JIL Terminal Evaluation Methodology Subgroup

JTEMS

Software Payment Point of Interaction Protection Profile

Date: 23th October 2023

Version: 1.0

FOR TRIAL USE

Table of Contents

History of Changes

Version	Date	Approved	Changes	Application Note (Reason for change, effects of change on work units, if applicable which comments of certification body were observed)
0.1	01.09.2022	-	Initial version	-
0.2	05.10.2022	-	Editorial updates	-
0.3	06.10.2022	-	Editorial updates	-
0.4	21.11.2022	-	Review updates	-
0.5	31.01.2023	-	Editorial updates	-
0.6	21.03.2023	-	Review Updates	-
0.7	23.03.2023	-	Update CC:2022 R1	-
0.8	13.04.2023	-	Editorial updates	-
0.9	24.07.2023	-	Editorial and review updates	-
0.91	17.08.2023	-	Editorial and review updates	
0.92	23.08.2023	-	Editorial updates	
0.93	28.08.2023	-	Review Updates	
1.0	23.10.2023	-	First Release	Version for trial use

1 Protection Profile Introduction

[ECSG B4] explains the specific security approach for POI that will use the Protection Profile defined in this document for evaluation (see chapter 2.2.4 of [ECSG B4]).

In traditional merchant payment scenarios, a PIN entry device (PED) that has been independently tested and validated against detailed security requirements is used to enable contact or contactless transactions to be performed. Traditional PEDs rely on hardware security as the primary protection mechanism to ensure the security of PIN data entered into the device and to protect other assets like cryptographic credentials.

For these scenarios [PP POI] shall be used for security evaluations.

This Software Payment POI Protection Profile follows a new method for card based payment transactions to be accepted by merchants. This new payment acceptance method utilizes Commercial Off-the-Shelf, (COTS) devices. With this paradigm shift the assurance of the POI moves away from the reliance on physical security to be based upon an initial security evaluation and the continuous monitoring by a back-end system. The COTS device is assumed not to contribute to the security.

Card Payment Schemes have introduced different acceptance methods to be implemented with COTS devices. This Software Payment POI Protection Profile provides for a modular approach to enable security evaluations for all of these acceptance methods.

1.1 Protection Profile Identification

1.1.1 Identification of the Software Payment POI Protection Profile

Title	**Software Payment Point of Interaction Protection Profile – base PP**
Identification	CC-SPPOI-BASE
Authors	Hirotaka Yoshida, AIST Leo Kool, SGS Brightsight Sven-Martin Hühne, SRC GmbH
Version	1.0
Publication date	23.10.2023
Sponsors	Joint Interpretation Library Terminal Evaluation Subgroup (JTEMS)
CC Version	CC:2022 Revision 1

1.2 Protection Profile Presentation

This Protection Profile (PP) was developed by the Joint Interpretation Library Terminal Evaluation Subgroup (JTEMS) to be used for the Common Criteria (CC) evaluation of Software Payment Point of Interaction.

European Card Stakeholder Group (ECSG) security requirements [ECSG B4], chap. 3.7.2 have been translated into CC functional and assurance security requirements.

The products in the scope of this Protection Profile are payment terminals using Commercial Off-the-Shelf, (COTS) devices, (hybrid) Card based online and offline, contact and contactless transaction capabilities. Products are focused on a Base Module which handles the interaction between the other modules and the payment application. A backend server component and a backend-Attestation and Risk Management Component provides for a continuous monitoring replacing the traditional hardware based security, that is not provided by the COTS device. Other functionalities than payment, which might be processed by the same device, e.g. fleet card processing, are out of scope of this PP.

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

Privacy shielding does not belong to the Target of Evaluation (TOE).

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

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

For the protection of the defined assets a modular approach built out of defined “Software POI Components” has been chosen. These Software POI Components defining the scope of the TOE of products to be evaluated and certified using this PP are

- the base component
- the Secure Card Reader Component
- the external Attestation/ Risk Management component
- the Backend/Terminal-Server component
- the Secure Element/TEE component.

These Software POI Components can be optionally configured to build a specific software architecture of a Software POI product. By using SEs or TEE components within these configurations security can be enhanced.

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

This Protection Profile is conformant to EAL 2 (AVA_VAN.2 Basic attack potential) augmented with ADV_IMP.1, ALC_DVS.2, and ALC_FLR.1.

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

This Protection Profile defined in this document require “strict” conformance. Security Targets or Protection Profiles conformant to this Protection Profile can extend the perimeter of the chosen Software POI configuration with additional functionalities if necessary.

The evaluation of this Protection Profile has been performed by XYZ. The PP has been certified by XYZ.

The ST author first has to choose one of the described TOE configurations. The suggested TOE configurations in chapter 2.4 are reflecting solutions used in the field, e.g. PCI CPOC, PCI SPOC, PCI MPOC and GBIC AppPOS, but are not limited to these.

1.3 References

[CC1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version CC:2022 Revision 1, November 2022, CCMB-2022-11-001, also referred by [CC_P1]

[CC2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version CC:2022 Revision 1, November 2022, CCMB-2022-11-002, also referred by [CC_P2]

[CC3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version CC:2022 Revision 1, November 2022, CCMB-2022-11-003, also referred by [CC_P3]

[CC4] Common Criteria, Part 4: Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, Version CC:2022 Revision 1, November 2022, CCMB-2022-11-004, also referred by [CC_P4]

[CC5] Common Criteria, Part 5: Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, Version CC:2022 Revision 1, November 2022, CCMB-2022-11-005, also referred by [CC_P5]

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version CC:2022 Revision 1, November 2022, CCMB-2022-11-006

[ECSG B4] SEPA CARDS STANDARDISATION (SCS) "VOLUME", Book 4, "Security", Version 10

[PP POI] Point of Interaction Protection Profile, 6th March 2015, Version: 4.0

[PP TEE] https://www.commoncriteriaportal.org/files/ppfiles/anssi-profil_PP-2014_01.pdf

[PP SE] https://www.commoncriteriaportal.org/files/ppfiles/CCN-CC-PP-5-2021.pdf

https://www.commoncriteriaportal.org/files/ppfiles/pp0109b_pdf.pdf

2 TOE Overview

The TOE is a product of type Software Point of Interaction (POI) realised as software TOE. The TOE can be enhanced by hardware components, which are also defined in this PP. In this case, security functions implemented in software are transferred to the associated hardware component. This allows for various existing infrastructures used in other schemes to be represented by Common Criteria requirements. The TOE provides protection for card based transactions, provides payment transaction data management, and external communication facilities for interaction with the Acquirer.

2.1 TOE Type

The TOE is a product of the type Software Point of Interaction (POI) running on a COTS device, which can be extended by optional hardware.

2.2 TOE Security Features

The TOE Security Features are:

- Confidentiality of PIN.
- Confidentiality, authenticity and integrity of PIN processing keys and transaction data.
- Authenticity and integrity of PIN processing software.
- Authenticity and integrity of POI management.
- Confidentiality, authenticity and integrity of POI data protection keys.
- Protection of IC Card Reader against tampering (if applicable, the SCR is certified separately).

2.3 Software POI Components

Figure 1 shows a generic overview of a Software POI Architecture.

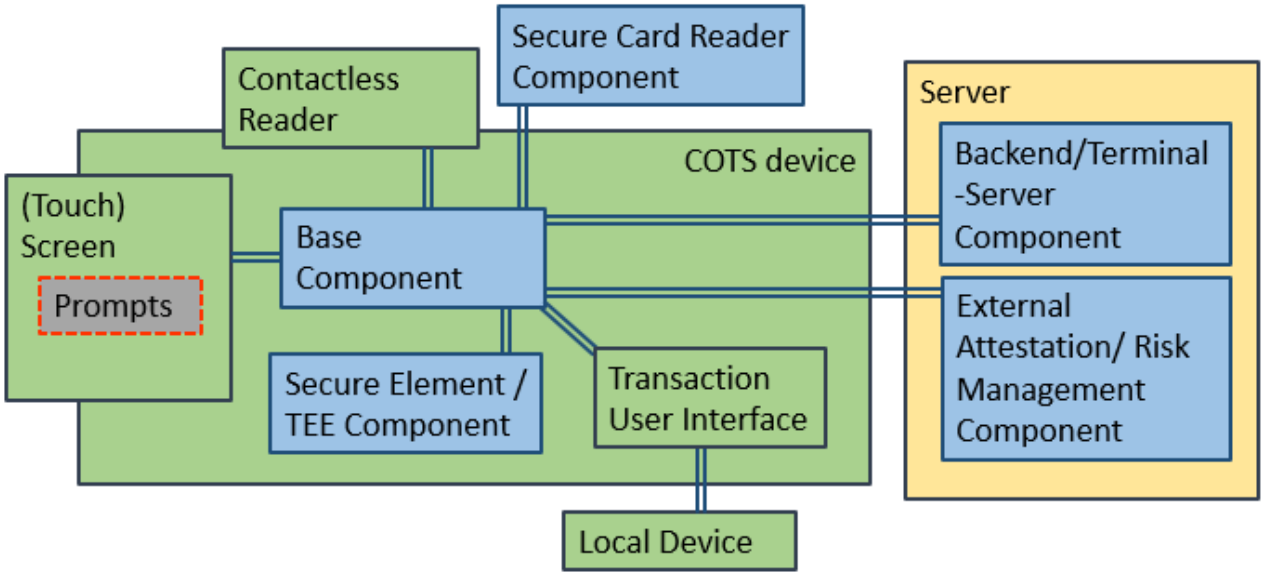

Figure 1: Generic POI architecture, TOE components are shown in blue

A payment is initiated by the Local Device (e.g. cash register) or directly on the Transaction User Interface and invokes payment functionality to the Base Module via the Transaction User Interface, which then processes the Payment.

The Software POI architecture consists of different modules:

- **Base component:** The base module is typically an application running on a COTS device. This module handles the interaction between the other modules and the payment application. The software is capable of processing payments for online and/or offline payment transactions, with and/or without PIN entry of the cardholder. The module can hold payment data, such as PIN data confidential and authentic. The base module enforces secure channels to other modules and the payment application.

- **Secure Card Reader component:** Secure Card Readers are devices that provide interfaces to cards. These Secure Card Readers may support different types of cards, (e.g. IC contact cards, IC contactless cards, and hybrid cards) allowing IC based payment transactions. The Secure Card Reader must have its own tamper-responsive enclosure and must be separated from the device running the Software POI. The secure card reader is an already certified component, but has to be certified in combination with the Software POI by fulfilling the requirements of ADV_COMP. The Secure Card Reader used is certified on basis of [PP POI].

- **External Attestation/ Risk Management component:** Attestation shall be done by a software application running on an external server. The attestation software is intended to provide software-based tamper detection and response for the Software POI, while

handling PINs as a CVM. The system service provider of the Software POI implements a risk management system. The following parameters are to be included in the assessment: Cases of incidents, anomalies in the communication behaviour of the Software POI, feedback from self-tests, monitoring the Software POI integrity.

- **Backend/Terminal-Server component:** The backend or terminal server completely takes over the transaction flow and attestation functionality of the software POI. An optionally connected and certified HSM may reduce the evaluation effort needed to achieve this.

- **Secure Element/TEE component:** Some devices offer the option to provide a secure element or trusted execution environment. For a pure software POI, security can be extended by allowing sensitive key material to be stored or processed in these environments. It is also possible to include the processing of PIN data here. The Secure Element/TEE component is an already certified component, but has to be certified in combination with the Software POI by fulfilling the requirements of ADV_COMP. The SE/TEE used is certified on basis of [PP SE] or [PP TEE].

- **Non-TOE components (external entities)**

    - Local device: cash register, printer, etc
    - Touch screen
    - Transaction user interface
    - Contactless reader
    - Payment Application

2.4 TOE Configuration

The defined components can be used to map commercially requested architectures. Each of these architectures is based on the base module. With the extension to the individual components, the security level aimed at for each architecture is mapped, as defined by payment schemes. In this context, the SFRs of the modules replace or extend those defined for the base module.

The following architectures are examples, for any configuration the base component must be used:

Examples for POI configurations	TOE components	nonTOE components
Software POI	Base Component	Touch screen Contactless reader Transaction user interface Local Device
Software POI with Secure Element/TEE	Base Component Secure Element/TEE Component	Touch screen Contactless reader Transaction user interface Local Device
Software POI with contactless reader only and attestation	Base Component External Attestation / Risk management Component	Contactless reader Touch screen Transaction user interface Local Device
Software POI with secure card reader and attestation	Base Component Secure Card Reader External Attestation / Risk management Component	Touch screen Transaction user interface Local Device
Software POI with Attestation/Backend	Base Component External Attestation / Risk management Component Backend/Terminal-Server component Secure Element/TEE component	Contactless reader Touch screen Transaction user interface Local Device

Table 1: POI configuration

2.5 TOE Life Cycle

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

- Developer Phase:
  - Development and testing
- Operational Phase (User Phase):
  - Installation
  - Initial Cryptographic Key Loading (Remote)
  - Acquirer Initialisation
  - Use by Merchant and Customer
  - End of life

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

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

Application Note:

The ST author shall update this life cycle according to the product specificities, e.g. integrated or distributed device, application loading during Initial Software Loading and/or during use, configuration of applications with device specific parameters, etc.

2.5.1 Developer phase

2.5.1.1 Development and testing

POI development consists of producing

- POI base component software
- Additional software for that POI (when applicable, e.g.)
- Initial Key Loading processes have to be initialised and if necessary upload of personalisation cryptographic keys

During software development, the POI is tested. Pre-personalisation is the manufacturing step when a POI receives the cryptographic keys to be used in the subsequent personalisation phase.

2.5.2 Operational Phase

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

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

2.5.2.1 Installation

It is up to the ST author to specify the actual installation steps for the evaluated POI. These steps may include:

- physical installation of the different POI components, e.g. card reader,

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

After delivery of the Software components representing the POI is installed on the device automatically.

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

The TOE is delivered as pure software without any cryptographic keys.

2.5.2.2 Initial Cryptographic Key Loading

Initial Cryptographic Keys are automatically loaded into the POI remotely once the base component is installed and the administrator account is activated. It is the task of the ST author to describe which cryptographic keys are loaded during the initialisation of Cryptographic keys and how these keys are protected in the operational environment.

Application note:

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

2.5.2.3 Acquirer Initialisation

Acquirer initialisation takes place with each Acquirer with whom the Merchant operating the Software POI has a contract.

Further cryptographic keys may be loaded during the Acquirer Initialisation to personalise the Software POI. This may also be done during initial cryptographic key loading process.

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

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

It is up to the ST author to specify the actual initialisation steps for the evaluated POI.

2.5.2.4 Use by merchant and customer

During the User phase at the Merchant premises, the POI performs card based payment transactions. POI administration is performed by an Acquirer either through a connection to a Terminal Management System or directly at the POI.

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

2.5.2.5 End of life

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

3 Conformance Claims

3.1 Conformance claim to CC

This Protection Profile is conformant to the Common Criteria version CC:2022 Revision 1:

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

3.2 Conformance claim to a package

This Protection Profile is conformant to EAL 2 (AVA_VAN.2 Basic attack potential) augmented with ADV_IMP, ALC_DVS.2 and ALC_FLR.1.

The dependencies of security assurance components of the package EAL2 are solved within the package [CCP3]. The component ALC_DVS.2 has no dependencies on other components. ADV_IMP.1 has the following dependencies: ADV_TDS.3 Basic modular design and ALC_TAT.1 Well-defined development tools. Following the dependency for ADV_TDS.3 ADV_FSP.4 is mandatory.

3.3 Conformance claim of the PP

This PP does not claim conformance to any other PP.

Conformance claim rationale:

This protection profile does not claim any conformance with other protection profiles. Therefore, no conformance claim rationale is provided here

3.4 Conformance claim to the PP

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

4 Security problem definition

4.1 Assets

The following table summarises the assets of the TOE and their sensitivity: Confidentiality (C), Authenticity (A) and Integrity (I). Some assets only need to be separately identified if a particular configuration is used.

Asset	Definition	Sensitivity
PIN	Personal Identification number	I, A, C
PAN	Primary Account Number	I, A, C
Transaction Data	Transaction Data is the data involved in the transaction between the cardholder and a merchant or an acquirer. This includes 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 attendant performs operations on the payment transaction data.	I, A
Attestation data	Information collected from the COTS device for the purposes of validating it is in an uncompromised and secure state, suitable for performing secure transactions.	I, A, C
Cryptographic Material	Cryptographic keys and related parameters (static and ephemeral) used to protect other sensitive assets such as account data, PINs, etc., as well as parameters used to establish secure channels and sign attestation data.	I, A, C Note: Public cryptographic keys do not need Confidentiality protection.
TOE Software	The compiled software which comprises the TOE	I, A

Table 2 Assets sensitivity

4.2 Users

Users are humans or IT entities external to the TOE that interact with the TOE. Human users are defined in Table 3 and external entities in Table 4.

Human users	Activities
Cardholder	The Cardholder interacts with the POI via man-machine interfaces: he reads payment transaction data displayed on the POI, inserts her/his IC card, authenticates herself/himself with her/his PIN, confirms the payment transaction and takes the receipt.
Attendant	The payment application in the POI or in a connected device may initiate a payment transaction at the request of the Attendant. The Attendant interacts with the TOE via a man-machine interface. The payment transaction is either initiated by the Attendant or by a Local Device. The Merchant himself can be the attendant.
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.
Terminal Administrator	The Terminal Administrator maintains the TOE directly by local operations or remotely through a Terminal Management System.

Table 3 Human users

External entities	Activities
Acquirer System	The Acquirer System is the entity that exchanges payment transaction data with the POI. Used by the Application Provider, the Acquirer or the Acquirer Processor.
External server architecture	The external server architecture is the entity used to administrate (installation, maintenance) a set of TOEs: software and parameter download and application activation / deactivation. Used by a Terminal Administrator. The external server architecture namely compromises of the terminal server/backend/external attestation/risk management component.
IC card	The Cardholder's IC Card is an entity interacting with the POI during a payment transaction. The Cardholder's IC Card acts on behalf of the Card Issuer.
Local Device	A payment transaction may be initiated at the request of the Attendant or a Local Device. Examples of Local Devices are the Electronic Cash Register (ECR), a Vending Machine Controller or a Pump Controller for Petrol Outdoor configurations. The connections to these external devices may be implemented by various means such as a private or public network.
Payment Application	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.

Table 4 External entities

4.3 Threats

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.PromptControl (Manipulation of Prompt Control)

Fraudsters gain unauthorised access to the Prompt Control 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).

T.Transaction (Transaction with stolen Cardholder identity)

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

Fraudsters use good IC cards and manipulate the TOE software to generate payment transactions that debit the wrong account in payment transaction data.

T.FundsAmount (Funds transfer other than correct amount)

A fraudulent cardholder issues valid payment instructions generating valid payment transaction data but later manipulates payment transaction data before they are collected.

T.BadDebt (Account overdraft, bad debt)

A fraudulent cardholder manipulates the TOE, thus preventing the Acquirer to collect funds and making the Merchant think the transaction performed correctly whereas no funds have been collected.

T.SecureCommunicationLines

An attacker manipulates or misuses the TOE services underlying the protection of external communication lines (i.e. trusted path) in order to disclose or modify the sent or received transaction data on external communication lines.

T.IllegalCodeInstall

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

T.SecureUpdate

An attacker manipulates the authenticity of a received update cannot downgrade the TOE's firmware to a previous version.

T.Cardholder.Denial

A fraudulent cardholder performs an authorized transaction at a Software POI and denies this authorization retrospectively by claiming that a fraudulent merchant has deceived him/her about the amount or result of the transaction by manipulating the Software POI.

T.Merchant.Manipulation.Progress

The cardholder will be deceived by a fraudulent merchant about the progress of a transaction. The cardholder believes that a transaction has been cancelled (e.g. due to communication errors with the background system) or he/she has explicitly cancelled the transaction himself/herself, but actually a transaction has been executed by logical attacks and the amount is (re)paid.

T.ExternalAttacker.FakeTerminal

An external attacker analyses an instance of the Software POI associated with its merchant identity and extracts the Software POI keys. With these keys, he can implement a fake app, which enables him to perform transactions in benefit of his terminal. The fake app runs as malware on the merchant's mobile device and performs transactions in order to get the cardholder PINs or directly transfer the shown amount to the merchant.

T.ExternalAttacker.DenialOfService

An attacker performs activities that are suitable to compromise the availability of the system.

A denial-of-service attack can be directed against a single instance of the Software POI app, against a group of instances of the app that have the same version or are connected to the same terminal HSM, for example, or against the entire system.

T.InternalAttacker

An internal attacker gains direct or indirect access to sensitive data or the processes of the Software POI app, the terminal HSM/Backend, the security functions generating the activation code and the Software POI keys during their development, startup/operation/execution or enables fraudulent transactions. In this case, the internal fraudster must work with either an unauthorized merchant or a fraudulent cardholder who has a financial advantage from the fraud.

T.Merchant.PINtheft

The cardholder is requested to enter his/her PIN on a mobile device by a fraudulent merchant. The mobile device has been enhanced with a corresponding display function for this purpose, which does not necessarily have to be part of the Software POI. The goal is to steal later the IC Card and to perform a transaction based on payment transaction data with the captured PIN and the stolen IC Card.

T.ExternalAttacker.Terminal-HSM/Backend/External Attestation/Risk Management component (if used)

The attacker gains direct or indirect access to the secret data or procedures of the terminal HSM/Backend in order to perform or prepare fraudulent transactions.

T.SE/TEE (If applicable)

The attacker gains direct or indirect access to the secret data or procedures of the SE or TEE.

4.4 Organisational Security Policies

OSP.WellFormedPayApp (Well-formed Payment Applications)

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

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

OSP.POISurvey

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

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

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

OSP.KeyManagement

Cryptographic keys have to be securely managed. Especially the generation and installation of cryptographic keys and certificates have to be done in a manner that private or secret cryptographic keys are protected against disclosure and that all cryptographic keys are protected

against modification when they are processed outside the POI. Furthermore there are procedures that support and maintain the unique identification of the TOE based on unique cryptographic keys for the protection of the online interface.

4.5 Assumptions

A.CONFIG

It is assumed that the TOE's security functions are configured correctly in a manner to ensure that the TOE security policies will be enforced. Especially, the device the TOE is installed is not rooted.

A.CHECK

It is assumed that issuer and acquirer check data/information received regarding to consistency.

A.CARD

It is assumed that issuer card is authentic.

A.ADMIN

The Terminal Administrator as well as the remote administration (External Attestation/ Risk Management component and Backend administrator) are trustworthy and well educated.

5 Security Objectives

5.1 Security Objectives for the TOE

O.PINEntry

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, etc.).

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.PIN

The TOE shall protect the confidentiality of the PIN and PIN related data until it is enciphered.

The TOE shall immediately delete the PIN after having enciphered it.

The TOE shall neither display nor print any PIN in clear.

This objective entails the following derived objectives:

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

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

This objective applies to Online PIN as well as Offline PIN verification.

O.SWHW

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

This objective entails the following derived objectives:

- The TOE shall check the authenticity and integrity of software and cryptographic keys upon downloading of new components and updating of existing ones.
- The TOE shall periodically check the authenticity and integrity of TOE software and if applicable of additional hardware (e.g. secure card reader) before every payment transaction.

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

O.SecureCardReader (if applicable)

The TOE shall be used with Common.SECC according [PP POI] approved Secure Card Readers only to ensure that the TOE resists attempts to penetrate the POI to make any additions, substitutions, or modifications to the Secure Card Reader hardware or software, in order to determine or modify PIN values. The TOE shall perform a secure pairing process and a 24h check of the pairing for integrity.

O.TrustedPath

The TOE shall provide trusted paths for communication via internal and external interfaces.

O.PaymentTransaction

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 payment data from unauthorized modification and disclosure at the external interface to the Acquirer as well as between physically separated parts of the POI.

This objective entails the following derived objectives:

- The TOE shall protect the confidentiality, authenticity, and integrity of the TOE.
- The TOE shall ensure the correct execution of TOE software.
- The TOE 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.
- Any information about the payment transaction shall be displayed, printed or acoustic signalled in an authentic way (controlled by the payment application based on user data) without deceiving either the Cardholder or the attendant.
- The TOE shall provide state-of-the-art cryptography for cryptographic means.
- Upon failure of any authenticity and integrity check or upon incorrect execution, the TOE shall be able to permanently erase any transaction data, hashes, attestation data, user data, account data, and cryptographic keys.

Initially, the base component is 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). This functionality may be provided by an external Backend/Terminal server and/or External attestation /Risk Management Components.

O.POIApplicationSeparation (Application Separation)

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 and any other related data owned by an application are only allowed to be accessed by another application if the other application has the necessary access rights.

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

All prompts are handled by the device and controlled by the base component. 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.SecureUpdate

The TSF verifies the authenticity of a received update. Files will be decrypted only if the received update content was verified to be authentic. Afterwards the update can be installed. The TOE has to ensure that the received update does not downgrade the TOE's firmware to a previous version.

O.Personalisation

Personalisation is controlled and verified by the TOE security functions.

O.AttestationoftheTOE

Hash value is checked periodically at least every 24 hours

O.SE/TEE (If applicable)

A secure channel must exist in between SE/TEE and base component, and the POI shall periodically check the authenticity and integrity of related Hardware/Software.

5.2 Security Objectives for the Operational Environment

OE.ApplicationDownload

The COTS device shall ensure the integrity and authenticity of application download or update.

OE.POISurvey

Procedural measures like inspections and guidance will prevent manipulations of the TOE enclosure. Those responsible for the TOE establish and implement procedures for training and

vetting administrators of the TOE, or training the supervisors. The user of the TOE installed on a COTS device has to follow the procedures to inspect the device and the TOE.

OE.MerchantSurvey

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

OE.KeyManagement

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

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.WellFormedApps

TOE applications implemented on the device will make use of the security mechanisms provided by the device in a sense that the security of the defined assets as specified in this PP cannot be affected.

OE.LocalDevices

The environment of the TOE shall protect the connection between local devices and other TOE components via security organisational measures or by using the cryptographic means provided by the TOE.

OE.UpdateDelivery

Updates are delivered encrypted only and are signed by the manufacturer. The TOE verifies the authenticity of the update before storing the content to the device.

5.3 Rationale between SPD and security objectives

	T.PromptControl	T.Transaction	T.FundsAmount	T.BadDebt	T.SecureCommunicationLines	T.IllegalCodeInstall	T.SecureUpdate	T.Cardholder.Denial	T.Merchant.Manipulation.Progress	T.ExternalAttacker.FakeTerminal	T.ExternalAttacker.DenialOfService	T.InternalAttacker	T.Merchant.PINtheft	T.ExternalAttacker.Terminal-	T.SE/TEE (optional)	OSP.WellFormedPayApp	OSP.MerchantSurvey	OSP.KeyManagement	A.CONFIG	A.CHECK	A.CARD	A.ADMIN
O.PINEntry		X	X										X									
O.PIN		X	X										X									
O.SWHW				X		X					X			X								
O.Secure-CardReader (optional)		X	X		X								X									
O.TrustedPath				X	X																	
O.Pay-mentTransaction		X		X																		
O.POIApplica-tionSeparation						X					X											
O.PromptControl	X			X																		
O.SecureUpdate							X															
O.Personalisa-tion						X			X													
O.Attestation-oftheTOE									X	X	X			X								
O.SE/TEE (optional)															X							
OE.Applica-tionDownload						X				X												

	T.PromptControl	T.Transaction	T.FundsAmount	T.BadDebt	T.SecureCommunicationLines	T.IllegalCodeInstall	T.SecureUpdate	T.Cardholder.Denial	T.Merchant.Manipulation.Progress	T.ExternalAttacker.FakeTerminal	T.ExternalAttacker.DenialOfService	T.InternalAttacker	T.Merchant.PINtheft	T.ExternalAttacker.Terminal-	T.SE/TEE (optional)	OSP.WellFormedPayApp	OSP.MerchantSurvey	OSP.KeyManagement	A.CONFIG	A.CHECK	A.CARD	A.ADMIN
OE.POISurvey				X		X		X		X	X			X					X	X		
OE.Mer-chantSurvey								X	X			X	X				X					
OE.KeyManage-ment																		X				
OE.PinAndCard-Management																				X	X	
OE.Well-FormedApps						X										X						
OE.LocalDevices					X																	X
OE.UpdateDeliv-ery						X	X															

Table 5 SPD coverage by objectives

6 Extended Requirements

This PP does not extend CC Part 2.

7 Security Requirements

7.1 Security Functional Requirements

7.1.1 Base Component

The PP author used the following notations in the following:

- Assignments and selections of the PP author are noted **in bold letters**
- Refinements of the PP author are noted underlined.
- Iterations are denoted by a slash "/" and the iteration indicator is placed after the component identifier.

7.1.1.1 General

7.1.1.1.1 FMT_MSA.1 Management of security attributes Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: access control SFP(s), information flow control SFP(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles].

7.1.1.1.2 FMT_MSA.3 Static attribute initialisation Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

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

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

7.1.1.1.3 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: the authorised identified roles].

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

7.1.1.1.4 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the TSF].

7.1.1.1.5 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

7.1.1.1.6 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes that explicitly authorise information flows].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes that explicitly deny information flows].

7.1.1.1.7 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

7.1.1.1.8 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

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

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

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

7.1.1.1.9 FPT_TST.1 TSF self-testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of the following self-tests **during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-test should occur]**[1] to demonstrate the correct operation of **the TSF**[2]: [assignment: list of self-tests run by the TSF].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of **TSF data**[3].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of **TSF**[4].

7.1.1.1.10 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: list of types of failures in the TSF].

7.1.1.2 Audit

7.1.1.2.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the **detailed**[5] level of audit; and c) **[user authentication, update (verification), transaction flow, prompt control, provisioning, attestation [assignment: other specifically defined auditable events]]**[6].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable

---

[1] [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-test should occur]]
[2] [selection: [assignment: parts of TSF], the TSF]
[3] [selection: [assignment: parts of TSF data], TSF data]
[4] [selection: [assignment: parts of TSF], TSF]
[5] [selection, choose one of: minimum, basic, detailed, not specified]
[6] [assignment: other specifically defined auditable events]

event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information].

7.1.1.2.2 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

7.1.1.3 Cryptography

7.1.1.3.1 FCS_COP.1/ENC_DEC Cryptographic operation

Hierarchical to: No other components.

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] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform **encryption and decryption operations**[7] in accordance with a specified cryptographic algorithm **according to Table 6**[8] and cryptographic key sizes **according to Table 6**[9] that meet the following: **RFC 3447, ANSI X9.62-2005, RFC 2631, FIPS PUB 197**.[10]

7.1.1.3.2 FCS_COP.1/HASH Cryptographic operation

Hierarchical to: No other components.

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] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform **hashing operations**[11] in accordance with a specified cryptographic algorithm **according to Table 6**[12] and cryptographic key sizes **according to**

[7] [assignment: list of cryptographic operations]
[8] [assignment: cryptographic algorithm]
[9] [assignment: cryptographic key sizes]
[10] [assignment: list of standards]
[11] [assignment: list of cryptographic operations]
[12] [assignment: cryptographic algorithm]

Table 6[13] that meet the following: **SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, FIPS PUB 180-4, FIPS 202, NIST SP 800-185**.[14]

Application note: Cryptographic operation shall be implemented by using white-box cryptography and code obfuscation. The white-box instance shall be changed within less than one month.

[13] [assignment: cryptographic key sizes]
[14] [assignment: list of standards]

Crypto-graphic Operation	Cryptographic Algorithm	Ref.	Parameter	Key Size/ Hash Size	Note
encryption and decryption (symmetric)	AES	SOGIS Agreed v1.2, FIPS PUB 197	secret key bit length	128, 192, 256	
Digital Signature, Key Establishment	DH key exchange Algorithm	SOGIS Agreed v1.2,	prime number bit length	3072, 4096, 6144, 8192	
Digital Signature, Key Establishment	DH key exchange algorithm “Legacy”	SOGIS Agreed v1.2,	prime number bit length	2048	valid until the end of 2025
encryption and decryption (asymmetric)	RSA	SOGIS Agreed v1.2,	public key bit length	>= 3000	
encryption and decryption (asymmetric)	RSA “Legacy”	SOGIS Agreed v1.2,	public key bit length	>= 1900	valid until the end of 2025
Digital Signature	ECDSA	SOGIS Agreed v1.2, FIPS PUB 186-4	public key bit length	256, 384, 521	
hashing	SHA-2	SOGIS Agreed v1.2, FIPS PUB 180-4	hash length	256, 384, 512	
hashing	SHA-2 “Legacy”	SOGIS Agreed v1.2, FIPS PUB 180-4	hash length	224	

Crypto-graphic Operation	Cryptographic Algorithm	Ref.	Parameter	Key Size/ Hash Size	Note
hashing	SHA-3	SOGIS Agreed v1.2, FIPS 202	hash length	256, 384, 512	

Table 6 Crypto table

7.1.1.3.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **by overwriting with zeros when the key is to be destroyed, or when a transient copy is no longer used**[15] that meets the following: **no standard**.[16]

Application note: key destruction related to WBC: If no SE is used, the Software POI has to destroy the stored binaries on the device.

7.1.1.4 Random number generation

7.1.1.4.1 FCS_RNG.1 Random number generation

Application note: The ST author may choose one of the following RNG definitions for the TOE in scope.

Hierarchical to: No other components.

Dependencies: No dependencies.

[15] [assignment: cryptographic key destruction method]

[16] [assignment: list of standards]

FCS_RNG.1.1/NTG1 The TSF shall provide a **non-physical true[17]** random number generator that implements:[18]

- **(NTG.1.1) The RNG shall test the external input data provided by a non-physical entropy source in order to estimate the entropy and to detect non-tolerable statistical defects under the condition [assignment: requirements for NPTRNG operation].**

- **(NTG.1.2) The internal state of the RNG shall have at least 100bit[19]. The RNG shall prevent any output of random numbers until the conditions for seeding are fulfilled.**

- **(NTG.1.3) The RNG provides backward secrecy even if the current internal state and the previously used data for reseeding, resp. for seed-update, are known.**

FCS_RNG.1.2/NTG1 The TSF shall provide [selection: bits, octets of bits, numbers [assignment: format of the numbers]] that meet:[20]

- **(NTG.1.4) The RNG generates output for which [assignment: number of strings] strings of bit length 128 are mutually different with probability [assignment: probability].**

- **(NTG.1.5) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A and none[21]. (NTG.1.6) The average Shannon entropy per internal random bit exceeds 0.997.**

Application note: done by source code review and Test Tool results only

FCS_RNG.1.1/DRG3 The TSF shall provide a **deterministic[22]** random number generator that implements:[23]

- **(DRG.3.1) If initialized with a random seed [selection: using a PTRNG of class PTG.2 as random source, using a PTRNG of class PTG.3 as random source, using**

[17] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]
[18] [assignment: a defined quality metric].
[19] [assignment: Min-entropy]
[20] [assignment: list of security capabilities]
[21] [assignment: additional test suites]
[22] [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]
[23] [assignment: list of security capabilities]

an NPTRNG of class NTG.1 and none[24]], the internal state of the RNG shall [selection: have 100bit of entropy[25], have [assignment: work factor], require [assignment: guess work]].

- **(DRG.3.2) The RNG provides forward secrecy.**
- **(DRG.3.3) The RNG provides backward secrecy even if the current internal state is known.**

FCS_RNG.1.2/DRG3 The TSF shall provide [selection: bits, octets of bits, numbers [assignment: format of the numbers]] that meet:[26]

- **(DRG.3.4) The RNG, initialized with a random seed [assignment: requirements for seeding], generates output for which [assignment: number of strings] strings of bit length 128 are mutually different with probability [assignment: probability].**
- **(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A and none[27].**

7.1.1.5 Data Protection (without secure element)

7.1.1.5.1 FPT_ITA.1 Inter-TSF availability within a defined availability metric

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITA.1.1 The TSF shall ensure the availability of [assignment: list of types of TSF data] provided to another trusted IT product within [assignment: a defined availability metric] given the following conditions [assignment: conditions to ensure availability].

7.1.1.5.2 FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to: No other components. Dependencies: No dependencies.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission

[24] [assignment: other requirements for seeding]
[25] [assignment: amount of entropy]
[26] [assignment: a defined quality metric]
[27] [assignment: additional test suites]

7.1.1.5.3 FPT_ITI.2 Inter-TSF detection and correction of modification

Hierarchical to: FPT_ITI.1 Inter-TSF detection of modification Dependencies: No dependencies.

FPT_ITI.2.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [assignment: a defined modification metric].

FPT_ITI.2.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [assignment: action to be taken] if modifications are detected.

FPT_ITI.2.3 The TSF shall provide the capability to correct [assignment: type of modification] of all TSF data transmitted between the TSF and another trusted IT product.

7.1.1.5.4 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components. Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from **modification**[28] when it is transmitted between separate parts of the TOE.

7.1.1.5.5 FPT_SSP.2 Mutual trusted acknowledgement

Hierarchical to: FPT_SSP.1 Simple trusted acknowledgement

Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection

FPT_SSP.2.1 The TSF shall acknowledge, when requested by another part of the TSF, the receipt of an unmodified TSF data transmission.

FPT_SSP.2.2 The TSF shall ensure that the relevant parts of the TSF know the correct status of transmitted data among its different parts, using acknowledgements.

7.1.1.6 User Authentication

7.1.1.6.1 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

[28] [selection: disclosure, modification]

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow **no TSF-mediated actions**[29] on behalf of the user to be performed before the user is identified.

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

7.1.1.6.2 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow **no TSF-mediated actions** on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. [assignment: list of TSF mediated actions]

7.1.1.7 Trusted Path

7.1.1.7.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

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 **the TSF**[30] to initiate communication via the trusted channel.

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

[29] [assignment: list of TSF-mediated actions]
[30] [selection: the TSF, another trusted IT product]

7.1.1.8 Update (verification)

7.1.1.8.1 FDP_ACC.1/UPDATE Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/UPDATE The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

7.1.1.8.2 FDP_ACF.1/UPDATE Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/UPDATE The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

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

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

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

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

7.1.1.8.3 FDP_ETC.2 Export of user data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

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

FDP_ETC.2.2/UPDATE The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/UPDATE The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4/UPDATE The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: additional exportation control rules].

7.1.1.8.4 FDP_ITC.2 Import of user data with security attributes

Hierarchical to: No other components.

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] FPT_TDC.1 Inter-TSF basic TSF data consistency

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

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

FDP_ITC.2.3/UPDATE 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/UPDATE 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/UPDATE The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: additional importation control rules].

7.1.1.8.5 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies

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

7.1.1.9 Transaction flow

7.1.1.9.1 FDP_IFC.2/TRANSACTION_FLOW Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1/TRANSACTION_FLOW The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/TRANSACTION_FLOW The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

7.1.1.9.2 FDP_IFF.1/TRANSACTION_FLOW Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control, FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/TRANSACTION_FLOW The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

FDP_IFF.1.2/TRANSACTION_FLOW The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

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

FDP_IFF.1.4/TRANSACTION_FLOW The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes that explicitly authorise information flows].

FDP_IFF.1.5/TRANSACTION_FLOW The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes that explicitly deny information flows].

7.1.1.9.3 FPR_UNO.1/TRANSACTION_FLOW Unobservability

Hierarchical to: No other components.

Dependencies: No dependencies

FPR_UNO.1.1/TRANSACTION_FLOW The TSF shall ensure that [assignment: list of users and/or subjects] are unable to observe the operation [assignment: list of operations] on [assignment: list of objects] by [assignment: list of protected users and/or subjects].

7.1.1.10 Prompt control

7.1.1.10.1 FDP_ACC.1/PROMPT Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/PROMPT The TSF shall enforce the [assignment: access control SFP] on[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

7.1.1.10.2 FDP_ACF.1/PROMPT Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/PROMPT The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

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

[assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

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

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

7.1.1.11 PIN handling (offline and online)

7.1.1.11.1 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1/PIN Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

7.1.1.11.2 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.

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

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

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

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

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

[assignment: additional control rules].

Application note:

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

PIN is only allowed to be entered at the keypad. The entry of any other data must be separate from the PIN entry process avoiding accidental display of PIN at the display. If any other data

and PIN are entered at the same keypad, the data entry and the PIN entry shall be clearly separate operations.

7.1.1.11.4 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.

Access to sensitive services requires authentication. Sensitive services provide ac-cess to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.

7.1.1.11.5 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 be-fore allowing any other TSF-mediated actions on behalf of that user.

7.1.1.11.6 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 num-ber of actions that can be performed and also after an imposed time limit. In both cases the PED is forced to return to its normal mode.

Application note:

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

7.1.1.12 Personalisation/Provisioning

7.1.1.12.1 FDP_ITC.2/PERSONALISATION Import of user data with security attributes

Hierarchical to: No other components.

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] FPT_TDC.1 Inter-TSF basic TSF data consistency

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

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

FDP_ITC.2.3/PERSONALISATION 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/PERSONALISATION 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/PERSONALISATION The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: additional importation control rules].

7.1.1.12.2 FDP_ITT.4/PERSONALISATION Attribute-based integrity monitoring

Hierarchical to: FDP_ITT.3 Integrity monitoring

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FDP_ITT.2 Transmission separation by attribute

FDP_ITT.4.1/PERSONALISATION The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [assignment: integrity errors], based on the following attributes: [assignment: security attributes that require separate transmission channels].

FDP_ITT.4.2/PERSONALISATION Upon detection of a data integrity error, the TSF shall [assignment: specify the action to be taken upon integrity error].

7.1.1.12.3 FTP_TRP.1/PERSONALISATION Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1/PERSONALISATION The TSF shall provide a communication path between itself and **remote[31]** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **Trusted path/channels modification, disclosure, [assignment: other types of integrity or confidentiality violation]**.[32]

FTP_TRP.1.2 The TSF shall permit **remote users[33]** to initiate communication via the trusted path. FTP_TRP.1.3 The TSF shall require the use of the trusted path for **personalisation[34]**.

7.1.1.13 Attestation

7.1.1.13.1 FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for **integrity errors[35]** on all objects, based on the following attributes: [assignment: user data attributes].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **become inoperative, erase all encryption keys and send message of being compromised to the payment backend.[36]**

---

[31] [selection: remote, local]

[32] [selection: Class FTP: Trusted path/channels modification, disclosure, [assignment: other types of integrity or confidentiality violation]]

[33] [selection: the TSF, local users, remote users]

[34] [selection: initial user authentication, [assignment: other services for which trusted path is required]]

[35] [assignment: integrity errors]

[36] [assignment: action to be taken]

7.1.1.13.2 FDP_RIP.2 Full residual information protection

Hierarchical to: FDP_RIP.1 Subset residual information protection Dependencies: No dependencies.

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from**[37] all objects

7.1.2 Secure Card Reader as additional hardware

7.1.2.1 Trusted Path (between Software and Secure Card Reader)

7.1.2.1.1 FTP_ITC.1/SCR Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/SCR 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/SCR The TSF shall permit **the TSF**[38] to initiate communication via the trusted channel.

FTP_ITC.1.3/SCR The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required].

7.1.3 Data Protection (with Secure Element/TEE)

7.1.3.1 FPT_ITA.1/SE_TEE Inter-TSF availability within a defined availability metric

Hierarchical to: No other components.

Dependencies: No dependencies.

[37] [selection: allocation of the resource to, deallocation of the resource from]

[38] [selection: the TSF, another trusted IT product]

FPT_ITA.1.1/SE_TEE The TSF shall ensure the availability of [assignment: list of types of TSF data] provided to a secure element[39] within [assignment: a defined availability metric] given the following conditions [assignment: conditions to ensure availability].

7.1.3.2 FPT_ITC.1/SE_TEE Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITC.1.1/SE_TEE The TSF shall protect all TSF data transmitted from the TSF to a secure element[40] from unauthorised disclosure during transmission

7.1.3.3 FPT_ITI.2/SE_TEE Inter-TSF detection and correction of modification

Hierarchical to: FPT_ITI.1 Inter-TSF detection of modification Dependencies: No dependencies.

FPT_ITI.2.1/SE_TEE The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a secure element[41] within the following metric: [assignment: a defined modification metric].

FPT_ITI.2.2/SE_TEE The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a secure element[42] and perform [assignment: action to be taken] if modifications are detected.

FPT_ITI.2.3/SE_TEE The TSF shall provide the capability to correct [assignment: type of modification] of all TSF data transmitted between the TSF and a secure element.[43]

7.1.3.4 FPT_ITT.1/SE_TEE Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1/SE_TEE The TSF shall protect TSF data from **modification[44]** when it is transmitted between separate parts of the TOE.

---

[39] Refinement: another trusted IT
[40] Refinement: another trusted IT product
[41] Refinement: another trusted IT product
[42] Refinement: another trusted IT product
[43] Refinement: another trusted IT product
[44] [selection: disclosure, modification]

7.1.3.5 FPT_SSP.2/SE_TEE Mutual trusted acknowledgement

Hierarchical to: FPT_SSP.1 Simple trusted acknowledgement

Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection

FPT_SSP.2.1/SE_TEE The TSF shall acknowledge, when requested by another part of the TSF, the receipt of an unmodified TSF data transmission.

FPT_SSP.2.2/SE_TEE The TSF shall ensure that the relevant parts of the TSF know the correct status of transmitted data among its different parts, using acknowledgements.

7.1.3.6 Trusted Path (between Software and SE/TEE)

7.1.3.6.1 FTP_ITC.1/SE_TEE Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/SE_TEE 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/SE_TEE The TSF shall permit **the TSF**[45] to initiate communication via the trusted channel.

FTP_ITC.1.3/SE_TEE The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required].

7.1.4 External Attestation/Risk Management

7.1.4.1 FDP_SDI.2/EXT Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring Dependencies: No dependencies.

[45] [selection: the TSF, another trusted IT product]

FDP_SDI.2.1/EXT The external attestation/risk management[46] shall monitor user data stored in containers controlled by the TSF for **integrity errors[47]** on all objects, based on the following attributes: [assignment: user data attributes].

FDP_SDI.2.2/EXT Upon detection of a data integrity error, the TSF shall **become inoperative, erase all encryption keys and send message of being compromised to the payment backend.[48]**

7.1.4.2 FDP_RIP.2/EXT Full residual information protection

Hierarchical to: FDP_RIP.1 Subset residual information protection Dependencies: No dependencies.

FDP_RIP.2.1/EXT The external attestation/risk management[49] shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from[50]** all objects

7.1.4.3 Trusted Path (between Software and External Attestation/Risk Management)

7.1.4.3.1 FTP_ITC.1/EXT Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/EXT 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/EXT The TSF shall permit **the TSF[51]** to initiate communication via the trusted channel.

FTP_ITC.1.3/EXT The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required].

---

[46] Refinement: TSF
[47] [assignment: integrity errors]
[48] [assignment: action to be taken]
[49] Refinement: TSF
[50] [selection: allocation of the resource to, deallocation of the resource from]
[51] [selection: the TSF, another trusted IT product]

7.1.5 Terminal-Server/Backend

7.1.5.1 Transaction flow

7.1.5.1.1 FDP_IFC.2/TRANSACTION_FLOW_TSB Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1/TRANSACTION_FLOW_TSB The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/TRANSACTION_FLOW_TSB The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

7.1.5.1.2 FDP_IFF.1/TRANSACTION_FLOW_TSB Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control, FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/TRANSACTION_FLOW_TSB The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].

FDP_IFF.1.2/TRANSACTION_FLOW_TSB The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

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

FDP_IFF.1.4/TRANSACTION_FLOW_TSB The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes that explicitly authorise information flows].

FDP_IFF.1.5/TRANSACTION_FLOW_TSB The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes that explicitly deny information flows].

7.1.5.1.3 FPR_UNO.1/TRANSACTION_FLOW_TSB Unobservability

Hierarchical to: No other components.

Dependencies: No dependencies

FPR_UNO.1.1/TRANSACTION_FLOW_TSB The TSF shall ensure that [assignment: list of users and/or subjects] are unable to observe the operation [assignment: list of operations] on [assignment: list of objects] by [assignment: list of protected users and/or subjects].

7.1.5.2 Trusted Path (between Software and Terminal/Server Backend)

7.1.5.2.1 FTP_ITC.1/TSB Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1/TSB 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/TSB The TSF shall permit **the TSF**[52] to initiate communication via the trusted channel.

FTP_ITC.1.3/TSB The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required].

7.2 Security Functional Requirements dependencies rationale

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.

The dependency analysis has directly been made within the description of each SFR in section 7.1. All dependencies from CC part 2 and defined by the extended components in chapter 6 are either fulfilled or their non-fulfilment is justified.

[52] [selection: the TSF, another trusted IT product]

7.3 Security Assurance Requirements

7.3.1 Security Assurance Requirements

Security Assurance Requirements EAL 2 augmented by ADV_IMP.1, ALC_DVS_.2, ALC_FLR.1		**Refinements**
Class ADV: Development	ADV_ARC.1	Standard
	ADV_FSP.4	Standard
	ADV_IMP.1	Standard
	ADV_TDS.3	Standard
Class AGD: Guidance Documents	AGD_OPE.1	Standard
	AGD_PRE.1	Standard
Class ALC: Life-Cycle Support	ALC_CMC.2	Standard
	ALC_CMS.2	Standard
	ALC_DEL.1	Standard
	ALC_DVS.2	**Refined**
	ALC_FLR.1	Standard
	ALC_TAT.1	Standard
Class ASE: Security Target Evaluation	ASE_CCL.1	Standard
	ASE_ECD.1	Standard
	ASE_INT.1	Standard
	ASE_OBJ.2	Standard
	ASE_REQ.2	Standard
	ASE_SPD.1	Standard
	ASE_TSS.1	Standard

Security Assurance Requirements EAL 2 augmented by ADV_IMP.1, ALC_DVS_.2, ALC_FLR.1		Refinements
Class ATE: Tests	ATE_COV.1	Standard
	ATE_DPT.1	Standard
	ATE_FUN.1	Standard
	ATE_IND.2	Standard
Class AVA: Vulnerability analysis	AVA_VAN.2	Standard

Table 7: Definition of EAL 2+

Security Assurance Requirements for Composition		Application Note
Class ADV_COMP: Composite design compliance	ADV_COMP.1	Standard

Table 8: Definition for Composition as defined in [CC3]

Security Assurance Requirements Rationale

The chosen assurance package represents the predefined assurance package EAL 2 (AVA_VAN.2 Basic attack potential) augmented with ADV_IMP, ALC_DVS.2 and ALC_FLR.1.

The selection of the component ADV_IMP provides a higher assurance than the predefined EAL2 package due to requiring to examine the implementation of SFR-enforcing modules in detail. [ECSG B4] requirements that fall outside standard SAR are addressed by additions (like ALC_DVS.2 and ALC.FLR.1) and by specific refinements stated in section 7.4.1.

For the chosen assurance components all the dependencies are met.

7.4 Refined security assurance requirements

7.4.1 ALC_DVS.2 Sufficiency of security measures

ALC_DVS.2.1D The developer shall produce and provide development security documentation.

Refinement:

The development environment stands for the design, manufacturing, assembling and maintenance environments of TOE components, including the final assembly and the Initial Key Loading facilities. The Initial Key Loading is defined as the point where responsibility for the TOE security-related components (here and in the following text "security-related" is used in the sense of "SFR-enforcing".) falls to the acquirers. The initial key here is not the Acquirer key, but is the key that assures the authentication of the hardware device independent of the its ultimate purpose and destination.

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Refinement:

Refinement:

In terms of Common Criteria security-related means SFR-enforcing.

The development security documentation shall meet the following requirements:

- *Common.SECC Rule Book Annex 2 - Security Requirements for Site Audits, Version 2.1, 30 July 2020 or latest version.*

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

Main life-cycle related areas of interest as part of the evaluation include the following:

- *Source code storage, e.g. server rooms, environment (cameras, motion detection), network, security policies for handling the source code*
- *Actual development area, e.g. fully encrypted notebooks with secure communication, home (policies for home office, logical security) or office (logical and physical security), staff, HR,*
- *Personalisation/Attestation/Initial Key Loading, same requirements as depicted in JTEMS POI Protection Profile, Version 4.0, 06.03.2015*
- *Attestation/Risk management/Terminal-Server/Backend locations have to be audited at least for physical and network security (if applicable)*

ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

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

ALC_DVS.2.2E The evaluator shall confirm that the security measures are being applied.

Refinement:

The evaluator shall confirm that the security measures are being applied by examination of the developer's documentation and evidences. The security measures involving the development facilities shall be checked during a site visit to each relevant site (as determined by the lifecycle description for ALC_DVS.2.1C).

7.5 Rationale Objectives-SFR

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.

Application note:
For the trial version the ST author is asked to add a rationale with any explanation about the chosen SARs, as long as it is coherent and neither the SARs nor the explanation have obvious inconsistencies with the remaining PP.

	O.PINEntry	O.PIN	O.SWHW	O.SecureCardReader (optional)	O.PaymentTransaction	O.POIApplicationSeparation	O.PromptControl	O.SecureUpdate	O.Personalisation	O.AttestationoftheTOE	O.SE/TEE
Base Component											
FMT_MSA.1			X								
FMT_MSA.3			X								
FMT_SMR.1			X								
FMT_SMF.1			X								
FDP_IFC.1	X	X	X		X	X	X	X	X	X	
FDP_IFF.1	X	X	X		X	X	X	X	X	X	
FDP_ACC.1								X	X		

	O.PINEntry	O.PIN	O.SWHW	O.SecureCardReader (optional)	O.PaymentTransaction	O.POIApplicationSepara-tion	O.PromptControl	O.SecureUpdate	O.Personalisation	O.AttestationoftheTOE	O.SE/TEE
FDP_ACF.1								X	X		
FPT_TST.1			X								
FPT_FLS.1	X	X	X	X	X	X	X	X	X	X	X
FAU_GEN.1		X	X	X	X	X	X	X	X	X	
FPT_STM.1			X		X			X	X	X	
FCS_COP.1/ENC_DEC	X	X									
FCS_COP.1/HASH			X	X	X	X	X	X	X	X	X
FCS_CKM.4	X	X	X	X	X	X	X	X	X	X	X
FCS_RNG.1	X	X	X								
FPT_ITA.1			X		X	X	X	X	X	X	
FPT_ITC.1					X						
FPT_ITI.2					X						
FPT_ITT.1					X						
FPT_SSP.2					X						
FIA_UID.1								X	X	X	
FIA_UAU.1								X	X	X	
FTP_ITC.1					X		X	X	X	X	

	O.PINEntry	O.PIN	O.SWHW	O.SecureCardReader (optional)	O.PaymentTransaction	O.POIApplicationSeparation	O.PromptControl	O.SecureUpdate	O.Personalisation	O.AttestationoftheTOE	O.SE/TEE
FDP_ACC.1/UPDATE								X			
FDP_ACF.1/UPDATE								X			
FDP_ETC.2								X	X	X	
FDP_ITC.2								X	X	X	
FDP_RIP.1								X	X	X	
FDP_IFC.2/TRANSACTION_FLOW					X						
FDP_IFF.1/TRANSACTION_FLOW					X						
FDP_ACC.1/PROMPT							X				
FDP_ACF.1/PROMPT							X				
FTA_TAB.1	X										
FDP_IFC.1/PIN_ENTRY	X	X									
FDP_ITC.1/PIN_ENTRY	X	X									
FIA_UAU.2/PIN_ENTRY	X	X									

	O.PINEntry	O.PIN	O.SWHW	O.SecureCardReader (optional)	O.PaymentTransaction	O.POIApplicationSeparation	O.PromptControl	O.SecureUpdate	O.Personalisation	O.AttestationoftheTOE	O.SE/TEE
FIA_UID.1/PIN_ENTRY	X	X									
FTA_SSL.3/PIN_ENTRY	X	X									
FDP_ITC.2/PERSONALISATION									X		
FDP_ITT.4/PERSONALISATION									X		
FTP_TRP.1/PERSONALISATION									X		
FDP_SDI.2										X	
FDP_RIP.2										X	
Secure Card Reader as additional hardware											
FTP_ITC.1/SCR				X							
Data Protection (with Secure Element/TEE)											
FPT_ITA.1/SE_TEE											X
FPT_ITC.1/SE_TEE											X
FPT_ITI.2/SE_TEE											X

	O.PINEntry	O.PIN	O.SWHW	O.SecureCardReader (optional)	O.PaymentTransaction	O.POIApplicationSepara-tion	O.PromptControl	O.SecureUpdate	O.Personalisation	O.AttestationoftheTOE	O.SE/TEE
FPT_ITT.1/SE_TEE											X
FPT_SSP.2/SE_TEE											X
FTP_ITC.1/SE_TEE											X
External Attestation/Risk Management											
FDP_SDI.2/EXT										X	
FDP_RIP.2/EXT										X	
FTP_ITC.1/EXT										X	
Terminal-Server/Backend											
FDP_IFC.2/TRANSAC-TION_FLOW_TSB					X						
FDP_IFF.1/TRANSAC-TION_FLOW_TSB					X						
FPR_UNO.1/TRANSAC-TION_FLOW_TSB					X						
FTP_ITC.1/TSB					X						

Table 9 Objectives coverage by SFRs

8 Glossary

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
(Bank) card	A card issued by a bank (or by a similar institution) to perform payment transactions.
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.
Card payment	Any payment transaction originating from a (bank) card.
Cardholder	A person using a (bank) card linked to an account to perform payment transactions.
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.

Term	Definition
Distributed architecture	POI architectures where (at least) two security relevant parts of the POI (usually the PED and the Card Reader) are separated devices (i.e. not integrated into one single tamper-responsive boundary).
Enciphered	Enciphered information.
Enciphered PIN	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.
Firmware	All the software present in the POI at the delivery point.
Hardware Security Module (HSM)	Hardware Security Module. A physically and logically protected hardware device that provides a secure set of cryptographic services.
IC	Integrated Circuit
ICC	Integrated Circuit Card
ICCR	Integrated Circuit Card Reader
Integrated Architecture	POI architectures where all security relevant parts of the POI are integrated into one single tamper-responsive boundary.
Issuer	A body issuing cards to Cardholders and authentic transactions initiated by this cards. Usually, an Issuer is represented by a bank or a financial institution. It can also be any body entitled to issue cards.
JIL	Joint Interpretation Library
JTEMS	JIL Terminal Evaluation Methodology Subgroup
Magnetic Stripe	Stripe containing magnetically encoded information.
Merchant	A retailer, or any other person, company, or corporation that agrees to accept (bank) cards in the framework of a contract with an Acquirer. In this Protection Profile the Merchant is also responsible for the TOE in order to protect the TOE against manipulations of the enclosure.
MSR	Magnetic Stripe Reader

Term	Definition
Multi application	A POI that may be used for more than one (card) application.
Offline	Deferred processing without direct communication.
Online	Direct communication between devices with electronic capability (e.g. POI to hosts).
Open Protocol (OP)	A set of requirements that ensures PIN entry devices using open security protocols and open communication protocols to access public networks and services do not have public domain vulnerabilities.
OS	In the scope of this PP, any underlying software providing services for code running in the device is considered part of the operating system. Examples of such services include: system initialization and boot, hardware abstraction layers, memory management, multitasking, synchronization primitives, file systems, device drivers and networking stacks. Services that provide security or may impact security are, in addition, considered firmware. Operating systems may range from hardware abstraction layer libraries and embedded micro-kernels, to complex multi-user operating systems.
PAN	Primary Account Number
Payment Application	A payment application is a particular type of Application, which uses functions provided by the core software of the POI to carry out payment transactions (and possibly card management functions). The Payment Application is excluded from the TOE.
Payment system	Any system processing payment transaction data.
Payment transaction	The act between a Cardholder and a Merchant or Acquirer that results in the exchange of goods or services against payment. For the purpose of this PP also the process performing all steps of a card payment related to the POI.
Payment transaction data	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

Term	Definition
	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.
PIN related data	All items related to the processing of a PIN, i.e. the PIN itself, the PIN encryption keys, etc.
Plaintext PIN	PIN which is allowed to be sent to the IC card as plaintext in order to be verified by the IC card.
POI	A POI is an electronic transaction acceptance product. A POI consists of hardware and software and is hosted in an acceptance equipment to enable a Cardholder to perform a card transaction. Thereby the POI may be attended or unattended. POI transactions are IC card based payment transactions as well as any other payment transactions e.g. based on Magnetic Stripe or any non-payment transactions like health, loyalty or government. The TOE is at minimum a POI excluding applications.
POI component	Any physical or logical device involved in a card payment at a POI (e.g. beeper, Card Reader, display, printer, PED).
POI management data	All PIN related or security related data used to manage and administer the POI. Examples for POI Management data are the risk management data, POI Unique Identifier or the Merchant Identifier. The Terminal Administrator performs operations on POI management data.

Term	Definition
Private key	That key of an entity's asymmetric key pair that should only be used by that entity. In the case of a digital signature scheme, the private key defines the signature function.
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.
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.
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.
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.
Secret (cryptographic) key	A cryptographic key used with symmetric cryptographic techniques and usable only by a set of specified entities.
Secure Application Module (SAM)	See Security Module.

Term	Definition
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.
Sensitive data	Data that must be protected against unauthorized disclosure, alteration or destruction, especially PINs, PAN/account data 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, PAN/account data 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.
SRED	Secure Read and Exchange – A set of requirements protection account data and account data related cryptographic data.
surrogate PAN	A value derived from the PAN, that can be exported outside the device, e.g. to update a loyalty application. Such surrogate PAN can be obtained by different methods: encryption, cryptographic hash (with salt), mask, or truncation.

Term	Definition
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.