UpTeq NFC3.2.2_Generic v1.0

MPP1.0.13vA.2.4 application

Common Criteria / ISO 15408
Security Target – Public version
EAL4+

Table of Contents

Table of Figures

1 Introduction

This document written from the AEPM's Guidance for Payment Application Package Security Target [PAP], provides a list of security requirements for a Payment Application Package (PAP) embedded in a (U)SIM card as specified in [PM] specifications.

This document is the Security Target for the **Mobile PayPass 1.0.13vA.2.4 on UpTeq NFC3.2.2_Generic v1.0 platform**, a Gemalto specific implementation of a TOE. This Product-specific fulfills the generic security requirements given in this security target in order to ensure End users, Mobile Network Operator (MNO) and Issuing Banks trust.

1.1 ST reference

Title:	Mobile Paypass 1.0.13vA.2.4 on UpTeq NFC3.2.2_Generic v1.0 platform - Security Target
Reference:	D1350241
Version:	1.2p
Date of Issue:	18/05/2016
Author:	GEMALTO
ITSEF:	SERMA Technologies
Certification Body:	ANSSI
CC Version:	CC 3.1 revision 4

This Security Target describes:

- The Target of Evaluation (TOE)
- The assets to be protected, the threats to be countered by the TOE itself during the usage of the TOE,
- The organizational security policies, and the assumptions,
- The security objectives for the TOE and its environment,
- The security functional requirements for the TOE and its IT environment,
- The TOE security assurance requirements,
- The security functions and associated rationales.

1.2 TOE reference

TOE is the composition of applet on (U)SIM platform.

Developer's name:	Gemalto
Product name:	UpTeq NFC3.2.2_Generic v1.0 smartcard
Name of applet:	Mobile PayPass 1.0.13vA.2.4
Reference of applet:	S1133159
Version of applet:	Release B
Name of (U)SIM platform:	UpTeq NFC3.2.2_Generic v1.0 platform using ST33G1M2
Reference of (U)SIM platform:	S1164861
Version of (U)SIM platform:	Release A

And its guidances

Guidance of applet:	[GUIDE]
Guidance of (U)SIM platform:	[NFC-GUIDE]

1.3 Reference Materials

Please refer to Part I: "Product Definition" [PM-1] – Section 2.4.

References	Description
[PM-1]	Mobile Contactless Proximity Payment - Part I: Product Definition April 2011, AEPM
[PM-2]	Mobile Contactless Proximity Payment - Part II: Technical Specification April 2011, AEPM
[PM-3]	Security Guidelines for Standard Operational Environment v1.0 – June 2009
[PM-6]	*Payez Mobile* MasterCard Implementation Guide – April 2011
[PP USIM]	(U)SIM Java Card Platform Protection Profile Basic Configuration V2.0.2, June 2010
[PP JCS]	Java Card™ System Protection Profile "Open Configuration" Version 2.6
[GP]	Global Platform 2.2, Specification GP
[GP-CCCM]	GlobalPlatform Card - Confidential Card Content Management, Card specification v2.2 – Amendment A. Version 1.0.1. January 2011
[GP-4]	GlobalPlatform Card Specification 2.2 - UICC Configuration v1.0.1
[GP-5]	GlobalPlatform Card – Amendment C v1.1.1
[PAP]	Guidance for Payment Application Package to write Security Target AEPM, ref: CP-2011-RT-407 / Version 1.0.2
[CC1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
[CC2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
[CC3]	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
[CPESC]	CCDB, Composite product evaluation for Smart Cards and similar devices, September 2007, Version 1.0 - Revision 1, September 2007, CCDB-2007-09-001
[MC-PayPass]	Mobile MasterCard PayPass – Mchip4 v1.0 April 2010MasterCard - PayPass M/CHIP – version 13, September 2005
[DCSSI2741]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard N° 2741/SGDN/DCSSI/SDS/LCR Version 1.10
[GUIDE]	- Mobile Paypass 1.0.13vA.2.4 on UpTeq NFC3.2.2_Generic v1.0 platform - Preparation Guidance. Ref: D1357242 (1.0). - Mobile Paypass 1.0.13vA.2.4 on UpTeq NFC3.2.2_Generic v1.0 platform - Guidance for administration. Ref: D1357097 (1.1). - Mobile MasterCard Paypass Card Applications V1.0, Installation Guide Ref: D1294923 (MobilePayPassInstallGuide_D1294923_RevB-6.pdf) - Mobile MasterCard Paypass Card Applications V1.0, Administration Guide Ref: D1294924 (MobilePayPassAdminGuide_D1294924_RevB-4.pdf) - Mobile MasterCard Paypass Card Applications V1.0, Developing Client Applications Guide Ref: D1294921 (MobilePayPassDevClientAppsGuide_D1294921_RevB-4.pdf)
[NFC-ST]	UpTeq NFC3.2.2_Generic v1.0 USIM Platform - Security Target. Ref: D1350235
[NFC-GUIDE]	– Upteq NFC 3.X platform – Preparation Guidance Ref: D1351549, version 1.1, Gemalto – Guidance for administration of Upteq NFC 3.X platform with Controlling Authority and Optional Verification Authority

	Ref: D1341170_w_CA, version 1.1, Gemalto – Guidance for administration of Upteq NFC 3.X platform without Controlling Authority and Optional Verification Authority Ref: D1341170_wo_CA, version 1.1, Gemalto – Guidance for Verification Authority for Upteq NFC 3.X platform Ref: D1341169_VA, version 1.0, Gemalto – GlobalPlatform Card – Composition Model – Security Guidelines for Basic Applications Ref: GPC_GUI_050, version 2.0, November 2014, GlobalPlatform – Guidance for secure application development on Upteq NFC platforms Ref: D1188231, release A13.1, Gemalto – Application management for certified Secure Elements – External Procedure Ref: D1258682, release C01, Gemalto – Patch Loading Management for certified Secure Elements – External procedure Ref: D1344508, release A00, Gemalto

1.4 Definitions

Please refer to Part I: “Product Definition” [PM-1] – Section 2.5.

1.5 Acronyms and Abbreviations

Please refer to Part I: “Product Definition” [PM-1] – Section 2.6.

Abbreviations	Meaning
AAC	Application Authentication Cryptogram
AFL	Application File Locator
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
ARPC	Authorisation Response Cryptogram (within a transaction)
ARQC	Authorisation Request Cryptogram (within a transaction)
ATC	Application Transaction Counter
CAS	Common Approval Scheme
CC	Common Criteria
CDOL	Card risk management Data Object List
CEM	Common Evaluation Methodology
CVM	Card Verification Method
CVR	Card Verification Results
DDA	Dynamic Data Authentication
DDOL	Dynamic Data Object List
EAL	Evaluation Assurance Level
EMV	Europay MasterCard Visa
ETR_COMP	Report for a composite Smart Card Evaluation
GP	Global Platform
IC	Integrated Circuit
IT	Information Technology
JCS	Java Card System

JSR	Java Specification Request
MMI	Man Machine Interface
MNO	Mobile Network Operator
NFC	Near Field Communication
OS	Operating system
OSP	Organizational Security Policy
OTA	Over The Air
PAN	Primary Account Number
PAP	Payment Application Package
PC	Personal Code
PIN	Personal Identification Number
POS	Point Of Sale
PP	Protection Profile
RSA	Rivest Shamir Adleman
SIM	Subscriber Identity Module
ST	Security Target
TOE	Target Of Evaluation
TSM	Trusted Service Manager
TSF	TOE Security Functions
USIM	Universal Subscriber Identity Module

1.6 TOE overview

This section briefly describes the usage of the TOE and its major security features, identifies the TOE type and any non-TOE hardware/software/firmware required by the TOE.

1.6.1 TOE type

The product to be evaluated is Gemalto **Mobile PayPass 1.0.13vA.2.4 on UpTeq NFC3.2.2_Generic v1.0 platform** (U)SIM card intended to be plugged in a mobile handset to provide secure payment services to an end-user (see Figure 1).

The TOE is composed of the following bricks:

- The Gemalto **UpTeq NFC3.2.2_Generic v1.0** (U)SIM Java Card platform certified conformant to [PP USIM] which is a piece of software (OS, Java Card System, (U)SIM APIs, …) embedded in an STMicroelectronics ST33G1M2 Integrated Circuit (IC). It shall be compliant with GlobalPlatform UICC[1] Configuration [GP-4] and GlobalPlatform Card Specification v2.2 [GP] including the extended ProcessData method as defined in Confidential Card Content Management (GP2.2 Card Specification v2.2 - Amendment A [GP-CCCM]). The (U)SIM also implements the mechanisms defined in GlobalPlatform Amendment C [GP-5].

- A Gemalto **Mobile PayPass 1.0.13vA.2.4** Payment Application Package[2] (PAP) compliant with [PM-1], [PM-2] and [PM-6].

[1] UICC stands for a (U)SIM card
[2] The term package doesn't correspond to the package in Java world but means the contactless mobile payment application

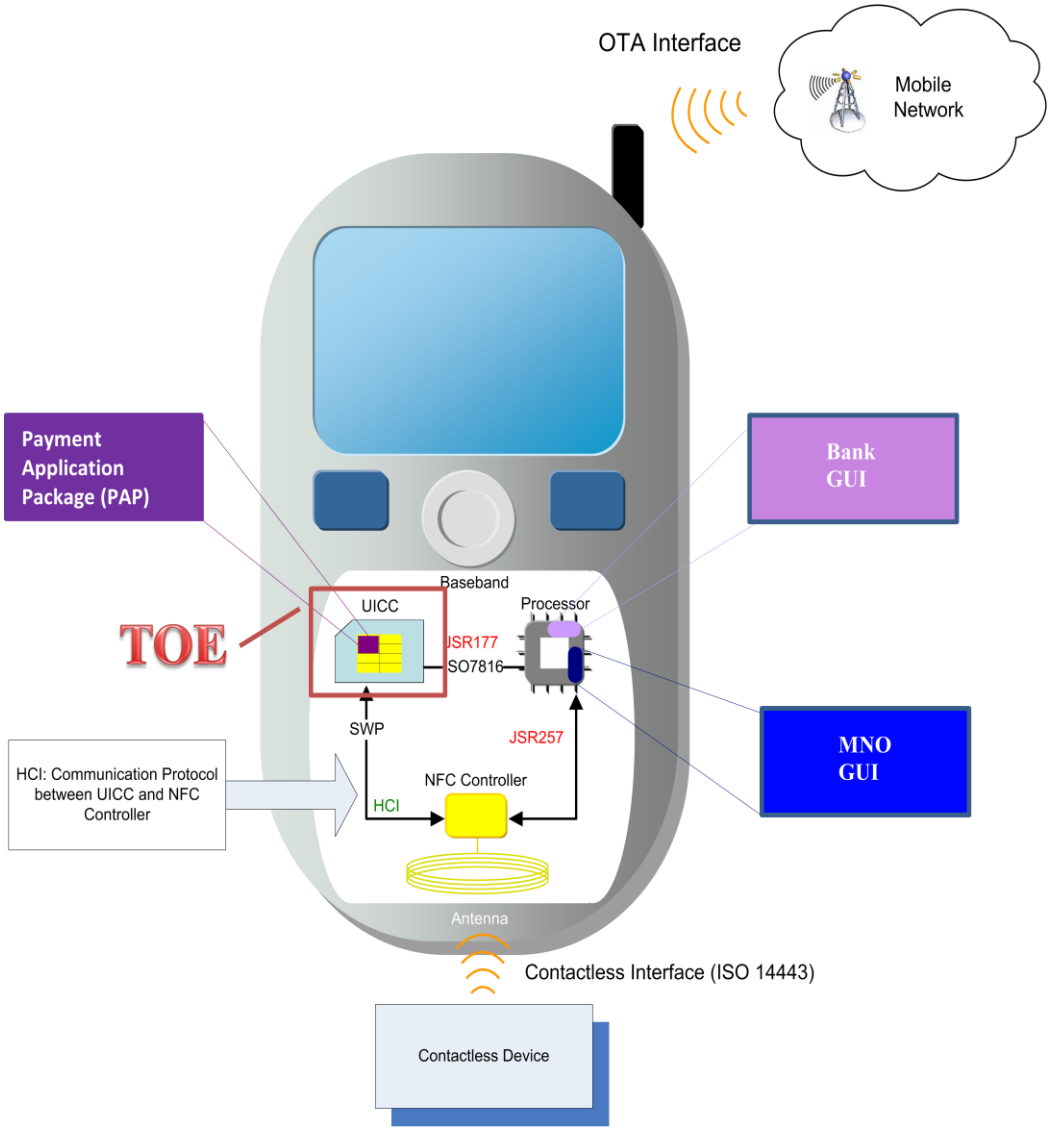

Figure 1: TOE type

The PAP application shall be compliant to the MasterCard [PM-6] Payez Mobile Implementation Guide.

For MasterCard, PAP is composed of:

- the Contactless Mobile Payment application or CMP application, defined section 1.7.1.1;
- the Payez Mobile Customization Package.

1.6.2 Usage and major security features of the TOE

Refer to [NFC-ST] for usage of the platform.

Payez Mobile introduces an innovative Contactless Mobile Payment (CMP) solution that enables CMP transactions via radio frequency with the payment function located on a mobile handset supporting NFC technologies.

One or more PAP can be installed in the (U)SIM card. To execute a CMP, customers simply hold their mobile handset close to a contactless reader to exchange payment information. Authorization and

clearing are processed similarly to an EMV or a magnetic stripe purchase transaction. The *Payez Mobile* solution can be used for any transaction amount, including low value transactions.

Payez Mobile CMP is characterized by a radio frequency short read range distance that requires the mobile handset to be presented close to the contactless reader to enable a transaction. Thus, only proximity purchase transactions are authorized ([PM-1], Section 4.2).

Two modes are offered to a customer to execute a *Payez Mobile* CMP: Mode 1 “PIN – TAP” and Mode 2 “TAP – PIN – TAP”.

Warning: the acronym PIN used in the two payment modes described below refers to the Personal Code provided by the Issuing Bank to the customer.

1.6.2.1 Mode 1: PIN – TAP

When making a purchase, first, the customer manually chooses the appropriate PAP to be used for the purchase transaction, enters his Personal Code then taps his mobile handset on the landing zone of the POS terminal[3] to submit a payment transaction with the amount requested by the merchant and indicated on the POS terminal. Figure 2 illustrates this mode of payment transaction in seven steps.

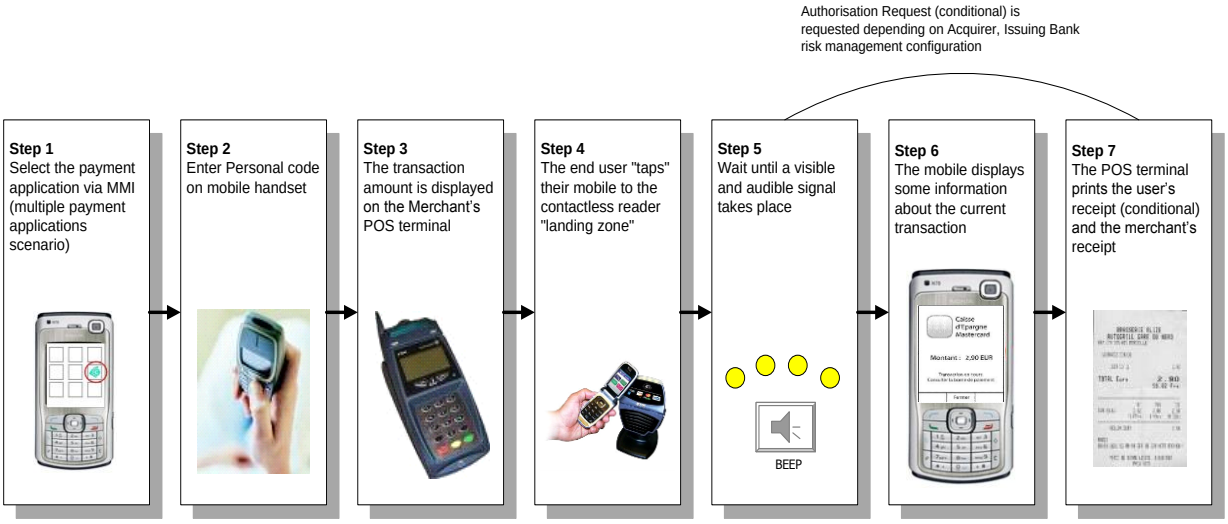

Figure 2: Mode 1: PIN - TAP

1.6.2.2 Mode 2: TAP – PIN – TAP:

In this mode, the customer first taps his mobile to the landing zone of the POS terminal which already displays a transaction amount; after that, if the transaction amount is lower than Personal Code Entry Limit (e.g. 20 EUR) then the transaction is processed without Personal Code (optional upon customer configuration). Otherwise, if the amount is above the Personal Code Entry Limit (see Personal Code Entry Conditions listed in Section 4.5.2.1, [PM-1]), then the customer enters his Personal Code and after that taps his mobile handset a second time on the landing zone of the merchant POS terminal in

[3] Point of sales (POS) stands for the merchant acceptance terminal used to execute and process a financial transaction by communicating with a customer device such as a mobile handset.
POS terminal includes stand alone, multi-lanes or ECR devices The POS incorporates a contactless interface device and may also include other components and interfaces.

order to proceed with the payment transaction. The steps of this mode of transaction are presented in Figure 3.

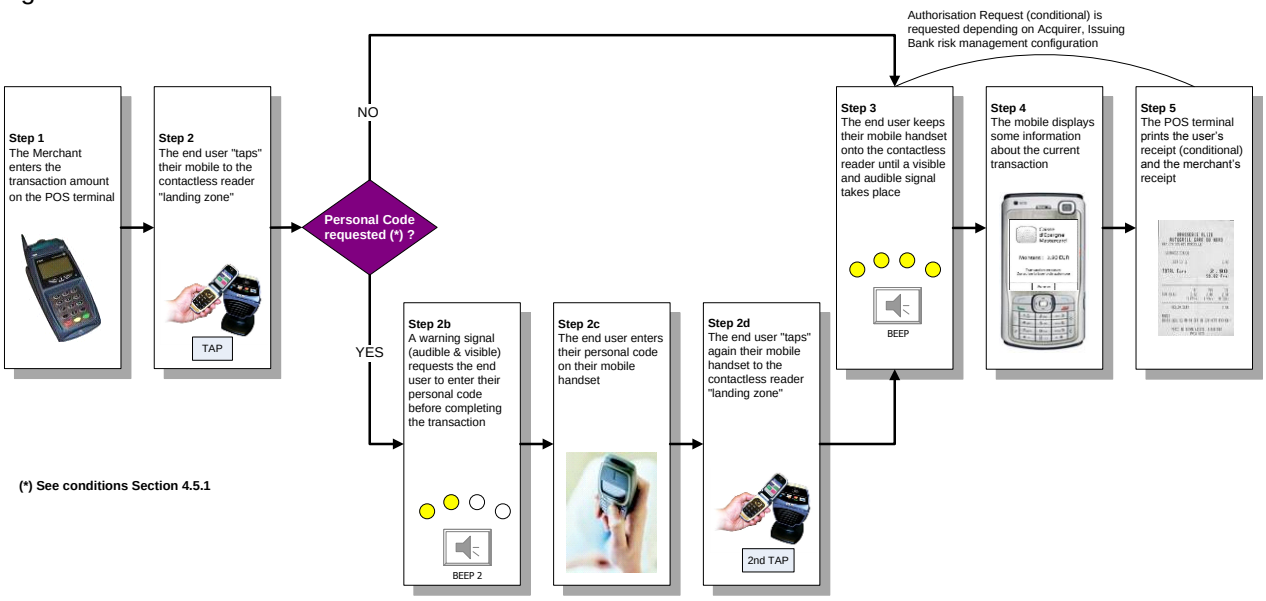

Figure 3: Mode 2 - TAP - PIN – TAP

1.6.2.3 Security features

In addition to the security functions supported by the (U)SIM platform (refer to [NFC-ST] for usage of the platform) , the PAP shall support the security features listed below:

- Offline communication with the POS terminal
- Offline Data Authentication
- Online Authentication and communication with the Bank Issuing
- Personal Code verification and management
- Transaction risk management analysis
- Transaction Certification
- Counter reset processing,
- Script processing via OTA bearer
- Auditing
- Log reading and update
- Administration management (Contactless life cycle management)

Depending on the Acquirer and Issuing Bank risk management configuration, the merchant POS terminal processes the proximity purchase transaction offline or online.

A *Payez Mobile* CMP transaction shall be executed according to *Payez Mobile* specification and under MasterCard, Visa or local scheme requirements and operating rules and should use the same authorization network and clearing system than standard credit and debit cards. The contactless payment application targeted is the Mobile PayPass 1.0.13vA.2.4 application according to MasterCard specifications.

1.6.3 Required non-TOE hardware/software/firmware

This section describes the hardware, software or firmware present in the environment of the TOE and that are required to have a functional correct usage of the TOE.

For a detailed description, see [PM-2], Section 2.2.

The non-TOE hardware/software/firmware required by the (U)SIM platform (e.g. Bytecode verifier) are also required by the TOE. More precisely all applications must follow the rules given inside guidances for Upteq M-NFC certified product (GPC_GUI_050 & D1188231).

Next paragraphs below describe the items required in the environment of the product but not required for secure usage of the TOE.

1.6.3.1 Payez Mobile Application[4] (AEPM CREL Application)

The *Payez Mobile* application is a CREL (Contactless Registry Event Listener) application according to Global Platform Amendment C [GP–5]. The *Payez Mobile* application applies the *Payez Mobile* business logic consisting to have only one activated Payment Application Package at a time. Upon a new activation request, this application is responsible for managing the deactivation of the current activated payment application.

The *Payez Mobile* application is the single application (except the CMP application itself) that can modify the CMP contactless life cycle state from "ACTIVATED" to "DEACTIVATED".
This application does not apply its business logic if the new application to be activated and the current activated application are members of the same application group, or in case of one-shot payment[5].

1.6.3.2 Proximity Payment System Environment (PPSE) application (EMVCo CREL Application)

The PPSE application is a CREL (Contactless Registry Event Listener) application according to GlobalPlatform Amendment C [GP–5].

This application is present in the Issuer Security Domain. Therefore, it is under the MNO's responsibility. Its role is to:

- Read the GP Registry in order to check the "ACTIVATED" CMP application. Only one CMP application is in the state "ACTIVATED" at a time. Therefore, the PPSE contains only one CMP application AID;
- Build the "SELECT PPSE" response. The PPSE response is updated each time an activation or deactivation notification is received from the CRS API (Contactless Registry Service Application Programming Interface);
- Upon reception of a "SELECT PPSE" command, the PPSE application returns the PPSE response built previously.

1.6.3.3 Bank TSM

This is a platform providing functions for transport encryption to manage the Bank Supplementary Security Domain (Bank SSD) by establishing a dedicated secure channel for management commands and data.

When using Delegated Management (DM) mode, it also provides functions to manage the request of SSD creation and after requesting a token DM to the MNO, to manage the payment application installation, instantiation and deletion.

1.6.3.4 UICC Management Platform

The UICC Management Platform is owned by the MNO and handles the global management of the customer's UICCs. This platform is mainly used during the payment service delivery.

1.6.3.5 Bank GUI Management Platform

The Bank GUI Management Platform enables the Bank GUI installation, its synchronization and its update.This platform shall be able to cover application portability issues and deliver the appropriate version of the Bank GUI, depending on the mobile handset used by customer.

---

[4] Not to be confused with the Payment Application Package (PAP).
[5] One-shot payment : The CMP application (that is not active by default) selected by the Customer is used only for the current payment transaction.

1.6.3.6 POS terminal

Point of sales (POS) stands for the merchant acceptance terminal used to execute and process a financial transaction by communicating with a customer device such as a mobile handset.

POS terminal includes stand alone, multi-lanes or ECR devices The POS incorporates a contactless interface device and may also include other components and interfaces

The POS terminal shall comply with *Payez Mobile* minimum requirements defined in [PM-2].

1.6.3.7 POS Application

The POS terminal hosts a payment application that complies with MasterCard (PayPass), Visa (PayWave) or local scheme contactless specifications and with *Payez Mobile* Specifications.

1.6.3.8 Mobile Handset

The TOE as a smartcard is intended to be plugged in a mobile handset. This equipment can be a mobile phone or a PDA or any other connecting device.

NFC Mobile handset shall comply with *Payez Mobile* minimum requirements defined [PM-2].

1.6.3.9 Bank GUI

The Bank GUI (Java, SDK Android…) is a graphical interface loaded into the mobile handset that allows the customer to access to the functions associated to their CMP applications.

The Bank GUI gives several functionalities to the customer for example:

- payment;
- set to ACTIVATED by default (Activate its CMP application);
- deactivate its CMP application;
- change the Personal Code;
- change the application name;
- CMP application parameters update;
- transaction log consultation;
- etc.

1.6.3.10 MNO GUI

The MNO GUI is the primary graphical interface loaded onto the mobile handset which allows the customer to access all their NFC services stored in the UICC.
If the customer selects one PAP, the MNO GUI launches the associated graphical interface (called Bank GUI).

This interface allows the Customer to identify the current active CMP application by displaying a logo beside the associated Bank GUI.

1.6.3.11 OTA Platform

Platform using OTA mechanisms providing functions to tunnel information messages exchanged between the UICC Management Platform or the Bank TSM and a (U)SIM.

1.7 TOE description

1.7.1 Physical scope of the TOE: all hardware, firmware, software and guidance

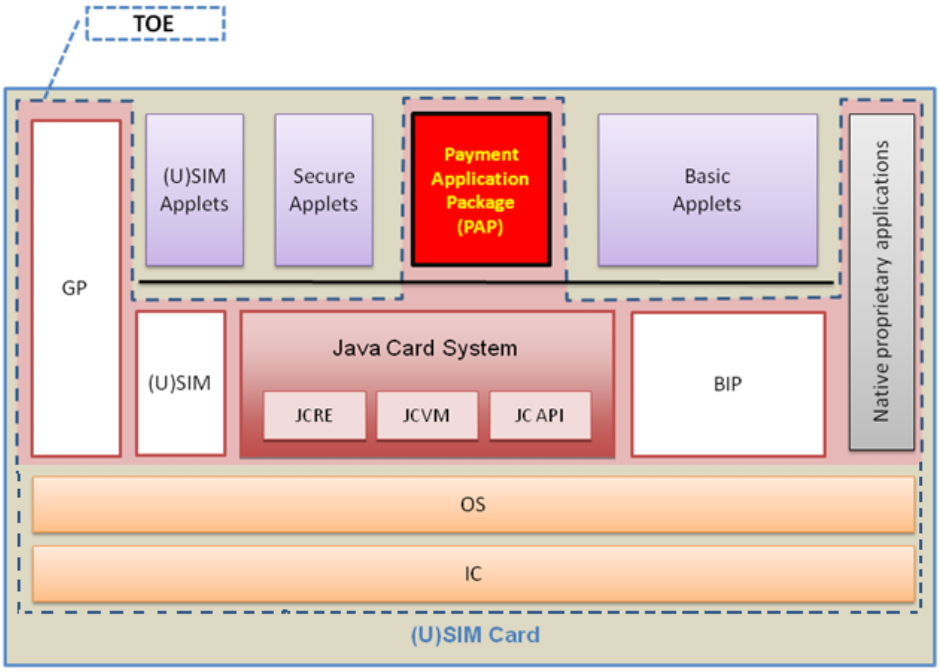

Figure 4: TOE physical scope like in [PAP]

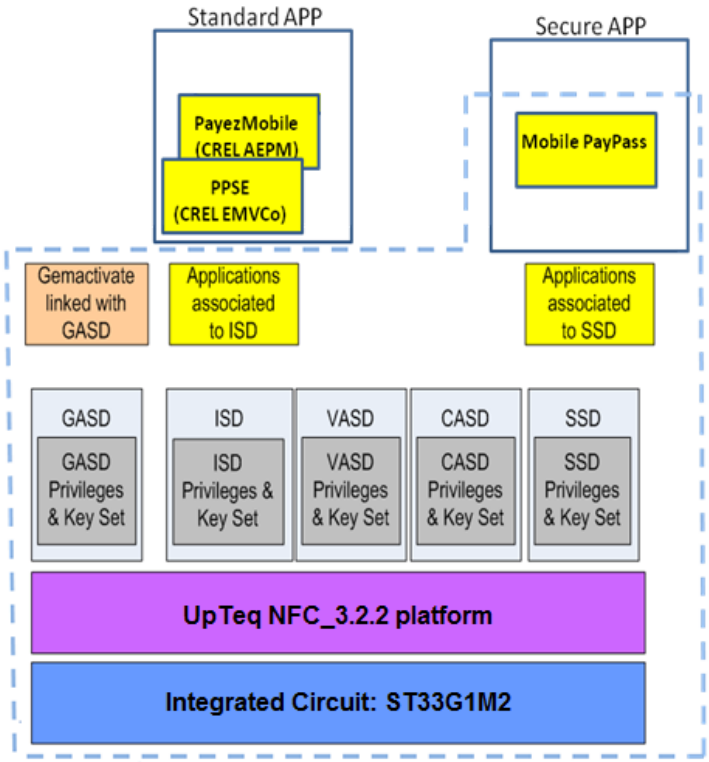

Figure 5: TOE logical boundaries

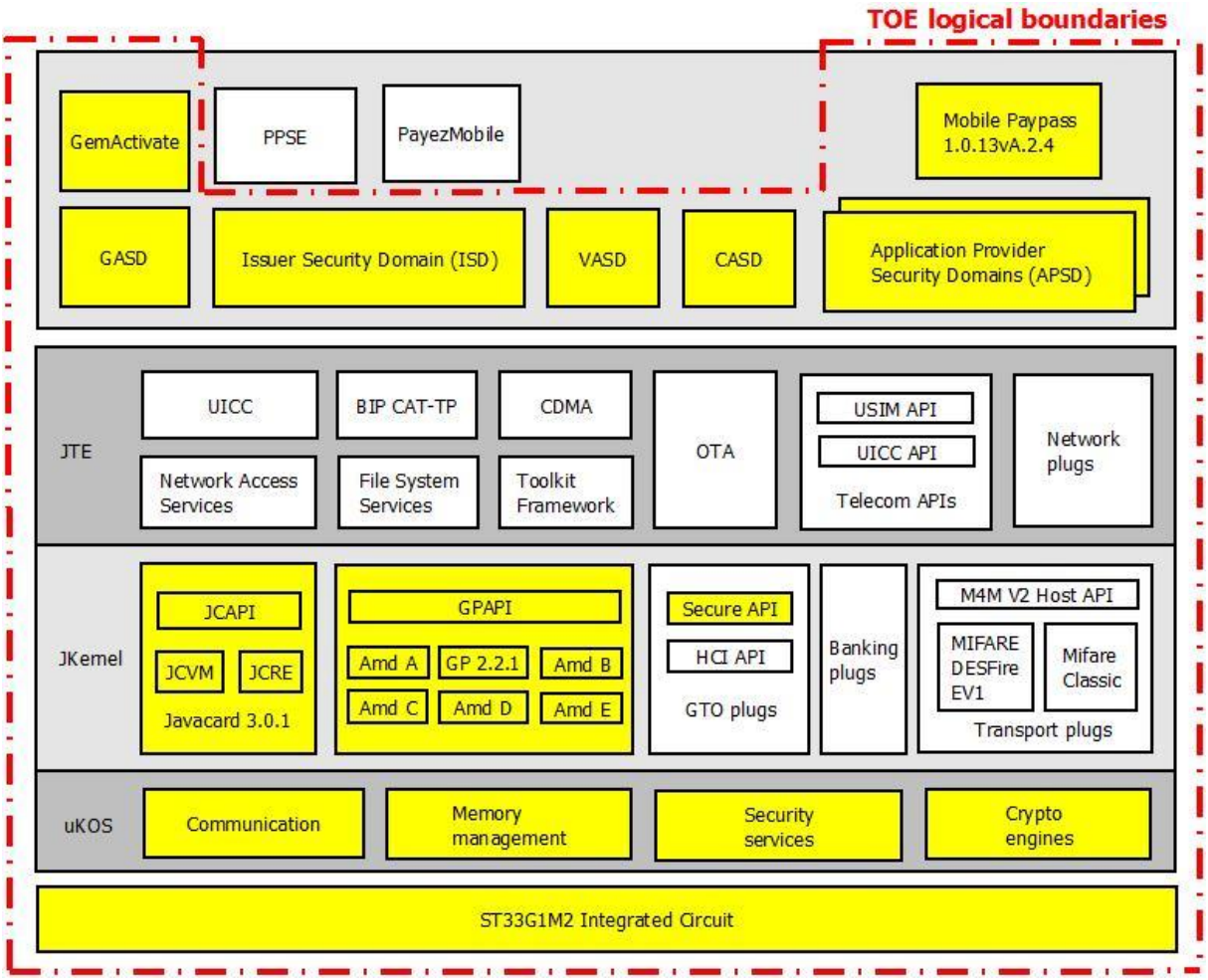

Figure 6: Major TOE items and scope

In this figure, the TSF components have been put in yellow color. The other components (in white color) do not participate to the TOE security.

The physical interfaces are those described in the platform ST [NFC-ST].

The following platform TOE components are described in details in the the platform ST [NFC-ST] compliant to the (U)SIM platform Protection Profile [PP USIM]:

- **ST33G1M2** Integrated Circuit (IC)
- **UpTeq NFC3.2.2_Generic v1.0** (U)SIM
- Java Card System according JCS Protection Profile [JCS PP] Open configuration
- GlobalPlatform (GP)

1.7.1.1 Payment Application Package (PAP)

The Payment Application Package is loaded on a Bank TSM (cf. [PM-6]).

The **Mobile PayPass 1.0.13vA.2.4** CMP application is compliant with the payment scheme specifications:

- MasterCard PayPass specifications (MChip/MagStripe)

It is possible to have several versions of the same CMP application loaded onto the UICC and thus several instance versions.

In our case the Mobile PayPass 1.0.13vA.2.4 is loaded on a Bank SSD.

For more details about the PAP Application, please refer to:

- Section 1.7.2 of this document;
- *Payez Mobile* MasterCard Implementation Guide **[PM-6]**.

1.7.2 Logical scope of the TOE: the logical security features offered by the TOE

Refer to [NFC-ST] for description of the platform security features.

This section describes the security features offered by the PAP. These are structured in several modules (see Figure 7). For a detailed description about these modules, refer to [PM-6] section 2.1.

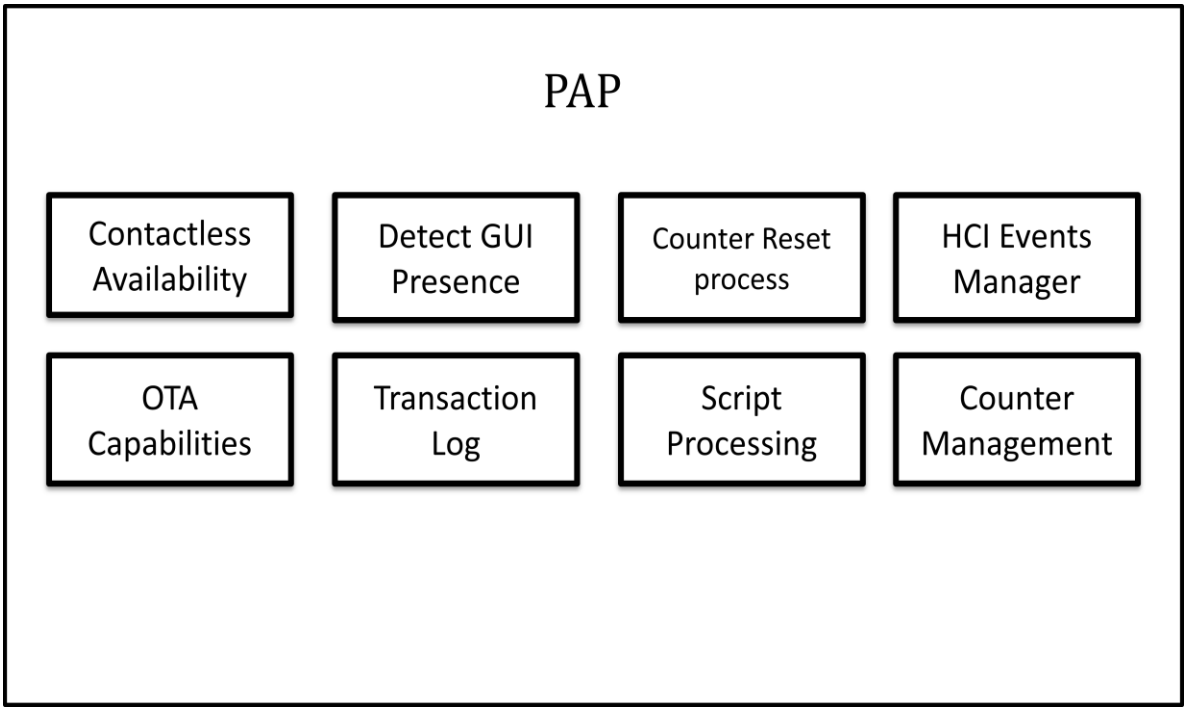

Figure 7: PAP Module

1.7.2.1 Contactless Availability

The contactless availability is responsible for:

- the CMP activation by using the activation interface of the CRS API (the contactless life cycle state will be updated to the value 'ACTIVATED' in the GP Registry)
- the CMP deactivation by using the deactivation interface of the CRS API (the contactless life cycle state will be updated to the value 'DEACTIVATED' in the GP Registry)
- the CMP blocking by setting up the contactless life cycle state to the value 'NON ACTIVATABLE' in the GP Registry (using the CRS API).

1.7.2.2 Script Processing Module

This is a functional module allowing the Issuing Bank to update some parameters of the application and strictly compliant with the payment scheme specifications.
This module supports Personal Code Change/Unblock command, Personal Code Entry Limit Update, etc.

For a detailed description about the Script Processing Module, refer to [PM-2], section 8.3.

1.7.2.3 Counters Management

This module enables the update of limits and counters partial renewal.
The offline counters are updated during a payment transaction if it is accepted offline. The counters are not updated if a transaction is completed online.

1.7.2.4 Counter Reset Processing Module

This module ensures that the CMP application counter limit is not exceeded. When counters exceed their limit, the CMP application requests an online authorization to finalize the transaction.

For more information about this process, please refer to [PM-2] Section 8.2.4, [PM-6].

1.7.2.5 Transaction Log Module

During a payment transaction, this module ensures that the data for the transaction are logged.
Moreover, it allows the Bank GUI to retrieve the transaction log data for display purposes.

1.7.2.6 Detect GUI Presence Module

This module enables to detect the presence of the Bank GUI. If the Bank GUI is not present, the transaction cannot be executed.

1.7.2.7 HCI Events Manager Module

The HCI events are used to wake up the Bank GUI when a user interaction is required (at the end of a transaction or when the Personal Code is required)[6].

1.7.2.8 Over-The-Air (OTA) Capabilities

Platform using OTA mechanisms providing functions to tunnel information messages exchanged between the UICC Management Platform or the Bank TSM and a (U)SIM.

[6] The only HCI event used in *Payez Mobile* solution is the EVT_TRANSACTION without the use of the parameter field. To be aware of the transaction context (i.e. why the Bank GUI has be awaken), the Bank GUI shall read the Mobile Cardholder Interaction Information

1.7.3 Overview of the TOE Life Cycle

The life cycle of the TOE is the life cycle of the (U)SIM card ((U)SIM Platform + PAP), from the development to the operational stage through manufacturing and personalization. Figure 8 illustrates the life cycle of the (U)SIM Platform as well as the life cycle of the PAP.

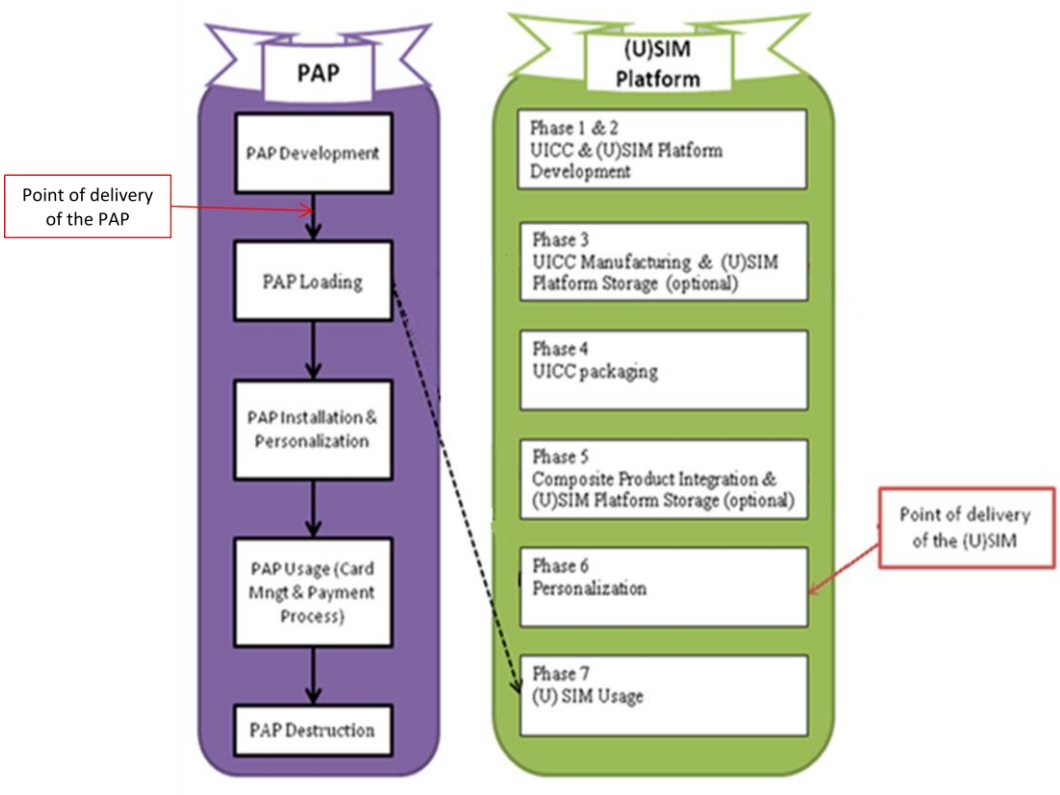

Figure 8: TOE life cycle

We refer to platform ST [NFC-ST] for the definition of the (U)SIM Platform life cycle.
The personalization phase (phase 6) includes the loading in pre-issuance of the 3 Standards APP according to the product configuration (i.e. **PPSE**, **Payez Mobile**).

The life cycle of the PAP consists of consecutive stages:

- **Development:** This stage is performed on behalf of the Issuing Bank in a secure development environment;
- **Loading:** This stage may occur in phase 7. Loading in Phase 7 is post-issuance, e.g. using OTA means;
- **Installation & Personalization:** This stage may occur in phase 7 in the usage environment;
- **Usage:** This stage occurs in phase 7. In PAP Usage phase, the MNO and/or the Issuing Bank may perform card management and PAP management activities such as updating parameters, PAP blocking/unblocking, etc;
- **Destruction:** At this stage, the PAP is destroyed.

We refer to platform Guides [NFC-GUIDE] for the security recommendations to apply.

PAP development (phase 1) is in the TOE evaluation scope, including the application verification according to rules given inside guidances for Upteq M-NFC certified product (GPC_GUI_050 & D1188231).

PAP verification and signature by Verification Authority (VASD) prior to PAP loading (phase 7) is out of the TOE evaluation scope (covered by the platform guidance).

The **Mobile PayPass 1.0.13vA.2.4** application, Secure APP, is loading in post-issuance during PAP loading phase (phase 7).

1.7.3.1 TOE role and environment

We refer to platform ST [NFC-ST] for the location of the (U)SIM Platform role and environment.

Stage	Role and Environment
PAP development	**PAP Application Developer** for Issuing Bank. Gemalto La Ciotat, La Vigie – Avenue du Jujubier – ZI Athélia IV, 13705 La Ciotat. Gemalto Singapore, 12 Ayer Rajah Crescent, 139941 Singapore. ITSEF **Secure environment.**
PAP loading	Application loader (i.e. TSM[7] entity) is in charge of secure application loading. The TSM-SP acting behalf Issuing Bank (SSD) to load the secure applications by OTA. The **TSM-SP** is composed of **Integrator** to setup the server and the **Server** (that contains secure application/DAP and software with required keys) to perform the loading. Before loading, all applications are verified by a Validation Laboratory for the Standard applications, or by ITSEF for the Secure applications. All applications are associated at load time to a **Verification Authority[8]** signature (Mandated DAP) that is verified on-card by the on-card representative of the VA prior to the completion of the application loading operation and prior to the instantiation of any applet defined in the loaded application. **Controlling Authority[9]**
PAP installation and personalization	**PAP Provider[10]** (Issuing Bank / SSD) personalize their applications and security domains in a confidential manner. They have security domain keysets enabling them to be authenticated to the corresponding security domain and to establish a trusted channel between the TOE and an external trusted device. These security domain keysets are not known by the **(U)SIM Card issuer.**
PAP usage (Card Mngt & Payment process)	**(U)SIM Card issuer** (MNO[11] / ISD) is initially the only entity authorized to manage applications (loading, instantiation, deletion) through a secure communication channel with the card, based on SMS or BIP technology. However he can grant these privileges to the **PAP Provider** through the delegated management function of GP.

[7] TSM means Trusted Services for Mobile NFC by linking MNO with the NFC world, managing services for banks and transport operators and always-on services backed by banking grade security. Several TSM exist: the TSM-SP acting on behalf the Service Provider (ie. Bank) and TSM-MNO acting on behalf the MNO (ie. Orange).
[8] The Verification Authority (VA), trusted third party represented on the (U)SIM card, acting on behalf of the MNO and responsible for the verification of applications signatures (mandated DAP) during the loading process. These applications shall be validated for the standard applications or certified for the secure ones.
[9] The Controlling Authority (CA), entity independent from the MNO represented on the (U)SIM card and responsible for securing the keys creation and personalization of the Application Provider Security Domain (APSD).
[10] The Application Provider (AP) of PAP, financial institution (a bank) responsible for the applications and their associated services.
[11] The Mobile Network Operator (MNO or mobile operator), issuer of the (U)SIM Java Card platform and proprietary of the (U)SIM. The platform guarantees that the issuer, once authenticated, could manage the loading, instantiation or deletion of applications.

	PAP Provider (Issuing Bank / SSD). **End-User** Unprotected environment.
PAP destruction	**PAP Provider** (Issuing Bank / SSD). Unprotected environment.

1.7.4 PAP on-card life cycle

The on-card life cycle of the PAP (see Figure 10: GP standard life cycle states) is compliant with the GlobalPlatform standard life cycle [GP]:

The PAP life cycle is divided in two parts:

- The contactless life cycle, concerning the contactless PAP states
- The life cycle status, concerning the standard GP states

1.7.4.1 Contactless life cycle

The contactless life cycle is composed of three states:

- **ACTIVATED** state in which the application is activated and can be selected by a terminal application;
- **DEACTIVATED** state in which the application is deactivated but still can be selected by a terminal application to receive appropriate commands. For instance, in this state, the customer is authorized to view his transactions log or change the Personal Code;
- **NON-ACTIVATABLE** state in which the application cannot be activated and its services are blocked either by the Issuing Bank or as a result of several (above the Personal Code Entry Limit) wrong Personal Code entry by the customer. When the life cycle status of the "Head Application" of an application group is NON ACTIVATABLE, then the members of the application group are automatically deactivated (application life cycle state changed to the value "DEACTIVATED"). Please refer to GlobalPlatform [GP] for more information.

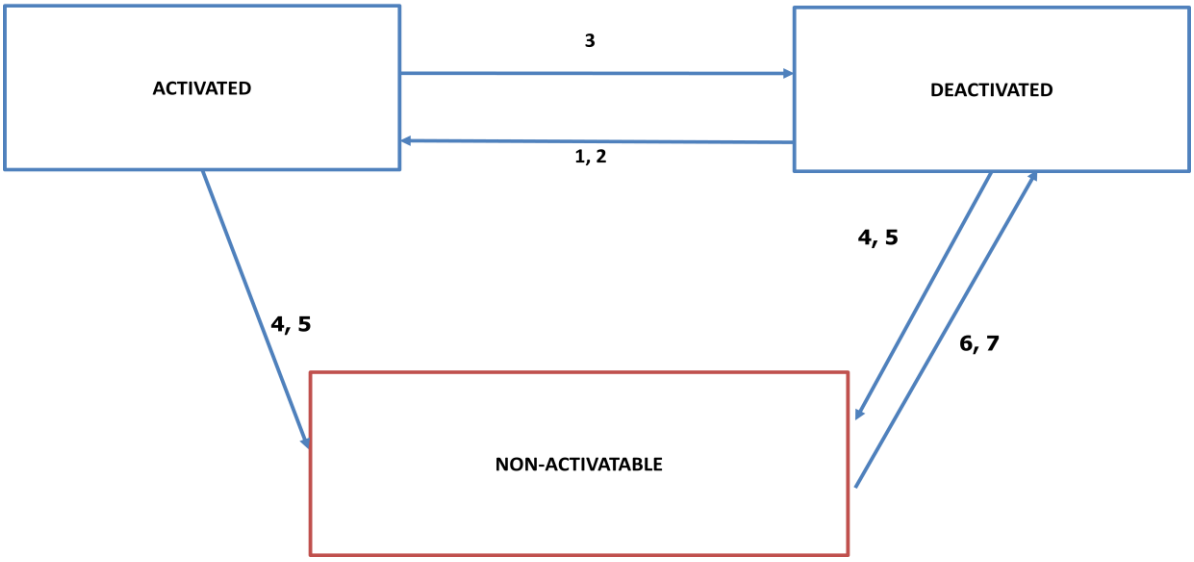

Figure 9: Contactless life cycle states

Steps Description:

1. Another CMP Application is ACTIVATED;
2. A Customer sets an application from “DEACTIVATED” to “ACTIVATED” via the function “Define a CMP application”
3. A Customer sets an application from “ACTIVATED” to “DEACTIVATED” via the function “Deactivate a CMP application”;;
4. The CMP application is blocked by the Issuing Bank (NON-ACTIVATABLE);
5. Three wrong personal codes have been entered by the Customer; the application is automatically blocked (NON-ACTIVATABLE). Personal Code unblock is required to unblock the CMP application;
6. The CMP Application is unblocked by the Issuing Bank;
7. The Personal Code is unblocked by the Issuing Bank.

1.7.4.2 GP standard life cycle

The life cycle status is the representation of the GP life cycle (compliant with [GP]).

The GP standard life cycle is composed of states:

- **INSTALLED** state corresponds to the status of the PAP after its installation. In this state, the PAP can also be personalized (for instance, with the Personal Code of the customer);
- **SELECTABLE** state that means that the Application is able to receive commands from off-card entities**;**
- **LOCKED** state which is a reversible state in which the PAP is NON SELECTABLE and its services are temporarily blocked.

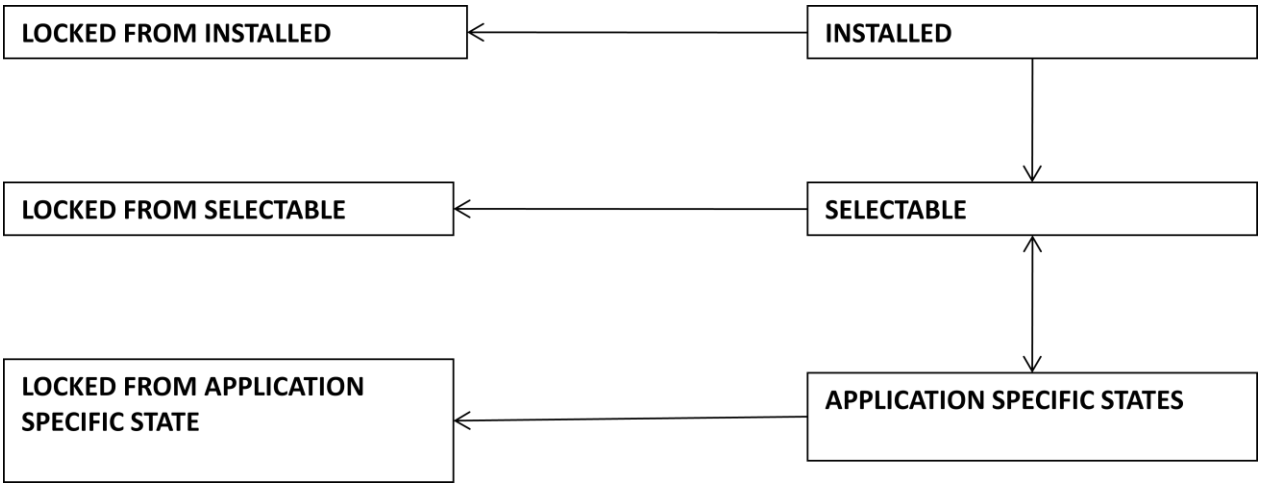

Figure 10: GP standard life cycle states

1.7.5 Configurations

Platform: **UpTeq NFC3.2.2_Generic v1.0 platform using ST33G1M2**

Configuration	Application		
	Mobile PayPass 1.0.13vA.2.4	PPSE	Payez Mobile
	(Mastercard)	(CREL EMVCo)	(CREL AEPM)
	Bank SD	MNO ISD	MNO ISD
N°1 – Mastercard EMVCo	X (1 per virtual card)	X (1 instance)	
N°2 – AEPM France/WW	X (1 per virtual card)	X (1 instance)	X (1 instance)

In our case:

- the **Mobile PayPass 1.0.13vA.2.4** application is considered as Secure APP
- the **PPSE**, **Payez Mobile** applications are considered as Standard APP

2 Conformance Claim

2.1 CC conformance claim

This Security Target is written using CC version 3.1 release 4.

This ST is CC Part 2 conformant and CC Part 3 conformant.

2.2 PP and Package claim

The evaluation assurance level of this security target is EAL4 augmented with:

- **ALC_DVS.2** Sufficiency of security measures
- **AVA_VAN.5** Advanced methodical vulnerability analysis

3 Security Problem Definition

3.1 Assets

This section identifies the assets of the PAP, protected by a combination of (U)SIM platform and PAP itself. Note that the PAP code is an asset of the (U)SIM platform, protected in integrity by means of JavaCard System access control.

In the following, the description of each asset states the type of protection required.

3.1.1 User data

User data are created by and for the user. These data do not affect the operation of the TSF. The following assets are user data.

POS Transaction Data

All data transmitted to the PAP from the POS terminal. This includes: Country Code, Terminal Verification Result, etc.

Protection: integrity.

Issuing Bank Transaction Data

All transaction data transmitted to the PAP by the Issuing Bank including Issuing Bank authentication data, ARPC, CDOL2, etc.

Protection: integrity.

Issuing Bank Scripts

All the scripts transmitted by the Issuing Bank to update PAP Transaction Parameters and PAP internal states (Application Block/Unblock, Counter Reset, Change/Unblock the Personal Code,etc)

Protection: integrity.

MNO Data

All data transmitted to the TOE by the MNO including the MNO authentication data.

Protection: integrity.

PAP Log File

PAP Log File and its associated format under EMV rules. This asset contains the log data of the last transactions performed by the PAP.

Protection: integrity

Customer Account Information

All customer bank account data including the PAN, the PAN Sequence Number, expiration date.

Protection: integrity.

PAP keys

The cryptographic keys owned by the payment application instances.

Protection: integrity and confidentiality

Application Note:

This asset includes secret keys, private keys and random numbers used for secret key generation.

PAP Transaction Parameters

Any data used for internal card risk management, including last on-line ATC, PAP AID, PDOL data, Currency code, Personal Code Entry Floor Limit, Personal Code indicators, CDOL1, CVM, PK certificates.

Protection: integrity.

PAP Selection and Activation parameters

The parameters allowing the POS to perform the selection and activation of the embedded PAP.

Protection: integrity.

Application Note:

For instance the AID, the longAID, the AFL, contactless life cycle state, etc.

3.1.2 TSF data

TSF data are data might affect the operation of the TOE.

3.1.2.1 TRANSACTION MANAGEMENT DATA

Reference Personal Code

The stored value of the Personal Code which allows the authentication of the customer to the PAP. This includes related parameters for entry checking (POS currency, Personal Code Entry Limit).

Protection: integrity and confidentiality.

PAP Counters

This asset covers two types of counters:

- risk analysis counters which is data used to count sensitive operations, for instance, the number of transactions processed by the PAP (ATC),
- secure counters such as the number of failed attempts to present the Personal Code (Personal Code Try Counter).

Protection: integrity

PAP State Machine

The PAP State Machine stores information about the PAP application internal states during its usage phase.

Protection: integrity.

3.1.2.2 TEMPORARY TRANSACTION DATA

PAP Transaction Data

All data used by the PAP when performing payment transactions, including Card Challenge, Dynamic Authentication related data, Session Keys, Card Verification Results, Cryptograms (AAC, TC and ARQC).

Protection: integrity

3.2 Users / Subjects

3.2.1 USERS

Users are entities (human or IT) outside the TOE that interact with the TOE.

U.CUSTOMER

The customer interacts with the TOE in its usage phase. The customer is able to perform a transaction using the PAP embedded in the (U)SIM card of his mobile handset.

U.ISSUING_BANK

The Issuing Bank is the PAP provider. The Issuing Bank is responsible of payment transactions authorisation and PAP administration (i.e. loading of PAP code, data and keys belonging to a specific customer).

U.MERCHANT_POS

The POS terminal used by the merchant. It initiates transactions with the PAP in the customer's mobile handset for payment of a good or a service.

U.MNO

The Mobile Network Operator is the (U)SIM Card Issuer. The MNO provides cards to the customers. The MNO is responsible for the secure management of all pre-issuance phases of the (U)SIM card life cycle status and for some post-issuance processes.

Application Note:

The MNO can provide privileges to Issuing Banks via the Delegated Management functionality. The MNO can also manage authorisation of applications permitted to reside on its (U)SIM cards.

U.APP

Any sensitive or non-sensitive application embedded in the (U)SIM card besides the PAP.

U.BANK_GUI

This is a graphical interface loaded into the mobile handset, that allows the customer to access to the functions associated to their CMP applications.

U.BANK_MNG_SW

This is the software that is in charge of establishing a secure channel with the (U)SIM to tunnel PAP management functions (loading, updating,...) and data.

U.MNO_MNG_SW

This is the software that is in charge of establishing a secure channel with the (U)SIM to tunnel MNO's management functions and data.

3.2.2 SUBJECTS

Subjects are active entities in the (U)SIM.

S.PAP

The PAP subject is the Payment Application Package.

S.BANK_TSM

The Bank TSM allows the Issuing Bank to submit PAP management operations (installation, selection, activation, block, counter reset, etc).

S.MNO_ISD

The MNO Issuer Security Domain allows the MNO to verify the Issuing Bank management operations in a Delegated Management privilege mode (token verification).

3.3 Threats

A threat agent wishes to abuse the assets by physical or logical attacks or by any other type of attacks. Any user may act as a threat agent.

3.3.1 DISCLOSURE

Unauthorised disclosure of assets.

T.DISCLOSURE_KEYS

An attacker may perform attacks leading to unauthorised knowledge of the keys.

Assets threatened: PAP keys.

T.DISCLOSURE_REF_PC

An attacker may perform attacks leading to unauthorised knowledge of the Reference Personal Code.

Assets threatened: Reference Personal Code.

3.3.2 INTEGRITY

Unauthorised modification of assets.

T.INTEG_LOG_FILE

Unauthorised modification of stored log files: an attacker modifies the log of transactions in order to hide malicious operations.

Asset threatened: PAP Log File.

T.INTEG_KEYS

Unauthorised modification of stored keys: an attacker modifies the value of the keys in order to input a known key.

Assets threatened: PAP keys.

T.INTEG_ACCOUNT_INFO

Unauthorised modification of stored customer account information: for instance an attacker modifies the value of the PAN.

Assets threatened: Customer Account Information.

T.INTEG_REF_PC

Unauthorised modification of stored Reference Personal Code: an attacker modifies the value of the Reference Personal Code stored in the PAP, for instance, in order to enter a known one.

Assets threatened: Reference Personal Code.

T.INTEG_TRANS_PARAM

Unauthorised modification of stored transactions parameters: an attacker modifies the value of transaction parameters which define the configuration of the PAP in order to bypass controls or a limitation enforced by the bank's risk management and let the PAP accepting counterfeited or replayed transactions.

Assets threatened: PAP Transaction Parameters, PAP State Machine.

T.INTEG_COUNT

Unauthorised modification of risk analysis counters or secure counters. Such as the Personal Code Try Counter stored in the TOE: an attacker modifies the value of the Personal Code Try Counter

stored in the PAP in order to change the limitation of the number of failing Personal Code required and finally gets unauthorised permission to submit a payment transaction.

Assets threatened: PAP Counters.

T.TEMPORARY_DATA

Unauthorised modification of temporary transaction data: an attacker modifies the value of transaction data in order to authorise counterfeited or replayed transactions.

Assets threatened: PAP Transaction Data, POS Transaction Data, Issuing-Bank Scripts, MNO Data, Issuing Bank Transaction Data.

T.INTEG_SEL_ACT_PARAM

Unauthorised modification of stored selection and activation parameters: an attacker modifies the value of parameters allowing the POS to perform the selection and activation of the embedded PAP in order to select and activate a counterfeited PAP.

Assets threatened: PAP Selection and Activation Parameters.

3.3.3 FRAUDULENT PAYMENT

T.STEALING

An attacker identifies and steals the mobile handset of the legitimate customer and if necessary disables the OTA channel (activating of the airplane mode, for instance) in order to use it to submit payment transactions.

Assets threatened: All assets.

T.MERCHANT_ACCOMPLICE

An attacker deals with a merchant in order to split payment into small amount payments that do not require Personal Code entry.

Assets threatened: PAP Transaction Parameters.

T.MAN-IN-THE-MIDDLE

An attacker installs on his mobile handset an application or uses a NFC device that is capable of relaying communications from the POS terminal to a mobile handset including a genuine payment application via NFC bearer or OTA bearer. The attacker presents his mobile handset or his NFC device to the POS terminal for a payment transaction, the request for payment is relayed from the POS terminal, through one or more intermediate attackers fake devices (NFC devices), to the victims mobile handset, which may be at a considerable distance.

Assets threatened: PAP Transaction parameters, PAP Counters.

T.TRANSACTION_REPUDIATION

Performing payment transactions without the customer authentication. It can lead to the repudiation of those transactions by the customer.

Assets threatened: PAP Log File and PAP Transaction Parameters.

T.TRANSACTION_COUNTERFEITING

Counterfeiting of payment transactions. This may take several forms depending on the type of the data available to the attacker:

- knowledge of all personalisation data to clone a payment application;
- knowledge of the MNOs master key or the Bank's TSM key to make a real fake payment application;
- exploiting cryptographic weaknesses to determine the keys.

Assets threatened: PAP keys, PAP Transaction Parameters, Customer Account Information, PAP Transaction Data.

T.TRANSACTION_REPLAY

Replay of a previous complete sequence of transaction operations.

Asset threatened: PAP Transaction data, POS Transaction data, Issuing Bank Transaction Data.

Application Note:

This attack may be done by exploiting cryptographic weaknesses to determine the random values used, for instance, in DDA computation and session key diversification in order to replay previous transactions and usurpate users' identities.

3.3.4 DENIAL-OF-SERVICE

T.CERTIF_CORRUPTION

Corruption of the transaction data (certificates) in order to deny participation to the transaction under the terms claimed by one party.

Assets threatened: PAP Transaction Parameters, PAP Transaction Data, POS Transaction Data.

T.APPLICATIONS_DOS

Exploiting OTA bearer or NFC bearer, an attacker initiates transactions of small amounts by simulating a POS terminal. He may also install fraudulently an application on the mobile handset (GUI) that initiates transactions with the (U)SIM card. This attack may cause denial of service on the payment applications.

Assets threatened: Issuing-Bank Scripts, MNO Data, Issuing Bank Transaction Data.

3.3.5 IDENTITY_USURPATION

T.MNO_USURPATION

An attacker is illegally granted the rights of the MNO to modify the transactions parameters in order to authorise fraudulent transactions.

Assets threatened: MNO Data.

T.ISSUING-BANK_USURPATION

An attacker is illegally granted rights of the Issuing Bank to make unauthorised PAP management operations.

Assets threatened: Issuing Bank Transaction Data.

T.CUSTOMER_USURPATION

An attacker is illegally granted the rights of the legitimate customer to submit unauthorised transactions on his/her behalf.

Assets threatened: All assets.

Application Note: Those attacks could be made by exploiting cryptographic weaknesses to determine the keys or random values used in the authentication process in order to usurpate users' identities.

3.4 Organisational Security Policies

3.4.1 HANDSET

OSP.POLICY

The mobile handset implements a security policy and a control access policy to resources ((U)SIM, network,etc)

OSP.CUSTOMER_PC_CONFID

The mobile handset never conserves the customer's Personal Code in its memory.

OSP.GUIS_IDENTIFICATION

The handset implements an access control mechanism that identifies GUIs authorised to communicate with the PAP (Cardlets).

3.4.2 MANAGEMENT

OSP.CERTIFICATES_MNGT

The lifetime of the (EMV-CDA) authentication certificates with the payment terminal varies according to the type of the payment application (application lifetime), and the (U)SIM card (lifetime). These certificates are updated via OTA during the term of the contract signed with the customer. Updating EMV certificates makes compromised payment applications inoperative.

OSP.Contactless_life cycle_MNGT

Each PAP holds the "Contactless Life Cycle State", which takes values from: ACTIVATED, DEACTIVATED, NON-ACTIVATABLE.

In a *Payez Mobile* implementation, there shall be at maximum one payment application in "ACTIVATED" state. The *Payez Mobile* application handles this requirement deactivating the previous payment application when a new one requests is activated. When the *Payez Mobile* application receives a notification from the CRS API that a payment application has just been activated, it uses the GP mechanisms as defined in the amendment C [GP-5] to deactivate the previous active payment application.

OSP.TOE_USAGE

The customer never reveals their Personal Code so that an attacker is unable to grant the rights of the legitimate customer to submit unauthorised transactions on his/her behalf. The customer shall respect the security rules given by the Issuing Bank.

OSP.PISHING

The Bank shall forbid remote payments (e.g. internet transactions), Mail Order / Telephone Order (MOTO), cash advance, quasi-cash and ATM cash withdrawal) so that an attacker cannot forge a message for the legitimate customer by usurpating his bank's identity in order to obtain desired information from him (name, address, PAN, activation code).

3.4.3 MERCHANT

OSP.MERCHANT_CONTROL

The Acquirer applies a specific security policy regarding the secure usage of the POS by the Merchant.

Application Note:

The Acquirer's role is:

- *acquires and processes clearing transaction files;*
- *forwards authorisation and clearing messages from the Merchant point of sale to the Issuing Bank through a Payment Scheme network;*
- *provides an accurate and reliable transaction flow transmission from the Merchant POS to the Issuing Bank;*
- *provides a POS terminal compliant with the Payment Scheme requirements and with the functionalities defined within the Payez Mobile specifications.*

3.4.4 BANK

OSP.BANKS_PRIVILEGES

The Issuing Bank has specific privileges. For instance:

- the ability to request the value of the ATC and Offline counters. That request should be done randomly or on response to an incident reported by the customer;
- the ability to reset offline counters through OTA bearer;
- the ability to perform complete personnalisation of its dedicated payment application through OTA bearer.

3.5 Assumptions

A.MERCHANT_AUTH

Merchant contract subscription guarantees the authenticity of the Merchant.

4 Security Objectives

4.1 Security Objectives for the TOE

4.1.1 TRANSACTION PROTECTION

O.TRANSACTION_UNIQUENESS

The TOE shall preserve the uniqueness of a transaction by limiting the probability of generating two identical copies of transactions certificates.

O.TRANSACTION_INTEGRITY

The TOE shall preserve the integrity of transactions and the integrity of all certified terms of the transactions.

O.TRANSACTION_BYPASS

The TOE shall prevent from bypassing a mandatory step of the transaction flow model as defined by the [PM-1] and [PM-2] specifications.

O.TRANSACTION_REPLAY

The TOE shall detect and reject replayed transactions.

4.1.2 AUTHENTICATION

O.USER_AUTH

The TOE shall provide customer authentication means for Personal Code change/unblock and for each payment transaction above the Personal Code Entry Limit.

Application Note:

No further customer authentication attempts shall be possible once the maximal number of attempts has been reached, until a special action is performed by a privileged user.

O.ISSUING_BANK_AUTH

The TOE shall authenticate the Issuing Bank before processing administration transactions.

O.MNO_AUTH

The TOE shall authenticate the MNO before granting him access to its services.

Handled by the (U)SIM platform (see O.COMM_AUTH in [PP USIM])

4.1.3 EXECUTION PROTECTION

The correct execution of the services provided by the PAP, applications resources control and applications isolation are handled by the (U)SIM platform on which the payment application package is embedded. They are satisfied by technical countermeasures implemented by the (U)SIM platform. [PP USIM]

O.AUTHORISATION_CONTROL

The consistency of payment transactions shall be checked according to *Payez Mobile* specifications [PM-1] and [PM-2] before granting the customer the authorisation to submit payment transactions.

4.1.4 DATA PROTECTION

O.DATA_DISCLOSURE

The TOE shall avoid unauthorised disclosure of TSF data stored and manipulated by the TOE and that must be protected in confidentiality.

Application Note:

This security objective is partially handled by the (U)SIM platform regarding physical attacks and unobservability of secrets.

O.DATA_INTEGRITY

The TOE shall avoid unauthorised modification of user data and TSF data managed or manipulated by the TOE.

O.DATA_USERS

The TOE shall ensure that user data are only accessed by authorised users.

4.1.5 RISK MANAGEMENT

O.RISK_MNGT

The TOE security functions behavior is limited by maximum values of risk management counters (number of transactions without authorisation, the aggregated amount without authorisation) that trigger an online authorisation request. These mechanisms are valid regardless the amount of the payment transaction.

O.APP_BLOCK

The TOE shall grant an authorised user the privilege to block the PAP and its data in a way to prohibit a positive response to payment authorisation requests. This is remotely operated through OTA bearer.

O.SIM_UNLOCK

The TOE shall require unlocking the (U)SIM card (by means of the PIN code) for each payment transaction.

Application Note:

Handled by the (U)SIM platform (see O.COMM_AUTH in [PP USIM])

O.AUDIT

The TOE shall record transactions to support effective security management.

O.CHANNELS

The TOE shall provide the means to identify the origin of a communication request intended to be routed by a specific communication channel (e.g. SWP for communications between the (U)SIM and the NFC Controller).

O.AUDIT_ACCESS

The TOE shall grant the customer access to log files in order to check the history of payment transactions that he has made lately.

4.1.6 GUI

O.GUIS_AUTH

The TOE ((U)SIM Platform and PAP) shall authenticate the GUIs authorised to communicate with the applications of (U)SIM card (Cardlets) before granting them access to its functionalities. The applications shall only accept communication from authenticated GUIs.

Application Note:

Handled by the (U)SIM platform (see O.APPLI_AUTH and O.COMM_AUTH in [PP USIM])

This security objective is handled by the (U)SIM platform..

4.2 Security objectives for the Operational Environment

4.2.1 HANDSET

OE.CUSTOMER_PC_CONFID

The mobile handset shall preserve the customer's Personal Code from disclosure during its transmission to the PAP in order to be compared with the Reference Personal Code. Thus, the mobile handset shall never keep the customer's Personal Code in its memory.

OE.GUI_INST_ALERT

The mobile handset shall provide mechanisms for determining the legitimacy of an installed GUI, alerting the customer on application installation attempts.

OE.TOE_USAGE

The Issuing Bank shall communicate to the customer the rules dealing with the use of the PAP. Especially it must inform the customer that he must not divulgate his Personal Code to anyone.

The customer shall enforce these rules.

OE.GUIS_IDENTIFICATION

The handset shall implement an access control mechanism that identifies GUIs authorised to communicate with the TOE (Cardlets).

OE.POLICY

The mobile handset shall implement a security policy and a control access policy to resources ((U)SIM, network,etc)

OE.NFC_PROTOCOL

The implementation of NFC protocol shall be compliant with ISO 14443. In particular, payment transactions shall be disabled beyond a given distance.

OE.TRANSACTION_DISPLAY

Related payment transaction information (amount, transaction status, etc) shall be systematically displayed on the screen of the customers mobile handset before or after the transaction.

OE.CHANNELS_SELECTION

The mobile handset shall provide the means to the customer to fix the communication channels that permit to communicate with the TOE (eg NFC, OTA, Bluetooth).

OE.GUIS_TIMEOUT

The GUIs shall detect when Personal Code Timeout limit values and unsuccessful authentication attempts occur related to the Personal Code timeout session. When the defined number of

unsuccessful authentication attempts has been surpassed, the GUI shall request the Personal Code again.

4.2.2 MERCHANT

OE.MERCHANT_CONTROL

In particular, a specific security policy shall be established by the Acquirer regarding the secure usage of the POS, by controlling the Merchants transactions flow in order to detect suspicious behavior.

Application Note:

For instance, by controlling Merchants accepting small payments amounts.

OE.MERCHANT_AUTH

The merchant shall subscribe for a contract that guarantees his authenticity.

OE.LATENCY_CONTROL

The POS terminal shall implement time-out mechanisms that disable NFC transactions with low latency.

OE.POS_APPROVAL

Payment terminals accepting *Payez Mobile* payment transactions shall be approved by a reference body.

OE.POS_APPLICATIONS

The contactless payment applications embedded in the POS terminal shall be protected in integrity and authenticity.

Application Note:

For instance, those applications are signed by a trusted third party and their signature is checked during installation process.

OE.POS_DEACTIVATION

Any POS terminal may be rendered inoperative remotely by the POS purchaser or the Acquirer.

4.2.3 MANAGEMENT

OE.CERTIFICATES_MNGT

The lifetime of the (EMV-CDA) authentication certificates with the payment terminal shall be variable according to the type of the payment application (transaction amount, application lifetime), and the (U)SIM card (lifetime). These certificates shall be updated via OTA during the term of the contract signed with the customer.

OE.Contactless_life cycle_MNGT

Upon a new activation request, *Payez Mobile* application is responsible for managing the deactivation of the current activated PAP. The *Payez Mobile* application shall guarantee that only one PAP is activated at any given time.

4.2.4 BANK

OE.NO_VAD

Remote payments (e.g. internet transactions), Mail Order / Telephone Order (MOTO), cash advance, quasi-cash and ATM cash withdrawal) shall be forbidden by the banks for PAP payments. Only proximity purchase transactions shall be authorised.

OE.BANKS_PRIVILEGES

The Issuing Bank shall be granted specific privileges.

5 Security Requirements

5.1 Security Functional Requirements

This section defines the security fonctional requirements (SFR) and the EAL. It provides the rationale between security objectives and SFRs, and the SFRs dependencies rationale.

The following two tables define the operations and security attributes involved in the Access Control and Information Control Policies for the product. The subjects, objects and information are given together with the definition of each particular policy.

Operation	Access Control SFP	Information Flow Control SFP
PAP Selection	PAP Application / PAP Activation	
PAP Activation/Deactivation - PAP Locking/Unlocking	PAP Application / PAP Administration Management	
Systematic Personal Code Activation	PAP Application / PAP Administration Management	
Personal Code Presentation for Payment	PAP Application / PAP Payment Transaction Management	
Personal Code Verification	PAP Application / PAP Payment Transaction Management	
Log Update	PAP Application / PAP Payment Transaction Management	
Log Reading	PAP Application / PAP Administration Management	
Reference Personal Code Change/Unblock	PAP Application / PAP Administration Management	
Counter Reset	PAP Application / Post-Issuance Bank Management	Post-Issuance Bank Management
Audit (Log creation)	PAP Application / Post-Issuance Bank Management	Post-Issuance Bank Management
PAP Offline Data Authentication	PAP Application / PAP Offline Authentication / PAP Transaction	PAP Offline Authentication
PAP Action Analysis	PAP Application / PAP Transaction	PAP Offline Transaction / PAP Online Transaction
PAP Offline Transaction	PAP Application / PAP Transaction	PAP Offline Transaction
PAP Online Transaction	PAP Application / PAP Transaction	PAP Online Transaction
Issuing Bank Script Processing	Post-Issuance Bank Management	Post-Issuance Bank Management

Security Attributes	Values
Contactless Life Cycle State	INSTALLED - ACTIVATED / DEACTIVATED - NON-ACTIVATABLE – LOCKED
(U)SIM Card Life Cycle Status	SELECTED / BLOCKED / NOT BLOCKED
PAP Transaction Processing State	Complies with [PM-1]&[PM-2] and indicates results of transaction processing steps / Does not comply with [PM-1]&[PM-2]
PAP Transaction Parameters Integrity	VERIFIED / NOT VERIFIED / CORRUPTED
PAP Transaction Parameters State	Issuing Bank risk management parameter value
PAP Keys Integrity	VERIFIED / NOT VERIFIED / CORRUPTED
PAP Reference Personal Code State	BLOCKED / UNBLOCKED
Systematic Personal Code State	ENABLED / DISABLED
PAP Reference Personal Code Integrity	VERIFIED / NOT VERIFIED / CORRUPTED
PAP Personal Code State	VERIFIED / NOT VERIFIED / ALWAYS REQUESTED / REQUESTED AT THE NEXT PAYMENT
PAP Personal Code Entry Amount	GREATER / LESSER THAN PERSONAL CODE ENTRY LIMIT VALUE
PAP Customer Account Information Integrity	VERIFIED / NOT VERIFIED / CORRUPTED
Log File Reading Status	PERMITTED (Log entry data is present) / NOT PERMITTED
Log File Update Status	ALLOWED / NOT ALLOWED
PAP Counters Integrity	VERIFIED / NOT VERIFIED / Corrupted
PAP Counters State	COUNTER IN RANGE / BLOCKED
PAP Selection and Activation Parameters	VERIFIED / NOT VERIFIED / CORRUPTED
Issuing Bank Transaction Data Integrity and Origin	VERIFIED / NOT VERIFIED / CORRUPTED
Issuing Bank Transaction Data Confidentiality, Integrity and Origin	VERIFIED / NOT VERIFIED / CORRUPTED
PAP Action Analysis State	Results of the PAP Action Analysis
PAP Risk Management Parameters Integrity	VERIFIED / NOT VERIFIED / CORRUPTED

5.1.1 ACCESS CONTROL POLICY

FDP_ACC.2/ PAP Application Complete access control

FDP_ACC.2.1/ PAP Application The TSF shall enforce the **PAP Application Access Control SFP** on **S.PAP, PAP State Machine** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/ PAP Application The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application Note: What follows are all operations among subjects and objects covered by this SFP:

PAP Selection
PAP Activation/Deactivation
PAP Locking/Unlocking
Systematic Personal Code Activation
Personal Code Presentation for Payment
Personal Code Verification
Log Update
Log Reading
Reference Personal Code Change/Unblock
Counter Reset
Audit
PAP Offline Data Authentication
PAP Action Analysis
PAP Offline Transaction
PAP Online Transaction
Issuing Bank Script Processing

FDP_ACC.2/ PAP Activation Complete access control

FDP_ACC.2.1/ PAP Activation The TSF shall enforce the **PAP Activation Access Control SFP** on
S.PAP;
PAP Transaction Parameters;
PAP Selection and Activation Parameters
and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/ PAP Activation The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application Note: What follows are all operations among subjects and objects covered by this SFP:

PAP Selection

FDP_ACC.2/ PAP Administration Management Complete access control

FDP_ACC.2.1/ PAP Administration Management The TSF shall enforce the **PAP Administration Management Access Control SFP** on

Subject:

S.PAP;

Objects:

PAP Selection and Activation Parameters;

PAP Log File;

PAP Keys;

PAP Counters;

Personal Code and Reference Personal Code

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/ PAP Administration Management The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application Note: What follows are all operations among subjects and objects covered by this SFP:

PAP Activation/Deactivation
PAP Locking/Unlocking
Systematic Personal Code Activation
Log Reading
Reference Personal Code Change/Unblock

FDP_ACC.2/ PAP Payment Transaction Management Complete access control

FDP_ACC.2.1/ PAP Payment Transaction Management The TSF shall enforce the **PAP Payment Transaction Management Access Control SFP** on

Subjects:

S.PAP;

S.BANK_TSM;

S.MNO_ISD;

Objects:

Personal Code;

PAP Log File,

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/ PAP Payment Transaction Management The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application Note: What follows are all operations among subjects and objects covered by this SFP:

Personal Code Presentation for Payment
Personal Code Verification
Log Update

FDP_ACC.2/ Post-Issuance Bank Management Complete access control

FDP_ACC.2.1/ Post-Issuance Bank Management The TSF shall enforce the **Post-Issuance Bank Management Access Control SFP** on

Subjects:

S.PAP;

S.BANK_TSM;

S.MNO_ISD;

Objects:

Issuing Bank Transaction Data;

Issuing Bank Scripts;

PAP Counters;

PAP Keys;

PAP Selection and Activation Parameters;

PAP Transaction Parameters;

PAP Log File

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/ Post-Issuance Bank Management The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application Note: What follows are all operations among subjects and objects covered by this SFP:

Counter Reset

Audit

Issuing Bank Script Processing

FDP_ACC.2/ PAP Offline Authentication Complete access control

FDP_ACC.2.1/ PAP Offline Authentication The TSF shall enforce the **PAP Offline Authentication control access SFP** on

Subject:

S.PAP;

Objects:

PAP Keys;

PAP Transaction Parameters;

PAP State Machine

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/ PAP Offline Authentication The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application Note: What follows are all operations among subjects and objects covered by this SFP:

PAP Offline Data Authentication

FDP_ACC.2/ PAP Transaction Complete access control

FDP_ACC.2.1/ PAP Transaction The TSF shall enforce the **PAP Transaction Access Control SFP** on

Subject:

S.PAP;

Objects;

Customer Account Information;

PAP Counters;

PAP Keys;

PAP State Machine;

PAP Transaction Parameters

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/ PAP Transaction The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application Note: What follows are all operations among subjects and objects covered by this SFP:

PAP Offline Data Authentication
PAP Action Analysis
PAP Offline Transaction
PAP Online Transaction

PAP Transaction processing is defined by above operations.

5.1.2 ACCESS CONTROL FUNCTIONS

FDP_ACF.1/ PAP Application Security attribute based access control

FDP_ACF.1.1/ PAP Application The TSF shall enforce the **PAP Application Access Control SFP** to objects based on the following:

Security attributes of the object PAP State Machine:

Contactless Life Cycle State;

(U)SIM Card Life Cycle Status.

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

PAP operations are allowed only if the:

Contactless Life Cycle State is ACTIVATED or DEACTIVATED;

(U)SIM Card Life Cycle Status is NOT BLOCKED.

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

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

If one of the conditions listed in FDP_ACF.1.2 is not fulfilled.

FDP_ACF.1/ PAP Activation Security attribute based access control

FDP_ACF.1.1/ PAP Activation The TSF shall enforce the **PAP Activation Access Control SFP** to objects based on the following:

Security attributes of the subject S.PAP:

Contactless Life Cycle State;

Security attributes of the object PAP Selection and Activation Parameters:

PAP Selection and Activation Parameters;

Security attributes of the object PAP Transaction Parameters:

PAP Transaction Parameters Integrity.

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

Selection is allowed only if:

Contactless Life Cycle State is INSTALLED;

PAP Selection and Activation Parameters is allowed only if:

PAP Selection and Activation Parameters is VERIFIED;

PAP Transaction Parameters is allowed only if:

PAP Transaction Parameters Integrity is VERIFIED.

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

None.

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

If one of the conditions listed in FDP_ACF.1.2 and FDP_ACF.1.3 is not fulfilled.

FDP_ACF.1/ PAP Administration Management Security attribute based access control

FDP_ACF.1.1/ PAP Administration Management The TSF shall enforce the **PAP Administration Management Access Control SFP** to objects based on the following:

Security attributes of the object Personal Code and Reference Personal Code:

PAP Reference Personal Code State;

PAP Reference Personal Code Integrity;

PAP Personal Code State;

Security attributes of the subject S.PAP:

Contactless Life Cycle State;

Security attributes of the object PAP Log File:

Log File Reading Status;

Security attributes of the object PAP Keys:

PAP Keys Integrity;

Security attributes of the object PAP Counters:

PAP Counters Integrity;

PAP Counters State.

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

Systematic Personal Code Activation/Deactivation is allowed only if:

PAP Reference Personal Code Integrity is VERIFIED;

PAP Personal Code State is VERIFIED;

Reference Personal Code Change/Unblock is allowed only if:

PAP Reference Personal Code Integrity is VERIFIED;

PAP Personal Code State is VERIFIED;

PAP Reference Personal Code State is UNBLOCKED;

Log Reading is allowed only if:

Contactless Life Cycle State is ACTIVATED or DEACTIVATED;

Log File Reading Status is PERMITTED (Log entry data is present);

PAP Activation/Deactivation is allowed only if:

Contactless Life Cycle State is ACTIVATED or DEACTIVATED;

PAP Reference Personal Code State Integrity is VERIFIED;

PAP Personal Code State is VERIFIED;

PAP Locking/Unlocking is allowed only if:

PAP (Issuing Bank) Keys Integrity is VERIFIED;

PAP (Issuing Bank secure script) Counters Integrity is VERIFIED;

PAP (Issuing Bank secure script) Counters State is NOT BLOCKED.

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

FDP_ACF.1.4/ PAP Administration Management The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **following rule:**

If one of the conditions listed in FDP_ACF.1.2 is not fulfilled.

FDP_ACF.1/ PAP Payment Transaction Management Security attribute based access control

FDP_ACF.1.1/ PAP Payment Transaction Management The TSF shall enforce the **PAP Payment Transaction Management Access Control SFP** to objects based on the following:

Security attributes of the object Personal Code:

PAP Reference Personal Code State;

PAP Reference Personal Code Integrity;

PAP Personal Code State;

PAP Personal Code Entry Amount;

Systematic Personal Code State;

Security attributes of the object PAP Log File:

Log File Update Status.

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

Personal Code Verification is allowed only if:

PAP Reference Personal Code State is UNBLOCKED;

PAP Reference Personal Code Integrity is VERIFIED;

Personal Code Presentation for Payment is requested only if:

PAP Personal Code State is NOT VERIFIED (by the Bank's GUI) or ALWAYS REQUESTED or REQUESTED AT THE NEXT PAYMENT;

PAP Personal Code Entry Amount is GREATER THAN PERSONAL CODE ENTRY LIMIT VALUE or the Systematic Personal Code State is ENABLED;

PAP Log File is allowed for all transactions besides those of Post-Issuance Bank Management (only during payment transactions):

Log File Update Status is ALLOWED

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

FDP_ACF.1.4/ PAP Payment Transaction Management The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **following rule:**

If one of the conditions listed in FDP_ACF.1.2 is not fulfilled.

FDP_ACF.1/ Post-Issuance Bank Management Security attribute based access control

FDP_ACF.1.1/ Post-Issuance Bank Management The TSF shall enforce the **Post-Issuance Bank Management Access Control SFP** to objects based on the following:

Security attributes of the object PAP Keys:

PAP Keys Integrity;

Security attributes of the object PAP Counters:

PAP Counters Integrity;

PAP Counters State;

Security attributes of the object PAP Transaction Parameters:

PAP Transaction Parameters Integrity;

Security attributes of the object Issuing Bank Transaction Data:

Issuing Bank Transaction Data Integrity and Origin;

Issuing Bank Transaction Data Confidentiality, Integrity and Origin.

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

Post-Issuance Bank Management operations are allowed only if:

PAP (Issuing Bank) Keys Integrity is VERIFIED;
PAP (Issuing Bank secure script) Counters Integrity is VERIFIED;
PAP (Issuing Bank secure script) Counters State is NOT BLOCKED;
Issuing Bank Transaction Data Integrity and Origin is VERIFIED;
Issuing Bank Transaction Data Confidentiality, Integrity and Origin is VERIFIED;
PAP Transaction Parameters Integrity is VERIFIED;

FDP_ACF.1.3/ Post-Issuance Bank Management The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **None**.

FDP_ACF.1.4/ Post-Issuance Bank Management The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **following rule:**
If one of the conditions listed in FDP_ACF.1.2 is not fulfilled.

FDP_ACF.1/ PAP Offline Authentication Security attribute based access control

FDP_ACF.1.1/ PAP Offline Authentication The TSF shall enforce the **PAP Offline Authentication Access Control SFP** to objects based on the following:
Security attributes of the subject S.PAP:
Contactless Life Cycle State;
(U)SIM Card Life Cycle Status;
Security attributes of the object PAP State Machine:
PAP Transaction Processing State;
Security attributes of the object PAP Keys:
PAP Keys Integrity;
Security attributes of the object PAP Transaction Parameters:
PAP Transaction Parameters State;
PAP Transaction Parameters Integrity.

FDP_ACF.1.2/ PAP Offline Authentication The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
PAP Offline Data Authentication is allowed only if:
(U)SIM Card Life Cycle Status is SELECTED;
Contactless Life Cycle State is ACTIVATED;
PAP Transaction Processing State complies with Transaction Flow;
PAP Keys Integrity is VERIFIED;
PAP Transaction Parameters Integrity is VERIFIED;
PAP Transaction Parameters State indicates a dynamic authentication process.

FDP_ACF.1.3/ PAP Offline Authentication The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **None**.

FDP_ACF.1.4/ PAP Offline Authentication The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **following rule:**
If one of the conditions listed in FDP_ACF.1.2 is not fulfilled.

FDP_ACF.1/ PAP Transaction Security attribute based access control

FDP_ACF.1.1/ PAP Transaction The TSF shall enforce the **PAP Transaction Access Control SFP** to objects based on the following:

Security attributes of the object PAP State Machine:

PAP Transaction Processing State;

Security attributes of the subject S.PAP:

Contactless Life Cycle State;

Security attributes of the object PAP Counters:

PAP Counters Integrity;

Security attributes of the object PAP Keys:

PAP Keys Integrity;

Security attributes of the object Customer Account Information:

PAP Customer Account Information Integrity (PAN integrity);

Security attributes of the object PAP Transaction Parameters:

PAP Transaction Parameters Integrity.

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

PAP Transaction processing is allowed only if:

(U)SIM Card Life Cycle Status is SELECTED;

Contactless Life Cycle State ACTIVATED;

PAP Transaction Processing State complies with Transaction Flows;

PAP Counters Integrity is VERIFIED;

PAP Counters State is not BLOCKED;

PAP Customer Account Information Integrity is VERIFIED;

PAP Risk Management Parameters Integrity is VERIFIED;.

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

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

If one of the conditions listed in FDP_ACF.1.2 is not fulfilled.

5.1.3 INFORMATION FLOW CONTROL POLICY

FDP_IFC.2/ PAP Offline Authentication Complete information flow control

FDP_IFC.2.1/ PAP Offline Authentication The TSF shall enforce the **PAP Offline Authentication information flow control SFP** on

Subjects:

S.PAP;

Information:

PAP Transaction Parameters;

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/ PAP Offline Authentication 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.

Application Note: What follows are all operations among subjects and objects covered by this SFP:

PAP Offline Data Authentication

FDP_IFC.2/ PAP Offline Transaction Complete information flow control

FDP_IFC.2.1/ PAP Offline Transaction The TSF shall enforce the **PAP Offline Transaction Information Flow Control SFP** on

Subject:

S.PAP;

Information:

PAP Transaction Parameters;

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/ PAP Offline Transaction 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.

Application Note: What follows are all operations among subjects and objects covered by this SFP:

PAP Action Analysis
PAP Offline Transaction

FDP_IFC.2/ PAP Online Transaction Complete information flow control

FDP_IFC.2.1/ PAP Online Transaction The TSF shall enforce the **PAP Online Transaction information flow control SFP** on

Subject:

S.PAP;

Information:

PAP Transaction Parameters;

Issuing Bank Transaction Data

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/ PAP Online Transaction 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.

Application Note: What follows are all operations among subjects and objects covered by this SFP:

PAP Action Analysis
PAP Online Transaction

FDP_IFC.2/ Post-Issuance Bank Management Complete information flow control

FDP_IFC.2.1/ Post-Issuance Bank Management The TSF shall enforce the **Post-Issuance Bank Management information flow control SFP** on

Subject:

S.PAP;

Information:

Issuing Bank Transaction Data;

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/ Post-Issuance Bank Management 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.

Application Note: What follows are all operations among subjects and objects covered by this SFP:

Counter Reset
Audit
Issuing Bank Script Processing

FDP_IFF.1/ PAP Offline Authentication Simple security attributes

FDP_IFF.1.1/ PAP Offline Authentication The TSF shall enforce the **PAP Offline Authentication information flow control SFP** based on the following types of subject and information security attributes:

Security Attributes of the subject S.PAP:

Contactless Life Cycle State;

Security Attributes of the information PAP Transaction Parameters:

PAP Transaction Parameters State.

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

S.PAP is the currently selected application;

Contactless Life Cycle State is ACTIVATED;

PAP Transaction Parameters State requires dynamic authentication.

FDP_IFF.1.3/ PAP Offline Authentication The TSF shall enforce the **following rules: none**.

FDP_IFF.1.4/ PAP Offline Authentication The TSF shall explicitly authorise an information flow based on the following rules: **None**.

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

If one of the conditions listed in FDP_IFF.1.2 is not fulfilled.

FDP_IFF.1/ PAP Offline Transaction Simple security attributes

FDP_IFF.1.1/ PAP Offline Transaction The TSF shall enforce the **PAP Offline Transaction information flow control SFP** based on the following types of subject and information security attributes:

Security Attributes of the subject S.PAP:

Contactless Life Cycle State;

PAP Action Analysis State;

Security Attributes of the information PAP Transaction Parameters:

PAP Transaction Processing State.

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

S.PAP is the currently selected application;

Contactless Life Cycle State is ACTIVATED;

PAP Transaction Processing State complies with [PM-1] & [PM-2];

PAP Action Analysis State requires offline processing;

PAP Action Analysis State does not reject the transaction.

FDP_IFF.1.3/ PAP Offline Transaction The TSF shall enforce the **following rules: None**.

FDP_IFF.1.4/ PAP Offline Transaction The TSF shall explicitly authorise an information flow based on the following rules: **none**.

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

If one of the conditions listed in FDP_IFF.1.2 is not fulfilled.

FDP_IFF.1/ PAP Online Transaction Simple security attributes

FDP_IFF.1.1/ PAP Online Transaction The TSF shall enforce the **PAP Online Transaction information flow control SFP** based on the following types of subject and information security attributes:

Security Attributes of the subject S.PAP:

Contactless Life Cycle State;

PAP Action Analysis State;

Security Attributes of the information PAP Transaction parameters:

PAP Transaction Processing State;

Security Attributes of the information Issuing Bank Transaction data:

Issuing Bank Transaction Data Integrity and Origin;

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

S.PAP is the currently selected application;

Contactless Life Cycle is ACTIVATED;

PAP Transaction Processing State complies with [PM-1] & [PM-2];

PAP Action Analysis State requires online processing;

PAP Action Analysis State does not reject the transaction;

Issuing Bank Transaction Data Integrity and Origin is VERIFIED;

FDP_IFF.1.3/ PAP Online Transaction The TSF shall enforce the **following rules: None**.

FDP_IFF.1.4/ PAP Online Transaction The TSF shall explicitly authorise an information flow based on the following rules: **None**.

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

If one of the conditions listed in FDP_IFF.1.2 is not fulfilled.

FDP_IFF.1/ Post-Issuance Bank Management Simple security attributes

FDP_IFF.1.1/ Post-Issuance Bank Management The TSF shall enforce the **Post-Issuance Bank Management information flow control SFP** based on the following types of subject and information security attributes:

Security Attributes of the subject S.PAP:

Contactless Life Cycle State;

Security Attributes of the information Issuing Bank Transaction Data:

Issuing Bank Transaction Data Confidentiality, Integrity and Origin.

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

S.PAP is the currently selected application;

Contactless Life Cycle is ACTIVATED or DEACTIVATED;

PAP Action Analysis State does not reject the transaction;

Issuing Bank Transaction Data Confidentiality, Integrity and Origin is VERIFIED.

FDP_IFF.1.3/ Post-Issuance Bank Management The TSF shall enforce the **following rules: None**.

FDP_IFF.1.4/ Post-Issuance Bank Management The TSF shall explicitly authorise an information flow based on the following rules: **None**.

FDP_IFF.1.5/ Post-Issuance Bank Management The TSF shall explicitly deny an information flow based on the following rules:

If one of the conditions listed in FDP_IFF.1.2 is not fulfilled.

5.1.4 SECURITY AUDIT

FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take **one of the following actions:**

locking the PAP;

blocking or terminating the (U)SIM card session (muting the (U)SIM card);

reinitializing secret data;

bringing the (U)SIM card to a secure state;

temporary disabling the services of the PAP until a privileged role performs a special action;

definitely disabling all the services of the PAP

upon detection of a potential security violation.

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of **the following auditable events:**

unauthorised use of the PAP services;

unauthorised read or modification of the PAP sensitive assets protected in integrity and confidentiality;

unauthorised modification of the PAP sensitive assets protected in integrity;

PAP Selection failure;

PAP Activation failure;

PAP Services failure

known to indicate a potential security violation;

b) **No other rules**.

FAU_GEN.1 Audit data generation

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 **not specified** level of audit; and

c) **The following auditable events:**

Payment transactions;

Application Note: **c) the Payment transactions auditable events are given in FAU_SAA.1.2.**

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 event definitions of the functional components included in the PP/ST.

Application Note: In the context of Payment transactions,

- Date/time is logged only for accepted/rejected transaction. For online transaction, date/time will not record.
- The only type of event is payment transaction.
- The records are given in FAU_SAR.1/CUSTOMER and FAU_SAR.1/ISSUING_BANK

FAU_SAR.1/CUSTOMER Audit review

FAU_SAR.1.1/CUSTOMER The TSF shall provide **U.CUSTOMER** with the capability to read **the following audit information:**

Purchase Amount;

Purchase Currency;

Transaction Date;

Cryptogram Information Data;

Application Transaction Counter;

Card Verification Results

from the audit records.

FAU_SAR.1.2/CUSTOMER The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.1/ISSUING_BANK Audit review

FAU_SAR.1.1/ISSUING_BANK The TSF shall provide **U.ISSUING_BANK** with the capability to read **all available information** from the audit records.

FAU_SAR.1.2/ISSUING_BANK The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.5 CRYPTOGRAPHIC SUPPORT

FCS_CKM.1/Session Keys Cryptographic key generation

FCS_CKM.1.1/Session Keys The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **PAP Session Keys Derivation** and specified cryptographic key sizes **16 bytes** that meet the following: **[PM-1] and [PM-2] standard**.

FCS_CKM.4/Session Keys Cryptographic key destruction

FCS_CKM.4.1/Session Keys The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **(clearKey() method)** that meet the following: **[JCAPI222]**.

Application Note:

- Same SFR than platform one.

FCS_COP.1/Offline Data Authentication Cryptographic operation

FCS_COP.1.1/Offline Data Authentication The TSF shall perform **Signature operation** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **176 bytes** that meet the following: **[PM-1] and [PM-2] specification**.

FCS_COP.1/Application Cryptogram Cryptographic operation

FCS_COP.1.1/Application Cryptogram The TSF shall perform **MAC CBC cryptogram generation** in accordance with a specified cryptographic algorithm **3DES** and cryptographic key sizes **16 bytes** that meet the following: **[PM-1] and [PM-2] specifications**.

FCS_COP.1/Script Processing Cryptographic operation

FCS_COP.1.1/Script Processing The TSF shall perform **Cryptogram generation** in accordance with a specified cryptographic algorithm **3DES** and cryptographic key sizes **16 bytes** that meet the following: **[PM-1] and [PM-2] specifications**.

FCS_COP.1/Messages Data Integrity Cryptographic operation

FCS_COP.1.1/Messages Data Integrity The TSF shall perform **MAC Computation** in accordance with a specified cryptographic algorithm **3DES** and cryptographic key sizes **16 bytes** that meet the following: **[PM-1] and [PM-2] specifications**.

FCS_COP.1/Messages Data Confidentiality Cryptographic operation

FCS_COP.1.1/Messages Data Confidentiality The TSF shall perform **Encipherment** in accordance with a specified cryptographic algorithm **3DES** and cryptographic key sizes **16 bytes** that meet the following: **[PM-1] and [PM-2] specifications**.

5.1.6 PROTECTION

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for **corruption** on all objects, based on the following attributes:

all stored Transaction management data;

all stored Temporary data during transaction processing integrity;

all stored Temporary data during Post-Issuance Bank Management.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall

deactivate and lock the PAP;

or Mute the (U)SIM card;

or Clear secret data;

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests **at the conditions: before PAP application usage** to demonstrate the correct operation of: **PAP application**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of: **Transaction Management Data (TSF persistent data)**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of: **PAP application code**.

Application Note:

- This is not TSF's self-tests but points are covered by SFRs of the platform to verify the integrity of persistent data and to verify the integrity of PAP application code during loading, and then covered by the composition with the platform.
- This **FPT_TST.1** is not useful to cover the security objectives of this document because already covered by FDP SFRs, but writen here according to [PAP].

FPT_RPL.1 Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: **Issuer Scripts and VERIFY commands** .

FPT_RPL.1.2 The TSF shall perform **reject the replay and increase counter** when replay is detected.

Application Note:

- ***if attack replay Issuer Scripts like PIN CHANGE UNBLOCK / APPLICATION UNBLOCK / UPDATE RECORD etc, the replay will be rejected and SMI counter will be increased***
- ***if attack replay VERIFY (PIN) Enciphered command which he sniffed from line, the replay will be rejected and Bad Crypto Counter will be increased***

FDP_RIP.1 Subset residual information protection

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

PAP Reference Personal Code;

PAP Personal Code;

PAP Keys.

Application Note:

- The PAP Reference Personal Code is created during personalization and cleared during reset personalization

5.1.7 MANAGEMENT

FMT_SMF.1/ Functionalities Specification of Management Functions

FMT_SMF.1.1/ Functionalities The TSF shall be capable of performing the following management functions:

Post-Issuance Bank Management (issuing-bank scripts);

Communication channels selection;

OTA Issuance Management (TSM can install the MPP instance over the air and personalize the installed instance over the air too);

Customer personal parameter setup (Customer can setup some personal parameters in MPP via MIDlet).

Application Note:

- The communication channels selection is to be considered as a way to identify the origin by determining the contact or contactless protocol.

FMT_MOF.1/ Parameters Management of security functions behaviour

FMT_MOF.1.1/ Parameters The TSF shall restrict the ability to **disable, enable and modify the behaviour of** the functions

PAP Selection;

PAP Activation/Deactivation;

PAP Offline Data Authentication;

PAP Offline Transaction;

PAP Online Transaction;

Personal Code Verification

to **the Issuing Bank**.

FMT_MTD.1/ Secrets Management of TSF data

FMT_MTD.1.1/ Secrets The TSF shall restrict the ability to **modify** the **PAP TSF data (all)** to **the Issuing Bank**.

FMT_MSA.1/ Issuing Bank Management of security attributes

FMT_MSA.1.1/ Issuing Bank The TSF shall enforce the **Post-Issuance Bank Management Access Control SFP and Post-Issuance Bank Management Information Control SFP** to restrict the ability to **modify** the security attributes **all the PAP security attributes** to **the Issuing Bank**.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for **security attributes defined in PAP Transaction Access Control SFP and PAP Offline Transaction, PAP Online Transaction Information Control SFP**.

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **following SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

SFPs are:

- **Post-Issuance Bank Management Access Control SFP/ Information Control SFP**
- **PAP Application Access Control SFP**
- **PAP Activation Access Control SFP**
- **PAP Administration Management Access Control SFP**
- **PAP Payment Transaction Management Access Control SFP**
- **PAP Offline Authentication Access Control SFP/Information Control SFP**
- **PAP Transaction Access Control SFP**
- **PAP Offline Transaction Information Control SFP**
- **PAP Online Transaction Information Control SFP**

FMT_MSA.3.2 The TSF shall allow the **Issuing Bank and MNO** to specify alternative initial values to override the default values when an object or information is created.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

Customer;

Issuing Bank;

MNO.

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

5.1.8 IDENTIFICATION / AUTHENTIFICATION

FIA_AFL.1/ Customer Authentication failure handling

FIA_AFL.1.1/ Customer The TSF shall detect when **Personal Code Try Counter Limit** unsuccessful authentication attempts occur related to **the Personal Code Verification**.

FIA_AFL.1.2/ Customer When the defined number of unsuccessful authentication attempts has been **surpassed**, the TSF shall

return an error, as specified in [PM-1] and [PM-2];

block the PAP Reference Personal Code until the Issuing Bank unblocks it.

Application Note:

- The Personal Code Try Counter Limit is created during personalization

FIA_AFL.1/ Issuing Bank Authentication failure handling

FIA_AFL.1.1/ Issuing Bank The TSF shall detect when **an administrator configurable positive integer within range of acceptable values** unsuccessful authentication attempts occur related to **Issuing Bank Authentication**.

FIA_AFL.1.2/ Issuing Bank When the defined number of unsuccessful authentication attempts has been **surpassed**, the TSF shall

return an error as specified in [GP-4].

Application Note: The range of values is 1~FFFFh.

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

Personal Code Verification Security Attributes (PAP Transaction Parameters);

Issuing Bank Authentication Security Attributes (PAP Transaction Parameters).

FIA_UAU.1/ PAP Online Transaction Timing of authentication

FIA_UAU.1.1/ PAP Online Transaction The TSF shall allow

PAP Action analysis;

establishment of a trusted path dedicated to the current payment transaction

on behalf of the user to be performed before the user is authenticated.

Refinement: "User authentication" stands for the authentication using the Personal Code of the PAP.

FIA_UAU.1.2/ PAP Online Transaction The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/ Post-Issuance Bank Management Timing of authentication

FIA_UAU.1.1/ Post-Issuance Bank Management The TSF shall allow

selecting a PAP on the (U)SIM card;

requesting data that identifies the Issuing Bank;

establishment of a trusted path dedicated to the Post-Issuance Bank Management

on behalf of the user to be performed before the user is authenticated.

Refinement:"User authentication" stands for the authentication using the Personal Code.

FIA_UAU.1.2/ Post-Issuance Bank Management The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/ Payment Transaction Timing of authentication

FIA_UAU.1.1/ Payment Transaction The TSF shall allow **all operations except payment transactions** on behalf of the user to be performed before the user is authenticated.

Refinement:"User authentication" stands for the authentication of the user to the (U)SIM card by mean of the PAP PIN code.

FIA_UAU.1.2/ Payment Transaction The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: This authentication shall be handled by the (U)SIM platform. The PAP shall be able to verify the state of the customer authentication by the (U)SIM platform.

FIA_UAU.3 Unforgeable authentication

FIA_UAU.3.1 The TSF shall **detect** use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall **detect** use of authentication data that has been copied from any other user of the TSF.

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

PAP Offline Data Authentication;

PAP Issuing Bank and MNO Authentication.

FIA_UAU.6/ Customer Re-authenticating

FIA_UAU.6.1/ Customer The TSF shall re-authenticate the user under the conditions**:**

- Pre-enter PIN not allowed by issuer (depends on issuer configuration)
- Transaction Context conflict
- After completion of one payment transaction (depends on issuer configuration and card holder option)
- After card reset
- Upon reception of SET-RESET-PARAMETERS with P1P2=Reset CVM

FIA_UID.1/ PAP Online Transaction Timing of identification

FIA_UID.1.1/ PAP Online Transaction The TSF shall allow **all TSF-mediated actions listed in FIA_UAU.1/PAP Online Transaction** on behalf of the user to be performed before the user is identified.

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

FIA_UID.1/ Post-Issuance Bank Management Timing of identification

FIA_UID.1.1/ Post-Issuance Bank Management The TSF shall allow **all TSF-mediated actions listed in FIA_UAU.1/ Post-Issuance Bank Management** on behalf of the user to be performed before the user is identified.

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

FIA_UID.1/ Payment Transaction Timing of identification

FIA_UID.1.1/ Payment Transaction The TSF shall allow **all TSF-mediated actions listed in FIA_UAU.1/ Payment Transaction** on behalf of the user to be performed before the user is identified.

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

FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

PAP Transaction Parameters State.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

PAP Transaction Parameters State initially indicates no identification/authentication of the user.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **none**.

FIA_SOS.2 TSF Generation of secrets

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet **the STANDARD level as specified in platform (refer to** [DCSSI2741]).

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for **the generation of the 8-bytes challenge used for cryptographic operations**.

Refinement: "secrets" stand for random values.

Application Note: The 8-bytes challenge is generated from Applicative Get Challenge from Platform Javacard API javacard.security.RandomData.generateData.

FDP_DAU.1 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **the following objects and information:**

Contactless Life Cycle;
(U)SIM Life Cycle Status;
PAP Code;
PAP Selection and Activation Parameters;
PAP Transaction Parameters;
PAP Keys;
Reference Personal Code;
PAP Log File;
PAP Counters;
PAP Customer Account Information.

FDP_DAU.1.2 The TSF shall provide **S.PAP** with the ability to verify evidence of the validity of the indicated information.

Application Note: This **FDP_DAU.1** is not appropriate but writen here according to [PAP]. This SFR has to be used as integrity control.

5.1.9 ACCESS and INFORMATION FLOW CONTROL SFP

FDP_ITC.2/ Post-Issuance Bank Management Import of user data with security attributes

FDP_ITC.2.1/ Post-Issuance Bank Management The TSF shall enforce the **Post-Issuance Bank Management Access Control and the Post-Issuance Bank Management Information Flow Control SFPs** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/ Post-Issuance Bank Management The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/ Post-Issuance Bank Management 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/ Post-Issuance Bank Management 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/ Post-Issuance Bank Management The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

the Issuing Bank Transaction Parameters are verified in origin and integrity (and confidentiality if required) following [PM-1] and [PM-2] specifications.

FDP_ITC.2/ PAP Transaction Import of user data with security attributes

FDP_ITC.2.1/ PAP Transaction The TSF shall enforce the **PAP Transaction Access Control and the PAP Online Transaction Information Flow Control SFPs** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/ PAP Transaction 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/ PAP Transaction 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/ PAP Transaction The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

the Issuing Bank Transaction Data are verified in origin and integrity (and confidentiality if required) following [PM-1] and [PM-2] specifications.

FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the **TOE's Access Control and Information Flow Control SFPs (all)** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes

FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the **Access Control and Information Flow Control SFPs (all except those enforced in FDP_ITC.2/ Post-Issuance Bank Management and FDP_ITC.2/ PAP Transaction)** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **None**.

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the **PAP Offline Transaction, PAP Online Transaction and the Post-Issuance Bank Management Information Flow Control SFPs** to **receive** user data in a manner protected from **replay, insertion, deletion and modification** errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion and replay** has occurred.

5.1.10 SECURE CHANNEL

FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **the following TSF data types** when shared between the TSF and another trusted IT product.

The TSF data types are:

- **PAP Reference Personal Code State**
- **PAP Counters Integrity and PAP Counters State**
- **Contactless Life Cycle State**
- **PAP Transaction processing State and Issuing Bank Transaction Data Confidentiality (if required), Integrity and Origin**

FPT_TDC.1.2 The TSF shall use **the rules defined in [PM-1]&[PM-2]** when interpreting the TSF data from another trusted IT product.

FTP_ITC.1 Inter-TSF trusted channel

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

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for

PAP Online Transaction;

Post-Issuance Bank Management.

5.1.11 UNOBSERVABILITY

FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF shall ensure that **all users and subjects** are unable to observe the operation **PIN comparison and key comparison** on **the Reference Personal Code and the PAP keys performed** by **S.PAP**.

5.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

6 TOE Summary Specification

This section defines the summary specification

The F.REACTION function allows to:

- Manage the policy of attack reaction according to the security violations (FAU_ARP.1, FAU_SAA.1)
- Manage the audit generation and review (FAU_GEN.1, FAU_SAR.1/CUSTOMER, FAU_SAR.1/ISSUING-BANK)
- Manage the automatic self-tests (FPT_TST.1)

The F.CRYPTO_OPERATION function allows to:

- Manage the creation and deletion of cryptographic keys (FCS_CKM.1/Session Keys, FCS_CKM.4/Session Keys)
- Manage the cryptographic operations (FCS_COP.1/Offline Data Authentication, FCS_COP.1/Application Cryptogram, FCS_COP.1/Script Processing, FCS_COP.1/Message Data Integrity and FCS_COP.1/Message Data Confidentiality)
- Manage the generation of secrets (FIA_SOS.2)

The F.ACCESS-AND-FLOW_CONTROL function allows to:

- Manage the access control and rules (FDP_ACC.2/PAP Application, FDP_ACF.1/PAP Application) for following operations:
    - SELECT
    - SET STATUS
    - APPLICATION-BLOCK and APPLICATION-UNBLOCK
    - VERIFY
    - GENERATE AC
    - READ RECORD
    - PIN CHANGE-UNBLOCK and OFFLINE CHANGE-PIN
    - COUNTER RESET
    - PUT DATA
    - UPDATE RECORD

  throw:
    - FDP_ACC.2/PAP Activation and FDP_ACF.1/PAP Activation
    - FDP_ACC.2/PAP Administration Management and FDP_ACF.1/PAP Administration Management
    - FDP_ACC.2/PAP Payment Transaction Management and FDP_ACF.1/PAP Payment Transaction Management
    - FDP_ACC.2/Post-Issuance Bank Management and FDP_ACF.1/Post-Issuance Bank Management

- Manage the information flow control and rules for following operations:
    - READ RECORD, GENERATE AC (FDP_IFC.2/PAP Offline Authentication, FDP_IFF.1/PAP Offline Authentication, FDP_IFC.2/PAP Offline Transaction, FDP_IFF.1/PAP Offline Transaction, FDP_IFC.2/PAP Online Transaction, FDP_IFF.1/PAP Online Transaction)
    - APPLICATION-, APPLICATION-UNBLOCK, PUT DATA, UPDATE RECORD, PIN CHANGE-UNBLOCK (FDP_IFC.2/Post-Issuance Bank Management, FDP_IFF.1/Post-Issuance Bank Management)

The F.DATA-IMPORT_EXPORT function allows to:

- Manage the import of data protected in term of integrity or confidentiality (FDP_ITC.2/Post-Issuance Bank Management, FDP_ITC.2/PAP Transaction,)
- Manage the export of data protected in term of integrity or confidentiality (FDP_ETC.1, FDP_ITC.1)

The F.CUSTOMER-AUTHENTICATION function allows to:

- Manage the customer authentication (FIA_AFL.1/Customer, FIA_ATD.1, FIA_UAU.6/Customer, FIA_USB.1)

The F.ISSUING-BANK-AUTHENTICATION function allows to:

- Manage the issuing-bank authentication (FIA_AFL.1/Issuing Bank, FIA_UAU.1/PAP Online Transaction, FIA_UAU.1/Post-Issuance Bank Management, FIA_UAU.1/Payment Transaction, FIA_UAU.3, FIA,UAU.4, FIA_UID.1/PAP Online Transaction, FIA_UID.1/Post-Issuance Bank Management, FIA_UID.1/Payment Transaction, FIA_USB.1)

The F.PROTECTION function allows to:

- Management (FMT_SMF.1, FMT_SMR.1)
- Manage the integrity or confidentiality of User data and TSF data that required integrity or confidentiality (FDP_DAU.1, FDP_SDI.2, FDP_UIT.1, FMT_MOF.1/Parameters, FMT_MTD.1/Secrets, FMT_MSA.1/Issuing Bank, FMT_MSA.2, FMT_MSA.3, FPT_TDC.1)
- Manage the replay detection (FDP_RPL.1)
- Manage the residual information protection (FDP_RIP.1)
- Manage the secure communication channel (FPT_ITC.1)
- Manage Reference Personal Code and PAP Keys unoservability (FPR_UNO.1)

END OF THE DOCUMENT