Common Criteria
for Information Technology
Security Evaluation

Protection Profile

Intersector Electronic Purse and Purchase Device
(version without Last Purchase Cancellation)

Version 1.3

Issue March 2001

This version is in compliance with CC V2.1

Registered at the French Certification Body under the number PP/0101

For any kind of request for comments, please e-mail at certification.dcssi@sgdn.pm.gouv.fr

This document is paginated from i to ii and from 1 to 62

Table of contents

Chapter 1

PP introduction

1.1 PP Identification

Title: Intersector Electronic Purse and Purchase device Protection Profile (version without last purchase cancellation), Version 1.3, February 2001.

Registration: PP/0101

1 A glossary of terms used in the PP is given in annex A.

1.2 PP overview

2 This Protection Profile developed by the Société Financière du Porte-Monnaie Electronique Interbancaire is derived from two Protection Profiles PP/9908 and PP/9909. It aims the assurance level of the PP/9909 (EAL 4 augmented) with the functionalities of the PP/9908, that is without last purchase cancellation.

3 The intent of this Protection Profile is to specify functional and assurance requirements applicable to an Intersector Electronic Purse (IEP) and a Purchase Device (PD) used within an IEP system.

4 The goal of an IEP system consists of allowing electronic low value financial transactions without manipulating any coins nor bills. An IEP is supposed to be implemented in a smartcard.

5 A PD is a physical device installed at the Service Provider used to accept payment from an IEP in a Purchase Transaction. It may include a Secure Application Module (SAM), built on a integrated circuit module or not. In both cases, the Purchase Device shall provide the necessary security for purchase transactions and the collection process.

6 The main objectives of this Protection Profile are:

- to describe the Target of Evaluation (TOE),
- to describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE or its environment, the assumptions that are done and the organisational security policies that are used,

- to describe the security objectives for the TOE and its supporting environment,
- to specify the security requirements which includes the TOE IT functional requirements and the TOE IT assurance requirements,
- to give a rationale for this PP.

7 The Assurance level for this PP is EAL 4 augmented.

8 A product compliant with this PP may also offer additional functionalities that are not covered by this PP such as:

- purse-to-purse functionality,
- off-line reload,
- reimbursement functionality: the balance of the IEP is debited and the corresponding value is returned in one way or another to the purse holder,
- currency exchange functionality,
- self loading functionality,
- last purchase cancellation.

9 The additional security requirements corresponding the functionalities described above will have to be defined in an appropriate Security Target.

1.3 References

10 This Protection Profile has been build on the following references:

- [CC-1] Common Criteria for Information Technology security Evaluation, Part 1: Introduction and general model CCIMB-99-031, version 2.1, August 1999.

- [CC-2] Common Criteria for Information Technology security Evaluation, Part 2: Security Functional Requirements CCIMB-99-032, version 2.1, August 1999.

- [CC-3] Common Criteria for Information Technology security Evaluation, Part 3: Security Assurance Requirements CCIMB-99-033, version 2.1, August 1999.

- [CEM-2] Common Methodology for Information Technology security Evaluation, Part 2: Evaluation Methodology CEM-99/045, version 1.0, August 1999.

- [PP/9908] Intersector Electronic Purse and Purchase device Protection Profile (version for pilot scheme only), version 1.2, February 1999.

- [PP/9909] Intersector Electronic Purse and Purchase device Protection Profile, version 1.2, February 1999.

Chapter 2

TOE Description

11 This part of the PP describes the TOE as an aid to the understanding of its security requirements and address the product type, the intended usage and the general IT features of the TOE.

2.1 Product type

2.1.1 Introduction

12 This PP is related to the transaction kernel at the level of the IEP inside an IEP system. The main goal of an IEP system is to allow Electronic Value (EV) financial transactions, using an IEP and a PD.

13 Electronic Value (EV) is the counterpart of funds received by the EV provider. It is defined by the identity of the EV provider, the currency denomination and the amount. IEP or PD receiving amounts in several transactions may aggregate them into a single EV amount, as long as this does not alter the balance of the EV provider. Conversely, the EV amount stored in a IEP may be broken up and dispensed in several transactions.

2.1.2 Description

14 The TOE that is considered in this PP is overviewed by the following figure:

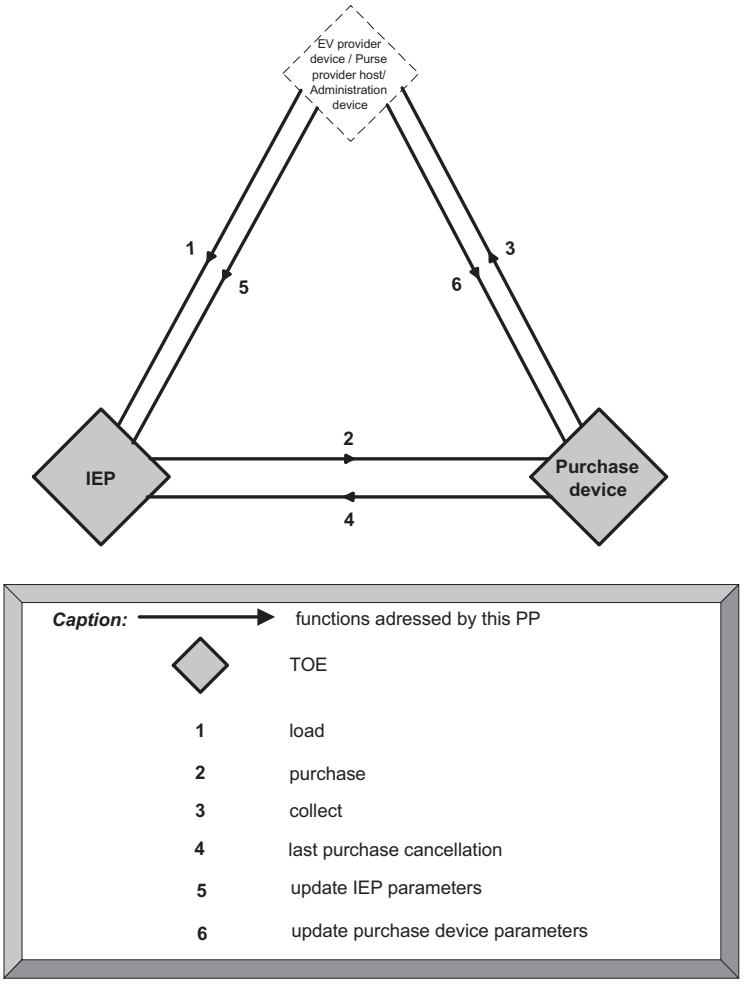

Fig. 2.1 - TOE Overview[1]

15 The TOE is composed of the IEP and the Purchase Device.

IEP

16 The IEP consists of an Integrated Circuit (IC) with an embedded software that is compliant with the PP Smartcard Integrated Circuit with Embedded Software (the PP/9809 is compliant with the PP/9806). The IC could support other applications including other IEPs. The main characteristics of an IEP are that it is prepaid, reloadable and interacts with the other part of the TOE: the purchase device. It may be anonymous or not. To be fully operational the IEP needs information. The actual introduction of this information is out of scope of this PP. The fully operational IEP contains various parameters that can be updated by an administration device.

1. Note that last purchase cancellation is out of the scope of this Protection Profile.

17 Towards the EV, an IEP is able to:

- store its amount of EV,
- indicate its amount of EV,
- debit its amount of EV via purchase transaction,
- credit its amount of EV via load transactions.

Purchase device

18 A PD is a physical device installed at the Service Provider used to accept payment from an IEP in a Purchase Transaction. It may include a Secure Application Module (SAM), built on a integrated circuit module or not. In both cases, the Purchase Device shall provide the necessary security for purchase transactions and the collection process. The PD is the part of the terminal of a retailer or a server used for electronic payment. It contains various parameters updated by the administration device.

19 Towards the EV, the purchase device is able to:

- store EV,
- receive an amount of EV from an IEP via purchase transaction,
- deliver stored EV via collect transaction.

2.1.3 Environment

IEP system overview

20 IEP system is a payment system intended for low value off line financial transactions. The global functioning of the IEP system is based on two cycles:

- a first one consisting in EV amount exchanges,
- as an economic counterpart, a second one consisting in payment and service,

21 To simplify, these cycles can be summarised as following:

- the purse holder gives funds (cash, credit cards, etc.) to the EV provider who loads his IEP with an equivalent amount of EV (load transaction),
- the purse holder asks the service provider for a service and transfers EV from his IEP to the PD (purchase transaction),
- the service provider asks the EV provider for cash or credit on its bank account (collection) in exchange for the EV.

22 The model proposed by this Protection Profile defines only one EV Provider: IEP systems with more than one EV provider may be modelized as many IEP systems that share purchase devices.

Actors

23 The actors identified in an IEP system are overviewed in the following figure:

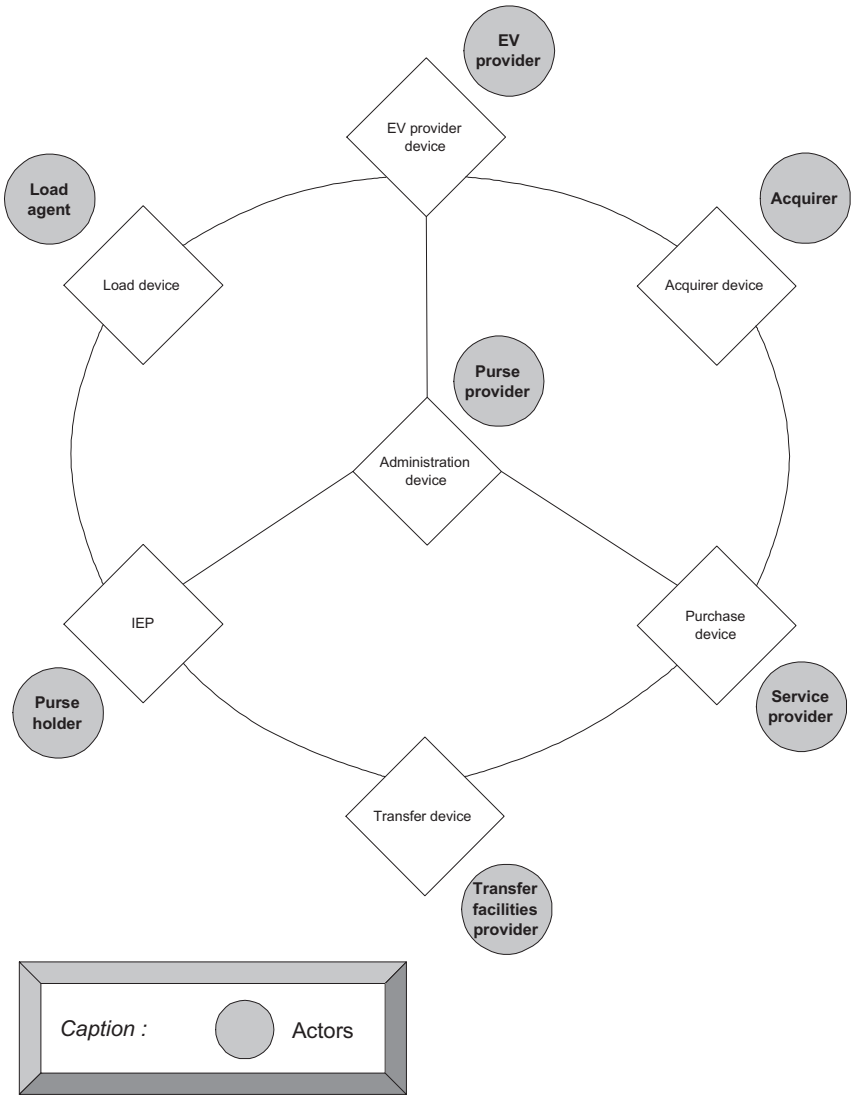

Fig. 2.2 - Actors

An entity may play the role of different actors in the IEP system.

Purse provider

24 A purse provider is fully responsible for the security of the IEP system. For example, he is responsible for the security of the IC itself and of the embedded software that can affect EV processing.The purse provider is also responsible for

administration of IEP and PD such as applets load or parameters update. In order to handle the administration operations the purse provider operates one or more administration devices. Administration operations include security management.

25 Depending on business arrangements with the service provider, the purse provider could ask the acquirer to aggregate several EV amounts associated with that service provider into a single EV amount in order to simplify EV collect and settlement process.

Purse holder

26 A purse holder is a person in possession of an IEP. Purse holders need to protect their IEP as if it is cash.

Service provider

27 A service provider sells services for which he accepts payment by IEP. In order to handle the purchase transactions the service provider operates one or more purchase devices in which he stores EV until collection and other information for his own purposes, if needed. The service provider is responsible for the operational security of the purchase device he controls.

28 The service provider can only be collected by its Acquirer.

Load agent

29 A load agent is a trusted agent of a EV provider, who executes the load transactions with the purse holder 's IEP on behalf of the EV provider, with EV created by the EV provider. It may also issue the IEP for the purse provider. In order to execute the load transaction the load agent operates a load device.

30 The load agent is responsible for the operational security of its part of the IEP system, and must protect the load devices he controls against unauthorised use.

Acquirer

31 An acquirer is a trusted agent of the EV provider who is responsible for collecting EV and, if possible, flow traceability data, from purchase devices concerning purchase transactions. He is also responsible for transferring payment received from the EV provider to the service provider for settlement. In order to handle the collection transactions the acquirer operates one or more acquirer devices.

EV provider

32 The EV provider guarantees the EV in IEP system. To this end, the EV provider:

- creates and dispenses EV in exchange for funds received,
- redeems collected EV and destroys it.

33 In order to handle these transactions, the EV provider operates one or more EV provider devices.

34 As a consequence of the EV provider guaranteeing for the EV in the IEP system, such an entity also defines the level of security required for the system to be protected against fraud. The purse provider is accountable to the EV provider for maintaining that level of security.

35 The management of the flow traceability data is under control of the EV provider.

Transfer facilities provider

36 The transfer facilities provider is responsible to transfer EV. It is optional as a transfer device can be reduced to a simple electric cable in certain cases. The transfer device contains no security functionality and so will be omitted in the next pages of the Protection Profile.

EV flow model

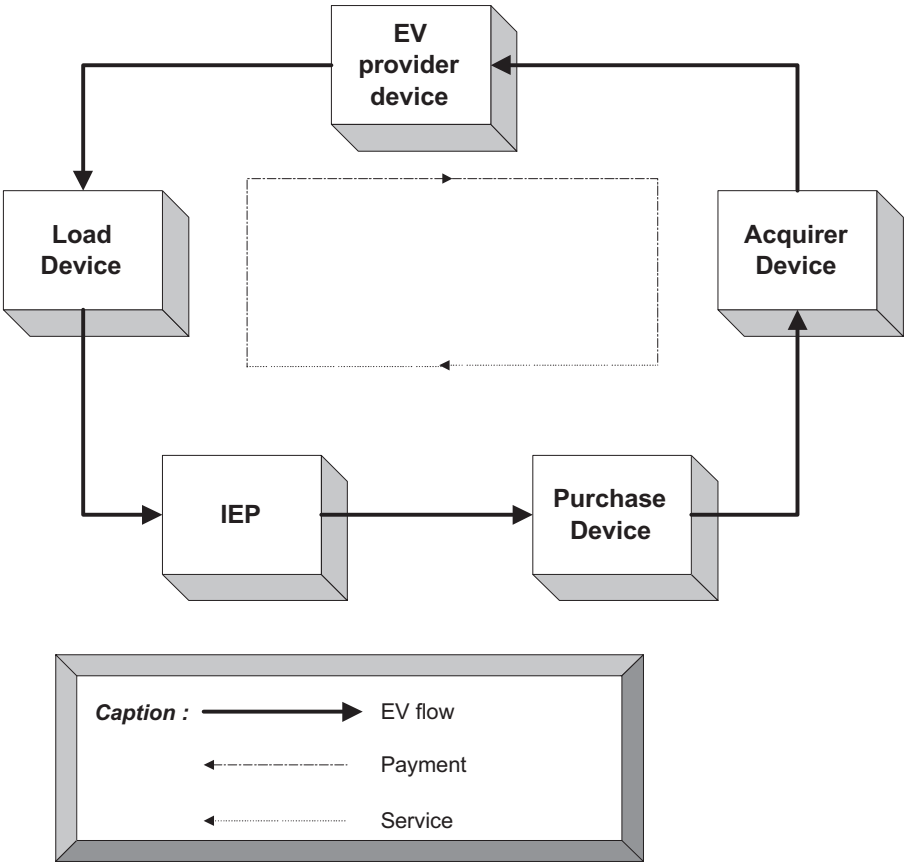

Fig. 2.3 - EV flow

37 EV is transferred only between the secure components of the participants in the IEP system. As an example, the flow of EV is described in figure 2.3.

38 During each transaction (load, purchase, collection) the EV credited on the one hand should always be equal to the EV debited on the other hand (as stated before (§32), only the EV provider is able to create / destroy EV). In order to settle, payment and services must be used.

2.2 IT features

39 The TOE IT functionalities consist of the following functions:

- load (1 of figure 2.1): the IEP is credited with an amount of EV created by the EV provider, via a load agent; the purse holder gives a corresponding amount of funds in turn (cf. “payment” of figure 2.3),
- purchase (2 of figure 2.1): the IEP is debited from an amount of EV while the purchase device receives the same amount of EV; the purse holder receives services in turn (cf. “service” of figure 2.3),
- collect (3 of figure 2.1): one or several amounts of the EV corresponding to a set of payment transactions stored by a PD is delivered to the EV provider device via an acquirer device; the service provider receives in turn the corresponding amount of money (cf. “payment” of figure 2.3),
- update IEP parameters (5 of figure 2.1): internal IEP parameters are updated by the purse provider. Parameters that are addressed are, for instance, the expense limit per transaction, the transaction keys,
- update PD parameters (6 of figure 2.1): internal purchase device parameters are updated by the purse provider.

Chapter 3

TOE Security Environment

40 This section describes the security aspects of the environment in which the TOE is intended to be used and addresses the description of the assets to be protected, the assumptions, the threats and the organisational security policies.

3.1 Assets

41 As the main objective of an IEP system is to preserve the EV flow, the assets that shall be protected are the following ones:

- Electronic Value (EV),
- Flow Traceability data,
- IEP and PD parameters such as the maximum amount of EV per IEP.

42 All these assets have to be protected in terms of integrity. Assets contained by PD that are addressed by this PP shall be protected in the same way than those contained by the IEP. PD and IEP shall have the same level of security.

43 These assets are all considered as user data for the Target of Evaluation.

3.2 Assumptions

44 The following general assumptions are done concerning the TOE:

A.AD	It is assumed that the Acquirer Device has capabilities to enter a secure state when a failure occurs during a collect transaction, or in case of any abnormal, corrupted, forged or replayed transactions.
A.LA	It is assumed that the LD has capabilities to enter a secure state when a failure occurs during a load transaction.
A. INDEP	The functionality of LA and the functionality of PD are independent applications: a SP could also be a load agent but in this case the application shall maintain two separate domains LA and PD: the two functionalities LA and PD have to be completely independent.

3.3 Threats

45 The TOE as defined in chapter 2 is required to counter the threats described hereafter; a threat agent wishes to abuse the assets either by functional attacks, environmental manipulations, specific hardware manipulations or by any other types of attacks.

MONEY LAUNDERING

T.LAUND_MON	Laundering of money in order to hide the real sources of the money.

USURPATION

46 Usurpation of identity of IEP system actors:

- actors not authorized by EV provider could be introduced in the IEP system in order to perform EV transactions,
- authorized actors could be used in the IEP system to play another role than those they are dedicated for.

47 This threat is divided into 7 threats:

T.USP_LA_LD	Usurpation of LA identity during a load transaction: an IEP is loaded with fraudulent EV by a fraudulent LD; it leads to EV creation and alters EV flow.[a]
T.USP_IEP_LD	Usurpation of IEP identity during a load transaction: a fraudulent IEP is loaded with EV by a LD; it leads to EV loss or alters EV flow.
T.USP_PP_EVP_PCH	Usurpation of PP and EVP identity during a purchase transaction: fraudulent EV is introduced in the PD by a fraudulent IEP; it leads to EV creation.
T.USP_PP_PCH_IEP	Usurpation of PP identity during a purchase transaction: EV is introduced in the PD by a fraudulent IEP; it alters EV flow.
T.USP_PP_PCH_PD	Usurpation of PP identity during a purchase transaction: EV is credited in a fraudulent PD; it leads to EV loss or it alters EV flow.

T.USP_PP_EVP_CLT	Usurpation of PP identity and EVP identity during a collect transaction: fraudulent EV is collected from a fraudulent PD by an AD; it leads to EV creation.
T.USP_A_CLT	Usurpation of A identity during a collect transaction: EV is collected from the PD by a fraudulent AD; it leads to EV loss and it alters EV flow.

a. It is understood as altering the EV flow model and then the traceability data.

REPLAY

48 Replay of a transaction. This type of threat is divided into 4 threats:

T.RPLY_LD	Replay of a load: different IEP are loaded, or the same IEP is loaded several times via a unique load transaction; it leads to EV creation.
T.RPLY_PCH_C	Replay of a purchase: different PD are credited, or the same PD is credited several times via a unique purchase transaction; it leads to EV creation.
T.RPLY_PCH_L	Replay of a purchase: different IEP are debited, or the same IEP is debited several times via a unique purchase transaction; it leads to EV loss.
T.RPLY_CLT	Replay of a collect: the same collect transaction is replayed several times to the A; it leads to EV creation.

FAILURE

49 A failure occurring during a transaction leads to a non-secure state inducing EV flow non-preservation. This type of threat is divided into 3 threats:

T.FAIL_PCH	Failure during a purchase transaction: EV is debited from an IEP whereas it is not credited in the PD; it leads to EV loss.
T.FAIL_CLT	Failure during a collect transaction: EV is collected from a PD whereas it is not credited in the AD; it leads to EV loss.
T.FAIL_LD	Failure during a load transaction: EV is debited from the LA whereas it is not credited in the IEP; it leads to EV loss.

FORGERY

50 Forgery of transactions characteristics such as EV amount in order to create or lose EV:

T.FORG_LD_C	Forgery of a load transaction in order to credit the IEP with an EV greater than the EV debited in the LD; it leads to EV creation.
T.FORG_LD_L	Forgery of a load transaction in order to credit the IEP with an EV lesser than the EV debited in the LD; it leads to EV loss.
T.FORG_PCH_C	Forgery of a purchase transaction in order to credit the PD with an EV greater than the EV debited in the IEP; it leads to EV creation.
T.FORG_PCH_L	Forgery of a purchase transaction in order to credit the PD with an EV lesser than the EV debited in the IEP; it leads to EV loss.
T.FORG_CLT_C	Forgery of a collect transaction in order to credit the AD with an EV greater than the EV collected from the PD; it leads to EV creation.
T.FORG_CLT_L	Forgery of a collect transaction in order to credit the AD with an EV lesser than the EV collected from the PD; it leads to EV loss.

FALSE REPUDIATION

Repudiation of transactions or part of transactions by IEP system actors:

T.REP_LD	The PH repudiates (at the EV provider) a load transaction in order to be loaded again; it leads to EV creation.
T.REP_PCH	The PH repudiates (at the EV provider) a purchase transaction in order to be recredited; it leads to EV creation.
T.REP_CLT	The SP repudiates (at its Acquirer) a collect transaction in order to be recredited; it leads to EV creation.
T.REP_PCH2	The SP repudiates (at the Purse Holder) a purchase transaction in order to be recredited; it leads to a theft against the PH.

LOSS OF INTEGRITY

51 Data stored at any step of the chain could be modified by unauthorized agents when it is stored or transferred; these concern EV, Flow Traceability data and IEP, PD parameters:

T.INTEG_EV	Unauthorized modification of stored EV.
T.INTEG_TD	Unauthorized modification of Flow Traceability data.
T.INTEG_PARA1	Unauthorized modification of IEP parameters.
T.INTEG_PARA2	Unauthorized modification of PD parameters.

3.4 Organisational Security policies

52 The following organisational security policies are mandatory for the TOE:

OSP.DEB_BEF_CRED	Debit always precedes credit during transaction.
OSP.AGGREG	When the PD is able to aggregate several amounts of EV into one overall amount, the result is a new total with the value equivalent to the sum of all the original totals.

OSP.PH_BEHAV	IEP shall be kept by PH as if they were real purses with coins and bank notes and shall not be lent, specially to untrusted persons.
OSP.A_LA_TRUSTED	The A and the LA are trusted agent of the EVP.
OSP.EV_INDIC	There shall exist means to indicate to the PH the amount of the EV of the transaction.
OSP.INTENT_TRANS	Each IEP transaction is an intentional operation of the user. A procedure defined by the Purse provider shall exist in order to allow the PH either accepts or rejects the transaction.
OSP.IEP_ID	The IEP shall have a unique identification within the system.
OSP.IEP_PD	The PD shall have a unique identification for the Acquirer device.
OSP.LINK_SP_PD	The SP shall be linked to his PD (his bank account has to be credited once the collect is done).
OSP.SP_A_CLT	The SP can only be collected by his A.
OSP.LOAD	During a load, the IEP is able to aggregate the amounts of loaded EV to its global overall amount of EV, the result is a new total with the value equivalent to the sum of all the amounts.
OSP.ROLE	The TOE shall maintain security roles and these roles shall be independent.

Chapter 4

Security objectives

53 The security objectives for the TOE and for its environment are listed hereafter.

4.1 Security objectives for the TOE

54 The main security objective for the TOE is to ensure EV flow preservation. To do so it shall use state of art technology to achieve the following security objectives:

O.EV	The TOE security functions shall provide the means to avoid unauthorized creation or loss of EV.
O.INTEG_DATA	The TOE security functions shall provide the means to avoid unauthorized modification of flow traceability data and IEP or PD parameters during transfers or storage.
O.LOGICAL	The TOE security functions shall prevent logical entry to the TOE by persons, equipments or processes with no rights to access it and prevent actors from bypassing the EV flow model.
O.AUTH	The TOE security functions shall ensure authentication of the TOE itself for load devices and acquirer devices.
O.ACCESS	The TOE security functions shall ensure that user data are only accessed by authorized users.
O.OPERATE	The TOE security functions shall ensure the continued correct operation of its security functions especially in case of abnormal process of transactions such as interruption during transactions.
O.REPLAY	The TOE security functions shall ensure that replayed transactions are detected and countered.
O.TAMPER	The TOE security functions shall prevent physical tampering with its security critical parts.

O.RECORD	The TOE security functions shall record flow traceability data to support effective security management.
O.LIMIT	The stored EV in the IEP shall be limited by the value of a maximum amount.
O.DOMAIN	The TOE security functions shall maintain a separate domain from other applications for the IEP application.

4.2 Security objectives for the environment

O.SYSTEM	The EV Provider shall guarantee the EV in IEP system based on the system security policy. The actors of the system, including the PH shall apply the system security policy. The EV provider shall communicate to the PH the rules dealing with the use of the IEP.
O.EV_DISTRIB	LD and AD shall not create EV: they shall distribute to authorized parties the same amount of EV they received.
O.LA_FAIL	LD shall enter a secure state in case of failure during load transactions, abnormal transactions, replayed or forged transactions, without any loss or creation of EV.
O.LA_DOMAIN	One security domain shall be available for LD for its own execution that protects it from interference and tampering by unstrusted agents.
O.LA_RECORD	LD shall record necessary events and data to ensure that the information exists to support effective security management.
O.AUTH2	LD and AD shall prevent users from gaining access to and performing operations on resources for which they do not have permission.
O.PSEUDO	During a load, LD shall maintain two separate domains: the debit transaction domain on one hand, and the IEP load transaction on the other hand and these domains shall be separated.

O. INSTALL	The purse provider shall ensure that the TOE is delivered and installed in a manner which maintains IT security.
O. MANAGE	The purse provider shall ensure that the TOE is managed, administered and operated in a manner which maintains IT security.
O.ACQ	AD shall enter a secure state in case of failure during transactions, abnormal transactions, replayed or forged transactions, without any loss or creation of EV.
O.A_RECORD	AD shall record necessary events and data to ensure that the information exits to support effective security management.

Chapter 5

TOE security functional requirements

55 The TOE security functional requirements define the functional requirements for the TOE using only functional requirements components drawn from the Common Criteria Part 2.

56 The minimum strength of function level for the TOE security requirements is SOF-high.

5.1 Class FAU Security Audit

5.1.1 FAU_GEN.1 Audit data generation

57 The TOE Security Functions shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions,

This aspect of the functionality is not applicable: the audit functions are active at any time.

b) not specified.

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

58 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, and the outcome (success or failure) of the event; and

Date and time of the event: this has to be interpreted as a sequence of events recognizable by the TOE.

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]*.

Iteration	List of defined auditable events as a minimum
IEP	**- last load transaction** **- last transaction**
PD	**- all purchase transactions from last collect** **- last collect transaction**

Tab. 5.1 - List of defined auditable events

5.1.2 FAU_SAR.1: Audit review

59 The TSF shall provide [*assignment: authorised users*] with the capability to read [*assignment: list of audit information*] from the audit records.

60 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.3 FAU_STG.1: Protected audit trail storage

61 The TSF shall protect the stored audit records from unauthorised deletion.

62 The TSF shall be able to **detect** modifications to the audit records.

5.2 Class FCO Communication

5.2.1 FCO_NRO.2: Enforced proof of origin

63 The TSF shall enforce the generation of evidence of origin for transmitted [*assignment: list of information types*] at all times.

64 The TSF shall be able to relate the [*assignment: list of attributes*] of the originator of the information, and the [*assignment: list of information fields*] of the information to which the evidence applies.

65 The TSF shall provide a capability to verify the evidence of origin of information to [*selection: originator, recipient, [assignment: list of third parties*]] given [*assignment: limitations on the evidence of origin*].

Iteration	List of information types	List of attributes	List of information fields	Selection	Limitations on the evidence of origin
Purchase	**purchase transaction**		**Examples are: - EV, - IEP Id, - unique transaction Id**	**recipient originator EVP**	**immediate**
Authentication of the IEP	**IEP identification**				
Authentication of the PD	**PD identification**				

Tab. 5.2 - Enforced proof of origin iterations

5.2.2 FCO_NRR.2: Enforced proof of receipt

66 The TSF shall enforce the generation of evidence of receipt for received [*assignment: list of information types*].

67 The TSF shall be able to relate the [*assignment: list of attributes*] of the recipient of the information, and the [*assignment: list of information fields*] of the information to which the evidence applies.

68 The TSF shall provide a capability to verify the evidence of receipt of information to [*selection: originator, recipient, [assignment: list of third parties*]] given [*assignment: limitations on the evidence of receipt*].

Iteration	List of information types	List of attributes	List of information fields	Selection	Limitations on the evidence of receipt
Load	**load**		**Examples are: - EV, - LA Id, - unique load Id**	**recipient originator EVP**	**at least until the next load transaction**
Collect	**collect**		**Examples are: - - EV, - - A Id, - - unique collect Id**	**recipient originator EVP**	**immediately after collect reception**

Tab. 5.3 - Enforced proof of receipt iterations

5.3 Class FCS Cryptographic support

5.3.1 FCS_COP.1: Cryptographic operation

69 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].

70 **This functionality is needed as a minimum for the following functionalities:**

- **FCO_NRO.2,**
- **FCO_NRR.2,**
- **FIA_UAU.1,**
- **FDP_DAU.1.**

5.4 Class FDP: User data protection

5.4.1 FDP_ACC.2: Complete access control

71 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.

72 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.4.2 FDP_ACF.1: Security attribute based access control

73 The TSF shall enforce the [*assignment: access control SFP*] to objects based on [*assignment: security attributes, named groups of security attributes*].

74 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*].

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

76 The TSF shall explicitly deny access of subjects to objects based on the [a*ssignment: rules, based on security attributes, that explicitly deny access of subjects to objects*].

5.4.3 FDP_DAU.1: Basic Data authentication

77 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **EV**.

78 The TSF shall provide [*assignment: list of subjects*] with the ability to verify evidence of the validity of the indicated information.

Iteration	List of subjects
IEP	**Purchase Device**
Purchase Device	**IEP**

Tab. 5.4 - Basic Data authentication iterations

5.4.4 FDP_ETC.1: Export of user data without security attributes

79 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 TSC.

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

5.4.5 FDP_IFC.1: Subset information flow control

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

Minimal Rules handled by the information flow control SFP
- mutual authentication for each transaction
- secure usage of the maximum amount of EV per IEP

Tab. 5.5 - Minimal List of events handled by the information flow control SFP

5.4.6 FDP_IFF.1: Simple security attributes

82 The TSF shall enforce the [*assignment: information flow control SFP*] based on the following types of subject and information security attributes: [*assignment: the minimum number and type of security attributes*].

83 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]*.

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

85 The TSF shall provide the following [*assignment: list of additional SFP capabilities*].

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

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

5.4.7 FDP_ITC.1 Import of user data without security attributes

88 The TSF shall enforce the [*assignment: access control SFP and/or information flow control SFP*] when importing user data, controlled under the SFP, from outside of the TSC.

89 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

90 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [*assignment: additional importation control rules*].

5.4.8 FDP_SDI.1: Stored data integrity monitoring

91 The TSF shall monitor user data stored within the TSC for [*assignment: integrity errors*] on all objects, based on the following attributes: [*assignment: user data attributes*].

5.5 Class FIA Identification and authentication

5.5.1 FIA_UID.1: Timing of identification

92 The TSF shall allow [*assignment: list of TSF mediated actions*] on behalf of the user to be performed before the user is identified.

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

Refinement	List of TSF-mediated actions	Refinement
IEP identification by PD	**Examples are:** **- read of EV amount,** **- read of status,** **- identification, authentication of PD by IEP.**	**The user is defined as IEP. The IEP is identified on an individual basis.**

Tab. 5.6 - Identification refinement

5.5.2 FIA_UAU.1: Timing of authentication

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

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

Iteration	List of TSF-mediated actions	Refinement
LA authentication by IEP	**Examples are:** **- authentication of the IEP by the LA,** **- transferring information from the IEP to the LA.**	**The user is defined as the LA.**
A authentication by PD	**Examples are:** **- authentication of PD by A,** **- transferring information from the PD to A.**	**The user is defined as the A.**
IEP authentication by PD	**Examples are:** **- authentication of PD by IEP,** **- transferring information from the PD to IEP.**	**The user is defined as the IEP.**
PD authentication by IEP	**Examples are:** **- identification, authentication of IEP by PD,** **- transferring information from the IEP to PD.**	**The user is defined as the PD.**

Tab. 5.7 - Authentication iterations

5.5.3 FIA_UAU.3: Unforgeable authentication

96 The TSF shall **detect and prevent** use of authentication data that has been forged by any user of the TSF.

97 The TSF shall **detect and prevent** use of authentication data that has been copied from any other user of the TSF.

5.5.4 FIA_UAU.4: Single-use authentication mechanisms

98 The TSF shall prevent reuse of authentication data related to [*assignment: identified authentication mechanism(s)*].

Iteration	Identified authentication mechanism(s)
LA authentication by IEP	**all authentication mechanisms of the LA**
A authentication by PD	**all authentication mechanisms of A**
IEP authentication by PD	**all authentication mechanisms of IEP**
PD authentication by IEP	**all authentication mechanisms of PD**

Tab. 5.8 - Single-use authentication mechanisms iterations

5.5.5 FIA_UAU.6: Re-authenticating

99 The TSF shall re-authenticate the user under the conditions [*assignment: list of conditions under which re-authentication is required*].

Iteration	List of conditions
LA authentication by IEP	**- begin of load transaction**
A authentication by PD	**- EV collect** **- flow traceability data delete**
IEP authentication by PD	**- begin of purchase transaction**
PD authentication by IEP	**- begin of purchase transaction**

Tab. 5.9 - Reauthenticating iterations

5.6 Class FPT Protection of the TSF

5.6.1 FPT_FLS.1: Failure with preservation of secure state

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

Iteration	List of types of failures in the TSF
Load	**load interrupt**
Purchase	**purchase interrupt**
Collect	**collect interrupt**

Tab. 5.10 - failure with preservation of secure state iterations

5.6.2 FPT_PHP.2: Notification of physical attack

101 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

102 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

103 For [*assignment: list of TSF devices/elements for which active detection is required*], the TSF shall monitor the devices and elements and notify [*assignment: a designated user or role*] when physical tampering with the TSF's devices or TSF's elements has occurred.

5.6.3 FPT_PHP.3: Resistance to physical attack

104 The TSF shall resist [*assignment: physical tampering scenarios*] to the [*assignment: list of TSF devices/elements*] by responding automatically such that the TSP is not violated.

5.6.4 FPT_RCV.4: Function recovery

105 The TSF shall ensure that [*assignment: list of SFs and failure scenarios*] have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

Iteration	List of SFs	Failure scenarios
Load		**load interrupt**
Purchase		**purchase interrupt**
Collect		**collect interrupt**

Tab. 5.11 - function recovery iterations

5.6.5 FPT_RPL.1: Replay detection

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

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

Iteration	List of identified entities	List of specific actions
Replay detection by IEP of a load by LA	**LD (load)**	**- if equals to last load then no more action - if different from last load ignore and/or trace**
Replay detection by PD of a purchase by IEP	**IEP (purchase)**	**- if equals to last purchase then no more action - if different from last purchase ignore and/or trace**
Collect	**PD (collect)**	**collect interrupt**

Tab. 5.12 - replay detection iterations

5.6.6 FPT_RVM.1: Non-bypassability of the TSP

108 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.6.7 FPT_SEP.1: TSF domain separation

109 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

110 The TSF shall enforce separation between the security domains of subjects in the TSC.

Chapter 6

TOE security assurance requirements

111 The assurance requirements is EAL 4 augmented of additional assurance components listed in the following sections.

112 These components are hierarchical ones to the components specified in EAL 4.

6.1 ADV_IMP.2 Implementation of the TSF

113 Developer action elements:

114 The developer shall provide the implementation representation for the entire TOE security functions.

115 Content and presentation of evidence elements:

116 The implementation representation shall unambiguously define the TOE security functions to a level of detail such that the TOE security functions can be generated without further design decisions.

117 The implementation representation shall be internally consistent.

118 The implementation representation shall describe the relationships between all portions of the implementation.

119 Evaluator action elements:

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

121 The evaluator shall determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

6.2 ALC_DVS.2 Sufficiency of security measures

122 Developer action elements:

123 The developer shall produce development security documentation.

124 Content and presentation of evidence elements:

125 The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the

confidentiality and integrity of the TOE design and implementation in its development environment.

126 The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

127 The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

128 Evaluator action elements:

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

130 The evaluator shall confirm that the security measures are being applied.

6.3 AVA_VLA.4 Highly resistant

131 Developer action elements:

132 The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

133 The developer shall document the disposition of identified vulnerabilities.

134 Content and presentation of evidence elements:

135 The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

136 The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

137 The evidence shall show that the search for vulnerabilities is systematic.

138 The analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

139 Evaluator action elements:

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

141 The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

142 The evaluator shall perform an independent vulnerability analysis.

143 The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

144 The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a high attack potential.

Chapter 7

Rationale

7.1 Introduction

146 This chapter presents the evidence used in the PP evaluation. This evidence supports the claims that the PP is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment.

7.2 Security Objectives rationale

147 This section demonstrates that the stated security objectives address all of the security environment aspects identified.

7.2.1 Threats

148 The table 7.1 maps the security objectives for the TOE and the security objective for the environment to the threats identified in the TOE environment.

Threats/ Objectives	Security objectives for the TOE	Security objectives for the environment	Para
T.LAUND_MON	O.LIMIT		149
T.USP_LA_LD	O.EV, O.LOGICAL, O.ACCESS		151
T.USP_IEP_LD	O.AUTH	O.AUTH2	154
T.USP_PP_EVP_PCH	O.EV, O.LOGICAL, O.ACCESS		156
T.USP_PP_PCH_IEP	O.LOGICAL, O.INTEG_DATA, O.ACCESS		158
T.USP_PP_PCH_PD	O.EV, O.LOGICAL, O.INTEG_DATA, O.ACCESS		160
T.USP_PP_EVP_CLT	O.AUTH	O.AUTH2	162
T.USP_A_CLT	O.EV, O.LOGICAL, O.INTEG_DATA, O.ACCESS		164
T.RPLY_LD	O.EV, O.REPLAY		166
T.RPLY_PCH_C	O.EV, O.REPLAY		168
T.RPLY_PCH_L	O.EV, O.REPLAY		170
T.RPLY_CLT		O.ACQ	172
T.FAIL_PCH	O.EV, O.OPERATE		174
T.FAIL_CLT	O.EV, O.OPERATE	O.ACQ	176
T.FAIL_LD	O.EV, O.OPERATE	O.LA_FAIL	178
T.FORG_LD_C	O.EV, O.INTEG_DATA		180
T.FORG_LD_L	O.EV, O.INTEG_DATA		182
T.FORG_PCH_C	O.EV, O.INTEG_DATA		184
T.FORG_PCH_L	O.EV, O.INTEG_DATA		186
T.FORG_CLT_C	O.EV, O.INTEG_DATA	O.ACQ	188
T.FORG_CLT_L	O.EV, O.INTEG_DATA	O.ACQ	190
T.REP_LD	O.EV, O.RECORD, O.ACCESS	O.PSEUDO, O.LA_RECORD, O.SYSTEM	192
T.REP_PCH	O.EV, O.RECORD, O.ACCESS	O.SYSTEM	194
T.REP_CLT	O.EV, O.RECORD, O.ACCESS	O.A_RECORD, O.SYSTEM	196
T.REP_PCH2	O.ACCESS, O.RECORD	O.SYSTEM	198
T.INTEG_EV	O.EV, O.LOGICAL, O.ACCESS, O.TAMPER, O.DOMAIN	O.EV_DISTRIB, O.INSTALL, O.MANAGE	200
T.INTEG_TD	O.ACCESS, O.LOGICAL, O.INTEG_DATA, O.TAMPER, O.DOMAIN		202
T.INTEG_PARA1	O.INTEG_DATA, O.LOGICAL, O.ACCESS, O.TAMPER, O.DOMAIN	O.INSTALL, O.MANAGE	204
T.INTEG_PARA2	O.INTEG_DATA, O.LOGICAL, O.ACCESS, O.TAMPER, O.DOMAIN	O.INSTALL, O.MANAGE	206

Tab. 7.1 - Threats and Security objectives

Threats on money laundering

149 T.LAUND_MON: money laundering in order to hide the real sources of the money. The IEP could be a means by which laundered money could be stored.

150 The threat T.LAUND_MON is addressed by the security objective for the TOE O.LIMIT:

- the objective O.LIMIT avoids the storage of important amount of EV in the IEP. This provides means to prevent laundering.

Threats on identity usurpation of IEP system actors

151 T.USP_LA_LD: usurpation of LA identity during a load transaction: a fraudulent load device loads fraudulent EV in an IEP.

152 The IEP is an identified IEP of the system; the fraudulent device is unknown of the system. Fraudulent EV means that this EV has no counterpart of a bank deposit. The IEP may be loaded with fraudulent EV, the result is that the global amount of EV has changed: it leads to EV creation and alters EV flow. The PH may use this amount of fraudulent EV in a purchase transaction.

153 The threat T.USP_LA_LD is addressed by the security objectives for the TOE O.EV, O.LOGICAL and O.ACCESS:

- the objective O.EV is applicable to the IEP and ensures EV flow preservation so that fraudulent creation or loss of EV is not allowed.

- the objectives O.LOGICAL and O.ACCESS are applicable to the IEP and ensure that the IEP will grant access to its own functionalities to authorized users or equipments which have been authenticated as a prerequisite.

154 T.USP_IEP_LD: usurpation of IEP identity during a load transaction: a load device of the IEP system loads a fraudulent IEP with EV. It leads to EV loss if EV is not used in the system anymore or alters EV flow if the fraudulent IEP wants to use this EV in a purchase transaction but this aspect of the threat is detailed by the threat T.USP_PP_PCH_PD.

155 The threat T.USP_IEP_LD is addressed by the security objective for the environment O.AUTH2 and the security objective for the TOE O.AUTH:

- the objective O.AUTH2 is applicable to the load device and ensure that the LD will distribute EV only to authorized users (authorized IEP) which have been previously authenticated.

- the objective O.AUTH is applicable to the IEP: IEP shall authenticate itself for the load device; this objective is the counterpart of the first one.

156 T.USP_PP_EVP_PCH: usurpation of PP and EVP identity during a purchase transaction: fraudulent EV (unknown from the system, it has no counterpart of a

bank deposit) is introduced in the Purchase Device by a fraudulent IEP. The result is that the global amount of EV has changed: it leads to EV creation.

157 The threat T.USP_PP_EVP_PCH is addressed by the security objectives for the TOE O.EV, O.LOGICAL and O.ACCESS:

- the objective O.EV is applicable to the PD and ensures EV flow preservation so that fraudulent creation of EV in the PD is not allowed.

- the objectives O.LOGICAL and O.ACCESS are applicable to the PD and ensure that the PD will grant access to its own functionalities to authorized users or equipments which have been authenticated as a prerequisite.

158 T.USP_PP_PCH_IEP: usurpation of PP identity during a purchase transaction: EV is introduced in the PD by a fraudulent IEP. This threat is comparable to the previous one but in this case, the PD will receive real EV so there is no EV creation, it only alters EV flow.

159 The threat T.USP_PP_PCH_IEP is addressed by the security objectives for the TOE O.LOGICAL, O.ACCESS, and O.INTEG_DATA:

- the objectives O.LOGICAL and O.ACCESS are applicable to the PD and ensure that the PD will grant access to its own functionalities to authorized users or equipments which have been authenticated as a prerequisite.

- the objective O.INTEG_DATA is applicable to the PD and ensures that the flow traceability data of the purchase transaction remain unmodified. This would be a means to detect such an attack a posteriori.

160 T.USP_PP_PCH_PD: usurpation of PP identity during a purchase transaction: EV from a IEP of the system is credited in fraudulent purchase device: there is no EV creation but this threat leads to EV flow inconsistency or EV loss.

161 The threat T.USP_PP_PCH_PD is addressed by the security objectives for the TOE O.EV, O.LOGICAL, O.INTEG_DATA, O.ACCESS:

- the objective O.EV is applicable to the IEP and ensures EV flow preservation so that fraudulent loss of EV is not allowed.

- the objectives O.LOGICAL and O.ACCESS are applicable to the IEP and ensure that the IEP will grant access to its own functionalities to authorized users or equipments which have been authenticated as a prerequisite.

- the objective O.INTEG_DATA is applicable to the IEP and ensures that the flow traceability data of the purchase transaction remain unmodified. This would be a means to detect such an attack a posteriori.

162 T.USP_PP_EVP_CLT: usurpation of PP identity and EVP identity during a collect transaction: fraudulent EV (it means that there is no counterpart in a bank deposit) is collected from a fraudulent purchase device by an acquirer device: it leads to EV creation.

163 The threat is addressed by the security objectives for the environment O.AUTH2 and the security objective for the TOE O.AUTH:

- the security objective O.AUTH2 is applicable to the acquirer device and ensure that the AD will collect EV only to authorized users (authorized PD) which have been previously authenticated.

- the security objective O.AUTH is applicable to the TOE (both IEP and PD): IEP shall authenticate itself for the load device and PD shall also authenticate itself for the acquirer device; this objective is the counterpart of the first one.

164 T.USP_A_CLT: usurpation of A identity during a collect transaction: EV is collected from the purchase device by a fraudulent acquirer device. It leads to EV loss and alters EV flow.

165 The threat T.USP_A_CLT is addressed by the security objectives for the TOE O.EV, O.LOGICAL, O.INTEG_DATA, O.ACCESS:

- the objective O.EV is applicable to the PD and ensures EV flow preservation so that fraudulent loss of EV is not allowed.

- the objectives O.LOGICAL and O.ACCESS are applicable to the PD and ensure that the PD will grant access to its own functionalities to authorized users or equipments (AD) which have been authenticated as a prerequisite.

- the objective O.INTEG_DATA is applicable to the PD and ensures that the flow traceability data of the collect transaction remain unmodified. This would be a means to detect such an attack a posteriori.

Threats on replayed transactions

166 T.RPLY_LD: replay of a load: different IEP are loaded or the same IEP is loaded several times via a unique load transaction; it leads to EV creation.

167 The threat T.RPLY_LD is addressed by the security objectives for the TOE O.EV and O.REPLAY:

- the objective O.EV is applicable to the IEP and ensures EV flow preservation so that fraudulent creation of EV in the IEP is not allowed.

- the objective O.REPLAY is applicable to the IEP and ensure that the IEP will operate in a continuous secure state in case of load replayed transaction; the replayed transaction will be detected and rejected by the IEP.

168 T.RPLY_PCH_C: replay of a purchase: different PD are credited or the same PD is credited several times via a unique purchase transaction; it leads to EV creation.

169 The threat T.RPLY_PCH_C is addressed by the security objectives for the TOE O.EV and O.REPLAY:

- the objective O.EV is applicable to the PD and ensures EV flow preservation so that fraudulent creation of EV in the PD is not allowed.

- the objective O.REPLAY is applicable to the PD and ensure that the PD will operate in a continuous secure state in case of purchase replayed transaction; the replayed transaction will be detected and rejected by the PD.

170 T.RPLY_PCH_L: replay of a purchase: different IEP are debited or the same IEP is debited several times via a unique purchase transaction; it leads to EV loss.

171 The threat T.RPLY_PCH_L is addressed by the security objectives for the TOE O.EV and O.REPLAY:

- the objective O.EV is applicable to the IEP and ensures EV flow preservation so that fraudulent loss of EV in the IEP is not allowed.

- the objective O.REPLAY is applicable to the IEP and ensure that the IEP will operate in a continuous secure state in case of purchase replayed transaction; the replayed transaction will be detected and rejected by the IEP.

172 T.RPLY_CLT: replay of a collect: the same collect transaction is replayed several times to the A; it leads to EV creation. This threat is not addressed by the TOE but by its environment.

173 The threat T.RPLY_CLT is addressed by the security objective for the environment O.ACQ:

- the objective O.ACQ ensures that the acquirer device will enter a secure state in case of collect replayed transactions, by detecting any replayed transactions and ignoring them.

Threats on failure during transactions

174 T.FAIL_PCH: failure during a purchase transaction: EV is debited from an IEP whereas it is not credited in the PD; it leads to EV loss.

175 The threat T.FAIL_PCH is addressed by the security objectives for the TOE O.EV and O.OPERATE:

- the objective O.EV is applicable to the TOE and ensures EV flow preservation so that fraudulent loss of EV in the TOE is not allowed.

- the objective O.OPERATE is applicable to the TOE and ensure that the TOE will continue correct operation of its security functions in case of abnormal process during transactions.

176 T.FAIL_CLT: failure during a collect transaction: EV is collected from the PD whereas it is not credited to the Acquirer Device; it leads to EV loss.

177 The threat T.FAIL_CLT is addressed by the security objectives for the TOE O.EV, O.OPERATE and the security objective for the environment O.ACQ:

- the objective O.EV is applicable to the TOE and ensures EV flow preservation in any case.
- the objective O.OPERATE is applicable to the TOE and ensure that the TOE will continue correct operation of its security functions in case of abnormal process during transactions.
- the objective O.ACQ ensures that the acquirer device will enter a secure state in case of abnormal process during collect transactions.

178 T.FAIL_LD: failure during a load transaction: EV is debited from the load device whereas it is not credited in the IEP; it leads to EV loss.

179 The threat T.FAIL_LD is addressed by the security objectives for the TOE O.EV, O.OPERATE and the security objective for the environment O.LA_FAIL:

- the objective O.EV is applicable to the TOE and ensures EV flow preservation in any case.
- the objective O.OPERATE is applicable to the TOE and ensure that the TOE will continue correct operation of its security functions in case of abnormal process during transactions.
- the objective O.LA_FAIL ensures that the load device will enter a secure state in case of failure during a load transaction without any loss or creation of EV.

Threats on forged transactions

180 T.FORG_LD_C: forgery of a load transaction in order to credit the IEP with an EV greater than the EV debited in the load device; it leads to EV creation.

181 The threat T.FORG_LD_C is addressed by the security objectives for the TOE O.EV, O.INTEG_DATA:

- the objective O.EV is applicable to the IEP and ensures EV flow preservation so that fraudulent creation of EV in the TOE is not allowed.
- the objective O.INTEG_DATA is applicable to the IEP and ensures that the flow traceability data of the load transaction remain unmodified. This would be a means to detect such an attack a posteriori.

182 T.FORG_LD_L: forgery of a load transaction in order to credit the IEP with an EV lesser than the EV debited in the load device; it leads to EV loss.

183 The threat T.FORG_LD_L is addressed by the same security objectives for the TOE O.EV, O.INTEG_DATA:

- the objective O.EV is applicable to the IEP and ensures EV flow preservation so that fraudulent loss of EV in the TOE is not allowed.

- the objective O.INTEG_DATA is applicable to the IEP and ensures that the flow traceability data of the load transaction remain unmodified. This would be a means to detect such an attack a posteriori.

184 T.FORG_PCH_C: forgery of a purchase transaction in order to credit the PD with an EV greater than the EV debited in the IEP; it leads to EV creation.

185 The threat T.FORG_PCH_C is addressed by the security objectives for the TOE O.EV, O.INTEG_DATA:

- the objective O.EV is applicable to the TOE and ensures EV flow preservation so that fraudulent creation of EV in the TOE is not allowed.

- the objective O.INTEG_DATA is applicable to the TOE and ensures that the flow traceability data of the purchase transaction remain unmodified. This would be a means to detect such an attack a posteriori.

186 T.FORG_PCH_L: forgery of a purchase transaction in order to credit the PD with an EV lesser than the EV debited in the IEP; it leads to EV loss.

187 The threat T.FORG_PCH_L is addressed by the same security objectives for the TOE O.EV, O.INTEG_DATA:

- the objective O.EV is applicable to the TOE and ensures EV flow preservation so that fraudulent loss of EV in the TOE is not allowed.

- the objective O.INTEG_DATA is applicable to the TOE and ensures that the flow traceability data of the load transaction remain unmodified. This would be a means to detect such an attack a posteriori.

188 T.FORG_CLT_C: forgery of a collect transaction in order to credit the AD with an EV greater than the EV collected from the PD; it leads to EV creation.

189 The threat T.FORG_CLT_C is addressed by the security objectives for the TOE O.EV, O.INTEG_DATA and requires the security objective for the environment O.ACQ:

- the objective O.EV is applicable to the TOE and ensures EV flow preservation so that fraudulent creation of EV in the TOE is not allowed.

- the objective O.INTEG_DATA is applicable to the PD and ensures that the flow traceability data of the collect transaction remain unmodified. This would be a means to detect such an attack a posteriori.

- the objective O.ACQ ensures that the acquirer device will enter a secure state in case of forged collect transactions.

190 T.FORG_CLT_L: forgery of a collect transaction in order to credit the AD with an EV lesser than the EV collected from the PD; it leads to EV loss.

191 The threat T.FORG_CLT_L is addressed by the same security objectives for the TOE O.EV, O.INTEG_DATA and the security objective for the environment O.ACQ:

- the objective O.EV is applicable to the PD and ensures EV flow preservation so that fraudulent creation of EV in the TOE is not allowed.
- the objective O.INTEG_DATA is applicable to the PD and ensures that the flow traceability data of the collect transaction remain unmodified. This would be a means to detect such an attack a posteriori.
- the objective O.ACQ ensures that the acquirer device will enter a secure state in case of forged collect transactions.

Threats on false repudiation

192 T.REP_LD: the PH repudiates a load transaction in order to be loaded again; it leads to EV creation.

193 The threat T.REP_LD is addressed by the security objectives for the TOE O.EV, O.RECORD, O.ACCESS and requires the security objectives for the environment O.LA_RECORD, O.PSEUDO, O.SYSTEM:

- the objective O.EV is applicable to the IEP and ensures EV flow preservation so that fraudulent creation of EV in the TOE is not allowed.
- the objective O.RECORD is applicable to the IEP and ensures that the IEP records necessary events and data (flow traceability data) in order to be presented again as elements of evidence of the real transaction.
- the objective O.ACCESS is applicable to the IEP and ensures that flow traceability data will be accessible to authorized users (Purse Provider and EV provider).
- the objective O.LA_RECORD is applicable to the load device and ensures that the LD records necessary events and data (flow traceability data) in order to be presented again as an element of evidence of the real transaction.
- the objective O.PSEUDO is applicable to the load device and ensures that during a load transaction, there will not be any recorded link between the IEP identity on one hand and the elements of identification of the debit transaction on the other hand. O.LA_RECORD and O.PSEUDO work together.
- the objective O.SYSTEM is applicable to the TOE environment and ensures that a security policy has been defined and rules have been explained to the PH: complaint process, period of time for complaint.

194 T.REP_PCH: a PH repudiates a purchase transaction in order to be recredited at the EV provider.

195 The threat T.REP_PCH is addressed by the security objectives for the TOE O.RECORD, O.EV, O.ACCESS and the security objective for the environment O.SYSTEM:

- the objective O.EV is applicable to the IEP and ensures EV flow preservation so that fraudulent creation of EV in the IEP is not allowed.
- the objective O.RECORD is applicable to the IEP and ensures that the IEP records necessary events and data (flow traceability data) in order to be presented again as an element of evidence of the real purchase transaction.
- the objective O.ACCESS is applicable to the IEP and ensures that flow traceability data will be accessible to authorized users (EV provider).
- the objective O.SYSTEM is applicable to the TOE environment and ensures that a security policy has been defined and rules have been explained to the PH: complaint process, period of time for complaint.

196 T.REP_CLT: the SP repudiates a collect transaction in order to be recredited; it leads to EV creation.

197 The threat T.REP_CLT is addressed by the security objectives for the TOE O.RECORD, O.EV, O.ACCESS and the security objectives for the environment O.A_RECORD, O.SYSTEM:

- the objective O.EV is applicable to the PD and ensures EV flow preservation so that fraudulent creation of EV in the PD is not allowed.
- the objective O.RECORD is applicable to the PD and ensures that the IEP records necessary events and data (flow traceability data) in order to be presented again as elements of evidence of the real collect transaction.
- the objective O.ACCESS is applicable to the PD and ensures that flow traceability data will be accessible to authorized users.
- the objective O.A_RECORD is applicable to the acquirer device and ensures that the AD records necessary events and data (flow traceability data) in order to be presented again as an element of evidence of the real transaction.
- the objective O.SYSTEM is applicable to the TOE environment and ensures that a security policy has been defined and rules have been detailed regarding complaint process, period of time for complaint.

198 T.REP_PCH2: the SP repudiates a purchase transaction in order to be credited again; it leads to a theft against the PH.

199 The threat T.REP_PCH2 is addressed by the security objectives for the TOE O.RECORD, O.ACCESS and the security objective for the environment O.SYSTEM:

- the objective O.RECORD is applicable to the TOE and ensures that the TOE records necessary events and data (flow traceability data) in order to be presented again as an element of evidence of the real transaction.

- the objective O.ACCESS is applicable to the TOE and ensures that flow traceability data will be accessible to authorized users (Purse Provider and EV provider).

- the objective O.SYSTEM is applicable to the TOE environment and ensures that a security policy has been defined and rules have been explained to the PH: complaint process, period of time for complaint.

Threats on loss of integrity

200 T.INTEG_EV: EV is stored within the TOE in the IEP and in the PD. This threat deals with unauthorized modifications of stored EV.

201 The threat T.INTEG_EV is addressed by the security objectives for the TOE O.EV, O.LOGICAL, O.ACCESS, O.TAMPER, O.DOMAIN and the security objectives for the environment O.EV_DISTRIB, O.INSTALL, O.MANAGE:

- the objective O.EV is applicable to the TOE and ensures EV flow preservation so that unauthorized modification of EV in the TOE (IEP/PD) is not allowed.

- the objective O.LOGICAL is applicable to the TOE and ensures that any user of the TOE will be authenticated accordingly.

- the objective O.ACCESS is applicable to the TOE and ensures that any EV modification will be accessible only to authorized users.

- the objective O.TAMPER is applicable to the TOE and prevents any physical tampering of the TOE in order to modify any stored EV amounts within the TOE (avoids fraudulent EV creation).

- the objective O.DOMAIN is applicable to the TOE and prevents fraudulent usage of the TOE in order to modify any stored EV amounts within the TOE,

- the objective O.EV_DISTRIB ensures that EV is not modified during load transactions or collect transactions.

- the objective O.INSTALL ensures that fraudulent EV is not created during delivery and installation of the PD or during delivery process of the IEP.

- the objective O.MANAGE ensures that the TOE is managed securely: no fraudulent EV is created during any administration procedures.

202 T.INTEG_TD: flow traceability data are stored within the TOE in the IEP and in the PD. This threat deals with unauthorized modifications of flow traceability data.

203 The threat T.INTEG_TD is addressed by the security objectives for the TOE O.INTEG_DATA, O.ACCESS, O.TAMPER, O. DOMAIN and O.LOGICAL:

- the objective O.INTEG_DATA is applicable to the TOE and ensures flow traceability data integrity so that unauthorized modification of flow traceability data in the TOE (IEP/PD) is not allowed.

- the objective O.LOGICAL is applicable to the TOE and ensures that any user of the TOE will be authenticated accordingly.

- the objective O.ACCESS is applicable to the TOE and ensures that any modification of flow traceability data will be accessible only to authorized users.

- the objective O.TAMPER is applicable to the TOE and prevents any physical tampering of the TOE in order to modify any stored traceability data within the TOE,

- the objective O.DOMAIN is applicable to the TOE and prevents fraudulent usage of the TOE in order to modify any stored EV amounts within the TOE.

204 T.INTEG_PARA1: this threat deals with unauthorized modifications of IEP parameters such as maximum amount of EV per transaction, maximum stored EV ...

205 The threat T.INTEG_PARA1 is addressed by the security objectives for the TOE O.INTEG_DATA, O.LOGICAL, O.ACCESS, O.TAMPER, O.DOMAIN and the security objectives for the environment O.INSTALL, O.MANAGE:

- the objective O.INTEG_DATA is applicable to the TOE and ensures that IEP parameters in the IEP will not be modified by fraudulent users.

- the objective O.LOGICAL is applicable to the IEP and ensures that any user of the TOE will be authenticated accordingly.

- the objective O.ACCESS is applicable to the IEP and ensures that any modification of IEP parameters will be accessible only to authorized users.

- the objective O.TAMPER is applicable to the IEP and prevents any physical tampering of the TOE in order to modify any stored parameters within the TOE.

- the objective O.DOMAIN is applicable to the TOE and prevents fraudulent usage of the TOE in order to modify any stored EV amounts within the TOE.

- the objective O.INSTALL ensures that the delivery process of the IEP is managed securely and appropriate IEP parameters are set.

- the objective O.MANAGE ensures that the TOE is managed securely: modification of IEP parameters is under control of security administrative procedures.

206 T.INTEG_PARA2: this threat deals with unauthorized modifications of PD parameters.

207 The threat T.INTEG_PARA2 is addressed by the security objectives for the TOE O.INTEG_DATA, O.LOGICAL, O.ACCESS, O.TAMPER, O.DOMAIN and the security objectives for the environment O.INSTALL, O.MANAGE:

- the objective O.INTEG_DATA is applicable to the TOE and ensures that PD parameters in the PD will not be modified by fraudulent users.

- the objective O.LOGICAL is applicable to the PD and ensures that any user of the TOE will be authenticated accordingly.

- the objective O.ACCESS is applicable to the PD and ensures that any modification of PD parameters will be accessible only to authorized users.

- the objective O.TAMPER is applicable to the PD and prevents any physical tampering of the TOE in order to modify any stored parameters within the TOE.

- the objective O.DOMAIN is applicable to the TOE and prevents fraudulent usage of the TOE in order to modify any stored EV amounts within the TOE.

- the objective O.INSTALL ensures that delivery and installation of the PD is managed securely and appropriate PD parameters are set.

- the objective O.MANAGE ensures that the TOE is managed securely: modification of PD parameters is under control of security administrative procedures.

7.2.2 Organisational security policies

208 Table 7.2 gives the mapping between organisational security policies to the security objectives.

OSP/Objectives	Security objectives for the TOE	Security objectives for the environment	Rationale
OSP.DEB_BEF_CRED		O.SYSTEM	O.SYSTEM ensures that a system security policy is in place in the IEP system; this policy is in charge of defining every security relevant parameters of the system such as parameters derived from this OSP.
OSP.AGGREG		O.SYSTEM	O.SYSTEM ensures that a system security policy is in place in the IEP system; this policy is in charge of defining every security relevant parameters of the system such as parameters derived from this OSP.
OSP.PH_BEHAV		O.SYSTEM	O.SYSTEM ensures that a system security policy is in place in the IEP system; the security rules to be applied by the PH are detailed by O.SYSTEM.
OSP.A_LA_TRUSTED		O.EV_DISTRIB O.AUTH2, O.PSEUDO O.ACQ O.LA_FAIL O.LA_RECORD O.A_RECORD	O.EV_DISTRIB contributes to this OSP: LD and AD distribute the same amount of EV they have received; there is no creation of EV. O.AUTH2 contributes to this OSP: LD and AD authenticate any user. O.PSEUDO contributes to the same objective: it establishes the domain separation between two domains: debit transaction domain and IEP load transaction domain so that no private information is available on the IEP load transaction domain. O.LA_FAIL and O.ACQ ensure that LD and AD will enter a secure state in case of abnormal events (failure, abnormal transactions, replayed or forged transactions). O.LA_RECORD and O.A_RECORD provide necessary accountability of any security relevant information.
OSP.EV_INDIC		O.SYSTEM	O.SYSTEM ensures that a system security policy is in place in the IEP system; this policy will have to define such a procedure.
OSP.INTENT_TRANS		O.SYSTEM	O.SYSTEM ensures that a system security policy is in place in the IEP system; this policy will have to define such a procedure.
OSP.IEP_ID		O.SYSTEM	O.SYSTEM ensures that a system security policy is in place in the IEP system; this policy will have to define such a procedure.
OSP.IEP_PD		O.SYSTEM	O.SYSTEM ensures that a system security policy is in place in the IEP system; this policy will have to define such a procedure.
OSP.LINK_SP_PD		O.SYSTEM	O.SYSTEM ensures that a system security policy is in place in the IEP system; the linkability of the PD to the SP is to be defined by the system security policy.
OSP.SP_A_CLT	O.LOGICAL O.AUTH		O.LOGICAL ensures that the LD will authenticate any AD; O.AUTH ensures that the LD will authenticate itself when communicating with the AD.

Tab. 7.2 - Mapping organisational security policies and security objectives

OSP/Objectives	Security objectives for the TOE	Security objectives for the environment	Rationale
OSP.LOAD		O.SYSTEM	O.SYSTEM ensures that a system security policy is in place in the IEP system; this policy is in charge of defining every security relevant parameters of the system such as parameters derived from this OSP.
OSP.ROLE	O.ACCESS	O.SYSTEM	O.SYSTEM ensures that all the roles managed by the TOE are defined by the security policy. O.ACCESS ensures that an access control policy defines access rules to the user data; these rules take into account the determined roles of the TOE.

Tab. 7.2 - Mapping organisational security policies and security objectives

7.2.3 Assumptions

209 Table 7.3 maps assumptions to security objectives.

Assumptions/ Objectives	Security objectives for the environment	Rationale
A.AD	O.ACQ	Obvious. O.ACQ is a refinement of A.AD
A.LA	O.LA_FAIL	Obvious. O.LA_FAIL is a refinement of A.LA
A.INDEP	O.LA_DOMAIN	Obvious. O.LA_DOMAIN is a refinement of A.INDEP

Tab. 7.3 -Mapping assumptions and security objectives

7.3 Security requirements rationale

210 The **Security requirements rationale** shall demonstrate that the set of TOE security requirements is suitable to meet the security objectives.

7.3.1 Security functional requirements rationale

211 This section demonstrates that the combination of the security requirements is suitable to satisfy the identified TOE security objectives.

212 Each of the TOE security objectives is addressed by either functional or assurance requirements.

213 The following table demonstrates which requirements contribute to the satisfaction of each TOE security objective.

Security objectives/ Requirements	O.LIMIT	O.EV	O.INTEG_DATA	O.LOGICAL	O.AUTH	O.ACCESS	O.OPERATE	O.REPLAY	O.TAMPER	O.RECORD	O.DOMAIN
FAU_GEN.1										X	
FAU_SAR.1										X	
FAU_STG.1			X							X	
FCO_NRO.2					X						
FCO_NRR.2										X	
FCS_COP.1		X	X	X	X					X	
FDP_ACC.2		X	X			X					
FDP_ACF.1		X	X			X					
FDP_ETC.1		X	X			X					
FDP_ITC.1		X	X			X					
FDP_IFC.1	X	X									
FDP_IFF.1	X	X									
FDP_SDI.1		X	X			X					
FDP_DAU.1		X									
FIA_UAU.1				X							
FIA_UAU.3				X							
FIA_UAU.4				X							
FIA_UAU.6				X							
FIA_UID.1				X							
FPT_FLS.1		X	X				X				
FPT_PHP.2		X	X						X		
FPT_PHP.3		X	X						X		
FPT_RPL.1		X	X					X			
FPT_RCV.4		X	X				X				
FPT_RVM.1	X	X	X	X	X	X	X	X	X	X	X
FPT_SEP.1											X

Tab. 7.4 - Mapping of security requirements and TOE security objectives

214 This section describes why the security requirements are suitable to meet each of the TOE security objectives.

Requirements	Objectives	Rationale
FAU_GEN.1	O.RECORD	Record of flow traceability data needed for O.RECORD
FAU_SAR.1	O.RECORD	Review of audited events; contributes to O.RECORD
FAU_STG.1	O.RECORD, O.INTEG_DATA	Protection of audited events; contributes to O.RECORD and O.INTEG_DATA
FCO_NRO.2	O.AUTH	Proof of origin of information: applies to purchase transaction, identification elements of IEP and identification elements of PD, then covers O.AUTH
FCO_NRR.2	O.RECORD	Proof of receipt of information: applies to integrity of any information exchanged with authorized equipments. Necessary for non repudiation of receipt. (O.RECORD).
FCS_COP.1	O.EV, O.INTEG_DATA, O.LOGICAL, O.AUTH, O.RECORD	The TOE needs a high authentication mechanism based on cryptographic operation (challenge/ response) either to authenticate an equipment (O.LOGICAL) or to authenticate the TOE itself (O.AUTH). The cryptographic operation is also needed for calculation and verification of digital signatures which contribute to O.EV, O.INTEG_DATA or necessary for non repudiation (O.RECORD).
FDP_ACC.2	O.EV, O.INTEG_DATA, O.ACCESS	Applies directly to O.ACCESS and then O.EV and O.INTEG_DATA
FDP_ACF.1	O.EV, O.INTEG_DATA, O.ACCESS	Applies directly to O.ACCESS and then O.EV and O.INTEG_DATA
FDP_ETC.1	O.EV, O.INTEG_DATA, O.ACCESS	The TOE is supposed to exchange user data with authorized equipments. The integrity of these data is to be protected during transmission; these user data will be transmitted without security attributes.
FDP_IFC.1	O.LIMIT, O.EV	This requirement imposes that information flow is controlled under a precised policy. It applies directly to O.LIMIT (secure usage of maximum amount of EV per IEP) and O.EV (mutual authentication for each transaction).
FDP_IFF.1	O.LIMIT, O.EV	This requirement precises the information flow control rules with security attributes: it provides definition of those information rules and applies directly to O.LIMIT (secure usage of maximum amount of EV per IEP) and O.EV (mutual authentication for each transaction).
FDP_ITC.1	O.EV, O.INTEG_DATA, O.ACCESS	The TOE is supposed to receive user data from authorized equipments. The integrity of these data is to be protected during transmission; these user data will be transmitted without security attributes.
FDP_SDI.1	O.EV, O.INTEG_DATA, O.ACCESS	Applies to integrity of user data during intermediate storage (IEP or PD). Complementary with FDP_ETC.1 and FDP_ITC.1 which concern transmitted user data.
FDP_DAU.1	O.EV	Applies to integrity of user data during transmission within the TOE (from IEP to PD). Complementary with FDP_ETC.1, FDP_ITC.1, FDP_SDI.1

Tab. 7.5 - Rationale of security requirements

Requirements	Objectives	Rationale
FIA_UAU.1	O.LOGICAL	Authentication mechanisms; contributes to O.LOGICAL. See table 7.6 below.
FIA_UAU.3	O.LOGICAL	Authentication mechanisms; contributes to O.LOGICAL. See table 7.6 below.
FIA_UAU.4	O.LOGICAL	Authentication mechanisms; contributes to O.LOGICAL. See table 7.6 below.
FIA_UAU.6	O.LOGICAL	Authentication mechanisms; contributes to O.LOGICAL. See table 7.6 below.
FIA_UID.1	O.LOGICAL	Identification mechanisms; contributes to O.LOGICAL (IEP identification by PD) See table 7.6 below.
FPT_FLS.1	O.EV, O.INTEG_DATA, O.OPERATE	This requirement imposes that the TOE remains in a secure state in case of any failure; contributes to O.EV, O.INTEG_DATA and O.OPERATE.
FPT_PHP.2	O.EV, O.INTEG_DATA, O.TAMPER	This requirement implies that the TOE is capable of detecting physical tampering (IEP and PD), (O.TAMPER) covers any fraudulent user data modification by physical tampering within the TOE (O.EV, O.INTEG_DATA). The IEP and PD shall have the same level of security.
FPT_PHP.3	O.EV, O.INTEG_DATA, O.TAMPER	This requirement implies that the TOE is capable of resisting physical tampering (IEP), PD, (O.TAMPER) covers any fraudulent user data modification by physical tampering within the TOE (O.EV, O.INTEG_DATA). complementary to FPT_PHP.2. The IEP and PD shall have the same level of security.
FPT_RPL.1	O.EV, O.INTEG_DATA, O.REPLAY	This requirements imposes that the TOE is capable of replay detection which contributes to O.REPLAY. indirectly contributes to integrity of user data (O.EV, O.INTEG_DATA).
FPT_RCV.4	O.EV, O.INTEG_DATA, O.OPERATE	This requirement provides recovery ensuring either successful completion or recovery to a secure state .
FPT_RVM.1	all objectives	This requirement applies to all objectives by ensuring that any security function could not be bypassed.
FPT_SEP.1	O.DOMAIN	This requirement provides domain separation within the TOE ensuring that the IEP application will be independent from other applications.

Tab. 7.5 - Rationale of security requirements

215 The following table describes the case of Identification and Authentication functionalities.

I&A functionality	IEP	PD
LA Identification	There is no identification functionality; identification mechanisms are implicit and associated with Authentication functionality.	Not applicable
PD Identification		
IEP Identification	Not applicable	IEP identification by PD (FIA_UID.1)
A identification	Not applicable	There is no identification functionality; identification mechanisms are implicit and associated with Authentication functionality.
LA Authentication	LA Authentication by IEP (FIA_UAU.1, FIA_UAU.3, FIA_UAU.4, FIA_UAU.6) Contributes to O.LOGICAL.	Not applicable
IEP Authentication	Not applicable	IEP Authentication by PD (FIA_UAU.1, FIA_UAU.3, FIA_UAU.4, FIA_UAU.6) Contributes to O.LOGICAL.
PD Authentication	PD Authentication by IEP (FIA_UAU.1, FIA_UAU.3, FIA_UAU.4, FIA_UAU.6) Contributes to O.LOGICAL.	Not applicable
A Authentication	Not applicable	A authentication by PD (FIA_UAU.1, FIA_UAU.3, FIA_UAU.4, FIA_UAU.6) Contributes to O.LOGICAL.

Tab. 7.6 - Identification and Authentication Functionalities

7.3.2 Security functional requirements dependencies

216 This section demonstrates that all dependencies between security functional requirements components included in this PP are satisfied.

217 The following table lists all functional components, with a numeric number. The dependencies of each component are listed alongside that component with a reference to the line number of the component which satisfies them. Component

reference line numbers followed by (H) indicate that the dependency is satisfied by a hierarchical component to that referenced.

Number	Name	Dependent on	Line number
1	FAU_GEN.1	**FPT_STM.1**	**see para 219**
2	FAU_SAR.1	FAU_GEN.1	1
3	FAU_STG.1	FAU_GEN.1	1
4	FCO_NRO.2	**FIA_UID.1**	**see para 220**
5	FCO_NRR.2	**FIA_UID.1**	**see para 221**
6	FCS_COP.1	**FDP_ITC.1 or FCS_CKM.1, FCS_CKM.4 FMT_MSA.2**	**see para 222**
7	FDP_ACC.2	FDP_ACF.1	8
8	FDP_ACF.1	FDP_ACC.1, **FMT_MSA.3**	H(7), **see para 225**
9	FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	H(7), 11
10	FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1 **FMT_MSA.3**	H(7), 11, **see para 228**
11	FPD_IFC.1	FDP_IFF.1	12
12	FDP_IFF.1	FDP_IFC.1 **FMT_MSA.3**	11, **see para 226**
13	FDP_SDI.1	No dependencies	-
14	FDP_DAU.1	No dependencies	-
15	FIA_UAU.1	FIA_UID.1	**see para 227**
16	FIA_UAU.3	No dependencies	-
17	FIA_UAU.4	No dependencies	-
18	FIA_UAU.6	No dependencies	-
19	FIA_UID.1	No dependencies	-
20	FPT_FLS.1	ADV_SPM.1	EAL4
21	FPT_PHP.2	**FMT_MOF.1**	**see para 229**
22	FPT_PHP.3	No dependencies	-
23	FPT_RPL.1	No dependencies	-
24	FPT_RCV.4	ADV_SPM.1	EAL4
25	FPT_RVM.1	No dependencies	-
26	FPT_SEP.1	No dependencies	-

Tab. 7.7 -Functional dependencies analysis

218 Table shows that the functional components dependencies are satisfied by any functional components of the PP except for the components stated in bold characters, which are discussed hereafter.

FAU_GEN.1:

219 The dependency with FPT_STM.1 is not relevant to the TOE: correctness of time is no use for the TOE objectives. A refinement of the functionality precises that the

"date and time of the event" has to be interpreted as a sequence of events recognizable by the TOE.

FCO_NRO.2:

220 The dependency with FIA_UID.1 is not relevant to the TOE: there is no identification functionality for this context; identification mechanisms are implicit and associated with authentication functionality.

FCO_NRR.2:

221 The dependency with FIA_UID.1 is not relevant to the TOE: there is no identification functionality for this context; identification mechanisms are implicit and associated with authentication functionality.

FCS_COP.1:

222 The dependency with FCS_CKM.1 "Cryptographic key generation" is not relevant; the different keys stored and used by the TOE will be delivered to the TOE.

223 The dependency with FCS_CKM.4 "Cryptographic key destruction" is not relevant: destruction of the keys is out of the scope of the TOE.

224 The dependency with FMT_MSA.2 is not relevant: Security attributes are defined during development and manufacturing of the TOE and could not be modified during operational use.

FDP_ACF.1:

225 The dependency with FMT_MSA.3 is not relevant: Security attributes are defined during development and manufacturing of the TOE and could not be modified during operational use.

FDP_IFF.1:

226 The dependency with FMT_MSA.3 is not relevant: Security attributes are defined during development and manufacturing of the TOE and could not be modified during operational use.

FIA_UAU.1:

227 The table 7.6 describes the dependencies between Identification and Authentication functionalities for the TOE. The dependency between FIA_UAU.1 and FIA_UID.1 is to be understood with this table. In particular, this dependency is only applicable for the case of the IEP Identification and Authentication by the PD.

FDP_ITC.1:

228 The dependency with FMT_MSA.3 is not relevant: Security attributes are defined during development and manufacturing of the TOE and could not be modified during operational use.

FPT_PHP.2:

229 The dependency with FMT_MOF.1 is not relevant: during operational use of the TOE, the behaviour of security functions could not be changed.

7.3.3 Strength of function level rationale

230 Due to the definition of the TOE, it is very important that the claimed SOF should be high since the product critical security mechanisms have to be only defeated by attackers possessing a high level of expertise, opportunity and resources, successful attack being judged to be beyond normal practicality.

7.3.4 Security assurance requirements rationale

231 The assurance requirements of this Protection Profile are summarized in the following table.

Requirement	Name	Type
EAL4	Methodically Designes, Tested and Reviewed	Assurance level
ADV_IMP2	Implementation of the TSF	Higher hierarchical component
ALC_DVS.2	Sufficiency of security measures	Higher hierarchical component
AVA_VLA.4	Highly resistant	Higher hierarchical component

Tab. 7.8 - PP assurance requirements

Evaluation assurance level rationale

232 An assurance level of EAL4 is required for this type of TOE since it is intended to defend against sophisticated attacks. This evaluation assurance level was selected since it is designed to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. EAL4 represents the highest practical level of assurance expected for a commercial grade product. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defence against such attacks, the evaluators should have access to the low level design and source code.

233 The assurance level of EAL4 is achievable, since it requires no specialist techniques on the part of the developer.

Assurance augmentations rationale

234 Additional assurance requirements are also required due to the definition of the TOE.

235 ADV_IMP.2 Implementation of the TSF

The implementation representation is used to express the notion of the least abstract representation of the TSF, specifically the one that is used to create the TSF itself without further design refinement. IC dedicated software source code and IC hardware drawings are examples of TSF implementation representation.

This assurance component is a higher hierarchical component to EAL 4 (only ADV_IMP.1). It is important for a smartcard IC that the evaluator evaluates the implementation representation of the entire TSF and determine if the functional requirements in the Security Target are addressed by the representation of the TSF.

ADV_IMP.2 has dependencies with ADV_LLD.1 “Descriptive Low-Level design”, ADV_RCR.1 “Informal correspondence demonstration”, ALC_TAT.1 “Well defined development tools”. These assurance components are included in EAL4, then these dependencies are satisfied.

236 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE.

This assurance component is a higher hierarchical component to EAL4 (only ALC_DVS.1). Due to the nature of the TOE, there is a need for any justification of the sufficiency of these procedures to protect the confidentiality and integrity of the TOE.

ALC_DVS.2 has no dependencies.

237 AVA_VLA.4 Highly resistant

Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks.

This assurance requirement is achieved by the AVA_VLA.4 component. Independent vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication.

AVA_VLA.4 has dependencies with ADV_FSP.1 “Informal functional specification”, ADV_HLD.2 “Security enforcing high-level design”, ADV_LLD.1 “Descriptive low-level design”, ADV_IMP.1 “Subset of the implementation of the

TSF", AGD_ADM.1 "Administrator Guidance", AGD_USR.1 "User Guidance". All these dependencies are satisfied by EAL4.

7.3.5 Security requirements are mutually supportive and internally consistent

238 The purpose of this part of the PP Rationale is to show that the security requirements are mutually supportive and internally consistent.

239 EAL4 is an established set of mutually supportive and internally consistent assurance requirements.

240 The dependencies analysis for the additional assurance components in the previous section has shown that the assurance requirements are mutually supportive and internally consistent.

241 The dependencies analysis for the functional requirements described above demonstrates mutual support and internal consistency between the functional requirements.

242 Inconsistency between functional and assurance requirements can only arise if there are functional-assurance dependencies that are not met, a possibility which has been shown not to arise.

Annex A

Glossary

Acquirer (A)

An acquirer is a trusted agent of the EV provider who is responsible for collecting EV and, if possibly, flow traceability data, from purchase devices concerning purchase and purchase cancellation transactions.

Acquirer Device (AD)

In order to handle the collection transactions the acquirer operates one or more acquirer devices.

Electronic Value (EV)

Electronic Value (EV) is the counterpart of funds received by the EV provider. It is defined by the identity of the EV provider, the currency denomination and the amount**.**

EV Provider (EVP)

The EV provider guarantees the EV in IEP system. To this end, the EV provider:

- creates and dispenses EV in exchange for funds received,
- redeems collected EV and destroys it.

Intersector Electronic Purse (IEP)

The IEP consists of an Integrated Circuit (IC) with an embedded software. The IC could support other applications including other IEPs. The main characteristics of an IEP are that it is prepaid, reloadable, anonymous and interacts with the other part of the TOE: the purchase device.

Purse Provider

A purse provider is fully responsible for the security of the IEP system. For example, he is responsible for the security of the IC itself and of the embedded software that can affect EV processing.The purse provider is also responsible for administration of IEP and PD such as applets load or parameters update. In order to handle the administration operations the purse provider operates one or more administration devices. Administration operations include security management.

Service Provider (SP)

A service provider sells services for which he accepts payment by IEP. In order to handle the purchase transactions the service provider operates one or more purchase devices in which he stores EV until collection and other information for his own purposes, if needed.