EBS 111
VERSION 1

EUROPEAN COMMITTEE
FOR
BANKING STANDARDS

EUROPEAN BANKING STANDARD: THE INTEROPERABLE FINANCIAL SECTOR ELECTRONIC PURSE

ECBS

Issued: June 1999

Avenue de Tervueren, 12, 1040 Brussels.

Comments or enquiries on the document may be addressed to the Secretary General at the above address.

TABLE OF CONTENTS

1. SCOPE

This document defines the minimum technical requirements for obtaining interoperability between Electronic Purse Schemes. It is based on the ECBS Technical Report TR103 “Banking Sector Requirements for an Electronic Purse” and ECBS TR104 “The Interoperability of Electronic Purse Systems” (Extending model C).

Interoperability in this Standard is defined as the ability to obtain European Electronic Purse (EEP) services across different Purse Schemes in a common way based on technical compatibility.

The model allows for an auditable Electronic Purse Scheme:

- Operating in multiple currencies, for instance local currency and Euro currency (EUR).
- And, in addition, operating with Unlinked Purses and purses linked to accounts. The EEP application may coexist with other applications in the same chip, e.g. debit/credit applications.

The technical specification for the EEP conforms to the relevant parts of the EMV’96 ICC specification, [EMV’96], and is based on CEN prEN 1546 [prEN 1546].

Part 1 covers the interoperable scenarios, and defines the set of transactions needed for interoperability. Part 2 describes the security-critical aspects of the transactions and components and specifies a security architecture. Parts 3 provides a general description of the transactions.

The following transactions are defined as a minimum set for interoperability, and are therefore included in this Standard:

- Balance Inquiry
- Currency Exchange
- Log Inquiry
- Load
- Purchase
- Incremental Purchase
- Purchase Cancellation

Refund and reimbursement transactions are not considered interoperable, and are therefore not treated in this Standard. The EEP application may, however, be deactivated as part of a Load or Currency Exchange Transaction. Furthermore the Purse Provider may provide command scripts to be delivered to the EEP card as an extension to the Load or Currency Exchange Transaction. Additional transactions may be supported domestically.

It is out of the scope of this Standard to try to define the monetary regulations related to the generation or the issuing of currencies in each country. The operating regulations related to claims, user interface, charge back, blacklist and emergency list management, risk management, and regulations related to the Certification Authority needed for interoperability, etc. are also not treated in this Standard.

This Standard comprises three parts, which provide a general framework for electronic purse interoperability:

- Functional Description
- Security Architecture
- Transaction Description

2. REFERENCES

2.1 REFERENCE DOCUMENTS

[ECBS TR103] Banking Sector Requirements for an Electronic Purse, 1996.

[ECBS TR104] The Interoperability of Electronic Purse Systems, 1997.

[EBS 105-1] PIN-based POS Systems Part 1: Minimum Criteria for Certification Procedures, 1998.

[EBS 105-2] POS Systems with On-line PIN Verification Part 2: Minimum Security and Evaluation Criteria, 1998

[EBS 105-3] POS Systems with Off-line PIN Verification Part 3: Minimum Security and Evaluation Criteria, 1998

[ECBS TR402] Certification Authorities (1997)

[EMV'96] Europay International S.A., Master-Card International Incorporated, VISA International Service Association: IC Card Specification for Payment Systems, version 3.1.1, May 1998.
"Copyright (c) 1998 Europay International S.A., MasterCard International Incorporated and Visa International Service Association. All right reserved. Please see restrictions contained therein."

[TCD 110-1] European Electronic Purse: Part 1: Functional Description, December 1998

[TCD 110-2] European Electronic Purse: Part 2: Security Architecture, December 1998

[TCD 110-3] European Electronic Purse: Part 3: Transaction Description and Message Flow, December 1998

[TCD 110-4] European Electronic Purse: Part 4: Detailed Functional Specification, December 1998

[TCD 110-5] European Electronic Purse: Part 5: Data Dictionary, December 1998

[TCD 110-6] European Electronic Purse: Part 6: Minimum Terminal Requirements, December 1998

2.2 NORMATIVE REFERENCES

[ISO 639] Codes for the representation of names and languages, 1988.

[ISO 3166] Codes for the representation of names of countries, 1993.

[ISO 4217] Codes for the representation of currencies and funds, 5th edition, December 1995.

[ISO/IEC 7812-1] Identification cards - Numbering systems and registration procedures for issuer identifiers, 1987

[ISO/IEC 7816-x] Identification cards - Integrated circuit(s) cards with contacts:

- ISO/IEC 7816-3: Electronic signals and transmission protocols, 1997
- ISO/IEC 7816-4: Inter-industry commands for interchange, 1995
- ISO/IEC 7816-5: Numbering system and registration procedure for application identifiers, 1994
- ISO/IEC 7816-6: Inter-industry data elements, 1996

[ISO 8859] Information processing - 8-bit single-byte coded graphic character sets, 1987.

[ISO 9564-1] Banking - Personal identification number management and security - Part 1: PIN protection principles and techniques, 1991

[ISO/IEC 9797] Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm, November 1993.

[prEN 1546-x] Identification card systems - Inter-sector electronic purse

- prEN 1546-1: Definitions, concepts and structures, March 1995
- prEN 1546-2: Security architecture, January 1996
- prEN 1546-3: Data elements and interchanges, December 1996

3. TERMINOLOGY

3.1 DEFINITIONS

Acceptor A merchant operating one or more Purchase Devices and providing goods and services in return for purse payments.

Acquiring Bank (Acquirer) The bank, which holds the Acceptor's account and co-operates with the Acquiring Technical Operator to settle the collected amounts.

Acquiring Technical Operator An organisation, which collects and possibly aggregates transactions from several Purchase Devices for delivery to one or more Purse Providers [prEN 1546-1].

Aggregation The process whereby the values of the individual transactions, in a given collection or group of collections, are accumulated and transmitted in a set of total amounts. No details of the individual transactions that make up the total are provided.

Auditability The ability to trace an EEP transaction from the point of origin to the Purse Provider or the Purse Provider's agent.

Balance Inquiry The user transaction that provides the user with the EEP balance (single currency EEP) or one or more specific currency Slot balances (multiple currency EEP) and related data.

Card Issuer The organisation which, from a business point of view, is the owner of the ICC (and responsible for handing over the ICC to the cardholder) in which an EEP is installed.

Card Session A link between the card and the terminal starting with the Answer to Reset and ending with a subsequent reset or a deactivation of the contacts.

Certification Authority An entity entrusted by one or more entities to create and assign certificates and to manage the revocation of certificates [ECBS TR 402].

Collection The process of transferring transaction data (Purchase Trace(s) and Purchase Cancellation Trace(s)) from the Purchase Device to the Acquiring Technical Operator by way of the Acceptor.

Completion Code A part of the response from any component on a given command. It indicates whether the command was successful or not. In the latter case the completion code indicates the reason why it was not successful [prEN 1546-2].

Currency Exchange Transaction An EEP transaction on-line to the Purse Provider during which, all applicable data elements of one Slot are converted from one currency into another (either in the same Slot or in another (active or inactive) Slot).

Current DF The latest DF selected in the card. The MF is considered to be a DF for this purpose.

Current EF The latest EF selected in the card if no DF has been selected since.

Data Origin Authentication The corroboration that the source of data received is as claimed.

Dual Authentication The process whereby, during an incremental Purchase Transaction, the EEP is authenticated by the Purchase Device for each step but the Purchase Device is only authenticated by the EEP for the first step.

EEP European Electronic Purse. An ICC application as described in this Standard.

EEP Message A string of bytes transmitted by the terminal to the card or vice-versa, excluding transmission control characters.

EEP ID The unique identification of an EEP. It consists of the Purse Provider ID and the Purse ID.

EEP Scheme A Purse Scheme that conforms to this Standard. (See Purse Scheme).

Electronic Value (EV) Electronic Value is the counterpart of a bank deposit. It is value stored and exchanged in an Electronic Purse Scheme and has no legal tender status [ECBS-TR103]. Both Electronic Value and bank deposit are in the same currency. The currency denomination of Electronic Value shall not be changed during its lifetime.

Elementary File (EF) A set of data records which share the same file identifier. It cannot be the parent of another file.

Entity Authentication The corroboration that an entity is who it claims to be.

Funding Bank The bank, which ultimately provides the funds relating to a Load Transaction to the Purse Provider and which has an account relationship with the person, who may or may not be the Purse Holder, who is funding the Load.

Funds Card The card issued to a cardholder by the Funding Bank. The card identifies the account from which the funds, used for loading the EEP application, will be debited. The card may either be a separate card from the EEP card or the reference to the funding account may reside in the EEP card.

Incremental Purchase Transaction The transaction performed using a Purchase Device whereby value is transferred from an EEP to the Purchase Device in a series of steps, in exchange for goods and services..

Interoperability The ability to obtain EEP services across different Purse Providers, Acquiring Technical Operators and Loading Operators in a common way based on technical compatibility.

Linked Load A load against the EEP’s associated account.

Linked Purse An EEP application with a reference to a funding account. This reference shall reside either in the EEP application or on the Purse Provider host.

Load Device A physical device, on-line to and operated by the Loading Operator, which is used to load Electronic Value or to do currency exchange, supplied on-line from the relevant Purse Provider, into an EEP.

Load Device ID The unique identification of a Load Device. It consists of the Loading Operator ID and the Load Device number.

Loading Operator An organisation, which operates Load Devices. It collects, processes and forwards all applicable transaction details to the Purse Providers.

Load Transaction The transaction performed using a Load Device whereby Electronic Value is transferred to an EEP.

Log Inquiry The user transaction that provides the user with the information contained in its EEP transaction log(s).

LSAM (Load SAM) A SAM installed at the Loading Operator's Side, providing the necessary security for the communication between the Loading Operator and the Purse Provider.

Master file The mandatory unique dedicated file representing the root of the file structure in the card.

Mutual Authentication The process, whereby, during a transaction (and for every step in an incremental Purchase Transaction) the EEP is authenticated by the terminal and the terminal is authenticated by the EEP.

Off-line PIN Verification The process whereby the ICC checks the transaction PIN.

Off-line transaction A transaction that does not require real-time connection to a PPSAM.

On-line PIN Verification The process whereby the PIN is sent to the Purse Provider and is checked there.

On-line transaction A transaction that requires a real-time connection to a PPSAM.

Parameter Update The transaction conducted under Purse Provider control whereby an EEP parameter is updated.

PPSAM (Purse Provider SAM) The SAM of the Purse Provider providing the necessary functionality for the secure transactions of the EEP Scheme as seen from the Purse Provider's viewpoint (e.g. secure activation, load and auditing functions) [prEN 1546].

Private Key That key of an entity's asymmetric key pair that shall only be known to and used by that entity. In the case of a digital signature scheme, the Private Key is needed to generate signatures.

PSAM
(Purchase SAM)
A SAM installed in connection with a Purchase Device providing the necessary security for purchase-related transactions and the collection process [prEN 1546].

PSAM Creator
The entity that creates the PSAMs to be used by the Acquirer

PSAM ID
The unique identification of a PSAM. It consists of the PSAM Creator ID and the PSAM number.

Public Key
That key of an entity's asymmetric key pair that may be made public. In the case of a digital signature scheme, the Public Key is needed to verify signatures.

Purchase Cancellation Trace
A set of data elements specifying all relevant details of a Purchase Cancellation Transaction kept in the Purchase Device.

Purchase Cancellation Transaction
A transaction performed at a Purchase Device in order to cancel the last Purchase Transaction in the EEP [prEN 1546-1].

Purchase Device
A physical device, operated by the Acceptor, used to accept payment from an EEP in a Purchase Transaction.

Purchase Reversal
A part of a Purchase Transaction that recovers the previous status of the EEP if a problem prevented the Purchase Transaction from being finished successfully.

Purchase Trace
A set of data elements specifying all relevant details of a Purchase Transaction kept in the Purchase Device.

Purchase Transaction
The transaction performed using a Purchase Device whereby value is transferred from an EEP to the Purchase Device in exchange for goods or services [prEN 1546-1].

Purse Holder
A person in possession of an (ICC with an) EEP [prEN 1546-1].

Purse Provider
The organisation which is responsible for installing the EEP application in the ICC and guaranteeing the Electronic Value in the EEP [prEN 1546-1].

Purse Scheme
A set of rules and regulations for issuance, acceptance and use of Electronic Purse cards established and enforced by an organisation(s).

Purse Scheme Administrator
The entity responsible for the Purse Scheme rules, security and overall scheme management.

Reading Device
A physical device allowing at least the balance of an EEP to be read and displayed. May be owned and operated by the card holder personally. May also be integrated into Purchase and Load Devices.

Record
A string of bytes which is retrieved as a whole from the card and referenced by a record number.

Record number A sequential number assigned to each record, which uniquely identifies the record within its EF.

Refund Transaction A transaction whereby Electronic Value is transferred from the Purchase Device to an EEP.

Reimbursement Transaction A transaction whereby the balance of an EEP Slot is debited and the corresponding value is returned in one way or another to the Purse Holder (e.g. via his bank account).

Script A command or a string of commands transmitted by the Purse Provider to the Load Device for the purpose of being sent serially to the EEP application as commands. A script may be part of the response message from the Purse Provider to the Load Device in on-line transactions (Load and/or Currency Exchange).

Secret Key A key used with symmetric cryptographic techniques. The key is kept secret at both the originator and recipient locations. Possession of the secret key permits secure communications between the originator and recipient.

Settlement A process performed by the Purse Provider. Based on data from Purchase and Load transactions, payment is effected from the Purse Provider to the Acquiring Bank and, when loaded against other means of payment, from the Loading Operator to the Purse Provider.

Slot A set of data elements (balance, currency code, currency exponent and maximum balance) in the EEP application. In an active Slot, these data elements are associated with a specific currency.

Total Transaction EV Electronic Value (amount and currency) corresponding to the Transaction. In case of an incremental Purchase Transaction, it is the total amount of Electronic Value corresponding to all the conducted steps of the complete transaction.

Transaction Details A set of data elements specifying all relevant details of an EEP transaction.

Truncation The process whereby Transaction Details are held and stored, at some point in the process chain and are not passed on to the Purse Provider or its agent. At the request of the Purse Provider, the Transaction Details shall be made available.

Unlinked Purse An EEP application without a reference to a funding account.

3.2 ABBREVIATIONS

ACK	Acknowledge Procedure Byte
ADF	Application Definition File
ADL	Application Data Locator
AID	Application Identifier
APDU	Application Protocol Data Unit
ATM	Automated Teller Machine
ATR	Answer-to-Reset
b1, b2, ...b8	Bits 1 (least significant) to 8 (most significant), respectively
CBC	Cipher Block Chaining
CEN	European Committee for Standardisation
CVM	Cardholder Verification Method
DDF	Directory Definition File
DF	Dedicated File
DES	Data Encryption Standard
EEP	European Electronic Purse
EF	Elementary File
EMV	Europay-MasterCard-Visa
EV	Electronic Value
FCI	File Control Information
FI	File Identifier
ICC	Integrated Circuit Card
IFD	Interface Device
IIN	Industry Identifier Number
ISO	International Organisation for Standardisation
LDA	Load Device Application (Load Device)
LRC	Longitudinal Redundancy Check
l.s.	Least Significant
LSAM	Load SAM
LSB	Least Significant Byte
MAC	Message Authentication Code
MF	Master File

m.s.	Most Significant
MSB	Most Significant Byte
PAN	Primary Account Number
PDA	Purchase Device Application (Purchase Device)
PIN	Personal Identification Number
PIX	Propietary application identifier extension
PK_{XXX}	Public Key of the component
POS	Point of Service
PPSAM	Purse Provider SAM
PSAM	Purchase SAM
PSE	Payment System Environment
PVS	PIN Verification Status
RFU	Reserved for Future Use
RID	Registered Application Identifier
RSA	Rivest, Shamir and Adleman (cryptographic algorithm)
SAM	Secure Application Module
S1	Signature 1
S2	Signature 2
S2-R	Reversal signature S2
S3	Signature 3
S3’	MAC S3’
S5	Signature 5
S6	Signature 6
SFI	Short File Identifier
Sig 2	Cryptogram of LSAM in case of Load against other means of payment
SST	Slot Status
S_{XXX}	Private Key of the component
TLV	Tag, Length, Value
TPDU	Transmission Protocol Data Unit
Var	Variable
Vcc	Supply Voltage

PART 1: FUNCTIONAL DESCRIPTION

1. FOUNDATIONS

1.1 TRANSACTIONS SPECIFIED BY THIS STANDARD

The EEP transactions specified by this Standard are Purchase (including Purchase Reversal), Purchase Cancellation, Incremental Purchase, Currency Exchange, Load, Balance Inquiry and Log Inquiry.

The Purchase (not including Purchase Reversal), Incremental Purchase, Balance and Log Inquiry are mandatory for the EEP. The transactions supported by a particular EEP application are indicated in a data element (Application Profile).

The Load Transaction is mandatory for the Loading Operator and the Purchase Transaction for the Acquiring Technical Operator.

The Currency Exchange Transaction is highly recommended for the EEP and Load Devices for interoperability reasons. For instance interoperability may not be guaranteed if

- the EEP has only one slot and does not support Currency Exchange,
- Load Devices only offer load of domestic currency and Euro and
- the Currency Exchange Transaction is not available at all Load Devices.

1.2 EEP OPERATING PRINCIPLES

1.2.1 OVERVIEW

The EEP application may contain Electronic Value in one or several currencies. The Electronic Value in the EEP is assigned to a number of slots, each with its own currency and balance.

The Purchase Transaction causes the balance of an EEP Slot to be decreased. If during the Purchase Transaction an incidence happens and it is not possible to finish the transaction, the Purchase Device may reverse (always in the same Card Session) the last incremental (or the only) step of the current Purchase Transaction, returning the slot to its previous status.

The Purchase Cancellation Transaction causes the balance in an EEP Slot to be increased by the amount of the last (or the only) step Purchase Transaction.

The Load Transaction is used to increase the balance in a Slot of the EEP. Two types of Load are supported:

- Linked Load: Load against the EEP’s associated account (Linked Purses)
- Load against other means of payment (Linked and Unlinked Purses)

The type of Load supported is an option for both the Load Device and Purse Provider.

In the case of Load against other means of payment, a cardholder initiating a Load Transaction at a Load Device may use cash or a funding application, which may be contained in the same card as the EEP or in a separate card.

The Currency Exchange Transaction updates the information either in a single Slot, or in two Slots if the target currency was already present in the EEP or not all of the source currency is to be exchanged.

This Standard also supports the Incremental Purchase Transaction e.g. for payphones. Purchase Devices, according to the nature of the services or goods provided, support either single step Purchase or Incremental Purchase Transactions.

Purchase and Purchase Cancellation Transactions are always performed off-line from the Purse Provider. Load and Currency Exchange Transactions are always on-line to the Purse Provider, with real-time access to a PPSAM. Balance Inquiry and Log Inquiry transactions are always performed off-line and need no access to a SAM.

1.2.2 GENERAL REQUIREMENTS

The Purchase, Purchase Reversal and Purchase Cancellation are always performed in the currency determined by the Purchase Device and supported by the EEP application. The cardholder may load any currency as long as it is supported by both the Loading Operator and the Purse Provider.

Purchase and Load Devices should be able to display the EEP balance before and/or after any EEP transaction. Spontaneous display of the balance at Purchase Devices may be prohibited by means of a data element included in the EEP application.

This Standard does not mandate printed receipts for the EEP transactions but note that these may be required by local law.

Any transfer of Electronic Value from the EEP shall be approved by the Purse Holder e.g. by pushing a button or inserting the EEP card. This requirement may not apply to each step of an Incremental Purchase Transaction.

In case a transaction is denied, the Purse Holder will be informed accordingly.

1.2.3 PURSE TYPES

This European Electronic Purse Standard supports two types of EEP applications:

- Unlinked
- Linked to an account

Both types of purse may coexist with other applications on the ICC e.g. Equivalent track data application or EMV debit/credit application.

An unlinked EEP is only able to support Load against other means of payment. A linked EEP may support both Load against the EEP’s associated account and Load against other means of payment.

In a Linked Purse a list with the possible Cardholder Verification Methods (CVM) is mandatory. Load Devices shall have a secure PIN pad according to [EBS105]. Two basic methods of PIN verification are supported:

- Off-line PIN verification, performed by the ICC itself where the PIN is transmitted to the ICC in plaintext or enciphered. [EMV’96]
- On-line PIN verification, performed by transmitting the encrypted PIN to the Funding Bank for verification.

1.2.4 MULTIPLE LANGUAGE SUPPORT

Language selection shall conform to [EMV'96]. The EEP may contain a data element indicating the preferred language(s) of the Purse Holder. Purchase and Load Devices may interpret this.

1.2.5 MULTI-CURRENCY HANDLING: SLOT CONCEPT

This Standard expands the CEN prEN 1546 standard by introducing a multi-currency concept, allowing an EEP application to support multiple Slots, each in a specific currency. Only one single Slot shall exist per currency.

The status of a Slot may either be:

- Active: i.e. with the currency code, exponent, maximum balance and balance data element encoded, or
- Inactive: i.e. not assigned to any specific currency.

The Purse Provider determines the maximum number of Slots supported in an EEP (minimum one). During the EEP application personalisation process, the Purse Provider may activate a Slot. After the EEP personalisation, the status of a Slot shall be changed from inactive to active only by means of a Load or a Currency Exchange Transaction.

The currency of an active Slot may be modified only if the Purse Provider supports the Currency Exchange Transaction. During the Currency Exchange Transaction, some or all of the data related to the Slot that is being converted is updated. The following sections describe the use of the currency Slots in the supported transactions.

1.2.5.1 LOAD TRANSACTION

During the Load Transaction, the Load Device shall display the currencies supported by the Loading Operator. The Purse Holder shall be able to select the currency among the ones displayed and specify the amount to be loaded.

If an active Slot with the requested currency is available, its balance is increased. If not, an inactive Slot is used and becomes activated. The EEP application shall check the maximum balance during a Load Transaction to ensure that the balance together with the amount to be loaded does not exceed the maximum balance.

If no Slots are available, the Load Device shall inform the Purse Holder and may propose that he should perform a Currency Exchange Transaction.

1.2.5.2 CURRENCY EXCHANGE TRANSACTION

During the Currency Exchange process, the Load Device should display the currencies and the respective balances of all the active Slots in the EEP and allow the Purse Holder to select the source and the target currency among the ones supported by the Loading Operator.

The Currency Exchange Transaction may be performed in one of two ways:

1. Currency Exchange into the same Slot (exchange of entire balance)
2. Currency Exchange by transfer of the electronic value from one Slot (source Slot) into another Slot (target Slot) (exchange of partial or entire balance).

Partial Currency Exchange is not possible in single slot purses.

The Currency Code and Currency Exponent associated with an active Slot shall be modified only by the use of the Currency Exchange Transaction.

The maximum balance of the target Slot need not be checked by the EEP application during a Currency Exchange Transaction.

When the cardholder wants to exchange the currency contained in a given (source) Slot into a currency existing in another (target) Slot, the entire or partial balance is transferred and the target Slot's balance will be increased. The status of the source Slot should become inactive if the entire balance was transferred, otherwise only the balance shall be decreased. The cardholder shall be informed in detail of the target and source Slot balances.

1.2.5.3 PURCHASE TRANSACTION

During the Purchase Transaction, the Purchase Device determines the currency in which the transaction shall be performed. If the currency is not contained in any Slot of the EEP application, the transaction cannot be carried out.

1.2.5.4 PURCHASE CANCELLATION TRANSACTION

The currency of the Purchase Cancellation Transaction shall be the same as the currency of the immediately previous Purchase Transaction.

1.3 EEP SCHEME STRUCTURE

1.3.1 PARTICIPANTS INVOLVED

This section is based on ECBS TR 103 "Banking Sector Requirements for an Electronic Purse".

The main entities in an EEP Scheme, and their assumed roles for the purpose of this Standard are described in the following.

It is understood that any participant in the EEP Scheme may delegate his role(s) to agents. Several roles may be grouped and assigned wholly or in part to a single entity (e.g. the Purse Provider and Card Issuer roles may be combined within the same institution).

ENTITY	**ROLE**
Acceptor	• Operates one or more Purchase Devices in order to perform Purchase Transactions. • Conforms to the Purse Scheme rules, especially those relating to security.
Acquiring Bank	• Credits the Acceptor for the Purchase Transactions (pays the Acceptor). • Receives from the Acquiring Technical Operator the information relating to the Electronic Value collected from each Acceptor. • Presents the claims to the Purse Provider for settlement. • Guarantees that the Acceptor will be paid for the Electronic Value collected. • Ensures that the Acquiring Technical Operator abides by scheme

rules.

Acquiring Technical Operator

- Collects the Purchase and Purchase Cancellation Traces stored in the Purchase Devices in a secure manner.
- Delivers the Purchase and Purchase Cancellation Traces to the Purse Providers, in accordance with the existing operational agreements.
- Informs the Acquiring Bank of the amounts collected from the Acceptors.
- Must be certified by the respective Purse Scheme Administrator on the basis of a common set of minimal security criteria via an agreed procedure.
- Is responsible for Purchase Device and PSAM security. The entity that creates the PSAM is referred to as the PSAM Creator.

Card Issuer

- Is the organisation, which, from a business point of view, is the owner of the ICC in which the Purse Provider installs the EEP application. This implies a contractual arrangement between Card Issuer and Purse Provider.
- Maintains a relationship with the cardholder.

Funding Bank

- Credits the Purse Provider (directly or via the Loading Operator), from the funding account, with the amount to be loaded in the EEP.

Loading Operator

A bank or bank agent which :

- Operates Load Devices for accepting the cardholder’s request for loading Electronic Value.
- Asks the Purse Provider to supply the Electronic Value to be loaded into the purse. In case of a load against other means of payment it provides the funds guarantee to the Purse Provider.
- Informs the Purse Holder of the outcome of the Load Transaction and/or the Currency Exchange Transaction.
- Is obliged by the Purse Scheme Administrator’s business regulations to use only certified Load Devices to ensure the correct and secure execution of the transactions.
- Is responsible for PIN pad and LSAM security.

Purse Holder

- Is any person in possession of a card with an EEP.

Purse Provider

- Guarantees the Electronic Value, and the acceptability of the Electronic Value, stored in the EEP application. Therefore, the Purse Provider shall keep the float account(s) for all the Slots in his cards.
- Loads Electronic Value into the EEP and therefore controls the

creation of Electronic Value.

- Provides other management functions such as deactivation of the EEP application.
- Is entitled to receive funds in exchange for a Load Transaction.
- Is responsible for the personalisation and initialisation of the EEP application.
- Guarantees that the Electronic Value collected by the Acquiring Technical Operator is redeemable.

Purse Scheme Administrator

- Is the overall entity responsible for key management rules, certificate generation and distribution.
- Defines operational rules.
- (Optionally) is in charge of fraud management, rules for the certification process and application of regulatory issues.

1.3.2 FLOW DIAGRAMS

The following diagrams illustrate the roles of the main participants in the EEP Scheme, and the relations between them, using the Load, Currency Exchange and Purchase Transactions:

Figure 1: LOAD TRANSACTION against the EEP's associated account.

Figure 2: LOAD TRANSACTION against other means of payment.

Figure 3: CURRENCY EXCHANGE TRANSACTION

Figure 4: PURCHASE TRANSACTION AND SETTLEMENT

1.3.2.1 LOAD TRANSACTION AGAINST THE EEP'S ASSOCIATED ACCOUNT

This load procedure described in figure 1 is valid for a Linked Purse application. In this case, the Purse Provider will ascertain the recovery of the funds.

FLOW DIAGRAM

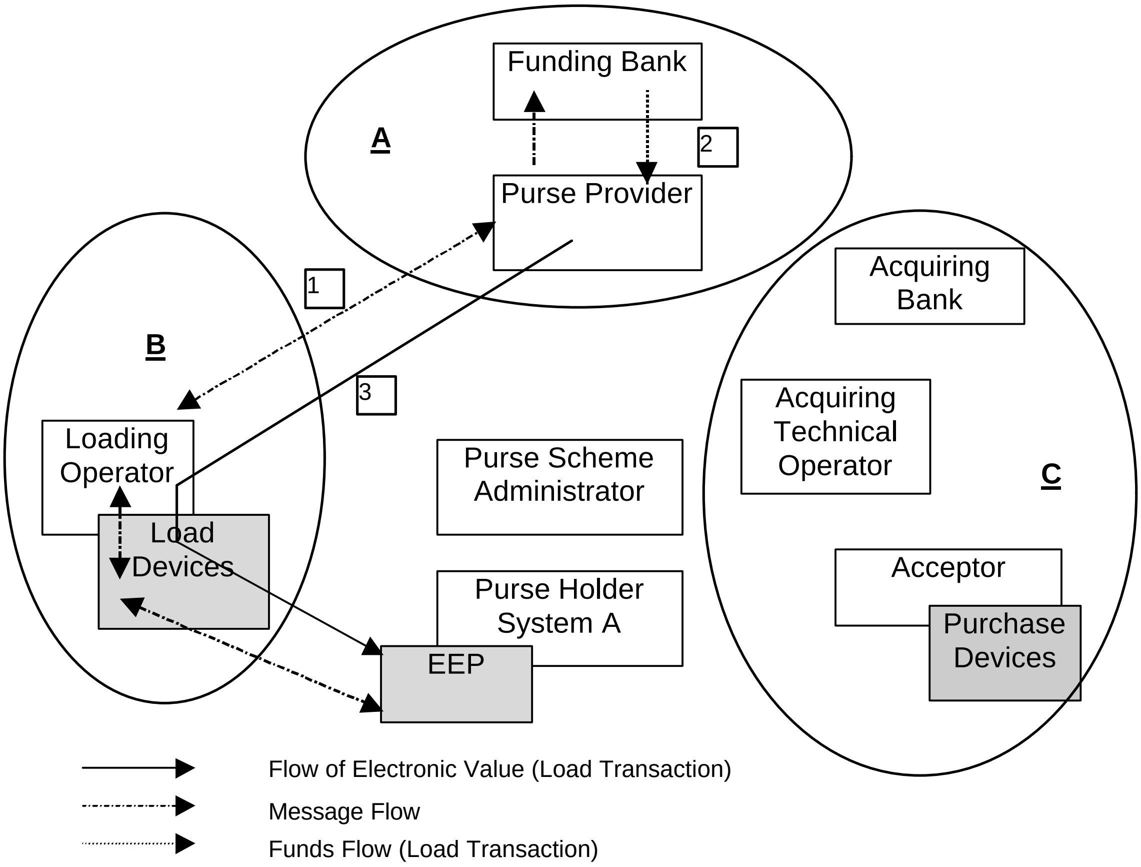


FIGURE 1: LOAD TRANSACTION AGAINST THE EEP'S ASSOCIATED ACCOUNT

GENERAL DESCRIPTION

1. During the Load Transaction, the Load Device sends a request-for-load message to the Purse Provider, possibly via the Loading Operator.
2. The Purse Provider sends an authorisation request message to the Funding Bank (cardholder account) with the amount of Electronic Value to be loaded. The Funding Bank sends an authorisation response to the Purse Provider. The Funding Bank debits the Purse Holder account and credits the Purse Provider. The Purse Provider credits the float account.
3. The Purse Provider provides the Electronic Value for the EEP application, possibly via the Loading Operator, to the Load Device, and assumes the Load is successful unless otherwise informed.

1.3.2.2 *LOAD TRANSACTION AGAINST OTHER MEANS OF PAYMENT*

The load procedure described in figure 2 is not only valid for an Unlinked Purse application but also applies where a Linked Purse is loaded with cash or with a Debit/Credit application in the same, or in another card.

FLOW DIAGRAM

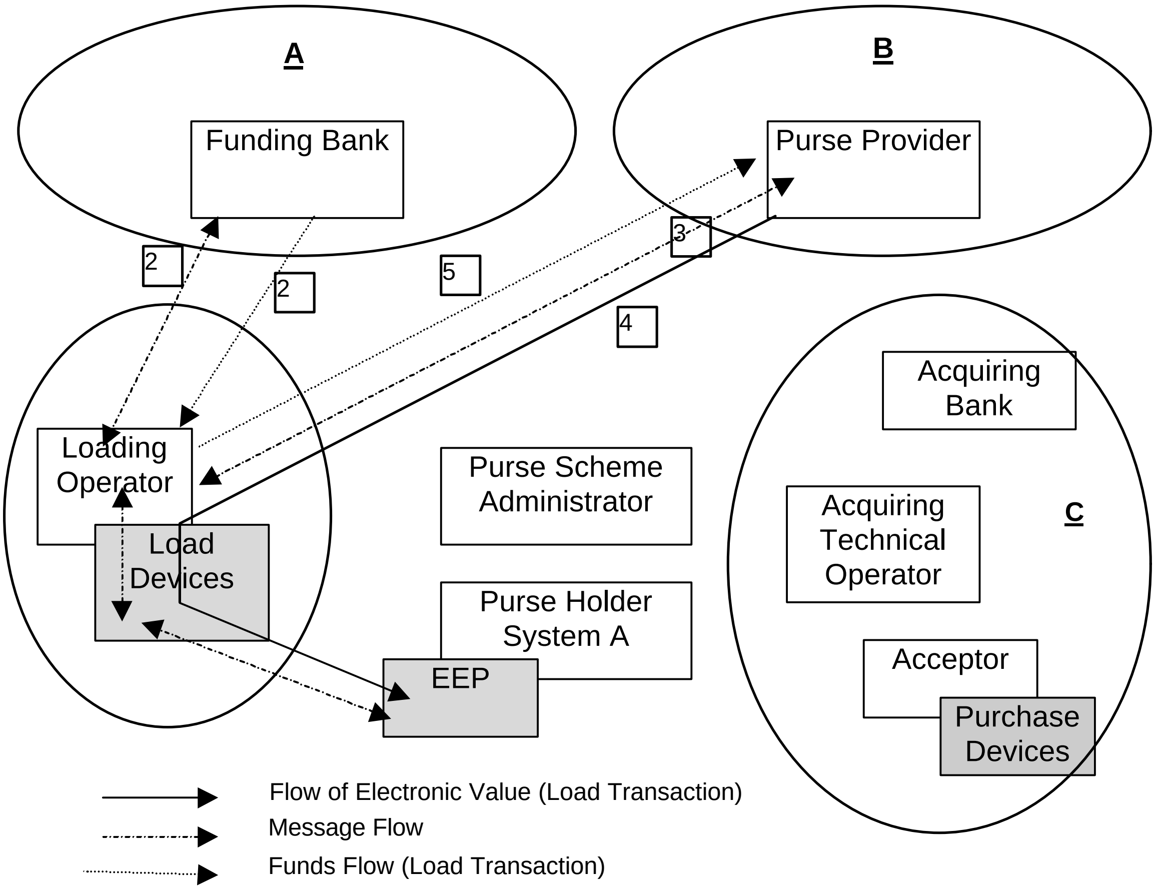


FIGURE 2: LOAD TRANSACTION AGAINST OTHER MEANS OF PAYMENT

GENERAL DESCRIPTION

1. The Load Device first determines how the funds are to be provided (e.g. Funding Bank or issuer authorisation system).
2. During the Load Transaction, the Load Device sends an authorisation request message, via the Loading Operator, stating the amount to be loaded to the Funding Bank (cardholder bank account), or to the issuer authorisation system responsible for the Debit/Credit application involved. The Funding Bank credits the Loading Operator and debits the funding account.
3. The Loading Operator informs the Purse Provider of the amount to be loaded and provides the guarantee to the Purse Provider that the funds will be provided.
4. The Purse Provider provides the Electronic Value for the EEP application to the Loading Operator and the Load Device. It shall be ensured that only the Loading Operator who initiated the Load is able to credit the EEP.
5. The Loading Operator credits the Purse Provider with the countervalue of the Electronic

Value and the Purse Provider then credits the float account.

Note: For some funding methods (e.g. cash) step 2 is not applicable.

1.3.2.3 CURRENCY EXCHANGE TRANSACTION

The general flow for the Currency Exchange Transaction is defined in figure 3.

FLOW DIAGRAM

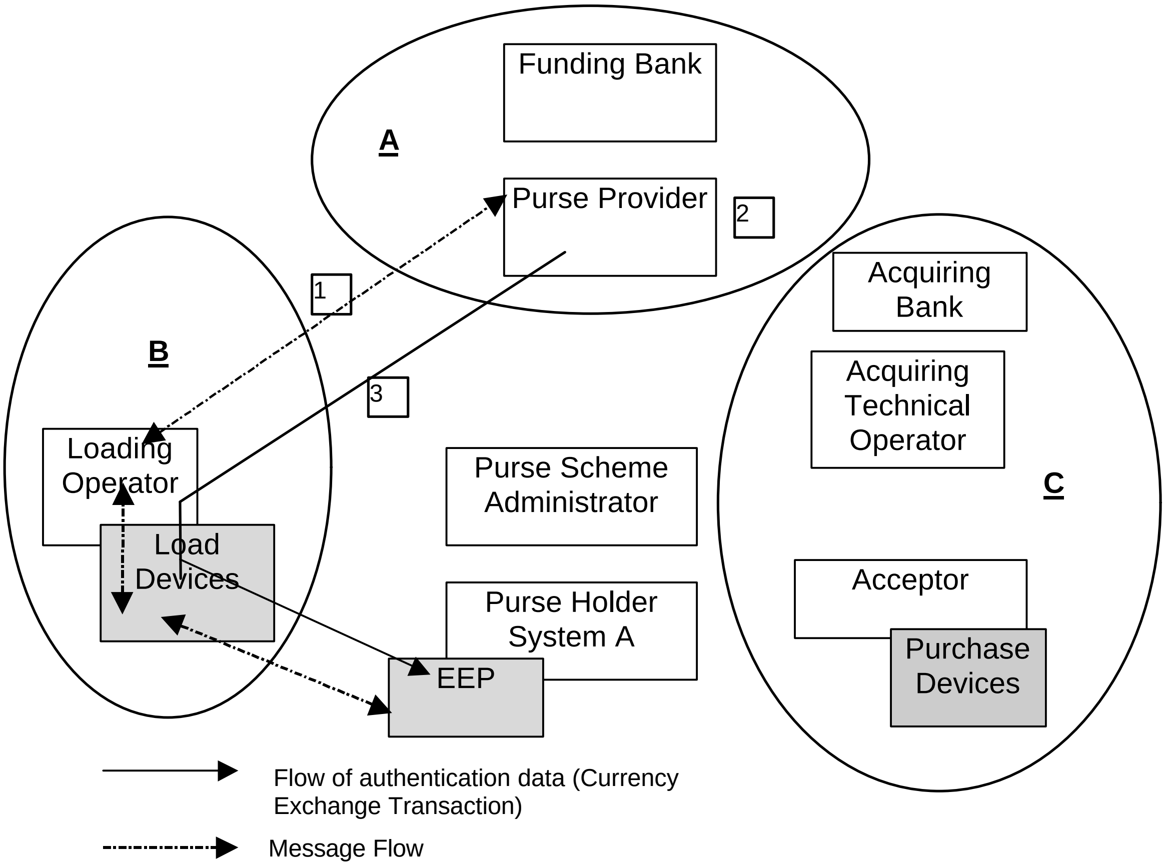


FIGURE 3: CURRENCY EXCHANGE TRANSACTION

GENERAL DESCRIPTION

1. The Load Device sends a Currency-Exchange-request message to the Purse Provider, possibly via the Loading Operator.
2. The Purse Provider converts the required amount of the currency, and creates other Slot data (currency code, balance, maximum balance, etc.) if the target Slot does not exist.
3. The Purse Provider provides the authentication data, corresponding to the target currency or the incremental amount of target currency, for the EEP application, possibly via the Loading Operator, to the Load Device.

1.3.2.4 *Purchase Transaction and Settlement*

The general flow for the Purchase Transaction is defined in figure 4.

FLOW DIAGRAM

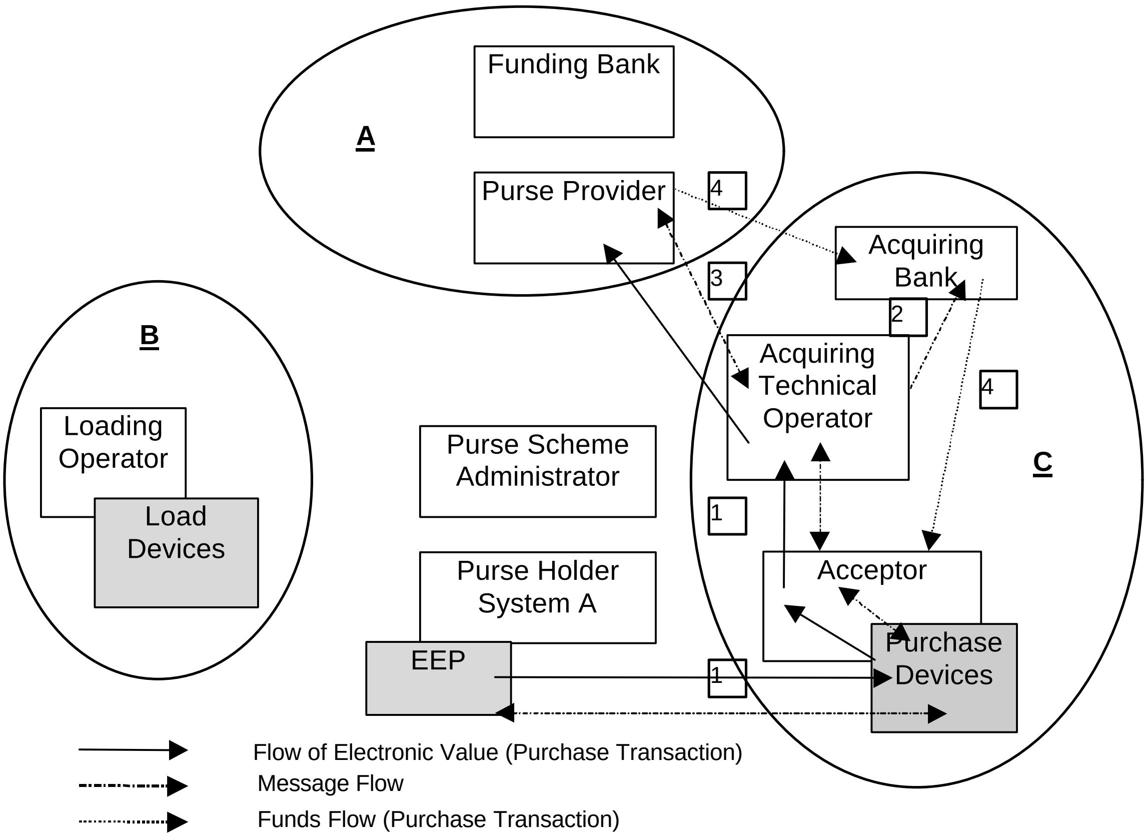


FIGURE 4: PURCHASE TRANSACTION AND SETTLEMENT

GENERAL DESCRIPTION

1. During the Purchase Transaction the Electronic Value is transferred from the EEP to the Purchase Device and is stored in a Purchase Trace. At intervals, the Acceptor collects the data stored in the Purchase Device in a secure manner and transmits it to the Acquiring Technical Operator.
2. The Acquiring Technical Operator informs the Acquiring Bank of the total amount of Electronic Value collected from the Acceptor.
3. The Acquiring Technical Operator informs the Purse Provider of the Purchase Traces collected from the Acceptor, as agreed between Acquiring Technical Operator and Purse Provider. The Electronic Value is transferred from the Acquiring Technical Operator to the Purse Provider.
4. The Acquiring Bank credits the Acceptor for the Purchase Transactions and presents the claims for settlement to the Purse Provider. The Purse Provider debits the float account.

2. SECURITY ASPECTS

This section covers some general requirements related to the security aspects of the EEP system. Detailed information related to the security aspects is given in part 2.

The security architecture proposed in this Standard allows EEPs to be loaded and used for Purchase and Purchase Cancellation Transactions without the need to share secret keys between Purse Providers, Acquirers, Loading Operators or Funding Banks.

2.1 REQUIREMENTS

The main security requirement is to ensure that Electronic Value shall not be created outside the control of the Purse Provider.

The EEP Scheme shall protect against:

- Injection of Electronic Value in an EEP or Purchase Device without a corresponding payment for the same countervalue.
- Cloning of valid cards.
- Creating of counterfeit EEP cards.
- False repudiation of transactions.
- Fraudulent terminals, debiting Electronic Value from the EEP without cardholder authorisation.
- Malfunctioning EEP cards.
- Internal fraud by the participants.
- Genuine terminals debiting Electronic Value for no financial gain.

2.2 CRYPTOGRAPHIC ALGORITHMS

Both asymmetric “Public Key” cryptography and symmetric key cryptography are used for authentication of off-line transactions.

The authorisation of Electronic Value for Load and Currency Exchange Transactions falls under the responsibility of the Purse Provider and consequently, the security procedures and cryptographic algorithms are to be selected by the Purse Provider himself (e.g. triple-DES).

Additional algorithms have to be agreed on between the Loading Operator and the Purse Provider in order to support Load against other means of payment.

2.3 TRANSACTIONS AND SECURITY

The EEP shall implement security mechanisms to ensure transaction security and to protect the key values.

Table 1 identifies the technical and security requirements for each EEP transaction.

EEP TRANSACTIONS	SECURITY MODULE	ICC REQUIRED KEYS	ON-LINE OR OFF-LINE
Balance Inquiry	None	None	Off-line
Currency Exchange	PPSAM	Currency Exchange Key	On-line

Load against the EEP's associated account	PPSAM PIN pad	Load Key	On-line
Load against other means of payment	PPSAM LSAM	Load Key	On-line
Log Inquiry	None	None	Off-line
Purchase	PSAM	Purchase Keys and Session keys	Off-line
Purchase Cancellation / Purchase Reversal	PSAM	Session Keys	Off-line

TABLE 1: TECHNICAL AND SECURITY REQUIREMENTS FOR EEP TRANSACTIONS

2.4 AUTHENTICATION

The security of the EEP transactions is based on entity and data origin authentication, as defined by CEN [prEN 1546].

In interoperable Purchase and Purchase Cancellation Transactions, authentication between an EEP and a Purchase Device is based on asymmetric and symmetric cryptography and certified Public Keys. Authentication of the EEP application by the Purchase Device is mandatory for both Purchase and Purchase Cancellation Transactions.

The Purse Provider decides whether authentication of the Purchase Device is required in all steps. One of the following authentication methods applies:

- Mutual authentication: authentication of both the EEP application and the Purchase Device.
- Dual authentication: mutual authentication in the first step and EEP application authentication only in the subsequent steps.

For a single step Purchase Transaction, all Purchase Devices shall support mutual authentication. For Incremental Purchase Transactions, dual authentication is the minimum requirement.

After debiting the balance, the Purchase Device stores the Purchase Trace indicating the transaction Electronic Value (amount and currency), the originating Purse Identifier (EEP ID), the receiving PSAM Identifier (PSAM ID) and a MAC (S6) verifiable by the Purse Provider.

The Load and Currency Exchange Transactions are executed on-line with the Purse Provider. In these transactions both EEP authentication by the Purse Provider and Purse Provider authentication by the EEP are mandatory. The procedures and techniques are selected by the Purse Provider (e.g. MAC computed using a double-length DES key).

A cryptogram is generated in order to authenticate the Loading Operator and to guarantee that the Purse Provider will receive payment from the Loading Operator during a Load against other means of payment.

2.5 KEY MANAGEMENT AND ADMINISTRATION

A Certification Authority is required. This Standard mandates a minimum of three layers for Public Key certification schemes. In certain environments EEP Schemes may opt for a four-layer hierarchy and include a regional authority. The four layers are:

- for the EEP: EEP, Purse Provider, Purse Provider Regional Authority, Purse Provider Certification Authority
- for the PSAM: PSAM, PSAM Creator or Acquirer, Acquirer Regional Authority, Acquirer Certification Authority

The session key computation method for the Load and Currency Exchange Transactions is the Purse Provider's responsibility.

2.6 BLACKLIST

All Purchase Devices should have the capability to support a blacklist (ranges of EEP identifiers), which is consulted at the start of the Purchase Transaction. The integrity of the blacklist shall be guaranteed.

This blacklist is essentially required for emergency situations and is used mainly to store ranges of counterfeit EEP cards. It does not concern lost or stolen cards. If a card is identified on the blacklist at the Purchase Device, the transaction will be denied.

An EEP is identified by the Purse Number and the Purse Provider ID. A range of cards may be identified either by:

- Purse Provider ID or
- the initial and final EEP identifiers (Purse Provider ID + Purse Number).

2.7 EEP DEACTIVATION

Whenever the EEP performs an on-line transaction, i.e. a Load or Currency Exchange Transaction, the Purse Provider may opt to deactivate the EEP application in the response message.

For all financial transactions, the EEP application shall verify the Deactivation status.

For auditing purposes, however, it should always be possible to select the EEP application and read data from the public data files (e.g. stored transactions and slot data) even if the EEP application has been deactivated.

Reactivating the EEP application shall be performed only by the Purse Provider. The reactivation process is out of the scope of this Standard.

3. TRANSACTIONS

This section defines both the mandatory and the optional interoperable transactions.

3.1 PURCHASE

The Purchase Transaction consists of a payment from an EEP to a Purchase Device (attended or unattended) in exchange for goods or services. Payments shall be made in a currency supported by the Purchase Device.

There are two types of Purchase Transactions:

- Single-step, in which a single amount is paid
- Incremental, in which the total transaction amount is the accumulation of incremental payments. The incremental payment amount may be different for each step and shall not be zero. In order to authenticate the card the first step may be zero.

Purchase Devices shall support at least one type of Purchase Transaction but may support both.

The EEP and the PSAM may be either local or remote from the point of sale.

Purchase Transactions require no PIN submission by the Purse Holder.

The Purchase Device may display the balance before and/or after the Purchase Transaction, unless explicitly forbidden by a data element contained within the EEP application, enabling the Purse Holder to verify that the EEP has been debited with the correct amount.

In the case of a single-step Purchase Transaction, the Purse Holder shall confirm the amount before the transaction takes place, e.g. by pushing a button or inserting the EEP card.

During the Purchase Transaction, the EEP will generate a payment signature (MAC) based on a unique secret key. This MAC shall be stored as part of the Purchase Trace permitting the Purse Provider to verify the authenticity of the transaction.

The Transaction Details stored in the terminal shall be certified using authentication codes (e.g. calculated with triple-DES), which means that any attempt to modify the data will be detectable by the Acquiring Technical Operator.

Interoperable Purchase Transactions are carried out using both asymmetric and symmetric cryptography for authentication of dynamic transaction data.

The Purchase Reversal is part of the Purchase Transaction. If a problem arises after the EEP has been debited (and the debit has been proven), the Purchase Device may initiate a Purchase Reversal authorising the EEP to be recredited, provided the Purchase Transaction in the same Card Session is not finished. In the case of an Incremental Purchase Transaction, only the last incremental step is reversed. The Purchase Reversal is optional for both the EEP and the Purchase Device (Acquiring Technical Operator). Both the PSAM and the EEP have to support Purchase Reversal for the transaction to be performed.

3.2 PURCHASE CANCELLATION

The Purchase Cancellation Transaction cancels the last successful transaction in the EEP. The Purchase Transaction to be cancelled shall be present in the Purchase Device log and shall not have been transmitted to the Acquiring Technical Operator. The PSAM in the Purchase

Device shall be the same as the one which was used in the transaction to be cancelled.

In the case of an Incremental Purchase Transaction, only the last incremental step is cancelled.

The Purchase Cancellation Transaction is an off-line transaction. The EEP and the PSAM may be either local or remote from the point of sale.

The Purchase Cancellation Transaction is optional for both the EEP and the Purchase Devices (Acquiring Technical Operator). Both the EEP and the PSAM have to support Purchase Cancellation for the transaction to be performed.

3.3 LOAD

The Load Transaction enables:

- the Purse Holder to load Electronic Value into an EEP using a Load Device and
- the Purse Provider to perform Purse Provider proprietary functions using script or discretionary data.

This Standard covers loading the EEP application with cash or from the associated funding account of a:

- Debit/credit application in another card (Debit/Credit application on magnetic stripe or chip)
- Debit/credit application in the same card (Debit/Credit application on magnetic stripe or chip, chip information having first priority)
- Linked Purse.

The Load Transaction shall be supported in all interoperable Load Devices, whereas it is optional for the Purse Provider.

The Load Device shall support multiple currencies for loading Electronic Value onto the EEP (see 1.2.5.1).

The Load Device shall display the balance before and after the Load Transaction. The EEP application shall check the maximum balance during the Load Transaction.

The Load Device transmits a request-for-load message to the Purse Provider via the Loading Operator. The Purse Provider authenticates the EEP and acknowledges the request for load. The Purse Provider is the only entity entitled to generate the certificates necessary to perform a Load Transaction. The Loading Operator sends all the necessary information to credit the EEP via the Load Device to the EEP.

In the case of Load against other means of payment (debit/credit application), the Load Device also sends an authorisation request message, via the Loading Operator, to the Funding Bank indicating the amount that will be loaded. An LSAM is mandatory to support this transaction.

The Load Transaction is carried out by means of one message pair between the Loading Operator and the Purse Provider.

The Purse Provider, in response to the request for load, may:

- Authorise or decline the Load Transaction
- Update EEP parameters (e.g. deactivate the EEP application)

In case of unsuccessful Load the Loading Operator shall notify the Purse Provider.

The Purse Provider may add a script envelope as an extension to the response to the request for load message. The script command performs functions that are not relevant to the current transaction but are important for the continued functioning of the EEP application, e.g. update parameters. Script processing shall be implemented according to [EMV'96].

3.4 CURRENCY EXCHANGE

The Currency Exchange Transaction is performed on-line to the PPSAM of the Purse Provider. This transaction converts some or all of the balance of one or more active Slots in an EEP and optionally the currency code, currency exponent and maximum balance of the slot(s) (see 1.2.5.2). It also allows the Purse Provider to perform Purse Provider proprietary functions using script.

The Currency Exchange Transaction is optional for both Loading Operator and Purse Provider.

The Load Device shall support multiple currencies for the Currency Exchange Transaction (see 1.2.5.2). The currency conversion itself will be performed by the Purse Provider.

The Currency Exchange Transaction is a stand-alone transaction and shall not be embedded in any other transaction. Any Currency Exchange Transaction shall be approved by the Purse Holder.

The conversion is effected according to Purse Provider policy (e.g. currency exchange rate between the source currency and the target currency). The Purse Provider sets the maximum balance of the source and target Slot. The maximum balance need not be checked by the EEP application during a Currency Exchange Transaction.

In the case of Currency Exchange into another active Slot, the entire or partial balance of the source Slot will be transferred. The source Slot should be inactivated if the entire balance was transferred.

Currency Exchange Transactions require no PIN submission by the Purse Holder.

The Currency Exchange Transaction is carried out by means of one message pair between the Loading Operator and the Purse Provider.

The Purse Provider, in response to the EEP Currency Exchange message, may:

- Authorise or decline the Currency Exchange Transaction
- Update parameters (e.g deactivate the EEP application).

The Purse Provider may add a script envelope as an extension to the response to the request for currency exchange. The script command performs functions that are not relevant to the current transaction but are important for the continued functioning of the EEP application, e.g. update parameters. Script processing shall be implemented according to [EMV'96].

3.5 BALANCE INQUIRY

The Balance Inquiry provides the Purse Holder with the balance-related data (e.g. balance, currency and maximum balance) of the active Slots in an EEP.

The EEP Balance Inquiry needs no access to any SAM.

The EEP Balance Inquiry may be performed at Purchase Devices, at Load Devices and at Reading Devices.

The Balance Inquiry is optional for the Acquiring Technical Operator and for the Loading Operator.

3.6 LOG INQUIRY

At least the last transaction shall be stored in the EEP application. The Purchase, Purchase Cancellation, Load and Currency Exchange Transactions shall be considered transactions to be stored.

Storing only successful or both successful and unsuccessful transactions is a Purse Provider option.

The Log Inquiry provides the Purse Holder with the Transaction Details of the latest transaction(s). The Purse Holder is provided with information, such as the transaction type, the amount, the currency code(s) (new and old), the date/time, the final Slot balance, the PSAM identifier (or PPSAM ID), and the Acquirer identifier.

The Log Inquiry needs no access to any SAM.

The Log Inquiry may be performed at Purchase Devices, Load Devices and Reading Devices.

4. COLLECTION AND CLEARING

4.1 COLLECTION

Truncation, i.e. the aggregation of transaction amounts in totals may be applied in the Purchase Device or in the Acquiring Technical Operator Host. Where Aggregation is supported, Transaction Details do not have to be stored.

The security architecture of this standard assumes that, if Aggregation is not supported, as a minimum, the Transaction Details of all transactions, where the Acquiring Technical Operator is entitled to receive payment from the Purse Provider, shall be sent to the Purse Provider by the Acquiring Technical Operator. The Transaction Details allow for system auditing.

Scheme rules may decide on the exact level of transaction detail required.

4.2 CLEARING

The authorisation, clearing and settlement are carried out according to international regulations. The following participants are involved:

- Purse Provider (or payment scheme)
- Acquiring Technical Operator
- Loading Operator
- Funding Bank
- Acquiring Bank

Except where Aggregation is supported, the Acquiring Technical Operator shall store all data elements (especially the Purchase Trace) for a possible later proof. This data shall be archived until the particular transaction has been accepted as bona fide and/or the funds have been received from the Purse Provider.

5. CARD RELATED CONSIDERATIONS

5.1 PHYSICAL AND ELECTRICAL CHARACTERISTICS

The physical and electrical characteristics shall conform to [EMV'96].

5.2 ICC TRANSMISSION PROTOCOLS

The ICC transmission protocols shall conform to [EMV'96].

5.3 MULTI-APPLICATION CARDS

The EEP may co-exist with any other application(s) on the same ICC, e.g. an EMV debit or credit application.

6. TERMINALS

6.1 TERMINAL TYPES

In an interoperable environment EEP cards may operate in different types of terminals, which may be classified as follows:

According to the type of transaction supported:

- Load Devices
- Purchase Devices
- Reading Devices

According to the physical nature of the terminal:

- Bank terminal, such as ATMs.
- Point of Sale terminal
- Portable user device, such as balance readers.

Application-specific functions, such as guiding the Purse Holder through the use of the machines, printing a receipt and other procedures, are outside the scope of this document. Standardising the way in which information is presented to the Purse Holder (sequence, language) would enhance Purse Holder acceptance but is not covered by this Standard.

6.2 LOAD DEVICES

Load Devices are used to increment the Electronic Value held in an EEP. Every Load Device shall be capable of processing Load Transactions for at least one of the EEP types conforming to this Standard and may support Currency Exchange Transactions. They shall also support processing of any script envelopes that may be present as extensions to Load and Currency Exchange messages.

The Load Device shall have an on-line interface to the Loading Operator. In the case of Linked Load or Currency Exchange, the Purse Provider may act as the Loading Operator directly.

The Load Device shall initiate the funds transfer and securely increase the EEP balance by the amount specified by the Purse Holder and authorised by the Purse Provider. If the Load should fail, the Loading Operator notifies the Purse Provider and, if appropriate, the Funding Bank.

Before and after the Load or Currency Exchange Transaction the EEP Slot balances shall be presented to the Purse Holder. The Load Device shall guide the Purse Holder through the transaction and indicate the result of the transaction.

Load Devices shall contain a secure PIN pad to be used for the Purse Holder verification for Load against the EEP's associated account and they shall use an LSAM to provide transaction processing integrity for Load against other means of payment.

Load Devices may also support Balance Inquiry and Log Inquiry.

6.3 PURCHASE DEVICES

In return for goods and services delivered to the Purse Holder, the (attended or unattended) Purchase Device accepts payments made by an EEP and decreases the balance of the EEP application.

In addition to the mandatory Purchase Transaction (single-step and/or incremental), the Purchase Device may also support:

- Purchase Cancellation/Purchase Reversal.
- Balance Inquiry
- Log Inquiry

Interoperable Purchase Devices shall support mutual authentication for the single-step Purchase Transaction and dual authentication as a minimum for the Incremental Purchase Transaction. A PSAM is mandatory for this. It shall be able to operate with both asymmetric and symmetric cryptography for authentication of dynamic transaction data. The EEP and PSAM may be either local or remote from the point of sale. A data element provided by the EEP application defines the authentication procedure selected for a particular transaction.

Purchase Devices are not required to support any type of cardholder verification. The Purchase Device shall, however require the Purse Holder to authorise the transaction, e.g. by pushing a button or inserting the EEP card, before securely deducting Electronic Value from the EEP application and securely storing that value. In the case of an Incremental Purchase transaction only the first step need be confirmed by the Purse Holder. The Purchase Device may display the balance if permitted by the EEP application.

If aggregation is not supported in the Purchase Device, the Purchase Device shall store the Transaction Details for each transaction of any type i.e. including Purchase Cancellation and Purchase Transaction with Purchase Reversal. The Purchase Device shall support an interface to the Acquiring Technical Operator to enable the collection of Electronic Value to be sent to the Purse Provider.

Purchase Devices shall unambiguously indicate the purchase amount and currency to the Purse Holder and shall be capable of indicating the result of the transaction to both the merchant and the Purse Holder.

Purchase Devices should have the capability to support a blacklist.

6.4 READING DEVICES

Reading Devices may support Balance Inquiry and/or Log Inquiry.

Both Balance Inquiry and Log Inquiry are performed off-line and a SAM is not needed.

Reading Devices are typically portable user devices, such as balance checkers, key rings, etc. They may also be PCs and other terminals capable of reading IC cards.

ooOOoo

PART 2: SECURITY ARCHITECTURE

1. INTRODUCTION

This part of the Standard describes the security-critical aspects of the EEP transactions and components and specifies an architecture to achieve the appropriate degree of security.

1.1 PARTICIPANTS AND TRANSACTIONS

With an EEP, a Purse Holder may make Purchase Transactions (payments) at *Purchase Devices* and may cancel them (Purchase Cancellation Transaction). At *Load Devices,* a Purse Holder may load Electronic Value on the EEP (Load Transaction) and may change the currency of Electronic Value held in the EEP (Currency Exchange Transaction) through on-line transactions to the Purse Provider.

The following participants are involved in the EEP security architecture: the Purse Holder, the Purse Scheme Administrator, the Purse Provider, the Acceptor, the Acquiring Technical Operator and the Loading Operator.

1.2 SECURITY REQUIREMENTS

The security architecture is the kernel of an European Electronic Purse Scheme. In contrast to traditional card based means of payment, prepaid Electronic Purse Schemes with insufficient security offer means to create Electronic Value outside the control of the banking regulations. Such possibilities shall be reduced to a controllable minimum. Otherwise Electronic Purse Schemes cannot be safely implemented.

Furthermore the Purse Providers, who issue Electronic Value, guarantee the funds via the Acquiring Banks to the Acceptors. The best available security techniques applicable to chip cards should be used throughout. Appropriate evaluation and certification procedures shall be implemented to ensure this.

The Purse Providers authorise the loading of amounts to the EEP and hold float accounts where the countervalues of the Load Transactions are credited. These float accounts are debited when Acceptors are credited for their Purchase Traces. The Electronic Value on the EEPs is guaranteed by the Purse Provider. Therefore the Purse Provider's float account must be protected.

As a consequence a Purse Provider only agrees to the acceptance of his EEPs in an interoperable environment if he is convinced that the appropriate security is provided. The Acquiring Technical Operator then needs an instrument that is well accepted in the European payments industry, which enables him to demonstrate, in a trustworthy way, that his infrastructure fulfils these requirements.

The essential security requirements are:

- it shall be verifiable by the Purse Provider that the Purchase Traces he receives were performed with his genuine cards.
- it shall be verifiable by the Acquiring Technical Operator that the Purchase Traces are submitted by genuine Purchase Devices (PSAMs).
- it shall be verifiable that Load Devices (LSAMs, PIN pads) used to increment the balance on the Purse Provider’s EEPs are built and operated in accordance with the appropriate security requirements.
- Acquiring Technical Operators shall perform appropriate control mechanisms, including

mechanisms to ensure that the Purchase Traces sent have not been cancelled.

This document specifies the security requirements of the ICC containing an EEP application and the applicable security requirements for PIN and Purchase Devices.

Additional standards will cover the minimum security requirements for items such as PSAMs and LSAMs.

To guarantee the implementation according to these requirements, the above mentioned security relevant components have to be evaluated and certified following the framework defined by [EBS 105-1].

1.3 TRUST MODEL

The usefulness of an interoperable model is dependent on the degree in which the different entities need to trust each other. The basic EEP security architecture allows the participants to choose their own security level without affecting the risk taken by the other participants. The appropriate means to ensure this trustworthiness shall be made available.

The basic trust assumptions in the EEP architecture with respect to Purchase Transactions are the following:

P-TA1 The Purse Provider trusts his EEP ICC (physical and logical security as well as functionality).

P-TA2 The Purse Holder trusts his Purse Provider.

P-TA3 The Acquiring Technical Operator trusts his Purchase Device (security and functionality) and PSAM.

P-TA4 The Acceptor trusts his Acquiring Technical Operator.

P-TA5 The Acquiring Technical Operator trusts the Purse Provider not to repudiate a Purchase Trace obtained from an EEP validated as genuine by the Purchase Device.

P-TA6 The Acquiring Technical Operator trusts the Certification Authority to certify only Public Keys of bona fide Purse Providers.

P-TA7 The Purse Provider trusts the Acquiring Technical Operator to maintain his system (especially PSAM) and processes in accordance with the certification and evaluation, which has been previously obtained.

The basic trust assumptions in the EEP architecture with respect to Load Transactions are the following:

L-TA1 The Purse Provider trusts his EEP ICC (physical and logical security as well as functionality).

L-TA2 The Purse Holder trusts his Purse Provider.

L-TA3 The Loading Operator trusts his Load Device (security and functionality) and LSAM.

L-TA4 The Loading Operator trusts the Purse Provider not to claim a loading amount if, during a Load against other means of payment, the EEP sent a proof of no transaction, which is validated as genuine by the Loading Operator.

L-TA5 The Purse Provider trusts the Loading Operator to maintain his system (especially LSAM) and processes in accordance with the certification and evaluation, which has been previously obtained.

1.4 SECURITY MECHANISMS

The security of a Purchase Transaction is based on the establishment of a *Purchase Trace* in the Purchase Device in such a way that the EEP proves the authenticity of the Purchase Trace.

Upon presentation of the Purchase Trace, the Purse Provider will pay the Electronic Value to the Acquiring Bank, who will pass it on to the Acceptor operating the Purchase Device. This information is contained within the Purchase Trace. Hence, the failure to deliver a valid Purchase Trace to the Purse Provider can correspond to a financial loss equivalent to the Electronic Value of the Purchase Trace.

It is in the interest of the Acquiring Technical Operator to make sure that the Purchase Traces are sent to the Purse Provider without losing their integrity. The Purse Provider shall be able to detect double submission of Purchase Traces.

When an error occurs after the EEP has been debited, but the card session is still running, the transaction may be reversed, i.e. the balance of the EEP is set back to the value prior to the transaction. In case of Incremental Purchase only the last step may be reversed.

The latest Purchase Transaction conducted by an EEP may be cancelled. This corresponds to a re-crediting of a balance in the EEP. It is the responsibility of the Acquiring Technical Operator not to request payment from the Purse Provider for Purchase Transactions which have been cancelled.

Except where Aggregation is supported, the Purchase Device sends the Transaction Details for each transaction of any type to the Acquiring Technical Operator who will forward to the Purse Provider, as a minimum, the Transaction Details where the Acquiring Technical Operator is entitled to receive payment from the Purse Provider. These transactions are:

- Purchase Transactions which have not been cancelled
- Purchase Transactions with Purchase Reversal and amount different from zero
- Purchase Cancellation of Incremental Purchase Transactions together with the original Purchase Trace

Purchase Device Authentication ensures that an EEP is only debited by a Purchase Device operated by a recognised Acquiring Technical Operator. The explicit user authorisation for payment shall be implemented in the user interface (display, OK button, etc.) of the Purchase Device.

If an EEP has been debited contrary to the intention of the Purse Holder, the possible beneficiary is identified by the PSAM ID contained in the EEP log. Hence an Acceptor who systematically defrauds, for the purpose of financial gain, will quickly be detected.

The Load and Currency Exchange Transactions are performed on-line to the Purse Provider. As far as the EEP is concerned the Load Device and the Loading Operator provide a transparent link to the Purse Provider, who is responsible for the security of these transactions. In case of Load against other means of payment, i.e. not against the associated account of the

EEP, security mechanisms shall be provided to ensure:

- that the Loading Operator guarantees to pay the funds to the Purse Provider.
- that only the Loading Operator, who initiated the Load Transaction, can credit the EEP.
- that a proof of an unsuccessful Load is available to the Loading Operator.

These security mechanisms are called:

- guarantee of payment
- authenticity of the Loading Operator, and
- proof of no transaction

2. GENERAL REMARKS

In this Standard signatures support data recovery. Data elements that can be retrieved shall not be sent in cleartext. Note that all the data elements that are necessary to check MACs and that cannot be deduced via other methods, have to be sent in cleartext.

A list of the minimum required data elements protected by signatures and MACs is given in section 3. Scheme rules will determine any additional data elements to be included and possibly the sequence in which these data elements are used to compute the signatures and MACs that are required for interoperability.

3 EEP TRANSACTIONS

Four types of security related transactions are specified within this part of this Standard. They are:

1. Purchase Transaction (including incremental and reversal),
2. Purchase Cancellation Transaction,
3. Load Transaction, and
4. Currency Exchange Transaction.

The basis for the security of the EEP transactions is mandatory entity and data origin authentication. Authentication in EEP transactions is based on the Electronic Purse protocols as defined in [prEN1546]. A short description is given of the authentication methods specified by this Standard in each of the four transactions.

3.1 PURCHASE TRANSACTION

3.1.1 SCOPE

The Purchase Transaction is a transaction between an EEP and a Purchase Device, conducted off-line from the Purse Provider and the Acquiring Technical Operator.

The Purchase Reversal is part of the Purchase Transaction. If a problem arises after the EEP has been debited, the Purchase Device may initiate a Purchase Reversal authorising the EEP to be recredited in the same Card Session.

The net effect of the transaction is:

1. The debiting of an EEP Slot balance by a given amount in the currency determined by the Purchase Device.
2. The availability, after this debit, of a Purchase Trace in the Purchase Device allowing the Acceptor to be credited.
3. Possibly, the recrediting of an EEP Slot balance by the amount of the current transaction (last incremental step) and the corresponding amendment in the Purchase Trace.

The main goals of the security protocol of the Purchase Transaction are:

1. To allow the PSAM to verify the authenticity of the EEP and the Purchase Trace.
2. To allow the EEP to verify the authenticity of the PSAM.
3. To provide a mechanism to conduct a Purchase Reversal.

For the Single-Step Purchase Transaction, Mutual Authentication is mandatory. The EEP receives **S2** and returns **S3** after debiting a Slot balance by the requested amount;

For the Incremental Purchase Transaction, two options are specified:

1. Mutual Authentication: mutual authentication is applied for all steps (as described for the single-step Purchase);
2. Dual Authentication:

- for the first payment step mutual authentication is applied, whereas

- for all subsequent payment steps, only the EEP application is authenticated

3.1.2 REQUIREMENTS OF THIS STANDARD

The Purchase Transaction specifies five authentication processes:

S2: A digital signature supplied to the EEP by the PSAM, exchanging a Session Key. If correct, the EEP is authorised to perform a debit.

S3: A MAC calculated with the Session Key, provided by the EEP, guaranteeing the integrity of relevant data, including **S6**, and the authenticity of the EEP to the Purchase Device. If correct, the Purchase Device signals the Acceptor or vending machine to supply goods/services in return for the debited Electronic Value.

S6 A MAC provided by the EEP, guaranteeing the integrity of the Purchase Trace (not including **S6**). If correct the Purse Provider credits the Acquirer with the countervalue of the Purchase Transaction.

S2-R A MAC calculated with the Session Key, for a reversal transaction supplied to the EEP by the PSAM,. If correct, the EEP is authorised to reverse the transaction (last incremental step).

S5 A MAC calculated by the PSAM after the transaction has been concluded (after **S3** has been verified). It provides a proof of the total amount that has been debited and is supplied to the Acquiring Technical Operator as an appendage to the Purchase Trace.

The Purchase Trace completely specifies a Purchase Transaction. The integrity of S6 and other data elements is guaranteed by **S3**, which also authenticates the data origin of the Purchase Trace as a genuine EEP. For the Purse Provider, the integrity of the Purchase Trace is guaranteed by computing the MAC **S6**.

The Purchase Device will forward the Purchase Trace and **S6** in due course to the Acquiring Technical Operator, who, if he is entitled to receive payment, will forward both to the Purse Provider. Provided the Purchase Trace is valid, the Purse Provider shall pay the Total Transaction Electronic Value to the Acquiring Bank, who in turn shall pay the Acceptor operating the Purchase Device, indicated in the Purchase Trace.

Considerations related to S5

The requirement for generating the MAC **S5** does not apply if the PSAM does not support Purchase Reversal.

The ability of the PSAM to generate a MAC **S5** is a necessary condition for performing a Purchase Reversal, which permits the recrediting of the Electronic Value in the EEP provided the Purchase Transaction in the same Card Session is not finished.

If the Purchase Device realises that it is not possible to provide the goods requested prior to the generation of **S5**, the current Purchase Transaction may be reversed.

S5 provides a proof of the total amount that has been debited. In case an incremental Purchase is reversed, **S5** is generated over the total amount of the successful steps. The signature is generated after the transaction has been concluded. The reversal signature **S2-R** shall not be calculated if **S5** has already been calculated for this transaction.

The PSAM computes **S5** for Purchase Transactions and for Purchase Transactions that have been reversed to enable the Acquiring Technical Operator to verify that all reversed transactions have been submitted by the Purchase Device. It shall not be forwarded to the Purse Provider.

As Purchase Reversal is part of the current Purchase Transaction, the PSAM transaction counter is not incremented and remains the same. Missing transaction numbers may indicate to the Acquiring Technical Operator that Purchase Transactions (performed or reversed) have not been submitted.

3.1.3 DYNAMIC DATA FOR AUTHENTICATION

During a Purchase Transaction, at least the following data are signed:

Name	Source
Session Key	PSAM
PSAM ID	PSAM
Acquirer ID	PSAM
PSAM Transaction Number	PSAM
Transaction Indicator	Purchase Device
Total Transaction Electronic Value	Constructed
Transaction Currency	Purchase Device
EEP ID	EEP
Purse Provider ID	EEP
EEP Transaction Number	EEP

For the subsequent steps in an Incremental Purchase Transaction, **S2** does not necessarily sign all the data listed above.

The MAC **S3** is calculated over dynamic data elements, including **S6**. As a minimum, **S3** signs the following data elements:

Name	Source
EEP Slot Balance	EEP
Transaction Type	EEP
MAC **S6**	EEP
Total Transaction Electronic Value	Constructed
Last step Electronic Value	Purchase Device

The MAC **S6** is calculated over the entire Purchase Trace (without **S6**) and is intended for the Purse Provider to check the validity of the Purchase Trace. It is recommended that **S6** be calculated over the following data elements.

Name	Source
Current Date and Time	Purchase Device
Discretionary Data	EEP
EEP Authentication Method	EEP
EEP Expiry Date	EEP
EEP ID	EEP
Purse Provider ID	EEP
EEP Slot Balance	EEP
EEP Transaction Number	EEP
Last Step Electronic Value	Purchase Device
Transaction Currency	Purchase Device
PSAM ID	PSAM
Acquirer ID	PSAM
PSAM Transaction Number	PSAM
Total Transaction Electronic Value	Constructed
Transaction Type and Status	EEP

As a minimum the MAC **S2-R** signs the following data elements:

Name	Source
Last Step Electronic Value	Known
Total Transaction Electronic Value	Known
Transaction Indicator	Constructed

The minimum dynamic data protected by means of **S5** are:

Name	Source
EEP ID	EEP
Purse Provider ID	EEP
EEP Transaction Number	EEP
MAC S6	EEP
PSAM ID	PSAM
Acquirer ID	PSAM
PSAM Transaction Number	PSAM
Total Transaction Electronic Value	Constructed
Transaction Currency	Purchase Device
Transaction Indicator	Purchase Device

3.2 PURCHASE CANCELLATION TRANSACTION

3.2.1 SCOPE

The Purchase Cancellation Transaction is a transaction between an EEP and a Purchase Device conducted off-line from the Purse Provider and Acquiring Technical Operator.

The net effect of the transaction is twofold:

1. The availability of a Purchase Cancellation Trace in the Purchase Device.
2. The re-crediting of an EEP Slot Balance with the amount and in the currency of the last Purchase Transaction (step).

The main goal of the security protocol of the Purchase Cancellation Transaction is to allow the EEP to verify that the transaction is being authorised by the PSAM that is identified in the Purchase Transaction to be cancelled.

There are three authentication processes:

S1: A MAC, calculated by the same Session Key as used for the Purchase Transaction, provided by the EEP guaranteeing its authenticity to the Purchase Device by signing its ID and Transaction Number. If correct, the PSAM may authorise the Purchase Cancellation.

S2: A MAC supplied to the EEP by a PSAM, guaranteeing its authenticity to the EEP. If correct, the EEP is authorised to perform the re-credit.

S5 A MAC calculated by the PSAM after the transaction has been concluded. It provides a proof of the total amount that has been cancelled and it is supplied to the Acquiring Technical Operator as an appendage to the Purchase Trace.

For the PSAM, the Purchase Cancellation can only be conducted if S1 validates.

For the EEP, the Purchase Cancellation can only be conducted if S2 validates.

The EEP generates **S1** and sends it to the Purchase Device. If correct, the PSAM generates **S2** and sends it to the EEP. If the transaction data and **S2** are correct, the EEP re-credits its balance with the amount of the last (last step) Purchase Transaction. The signature **S2** is used to cancel exactly one Purchase Transaction in one specific EEP.

After the transaction has been concluded the PSAM stores the EEP response and generates the MAC **S5**. The ability of the PSAM to generate a MAC **S5** is a necessary condition for performing a Purchase Cancellation.

The PSAM computes **S5** for Purchase Cancellation Transactions to enable the Acquiring Technical Operator to verify that all cancelled transactions have been submitted by the Purchase Device. It provides a proof of the total amount that has been cancelled. **S5** shall not be forwarded to the Purse Provider. The Acquiring Technical Operator shall put the necessary procedures in place to guarantee that he does not request payment from the Purse Provider for Purchase Transactions (last step) which have been cancelled.

The EEP may store internally information concerning the Purchase Cancellation Transaction by logging the EEP Transaction Number of these transactions and information related to the PSAM.

4.2.2 DYNAMIC DATA FOR AUTHENTICATION

As a minimum **S1** signs the following data elements:

Name	Source
EEP ID	EEP
Purse Provider ID	EEP
EEP Transaction Number	EEP
Transaction Type	Constructed
PSAM ID of the transaction to be cancelled	EEP
Acquirer ID of the transaction to be cancelled	EEP
PSAM Transaction Number of the transaction to be cancelled	EEP
Total Transaction Amount	EEP
Transaction Currency	EEP
Transaction Amount of the Purchase Device (last step Electronic Value)	EEP

As a minimum **S2** signs the following data elements :

Name	Source
PSAM Transaction Number (new)	PSAM
Transaction Type	Constructed

As a minimum **S5** protects the following data elements:

Name	Source
EEP ID	EEP
Purse Provider ID	EEP
EEP Transaction Number	EEP
PSAM ID	PSAM
Acquirer ID	PSAM
PSAM Transaction Number	PSAM
Total Transaction Electronic Value	EEP
Transaction Currency	EEP
Transaction Indicator	Purchase Device

3.3 LOAD TRANSACTION

3.3.1 SCOPE

The Load Transaction is always a transaction between an EEP and the Purse Provider. In case of Load against other means of payment the Loading Operator and possibly the funding bank will take part in the transaction.

From the point of view of the EEP, there are two types of Load Transactions:

1. A currency is loaded in an active Slot;
2. An inactive Slot has to be activated for the currency to be loaded.

This Standard requires three authentication processes:

S1: A MAC provided by the EEP allowing the Purse Provider to verify its authenticity

S2: A MAC supplied to the EEP by the Purse Provider, authenticating transaction data from the Purse Provider. If correct, the EEP is authorised to perform a credit, or the application may be deactivated.

S3: A MAC provided by the EEP and intended for the Purse Provider, signing the state of the EEP after the operation, indicating proof of credit, or non-credit, or application deactivated.

In case of Load against other means of payment this Standard requires two additional authentication processes:

- between the LSAM and the Purse Provider

Sig2: A cryptogram provided by the LSAM allowing the Purse Provider to authenticate the transaction data. If correct, it represents the Loading Operator’s guarantee of payment.

- between the EEP and the Loading Operator

S3’: A MAC provided by the EEP and intended for the Loading Operator, authenticating the unsuccessful outcome of the transaction. If the authentication is correct, the LSAM signals the Loading Operator to refund the load amount.

The Purse Provider validates the authenticity of the EEP by verifying **S1** and in addition, **Sig2** as a guarantee of payment in case of Load against other means of payment. He decides either to reject the transaction, to authorise the EEP to credit a Slot balance, or to update the parameters of the EEP application. The last two are triggered in the EEP by its verification of **S2**. In case of Load against other means of payment and when the transaction has been authorised by the Purse Provider, **S2** is sent encrypted to the Loading Operator, to ensure that only the Loading Operator who initiated the Load is able to credit the EEP.

Then the EEP generates a proof for the Purse Provider of credit, non-credit or parameters updated in the form of **S3**.

If **S3** is available, it shall be sent to the Purse Provider in case of unsuccessful Load

Transactions. It may be transmitted in case of successful Load Transactions.

In the case of Load against other means of payment, if the transaction is unsuccessful, the EEP additionally provides a proof for the Loading Operator of non-credit in the form of **S3'**. The Purse Provider must have previously sent a check value of **S3'** to the Loading Operator. This check value is computed using a one-way function (agreed between Purse Provider and Loading Operator) on **S3'**.

The Loading Operator checks that the **S3'** provided by the EEP corresponds to the check value provided by the Purse Provider by computing the one-way function on **S3'** and verifying that the result matches the check value.

In the case of Load against other means of payment, if the transaction was successful, the Load Device does not interpret or use **S3'**. **S3'** is only used in case of unsuccessful credit.

In the dynamic data for **S1**, there may be a data element indicating the Slot status (active/inactive).

In the case of loading into an active Slot, the Slot balance and maximum balance impose an upper limit on the transaction amount.

In the case of loading into an inactive Slot, all the data elements to activate the Slot shall be provided by the Purse Provider and shall all be included in the dynamic data authenticated by **S2**.

3.3.2 DYNAMIC DATA FOR AUTHENTICATION

The recommended data elements protected by means of **S1** are:

Name	Source
Discretionary Data	EEP
EEP ID	EEP
Purse Provider ID	EEP
EEP Expiry Date	EEP
EEP Slot Balance	EEP
EEP Transaction Number	EEP
Load Device/LSAM ID [(1)]	Load Device/LSAM
Loading Operator ID [(1)]	Load Device/LSAM
Challenge [(1)]	Load Device/LSAM
PIN Verification Status	EEP
Slot Status	EEP
Transaction Electronic Value	Load Device
Transaction Currency	Load Device

[(1)] In case of Load against other means of payment the origin of these data elements is the LSAM. S1 shall include ID_{LSAM} instead of ID_{LDA}. If an LSAM is present, it may also be used in Linked Load.

The recommended data elements protected by means of **S2** are:

Name	Source
Discretionary Data	Purse Provider
EEP Deactivation Date	Purse Provider
EEP ID	EEP
Purse Provider ID	EEP
EEP Slot Maximum Balance	EEP
EEP Transaction Number	EEP
PPSAM ID and Challenge	Purse Provider
Transaction Electronic Value	Load Device
Transaction Currency	Load Device

The recommended data elements protected by means of **S3** are:

Name	Source
Discretionary Data	EEP
EEP ID	EEP
Purse Provider ID	EEP
EEP Transaction Number	EEP
PPSAM ID and Challenge	Purse Provider
Transaction Completion Code	EEP

The recommended data elements protected by means of **Sig2** are:

Name	Source
EEP ID	EEP
Purse Provider ID	EEP
EEP Transaction Number	EEP
LSAM ID and Transaction Number	LSAM
Loading Operator ID	LSAM
Transaction Electronic Value	Load Device
Transaction Currency	Load Device

S3’ is an 8-byte value authenticating the non-credit and computed by the EEP only if it has not been credited. It should be an unpredictable value, for anyone except the Purse Provider. This could be implemented by computing the MAC on the following data elements.

Name	Source
EEP ID	EEP
Purse Provider ID	EEP
EEP Transaction Number	EEP

3.3.3 KEYS AND ALGORITHMS FOR LOAD AGAINST OTHER MEANS OF PAYMENT

Load against other means of payment requires the computation of **Sig2,** a cryptogram using either symmetric or asymmetric cryptography. The algorithm used to compute this cryptogram will be agreed between the Purse Provider and the Loading Operator.

In the case of an unsuccessful Load Transaction, the EEP generates a MAC **S3'** to authenticate the outcome of the transaction. **S3'** provides a proof for the Loading Operator of non-credit. The one-way function used to compute the check value from **S3'** will be agreed between the Purse Provider and the Loading Operator.

3.3.3.1 SIG2 COMPUTATION BY MEANS OF SYMMETRIC CRYPTOGRAPHY

In this case **Sig2** has to be computed as a MAC using a symmetric key. This symmetric key may already be shared between the Loading Operator and the Purse Provider or it may be chosen randomly by the LSAM and forwarded in a secure manner to the Purse Provider (node to node encryption). The key used for the **Sig2** computation is also used for enciphering **S2**.

After verifying **Sig2** successfully, the PPSAM encrypts **S2** for an approval using the symmetric key and, if requested by the LSAM, computes a check value of **S2** (plain text) using a one-way function. This mechanism enables the Loading Operator to check whether the **S2** that he has decrypted is correct or not.

In order to make sure that the PPSAM uses algorithms supported by the LSAM, the data element defining the agreed algorithm is sent along with **Sig2**. This data element also defines which one-way function shall be used to calculate the check value in case it is required by the LSAM.

3.3.3.2 SIG2 COMPUTATION BY MEANS OF ASYMMETRIC CRYPTOGRAPHY

To allow for future developments this Standard provides for the possibility of computing **Sig2** as a signature using an asymmetric key. The data element is able to support the coding of asymmetric algorithms and associated key lengths. Scheme rules will define the necessary certificates for LSAM Public Key cryptography.

3.3.3.3 S3' COMPUTATION

To provide an off-line proof of no transaction for the Loading Operator, the EEP computes the MAC **S3'**. This value shall be predictable by the Purse Provider and unpredictable by anyone else.

This could be implemented by a MAC computed on transaction-dependent data elements and using a dedicated key. **S3'** shall only be computed by the EEP if the transaction was unsuccessful.

3.4 CURRENCY EXCHANGE TRANSACTION

3.4.1 SCOPE

The Currency Exchange Transaction is a transaction between an EEP and the Purse Provider.

From the point of view of the EEP, there are two types of Currency Exchange Transactions:

1. Currency Exchange within the same Slot (the source Slot is the same as the target Slot). As only a single Slot shall exist per currency, the target currency shall therefore be a new currency for the EEP.
2. Currency Exchange by transferring some or all of the Electronic Value from a Slot to another active Slot in the EEP (the source Slot is different from the target Slot).

Three authentication processes are specified in this Standard:

S1: A MAC provided by the EEP allowing the Purse Provider to verify its genuineness.

S2: A MAC supplied to the EEP by the Purse Provider, authenticating transaction data. If correct, the EEP is authorised to perform a Currency Exchange Transaction or to update the parameters of the application.

S3: A MAC provided by the EEP, intended for the Purse Provider, authenticating the state of the EEP after operation, indicating proof of currency exchange, or parameter update.

The Purse Provider, who verifies the genuineness of the EEP by verifying **S1**, decides to reject, to authorise the Currency Exchange Transaction or to update parameters of the EEP application. The last two are triggered in the EEP by its verification of **S2**. Then the EEP provides a proof of currency exchange, or no exchange of currency, or parameters updated in the form of **S3**.

If **S3** is available, it shall be sent to the Purse Provider in case of unsuccessful Currency Exchange Transactions. It may be transmitted in case of successful Currency Exchange Transactions.

In the case of Currency Exchange within the same Slot, all data elements of the Slot to be updated shall be provided by the Purse Provider and shall be included in the dynamic data authenticated by **S1** and **S2**. **S3** authenticates the balances of the updated Slot(s).

In the case of transferring value between Slots, the target Slot data (balance, currency code and exponent) shall be advised to the Purse Provider to determine whether the Currency Exchange may take place. Hence these data elements shall all be included in the dynamic data authenticated by **S1**. All affected data elements of the target Slot shall be included in the dynamic data authenticated by **S2**.

3.4.2 DYNAMIC DATA FOR AUTHENTICATION

The recommended data elements protected by means of **S1** are:

Name	Source
Discretionary Data	EEP
EEP Slot(s) Balance and Maximum Balance	EEP

EEP Source Currency	Load Device
EEP ID	EEP
Purse Provider ID	EEP
EEP Expiry Date	EEP
EEP Transaction Number	EEP
Load Device/ LSAM ID (1)	Load Device/LSAM
Loading Operator ID (1)	Load Device/LSAM
Challenge (1	Load Device/LSAM
Slot Status	EEP
Transaction Amount	Load Device
Transaction Currency	Load Device

(1) If an LSAM is present, the origin of these data elements may be the LSAM. In that case S1 will include ID_{LSAM} instead of ID_{LDA}.

The recommended data elements protected by means of **S2** are:

Name	Source
Discretionary Data	Purse Provider
EEP Deactivation Date	Purse Provider
EEP ID	EEP
Purse Provider ID	EEP
EEP Slot(s) Balance and Maximum Balance	Purse Provider
EEP Target Currency	EEP
EEP Transaction Number	EEP
PPSAM ID and Challenge	Purse Provider

The recommended data elements protected by means of **S3** are:

Name	Source
Discretionary Data	EEP
EEP ID	EEP
Purse Provider ID	EEP
EEP Slot(s) Balance and Maximum Balance	Purse Provider
EEP Transaction Number	EEP
PPSAM ID and Challenge	Purse Provider
Transaction Completion Code	EEP

4. AUTHENTICATION PROCESSES

4.1 ENTITY AUTHENTICATION

While the transactions are being performed, four cases of authentication processes are distinguished:

1. The Purse Provider verifies the authenticity (genuineness) of the EEP.
2. The EEP verifies the authenticity (genuineness) of the Purse Provider/PPSAM.
3. The Purchase Device verifies the authenticity (genuineness) of the EEP.
4. The EEP verifies the authenticity (genuineness) of the Purchase Device/PSAM.

The first two cases are denoted by the term *on-line*, the last two cases by *off-line*.

On-line authentication takes place between two entities that share secret key information. The authentication method is based on appending MACs to the relevant messages.

Since the Load Device is not engaged in cryptographic computations during these transactions, the cryptographic key architecture and algorithms adopted are at the discretion of the Purse Provider and thus outside the scope of this Standard. MACs computed with double-length *unique session* keys derived from *diversified* EEP keys would be a typical choice. The EEP Transaction Number shall be included in the dynamic data for authentication. This may be done by using it in the key derivation process or by explicitly including it in the data protected by a MAC.

In an interoperable transaction, off-line authentication takes place between an EEP and a Purchase Device that do not in general share secret keys. Therefore, the authentication cannot be implemented using symmetric cryptography only. In these cases, the authentication of dynamic transaction data is based on an asymmetric signature, used to exchange a session key that will be used for further authentication processes.

Both in the on-line and the off-line case, replay attacks shall be prevented by including a challenge from the verifier in the computation of the MAC or digital signature. In most cases this challenge will consist of the (unique) Transaction Number of the verifying party.

4.2 DATA ORIGIN AUTHENTICATION

4.2.1 DATA ORIGIN AUTHENTICATION FOR OFF-LINE TRANSACTIONS

After an off-line transaction has been concluded, two authentication processes are distinguished:

- The Acquiring Technical Operator verifies the authenticity of the Purchase Trace.
- The Purse Provider verifies the authenticity of the Purchase Trace.

In the first case, if the MAC **S5** was generated, the Acquiring Technical Operator verifies the validity of **S5** when processing the Purchase Traces.

In the second case, the MAC **S6**, which is included in the Purchase Trace, is intended for the Purse Provider and is used to verify the validity of this Purchase Trace.

4.2.2 DATA ORIGIN AUTHENTICATION FOR ON-LINE TRANSACTIONS

In case of Load against other means of payment two authentication processes are distinguished:

- The Purse Provider verifies on-line the guarantee of payment of the Loading Operator.
- The Loading Operator verifies off-line the proof of unsuccessful Load Transaction.

In the first case the Purse Provider verifies the validity of **Sig2** when processing the on-line request for load.

In the second case the MAC **S3'**, which is computed by the EEP and intended for the Loading Operator, is used to verify the unsuccessful outcome of the Load Transaction and to decide off-line if the load amount should be refunded.

5. KEY MANAGEMENT

5.1 SECRET AND PRIVATE EEP KEYS

The EEP application needs secret and Private Keys for supporting authentication in EEP transactions.

The way these keys are stored and protected internally by the ICC is out of the scope of this Standard and up to the discretion of the Purse Provider. It is essential that these keys are only accessible by the EEP for the execution of cryptographic computations in such a way that it is not feasible to extract their value, even partially.

If the EEP is required to execute a cryptographic computation in the course of a command and the necessary key is absent or corrupted, the command shall be aborted and the EEP shall return the appropriate error code.

5.2 PUBLIC KEY CERTIFICATES

This section deals in detail with a three-level hierarchy.

However, in some cards there can be an additional layer of certificates. In this case, deciphering the first certificate read from the card recovers the Regional Authority Public Key to be used for decyphering the Purse Provider Public Key Certificate and the Purse Provider Public Key Certificate is the second certificate to be sent.

Also in some Purchase Devices there can be an additional layer of certificates. In this case, deciphering the first certificate sent to the card recovers the Regional Authority Public Key to be used for decyphering the Acquirer Public Key Certificate and the Acquirer Public Key Certificate is the second certificate to be read.

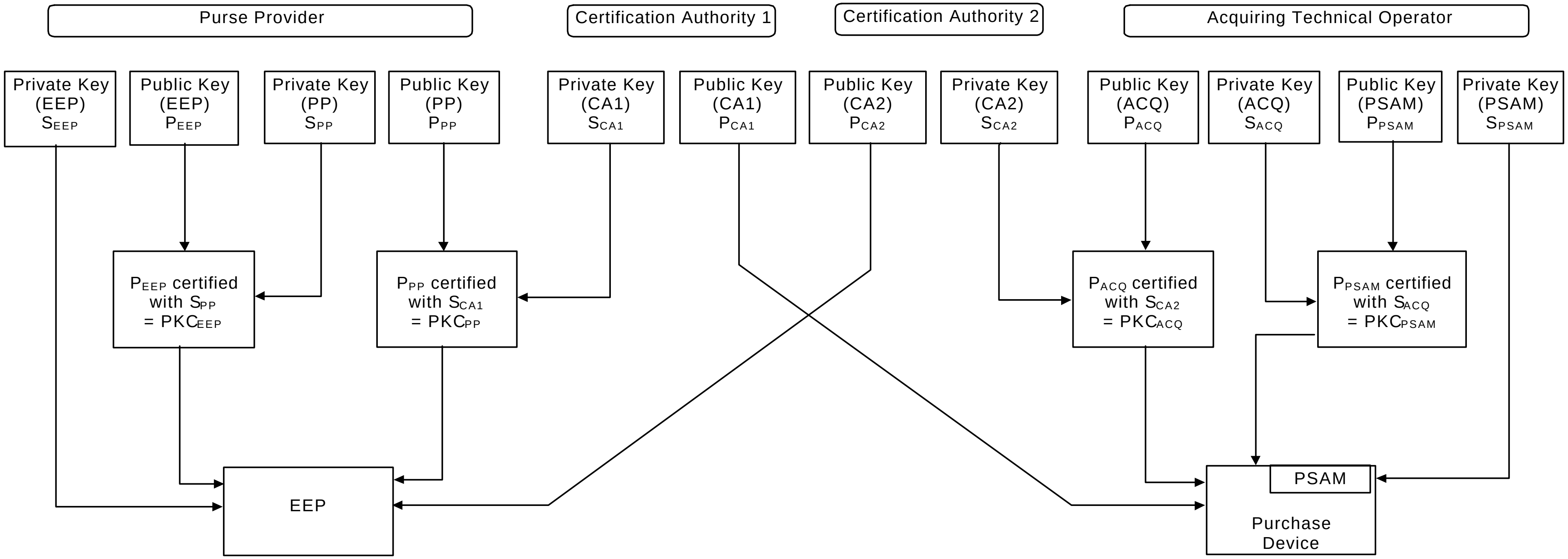
As off-line authentication (EEP to Purchase Device, Purchase Device/PSAM to EEP) is based on the generation and verification of Public Key signatures, the Public Key, needed for verification, has to be communicated to the verifying party in an authentic way.

This shall be achieved by the exchange of Public Key certificates, generated in the framework of a Public Key certification hierarchy, as specified in [EMV'96]. The EEP and the Purchase Device shall support a multi-layer hierarchy of keys.

The EEP contains only one version of the Acquirer Certification Authority Public Key and only one Purse Provider Public Key certificate.

The key version of the Certification Authority Public Key, corresponding to this certificate, is stored in the EEP application. The Purchase Device shall support all the different Certification Authority Public Keys for the key versions in use and shall contain the certificates corresponding to all the different Certification Authority Public Keys in use.

The following diagram shows the relationships between the various entities keys and certificates in a three-layer environment. The two Certification Authorities shown could be separate entities or one single entity and the diagram could then be representing two versions of the Certification Authority Public Key.


Purse Provider
Certification Authority 1
Certification Authority 2
Acquiring Technical Operator
Private Key (EEP) S_{EEP}
Public Key (EEP) P_{EEP}
Private Key (PP) S_{PP}
Public Key (PP) P_{PP}
Private Key (CA1) S_{CA1}
Public Key (CA1) P_{CA1}
Public Key (CA2) P_{CA2}
Private Key (CA2) S_{CA2}
Public Key (ACQ) P_{ACQ}
Private Key (ACQ) S_{ACQ}
Public Key (PSAM) P_{PSAM}
Private Key (PSAM) S_{PSAM}
P_{EEP} certified with S_{PP} = PKC_{EEP}
P_{PP} certified with S_{CA1} = PKC_{PP}
P_{ACQ} certified with S_{CA2} = PKC_{ACQ}
P_{PSAM} certified with S_{ACQ} = PKC_{PSAM}
EEP
PSAM
Purchase Device

EEP Authentication		**EEP Authentication**
Sends PKC_{PP} to terminal	→	Uses P_{CA1} to verify PKC_{PP}
Sends PKC_{EEP} to terminal	→	Uses P_{PP} to verify PKC_{EEP}
PSAM Authentication		**PSAM Authentication**
Uses P_{CA2} to verify PKC_{ACQ}	←	Sends PKC_{ACQ} to EEP
Uses P_{ACQ} to verify PKC_{PSAM}	←	Sends PKC_{PSAM} to EEP
		Calculates Session Key
		Creates DS [session key] using S_{PSAM}
Uses S_{EEP} to decipher DS	←	Enciphers DS with P_{EEP} and sends DS to EEP
Uses P_{PSAM} to verify DS and recover session key		
Generates MAC with session key and sends it to PSAM	→	

5.2.1 PSAM AND ACQUIRING TECHNICAL OPERATOR CERTIFICATES

For the detailed description of the PSAM and Acquirer certificates refer to section 6.

The key that is used by the PSAM to sign a session key in the digital signature is called the *PSAM Private Key*. The key needed by the EEP to verify the digital signature and recover the session key is called the *PSAM Public Key*.

1. The Purchase Device sends the *Acquirer Public Key Certificate* to the EEP. The EEP verifies it using *the CA Public Key* and stores the *Acquiring Technical Operator Public Key*
2. The Purchase Device sends the *PSAM Public Key Certificate* to the EEP. The EEP verifies it using *the Acquirer Public Key* and stores the *PSAM Public Key*.
3. The Purchase Device/PSAM sends **S2** , enciphering the digital signature, to the EEP. The EEP verifies it using the *EEP Private Key* and the *PSAM Public Key*

5.2.2 EEP AND PURSE PROVIDER CERTIFICATES

For the detailed description of the EEP and Purse Provider certificates refer to section 6.

The key that is used by the EEP to decipher **S2** and obtain the digital signature is called the *EEP Private Key*. The key needed by the PSAM to encipher the digital signature is called the *EEP Public Key*.

The Purchase Device requests the necessary Public Key certificates before enciphering the digital signature. The EEP sends the *EEP Public Key Certificate*, authenticating the *EEP Public Key* to the Purchase Device. This certificate is generated by the Purse Provider using the *Purse Provider Private Key* and written into the non-volatile memory of the ICC at personalisation time.

For the verification of the *EEP Public Key Certificate*, the Purchase Device needs an authentic copy of the *Purse Provider Public Key*. Since there may be many Purse Providers, the PSAM cannot be expected to have the Public Keys of all Purse Providers. Instead, the Purchase Device is provided with a *Certification Authority Public Key*.

This Certification Authority generates *Purse Provider Public Key Certificates* using the *CA Private Key*. Prior to sending the *EEP Public Key Certificate*, the EEP sends the *Purse Provider Public Key Certificate* to the Purchase Device.

The sequence in a three-layer environment is summarised as follows:

1. The EEP sends *Purse Provider Public Key Certificate* to the Purchase Device. The Purchase Device verifies it using the correct version of the *CA Public Key* and stores the *Purse Provider Public Key*.
2. The EEP sends *EEP Public Key Certificate* to the Purchase Device. The Purchase Device verifies it using the *Purse Provider Public Key* and stores the *EEP Public Key*.
3. The EEP sends a MAC (**S3** in the case of the Purchase Transaction, **S1** in the case of the Purchase Cancellation Transaction) to the Purchase Device. The Purchase Device/PSAM verifies it using the exchanged session key.

5.2.3 KEY LENGTHS

The minimum lengths of the Public Key modulo as specified by this Standard are:

- 1024 bits for Certification Authority keys;
- 896 bits for the Purse Provider and Acquiring Technical Operator keys;
- 768 bits for the EEP
- 736 bits for the PSAM

Except for the EEP, the public exponents shall have a value equal to 2, 3 or 2^{16}+1. [EMV'96]. The public exponents for the EEP have a value equal to 3 or 2^{16}+1.

6. SIGNATURE GENERATION AND CERTIFICATE VERIFICATION

For security mechanisms and approved cryptographic algorithms, refer to [EMV'96].

6.1 EEP AUTHENTICATION

6.1.1 EEP KEYS AND CERTIFICATES

To support card authentication, an EEP shall own its own unique Public Key pair consisting of a private signature key and the corresponding public verification key. The EEP Public Key shall be stored on the EEP in a Public Key certificate.

More precisely, a multi-layer Public Key certification scheme is used. In this section, a three-layer certifcation scheme is elaborated (Certification Authority, Purse Provider, EEP). The same reasoning can be applied to a four-layer certification scheme (Certification Authority, Regional Authority, Purse Provider, EEP) or a multi-level scheme.

Each EEP Public Key is certified by its Purse Provider, and the Certification Authority certifies the Purse Provider Public Key. This implies that, for the verification of an EEP signature, the terminal first needs to verify two certificates (or only one, the EEP certificate, if the correct Purse Provider Public Key is cached) in order to retrieve and authenticate the EEP Public Key, which is then used to verify the EEP's dynamic signature.

The bit length of all moduli shall be a multiple of 8, the leftmost bit of its leftmost byte being 1. All lengths are given in bytes.

The signature scheme specified in [EMV'96] is applied on the data in Table 1 and on the data in Table 2 using the Certification Authority Private Key $S_{CA,PP}$ and the Purse Provider Private Key S_{PP} in order to obtain the Purse Provider Public Key Certificate and EEP Public Key Certificate, respectively.

The Public Key pair of the Certification Authority has a Certification Authority Public Key Modulus of $LPKM_{CA,PP}$ bytes, where $LPKM_{CA,PP} \leq 248$. The Certification Authority Public Key Exponent shall be 2, 3 or $2^{16}+1$.

The Public Key pair of the Purse Provider has a Public Key modulus of $LPKM_{CA,PP}$ bytes, where $LPKM_{PP} < 248$ and $LPKM_{PP} < LPKM_{CA,PP}$. If $LPKM_{PP} > (LPKM_{CA,PP} - 36)$, the Purse Provider Public Key Modulus is split into two parts, namely one part consisting of the $LPKM_{CA,PP}$ - 36 most significant bytes of the modulus (the Leftmost Digits of the Purse Provider Public Key) and a second part consisting of the remaining $LPKM_{PP} - (LPKM_{CA,PP} - 36)$ least significant bytes of the modulus (the Purse Provider Public Key Remainder). The Purse Provider Public Key Exponent shall be equal to 2, 3 or $2^{16}+1$.

The Public Key pair of the EEP has an EEP Public Key Modulus of $LPKM_{EEP}$ bytes, where $LPKM_{EEP} \leq 128$ and $LPKM_{EEP} < LPKM_{PP}$. If $LPKM_{EEP} > (LPKM_{PP} - 42)$, the EEP Public Key Modulus is divided into two parts, one part consisting of the $LPKM_{PP}$ - 42 most significant bytes of the modulus (the Leftmost Digits of the EEP Public Key) and a second part consisting of the remaining $LPKM_{EEP} - (LPKM_{PP} - 42)$ least significant bytes of the modulus (the EEP Public Key Remainder). The EEP Public Key Exponent shall be equal to 3 or $2^{16}+1$.

To execute authentication, the terminal shall first retrieve and authenticate the EEP Public Key (this process is called EEP Public Key authentication). All the information necessary for the EEP Public Key authentication is specified in Table 3 and stored in the EEP. With the exception of the RID, which can be obtained from the AID, this information may be retrieved with the Read Record command or by means of caching where the Purse Provider Certificate is concerned.

Field Name	Length	Description	Format
Certificate Format	1	Hex. value ‘02’	b
Purse Provider Identification number	4	Identifier for a Purse Provider	b
Certificate Expiration Date	2	MMYY after which this certificate is invalid	n 4
Certificate Serial Number	3	Binary Number unique to this certificate assigned by the Certification Authority	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme	b
Purse Provider Public Key Algorithm Indicator	1	Identifies the digital signature algorithm and the public key exponent to be used with the Purse Provider Public Key	b
Purse Provider Public Key Length	1	$LPKM_{PP}$	b
Filler	1	Value '00'	b
Purse Provider Public Key or Leftmost Digits of the Acquirer Public Key [(1)]	$LPKM_{CA, PP}$ - 36	This field consists of the $LPKM_{CA, PP}$ - 36 most significant bytes of the Purse Provider Public Key[(1)]	b
Purse Provider Public Key Remainder	0 to 35	PKR_{PP} consists of the $LPKM_{PP}$ - $LPKM_{CA, PP}$ + 36 least significant bytes of the Purse Provider Public Key	b

TABLE 1 - PURSE PROVIDER PUBLIC KEY DATA TO BE SIGNED BY THE CERTIFICATION AUTHORITY
(i.e. input to the hash algorithm)

[(1)] $LPKM_{CA, PP}$ - 22 bytes of the data signed is retrieved from the signature. Since the first to the eight data element in table 1 are 14 bytes long, there are $LPKM_{CA, PP}$ - 22 - 14= $LPKM_{CA, PP}$ - 36 bytes remaining in the signature to store the Purse Provider Public Key Modulus.

Field Name	Length	Description	Format
Certificate Format	1	Hex. value ‘04’	b
Purse Identifier	10	Concatenation of Purse Provider ID (4 byte), EEP ID (6 byte).	b
Certificate Expiration Date	2	MMYY after which this certificate is invalid	n 4
Certificate Serial Number	3	Binary Number unique to this certificate assigned by the Certification Authority	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme	b

EEP Public Key Algorithm Indicator	1	Identifies the digital signature algorithm and the public key exponent to be used with the EEP Public Key	b
EEP Public Key Length	1	$LPKM_{EEP}$	b
Filler	1	Value ‘00'	b
EEP Public Key or Left most Digits of the EEP Public Key	$LPKM_{PP}$ - 42	This field consists of the $LPKM_{PP}$ - 42 most significant bytes of the EEP Public Key [(1)]	b
EEP Public Key Remainder	0 to 41	PKR_{EEP} consists of the $LPKM_{EEP}$ - $LPKM_{PP}$ + 42 least significant bytes of the Purse Provider Public Key	b

TABLE 2 - EEP PUBLIC KEY DATA TO BE SIGNED BY THE PURSE PROVIDER
(i.e. input to the hash algorithm)

[(1)] $LPKM_{PP}$ - 22 bytes of the data signed is retrieved from the signature. Since the length of the first to the eight data element in table 2 is 20 byte, there are $LPKM_{PP}$ - 22 - 20= $LPKM_{PP}$ - 42 bytes remaining for the data to be stored in the signature.

Acronym	Length	Value	Format
	5	Registered Application Provider Identifier (RID)	b
$VK_{CA,PP}$	1	Purse Provider Certification Authority Public Key version	b
PKC_{PP}	$LPKM_{CA,PP}$	Purse Provider Public Key Certificate	b
PKR_{PP}	$LPKM_{PP}$ - $LPKM_{CA,PP}$ + 36	Purse Provider Public Key Remainder, if present	b
PKE_{PP}	$LPKE_{PP}$	Purse Provider Public Key Exponent, derived from the algorithm indicator	b
PKC_{EEP}	$LPKM_{PP}$	EEP Public Key Certificate	b
PKR_{EEP}	$LPKM_{EEP}$ - $LPKM_{PP}$ + 42	EEP Public Key Remainder, if present	b
PKE_{EEP}	$LPKE_{EEP}$	EEP Public Key Exponent, derived from the algorithm indicator	b

TABLE 3 - DATA OBJECTS REQUIRED FOR PUBLIC KEY AUTHENTICATION FOR EEP AUTHENITCATION

6.1.1.1 *RETRIEVAL OF THE CERTIFICATION AUTHORITY PUBLIC KEY*

The terminal reads the Purse Provider Certification Authority Public Key version. Using this Public Key version and the RID, the terminal can identify which certificates and associated key-related information to send and the corresponding algorithm to be used.

6.1.1.2 *RETRIEVAL OF THE PURSE PROVIDER PUBLIC KEY*

1. If the Purse Provider Public Key Certificate has a length different from the length of the

Public Key modulus obtained from the previous level, authentication has failed.

2. In order to obtain the recovered data specified in table 4, apply the recovery function specified in [EMV'96] on the Purse Provider Public Key Certificate using the Public Key obtained from the previous level, in conjunction with the corresponding algorithm. If the Recovered Data Trailer is not equal to 'BC', dynamic data authentication has failed.

Field Name	Length	Description	Format
Recovered Data Header	1	Hex. value '6A' or '4A' (if no remainder present)	b
Certificate Format	1	Hex. value '02'	b
Purse Provider Identification number	4	Identifier for a Purse Provider	b
Certificate Expiration Date	2	MMYY after which this certificate is invalid	n 4
Certificate Serial Number	3	Binary Number unique to this certificate assigned by the Certification Authority	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme	b
Purse Provider Public Key Algorithm Indicator	1	Identifies the digital signature algorithm and the public key exponent to be used with the Purse Provider Public Key	b
Purse Provider Public Key Length	1	$LPKM_{PP}$	b
Filler	1	Value '00'	b
Purse Provider Public Key or Leftmost Digits of the Purse Provider Public Key	$LPKM_{CA, PP}$ - 36	This field consists of the $LPKM_{CA, PP}$ - 36 most significant bytes of the Purse Provider Public Key	b
Hash Result	20	Hash of the Purse Provider Public key and its related information	b
Recovered Data Trailer	1	Hex. value 'BC'	b

TABLE 4 - FORMAT OF THE DATA TO BE RECOVERED FROM THE PURSE PROVIDER PUBLIC KEY CERTIFICATE

3. Check the Recovered Data Header. If it is not '6A' or '4A', card authentication has failed.

4. Check the Certificate Format. If it is not '02', card authentication has failed.

5. Concatenate from left to right the second to the tenth data element in table 4 (that is, Certificate Format through Purse Provider Public Key or Leftmost Digits of the Purse Provider Public Key), followed by the Purse Provider Public Key Remainder (if present.

6. Apply the indicated hash algorithm (derived from the Hash Algorithm Indicator) to the result of the concatenation of the previous step to produce the hash result.

7. Compare the calculated hash result from the previous step with the Recovered Hash Result.

If they are not the same, dynamic data authentication has failed.

8. Verify that the Purse Provider Identification Number matches the Purse Provider Identifier obtained from the EEP application. If not, the authentication has failed.

9. Verify that the last day of the month specified in the Certificate Expiration Date is equal to or later than today's date. If the Certificate Expiration Date is earlier than today's date, the certificate has expired, in which case authentication has failed.

10. Verify that the concatenation of RID, Purse Provider Certification Authority Public Key version, and Certificate Serial Number is valid. If not, the authentication has failed. (This step is optional and is to allow the revocation of the Purse Provider Public Key Certificate against a list that may be kept in the terminal.)

11. If the Purse Provider Public Key Algorithm Indicator is not recognised, card authentication has failed.

12. If all the above checks are correct, concatenate the Leftmost Digits of the Purse Provider Public Key and Purse Provider Public Key Remainder (if present) to obtain the Purse Provider Public Key Modulus, and continue with the next steps for retrieval of the EEP Public Key.

6.1.1.3 *RETRIEVAL OF THE EEP PUBLIC KEY*

1. If the EEP Public Key Certificate has a length different from the length of the Purse Provider Public Key modulus obtained in the previous section, authentication has failed.

2. In order to obtain the recovered data specified in table 5, apply the recovery function specified in [EMV'96] on the EEP Public Key Certificate using the Purse Provider Public Key in conjunction with the corresponding algorithm. If the Recovered Data Trailer is not equal to 'BC', dynamic data authentication has failed.

Field Name	Length	Description	Format
Recovered Data Header	1	Hex. value '6A' or '4A' (if no remainder present)	b
Certificate Format	1	Hex. value '04'	b
Purse Identifier	10	Concatenation of Purse Provider ID (4 byte), EEP ID (6 byte).	b
Certificate Expiration Date	2	MMYY after which this certificate is invalid	n 4
Certificate Serial Number	3	Binary Number unique to this certificate assigned by the Certification Authority	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme	b
EEP Public Key Algorithm Indicator	1	Identifies the digital signature algorithm and the public key exponent to be used with the EEP Public Key	b
EEP Public Key Length	1	LPKM$_{EEP}$	b
Filler	1	Value '00'	b
EEP Public Key or	LPKM$_{PP}$ -	This field consists of the LPKM$_{PP}$ - 42 most	b

Left most Digits of the EEP Public Key	42	significant bytes of the EEP Public Key	
Hash Result	20	Hash of the Purse Provider Public key and its related information	b
Recovered Data Trailer	1	Hex. value 'BC'	b

TABLE 5 - FORMAT OF THE DATA TO BE RECOVERED FROM THE EEP PUBLIC KEY CERTIFICATE

3. Check the Recovered Data Header. If it is not '6A' or '4A', card authentication has failed.

4. Check the Certificate Format. If it is not '04', card authentication has failed.

5. Concatenate from left to right the second to the tenth data element in table 5 (that is, Certificate Format through EEP Public Key or Leftmost Digits of the EEP Public Key), followed by the EEP Public Key Remainder (if present) and finally the EEP Public Key Exponent.

6. Apply the indicated hash algorithm (derived from the Hash Algorithm Indicator) to the result of the concatenation of the previous step to produce the hash result.

7. Compare the calculated hash result from the previous step with the Recovered Hash Result. If they are not the same, dynamic data authentication has failed.

8. Check if the recovered EEP Identification Number is equal to the concatenation of the Purse Provider Identifier and the EEP Identifier. If not, the authentication has failed.

9. Verify that the last day of the month specified in the Certificate Expiration Date is equal to or later than today's date. If not, case authentication has failed.

10. If the EEP Public Key Algorithm Indicator is not recognised, card authentication has failed.

11. If all the above checks are correct, concatenate the Leftmost Digits of the EEP Public Key and EEP Public Key Remainder (if present) to obtain the EEP Public Key Modulus.

6.2 TERMINAL AUTHENTICATION

6.2.1 TERMINAL KEYS AND CERTIFICATES

To support terminal authentication, a PSAM shall own its own unique Public Key pair consisting of a private signature key and the corresponding public verification key. The PSAM Public Key shall be stored on the PSAM/terminal in a Public Key certificate.

More precisely, a multi-layer Public Key certification scheme is used. In this section, a three-layer certification scheme is elaborated (Certification Authority, Acquirer, PSAM). The same reasoning can be applied to a four-layer certification scheme (Certification Authority, Regional Authority, Acquirer, PSAM) or a multi-level scheme.

Each PSAM Public Key is certified by its Acquirer, and the Certification Authority certifies the Acquirer Public Key. This implies that, for the verification of a PSAM signature, the terminal first needs to verify two certificates (or only one, the PSAM certificate, if the correct Acquirer Certificate is cached) in order to retrieve and authenticate the PSAM Public Key, which is then used to verify the PSAM's dynamic signature.

The bit length of all moduli shall be a multiple of 8, the leftmost bit of its leftmost byte being 1. All lengths are given in bytes.

The signature scheme specified in [EMV'96] is applied on the data in Table 6 and on the data in Table 7 using the Certification Authority Private Key $S_{CA,ACQ}$ and the Acquirer Private Key S_{ACQ} in order to obtain the Acquirer Public Key Certificate and EEP Public Key Certificate, respectively.

The Public Key pair of the Certification Authority has a Certification Authority Public Key Modulus of $LPKM_{CA,ACQ}$ bytes, where $LPKM_{CA,ACQ} \leq 248$. The Certification Authority Public Key Exponent shall be 2, 3 or $2^{16}+1$.

The Public Key pair of the Acquirer has a Public Key modulus of $LPKM_{CA,PP}$ bytes, where $LPKM_{ACQ} < 209$ and $LPKM_{ACQ} < LPKM_{CA,ACQ}$. If $LPKM_{ACQ} > (LPKM_{CA,ACQ} - 36)$, the Acquirer Public Key Modulus is split into two parts, namely one part consisting of the $LPKM_{CA,ACQ} - 36$ most significant bytes of the modulus (the Leftmost Digits of the Acquirer Public Key) and a second part consisting of the remaining $LPKM_{ACQ} - (LPKM_{CA,ACQ} - 36)$ least significant bytes of the modulus (the Acquirer Public Key Remainder). The Acquirer Public Key Exponent shall be equal to 2,3 or $2^{16}+1$.

The Public Key pair of the PSAM has an PSAM Public Key Modulus of $LPKM_{EEP}$ bytes, where $LPKM_{PSAM} \leq LPKM_{EEP}$-4 and $LPKM_{PSAM} < LPKM_{ACQ}$. If $LPKM_{PSAM} > (LPKM_{ACQ} - 42)$, the PSAM Public Key Modulus is divided into two parts, one part consisting of the $LPKM_{ACQ} - 42$ most significant bytes of the modulus (the Leftmost Digits of the PSAM Public Key) and a second part consisting of the remaining $LPKM_{PSAM} - (LPKM_{ACQ} - 42)$ least significant bytes of the modulus (the PSAM Public Key Remainder). The PSAM Public Key Exponent shall be equal to 2, 3 or $2^{16}+1$.

To execute authentication, the EEP shall first retrieve and authenticate the PSAM Public Key (this process is called PSAM Public Key authentication). All the information necessary for the PSAM Public Key authentication is specified in Table 8 and stored in the terminal/PSAM. Based on the Acquirer Certification Authority Public Key version ($VK_{CA,ACQ}$) and the RID, which can be derived from the AID, the terminal decides on which certificates, Public Key remainders and Public Key exponents are sent to the card with the Verify Certificate command. The terminal need not send the Acquirer Public Key Certificate, the Acquirer Public Key Remainder and the Acquirer Public Key Exponent if the card has cached the correct Acquirer Public Key.

Field Name	Length	Description	Format
Certificate Format	1	Hex. value '82'	b
PSAM Creator	9	PSAM Creator Identifier	b
Certificate Expiration Date	2	MMYY after which this certificate is invalid	n 4
Certificate Serial Number	3	Binary Number unique to this certificate assigned by the Certification Authority	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme	b
Acquirer Public Key Algorithm Indicator	1	Identifies the digital signature algorithm and the public key exponent to be used with the Acquirer Public Key	b

Acquirer Public Key Length	1	LPKM$_{ACQ}$	b
Filler	1	Value '00'	b
Acquirer Public Key or Leftmost Digits of the Acquirer Public Key	LPKM$_{CA, ACQ}$ - 41	This field consists of the LPKM$_{CA, ACQ}$ - 41 most significant bytes of the Acquirer Public Key[(1)]	b
Acquirer Public Key Remainder	0 to 40	PKR$_{ACQ}$ consists of the LPKM$_{ACQ}$ - LPKM$_{CA, ACQ}$ + 41 least significant bytes of the Acquirer Public Key	b

TABLE 6 - ACQUIRER PUBLIC KEY DATA TO BE SIGNED BY THE CERTIFICATION AUTHORITY
(i.e. input to the hash algorithm)

[(1)] LPKM$_{CA, ACQ}$ - 22 bytes of the data signed is retrieved from the signature. Since the length of the first to the eight data element in table 6 is 16 bytes, there are LPKM$_{CA, ACQ}$ - 22 - 19= LPKM$_{CA, ACQ}$ - 41 bytes remaining in the signature to store the Acquirer Public Key Modulus.

Field Name	Length	Description	Format
Certificate Format	1	Hex. Value ‘84’ ‘	b
PSAM Identifier	10	PSAM ID	b
Certificate Expiration Date	2	MMYY after which this certificate is invalid	n 4
Certificate Serial Number	3	Binary Number unique to this certificate assigned by the Certification Authority	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme	b
PSAM Public Key Algorithm Indicator	1	Identifies the digital signature algorithm and the public key exponent to be used with the PSAM Public Key	b
PSAM Public Key Length	1	LPKM$_{PSAM}$	b
Filler	1	Value '00'	b
PSAM Public Key or Left most Digits of the PSAM Public Key	LPKM$_{ACQ}$ - 42	This field consists of the LPKM$_{ACQ}$ - 42 most significant bytes of the PSAM Public Key[(1)]	b
PSAM Public Key Remainder	0 to 41	PKR$_{PSAM}$ consists of the LPKM$_{PSAM}$ - LPKM$_{ACQ}$ + 42 least significant bytes of the Acquirer Public Key	b

TABLE 7 - PSAM PUBLIC KEY DATA TO BE SIGNED BY THE ACQUIRER
(i.e. input to the hash algorithm)

[(1)] LPKM$_{ACQ}$ - 22 bytes of the data signed is retrieved from the signature. Since the length of the first to the eight data element in table 7 is 20 bytes, there are LPKM $_{ACQ}$ - 22 - 20= LPKM $_{PP}$ - 42 bytes remaining for the data to be stored in the signature.

Acronym	Length	Value	Format
	5	Registered Application Provider Identifier (RID)	b
VK$_{CA,ACQ}$	1	Acquirer Certification Authority Public Key version	b
PKC$_{ACQ}$	LPKM$_{CA,ACQ}$	Acquirer Public Key Certificate	b
PKR$_{ACQ}$	LPKM$_{ACQ}$ – LPKM$_{CA,ACQ}$ + 41	Acquirer Public Key Remainder, if present	b
PKE$_{ACQ}$	LPKE$_{ACQ}$	Acquirer Public Key Exponent, derived from algorithm indicator	b
PKC$_{PSAM}$	LPKM$_{ACQ}$	PSAM Public Key Certificate	b
PKR$_{PSAm}$	LPKM$_{PSAM}$ - LPKM$_{AcQ}$ + 42	PSAM Public Key remainder, if present	b
PKE$_{PSAM}$	LPKE$_{PSAM}$	PSAM Public Key Exponent, derived from algorithm indicator	b

TABLE 8 - DATA OBJECTS REQUIRED FOR PUBLIC KEY AUTHENTICATION FOR TERMINAL AUTHENITCATION

6.2.1.1 *RETRIEVAL OF THE CERTIFICATION AUTHORITY PUBLIC KEY*

The terminal reads the Acquirer Certification Authority Public Key version. Using this Public Key version and the RID, the terminal can identify which certificates and associated key-related information (exponent, remainder) to send and the corresponding algorithm to be used.

6.2.1.2 *RETRIEVAL OF THE ACQUIRER PUBLIC KEY*

1. If the Acquirer Public Key Certificate has a length different from the length of the Public Key modulus obtained from the previous level, authentication has failed.

2. In order to obtain the recovered data specified in table 9, apply the recovery function specified in [EMV'96] on the Acquirer Public Key Certificate using the Public Key obtained from the previous level in conjunction with the corresponding algorithm. If the Recovered Data Trailer is not equal to 'BC', authentication has failed.

Field Name	Length	Description	Format
Recovered Data Header	1	Hex. value '6A' or '4A' (if no remainder present)	b
Certificate Format	1	Hex. value '82'	b
PSAM Creator ID	9	PSAM Creator Identifier	b
Certificate Expiration Date	2	MMYY after which this certificate is invalid	n 4
Certificate Serial Number	3	Binary Number unique to this certificate assigned by the Certification Authority	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme	b

Acquirer Public Key Algorithm Indicator	1	Identifies the digital signature the and public key exponent to be used with the Acquirer Public Key	b
Acquirer Public Key Length	1	LPKM$_{ACQ}$	b
Filler	1	Value '00'	b
Acquirer Public Key or Leftmost Digits of the Acquirer Public Key	LPKM$_{CA, ACQ}$ - 41	This field consists of the LPKM$_{CA, ACQ}$ - 41 most significant bytes of the Acquirer Public Key	b
Hash Result	20	Hash of the Acquirer Public Key and its related information	b
Recovered Data Trailer	1	Hex. value ‘BC’	b

TABLE 9 - FORMAT OF THE DATA TO BE RECOVERED FROM THE ACQUIRER PUBLIC KEY CERTIFICATE

3. Check the Recovered Data Header. If it is not ‘6A’ or '4A', authentication has failed.

4. Check the Certificate Format.

5. Concatenate from left to right the second to the tenth data element in table 9 (that is, Certificate Format through Acquirer Public Key or Leftmost Digits of the Acquirer Public Key), followed by the Acquirer Public Key Remainder (if present).

6. Apply the indicated hash algorithm (derived from the Hash Algorithm Indicator) to the result of the concatenation of the previous step to produce the hash result.

7. Compare the calculated hash result from the previous step with the Recovered Hash Result. If they are not the same, authentication has failed.

8. Verify that the Acquirer Identification Number matches the Acquirer Identifier obtained from the Verify Certificate command. If not, the authentication has failed.

9. If the Acquirer Public Key Algorithm Indicator is not recognised, authentication has failed.

10. If all the above checks are correct, concatenate the Leftmost Digits of the Acquirer Public Key and Acquirer Public Key Remainder (if present) to obtain the Acquirer Public Key Modulus, and continue with the next steps for retrieval of the PSAM Public Key.

6.2.1.3 Retrieval of the PSAM Public Key

1. If the PSAM Public Key Certificate has a length different from the length of the Acquirer Public Key modulus obtained in the previous section, authentication has failed.

2. In order to obtain the recovered data specified in table 10, apply the recovery function specified in [EMV’96] on the PSAM Public Key Certificate using the Acquirer Public Key in conjunction with the corresponding algorithm. If the Recovered Data Trailer is not equal to ‘BC’, authentication has failed.

Field Name	Length	Description	Format
Recovered Data Header	1	Hex. value ‘6A’ or '4A' (if no remainder present)	b
Certificate Format	1	Hex. value ‘84’	b
PSAM Identifier	10	PSAM Identifier	b
Certificate Expiration Date	2	MMYY after which this certificate is invalid	n 4
Certificate Serial Number	3	Binary Number unique to this certificate assigned by the Certification Authority	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme	b
PSAM Public Key Algorithm Indicator	1	Identifies the digital signature algorithm and the public key exponent to be used with the Acquirer Public Key	b
PSAM Public Key Length	1	$LPKM_{PSAM}$	b
Filler	1	Value '00'	b
PSAM Public Key or Leftmost Digits of the acquirer Public Key	$LPKM_{ACQ}$-42	This field consists of the $LPKM_{PSAM}$ - 42 most significant bytes of the PSAM	b
Hash Result	20	Hash of the Acquirer Public key and its related information	b
Recovered Data Trailer	1	Hex. value ‘BC’	b

TABLE 10 - FORMAT OF THE DATA TO BE RECOVERED FROM THE PSAM PUBLIC KEY CERTIFICATE

3. Check the Recovered Data Header. If it is not ‘6A’ or '4A', authentication has failed.

4. Check the Certificate Format.

5. Concatenate from left to right the second to the tenth data element in table 10 (that is, Certificate Format through PSAM Public Key or Leftmost Digits of the PSAM Public Key), followed by the PSAM Public Key Remainder (if present).

6. Apply the indicated hash algorithm (derived from the Hash Algorithm Indicator) to the result of the concatenation of the previous step to produce the hash result.

7. Compare the calculated hash result from the previous step with the Recovered Hash Result. If they are not the same, authentication has failed.

8. Check if the recovered PSAM Identification Number matches the identifier obtained through the Verify Certificate command.. If not, the authentication has failed.

9. If the PSAM Public Key Algorithm Indicator is not recognised, authentication has failed.

10. If all the above checks are correct, concatenate the Leftmost Digits of the PSAM Public Key and PSAM Public Key Remainder (if present) to obtain the PSAM Public Key Modulus.

7. EEP MINIMUM SECURITY REQUIREMENTS

This section describes the security mechanisms required by this Standard to be implemented in the EEP application in order to protect the key material and ensure transaction security.

7.1 DATA INTEGRITY MECHANISMS

As a minimum requirement, the integrity of the following sensitive data elements shall be ensured: EEP ID, Slot Data, Transaction Number and cryptographic keys. The way in which this is implemented is at the discretion of the Purse Provider. Appropriate completion codes shall be provided ([ISO/IEC 7816-4] or application specific).

7.2 INDIVISIBILITY OF EEP COMMANDS

The integrity of the EEP data elements in non-volatile memory (e.g. an EEP Slot Balance) shall be maintained against interruption of command execution either caused by card withdrawal, accidental power-failure or any other cause.

For this purpose, the commands shall be implemented in a way that guarantees the integral modification of data elements in non-volatile memory of the ICC, including security-related data. Hence, if the execution of a command requires the updating of a number of data elements in non-volatile memory, the EEP application shall behave afterwards in one of two possible ways:

1. as if all data elements corresponding to this command are updated;
2. as if no data elements have been updated.

This may be implemented by means of a mechanism that, in the case of a partial update of data elements, restores (“rolls back”) the internal status to the one prior to the execution of the interrupted command.

If the command execution is interrupted during the transmission of the command response, the command shall not be rolled back.

7.3 EEP COMMAND CONTROL

In all four transactions described in section 3, the EEP receives two commands: an *initialisation* command and an *action* command, which execute the *debit*, *credit*, *re-credit* or *currency exchange*.

An action command shall only be accepted if it has been preceded in the same Card Session by the corresponding initialisation command and if the outcome of this command was successful.

7.3.1 EEP TRANSACTION NUMBER

A Transaction Number shall be present in the EEP. This Transaction Number is incremented internally for each transaction and must assure that no signature is generated twice over the same data elements.

After personalisation the Transaction Number shall be initialised. If not initialised or corrupted the EEP initialisation command will be aborted and an appropriate error code will be returned by the EEP. If the Transaction Number has reached its maximum, the EEP will give the appropriate error code as a response to commands.

7.3.2 UNIQUENESS OF MAC AND SIGNATURE GENERATION

In order to prevent replay attacks, it is very important that the EEP (and equally the PSAM and the LSAM) shall never generate any MAC or signature on the same dynamic data more than once. This is assured by including the EEP Transaction Number in the dynamic data for every authentication.

The command control and incrementation of the EEP Transaction Number in every initialisation command ensures that the Transaction Number is different for every instance of authentication.

However, this is not the case in the subsequent debits in an Incremental Purchase Transaction. In an Incremental Purchase Transaction, a single initialisation command is followed by several debit commands. In this case the Total Transaction Amount is part of the dynamic data that will be authenticated. The fact that the EEP does not accept a subsequent debit with amount 0, guarantees that the Total Transaction Amount is always different for the same Transaction Number.

This is also not the case for the Purchase Reversal. In this case however the value of Transaction Indicator is different for the reversal signature **S2-R**.

7.4 PURCHASE CANCELLATION HANDLING

If the consequence of a Purchase Cancellation in an EEP is merely the re-crediting of the applicable balance, the Purse Provider implicitly relies on Trust Assumption **P-TA7**.

Due to malfunction or a compromise of security, the Purchase Device may have failed to modify its internal state conforming to the Purchase Cancellation Transaction. The Purse Provider is able to determine the EEP involved in a unilateral Purchase Cancellation and the transaction amount. This may uniquely identify the transaction if the transaction amount occurs only once.

In general however, the Purse Provider needs to rely on the Purchase Device and the Acquiring Technical Operator not to submit the corresponding Purchase Trace at a later stage.

7.5 EEP LOG

The EEP shall store the Transaction Details of at least the last transaction. The Transaction Details may be retrieved by means of the EEP Inquiry or the Read Record command. Although they have no proof value and are purely there for the information of the Purse Holder, they may be helpful in settling disputes.

7.6 SECURITY CERTIFICATION

To ensure the security requirements outlined in this document, the Purse Scheme Administrators shall have a commonly agreed list of security criteria. He shall put in place a commonly agreed evaluation and certification procedure, which enables the Purse Providers to trust the Acquirers (and vice versa) when using their cards in interoperability.

The Purse Providers themselves have to make sure that their ICCs are evaluated and certified accordingly. This also applies to Acquiring Technical Operators and their PSAMs and to Loading Operators and their LSAMs and/or PIN pads.

8. PURCHASE DEVICE ISSUES

8.1 NEED FOR A PSAM

A PSAM is required in the Purchase Device for Purchase Device Authentication, for managing the transaction counter of the Purchase Device, for verifying certificates and for **S5** generation. The PSAM contains the PSAM Private Key and has the functionality to generate the required digital signatures.

8.2 RECOVERY PROCEDURES

The accidental interruption of a transaction cannot be prevented. Typical causes are premature ICC withdrawal and interruption of power supply.

In a transaction, the Purchase Device sends several commands to the EEP. If the interruption takes place between commands, the status of the EEP is known. If the interruption takes place during the processing of a command by the ICC, the status of the EEP is uncertain.

After an interruption, the cause of the problem may be removed, (i.e. the EEP is reinserted or the plug is reconnected). Lost information on the EEP status may be recovered by means of retrieving the previous signature. Depending on the command that was interrupted, the status returned by the EEP and the decision of the Acceptor and/or card holder, the Purchase Device may be instructed to initiate a new transaction (if no debit or re-credit has taken place in the EEP) or to complete the transaction, which has been interrupted.

9. LOAD DEVICE ISSUES

9.1 NEED FOR AN LSAM

An LSAM is required for implementing the security functions necessary to support Load against other means of payment, i.e. Load Device/LSAM authentication, transaction counter management and cryptographic functions.

9.2 PIN HANDLING

In the loading of an EEP application, which is linked to an account, cardholder PIN verification is required. Load Devices shall have a secure PIN pad [EBS105].

PIN verification methods conforming to this standard are:

1. **EMV On-line PIN verification:** the PIN pad shall encipher the PIN upon entry for transmission to the Purse Provider. This shall conform to [ISO 9564-1].
2. **EMV Off-line PIN verification:** the PIN is submitted to the ICC that compares it to a reference value. The PIN may be submitted to the EEP either:
    - In cleartext: the PIN is not enciphered prior to submission [EMV'96].
    - Enciphered: the PIN is enciphered prior to submission [EMV'96]. A data element indicates if a PIN certificate is present.

A data element gives the preferred verification methods of the Purse Provider and also indicates whether the PIN used for off-line PIN verification shall be enciphered or in plaintext when presented to the card.

ANNEX A (INFORMATIVE): COLLECTION AND SETTLEMENT

In the Collection process, the Purchase Traces are sent from the Purchase Device to the Acquiring Technical Operator. In the Settlement process the Acquiring Technical Operator sends them to the Purse Provider.

Via the Settlement process, the Purse Provider receives a Purchase Trace for every Purchase Transaction conducted by any of his Purses. The Purchase Trace includes the MAC **S6**. The Purse Provider verifies the validity of this MAC. If correct, the Purse Provider shall transfer the Transaction Amount to the Acquiring Bank that is linked to the Acquiring Technical Operator indicated in the Purchase Trace. The Acquiring Bank shall transfer the corresponding amount to the account of the Acceptor associated with the PSAM ID in the Purchase Trace.

If the MAC is not correct, the Purse Provider shall inform the Acquiring Technical Operator based on business agreements.

A Purchase Trace only represents the flow of funds towards a particular Acceptor, associated with a particular Acquiring Technical Operator.

It is the responsibility of the Acquiring Technical Operator/Acquiring Bank to ensure the integrity of the Purchase Traces, as the Purse Provider is only obliged to pay if a valid Purchase Trace is presented.

A.1 COLLECTION SECURITY MECHANISMS

Fundamentally, it is the Purse Provider's responsibility not to pay for an individual Purchase Trace more than once. Due to a variety of possible causes, e.g. human and technical errors, implementation bugs or fraud on behalf of the Acquiring Bank, Acquiring Technical Operator or Acceptors, a Purchase Trace may be presented to a Purse Provider more than once.

The Purse Provider may detect double submission by keeping a database of received Purchase Traces. The task of the Purse Provider may be alleviated if the Acquiring Technical Operator implements measures to reduce (or eliminate) the risk of double presentation of Purchase Traces. This section presents mechanisms that may be adopted by the Acquiring Technical Operator to detect:

- the double submission of Purchase Traces;
- the submission of invalid (**S6**) Purchase Traces.

3. The PSAM shall behave in such a way that for every transaction, the PSAM Transaction Number is incremented.
4. The integrity of the Purchase Traces may be protected by a MAC (**S5**). PSAMs that support Purchase Cancellation and/or Purchase Reversal, shall be capable of generating MACs (**S5**). These PSAMs shall generate and transmit a MAC (**S5**) for every individual Purchase Trace.
5. All Purchase Traces are sent to the Acquiring Technical Operator, including those corresponding to cancelled, partial or refused transactions. The unique PSAM Transaction Number is part of the Purchase Trace. If the same PSAM Transaction Number is used for domestic transactions and these transactions are truncated in the Purchase Device, the PSAM Transaction Numbers in the Collection file are not consecutive, but still shall be strictly increasing. In this way it is easy for the Acquiring Technical Operator to verify that transaction data is only processed once.

6. To detect the duplication of Purchase Traces between different collections for a Purchase Device, the Acquiring Technical Operator may keep a database of the last PSAM Transaction Numbers of the received Purchase Traces for all Purchase Devices.
7. At intervals, the Purchase Traces that have been collected by the Acquiring Technical Operator shall be sorted and sent to the respective Purse Providers. The Acquiring Technical Operator may prevent duplication of Purchase Traces in his Host (or minimise the risk) by using a suitable database tool.
8. When a batch of Purchase Traces is submitted to a Purse Provider, it may be stored separately and archived until a signed acknowledgement is received from the Purse Provider. At that moment, the batch shall be marked as submitted, so that the Acquiring Technical Operator will not submit it again.

A.2 SETTLEMENT SECURITY MECHANISMS

Purchase Traces shall be submitted in such a way that they cannot be repudiated. A suitable key management scheme, an arbitrating third party and Public Key signatures could be used to provide the non-repudiation of Purchase Traces.

This section presents mechanisms supporting non-repudiation of submission and acknowledgement for the settlement process.

After sorting the Purchase Traces per Purse Provider, the Acquiring Technical Operator transmits the Purchase Traces to the Purse Provider.

Upon receipt, the Purse Provider checks the digital signature on the batch of Purchase Traces. If correct, every Purchase Trace is processed in the following way:

- verify the validity by checking **S6**;
- verify whether the Purchase Trace has been submitted before (using a logging database).

After verifying the complete batch, a digitally signed acknowledgement is returned with the result of the verifications. For all valid Purchase Traces, the Acquiring Bank will be paid the amount corresponding to the Electronic Value in the Purchase Trace.

ANNEX B (INFORMATIVE): FRAUD CONTAINMENT SCENARIOS

This annex describes the way in which fraud that affects multiple participants may be detected in the EEP Scheme and how the different participants may react to contain it.

B.1 COMPROMISE OF EEP KEYS AND BLACKLISTS

A compromise of an EEP (or Purse Provider) Private Key allows the fraudulent creation of Electronic Value in the following way.

Knowledge of the Private Key allows the impersonation of an EEP with respect to any Purchase Device.

The result is that the Purchase Device will accept a payment, but the corresponding Purchase Trace is invalid. This will be noticed in the Settlement process and the Purse Provider will not pay the corresponding transaction amounts to the Acquiring Bank.

Although the Purse Provider is responsible for the security of his EEPs, the (initial) victim is the Acquiring Bank. Acquiring Technical Operators, affected by this type of fraud, may detect it by analysing the EEP IDs from the invalid Purchase Traces. If **S3** is available, it is possible to prove to an arbitrating third party that the Private Key of a given EEP has been compromised. In general, **S3** is not stored in a Purchase Device. However, by using a “list of suspect EEPs”, it is possible to selectively store **S3** for those EEPs.

If an EEP Private Key **and** the key used to compute **S6** are known, it is possible to impersonate a genuine EEP accepted by any Purchase Device **and** have a valid Purchase Trace in the Purchase Device.

The fraud will not be detected in the Settlement process, but the Purse Provider will typically notice it in his auditing system. In this case, the Purse Provider is the victim of the fraud. It is not implausible that these security problems may result in the bankruptcy of the affected Purse Provider, in which case Acquiring Banks will not be compensated for transactions conducted by that Purse Provider’s EEPs.

In both cases, the appropriate protection mechanism is the *blacklist* in the Purchase Device containing the Purse Provider ID of the compromised EEP. A Purchase Device should have the capability to support a *blacklist* containing zero or more Purse Provider Identifiers, and possibly for each Purse Provider ID a range or a set of ranges of EEP IDs.

Before each Purchase Transaction, the EEP is checked against the blacklist. If it is identified, the EEP will be refused. If the blacklist mechanism is not supported, the Purchase Device will accept any EEP originating from a Purse Provider certified by the Certification Authority.

It is clearly in the interest of the Acquiring Bank to support blacklists with Purse Provider IDs in his Purchase Devices. The additional support of ranges of EEP IDs per Purse Provider in the blacklists may be seen as a service provided by the Acquiring Technical Operator to Purse Providers whose security is only partially compromised.

If the blacklist mechanism is present, the blacklists in the Purchase Devices shall be updated whenever necessary. This is the full responsibility of the Acquiring Technical Operator. He shall assure that the Purchase Devices verify the authenticity and the data origin of the blacklist updates in such a way that their timeliness is guaranteed. This may be implemented by means of a MAC mechanism, if a PSAM is present in the Purchase Device, or by digital signatures, if no PSAM is available. The timeliness may be guaranteed by a challenge-response mechanism.

B.2 COMPROMISE OF PSAM PRIVATE KEYS

A compromise of PSAM Private Keys has two different consequences:

- Debit of an EEP without the presence of a genuine Purchase Device.
- Fraudulent Purchase Cancellation Transactions.

The first fraud does not allow the creation of Electronic Value. There is no financial motive for such an attack as the fraudster is unable to benefit from the resulting Purchase Traces.

For the EEP there is no realistic way to protect against this threat because the EEP does not support a blacklist.

Additionally, the expiry date in PSAM Public Key Certificates does not limit the usage of the Private Key afterwards, because an EEP does not contain an internal clock.

The second fraud would allow a Purchase Cancellation to be performed in any EEP. The financial benefit is evident.

If the attacker is able to obtain a Private Key from any PSAM able to perform cancellations, he could cancel succesful Purchase Transactions without the control of the PSAM involved in the orginal Purchase Transaction.

To avoid this fraud, it shall be ensured that the same PSAM that performs a Purchase Transaction is the only one allowed to cancel this transaction. Implementation details are outside the scope of this Standard but a possible mechanism would be to verify the PSAM identity by comparing the PSAM ID retrieved from the PSAM certificate verification process in the Purchase Transaction with the same data retrieved from the PSAM certificate verification in the Purchase Cancellation Transaction.

B.3 COMPROMISE OF PURCHASE DEVICE AND ACQUIRING TECHNICAL OPERATOR SECURITY

A compromise of Purchase Device security would allow a Purchase Cancellation to be undone, the duplication of Purchase Traces or the creation of dummy Purchase Traces in the Collection. If the Acquiring Technical Operator does not detect the compromise, he will submit Purchase Traces corresponding to cancelled Transactions, duplicate or counterfeit Purchase Traces to Purse Providers. When a Purse Provider detects the submission of such Purchase Traces, he may advise the Acquiring Technical Operator enabling the latter to identify the defective or defrauded Purchase Device.

ANNEX C (INFORMATIVE): TRUNCATION AND AGGREGATION

Truncation, i.e. the aggregation of transaction amounts in totals may be applied in the Purchase Device or in the Acquiring Technical Operator Host. However, this implies a high degree of trust of the Purse Providers in Acquiring Technical Operator/Acquiring Banks and is based on bilateral agreements.

The Purse Provider may pay certain Acquiring Technical Operators without demanding Purchase Traces based on the degree of trust in the specific Acquiring Technical Operator.

Full auditability by a Purse Provider of his EEPs is only possible if submission of Purchase Traces is mandated.

C.1 TRUNCATION IN THE ACQUIRING TECHNICAL OPERATOR HOST

In this case, the Purse Provider does not receive the Purchase Traces, and is therefore not able to verify whether the claim of the Acquiring Bank is genuine. The Purse Provider may, however, request Purchase Traces concerning specific transactions, according to scheme regulations.

C.2 TRUNCATION IN THE PURCHASE DEVICE

If the Acquiring Bank of the Purchase Device has a bilateral agreement with certain Purse Providers, Purchase Traces corresponding to Purchase Transactions originating from EEPs issued by these Purse Providers do not have to be archived. For these Purse Providers, the Purchase Device shall hold a total for every Purse Provider-Currency combination that has occurred in the received payments.

For security reasons the crediting of the totals shall be under the control of a PSAM. The PSAM shall contain the functionality of certificate and signature verification. In a Purchase Transaction, the credit of the appropriate total shall not be possible before the PSAM has successfully verified the certificate chain and **S3**. In a Purchase Cancellation Transaction, **S2** shall only be generated after the appropriate total has been debited.

In the Collection, the totals are sent from the Purchase Devices to the Acquiring Technical Operator in an authenticated way, e.g. by means of a MAC based on a challenge from the Acquiring Technical Operator. The PSAM shall contain the secret key and the functionality to support this.

ooOOoo

PART 3: TRANSACTION DESCRIPTION

1. SCOPE

This part of the Standard provides the functional description of the following EEP transactions:

- Purchase
- Incremental Purchase
- Purchase Cancellation
- Purchase Reversal
- Load
- Currency Exchange
- Balance Inquiry
- Log Inquiry

2. PRINCIPLES

2.1 BASIC PRINCIPLES

The CEN standard [prEN 1546-2] is the reference used to specify those parts of the transactions involving the EEP application, e.g. EEP initialisation, EEP authentication, terminal/PSAM authentication, debit/credit/recredit of the EEP application.

Only transactions performed in an interoperable environment are described in this document. Proprietary processes are out of the scope of the document.

2.2 TRANSACTIONS

This section describes the transactions supported by this Standard for interoperability purposes.

2.2.1 PURCHASE

2.2.1.1 PURCHASE SINGLE STEP

The Purchase Transaction is a transaction between an EEP and a Purchase Device conducted off-line from the Purse Provider and the Acquiring Technical Operator.

The transaction currency shall be common to the EEP application and the Purchase Device and has to be determined prior to starting the Purchase Transaction.

- In the response to the Initialise EEP for Purchase command, the EEP, based on information received, communicates the authentication method to be used in the Purchase Transaction. Purchase Device Authentication is performed using the signature **S2**. If Purchase Device Authentication fails, the transaction is aborted.
- If the Slot balance is sufficient, the amount is debited.
- A MAC **S3** generated by the EEP using symmetric cryptography guarantees the authenticity of the EEP to the Purchase Device as well as the integrity of **S6** and other relevant transaction data.
- The EEP computes the MAC **S6**, which guarantees the integrity of the Purchase Trace to the Purse Provider, to be sent together with the Purchase Trace to the Purse Provider. The EEP stores the Purchase Trace.
- The Purchase Device stores the Purchase Trace and verifies **S3**. If correct, the Purchase Device signals the Acceptor or vending machine to supply goods/services in return for the debited Electronic Value.
- If the PSAM supports either Purchase Reversal and/or Purchase Cancellation, an additional MAC **S5** is generated over some elements in the Purchase Trace, including the PSAM Transaction Number.

2.2.1.2 INCREMENTAL STEP

This transaction is a Purchase Transaction, the final amount of which is unknown when the transaction is initiated.

Amounts are debited repeatedly from the EEP in relation with events occurring in the

Purchase Device (e.g. Telephone ticks, litres of gasoline).

- When Purchase Device Authentication is required by the EEP, it is performed using signature **S2**. If Purchase Device Authentication fails or if it is not supported by the Purchase Device, the transaction is aborted.
- For each single step:

  - the balance is checked,

  - the EEP is debited,

  - the EEP generates **S6** and **S3** for the accumulated amount,

  - the EEP stores the current status,

  - the Purchase Device verifies the current **S3** and stores the Purchase Trace (including **S6**).

After the transaction has been concluded, the PSAM generates **S5** only once for the total amount of the Purchase Transaction.

2.2.1.3 *PURCHASE REVERSAL*

The Purchase Reversal is considered a part of the current Purchase Transaction. The Purchase Device reverses the Purchase Transaction (last step) that is being conducted in the same Card Session.

The following steps are executed after the EEP returns the **S3** signature:

- After verifying that the EEP has been debited, the Purchase Device sends the reversal MAC **S2-R** to the EEP.
- The EEP verifies **S2-R** and checks the Transaction Details. If correct, it re-credits its EEP Slot Balance with the amount (the last step amount) of the Purchase Transaction.
- The PSAM generates the MAC **S5** as a proof of the total amount that was successfully debited. If a single step Purchase Transaction has been reversed, the total amount (of the Purchase Trace) will be zero. If an Incremental Purchase Transaction has been reversed, the Purchase Device shall store the current and previous step values of **S6** to enable it to calculate the **S5** across the total amount of the successful steps.

2.2.2 PURCHASE CANCELLATION

The purpose of the Purchase Cancellation Transaction is to cancel the last (most recent) successful Purchase Transaction (last step) in the EEP application. The Purchase Transaction to be cancelled shall be present in the Purchase Device log and shall not yet have been transmitted to the Acquiring Technical Operator.

The ability of the PSAM to generate a MAC **S5** is a necessary condition for performing a Purchase Cancellation.

- The EEP generates a MAC **S1** over the data of the transaction to be cancelled.
- The PSAM verifies the MAC and checks that the transaction in the EEP is present in the Purchase Device log and has not yet been sent to the Acquiring Technical Operator. The PSAM increments its transaction number generates a MAC **S2** for recrediting the EEP and provisionally stores the Transaction Details.

- The EEP verifies the MAC , credits the balance and stores the Purchase Cancellation Trace.
- The PSAM stores the EEP response and computes MAC **S5** for the Purchase Cancellation Transaction.

2.2.3 LOAD

The Load Transaction is performed on-line to the Purse Provider.

The payment method used for the loading operation may either be supported by the EEP application (through debiting the associated bank account) or by another application (e.g. an EMV debit/credit application). In the first case the loading operation is called Load against the EEP's associated account. In the second case it is called 'Load against other means of payment'.

The reference to the funding account may reside either in the EEP application or in another application in the same card or in a separate card.

- Depending on the amount and the currency to be loaded,
  - the Load Transaction may be denied (maximum balance exceeded, no slot available).
  - the Load Transaction is accepted and the EEP generates a MAC **S1** over the Transaction Details for an active or an inactive Slot .
- The Load Device sends a request for Load message to the Purse Provider based on the data retrieved from the EEP. In case of Load against other means of payment the LSAM supplies a cryptogram **Sig2** as a guarantee of payment for the Purse Provider.
- The Purse Provider verifies the MAC **S1** and in addition **Sig2** for Load against other means of payment checks the validity of the request (EEP data) and generates a credit message (including **S2**), that is transmitted to the Load Device. This message may include a script envelope to be submitted to the EEP. In Load against other means of payment the Purse Provider also encrypts **S2** for approved transactions.
- The Load Device analyses the message received from the Purse Provider and the LSAM decrypts **S2**, if needed, in case of Load against other means of payment.
- If a script message with a tag 71h is present, the related command(s) are submitted to the EEP for processing.
- The credit EEP for Load command is submitted to the EEP, which verifies **S2**, credits the balance, and stores the Transaction Details. The EEP generates a MAC **S3** and sends it to the Load Device. In the case of unsuccessful Load against other means of payment the EEP additionally generates a MAC **S3'** to provide a proof for the Loading Operator that the Load Transaction failed (proof of non-credit). The Load Device stores the Transaction Details and **S3**. **S3** shall be transmitted to the Purse Provider in case of an unsuccessful Load Transaction.
- If a script message with a tag 72h is present, the related command(s) are submitted to the EEP for processing.

The mechanism for providing information on the script result to the Purse Provider is outside the scope of this Standard.

2.2.4 CURRENCY EXCHANGE

The Currency Exchange Transaction is performed on-line to the Purse Provider. The transaction converts some or all of the currency of an active Slot in an EEP. The conversion is performed under the control of the Purse Provider, who provides the new balances and possibly the new maximum balances of both the source and target Slots.

There are two types of Currency Exchange Transactions:

- Into the same Slot (the source Slot is the same as the target Slot).
- By transferring some or all of the Electronic Value of one Slot to another Slot, either active or inactive (the source Slot is different from the target Slot).

- The EEP generates a MAC **S1**.
- The Load Device sends a request for currency exchange based on the data retrieved from the EEP to the Purse Provider.
- The Purse Provider verifies the MAC **S1** and checks the validity of the request. The Purse Provider generates an update message including the MAC **S2**, the new balance and possibly maximum balance and transmits it. This message may include a script envelope.
- The Load Device analyses the message received from the Purse Provider.
- If a script message with a tag 71h is present, the related command(s) are submitted to the EEP for processing.
- The Currency Exchange command is submitted to the EEP, which verifies **S2**, updates the currency code, the balance and, if applicable, the EEP maximum balance of the appropriate Slot(s) and stores the Transaction Details. The EEP generates a MAC **S3** and sends it to the Load Device. The Load Device stores the Transaction Details and **S3**. **S3** shall be transmitted to the Purse Provider in case of an unsuccessful Currency Exchange Transaction.
- If a script message with a tag 72h is present, the related command(s) are submitted to the EEP for processing.

2.2.5 BALANCE INQUIRY

The Balance Inquiry is performed off-line at the convenience of the Purse Holder in order to display the data related to the active Slots in an EEP (e.g. balance, currency and maximum balance). The EEP Inquiry or Read Record command may be used for this purpose.

2.2.6 LOG INQUIRY

The Log Inquiry is performed off-line at the convenience of the Purse Holder in order to display the information stored by the EEP application relating to the last transaction(s). The EEP Inquiry or Read Record command may be used for this purpose.

ooOOoo