmed to handle unexpected inputs and buffer overflow attacks. Upon discovery of any anomaly that cannot be handled, all sensitive data will be erased. All sensitive services will be disabled except firmware updating. All operations on the keypad, magnetic card and IC card will be disabled.
FDP_ACC.1/ApplicationLoader FDP_ITC.1/ApplicationLoader	The subjects, objects and operations of the Payment Application Loader Access Control SFP are defined in this requirement. FDP_ACC.1/ApplicationLoader does not mandate any specific TOE features. Initial firmware loading is carried out within a secure facility, following completion of a challenge/response sequence to load the boot loader. The firmware is loaded into RAM, and a CRC check is used to ensure the firmware is loaded correctly before it is copied to EEPROM. Field updates rely on the DUKPT mechanism to protect the integrity of the firmware. The host will also verify the firmware signature before transmission to the device. The CRC check is used to ensure the firmware is loaded correctly before it is copied to EEPROM.
PED Prompt Control Package	
FDP_ACC.1/PEDPromptControl FDP_ACF.1/PEDPromptControl	The subjects, objects and operations of the PED Prompt Control SFP are defined in FDP_ACC.1/PEDPromptControl. The PED keypad is used only PIN entering PIN data. Cleartext PINs and secret cryptographic keys are never displayed on the SKP screen. The SKP is tamper responsive. Any attempt to access prompt controls will result in erasure of cryptographic keys.
Cryptography Package	
FCS_RND.1	Random numbers are generated using the RNG on the ATMEL AT91SO processor. The hardware RNG has been tested against the *PCI POS PIN Entry Device Derived Test Requirements* version 1.3. The post processing is a DRNG that conforms to the NIST Digital Signature Standard (FIPS Pub 186-

SFR	Implementation
	2).
FCS_COP.1(1 TDES)	See entries within key table in Section 12 for details on uses of TDES. In the SCR200, there are 8 DUKPT key slots. During the key injection stage, each key slot is injected with an initial key. For each key slot, 21 future keys are generated from the initial key and stored in the NVM. The initial key is then discarded. As a result, each key slot will have 21 future keys. The current key is one of the 21 future keys, and is rolled after every message exchange. The data encryption key, MAC key and PIN encryption key are derived from the current key and erased after use. The current key can only be rolled forward. Once it is rolled, its content in the one of the 21 future key registers will overwritten by new future key.
FCS_COP.1(2 HMAC)	HMAC SHA-256 is used for integrity checks of the device firmware and boot loader.
FCS_COP.1(3 RSA)	RSA is used for key exchange during establishment of communications between the SCR200 and SKP200.
FCS_COP.1(4 SHA)	Hashes are generated in support of integrity checking using SHA-256.
FDP_ITC.2	All messages containing PIN data, and user and management data, are encrypted using DUKPT (ANSI X9.24 and ANSI TR-31).
FTP_ITC.1	Initial keys are loaded in clear text. The key injection process is done in DPS secure loading room by authorized person using a dedicate machine connected to the Thales HSM module array. The keys are verified by SCR200 during the key loading process using the key verification code. If the KVC does not match, the key loading process is aborted. The SCR200 does not have its own communication channel to DPS host. It requires the POS application to provide a channel. When SCR200 wants to send a message to DPS host, it sends the message to the POS application and the POS application forwards it to DPS host. When a response is received from DPS host by the POS application, the POS application forwards the response to SCR200.
FPT_TDC.1	The actual message exchanged between SCR200 and DPS host is embedded in the SCR200 serial protocol message. The host interface message is encrypted and MAC'ed using the DUKPT key management scheme. The DUKPT key management scheme is described in the ANSI X9.24-1 specification.
Physical Protection Package	
FPT_PHP.3/CoreTSF	A removal detection sensor between the front bezel and the card reader of the SCR200 is continually monitored by MSP430 grid monitoring software running on the low power MSP430F233 microcontroller. When the bezel is removed it triggers an unlatched state that prevents transactions from being processed. This unlatched state is propagated to the DPS HOST.

SFR	Implementation
	The SKP contains four removal sensors, located on the underside of the metal fascia. The switches consist of two metal contacts in a folded flex circuit, which are sandwiched together between the PIN pad fascia and containing cabinet. Two switches are located on the left edge of the device, and another two on the right edge of the device. The removal detection system works in the same way as the SCR200. The devices have a specified operating temperature range of between -30C to 75C. Temperatures outside of the range -40C to 85C will trigger a security tamper event. All secure areas of the devices are protected against penetration by tamper detection meshes that are monitored by firmware.
FPT_EMSEC.1/CoreTSF	In order to safeguard against differential power analysis attacks the TOE seeks to randomise the power signature by adding or stealing clock cycles during processing.
FPT_PHP.3/ICCardReader	The secure area of SCR200 is protected by tamper meshes, and monitored by the firmware running in a MSP430 micro. Once mesh monitoring is enabled, the MSP430 micro checks the integrity of the meshes continuously, running off an internal coin cell battery. If a tamper condition is detected, the MSP430 micro will notify the AT91SO51 secure MCU by asserting the secure MCU’s tamper pin. The secure MCU will in turn erase all secure information inside it. The MSP430 is also configured to monitor the unscrew switch. The unscrew switch is used to detect the situation when the SCR200 or SKP200 is removed from its mount. The unscrew situation will not erase the secure information inside the secure MCU, but will cause the device to stop accepting user input until the device is remounted and re-enabled through software. On the initial power-up on of the MSP430, the grid and unscrew check are not enabled. The secure MCU AT91SO51 needs to enable the check. Once the check is enabled, the MSP430 performs the check until it detects a tamper condition or an unscrew condition.
FPT_PHP.3/MSR	The magnetic card read head is a separate part of SCR200 which is not controlled by the AT91SO51 MCU. It is encapsulated in a separate secure area and communicates with the main AT91SO51 MCU via UART interface. It consists of a STM32 (F101T8) MCU, a Magtek triple track delta ASIC and a Magtek 2-track head. The STM32 MCU decodes the raw magnetic card data, encrypts the result with preloaded 3DES and sends the encrypted result to AT91SO51. Currently the STM32 MCU is protected by a mesh but it is not notified when a tamper situation is detected. Thus, it will not erase the keys after tampering. However, from the entire system point of view, it is not unsecure, because the entire device will stop functioning due to the fact that all keys in AT91SO51 have been erased.

11 GLOSSARY

298 For the Common Criteria oriented sections it is assumed the reader is familiar with the language used. If not, please refer to [CC1]. Those definitions are not repeated here.

Term	Definition
Acquirer	A body acquiring card related transactions from Merchants or other parties, and transmitting these transactions to an Issuer. Usually, an Acquirer is represented by a bank or a financial institution. It can also be any body entitled to acquire card related transactions. It is responsible for the Merchant's compliance to the security rules.
Acquirer Processor	An entity acting for or on behalf of an Acquirer in acquiring card related transactions.
Application	The objective of a POI is to execute applications issued by different application providers (e.g. bank, health, loyalty, government, etc.). A POI may support a multi application environment where several applications are executed simultaneously. The applications use functions provided by the core software of the POI. Applications may consist of data and software. The applications are excluded from the TOE.
Attended	In an attended POI, the Merchant typically provides a member of staff who processes purchased items and provides assistance to the Cardholder in using different payment applications.
(Bank) card	A card issued by a bank (or by a similar institution) to perform payment transactions.
Cardholder	A person using a (bank) card linked to an account to perform payment transactions.
Card payment	Any payment transaction originating from a (bank) card.
CHV	Cardholder Verification Devices (CHV): devices for Cardholder authentication, e.g. a PIN Entry Device (PED). A PED contains a keypad, a display, a Security Module (SM) for PIN encryption and may also include an IC Card Reader. POI as per this Protection Profile includes at least one PED thus allowing Cardholder PIN authentication.
Device	In contrast to distributed architectures an enclosed IT product with external communication interfaces.
DUKPT	Derived Unique Key per Transaction: a key management scheme in which a unique key is used for each transaction that is derived from a fixed key.
Enciphered	Enciphered information.
Enciphered PIN	PIN that is only allowed to leave the POI in enciphered form when it has to be verified by the IC Card or by the Issuer.
Encrypted	Synonym for enciphered.

Term	Definition
Firmware	All the software present in the POI at the delivery point.
Hardware Security Module (HSM)	Hardware Security Module. A physically and logically protected hardware device that provides a secure set of cryptographic services.
Issuer	A body issuing cards to Cardholders and authentic transactions initiated by this cards. Usually, an Issuer is represented by a bank or a financial institution. It can also be any body entitled to issue cards.
Magnetic Stripe	Stripe containing magnetically encoded information.
Merchant	A retailer, or any other person, company, or corporation that agrees to accept (bank) cards in the framework of a contract with an Acquirer. In this Protection Profile the Merchant is also responsible for the TOE in order to protect the TOE against manipulations of the enclosure.
Multi application	A POI that may be used for more than one (card) application.
Offline	Deferred processing without direct communication.
Online	Direct communication between devices with electronic capability (e.g. POI to hosts).
Payment system	Any system processing payment transaction data.
Payment transaction	The act between a Cardholder and a Merchant or Acquirer that results in the exchange of goods or services against payment. For the purpose of this PP also the process performing all steps of a card payment related to the POI.
Payment transaction data	Data that are involved in a payment transaction. Examples for payment transaction data are the amount, the currency, the date of the payment transaction, cryptogram data, the data used to perform Dynamic Data Authentication and stored in the POI, any data which is transferred between Issuer and IC card as card script processing and card management, the Transaction Counter and any other payment transaction data processed by the POI. The Acquirer, the Cardholder and the attended performs operations on the payment transaction data.
PCI	Payment Card Industry. Issuer of security requirements. Jointly formed by MasterCard, Visa and other card payment schemes.
PIN Entry Device (PED)	A device for secure PIN entry and processing. The PED typically consists of a keypad for PIN entry, laid out in a prescribed format, a display for user interaction, a Security Module consisting of a processor and memory performing cryptographic operations with cryptographic keys on PINs and firmware. A PED has a clearly defined physical and logical boundary, and a tamper resistant or tamper evident shell. The PED is a CHV.
Plaintext PIN	PIN which is allowed to be sent to the IC card as plaintext in order to be

Term	Definition
	verified by the IC card.
POI	A POI is an electronic transaction acceptance product. A POI consists of hardware and software and is hosted in an acceptance equipment to enable a Cardholder to perform a card transaction. Thereby the POI may be attended or unattended. POI transactions are IC card based payment transactions as well as any other payment transactions e.g. based on Magnetic Stripe or any non-payment transactions like health, loyalty or government. The TOE is at minimum a POI excluding applications.
POI component	Any physical or logical device involved in a card payment at a POI (e.g. beeper, Card Reader, display, printer, PED).
POI management data	All PIN related or security related data used to manage and administer the POI. Examples for POI Management data are the risk management data, POI Unique Identifier or the Merchant Identifier. The Terminal Administrator performs operations on POI management data.
PIN related data	All items related to the processing of a PIN, i.e. the PIN itself, the PIN encryption keys, etc.
Private key	That key of an entity’s asymmetric key pair that should only be used by that entity. In the case of a digital signature scheme, the private key defines the signature function.
Public key	That key of an entity’s asymmetric key pair that can be made public. In the case of a digital signature scheme, the public key defines the verification function.
Public key certificate	The public key and identity of an entity together with some other information, rendered unforgeable by signing with the private key of the certification authority that issued that certificate.
Processor	Any organisation or system processing card payment transactions. An entity operating a data or host processing centre as agent of an Acquirer, Issuer or Merchant to process card payment transactions.
Prompts	Prompts are the text shown on the PED display.
Receipt	A hard copy document recording a payment transaction that took place at the POI, with a description that usually includes: date, Merchant name/location, primary account number, amount, and reference number.
Reconciliation	An exchange of messages between two institutions (Acquirer, Issuer or their agents) to reach agreement on financial totals.
Retailer protocol	Protocol used between the sale system (electronic cash register, vending unit, service station infrastructure,..) and the POI.
Reversal	Cancellation of a previous transaction. There might be manual as well as automatic reversals.
Secret (crypto-	A cryptographic key used with symmetric cryptographic techniques and

Term	Definition
graphic) key	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 software	All software that are involved in the secure handling of IC card payment transaction, i.e. PIN encryption, parameter and software authentication, card and transaction data protection, etc.
Security Module (SM)	Any (physical or logical) device that manages secret cryptographic keys and cryptographic functions and performs cryptographic operations using keys that have a justified level of protection (e.g. a Hardware Security Modules (HSM) or an external Security Application Module (SAM) for a purse application (PSAM)).
Security related data	All items, other than PIN related data, related to security protection of the payment transaction. E.g. critical parameters, cryptographic keys, etc.
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.

12 KEY TABLE

299 The table in this section identifies all cryptographic keys that can be used by the TOE. And shows their relationship to the key types identified in [POI PP].

Key name	Purpose/ Usage	PP	Algorithm	Size(Bits)	Generated By	Form Factor Loaded to Device In	Number of Available Key Slots (Registers)	Unique per device/ acquirer/ vendor-specific/ other (describe)
Key Encryption Key	Encryption of all other keys used in SCR	ENC_PIN_SK, PLAIN_PIN_SK	TDES	112	Device	Randomly generated by device at first initialization	1	Device
DUKPT Initial Key	Used to derive unique-per-transaction keys for SCR-DPS host message exchange	ENC_PIN_SK	TDES	112	Acquirer	Plain-text from key injection device	8	Device
DUKPT Message Encryption Key	Encryption of messages exchanged between SCR and DPS host	POI_SK	TDES	112	Device	Derived from DUKPT initial key	1	Device
DUKPT Message Authentication Key	MAC generation of messages exchanges between SCR and DPS host	POI_SK	TDES	112	Device	Derived from DUKPT initial key	1	Device
DUKPT PIN Encryption Key	Encryption of PIN block exchanged between SCR and DPS host foronline PIN	ENC_PIN_SK	TDES	112	Device	Derived from DUKPT initial key	1	Device
SCR-SCP Key Exchange Root Public Key	Derive session keys for SCR-SKP secure channel	POI_PK	RSA	2048	Manufacturer	Plain-text from key injection device	1	Vendor specific
SCR Public Key for SCR-SKP Key Exchange	Derive session keys for SCR-SKP secure channel	POI_SK	RSA	2048	Manufacturer	Certificate signed with manufacturer’s	1	Device

Key name	Purpose/ Usage	PP	Algorithm	Size(Bits)	Generated By	Form Factor Loaded to Device In	Number of Available Key Slots (Registers)	Unique per device/ acquirer/ vendor-specific/ other (describe)
						private key		
SCR Private Key for SCR-SKP Key Exchange	Derive session keys for SCR-SKP secure channel	POI_PK	RSA	2048	Manufacturer	Plain-text from key injection device	1	Device
SCR-SKP Message Encryption Key	Encryption of messages exchanged between SCR and SKP	POI_SK	TDES	112	Device	Generated by device randomly	1	Device
SCR-SKP Message Authentication Key	MAC generation for messages exchanged between SCR and SKP	POI_SK	TDES	112	Device	Generated by device randomly	1	Device
SCR-SKP PIN Encryption Key	Encryption of PIN block exchanged between SCR and SKP	ENC_PIN_SK, PLAIN_PIN_SK	TDES	112	Device	Generated by device randomly	1	Device
Local Track Data Encryption Key	Encryption of data sent by magnetic head	ENC_PIN_SK, PLAIN_PIN_SK	TDES	112	Device	Generated by device randomly	1	Device
SBOOT HMAC Key	Integrity verification of firmware	ENC_PIN_SK	HMAC	256	Device	Generated by device randomly	1	Device
SBOOT Challenge Key	Authentication for secure boot loader access	ENC_PIN_SK	TDES	112	Device	Plain-text from key injection device	1	Device