IG112-2
VERSION 0

EUROPEAN COMMITTEE
FOR
BANKING STANDARDS

IMPLEMENTATION GUIDELINE FOR THE INTEROPERABLE FINANCIAL SECTOR ELECTRONIC PURSE

PART 2: DETAILED FUNCTIONAL SPECIFICATION

ECBS

Issued: April 1999

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

TABLE OF CONTENTS

1. SCOPE

This document is the detailed functional specification for the European Electronic Purse (EEP). It is based on the CEN standard for the Inter-sector Electronic Purse [prEN 1546] and the EMV'96 ICC Specification for Payment Systems [EMV'96].

This document conforms to the fixed format option for application profile described in section 6.2.4 of [prEN 1546-3].

The data structures are described in section 4.

Sections 5 and 6 list the set of commands and give a detailed description of each command.

For details about the interface of the card to the external world, please refer to the part I Electromechanical Characteristics, Logical Interface, and Transmission Protocols of reference [EMV'96].

2. APPLICABLE DOCUMENTS

See EBS111 V0.

3. TERMINOLOGY

3.1 DEFINITIONS

See EBS111 V0

3.2 ABBREVIATIONS

See EBS111 V0

3.3 NOTATIONS

3.3.1 BINARY AND HEXADECIMAL NOTATION

- Whenever a value is expressed in binary, it is followed by the letter b. For example the decimal value 13 expressed in binary becomes 1101b.
- A hexadecimal number is followed by the letter h. For example the decimal value 13 expressed in hexadecimal becomes 0Dh.
- A byte B consists of 8 bits b_8 b_7 b_6 b_5 b_4 b_3 b_2 b_1: b_8 is the most significant bit and b_1 the least significant bit.
- A string of bytes consists of n concatenated bytes B_nB_{n-1} ... B_2B_1: B_n is the most significant byte and B_1 the least significant byte.
- The transfer order of bytes (or bits in bytes) is as specified by Part I-3.2 and Part I-4.3 of [EMV'96].

3.3.2 OPERATORS, FUNCTIONS, ABBREVIATIONS, ETC.

- The abbreviation 'CURR' covers both the currency code and the currency exponent.

4. EEP DATA STRUCTURES

These data structures, grouped in several records, contain data elements necessary for the EEP application to perform the transactions described in EBS111 V0.

4.1 EEP INFORMATION DATA

The EEP information data is retrieved by means of the Read Record command. The first entry in the Application Data Locator (ADL) data element points to this record. The information about the EEP application contains the following fixed data elements and parameters.

Description	Data Element	Length (bytes)
Purse Provider Identifier	ID_{PP}	4
EEP Identifier	ID_{EEP}	6
Expiry date	$DEXP_{EEP}$	4
Activation date	$DACT_{EEP}$	4
Deactivation date	$DDEA_{EEP}$	4
Purse Provider Country Code	$CNTY_{PP}$	2
Home Currency	HC_{PP}	3
Home Currency Label	HCL_{PP}	3
Purse Provider Certification Authority Public Key Version	$VK_{CA,PP}$	1
Acquirer Certification Authority Public Key Version	$VK_{CA,ACQ}$	1
Cardholder Verification Method List	CVML	3
PAN length	PANL	1
Application Primary Account Number (optional)	PAN	Var. up to 10
Discretionary data	DD_{EEP}	0 to 16

4.2 EEP AUTHENTICATION PUBLIC KEY DATA ELEMENTS

These data elements are required for EEP Dynamic Data Authentication and are retrieved by means of the Read Record command as constructed data objects (70 template).

The ADL points to the key related information. The following data elements shall be provided for the Purse Provider Public Key Certificate and the EEP Public Key Certificate.

Description	Data Element	Length (bytes)
Purse Provider Public Key Certificate	PKC_{PP}	$LPKM_{CA, PP}$
Purse Provider Public Key Exponent	PKE_{PP}	1 or 3
Purse Provider Public Key Remainder	PKR_{PP}	0 or $LPKR_{PP}$
EEP Public Key Certificate	PKC_{EEP}	$LPKM_{PP}$
EEP Public Key Exponent	PKE_{EEP}	1 or 3
EEP Public Key Remainder	PKR_{EEP}	0 or $LPKR_{EEP}$

4.3 EEP SLOT DATA

This structure contains information about the balance, currency and maximum balance data elements of a specific Slot.

The Slot information related to the last transaction performed by the EEP (Purchase, Load or Currency Exchange Transaction), may be available in the response to the Select command.

Depending on the coding in the Application Profile data element (AP_{EEP}) information on other Slots may be retrieved by means of the EEP Inquiry command or the Read Record command.

When the Read Record command is used, the ADL is used to point to the location of the Slot data. There is one record for every currency supported by the EEP. The record is structured as follows:

Description	Data Element	Length (bytes)
Currency Code	$CURRC_{EEP}$	2
Currency Exponent	$CURRE_{EEP}$	1
EEP Balance	BAL_{EEP}	4
Maximum Balance	$BALMAX_{EEP}$	4

4.4 EEP LOG DATA

The Load, Purchase, Purchase Cancellation and Currency Exchange Transactions shall be considered transactions to be stored. At least the last transaction shall be stored. Recording only successful or both successful and unsuccessful operations is a Purse Provider option.

The standard specifies two mechanisms for accessing information on stored transactions: the EEP Inquiry command and the Read Record command. The coding of the Application Profile data element (AP_{EEP}) indicates which implementation(s) is supported by the EEP. The terminal shall have the capability to handle both mechanisms, if it supports Log Inquiry.

In order to facilitate display and printing functions at terminal level, the way in which the data elements of the log data will be presented in the response to the different inquiries has been harmonised. The sequence is as described below.

Only those data elements marked with ‘x’ are transmitted in the response message.

Description	Data Element	Length	LOAD	PURCHASE/ PURCHASE CANCELLATION	CURRENCY EXCHANGE
Transaction type	TRT_{EEP}	1	x	x	x
Transaction Number	NT_{EEP}	2	x	x	x
Transaction Completion Code	CC_{TRX}/ CC_{EEP}	2	x	x	x
Date/time (YYYYMMDDHHMM)	$DTHR_{LDA}$/ $DTHR_{PDA}$	6	x	x	x
EEP balance of the target Slot - new EEP balance	$BAL_{EEPtarget}$	4	x	x	x
Loading Operator Identifier/ Acquirer Identifier	ID_{LO}/ID_{ACQ}	6	x	x	x
PPSAM Identifier /PSAM Identifier	ID_{PPSAM}/ ID_{PSAM}	4	x	x	x

Random Number/ PSAM Transaction Number	R_{PPSAM}/ NT_{PSAM}	4	x	x	x
Amount received from LDA/ Total amount of the transaction	M_{LDA} / $MTOT_{EEP}$	4	x	x	x
Currency received from LDA/PDA/Source Slot	$CURR_{LDA/PDA/EEP}$	3	x	x	x
Identifier of LDA	ID_{LDA}	4	x	-	x
Maximum Balance of the EEP (target Slot)	$BALMAX_{EEPtarget}$	4	x	-	x
Balance (old) of the EEP (target Slot)	$BAL_{EEPtarget}$	4	-	-	x
Balance of the EEP (source Slot)	$BAL_{EEPsource}$	4	-	-	x
Maximum balance of the EEP (source Slot)	$BALMAX_{EEPsource}$	4	-	-	x
Currency Code (target Slot)	$CURR_{EEPtarget}$	3	-	-	x
Latest amount received from the PDA	M_{PDA}	4	-	x	-
Transaction Indicator	TI	1	-	x	-
Authentication Method	AM_{EEP}	1	-	x	-

4.4.1 ACCESS USING THE EEP INQUIRY COMMAND

When Log Inquiry is implemented by means of the EEP Inquiry command, the standard does not mandate any structure. The location of the stored information in the EEP is completely transparent to the terminal.

4.4.2 ACCESS USING THE READ RECORD COMMAND

When Log Inquiry is implemented by means of the Read Record command, the standard mandates that the information be stored as described above.

The ADL points to the following records:

- Purchase and Purchase Cancellation log file
- Load log file
- Currency Exchange log file.

5. GENERAL PURPOSE COMMANDS

The following sections define the subset of EMV'96 commands that shall be supported by the EEP application. They further define the minimum set of options that shall be supported.

5.1 SELECT

5.1.1 DEFINITION AND SCOPE

The EEP application will be selected according to [EMV'96]. EEP support for the selection of a DF file using only a partial DF name is recommended.

5.1.2 COMMAND MESSAGE

Command message for Select

Field	Value	Length (bytes)
CLA	00h	1
INS	A4h	1
P1	04h	1
P2	Selection Options	1
Lc	05h - 10h	1
Data	File name	5-16
Le	00h	1

P2 Selection Options

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	0	0	First or only occurrence
-	-	-	-	-	-	1	0	Next occurrence
-	-	-	-	-	-	-	-	RFU

5.1.3 RESPONSE MESSAGE

Response to Select

Tag h	Length h	Value	M/O
6F	var.	FCI Template	M
84	05-10	AID$_{EEP}$ (Application Identifier of the EEP)	M
A5	var.	FCI Proprietary Template	M
87	01	API (Application priority indicator)	O
5F2D	02-08	LANG (Language preference)	O
BF0C	var.	FCI Issuer Discretionary Data	M

DF10	n x 4	ADL (Application Data Locator)	M
C2	02	AP_{EEP} (Application Profile)	M
DF09	01	SDI (Spontaneous Display Indicator)	O
DF04	11	$SLOT_{EEP}$ (EEP Slot Data)	O
	02	Status bytes (SW1-SW2)	M

5.1.4 STATUS CONDITIONS

See [EMV'96]

5.2 READ RECORD

5.2.1 DEFINITION AND SCOPE

The command "Read Record" reads a record in a linear or cyclic file.

5.2.2 COMMAND MESSAGE

Command message for Read Record

Field	Value	Length (bytes)
CLA	00h	1
INS	B2h	1
P1	Record number	1
P2	Reference Control Parameter (See table)	1
Le	00h	1

Reference control parameter of the command message

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	-	-	-	SFI
-	-	-	-	-	1	0	0	P1 is a record number

5.2.3 RESPONSE MESSAGE

The data field of the response message of any successful Read Record command contains the data read.

If the record contains TLV encoded data it shall be coded as shown below

70h	Length	Record Template

Otherwise, it shall be coded as

50h	Length	Data

5.2.4 STATUS CONDITIONS

SW1	SW2	Meaning
64h	00h	State of non-volatile memory unchanged
62h	81h	Part of returned data may be corrupted.
67h	00h	Wrong length (Le field not present)
69h	81h	Command incompatible with file organisation
6Ah	81h	Function not supported
6Ah	82h	File not found
6Ah	83h	Record not found

5.3 GET CHALLENGE

The Get Challenge command is used in the case of off-line encrypted PIN. An ADL entry indicates whether an off-line PIN certificate is present in the EEP.

See [EMV'96].

5.4 VERIFY

5.4.1 DEFINITION AND SCOPE

The Verify command is processed in the EEP after analysing the Cardholder Verification Method List (CVML), which is retrieved from the EEP Information Data.

The Verify command initiates in the EEP the comparison of the Transaction PIN Data sent in the data field of the command with the reference PIN data associated with the application. The manner in which the comparison is performed is proprietary to the application in the EEP.

The Verify command applies when the Cardholder Verification Method (CVM) chosen from the CVM List is an off-line PIN. The processing of the Verify command in the EEP should know how to find the PIN data unambiguously.

5.4.2 COMMAND MESSAGE

Command message for Verify

Field	Value	Length (bytes)
CLA	00h	1
INS	20h	1
P1	00h	1
P2	Qualifier of the reference data (see Table)	1
Lc	Var.	1
Data	Transaction PIN Data	8 or LPKM_{EEP}

Le	00h	1

Verify Command Qualifier of Reference Data (P2)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	As defined in [ISO7816-4]
1	0	0	0	0	0	0	0	Plaintext PIN, format as defined below
1	0	0	0	0	x	x	x	RFU
1	0	0	0	1	0	0	0	Enciphered PIN, format as defined in [EMV'96]
1	0	0	0	1	0	x	x	RFU
1	0	0	0	1	1	x	x	Reserved for the individual payment systems
1	0	0	1	x	x	x	x	Reserved for the Purse Provider

The plaintext offline PIN block shall be formatted as follows:

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

where

	Name	Value
C	Control field	2 coded as a 4-bit binary field (0010b)
N	PIN length	From 4 to 12 coded as a 4-bit binary field (0100b to 1100b)
P	PIN digit	From 4 to 12 coded as a 4-bit binary field (0000b to 1001b)
P/F	PIN/Filler	Determined by PIN length
F	Filler	1111b

5.4.3 RESPONSE MESSAGE

The data field of the response message is not present.

5.4.4 STATUS CONDITIONS

SW1	SW2	Meaning
63h	Cx	Verification failed, 'x' indicates the number of further

		retries still possible.
64h	00h	State of non-volatile memory unchanged
69h	83h	Authentication method (PIN) blocked
69h	84h	Referenced data invalidated
6Ah	86h	Incorrect parameters P1 P2
6Ah	88h	Referenced data not found

5.4.5 CONDITIONAL USAGE AND SECURITY

When for the currently selected application the comparison between the Transaction PIN Data and the reference PIN data performed by the Verify command fails, the EEP shall return SW2 = ‘Cx’, where ‘x’ represents the number of retries still possible.

When the card returns ‘C0’, no more retries are left, and the CVM shall be blocked. Any subsequent Verify command applied in the context of that application shall then fail with SW1 SW2 = ‘6983’.

6. EEP SPECIFIC COMMANDS

6.1 GENERAL OBSERVATIONS

Full details about signature computation are given in [EBS 111 V0].

The following sections contain information on the status conditions, the conditional usage and security and the command processing that apply and may be included in the response messages to all commands.

Every time the EEP application is selected, the value of TRT_{EEP} is set to the default value.

6.1.1 GENERAL STATUS CONDITIONS

General Status Conditions

SW1	SW2	Meaning
90h	00h	Normal processing, data may be present in the response field
61h	xxh	For T=1 in [EMV'96]. Normal processing. Length of returned data is xx.
65h	81h	Memory failure
67h	00h	Lc incorrect
69h	85h	Conditions of use not satisfied (EEP not selected)
6Ah	86h	Incorrect parameters P1-P2, no further information
6Ah	87h	Lc inconsistent with P1-P2
6Dh	00h	Instruction not allowed or incompatible with class
6Eh	00h	Class not allowed
91h	01h	EEP is not active
91h	06h	EEP has been deactivated

6.1.2 CONDITIONAL USAGE AND SECURITY

The command is rejected if the current DF does not contain an EEP application.

The command is rejected if the length of Lc is incorrect or inconsistent, if the parameters P1 and P2 are invalid, if the EEP is not active or if it has been deactivated.

A memory failure error will occur if one of the internal data elements necessary for the command execution is absent or invalid. The data set includes all the application data elements checked during the command processing and all the data elements used in signature computation that are returned in the response.

6.1.3 COMMAND PROCESSING

The following verification steps will take place at the beginning of every command. The SW1 and SW2 listed with the verification steps are returned in case the verification fails. If the validation checks have been performed successfully, the SW1/SW2 value will be 90h 00h or 61h xxh (normal processing). Otherwise, no additional data will be returned by the EEP.

Verification	SW1	SW2
The current DF shall contain an EEP application	69h	85h
Check length of Lc	67h	00h
The necessary parameters shall be valid	6Ah	86h
The EEP shall be active (Activation Date $DACT_{EEP} \neq 0$)	91h	01h
The EEP shall not have been deactivated (Deactivation Date $DDEA_{EEP} = 0$)	91h	06h
The data necessary for the command shall be valid: increase NT, update the transaction data (balance, log record).	65h	81h

6.2 INITIALISE EEP FOR LOAD

6.2.1 DEFINITION AND SCOPE

The “Initialise EEP for Load” command initiates a Load Transaction.

The EEP Transaction Number (NT_{EEP}) is incremented by 1.

S1 is returned to the PPSAM via the Load Device for verification.

6.2.2 COMMAND MESSAGE

Command message for Initialise EEP for Load

Field	Value	Length (bytes)
CLA	90h	1
INS	50h	1
P1	00h	1
P2	00h, 80h	1
Lc	1Bh + length of DD_{LDA}.	1
M_{LDA}	Amount received from the Load Device	4
$CURR_{LDA}$	Currency received from the Load Device	3
ID_{LDA}/ID_{LSAM}	Identifier for an LDA/LSAM	4
R_{LDA}	Challenge	4
$DTHR_{LDA}$	Date/time of Load operation	6
ID_{LO}	Loading Operator Identifier	6
DD_{LDA}	Discretionary Data	0 to 16
Le	00h	1

Usage and coding of P2

P2	Description
00h	Load against the EEP's associated account
80h	Load against other means of payment

6.2.3 RESPONSE MESSAGE

Response to Initialise EEP for Load

Field	Value	Length (bytes)
$ALGL_{EEP}$	Algorithm used by the EEP for Load	1
BAL_{EEP}	EEP Balance	4
NT_{EEP}	EEP Transaction Number	2
VK_{EEP}	EEP Key Version	1
SST	Slot Status	1
PVS	PIN Verification Status	1
S1	MAC of the EEP	8
DD_{EEP}	Discretionary Data	0 to 16
SW1-SW2	Status Bytes	2

6.2.4 STATUS CONDITIONS

Status Conditions for Initialise EEP for Load

SW1	SW2	Meaning
91h	02h	EEP Transaction Number has reached its limit
94h	01h	Currency error
94h	02h	Amount is too high for credit.
94h	06h	No inactive Slot available

6.2.5 CONDITIONAL USAGE AND SECURITY

The command is rejected if the currency code received from the Load Device does not exist in the EEP.

The command is rejected if there is no inactive Slot in the EEP.

The command is rejected if the amount received from the Load Device is too high to be loaded.

The command is aborted if the Transaction Number's limit has been reached.

If the command is successful, TRT_{EEP} is set to 00001111b otherwise it is set to 00001110b.

6.2.6 COMMAND PROCESSING

Verification	SW1	SW2
Verify NT_{EEP} has not reached its limit	91h	02h
Check if the currency is present (Verify $CURR_{LDA}=CURR_{EEP}$)	94h	01h
Check for the balance (Verify $BAL_{EEP}+M_{LDA}\leq BALMAX_{EEP}$[1])	94h	02h
Check if an inactive Slot is available	94h	06h

6.3 INITIALISE EEP FOR PURCHASE

6.3.1 DEFINITION AND SCOPE

The “Initialise EEP for Purchase” command initiates a Purchase Transaction.

A 4-byte variable denoted $MTOT_{EEP}$ is initialised to zero in RAM memory. At each step of the Purchase Transaction, this variable will be increased with the amount received from the Purchase Device and stored. Moreover, it will be used as a diversification element for the signatures S2 and S3.

The EEP Transaction Number (NT_{EEP}) is incremented by 1.

6.3.2 COMMAND MESSAGE

Command message for Initialise EEP for Purchase

Field	Value	Length (bytes)
CLA	90h	1
INS	50h	1
P1	01h	1
P2	00h	1
Lc	0Fh + length of DD_{PDA}	1
$CURR_{PDA}$	EEP Currency to be used	3
ALG_{PDA}	Cryptographic algorithm supported for purchase	1
AM_{PDA}	Purchase Device Authentication Method	1
$MEST_{PDA}$	Estimated maximum transaction amount	4
$DTHR_{PDA}$	Date/time of Purchase Device	6
DD_{PDA}	Discretionary Data	0 to 16
Le	00h	1

[1] If the sum of the balance and the amount exceeds FFFFFFFFh, the same error “94 02h” will be returned to the terminal.

6.3.3 RESPONSE MESSAGE

Response to Initialise EEP for Purchase

Field	Value	Length (bytes)
$ALGP_{EEP}$	Algorithm used by the EEP for Purchase	1
BAL_{EEP}	EEP Slot Balance	4
$CURR_{EEP}$	EEP Currency	3
AM_{EEP}	EEP Authentication method	1
NT_{EEP}	EEP Transaction Number	2
$PKSER_{PP}$	Serial number of the Purse Provider certificate	3
$PKSER_{ACQ}$	Serial number of the Acquirer certificate	3
DD_{EEP}	Discretionary Data	0 to 16
SW1-SW2	Status Bytes	2

6.3.4 STATUS CONDITIONS

Status Conditions for Initialise EEP for Purchase

SW1	SW2	Meaning
91h	02h	EEP Transaction Number has reached its limit
94h	01h	Currency error
94h	05h	Authentication method not supported

6.3.5 CONDITIONAL USAGE AND SECURITY

The command is aborted if the Transaction Number’s limit has been reached.

The command is rejected if the currency requested is not present.

The command is aborted if the Purchase Device does not offer an authentication method required by the EEP.

If the command is successful, TRT_{EEP} is set to 00101111b otherwise it is set to 00101110b.

6.3.6 COMMAND PROCESSING

Verification	SW1	SW2
Verify NT_{EEP} has not reached its limit	91h	02h
Check whether authentication method acceptable	94h	05h
Check if the currency is present	94h	01h

6.4 INITIALISE EEP FOR PURCHASE CANCELLATION

6.4.1 DEFINITION AND SCOPE

The “Initialise EEP for Purchase Cancellation” command initiates a Purchase Cancellation Transaction.

The EEP Transaction Number (NT_{EEP}) is incremented by 1.

S1 is returned via the Purchase Device to the PSAM for verification.

6.4.2 COMMAND MESSAGE

Command message for Initialise EEP for Purchase Cancellation

Field	Value	Length (bytes)
CLA	90h	1
INS	50h	1
P1	02h	1
P2	00h	1
Lc	06h + Length of DD_{PDA}	1
$DTHR_{PDA}$	Date/time of Purchase Device	6
DD_{PDA}	Discretionary Data	0 to 16
Le	00h	1

6.4.3 RESPONSE MESSAGE

Response to Initialise EEP for Purchase Cancellation

Field	Value	Length (bytes)
$ALGP_{EEP}$	Algorithm used by the EEP	1
S1	Signature of the EEP	$LPKM_{EEP}$
$PKSER_{PP}$	Serial number of the Purse Provider certificate	3
$PKSER_{ACQ}$	Serial number of the Acquirer certificate	3
DD_{EEP}	Discretionary Data	0 to 16
SW1-SW2	Status Bytes	2

6.4.4 STATUS CONDITIONS

Status Conditions for Initialise EEP for Purchase Cancellation

SW1	SW2	Meaning

91h	02h	EEP Transaction Number has reached its limit
94h	09h	Last transaction was not a Purchase
95h	04h	Last Purchase was not successful
95h	05h	Last Purchase has been cancelled

6.4.5 CONDITIONAL USAGE AND SECURITY

The command is aborted if the Transaction Number's limit has been reached.

The command is only accepted if the last transaction was a successful Purchase Transaction., which did not include a reversal.

If the command is successful, TRT_{EEP} is set to 01001111b otherwise it is set to 01001110b.

6.4.6 COMMAND PROCESSING

Verification	SW1	SW2
Verify NT_{EEP} has not reached its limit	91h	02h
The Purchase shall not have been cancelled before (check $TRT_{EEP,log}$)	95h	05h
The last EEP transaction was not a Purchase	94h	09h
The corresponding Purchase was not successful (check $TRT_{EEP,log}$)	95h	04h

6.5 INITIALISE EEP FOR CURRENCY EXCHANGE

6.5.1 DEFINITION AND SCOPE

The "Initialise EEP for Currency Exchange" command initiates a Currency Exchange Transaction.

The EEP Transaction Number (NT_{EEP}) is incremented by 1.

S1 is returned via the Load Device to the PPSAM for verification.

6.5.2 COMMAND MESSAGE

Command message for Initialise EEP for Currency Exchange

Field	Value	Length (bytes)
CLA	90h	1
INS	50h	1
P1	03h	1
P2	00h	1
Lc	1Eh + length of DD_{LDA}	1
$CURR_{LDAsource}$	EEP Currency Source Slot	3

$\text{CURR}_{\text{LDAtarget}}$	EEP Currency Target Slot	3
M_{LDA}	Amount to be exchanged	4
ID_{LDA}	LDA Identifier	4
ID_{LO}	Loading Operator Identifier	6
R_{LDA}	Challenge	4
DTHR_{LDA}	Date/Time of Load Device	6
DD_{LDA}	Discretionary Data	0 to 16
Le	00h	1

6.5.3 RESPONSE MESSAGE

Response to Initialise EEP for Currency Exchange

Field	Value	Length (bytes)
$\text{ALGCE}_{\text{EEP}}$	Algorithm used by the EEP	1
$\text{BAL}_{\text{EEPsource}}$	EEP Source Slot Balance	4
$\text{BALMAX}_{\text{EEPsource}}$	EEP Source Slot Maximum Balance	4
$\text{BAL}_{\text{EEPtarget}}$	EEP Target Slot Balance	4
$\text{CURR}_{\text{EEPtarget}}$	EEP Currency	3
$\text{BALMAX}_{\text{EEPtarget}}$	EEP Target Slot Maximum Balance	4
NT_{EEP}	EEP Transaction Number	2
VK_{EEP}	EEP Key Version	1
SST	Slot Status	1
S1	MAC of the EEP	8
DD_{EEP}	Discretionary Data	0 to 16
SW1-SW2	Status Bytes	2

The command message (6.5.2) contains the currencies, which have been requested by the Purse Holder:

- $\text{CURR}_{\text{LDAsource}}$: the currency to be converted
- $\text{CURR}_{\text{LDAtarget}}$: the currency into which $\text{CURR}_{\text{LDAsource}}$ will be converted.

The response message provides the actual information about the currencies contained within the EEP Slots and will indicate into which Slot the requested currency has to be transferred:

The data element $\text{CURR}_{\text{EEPtarget}}$ will be set to the value as indicated below depending on the availability of a target Slot:

a) If $\text{CURR}_{\text{EEPtarget}} = \text{CURR}_{\text{LDAtarget}}$ the EEP already contains a Slot with the target currency. The required value from the source Slot will be converted, the source Slot decremented and the target Slot incremented.

b) If $CURR_{EEPtarget}$ = $CURR_{LDAsource}$ the target currency does not exist.

- If all of the source currency is to be exchanged, the value in the source Slot will be replaced by the corresponding value in the target currency. As a consequence, the balances of the source Slot and of the target Slot will be the same as they are one and the same Slot.
- If part of the source currency is to be exchanged, an inactive Slot, if available (SST), will be activated.

6.5.4 STATUS CONDITIONS

Status Conditions for Initialise EEP for Currency Exchange

SW1	SW2	Meaning
91h	02h	EEP Transaction Number has reached its limit
94h	20h	Source currency does not exist
94h	02h	Amount too high
94h	06h	No inactive Slot available

6.5.5 CONDITIONAL USAGE AND SECURITY

The command is aborted if the Transaction Number’s limit has been reached.

The command is rejected if the source currency is not present.

The command is rejected if the amount to be exchanged is greater than the balance of the source Slot.

The command is rejected if there is no inactive Slot available.

If the command is successful, TRT_{EEP} is set to 01101111b otherwise it is set to 01101110b.

6.5.6 COMMAND PROCESSING

Verification	SW1	SW2
Verify source currency	94h	20h
Check amount to be converted is not greater than source Slot balance	94h	02h
Check if an inactive Slot is available	94h	06h
Verify NT_{EEP} has not reached its limit	91h	02h

6.6 CREDIT EEP FOR LOAD

6.6.1 DEFINITION AND SCOPE

The “Credit EEP for Load” command increases the actual balance of the EEP by the amount received from the Load Device.

For P2 = 00h, the signature S2 received from the Purse Provider is verified by the card. The outcome of this verification will result in one of the following situations:

- The balance is increased with the amount received in the previous Initialise EEP for Load command.
- If the target currency is not available, an inactive Slot is activated. In this case $CURR_{EEPtarget}$ = $CURR_{LDA}$ and $BAL_{EEPtarget}$ = M_{LDA}. Both $CURR_{LDA}$ and M_{LDA} were sent in the Initialise EEP for Load command.
- If $DDEA_{EEP}$ is not zero, the EEP application is deactivated.

If the balance is increased, the log record shall be updated. The content of such a record is defined in section 4.4.

The EEP Slot balance and the log record are updated in non-volatile memory in an indivisible operation.

For P2=01h (Load was authorised by the Purse Provider but not by the Funding Bank), the balance shall not be incremented but S3 shall be generated. S2 may be correct but shall not be checked by the EEP.

A signature S3 is computed and returned to the Load Device.

6.6.2 COMMAND MESSAGE

Command message for Credit EEP for Load

Field	Value	Length (bytes)
CLA	90h	1
INS	52h	1
P1	00h	1
P2	00h - 01h	1
Lc	18h + length of DD_{PPSAM}	1
S2	MAC computed by the PPSAM	8
ID_{PPSAM}	Identifier for a PPSAM	4
R_{PPSAM}	Challenge	4
$BALMAX_{EEP}$	Maximum balance of the Target Slot	4
$DDEA_{EEP}$	Deactivation date of the EEP	4
DD_{PPSAM}	Discretionary Data	0 to 16
Le	00h	1

In Load against other means of payment, the Loading Operator requires a valid S2 from the Purse Provider and a positive authorisation response from the Funding Bank to load the

Electronic Value onto the EEP application.

In case the Funding Bank does not send a positive authorisation response, the balance shall not be incremented. Nevertheless the EEP application will generate S3 to prove to the Purse Provider that the Electronic Value was not loaded.

Usage and coding of P2

P2	Description
00h	Normal processing
01h	Balance shall not be incremented, S3 shall be generated.

6.6.3 RESPONSE MESSAGE

Response to Credit EEP for Load against the EEP's associated account

Field	Value	Length (bytes)
CC_{TRX}	Transaction Completion Code	2
BAL_{EEP}	Actual Slot Balance	4
S3	MAC computed by the card	8
DD_{EEP}	Discretionary Data	0 to 16
SW1-SW2	Status bytes	2

Response to Credit EEP for Load against other means of payment

Field	Value	Length (bytes)
CC_{TRX}	Transaction Completion Code	2
BAL_{EEP}	Actual Slot Balance	4
S3	MAC computed by the card	8
S3'	MAC computed by the card (proof of no transaction)	8
DD_{EEP}	Discretionary Data	0 to 16
SW1-SW2	Status bytes	2

6.6.4 STATUS CONDITIONS

So that the EEP can return the S3, the command-specific status conditions are returned in CC_{TRX} and SW1 SW2 shall be 90h 00h in these cases.

6.6.5 CONDITIONAL USAGE AND SECURITY

If the transaction is not completed successfully, the EEP balance shall be restored and the log record updated as a Purse Provider option.

If the command is successful, TRT_{EEP} is set to 00000111b otherwise it is set to 00000110b.

6.6.6 COMMAND PROCESSING

The Transaction Completion Code (CC_{TRX}) provides the status conditions for proof of transaction, proof of no transaction and EEP deactivation. Additional checks in the case of proof of no transaction have been defined as follows:

- Verify if TRT_{EEP} allows “Credit EEP for Load”. The command is rejected if TRT_{EEP} value is different from 00001111b. (P2=00h, 01h).
- Verify if P2=01h. The Load was not performed because funds authorisation was not successful.
- Verify if P2=00h and verify MAC S2. The command is rejected if P2=00h and S2 is not correct.

6.7 DEBIT EEP FOR PURCHASE

6.7.1 DEFINITION AND SCOPE

The “Debit EEP for Purchase” command (first and subsequent steps) decreases the actual balance of the EEP with the amount received from the Purchase Device.

The signature S2 received from the Purchase Device is verified by the card, according to the authentication method (AM_{EEP}, see below), then the balance is decreased by the amount received from the Purchase Device.

If the PSAM supports Purchase Reversal and/or Purchase Cancellation, the signature S5 shall always be appended to the Purchase Trace.

If the “First Debit” is successful, a new record shall be created. However in case of a successful “Subsequent Debit”, the content of the current record is updated. The content of such a record is defined in section 4.4.

The Slot balance and the log record are updated in non-volatile memory in an indivisible operation.

If the transaction is successful, the signatures S3 and S6 are computed and returned to the Purchase Device. S3 includes the total amount of the Purchase $MTOT_{EEP}$ (already increased with the amount of the actual step).

Authentication Method (AM_{EEP})

Single authentication means S2 is not provided.

Mutual authentication means S2 is verified during every step.

Dual authentication means S2 is only generated, transmitted and verified during the first step.

6.7.2 COMMAND MESSAGE

Command message for Debit EEP for Purchase (First Step)

Field	Value	Length (bytes)
CLA	90h	1
INS	54h	1

P1	00h (first step)	1
P2	00h, 01h	1
Lc	15h (00h)* + S2 length + length DD_{PDA}	1
ID_{PSAM}	PSAM Identifier.	4 (0)*
NT_{PSAM}	PSAM Transaction Number.	4 (0)*
M_{PDA}	Amount received from the Purchase Device	4 (0)*
$CURR_{PDA}$	Currency received from the Purchase Device	3 (0)*
ID_{ACQ}	Acquirer Identifier	6 (0)*
S2	Signature	0 or $LPKM_{PSAM}$
DD_{PDA}	Discretionary Data	0 to 16
Le	00h	1

* If P2=01h, S2 is not provided and all these data elements have to be sent in cleartext.

Usage and coding of P2

P2	Description
00h	Normal processing
01h	Single authentication (S2 is not provided)

Command message for Debit EEP for Purchase (Subsequent Steps)

Field	Value	Length (bytes)
CLA	90h	1
INS	54h	1
P1	01h (subsequent steps)	1
P2	00h	1
Lc	07h + S2 length	1
M_{PDA}	Amount received from the Purchase Device	4
$CURR_{PDA}$	Currency received from the Purchase Device	3
S2	Signature	0 or $LPKM_{PSAM}$
Le	00h	1

6.7.3 RESPONSE MESSAGE

Response to Debit EEP for Purchase

Field	Value	Length (bytes)

S3	Signature computed by the card [1]	$LPKM_{EEP}$
DD_{EEP}	Discretionary Data	0 to 16
SW1-SW2	Status bytes	2

[1] The MAC S6 is recovered from the signature S3.

If the transaction is unsuccessful, only SW1-SW2 are returned by the EEP application.

6.7.4 STATUS CONDITIONS

Status Conditions for Debit EEP for Purchase

SW1	SW2	Meaning
93h	01h	Missing public key.
93h	02h	Invalid signature
94h	01h	Currency error
94h	03h	Amount is too high for debit.
94h	04h	Value out of range (Amount zero in incremental purchase)
94h	05h	Authentication method not supported
95h	01h	Signature is missing.
95h	80h	Command out of sequence (purchase (first step)/subsequent step – not allowed).

6.7.5 CONDITIONAL USAGE AND SECURITY

The command is rejected if TRT_{EEP} is different from 00101111b in the case of P1=00h.

In case P1=01h, the command is rejected if TRT_{EEP} is different from 00100111b for the first step or if TRT_{EEP} is different from 00100011b for the further subsequent steps.

The command is rejected if the currency code received from the Purchase Device is different from the currency code received in the initialisation command.

The command is rejected if the amount received from the Purchase Device is higher than the actual Slot balance or zero in any subsequent incremental Purchase step.

The command is rejected, if the EEP requested PSAM authentication for this purchase (step) and no S2 is provided by the PSAM or no Public Key certificate was provided to the EEP.

If the transaction is not completed successfully, the EEP balance shall not be affected.

The value of TRT_{EEP} is set according to the following table.

	P1=00h	P1=01h
Successful	00100111b	00100011b
Unsuccessful	00100110b	00100010b

6.7.6 COMMAND PROCESSING

Verification	SW1	SW2
The EEP status shall allow “First Debit EEP”[1]	95h	80h
Check additional authentication method criteria	94h	05h
Check for the currency (Verify $CURR_{PDA}$=$CURR_{PDA}$ init command)	94h	01h
Check balance (Verify $BAL_{EEP} \geq M_{PDA}$)	94h	03h
Check $M_{PDA} > 0$ if subsequent step	94h	04h
Verify public key data	93h	01h
Verify presence of signature	95h	01h
Verify the signature S2	93h	02h

6.8 PURCHASE REVERSAL

6.8.1 DEFINITION AND SCOPE

The ‘Recredit EEP for Purchase Reversal’ command does not require an Initialise EEP command as it is part of the Purchase Transaction. It is sent after the Debit EEP for Purchase command.

The PSAM calculates the reversal signature S2-R and sends it to the EEP. After the EEP verifies S2-R, the balance increased with the amount of the latest successful Purchase Transaction or with the amount of the latest step of an Incremental Purchase Transaction, retrieved from the stored Transaction Details.

The PSAM generates the signature S5, which is sent to the Acquiring Technical Operator for verification.

6.8.2 COMMAND MESSAGE

Command message for Recredit EEP for Purchase Reversal

Field	Value	Length (bytes)
CLA	90h	1
INS	5Eh	1
P1	01h	1
P2	00h	1
Lc	07h + S2-R length + length of DD_{PDA}	1
ALG_{PDA}	001b (RSA)	1

[1] Or “Subsequent Debit EEP” in case of a subsequent debit.

ID_{ACQ}	Acquirer identifier	6
S2-R	Signature	$LPKM_{PSAM}$
DD_{PDA}	Discretionary Data	0 to 16

6.8.3 RESPONSE MESSAGE

Response to Recredit EEP for Purchase Reversal

Field	Value	Length (bytes)
SW1-SW2	Status bytes	2

6.8.4 STATUS CONDITIONS

Status Conditions for Recredit EEP for Purchase Reversal

SW1	SW2	Meaning
93h	02h	Invalid signature
95h	80h	Command out of sequence

6.8.5 CONDITIONAL USAGE AND SECURITY

The command shall be rejected if the TRT of the actual session does not equal 00100111b or 00100011b.

The command shall be rejected if the signature S2-R is not valid.

6.8.6 COMMAND PROCESSING

Verification	SW1	SW2
The EEP status shall allow “Recredit EEP for Reversal”	95h	80h
Verify signature S2-R	93h	02h

6.9 RECREDIT EEP FOR PURCHASE CANCELLATION

6.9.1 DEFINITION AND SCOPE

The “Recredit EEP for Purchase Cancellation” command increases the actual balance of a Slot in the EEP with the total amount of the latest successful Purchase Transaction or with the amount of the latest step of an Incremental Purchase Transaction, if it was the last EEP transaction.

The signature S2 received from the Purchase Device is verified by the EEP, then the balance increased with the amount of the latest successful Purchase Transaction or with the amount of the latest step of an Incremental Purchase Transaction, retrieved from the stored Transaction Details.

If the Purchase Cancellation Transaction is successful, a new record is created. The content of such a record is defined in section 4.4.

The Slot balance and the log record are updated in non-volatile memory in an indivisible operation.

The PSAM generates the signature S5, which is sent to the Acquiring Technical Operator for verification.

6.9.2 COMMAND MESSAGE

Command message for Recredit EEP for Purchase Cancellation

Field	Value	Length (bytes)
CLA	90h	1
INS	52h	1
P1	01h	1
P2	00h	1
Lc	04h + $LPKM_{PSAM}$ + length of DD_{PDA}	1
S2	Signature	$LPKM_{PSAM}$
NT_{PSAM}	PSAM Transaction Number	4
DD_{PDA}	Discretionary Data	0 to 16

6.9.3 RESPONSE MESSAGE

Response to Recredit EEP for Purchase Cancellation

Field	Value	Length (bytes)
SW1-SW2	Status bytes	2

6.9.4 STATUS CONDITIONS

Status Conditions for Recredit EEP for Purchase Cancellation

SW1	SW2	Meaning
93h	01h	Invalid or missing public key.
93h	02h	Invalid signature.
95h	01h	Signature is missing.
95h	80h	Command out of sequence (Recredit not allowed).

6.9.5 CONDITIONAL USAGE AND SECURITY

The command is rejected if TRT_{EEP} value is different from 01001111b.

The command is rejected if the signature S2 is not present or is not valid.

If the transaction is not completed successfully, the Slot balance shall be restored and the log record updated as a Purse Provider option.

If the command is successful, TRT_{EEP} is set to 01000111b otherwise it is set to 01000110b.

6.9.6 COMMAND PROCESSING

Verification	SW1	SW2
The EEP status shall allow “Recredit EEP for Cancellation”	95h	80h
Verify public key data	93h	01h
Verify presence of signature S2	95h	01h
Verify the signature S2	93h	02h

6.10 EXCHANGE EEP CURRENCY

6.10.1 DEFINITION AND SCOPE

The “Exchange EEP Currency” command updates in the same operation the currency code, the currency exponent, the balance and the maximum balance of the source Slot and of the target Slot.

The MAC S2 received from the Load Device is verified by the EEP, then the parameters ($CURR_{EEP}$, BAL_{EEP} and $BALMAX_{EEP}$) are updated for both the source and target Slots in the EEP. If the transaction is successful, a new record is created in the log. The content of such a record is defined in section 4.4.

The balance, currency code, maximum balance and the log record are updated in non-volatile memory in an indivisible operation.

The MAC S3 is computed and returned to the Load Device.

6.10.2 COMMAND MESSAGE

Command message for Exchange EEP Currency

Field	Value	Length
CLA	90h	1
INS	56h	1
P1	00h	1
P2	00h	1
Lc	24h + length of DD_{PPSAM}	1
ID_{PPSAM}	Purse Provider SAM Identifier	4
R_{PPSAM}	Challenge	4
$BAL_{EEPsource}$	New Slot balance of source Slot	4
$BAL_{EEPtarget}$	New Slot balance of target Slot	4
$BALMAX_{EEPsource}$	New maximum balance of source Slot	4

$BALMAX_{EEPtarget}$	New maximum balance of target Slot	4
S2	MAC computed by the Purse Provider SAM	8
$DDEA_{EEP}$	Deactivation date of the EEP	4
DD_{PPSAM}	Discretionary Data	0 to 16
Le	00h	1

6.10.3 RESPONSE MESSAGE

Response to Exchange EEP Currency

Field	Value	Length (bytes)
CC_{TRX}	Transaction Completion Code	2
S3	MAC computed by the card	8
DD_{EEP}	Discretionary Data	0 to 16
SW1-SW2	Status bytes	2

In the case of Currency Exchange from one Slot into another, whereby the balance of the source Slot becomes zero, the source Slot is inactivated after the Currency Exchange Transaction is completed.

6.10.4 STATUS CONDITIONS

Status Conditions for Exchange EEP Currency

SW1	SW2	Meaning
93h	02h	Invalid signature
94h	01h	Currency error
94h	04h	Value out of range
95h	80h	Command out of sequence (currency exchange not allowed)

6.10.5 CONDITIONAL USAGE AND SECURITY

The command is rejected if TRT_{EEP} value is different from 01101111b.

The command is rejected if the deactivation date is different from zero.

The command is rejected if the new currency code is different from the currency code received in the initialisation command.

If the transaction is not completed successfully, the EEP balance, the currency code, the maximum balance and the content of the Transaction Details shall be restored.

If the command is successful, TRT_{EEP} is set to 01100111b otherwise it is set to 01100110b.

6.10.6 COMMAND PROCESSING

Verification	**SW1**	**SW2**
The EEP status shall allow "Exchange EEP Currency"	95h	80h
Check DDEA$_{EEP}$ ≠ 0	94h	04h
Check the currency (Verify CURR$_{NEW}$=CURR$_{EEPtarget}$ init command)	94h	01h
Verify the MAC S2	93h	02h

6.11 EEP INQUIRY

6.11.1 DEFINITION AND SCOPE

The "EEP Inquiry" command serves a twofold purpose. It provides information relating to (at least) the last transaction that was computed and stored by the EEP. The command also supports access to Slot(s) related information such as Slot balance and currency code.

6.11.2 COMMAND MESSAGE

Command message for EEP Inquiry

Field	Value	Length (bytes)
CLA	90h	1
INS	5C	1
P1	See coding table for P1	1
P2	See coding table for P2	1
Le	00h	1

6.11.3 COMMAND PARAMETERS

The EEP Inquiry command permits information, either about stored transactions or about the EEP Slots, to be retrieved in a number of ways depending on the values of the parameters P1 and P2.

6.11.3.1 Coding of P1

P1 indicates whether the information requested concerns EEP Slot data or stored transactions.

In case details are requested about stored transactions, P1 specifies the kind of transaction (load, purchase, currency exchange or 'not specified').

P1	Description
00h	Any Transaction Type (not specified)
01h	Load Transaction
02h	Purchase Transaction
03h	Purchase Cancellation Transaction

04h	Currency Exchange Transaction
10h	EEP Slot data
$8x_1h$	Currency selection

6.11.3.2 Coding of P2

P2 indicates the processing sequence of the requested transaction (the last transaction or the preceding transaction), when issuing consecutive EEP Inquiry commands.

It also indicates which Slot shall be accessed. Consecutive inquiries with P2=01h allow scrolling through the active Slots. It is up to the Purse Provider to define the retrieval sequence on consecutive EEP Inquiry commands.

P2	**Description**		
	P1=00h, 01h, 02h, 03h or 04h	**P1=10h**	**P1=$8x_1h$**
00h	Most recent transaction	First slot related data	-
01h	Preceding transaction	Slot related data	-
x_2x_3h			Currency code = $x_1x_2x_3$

6.11.4 RESPONSE MESSAGE

Response to EEP Inquiry

Field	**Value**	**Length (bytes)**
Log entry	As described below.	Variable
SW1-SW2	Status Bytes	2

The response message includes the EEP data structure as described in section 4.3 EEP Slot Data and 4.4 EEP Log Data and the status bytes SW1-SW2.

The response message has a variable length depending on the data that is read. No tag and length fields are transmitted.

Data (Slot or stored information)	**Length**
EEP Slot Data	11 bytes
Load Transaction	44 bytes
Purchase Transaction	42 bytes
Purchase Cancellation Transaction	42 bytes
Currency Exchange Transaction	59 bytes

6.11.5 STATUS CONDITIONS

Status Conditions for EEP Inquiry

SW1	SW2	Meaning
6A	82h	File not found
6A	83h	Record not found

6.11.6 CONDITIONAL USAGE AND SECURITY

The command is rejected if the requested transaction type is not present and if subsequently there is no transaction corresponding to the processing sequence indicated in P2.

The command is rejected if no EEP Slots are available.

6.11.7 COMMAND PROCESSING

Verification	SW1	SW2
Verify presence of Transaction Type	6A	82h
Verify presence of Transaction or EEP Slot	6A	83h

6.12 VERIFY CERTIFICATE

6.12.1 DEFINITION AND SCOPE

The Verify Certificate command asks the EEP application to verify a certificate with a higher level Public Key and to recover and store a lower level Public Key.

6.12.2 COMMAND MESSAGE

Command message for Verify Certificate

Field	Value	Length (bytes)
CLA	90h	1
INS	82h	1
P1	01h	1
P2	01h, 02h or 03h	1
Lc	Var.	1
PKC	Public Key Certificate	LPKC
LID	Length of ID_{XXX}	1
ID_{xxx}	Regional Authority, Acquirer or PSAM ID	6 or 4
LPKM	Length of Public Key Modulus	1
PKR	Public Key Remainder	LPKR
PKE	Public Key Exponent	1 or 3

The following table contains the different values depending on P2

Value	Meaning
01h	Verify using the CA Public Key
02h	Verify using the cached Public Key
03h	Verify using the key recovered from the previous Verify Certificate command

6.12.3 RESPONSE MESSAGE

Response to Verify Certificate

Field	Value	Length (bytes)
SW1-SW2	Status Bytes	2

6.12.4 STATUS CONDITIONS

Status Conditions for Verify Certificate

SW1	SW2	Meaning
6Ah	88h	Public Key not already present
63h	00h	Authentication failed
6Fh	80h	Certificate expired
64h	00h	State of non-volatile memory unchanged

6.12.5 COMMAND PROCESSING

P1=01h and P2=01h

Verification	**SW1**	**SW2**
Check for the presence of PK$_{CA, ACQ}$ in the EEP	6Ah	88h
Decrypt the certificate with the PK $_{CA, ACQ}$ and check it	63h	00h
Check expiry date of certificate	6Fh	80h
Check if verification took place	64h	00h

P1=01h and P2=02h or 03h

Verification	**SW1**	**SW2**
Check for the presence of cached or recovered PK in the EEP	6Ah	88h
Decrypt the certificate with cached or recovered PK and check it	63h	00h
Check expiry date of certificate	6Fh	80h

Check if verification took place	64h	00h

6.13 GET PREVIOUS SIGNATURE

6.13.1 DEFINITION AND SCOPE

The Get Previous Signature command retrieves a signature or MAC previously generated by the EEP that may have been lost or corrupted. This signature or MAC may be retrieved from the appropriate data or may be recalculated. It shall not be recalculated on exactly the same data.

The usage of the command is limited to the retrieval of a signature or MAC sent in the response to the Debit EEP for Purchase command and the Credit EEP for Load command in the case of Load against other means of payment. The command shall only be capable of being used once for one value of NT_{EEP}.

6.13.2 COMMAND MESSAGE

Command message for Get Previous Signature

Field	Value	Length
CLA	90h	1
INS	5Ah	1
P1	00h	1
P2	00h	1
Lc	02h	1
NT_{EEP}	EEP Transaction Number	2
Le	00h	1

6.13.3 RESPONSE MESSAGE

The content of the response message depends on the transaction that was previously performed. This transaction could be either a Purchase Transaction or a Load transaction against other means of payment.

Response to Get Previous Signature

Field	Value	Length
S3 or S3’	Signature S3 (Purchase) or MAC S3’ (Load)	$LPKM_{EEP}$ or 8
SW1-SW2	Status bytes	2

6.13.4 STATUS CONDITIONS

Status Conditions for Get Previous Signature

SW1	SW2	Meaning
94h	04h	Value out of range

6.13.5 CONDITIONAL USAGE AND SECURITY

The command is rejected if the value of NT_{EEP} is different from the value stored in the previous signature or MAC data.

6.13.6 COMMAND PROCESSING

Verification	SW1	SW2
Verify NT_{EEP}	94h	04h

6.14 SCRIPT PROCESSING

6.14.1 PURPOSE

A Purse Provider may provide command scripts to be delivered to the EEP by the Load Device to perform functions that are not necessarily relevant to the current transaction but are important for the continued functioning of the application in the EEP. Multiple scripts may be provided with either a Load message or a Currency Exchange message from the Purse Provider. Each message may contain any number of script commands.

Script processing is provided to allow for functions that are outside the scope of this specification but are nonetheless necessary.[1]

A script may contain script commands not known to the Load Device, but each command shall be delivered by the Load Device to the EEP individually according to this specification.

The mechanism for providing the information on the script result to the Purse Provider is not covered by this Standard.

6.14.2 SEQUENCE OF EXECUTION

Two separate script tags are defined that are available for use by the Purse Provider. Scripts with tag 71h shall be processed prior to issuing either the credit EEP for load or the EEP currency exchange command. Scripts using tag 72h shall be processed after issuing one of the previous two commands.

6.14.3 DESCRIPTION

A Script is a constructed data object (tag 71h or 72h) containing (optionally) a Script Identifier and a sequence of Script Command APDUs to be delivered serially to the EEP. The Script Identifier is optional and is not interpreted by the terminal; it is meaningful only to the Purse Provider. Figure 3 and Figure 4 illustrate a Script containing a Script Identifier and three commands.

T	L	T	L	Script ID	Commands
71h or 72h	L (Sdata, including Script ID, tags, and lengths)	9F18h	04	Identifier (4 bytes)	(see Figure 4)

[1] An example might be unlocking of an offline PIN, which might be done differently by various issuers or payment systems.

Figure 3 - Script Format

T_1	L_1	V_1	T_2	L_2	V_2	T_3	L_3	V_3
86h	$L(V_1)$	Command	86h	$L(V_2)$	Command	86h	$L(V_3)$	Command

Figure 4 - Script Command Format (Shown with Three Commands)

It is possible for multiple Scripts to be delivered with a single load message or currency exchange message. Each Script shall be processed by the Load Device in the sequence in which it appears in the message according to the following rules:

- Script Commands shall be separated using the BER-TLV coding of the data objects defining the commands (tag 86h);
- Each command will be delivered to the EEP as a command APDU in the sequence in which it appeared in the Script;
- The Load Device shall examine only SW1 in the response APDU and perform one of the following actions:

  If SW1 indicates either normal processing or a warning according to the conventions described in [EMV'96], the Load Device shall continue with the next command from the Script (if any);

  If SW1 indicates an error condition, the processing of the Script shall be terminated.

The Load Device shall be able to support at least one or more Scripts in each load message or currency exchange message it receives, where the total length of all Scripts in the response is no greater than 128 bytes.

The Load Device shall be able to recognise the tag for the Script transmitted in the message.

- If the tag is 71h, the Load Device shall process the script before issuing either the credit for Load or the currency exchange command.
- If the tag is 72h, the Load Device shall process the script after issuing one of the two previous commands.

ooOOoo