ALCHEMY – Public Security Target

VMPA 1.4.2 - OT v1.0 on NFC FlyBuy Platinum v2.0 on ST33F1ME

Legal Notice

Specifications and information are subject to change without notice.

The products described in this document are subject to continuous development and improvement.

All trademarks and service marks referred to herein, whether registered or not in specific countries, are the properties of their respective owners.

*** Printed versions of this document are uncontrolled ***

Table of contents

List of tables

List of figures

1 SECURITY TARGET INTRODUCTION

1.1 Scope of the document

This document describes the Security Target for the PAP application VISA mobile version 1.0.

This security target is based on the security requirements for mobile contactless proximity payments [75] [76].

The objectives of this Security Target are:

- To describe the Target of Evaluation (TOE), its life cycle and to position it into the smart card life cycle
- To describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by the operational environment during the platform active phases
- To describe the security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of sensitive information. It includes protection of the TOE (and its documentation) during the platform active phases
- To specify the security requirements which include the TOE functional requirements, the TOE assurance requirements and the security requirements for the environment
- To describe the summary of the TOE specification including a description of the security functions and assurance measures that meet the TOE security requirements
- To present evidence that this ST is a complete and cohesive set of requirements that the TOE provides on an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements

This document written from the AEPM's Guidance for Payment Application Package Security Target [78], provides a list of security requirements for a Payment Application Package (PAP) embedded in a Oberthur (U)SIM card as specified in PAP specifications [[75][76][77][79][80][81][82]].

This document is the Security Target for the Mobile VISA VMPA 1.4.2 on NFC FlyBuy Platinum v2.0. This Product-specific fulfils the generic security requirements given in Payment Mobile Specifications [[75][76][77][79][80][81][82]].The objective is to ensure end users, Mobile Network Operator (MNO) and Issuing Banks trust.

1.2 TOE References

1.2.1 Security Target Reference

The security Target is identified as follows:

Title	ALCHEMY Security Target
TOE name	ALCHEMY
Commercial name	VMPA 1.4.2 – OT v1.0 on NFC FlyBuy Platinum v2.0 on ST33F1ME
ST Reference	FQR 110 6752
Editor	Oberthur Technologies
CC version	3.1 revision 4
EAL	EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5
ITSEF	Thales
Certification Body	ANSSI
Evaluation Scheme	FR

Table 1 Security Target Reference

1.2.2 TOE Reference

Code/Hardware Identification	0768910
Card Manager Identification	GOP Ref V1.8.v
Applet Identification (Version)	03
Label PVCS code for Application	VMPA_OT_V01_00_03
Label PVCS Code for Platform	USIM_V31_NFC_V2_EAL4_CCD2_0768910
ST-lite Platform	[85]
Platform Certificate	[91]
IC reference	ST33F1ME
IC ST lite	[29]
IC Certificate	[95]
IC Surveillance	[96]

Table 2 TOE References

1.3 TOE Identification

The aim of the paragraphs is to allow the user to identify uniquely the TOE.

The TOE is composed of application and a platform (((U)SIM Java card, the OS and the IC).

1.3.1 Application Identification

This chapter presents the means to identify the evaluated applet.
It's composed of 1 package, containing 3 applets.
Here

AID Description	AID
Package AID	**A0 00 00 00 77 01 00 85 01 10 00 00 0x 00 03**
VMPA Applet Class AID	**A0 00 00 00 77 01 00 85 01 10 00 00 0x 00 03 56**
Multi-Access Class AID	**A0 00 00 00 77 01 00 85 01 10 00 00 0x 00 03 4D**
Toolkit Applet Class AID	**A0 00 00 00 77 01 00 85 01 10 00 00 0x 00 03 54**

'x' is a value between 0 and F used to uniquely assign a package to a bank.

Once applet is instantiated, a GET DATA may be used to retrieve the VISA Application identifier:

```
Command       : 00 A4 04 00 07
Input Data    : A0 00 00 00 03 10 10
Output Data   : 6F 31 84 07 A0 00 00 00 03 10 10 A5 26 9F 38 1B
         : 9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A
         : 02 9A 03 9C 01 9F 37 04 9F 4E 14 BF 0C 05 9F 4D
         : 02 14 14
Status        : 90 00

Command       : 80 CA 9F 7E 04
Input Data    : none
Le       : 04
Output Data   : 9F 7E 01 03
Status        : 90 00
```

Application Identifier Version (Tag 0x9F7E) shows the ID version of the current installed VMPA applet:
'Applet Identifier Version' (1 byte) is currently **03**

1.3.2 Platform Identification

This chapter presents the means to identify the platform even if the means are already specified in the ST-Lite of the OPERA FlyBuy Platinum.

In order to assure the authenticity of the card within the application, the product identification shall be verified by analyzing the following element:

ATR	3B 9F 96 80 3F C7 00 80 31 E0 73 FE 21 1B 64 **07 68 9A** 00 82 90 00 (Where **07 68 9A** is the SAAAAR code)

The meaning of the **green bytes** in the ATR is

07 68 9A	SAAAR code

GET DATA response	Command Output Data Status	: 80 CA 9F 7F 2D : 9F 7F 2A **47 50 00 00 82 31 21 02 33 22** 00 00 00 : 00 00 00 00 00 00 00 00 00 00 00 00 00 14 34 12 : 80 00 00 00 00 14 34 03 36 00 00 00 00 : 90 00

The meaning of the **green bytes** in the command response is

47 50	FAB_ID
00 00	IC_ID
82 31	OS_ID
21 02	OS_Release_Date
33 22	OS_Release_Level

GET DATA Card manager release	Command Output Data Status	: 80 CA DF 6C 13 : DF 6C 10 **47 4F 50 20 52 65 66 20 56 31 2E 38 2E 76 2F XX** : 90 00

The last return byte ‘XX’ depends on the personalization (see table below):

b8	b7	b6	b5	b4	b3	b2	b1	Description
	X							Listing API libraries on GET_STATUS Package
		x						Token using TDES 2 Keys cryptographic scheme
			x					Receipt using RSA 1024 PKCS 1 cryptographic scheme
							0	SSD with Authorized Management not supported
0				0	0	0	-	RFU

1.3.3 Configuration Identification of the Platform

1.3.3.1 Mandated DAP

To identify the configuration with or without MANDATED DAP the GET STATUS command (see [12]) should be used to retrieve information on installed Security Domain(s):

CLA	INS	P1	P2	Lc	Data	Le
80	F2	40	00 or 01	02	4F 00	Xx

Where P2 means:

- '00': Get first or all occurrence(s)
- '01': Get next occurrence(s)

Application Note

In order to process the GET STATUS command, a Secure Channel (SCP02) must be opened first (see [12] for details).

Response data field is formatted as follow:

Name	Length	Value
Length of Application AID	1	'05'-'10'
Application AID	5-16	'xxxxx…'
Life Cycle State	1	'xx' (see Table 3 and Table 4)
Privileges (byte 1)	1	'xx' (see Table 5)

b8	b7	B6	b5	b4	b3	B2	b1	Meaning
0	0	0	0	0	0	1	1	INSTALLED
0	0	0	0	0	1	1	1	SELECTABLE
0	0	0	0	1	1	1	1	PERSONALIZED
1	0	0	0	-	-	1	1	LOCKED

Table 3 Security Domain Life Cycle Coding

b8	b7	B6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	1	1	OP_READY
0	0	0	0	0	1	1	1	INITIALIZED
0	0	0	0	1	1	1	1	SECURED
0	1	1	1	1	1	1	1	CARD_LOCKED
1	1	1	1	1	1	1	1	TERMINATED

Table 4 Card Life Cycle Coding

b8	b7	b6	B5	b4	b3	B2	b1	Meaning
1	-	-	-	-	-	-	-	Security Domain

1	1	-	-	-	-	-	0	DAP Verification
1	-	1	-	-	-	-	-	Delegated Management
-	-	-	1	-	-	-	-	Card Lock
-	-	-	-	1	-	-	-	Card Terminate
-	-	-	-	-	1	-	-	Card Reset
-	-	-	-	-	-	1	-	CVM Management
1	1	-	-	-	-	-	1	**Mandated DAP Verification**

Table 5 Privileges (byte 1)

A successful execution of the command shall be indicated by status bytes '90' '00'.

The command may return the following warning condition: '63' '10' More data available. If so, a subsequent GET STATUS [get next occurrence(s)] may be issued to retrieve additional data.

If the AID of the Security Domain with Mandated DAP Privilege is known, the command to perform for checking that this SD is present on the card is the following:

Command : 80 F2 40 00 [Length of SD +2] 4F [Length of SD] [AID of SD]
Output Data : [Length of SD] [AID of SD] [Life Cycle State]$_{1\ \text{byte}}$ C1
Status : 90 00

For instance, if AID of SD MD = A0 00 00 00 01 23 45 67, the command will be:

Command : 80 F2 40 00 0A 4F 08 A0 00 00 00 01 23 45 67
Output Data : 08 A0 00 00 00 01 23 45 67 0F **C1**
Status : 90 00

1.3.3.2 Card Lock

The card must be in a locked configuration.

This can be verified with the following command which shall send 0xFF as output data.

Command : A0 BC 00 00 01
Output Data : FF
Status : 90 00

Application note

The ADM1 PIN must be verified before using the described command.

1.3.3.3 Authorized Management Lock

In order to check that the card does not allow SSD with Authorized Management privilege, the command GET DATA "Card Manager Release" should be used.
The last byte in the response data is the value of the TAG '7F' of the Card Manager Install parameter: bit 1 shall be set to '0'.

1.4 TOE Guidance

The table below lists the guidance for the users of the TOE (the Platform).

Once the PAP application is loaded and personalized, the product is still open. It means that the Platform guidance have to be respected by all the TOE users.

1.4.1 U(SIM) Platform references

Guidance document for platform production	[87]
Guidance document for development of secure application to certify on the Platform	[88] [89]
Guidance document for development of application on Platform	[6] [67][68] [89]
Guidance document for Platform Issuer	[90]

Table 6 Guidance references for the Platform

1.4.2 PAP references

The table below lists the guidance for the users of the TOE PAP application on the platform.

Guidance document for use of AEPM Application	[75] [76] [77] and chapter 5.2
Guidance document for AEPM personalisation	[83]
Guidance document for ALCHEMY – AGD_OPE	[93]
Guidance document for ALCHEMY – AGD_PRE	[94]

Table 7 Guidance references for the PAP application

2 TOE DESCRIPTION

The ALCHEMY TOE is a composition between the Payment Application Package (PAP) and a Common Criteria certified U(SIM) platform.

2.1 TOE overview

The product to be evaluated is the composition of a Payment Application Package (the applet) with NFC FlyBuy Platinum v2 (U(SIM) platform). It is intended to be plugged in a mobile handset to provide secure payment services to a customer.

2.1.1 TOE environment

The TOE is composed of the following bricks:

- A (U)SIM Java Card platform certified conformant to [84] which is a piece of software (OS, Java Card System, (U)SIM APIs, …) embedded in an Integrated Circuit (IC).
- A Payment Application Package (PAP) compliant with [[75] [76] [77] [79] [80] [81] [82]].

Only one PAP is included into the TOE. But (U)SIM Card can embed more than one PAP application.

This part of the TOE i.e. (U)SIM Java Card platform is already evaluated. It means that the evaluation is a composition between this Platform and the PAP application.

The TOE is clearly identified in red colour and is described in § 2.2. The TOE life cycle is described in § 2.3. The other elements of the TOE environment are outside the TOE scope and described in §2.4.

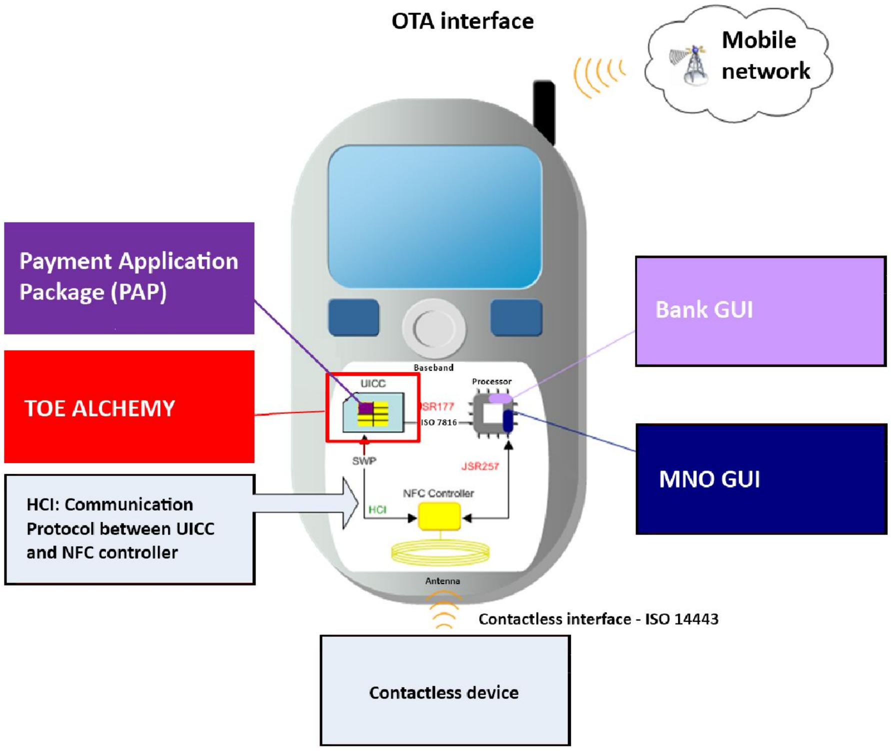

Figure 1 TOE Type & TOE environment

2.1.2 Security features

The TOE is composed of TOE security functionalities (TSF) that implements security requirements and Non TOE Security functionality (non TSF). All are part of this evaluation (even if some doesn't contain TSF).

2.1.2.1 Platform Security Functionalities

Regarding the platform, those elements are the following:

System	SubSystems	Contains TSF?
TELECOM	(U)SIM , Perso Cmds, UICC, OTA RFM, OTA RAM, OTA BIP	No
	OTA SCP 80	Yes
Global Platform 2.2 (GP)	GP API, OP API (Open Platform), Contactless Registry Services (CRS) API, Amd A, Amd C, GP CL registry	Yes
Java Card 3.01. Classic Edition	JCRE, JCVM, JCAPI	Yes
Security Domains	ISD, SD_1...SD_X	Yes
ETSI API	(U)SIM Access API, (U)SIM Toolkit API, NFC API	No
Operating System	Crypto, BIOS	Yes
Integrated Circuit		Yes

Table 8 Platform Security Functionalities

2.1.2.2 PAP security features

The TOE includes the following security features:

- Security functions offered by the USIM platform
- The PAP security functions

The PAP security functions are the following:

- 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 VISA operating rules and should use the same authorization network and clearing system than standard credit and debit cards.

2.1.2.3 PTF security features

The platform security features are described in § 2.5.10 [34].

2.1.3 Usage

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 ([75], Section 4.2).

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

Nota bene

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

2.1.3.1 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[1] 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.

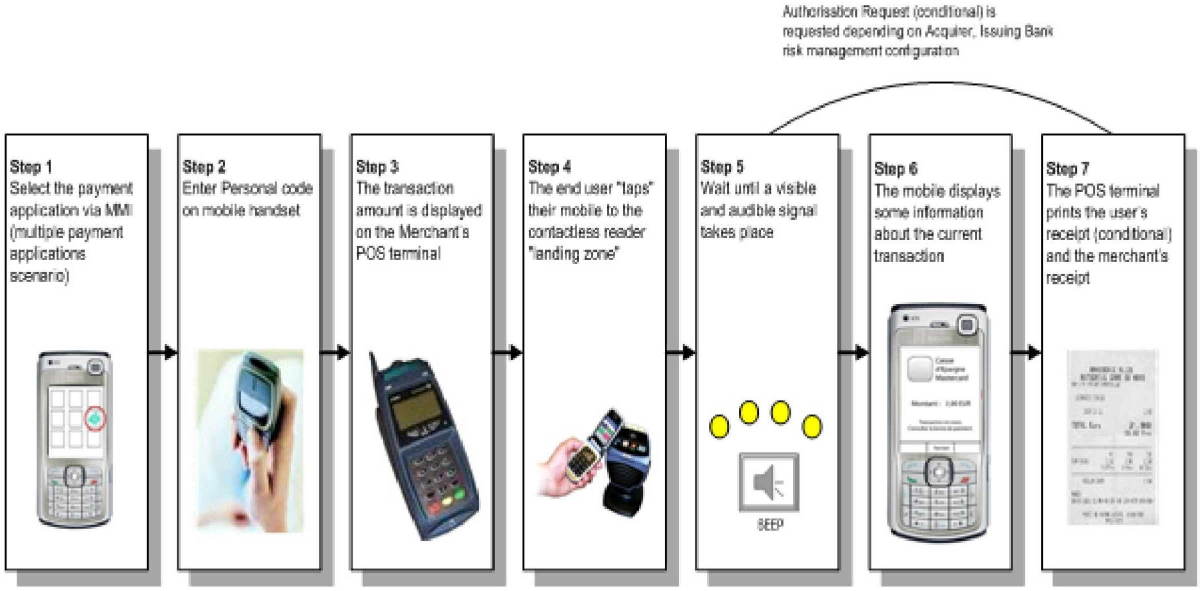
Authorisation Request (conditional) is requested depending on Acquirer, Issuing Bank risk management configuration
Step 1
Select the payment application via MMI (multiple payment applications scenario)
Step 2
Enter Personal code on mobile handset
Step 3
The transaction amount is displayed on the Merchant's POS terminal
Step 4
The end user "taps" their mobile to the contactless reader "landing zone"
Step 5
Wait until a visible and audible signal takes place
BEEP
Step 6
The mobile displays some information about the current transaction
Step 7
The POS terminal prints the user's receipt (conditional) and the merchant's receipt

Figure 2 Mode 1 PIN-TAP

[1] *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.

2.1.3.2 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, [75]), 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 order to proceed with the payment transaction. The steps of this mode of transaction are presented in Figure 3.

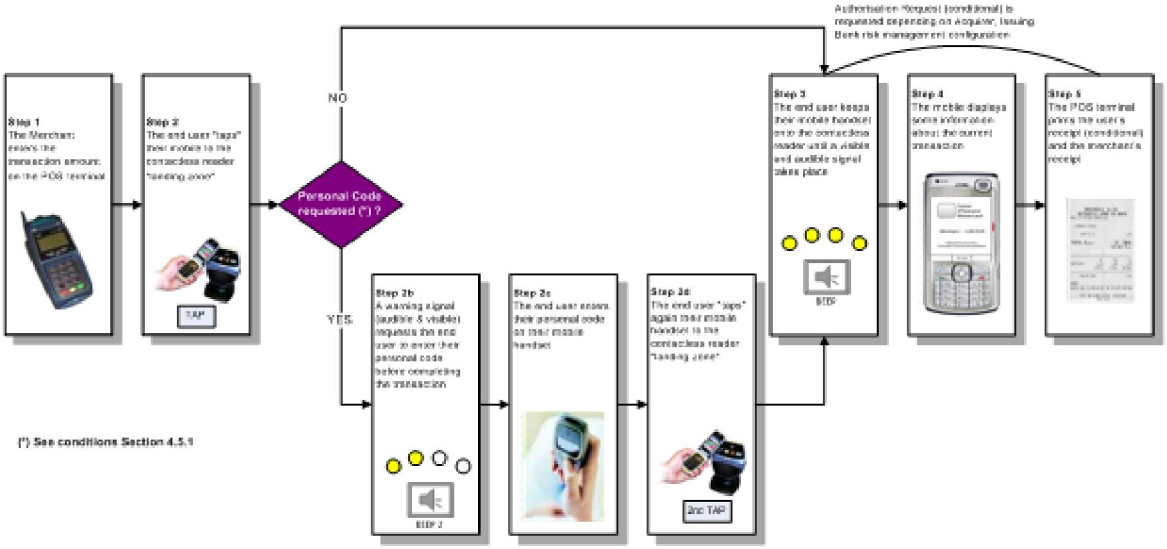
Authorisation Request (conditional) is requested depending on Acquirer, Issuing Bank risk management configuration
Step 1
The Merchant enters the transaction amount on the POS terminal
Step 2
The end user "taps" their mobile to the contactless reader "landing zone"
TAP
Personal Code requested (*) ?
NO
YES
Step 2b
A warning signal (audible & visible) requests the end user to enter their personal code before completing the transaction
BEEP 2
Step 2c
The end user enters their personal code on their mobile handset
Step 2d
The end user "taps" again their mobile handset to the contactless reader "landing zone"
2nd TAP
Step 3
The end user keeps their mobile handset on to the contactless reader until a visible and audible signal takes place
BEEP
Step 4
The mobile displays some information about the current transaction
Step 5
The POS terminal prints the user's receipt (conditional) and the merchant's receipt
(*) See conditions Section 4.5.1

Figure 3 Mode 2 TAP-PIN-TAP

2.2 TOE logical scope

For a complete description for the logical security description of the TOE, please see the dedicated chapters 2.5.10 in of Platform public ST [31].

The logical scope of the TOE may be depicted as follows:

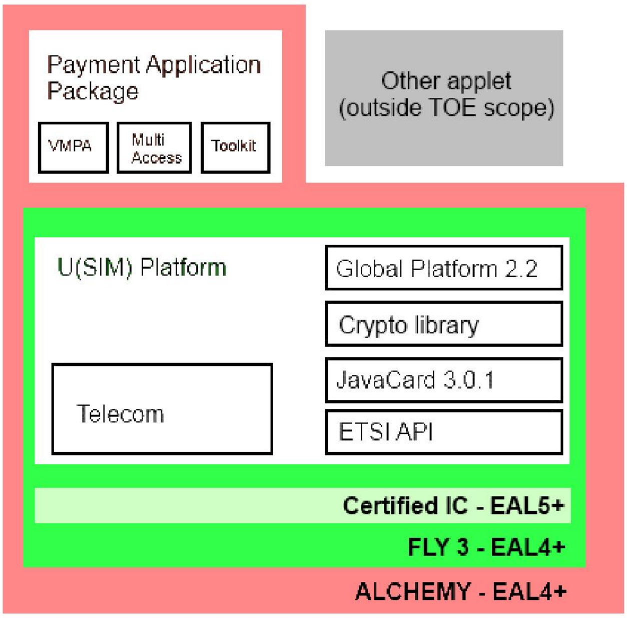

Figure 4 Logical scope

Nota bene

> *There are no known applets that are out of the ALCHEMY TOE scope*
> *There are no applets known outside of the FLY3 TOE scope included and required for ALCHEMY evaluation*

2.2.1 PAP applets description

The PAP is composed with three applets that are identified in the following paragraphs.

2.2.1.1 VMPA

VMPA applet is a VISA Mobile Payment Application, compliant with VISA 1.4.2 VMPA recommendation [82]. The VMPA applet is described in §4 of [86].

2.2.1.2 Multi Access

The Multi-Access applet is implemented to enable sharing of data between several VMPA instances. Where the Multi application AIDs is supported, this applet has access to any components of the VMPA applet visible at the package level and has an ability to create a VMPA object based on the VMPA applet.
The Multi Access applet is described in §5 of [86].

2.2.1.3 SIM Toolkit

The SIM Toolkit applet implements some SIM Toolkit (STK) features and is composed of two elements:

- Toolkit component, that represents the following interfaces:
  - OTA communication to/from the Mobile Gateway
  - The SMS Push Message from the Issuer

  - The VMA to/from the toolkit application
- The Process Message component: represents the interface between the VMPA applet and the toolkit component (to process incoming messages)

The SIM Toolkit applet is described in §6 of [86].

2.2.2 U(SIM) platform overview

The U(SIM) platform overview is described in the platform security target [85]

2.2.3 PAP overview

This section describes the security features offered by the PAP. These are structured in several modules. For a detailed description about these modules, refer to [79] section 2.1, and [80]. The list of modules presented here is not exhaustive, and there might be other modules depending on the use of VISA.

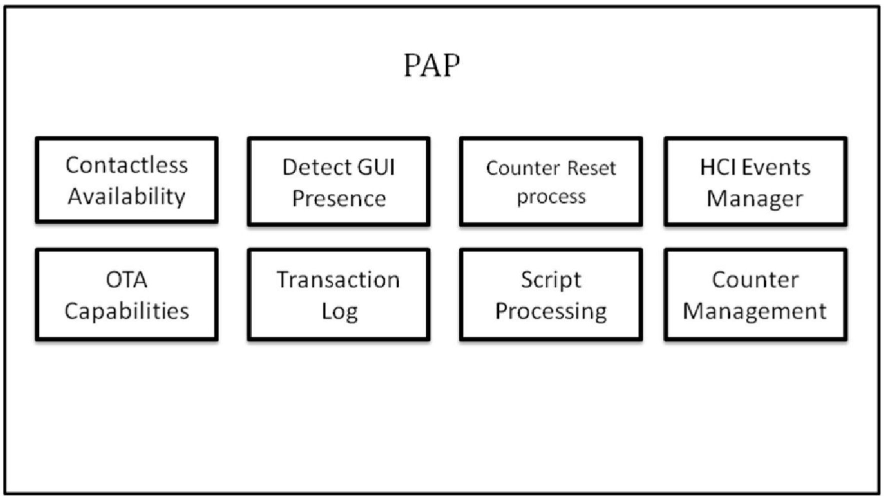

Figure 5 PAP Module

The PAP application is compliant to the VISA [79] Payez Mobile Implementation Guide. For Visa, there are no supplementary packages added to CMP application. All the functionalities of “Payez Mobile Solution” are handled by the CMP itself.

2.2.3.1 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).

2.2.3.2 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 [76], section 8.3.

2.2.3.3 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.

2.2.3.4 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 [76] Section 8.2.4, [79] and [80].

2.2.3.5 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.

2.2.3.6 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.

2.2.3.7 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).

2.2.3.8 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.

2.3 TOE Life Cycle

This paragraph presents the ALCHEMY TOE life cycle.

As a product composition, ALCHEMY is a composition between:

- PAP life cycle presented in § 1.7.3 [92]
- Underlying U(SIM) platform described in § 2.5.8 [34]
- Underlying IC described in § 3.3 [32]

[PTF] is relative to the scope of the platform certificate, Platinum v2.

[IC] is relative to the scope of the underlying IC certificate, ST33F1ME.

[PAP] is relative to the scope of this security target.

[CRYPTO] is relative to the Oberthur Technologies cryptographic library development

For more information on the AGD documentation, please refer to Table 5 and Table 6.

2.3.1 Overview of the life cycle

This paragraph presents an overview of the TOE life cycle.

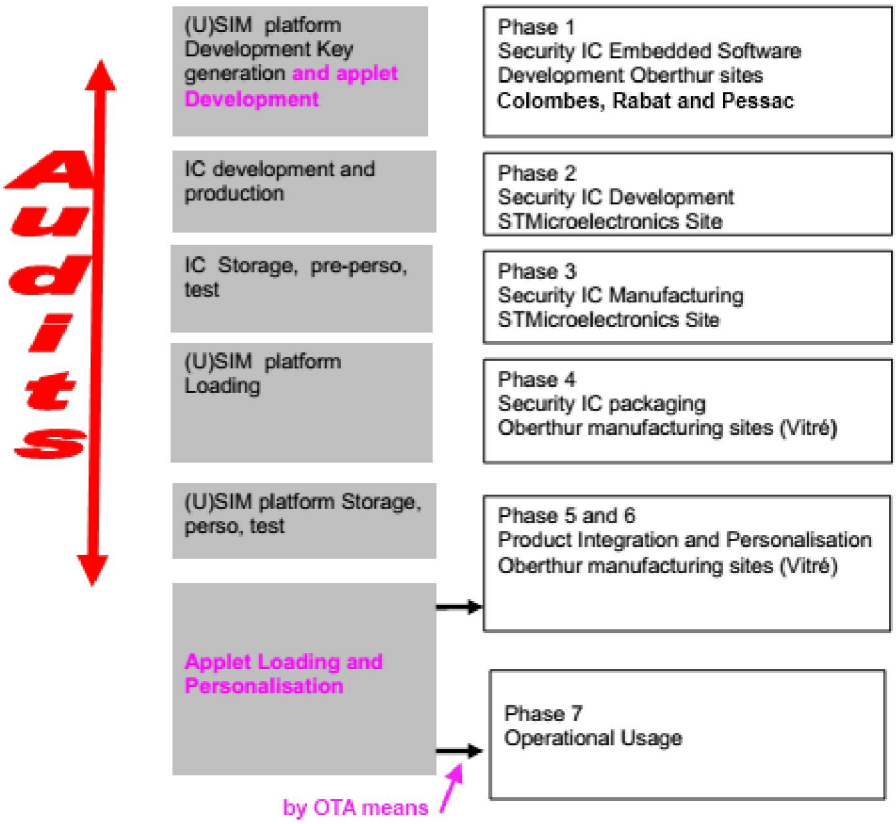
Audits
(U)SIM platform Development Key generation and applet Development
Phase 1 Security IC Embedded Software Development Oberthur sites Colombes, Rabat and Pessac
IC development and production
Phase 2 Security IC Development STMicroelectronics Site
IC Storage, pre-perso, test
Phase 3 Security IC Manufacturing STMicroelectronics Site
(U)SIM platform Loading
Phase 4 Security IC packaging Oberthur manufacturing sites (Vitré)
(U)SIM platform Storage, perso, test
Phase 5 and 6 Product Integration and Personalisation Oberthur manufacturing sites (Vitré)
Applet Loading and Personalisation
Phase 7 Operational Usage
by OTA means

Figure 6 TOE life cycle

2.3.2 PAP life cycle

The life cycle of the PAP consists of 5 consecutive stages:

Life cycle phases	Description
Development	This stage is performed on behalf of the Issuing Bank in a secure development environment at Oberthur promises The applet pass the Offcard Byte Code Verifier, such as to comply with the platform requirements [88] (OE.VERIFICATION)
Loading	This stage can occur in phase 6: pre-issuance and or in phase 7: in post-issuance, when the (U)SIM is already delivered to the end-user, in this case, the applet loading is done using OTA means
Installation & Personalization	This stage occurs in phase 6, in production phase or in phase 7 in the usage environment by OTA means
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

Table 9 PAP life cycle

The rationale of the life cycle is the following:

Life cycle phases	Coverage
Development	ALC [PTF] [PAP]
Loading	AGD_OPE [PTF] AGD_PRE [PAP]
Installation & Personalization	AGD_OPE [PTF] AGD_PRE [PAP]
Usage	AGD_OPE [PAP]
Destruction	At this stage, the PAP is destroyed

Table 10 PAP life coverage

2.3.3 PAP life cycle vs U(SIM) PTF life cycle

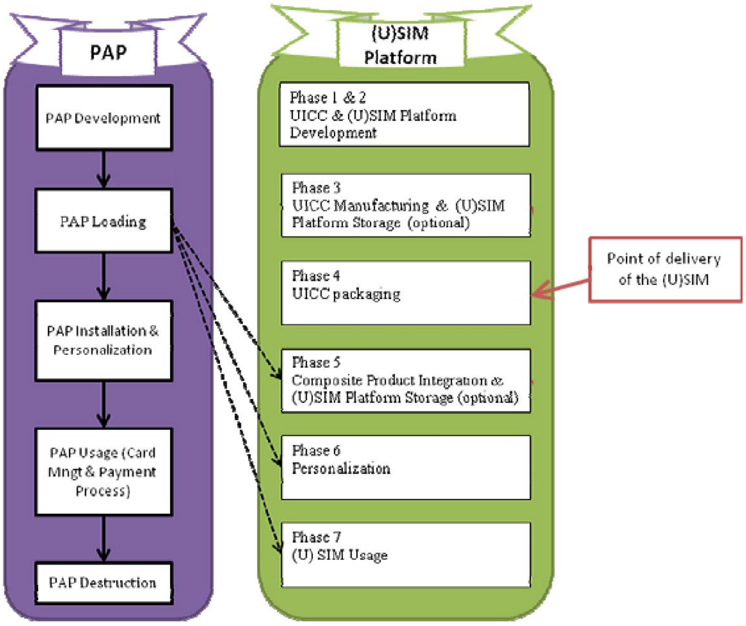
PAP
PAP Development
PAP Loading
PAP Installation & Personalization
PAP Usage (Card Mngt & Payment Process)
PAP Destruction
(U)SIM Platform
Phase 1 & 2 UICC & (U)SIM Platform Development
Phase 3 UICC Manufacturing & (U)SIM Platform Storage (optional)
Phase 4 UICC packaging
Phase 5 Composite Product Integration & (U)SIM Platform Storage (optional)
Phase 6 Personalization
Phase 7 (U) SIM Usage
Point of delivery of the (U)SIM

Figure 7 TOE life cycle vs PTF life cycle

We refer to [84] for the definition of the (U)SIM Platform life cycle.
The rationale of the U(SIM) Platform life cycle is the following:

Life cycle State	Environment	Covered by
Phase 1	Development [PTF] [PAP]	ALC [PTF] [PAP]
Phase 2	Development [IC]	ALC [IC]
Phase 3	Security IC manufacturing	ALC [IC]
Phase 4	Security IC packaging	ALC [PTF]
Phase 5&6	Construction of part of the TOE (PTF) or the entire TOE (PTF and PAP loading)	ALC [PTF]
	PAP loading	AGD_OPE [PTF] AGD_PRE [PAP]
	PAP personalisation	AGD_PRE [PAP] AGD_OPE [PTF] [PAP]
Phase 7	PAP loading	AGD_OPE [PTF] AGD_PRE [PAP]
	PAP personalisation	AGD_PRE [PAP] AGD_OPE [PTF] [PAP]
	PAP usage	AGD_OPE [PTF] AGD_OPE [PAP]
	PAP destruction	

Table 11 U(SIM) PTF life cycle coverage

2.3.4 TOE life cycle actors

This paragraph identified the Actors acting on the TOE during the PAP life cycle.

PAP Life cycle phases	Actors
Development	[PTF]: OT Pessac [CRYPTO]: OT Colombes [PAP]: OT Rabat
Loading	Depending on the phase where occurs the loading: 4, 5, 6 : OT Vitré 7 : S.BANK_TSM
Installation & Personalization	S.BANK_TSM
Usage	MNO, Issuing Bank or Customer
Destruction	S.BANK_TSM

Table 12 TOE life cycle actors

Application note

Users are defined in chapter Users/Subjects below (§4.2)

2.3.5 PAP on-card life cycle

The on-card life cycle of the PAP is compliant with the Global Platform standard life cycle [9]:
The PAP life cycle is divided in two parts:

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

2.3.6 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 [9] for more information.

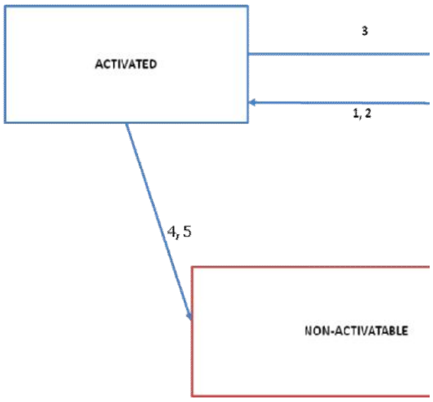

Figure 8 Contactless life cycle states

Steps Description

1- Another CMP Application is ACTIVATED
2- A Customer sets an application from “ACTIVATED” to “DEACTIVATED” via the function “Deactivate a CMP application”
3- A Customer sets an application from “DEACTIVATED” to “ACTIVATED” via the function “Define 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

2.3.7 GP standard life cycle

The life cycle status is the representation of the GP life cycle (compliant with [9]).

The GP standard life cycle is composed with 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.

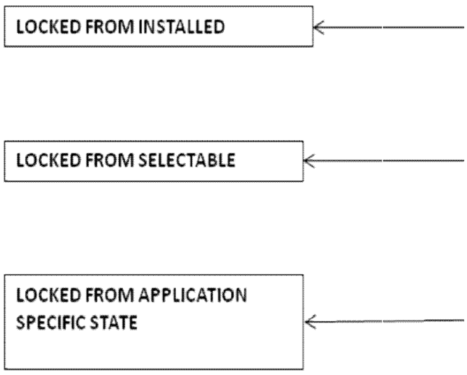

Figure 8 GP Life Cycle Status

2.4 Non-TOE available to the TOE

This action describes the hardware, software or firmware present in the environment of the TOE and that are required to have a correct usage of the TOE.
For a detailed description, see [76], Section 2.2.

2.4.1 Umbrella Application

The umbrella application transfers the Payment Application Package AIDs and its life cycle status to the MNO GUI in order to allow the MNO GUI to make the reconciliation between the CMP applications loaded in the UICC and the associated Bank GUIs installed on the mobile handset.

2.4.2 Payez Mobile Application[2](CREL Application)

The *Payez Mobile* application is a CREL (Contactless Registry Event Listener) application according to Global Platform Amendment C [13]. 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[3].

[2] Not to be confused with the Payment Application Package (PAP).

[3] One-shot payment: The CMP application (that is not active by default) selected by the Customer is used only for the current payment transaction. (Not supported in the current implementation).

2.4.3 Proximity Payment System Environment (PPSE) application

The PPSE application is a CREL (Contactless Registry Event Listener) application according to GlobalPlatform Amendment C [13].

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.

2.4.4 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.

2.4.5 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.

2.4.6 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.

2.4.7 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 [76].

2.4.8 POS Application

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

2.4.9 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 [76].

2.4.10 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.

2.4.11 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.

2.4.12 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.

3 CONFORMANCE CLAIMS

3.1 Common Criteria conformance claims

This Security Target claims conformance to **CC version 3.1 R4** with the following documents:

"Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model", September 2012, Version 3.1 revision 4

"Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements", September 2012, Version 3.1 revision 4

"Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance requirements", September 2012, Version 3.1 revision 4

Conformance is claimed as follows:

- Part 1: conformant
- Part 2: conformant
- Part 3: conformant EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

3.2 Protection profile claims

No protection profile is claimed for ALCHEMY.

Nevertheless, this document has been written in accordance with the *Payez Mobile Guidance for Security Target version 1.0.3* [81].

4 SECURITY PROBLEM DEFINITION

4.1 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.

4.1.1 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.

User data	Description	Protection
POS Transaction Data	All data transmitted to the PAP from the POS terminal. This includes: Country Code, Terminal Verification Result, etc	Integrity
Issuing Bank Transaction Data	All transaction data transmitted to the PAP by the Issuing Bank including Issuing Bank authentication data, ARPC, CDOL2, etc	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)	Integrity
MNO Data	All data transmitted to the TOE by the MNO including the MNO authentication data	

4.1.2 TSF data

TSF data are created by and for the TOE. These data might affect the operation of the TOE.

4.1.2.1 TRANSACTION MANAGEMENT DATA

Transaction management data	Description	Protection
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).	Integrity confidentiality
PAP Log File	PAP Log File and its associated format under EMV rules. This asset contains the log data of the last transactions	Integrity

	performed by the PAP.	
Customer Account Information	All customer bank account data including the PAN, the PAN Sequence Number, expiration date.	Integrity
PAP keys	The cryptographic keys owned by the payment application instances.	Integrity confidentiality
PAP Transaction Parameters	PAP keys asset includes secret keys, private keys and random numbers used for secret key generation. 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.	Integrity
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).	Integrity
PAP Selection and Activation parameters	The parameters allowing the POS to perform the selection and activation of the embedded PAP (eg AID, long AID, contactless life cycle state, ...)	Integrity
PAP State Machine	The PAP State Machine stores information about the PAP application internal states during its usage phase.	Integrity

Application Note

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

4.1.2.2 TEMPORARY TRANSACTION DATA

Temporary Transaction data	Description	Protection
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)	Integrity

4.2 Users / Subjects

4.2.1 USERS

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

Users	Description
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.
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.

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.

4.2.2 SUBJECTS

Subjects are active entities in the TOE.

Subjects	Description
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).

4.3 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.

All threats of the Platform are included in this ST. Please refer to [31]. Compatibilities are showed in chapter 8.

4.3.1 DISCLOSURE

Unauthorized disclosure of assets.

Disclosure	Description	Assets
T.DISCLOSURE_KEYS	An attacker may perform attacks leading to unauthorized knowledge of the keys.	PAP keys
T.DISCLOSURE_REF_PC	An attacker may perform attacks leading to unauthorized knowledge of the Reference Personal Code.	Reference Personal Code

4.3.2 INTEGRITY

Unauthorized modification of assets.

Integrity	Description	Assets
T.INTEG_LOG_FILE	Unauthorized modification of stored log files: an attacker modifies the log of transactions in order to hide malicious operations.	PAP Log File
T.INTEG_KEYS	Unauthorized modification of stored keys: an attacker modifies the value of the keys in order to input a known key	PAP keys
T.INTEG_ACCOUNT_INFO	Unauthorized modification of stored customer account information: for instance an attacker modifies the value of the PAN	Customer Account Information
T.INTEG_REF_PC	Unauthorized 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.	Reference Personal Code
T.INTEG_TRANS_PARAM	Unauthorized 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.	PAP Transaction Parameters PAP State Machine

Integrity	Description	Assets
T.INTEG_COUNT	Unauthorized 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 unauthorized permission to submit a payment transaction.	PAP Counters
T.TEMPORARY_DATA	Unauthorized modification of temporary transaction data: an attacker modifies the value of transaction data in order to authorize counterfeited or replayed transactions.	PAP Transaction Data POS Transaction Data Issuing-Bank Scripts MNO Data Issuing Bank Transaction Data
T.INTEG_SEL_ACT _PARAM	Unauthorized 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.	PAP Selection and Activation Parameters

4.3.3 FRAUDULENT PAYMENT

Fraudulent payment	Description	Assets
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	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.	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.	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	PAP Log File and PAP Transaction Parameters

Fraudulent payment	Description	Assets
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	PAP keys PAP Transaction Parameters Customer Account Information PAP Transaction Data.
T.TRANSACTION_REPLAY	Replay of a previous complete sequence of transaction operations.	PAP Transaction data POS Transaction data Issuing Bank Transaction Data

Application Note

The Transaction Replay 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.

4.3.4 DENIAL-OF-SERVICE

Denial of service	Description	Assets
T.CERTIF_CORRUPTION	Corruption of the transaction data (certificates) in order to deny participation to the transaction under the terms claimed by one party.	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.	Issuing-Bank Scripts MNO Data Issuing Bank Transaction Data

4.3.5 IDENTITY_USURPATION

Identity usurpation	Description	Assets
T.MNO_USURPATION	An attacker is illegally granted the rights of the MNO to modify the transactions parameters in order to authorize fraudulent transactions.	MNO Data

Identity usurpation	Description	Assets
T.ISSUING-BANK_USURPATION	An attacker is illegally granted rights of the Issuing Bank to make unauthorized PAP management operations.	Issuing Bank Transaction Data
T.CUSTOMER_USURPATION	An attacker is illegally granted the rights of the legitimate customer to submit unauthorized transactions on his/her behalf.	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.

4.4 Organisational Security Policies

All Organisational Security Policies of the Platform are included in this ST. Please refer to [31]. Compatibilities are showed in chapter 8.

4.4.1 HANDSET

Handset	Description
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 authorized to communicate with the PAP (Cardlets).

4.4.2 MANAGEMENT

Management	Description
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_lifecycle _MNGT	Each PAP holds the "Contactless Life Cycle State", which takes values from: o ACTIVATED o DEACTIVATED o 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 [13] 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 unauthorized 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).

4.4.3 MERCHANT

Merchant	Description
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*

4.4.4 BANK

Bank	Description
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.

4.5 Assumptions

All platform assumptions [31] are part of this composite ST. Compatibilities are showed in chapter 8.

Assumption	Description
A.MERCHANT_AUTH	Merchant contract subscription guarantees the authenticity of the Merchant

5 SECURITY OBJECTIVES

5.1 Security Objectives for the TOE

All security objectives of the Platform are included in this ST. Please refer to [31]. Compatibilities are showed in chapter 8.

5.1.1 TRANSACTION PROTECTION

Transaction protection	Description
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 [76] and [75] specifications
O.TRANSACTION_REPLAY	The TOE shall detect and reject replayed transactions

5.1.2 AUTHENTICATION

Authentication	Description
O.USER_AUTH	The TOE shall provide customer authentication means for Personal Code change and for each payment transaction above the Personal Code Entry Limit.
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.

Application Note

> *Regarding O.USER_AUTH, 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.MNO_AUTH is handled by the (U)SIM platform (see O.COMM_AUTH in [84])*

5.1.3 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 *[84]*

Execution protection	Description
O.AUTHORISATION_CONTROL	The consistency of payment transactions shall be checked according to *Payez Mobile* specifications [75] and [76] before granting the customer the authorisation to submit payment transactions.

5.1.4 DATA PROTECTION

Data protection	Description
O.DATA_DISCLOSURE	The TOE shall avoid unauthorized disclosure of TSF data stored and manipulated by the TOE and that must be protected in confidentiality
O.DATA_INTEGRITY	The TOE shall avoid unauthorized 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 authorized users

Application Note

O.DATA_DISCLOSURE is partially handled by the (U)SIM platform regarding physical attacks and unobservability of secrets.

5.1.5 RISK MANAGEMENT

Risk Management	Description
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 authorized user the privilege to block the PAP and its data in a way to prohibit a positive response to payment authorisation requests
O.SIM_UNLOCK	The TOE shall require unlocking the (U)SIM card (by means of the PIN code) for each payment transaction
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

Application Note

O.SIM_UNLOCK is handled by the (U)SIM platform (see O.COMM_AUTH in in [84])

5.1.6 OBJECTIVES handled by (U)SIM Platform

U(SIM) Platform	Description
O.GUIS_AUTH	The TOE ((U)SIM Platform and PAP) shall authenticate the GUIs authorized 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.COMM_AUTH in [84]). For instance, using ACF mechanism (cf. [AEPM-2], Section C.2.3)

5.2 Security objectives for the Operational Environment

All security objectives for the Operational Environment of the Platform are included in this composite ST. Please refer to [31].

5.2.1 HANDSET

Handset	Description
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 authorized 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 customer mobile handset before or after the transaction

Handset	Description
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

5.2.2 MERCHANT

Merchant	Description
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
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
OE.POS_DEACTIVATION	Any POS terminal may be rendered inoperative remotely by the POS purchaser or the Acquirer

Application Note

For OE.MERCHANT_CONTROL, for instance, by controlling Merchants accepting small payments amounts

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

5.2.3 MANAGEMENT

Management	Description
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

5.2.4 BANK

Bank	Description
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 authorized
OE.BANKS_PRIVILEGES	The Issuing Bank shall be granted specific privileges

6 SECURITY REQUIREMENTS

6.1 Security Functional Requirements

This section defines the security functional 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
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

Table 13 Operation involved in the Access Control and Information Control Policies

Security Attributes	**Possible Values for Security Attributes;**
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 [75] and [76] and indicates results of transaction processing steps / Does not comply with [75] and [76]
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

Table 14 Security attributes involved in the Access Control and Information Control Policies

6.1.1 ACCESS CONTROL POLICY

FDP_ACC.2/ PAP Application Complete access control

FDP_ACC.2.1/ PAP Application The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

The TSF shall enforce the ***PAP Application Access Control SFP*** on ***S.PAP, PAP Sate 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 **PAP Application Access Control 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 [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

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 **PAP Activation Access Control SFP**:*

- *PAP Selection*

FDP_ACC.2/ PAP Administration Management Complete access control

FDP_ACC.2.1/ PAP Administration Management The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

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 **PAP Administration Management Access Control 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 [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

The TSF shall enforce the ***PAP Payment Transaction Management Access Control SFP*** on

- ***Subjects:***
  - ***S.PAP;***
  - ***S.BANK_TSM;***

- ***S.MNO_ISD;***

o ***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 **PAP Payment Transaction Management Access Control 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 [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

The TSF shall enforce the ***Post-Issuance Bank Management Access Control SFP*** on

o ***Subjects:***

- ***S.PAP;***
- ***S.BANK_TSM;***
- ***S.MNO_ISD;***

o ***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 **Post-Issuance Bank Management Access Control 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 [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

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 **PAP Offline Authentication control access SFP:***

- *PAP Offline Data Authentication*

FDP_ACC.2/ PAP Transaction Complete access control

FDP_ACC.2.1/ PAP Transaction The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

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 **PAP Transaction Access Control SFP**:*

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

PAP Transaction processing is defined by the above operations

6.1.2 ACCESS CONTROL FUNCTIONS

FDP_ACF.1/ PAP Application Security attribute based access control

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

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

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 authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

The TSF shall explicitly authorize 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:[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- o *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 [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

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

- o ***Security attributes of the subject S.PAP:***
  - ***Contactless Life Cycle State;***
- o ***Security attributes of the object PAP Selection and Activation Parameters:***
  - ***PAP Selection and Activation Parameters;***
- o ***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: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

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

- o ***Selection is allowed only if***
  - ***Contactless Life Cycle State is Installed;***
- o ***PAP Selection and Activation Parameters is allowed if:***
  - ***PAP Selection and Activation Parameters is Verified;***
- o ***PAP Transaction Parameters is allowed if:***
  - ***PAP Transaction Parameters Integrity is Verified***.

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

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

- o ***none***

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

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***following rule:***

- o ***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 [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].

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

- o ***Security attributes of the object Reference Personal Code and Personal Code:***
  - ***PAP Reference Personal Code State;***
  - ***PAP Reference Personal Code Integrity;***
- o ***Security attributes of the object Personal Code:***
  - ***PAP Personal Code State;***
- o ***Security attributes of the subject S.PAP:***
  - ***Contactless Life Cycle State;***
- o ***Security attributes of the object PAP Log File:***
  - ***Log File reading Status;***
- o ***Security attributes of the object PAP Keys:***
  - ***PAP Keys Integrity;***
- o ***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: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

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

- o ***Systematic Personal Code Activation/Deactivation is allowed only if:***
  - ***PAP Reference Personal Code Integrity is VERIFIED;***
  - ***PAP Personal Code State is VERIFIED;***
- o ***Reference Personal Code Change is allowed only if:***
  - ***PAP Reference Personal Code Integrity is VERIFIED;***
  - ***PAP Personal Code State is VERIFIED;***
  - ***PAP Reference Personal Code State is UNBLOCKED;***
- o ***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);***
- o ***PAP Activation/Deactivation is allowed only if:***
  - ***Contactless Life Cycle State is ACTIVATED or DEACTIVATED;***
  - ***PAP Reference Personal Code 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 counter integrity is VERIFIED;***
  - ***PAP Issuing Bank secure script counter State is NOT BLOCKED***.

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

The TSF shall explicitly authorize 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:[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

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

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

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

- ***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;***

- ***Log Update is allowed for all transactions besides those of Post-Issuance Bank Management (only during payment transactions) only if***:
  - ***Log Update is ALLOWED.***
- ***Personal Code Verification is allowed only if:***
  - ***PAP Reference Personal Code State is UNLOCKED***;
  - ***PAP Reference Personal Code Integrity is Verified***

FDP_ACF.1.3/ PAP Payment Transaction Management The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

The TSF shall explicitly authorize 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:[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

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

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

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 counter integrity is VERIFIED;***
- ***PAP Issuing Bank secure script counter 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 authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

The TSF shall explicitly authorize 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:[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

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

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

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 authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

The TSF shall explicitly authorize 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:[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

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

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***
  - ***(U)SIM Card Life Cycle Status is SELECTED;***
  - ***Contactless Life Cycle State;***
- ***Security attributes of the object PAP Counters:***
  - ***PAP Counters Integrity;***
  - ***PAP Counters state;***
- ***Security attributes of the object Customer Account Information:***
  - ***PAP Customer Account Information Integrity (PAN integrity);***

- ***Security attributes of the object PAP Keys:***
  - ***PAP Keys 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: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

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:

- ***PAP Transaction Processing State complies with Transaction Flows following [75] and [76] specifications;***
- ***(U)SIM Card Life Cycle Status is SELECTED;***
- ***Contactless Life Cycle State ACTIVATED;***
- ***PAP Counter Integrity is VERIFIED;***
- ***PAP Counter State is not BLOCKED;***
- ***PAP Customer Account Information Integrity is VERIFIED;***
- ***PAP keys integrity is VERIFIED;***
- ***PAP Transaction Parameters Integrity is VERIFIED***.

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

The TSF shall explicitly authorize 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:[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

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***.

6.1.3 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 [assignment: information flow control SFP] on [assignment: list of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.

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 [assignment: information flow control SFP] on [assignment: list of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.

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 [assignment: information flow control SFP] on [assignment: list of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.

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 [assignment: information flow control SFP] on [assignment: list of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.

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

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: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

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 [assignment: additional information flow control SFP rules].

The TSF shall enforce the ***following rules: none***.

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

The TSF shall explicitly authorize 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: [assignment: rules, based on security attributes, that explicitly deny information flows].

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

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: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

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 [75] and [76]***
- ***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 [assignment: additional information flow control SFP rules].

The TSF shall enforce the ***following rules: None***.

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

The TSF shall explicitly authorize 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: [assignment: rules, based on security attributes, that explicitly deny information flows].

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

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: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

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 PAP specifications [75] and [76]***
- ***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 [assignment: additional information flow control SFP rules].

The TSF shall enforce the ***following rules: None***.

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

The TSF shall explicitly authorize 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: [assignment: rules, based on security attributes, that explicitly deny information flows].

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

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 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: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

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 [assignment: additional information flow control SFP rules].

The TSF shall enforce the ***following rules: None***.

FDP_IFF.1.4/ Post-Issuance Bank Management The TSF shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes that explicitly authorize information flows].

The TSF shall explicitly authorize 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: [assignment: rules, based on security attributes that explicitly deny information flows].

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***.

6.1.4 SECURITY AUDIT

FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take [assignment: list of actions] upon detection of a potential security violation.

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 [assignment: subset of defined auditable events] known to indicate a potential security violation;

b) [assignment: any other rules].

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

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

- ***unauthorized use of the PAP services;***
- ***unauthorized read or modification of the PAP sensitive assets protected in integrity and confidentiality;***
- ***unauthorized 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 [selection: choose one of: minimum, basic, detailed, not specified] level of audit; and

c) [assignment: other specifically defined auditable events].

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;***.

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, [assignment: other audit relevant information].

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,

- ***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***.

Refinement

Payment transactions auditable events are specified in FAU_SAA.1.2

FAU_SAR.1/CUSTOMER Audit review

FAU_SAR.1.1/CUSTOMER The TSF shall provide [assignment: authorized users] with the capability to read [assignment: list of audit information] from the audit records.

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 [assignment: authorized users] with the capability to read [assignment: list of audit information] from the audit records.

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.

6.1.5 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 [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

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: ***[75] and [76] standard***.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards].

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method***: The keys are reset in accordance with ["Java Card - API" Application Programming Interfaces, Classic Edition, Version 3.01, February 23, 2009, Sun Microsystems] in class Key with the method clearKey()***.

Application note

This SFR is implemented by the Platform. That also prevents the destroyed keys from being referenced. ***Any access to a cleared key attempting to use it for ciphering or signing shall throw an exception*** *that meets the following: ["Java Card - API" Application Programming Interfaces, Classic Edition, Version 3.01, February 23, 2009, Sun Microsystems].*

FCS_COP.1/Offline Data Authentication Cryptographic operation

FCS_COP.1.1/Offline Data Authentication The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

The TSF shall perform ***Signature operation*** in accordance with a specified cryptographic algorithm ***RSA*** and cryptographic key sizes ***176 bytes*** that meet the following: ***[75] and [76] specification***.

FCS_COP.1 PIN Cryptographic operation

FCS_COP.1.1 PIN The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

Operations	**Algorithm**	**Key sizes**	**Standards**
Encryption and decryption	RSA	From 768 bits to 1920 bits with a step of 32-bit	[11], [16], [19]
	3DES	16 bytes	[75], [76]

FCS_COP.1/Application Cryptogram Cryptographic operation

FCS_COP.1.1/Application Cryptogram The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

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: ***[75] and [76] specifications***.

FCS_COP.1/Script Processing Cryptographic operation

FCS_COP.1.1/Script Processing The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

The TSF shall perform ***Cryptogram generation*** in accordance with a specified cryptographic algorithm ***3DES*** and cryptographic key sizes ***16 bytes*** that meet the following: ***[75] and [76] specifications***.

FCS_COP.1/Messages Data Integrity Cryptographic operation

FCS_COP.1.1/Messages Data Integrity The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

The TSF shall perform ***MAC Computation*** in accordance with a specified cryptographic algorithm ***3DES*** and cryptographic key sizes ***16 bytes*** that meet the following: ***[75] and [76] specifications***.

FCS_COP.1/Messages Data Confidentiality Cryptographic operation

FCS_COP.1.1/Messages Data Confidentiality The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

The TSF shall perform ***Encipherment*** in accordance with a specified cryptographic algorithm ***3DES*** and cryptographic key sizes ***16 bytes*** that meet the following: ***[75] and [76] specifications***.

6.1.6 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 [assignment: integrity errors] on all objects, based on the following attributes: [assignment: user data attributes].

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 [assignment: action to be taken].

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 [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of [selection: [assignment: parts of TSF], the TSF].

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 authorized users with the capability to verify the integrity of [selection: [assignment: parts of TSF data], TSF data].

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

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of [selection: [assignment: parts of TSF], TSF].

The TSF shall provide authorized users with the capability to verify the integrity of ***PAP application code***.

Application Note

FPT_TST.1 shall not be interpreted as TSF's self-tests but as protection of integrity of Transaction Management Data (TSF persistent data) and PAP application code during loading of the applet, and covered by the (U)SIM platform (with the SFRs that meet the objective O.COMM_INTEGRITY).

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 [75] and [76]** when interpreting the TSF data from another trusted IT product.

FPT_RPL.1 Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [assignment: list of identified entities].

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

FPT_RPL.1.2 The TSF shall perform [assignment: list of specific actions] when replay is detected.

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. If attack replay VERIFY (PIN) Enciphered command which he sniffed from line, the replay will be rejected and PTC will be decremented.

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 [selection: allocation of the resource to, deallocation of the resource from] the following objects: [assignment: list of objects].

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

This function shall be implemented by the (U)SIM platform

6.1.7 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: [assignment: list of management functions to be provided by the TSF].

The TSF shall be capable of performing the following management functions:

- ***Communication channels selection;***
- ***Post-Issuance Bank Management;***
- ***Customer Personal Parameter setup (Customer can setup some personal parameters via Midlet).***

Application Note

OTA Issuance Management (TSM can install the instance OTA and personalize the installed instance OTA) is implemented by the platform.

FMT_MOF.1/ Parameters Management of security functions behaviour

FMT_MOF.1.1/ Parameters The TSF shall restrict the ability to [selection: determine the behavior of, disable, enable, modify the behaviour of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].

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 [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

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 [assignment: access control SFP(s), information flow control SFP(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles].

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 [assignment: list of security attributes].

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 initialization

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

The TSF shall enforce the:

- Post-Issuance Bank Management Access Control SFP and Post-Issuance Bank Management Information Control SFP

- PAP Application Access Control SFP;

- PAP Payment Transaction Management Access Control SFP;

- PAP Activation Access Control SFP;

- PAP Administration Management Access Control SFP;

- PAP Transaction Access Control SFP;

- PAP Offline Authentication Access Control SFP and PAP Offline Authentication Information Control SFP;

- PAP Offline Transaction Information Control SFP;

- PAP Online Transaction Information Control SFP;

to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

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

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 [assignment: the authorized identified roles].

The TSF shall maintain the roles

- ***Customer;***
- ***Issuing Bank;***
- ***MNO***.

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

6.1.8 IDENTIFICATION / AUTHENTIFICATION

FIA_AFL.1/ Customer Authentication failure handling

FIA_AFL.1.1/ Customer The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to [assignment: list of authentication events].

The TSF shall detect when ***an administrator configurable positive integer at personalisation (the Personal Code Try Counter Limit)*** within ***within [1, FFFFh]*** 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 [selection: met, surpassed], the TSF shall [assignment: list of actions].

When the defined number of unsuccessful authentication attempts has been ***surpassed***, the TSF shall

- ***return an error, as specified in [75] and [76]***
- ***block the PAP Reference Personal Code until the Issuing Bank unblocks it***.

Application Note

*The value of the **Personal Code Try Counter Limit** is defined during personalization (2 bytes, from 1 to FFFFh).*

FIA_AFL.1/ Issuing Bank Authentication failure handling

FIA_AFL.1.1/ Issuing Bank The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts occur related to [assignment: list of authentication events].

The TSF shall detect when ***1*** 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 [selection: met, surpassed], the TSF shall [assignment: list of actions].

When the defined number of unsuccessful authentication attempts has been ***surpassed***, the TSF shall **slow down the next authentication. The waiting time is augmented with a maximum number of unsuccessful authentications of 15**

FIA_ATD.1 User attributes definition

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

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 [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

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.

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 [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

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 [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

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 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 [selection: detect, prevent] use of authentication data that has been forged by any user of the TSF.

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 [selection: detect, prevent] use of authentication data that has been copied from any other user of the TSF.

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 [assignment: identified authentication mechanism(s)].

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 [assignment: list of conditions under which re-authentication is required].

The TSF shall re-authenticate the user under the conditions*:*

- Upon reception of Consumer device Update with P1P2 parameters indicating 'Passcode Try Counter' (tag '9F17')

FIA_UID.1/ PAP Online Transaction Timing of identification

FIA_UID.1.1/ PAP Online Transaction The TSF shall allow [assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is identified.

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 [assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is identified.

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 [assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is identified.

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: [assignment: list of user security attributes].

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: [assignment: rules for the initial association of attributes].

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: [assignment: rules for the changing of attributes].

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 [assignment: a defined quality metric].

The TSF shall provide a mechanism to generate secrets that meet ***the STANDARD level as specified in platform (refer to [30])***.

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for [assignment: list of TSF functions].

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

Refinement: "secrets" stand for random values.

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 [assignment: list of objects or information types].

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 [assignment: list of subjects] with the ability to verify evidence of the validity of the indicated information.

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

6.1.9 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 [assignment: access control SFP(s) and/or information flow control SFP(s)] when importing user data, controlled under the SFP, from outside of the TOE.

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: [assignment: additional importation control rules].

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 [75] and [76] specifications***.

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

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

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: [assignment: additional importation control rules].

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 [75] and [76] specifications***.

FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] when exporting user data, controlled under the SFP(s), outside of the TOE.

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

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: [assignment: additional importation control rules].

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 [assignment: access control SFP(s) and/or information flow control SFP(s)]to [selection: transmit, receive] user data in a manner protected from [selection: modification, deletion, insertion, replay] errors.

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 [selection: modification, deletion, insertion, replay] has occurred.

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

6.1.10 SECURE CHANNEL

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 [selection: the TSF, another trusted IT product] to initiate communication via the trusted channel.

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 [assignment: list of functions for which a trusted channel is required].

The TSF shall initiate communication via the trusted channel for

- ***PAP Online Transaction;***
- ***Post-Issuance Bank Management***.

6.1.11 UNOBSERVABILITY

FPR_UNO.1 Unobservability

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

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***.

6.2 Security Assurance Requirements

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

7 TOE SUMMARY SPECIFICATION

7.1 TOE Summary Specification

This chapter presents the TOE summary specification. It presents all security function implemented in the TOE.

SF_PAP_ACCESS_CONTROL

This security function ensures that access to the operations is done regarding:

- The State Machine Policy (SELECTED, INITIATED)
- The Blocked/Unblocked state
- The contactless visibility of the PAP Application (ACTIVATED, DEACTIVATED, NON ACTIVABLE)
- The life phase state (STATE_NOT_PERSONALIZED, STATE_PERSONALIZED)

These conditions are checked by the dispatcher who permits to determine which operation is to be executed following input data and parameters. These conditions are also checked again by commands modules if necessary before processing the received commands.

Application Note

For a payment Transaction, the used mode must be Payment Mode and the CL Life Cycle of the PAP must be ACTIVATED. The PAP Application must be SELECTABLE and must Selected before initiating any action on it. For a payment Transaction, the used mode must be Payment Mode and the CL Life Cycle of the PAP must be ACTIVATED. The PAP Application must be SELECTABLE and must Selected before initiating any action on it

SF_UNOBSERVABILITY_PKC

This function assures that processing based on secure elements of the TOE does not reveal any information on those elements. For example, observation of a PIN verification cannot reveal the PIN value, observation of key comparaison cannot give information on the key.

SF_DISPATCHER

This function controls which operation can be executed regarding input data and parameters. it determines all supported commands including Bank management commands: APPLICATION BLOCK, APPLICATION UNBLOCK, PUT DATA, PASSCODE CHANGE UNBLOCK, OFFLINE PIN CHANGE.

Application Note

Implemented in ProcessData

SF_PLATFORM

This requirement is implemented by the platform. Details are in the Platform ST-lite [31].

SF_SINGLE_ACTIVATION

Implemented within the CRS, this function ensures that only one instance is active at the same time.

SF_INTEGRITY_CONFIDENTIALITY

This security function enforces check of confidentiality, integrity and/or origin of several objects especially the following ones: -PAP Keys; -PAP Counters; -PAP Transaction Parameters; -Issuing Bank Transaction Data;

These objects are accessed if their state permits it and if their confidentiality are well ensured. PAP Keys are handled by Cryptographic objects owned by the platform and are protected against disclosure and their integrity is ensured by the platform. Integrity is ensured by computing and checking MAC and Cryptogram using Session Keys. Mirrors are also used for this purpose. Input data are encrypted when confidentiality is required. These attributes are implemented within commands that handle those objects (GENERATE AC, PUT DATA, UPDATE RECORD, PIN CHANGE/UNBLOCK, APPLICATION BLOCK/UNBLOCK, and Second GENERATE AC).

SF_PAYMNT_AND_ADMIN_MANAGMNT

This security function implements security attributes (ACF.1.1) and rules (ACF.1.2) and enforces them through the commands that handle Reference Personal Code, PAP Counters, PAP Activation/Deactivation, PAP Locking/Unlocking and Log Entry. [Log entry can be accessed, for reading (if not empty) or for update, in both management and payment modes. The Log update is implemented within GENERATE AC command.] The integrity of data is ensured through MAC computation and comparison. [Reference Personal Code is managed by an object (OWNER PIN) owned by platform. The platform is in charge of controlling the integrity of the Reference Personal Control and the key by handling a checksum.] The Personal Code Presentation is requested in payment mode 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;

SF_TRANSACTION_FLOW

This security function implements Transaction flow following [75] and [76] specifications.

SF_TRANSACTION

This security function implements the use, by the S.PAP, of the necessary objects (Customer Account Information, PAP Counters, PAP Keys, PAP State Machine, PAP Transaction Parameters) involved in a transaction (Read only for some of these objects and update of some others). This function is implements through commands that handle these objects (GPO, Read Record, and Generate AC/CDA). This function ensures the authentication (Online and OffLine) with the POS and the Issuing Bank.

SF_CARD_RISK_MANAGMNT

This security function implements the Card Action Analysis and ensures that the transaction is not rejected.

SF_ALARM

This security function detects all security violation (SAA) and takes appropriate actions (ARP).

SF_AUDIT_LOG

This SF stores a log with all auditable events (purchase currency, transaction date, transaction time, merchant's name, ...) these events are accessible on read only by U.Customer and U.Issuing bank.

SF_NO_REPLAY

This security function ensures that there is no replay on commands (ISSUERS Scripts and Verify) by updating a set of counters for each command.

SF_MANAGEMENT

The SF ensures access control and flow control for management of functionalities, behaviour of the PAP application, modification of user data and TSF data and security attributes of the PAP application. This TSF allows the Issuing Bank to provide restrictive values for security attributes. These security attributes have to be restrictive by default. The operations are allowed at post issuance by the issuing Bank once it's authenticated.

SF_USER_AUTH

This security function checks the authentication of the User (Customer or Issuing BANK). For the user, it checks the given Personal Code and detects unsuccessful authentication. It blocks the PAP Reference Personal Code if the maximum number of tries is reached (Handled by the VERIFY command).

For the Issuing Bank, it checks the issuing authentication data and detects the unsuccessful authentication. When the defined number of unsuccessful is reached, this function returns an error as specified in [12]

By default, the AP Transaction Processing State initially indicates no identification/authentication of the user.

Application Note

The Issuing authentication data is the cryptogram. The cryptogram is based on the ARPC and the application cryptogram generated during first Generate AC.

SF_CHALLENGE

This function ensures to generate an 8 bytes challenge generated by API javacard.security.RandomData.generateData.

SF_DATA_VALIDITY

This function assures the validity of the following data (Personnal code, counters,..).

SF_TIME_OUT

This function checks the timeout and cancels the transaction when it's reached. it's implemented within the middlet.

SF_SECURE_CHANNEL

This function ensures use of secure channel for exchange between PAP application and external entity (BANK TSM or MNO). The Secure Channel is opened to the initiative of an external entity, and it ensures integrity and confidentiality of the exchanges between PAP and this external entity.

8 ANNEX

8.1 Related documents

[1] "Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model", September 2012, Version 3.1 revision 4.

[2] "Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements", September 2012, Version 3.1 revision 4.

[3] "Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance requirements", September 2012, Version 3.1 revision 4.

[4] “Composite product evaluation for Smart Cards and similar devices”, September 2007, Version 1.0, CCDB-2007-09-001.

[5] PP SUN Java Card™ System Protection Profile Open Configuration V2.6, April 19, 2010.

[6] "Java Card - API" Application Programming Interfaces, Classic Edition, Version 3.01, February 23, 2009, Sun Microsystems.

[7] "Java Card – JCRE” Runtime Environment Specification, Classic Edition, Version 3.01, February 23, 2009, Sun Microsystems.

[8] "Java Card - Virtual Machine Specifications" Classic Edition, Version 3.01, February 23, 2009, Sun Microsystems.

[9] GlobalPlatform Card Specification – Version 2.2.1 – January 2011.

[10] GlobalPlatform Card Mapping Guidelines of existing GP v2.1.1 implementations on v2.2.1 – Version 1.0.1 – January 2011.

[11] GlobalPlatform Card Confidential Card Content Management – Card Specification v 2.2 – Amendment A – Version 1.0.1 – January 2011.

[12] GlobalPlatform Card UICC Configuration – Version 1.0.1 – January 2011.

[13] GlobalPlatform Card Contactless Services Card Specification v 2.2 – Amendment C Version 1.0– February 2010.

[14] Visa GlobalPlatform 2.1.1 Card Implementation Requirements – Version 2.0 – July 2007.

[15] "Identification cards - Integrated Circuit(s) Cards with contacts, Part 6: Inter industry data elements for interchange", ISO / IEC 7816-6 (2004).

[16] FIPS PUB 46-3 “Data Encryption Standard”, October 25, 1999, National Institute of Standards and Technology

[17] FIPS PUB 81 “DES Modes of Operation”, December, 1980, National Institute of Standards and Technology

[18] FIPS PUB 140-2 “Security requirements for cryptographic modules”, May 2001, National Institute of Standards and Technology

[19] FIPS PUB 180-3 “Secure Hash Standard”, October 2008 , National Institute of Standards and Technology

[20] FIPS PUB 186-3 "Digital Signature Standard (DSS)", June 2009, National Institute of Standards and Technology

[21] FIPS PUB 197, "The Advanced Encryption Standard (AES)", November 26, 2001, National Institute of Standards and Technology

[22] SP800_90 "Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)", March 2007, National Institute of Standards and Technology

[23] ANSI X9.31 "Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)", 1998, American National Standards Institute

[24] ISO/IEC 9796-1, Public Key Cryptography using RSA for the financial services industry", annex A, section A.4 and A.5, and annex C (1995)

[25] ISO/IEC 9797-1, "Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher", 1999, International Organization for Standardization

[26] PKCS#1 The public Key Cryptography standards, RSA Data Security Inc. 1993

[27] IEEE Std 1363a-2004, "Standard Specification of Public Key Cryptography – Amendment 1: Additional techniques", 2004, IEEE Computer Society

[28] IC Platform Protection Profile, Version 1.0, reference BSI-PP-0035 (15.06.2007).

[29] ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E, SC33F384E, all with optional cryptographic library NESLIB 3.0 Security Target - Public Version. SMD_Sx33Fxxx_ST_10_002 Rev 01.00. October 2010

[30] 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

[31] Security Target FLY3, NFC FlyBuy Platinum, FQR 110 6039, Issue 3, June 2012.

[32] 3GPP TS 21.111 (v6.3.0, Rel-6): USIM and IC card requirements

[33] 3GPP TS 22.038 (v6.5.0, Rel-6): USIM Application Toolkit (USAT) - Stage 1

[34] 3GPP TS 23.040 (v6.9.0, Rel-6): Technical realization of the Short Message Service (SMS)

[35] 3GPP TS 23.041 (v6.2.0, Rel-6): Technical realization of Cell Broadcast Service (CBS)

[36] 3GPP TS 23.048 (v5.9.0, Rel-5): Security Mechanisms for the (U)SIM application toolkit; Stage 2

[37] 3GPP TS 31.048 (v5.1.0, Rel-5): Test of (U)SAT security

[38] 3GPP TS 31.101 (v6.5.1, Rel-6): UICC-Terminal interface; Physical and Logical Characteristics

[39] 3GPP TS 31.102 (v6.21.0, Rel-6): Characteristics of the USIM Application

[40] 3GPP TS 31.103 (v6.11.0, Rel-6): Characteristics of the ISIM Application

[41] 3GPP TS 31.111 (v6.14.0, Rel-6): USIM Application Toolkit (USAT)

[42] 3GPP TS 31.115 (v6.5.0, Rel-6): Secured packet structure for (U)SIM Toolkit applications

[43] 3GPP TS 31.116 (v6.8.0, Rel-6): Remote APDU Structure for (U)SIM Toolkit applications

[44] 3GPP TS 31.122 (v6.3.0, Rel-6): USIM conformance test (card side)

[45] 3GPP TS 31.130 (v6.5.0, Rel-6): (U)SIM Application Programming Interface; (U)SIM API for Java™ Card

[46] 3GPP TR 31.900 (v7.1.0, Rel-7): SIM/USIM Internal and External Inter-working Aspects

[47] 3GPP TS 31.919 (v6.1.0, Rel-6): 2G/3G Java Card™ API based applet interworking

[48] 3GPP TS 33.102 (v6.5.0, Rel-6): 3G Security; Security architecture

[49] 3GPP TS 33.105 (v6.0.0, Rel-6): Cryptographic algorithm requirements

[50] 3GPP TS 35.205 (v6.0.0, Rel-6): Specification of the MILENAGE Algorithm Set

[51] 3GPP TS 42.017 (v4.0.0, Rel-4): SIM functional characteristics

[52] 3GPP TS 42.019 (v5.6.0, Rel-5): SIM API for Java Card™ - Stage 1 -

[53] 3GPP TS 43.019 (v5.6.0, Rel-5): Subscriber Identity Module Application Programming Interface; (SIM API) for Java Card™; Stage 2

[54] 3GPP TS 51.011 (v4.15.0, Rel-4): Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface

[55] 3GPP TS 51.014 (v4.5.0, Rel-4): Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface

[56] 3GPP TS 51.017 (v4.2.0, Rel-4): Test of SIM-ME interface (card side)

[57] ETSI TS 101 220 (v6.7.0, Rel-6): Application Identifiers for telecommunications

[58] ETSI TS 102 124 (v6.1.0, Rel-6): Transport Protocol for CAT Applications - Stage 1

[59] ETSI TS 102 127 (v6.13.0, Rel-6): Transport Protocol for CAT applications; Stage 2

[60] ETSI TS 102 151 (v6.0.0, Rel-6): Measurement of Electromagnetic Emission of SIM cards

[61] ETSI TS 102 221 (v6.12.0, Rel-6): UICC-Terminal interface; Physical and logical characteristics

[62] ETSI TS 102 222 (v6.11.0, Rel-6): Administrative Commands for telecommunications applications

[63] ETSI TS 102 223 (v6.13.0, Rel-6): Card Application Toolkit

[64] ETSI TS 102 224 (v6.1.0, Rel-6): CAT security – Stage 1

[65] ETSI TS 102 225 (v6.8.0, Rel-6): Secured packet structure for UICC applications

[66] ETSI TS 102 226 (v6.18.0, Rel-6): Remote APDU Structure for UICC based Applications

[67] ETSI TS 102 240 (v6.2.0, Rel-6): UICC Java Card™ API - Stage 1

[68] ETSI TS 102 241 (v6.12.0, Rel-6): UICC Java Card™ API - Stage 2

[69] ETSI TS 102 613 (v7.9.0, Rel-7): UICC – Contactless Front-end (CLF) Interface – Part 1: Physical and data link layer characteristics

[70] ETSI TS 102 622 (v7.9.0, Rel-7): UICC – Contactless Front-end (CLF) Interface – Host Controller Interface (HCI)

[71] ETSI TS 102 705 (v9.2.0, Rel-9): UICC Application Programming Interface for Java Card™ for Contactless Applications

[72] ETSI TS 131.111, Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) (Release 6)

[73] ETSI TS 131.130, Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS); (U)SIM Application Programming Interface (API);(U)SIM API for Java Card (3GPP TS 31.130 version 6.6.0 Release 6)

[74] CERTIFICATION OF APPLICATIONS ON “OPEN AND ISOLATING PLATFORM, Paris, the 4th March 2011. Reference: ANSSI-CCNOTE/10EN.01deW3

[75] [AEPM-1] Part I: Product Definition Release 3.0 – April 2011

[76] [AEPM-2] Part II: Technical Specification Release 3.0 – April 2011

[77] [AEPM-3] Payez Mobile - Visa Implementation Guide R3 0 - v1-1 – November 2011

[78] [AEPM-5] Guidance for Payment Application Package Security Target v2.1 – July 2009

[79] [Visa-1] Visa Mobile Contactless Payment Specification v1.4 – March 2011

[80] [Visa-UL#2] Visa Mobile Contactless Payment Specification v1.4 Update List Version 2 November 2012

[81] [Visa-2] Visa Mobile Contactless Payment Specification – Toolkit And Process Message Specification – Version 1.1 July 2011

[82] [Visa-3] Multi-Access Specification for Visa Mobile Payment Application – Version 1.1 September 2011

[83] [OT#1] VMPA Applet Software Requirement Specifications; 900234 00 SRS

[84] (U)SIM Java Card Platform Protection Profile Basic Configuration. ANSSI-CC-PP 2010/04

[85] Platform ST-Lite - FQR: 110 6052 issue 3 June 2012

[86] 900234 SRS – VMPA v1.0 SRS

[87] USIM V2.0 NFC V2 EAL4+ 768K on CCD2 - AGD_PRE FlyBuy Platinum / FQR 110 5884 Ed 6

[88] USIM V2.0 NFC V2 EAL4+ 768K on CCD2 - Application Security Recommendations - Flybuy Platinum/ FQR 110 5886 Ed 2

[89] USIM V2.0 NFC V2 EAL4+ 768K on CCD2 - Application Development Guide - Flybuy Platinum / FQR 110 5885 Ed 1

[90] USIM V2.0 NFC V2 EAL4+ 768K on CCD2 - Application Management Guide - Flybuy Platinum/FQR 110 5887 Ed 4

[91] NFC FlyBuy Platinum v2 – platform certificate - ANSSI-CC-2012/39

[92] Payez Mobile^{TM} Guidance for PAP Security Target - August 2011 version 1.0.3

[93] ALCHEMY – AGD_OPE – FQR 900 0140

[94] ALCHEMY – AGD_PRE – FQR 900 0141

[95] ANSSI-CC-2011/07

[96] ANSSI-CC-2011/07-M02

8.2 Abbreviations

Abbreviations	Definition
AAC	Application Authentication Cryptogram
AFL	Application File Locator
AES	Advanced Encryption Standard

Abbreviations	Definition
AID	Applet Identifier
APDU	Application Protocol Data Unit
API	Application Programmer Interface
APSD	Application Provider Security Domain
ARPC	Authorisation Response Cryptogram (within a transaction)
ARQC	Authorisation Request Cryptogram (within a transaction)
ATC	Application Transaction Counter
BIOS	Basic Input/Output System
CAS	Common Approval Scheme
CASD	Controlling Authority Security Domain
CC	Common Criteria
CDOL	Card risk management Data Object List
CEM	Common Evaluation Methodology
CVM	Card Verification Method
CVR	Card Verification Results
CM	Card Manager
CPLC	Card Production Life Cycle
DAP	Data Authentication Pattern
DDA	Dynamic Data Authentication
DDOL	Dynamic Data Object List
DES	Cryptographic module "Data Encryption Standard"
EAL	Evaluation Assurance Level
EC	Elliptic Curves
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMV	Europay MasterCard Visa
ES	Embedded Software
ETR_COMP	Report for a composite Smart Card Evaluation
FAT	File Allocation Table
GP	Global Platform
IC	Integrated Circuit
ISD	Issuer Security Domain
IT	Information Technology
JCP	Java Card Platform
JCR	Java Specification Request
JCRE	Java Card Runtime Environment
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

Abbreviations	Definition
PAP	Payment Application Package
PC	Personal Code
PIN	Personal Identification Number
POS	Point Of Sale
PP	Protection Profile
RNG	Random Number Generation
ROM	Read Only Memory
RSA	Cryptographic module "Rivest, Shamir, Adleman"
SF	Security Function
SFP	Security Function Policy
SHA-1	Cryptographic module "Secure hash standard"
SIM	Subscriber Identity Module
ST	Security Target
TOE	Target of Evaluation.
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
USIM	Universal Subscriber Identity Module
VASD	Validation Authority Security Domain
VM	Virtual Machine