

Identification card systems — Inter-sector electronic purse —

Part 3: Data elements and interchanges

The European Standard EN 1546-3:1999 has the status of a
British Standard

ICS 35.240.15

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSI
Documents



Document Sharing Hub

National foreword

This British Standard is the English language version of EN 1546-3:1999.
The UK participation in its preparation was entrusted to Technical Committee IST/17, Identification cards and related devices, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 83 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 January 2000

© BSI 01-2000

ISBN 0 580 35215 3

Amendments issued since publication

Amd. No.	Date	Comments

English version

Identification card systems – Inter-sector electronic purse – Part 3: Data elements and interchanges

Systèmes de cartes d'identification – Porte-monnaie
électronique intersectoriel – Partie 3: Eléments de données
et échanges

Identifikationskartensysteme – Branchenübergreifende
elektronische Geldbörse – Teil 3: Datenelemente und
Datenaustausch

This European Standard was approved by CEN on 20 May 1999.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the Central Secretariat has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Central Secretariat: rue de Stassart, 36 B-1050 Brussels

Contents

1	Scope	4
2	Normative references	4
3	Definitions	5
4	Symbols and abbreviations	6
5	General information.....	8
5.1	Introduction.....	8
5.2	Discretionary Data	8
6	IEP data elements	8
6.1	General remarks.....	8
6.2	List of data elements	8
7	IEP commands and responses	16
7.1	General remarks.....	16
7.2	Application selection.....	17
7.3	Application specific commands to the IEP	19
Annex A	(informative) Examples of further IEP commands.....	30
A.1	Application specific commands to the IEP.....	30
Annex B	(informative) Example of an IEP file structure	36
B.1	General remarks	36
B.2	Definitions	36
B.3	General remarks	36
B.4	Data elements.....	37
B.5	Logical model for an IEP.....	38
B.6	Common data files	39
B.7	Application specific files	39
Annex C	(informative) A PSAM implementation.....	44
C.1	General remarks	44
C.2	PSAM specific data elements	44
C.3	A file structure for the PSAM	48
C.4	Application specific commands to the PSAM	53
Annex D	(informative) Completion Codes used in IEP Systems	72
D.1	List of all Completion Codes.....	72
D.2	Cross reference of Completion Codes used by IEPs	74
D.3	Cross Reference of Completion Codes used by PSAMs	75
Annex E	(informative) Data elements for DES	78
E.1	General remarks	78
E.2	List of data elements	78
Annex F	(informative) Data elements for RSA	79
F.1	General remarks.....	79
F.2	List of data elements	79
Annex G	(informative) Data elements for DSS.....	81
G.1	General remarks.....	81
G.2	List of data elements	81

Foreword

This European Standard has been prepared by Technical Committee CEN/TC 224 "Machine-readable cards, related device interfaces and operations", the Secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by January 2000, and conflicting national standards shall be withdrawn at the latest by January 2000.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

This European Standard consists of the following parts, under the general title "Identification card systems - Inter-sector electronic purse":

- *Part 1: Definitions, concepts and structures*
- *Part 2: Security architecture*
- *Part 3: Data elements and interchanges*
- *Part 4 : Data objects*

1 Scope

This part of EN 1546 provides the necessary information on the data elements to be stored and exchanged in order to enable IEP Systems conforming to this standard to be interoperable.

The transaction types involving IEPs as defined in prEN 1546-1 (Definitions, concepts and structures) and EN 1546-2 (Security architecture) are covered by this part of EN 1546.

Formats for commands and responses, including the detailed definitions of single data elements, are defined, whereas the exact way the data may be stored in the components is outside the scope of EN 1546.

Methods for selection of the IEP application are defined.

Examples of formats for commands and responses to implement informative transaction types, as defined in EN 1546-2, are given in Annex A.

A possible file structure for the IEP and methods for reading out the content of files is not defined as it is not critical to interoperability. However, an example is given in Annex B.

The processing of the commands within the receiving devices is not defined by this part of EN 1546 as it is covered from a security point of view in EN 1546-2 (Security architecture).

The interface and functionality of the IEP are specified in detail, as the device that implements it is critical in achieving interoperability between different IEP Systems. An example of a PSAM implementation is given in Annex C, whereas LSAMs and PPSAMs are considered outside the scope of this part of EN 1546.

2 Normative references

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

EN 726-3, *Terminal equipment (TE) - Requirements for IC cards and terminals for telecommunication use - Part 3 : Application independent card requirements.*

prEN 1546-1, *Identification card systems - Inter-sector electronic purse - Part 1 : Definitions, concepts and structures.*

EN 1546-2:1996, *Identification card systems - Inter-sector electronic purse - Part 2 : Security architecture.*

prEN 1546-4, *Identification card systems - Inter-sector electronic purse - Part 4 : Devices.*

ISO 4217, *Codes for representation of currencies and funds.*

ISO/IEC 7812-1:1993, *Identification cards. Numbering system.*

ISO/IEC 7816-3:1989, *Information technology - Identification cards - Integrated circuit(s) cards with contacts. Part 3: Electronic signals and transmission protocols.*

ISO/IEC 7816-4:1995, *Information technology - Identification cards - Integrated circuit(s) cards with contacts. Part 4: Inter-industry commands for interchange.*

ISO/IEC 7816-5:1994, *Information technology - Identification cards - Integrated circuit(s) cards with contacts. Part 5: Registration system for applications in IC cards.*

ISO/IEC 7816-6:1996, *Information technology - Identification cards - Integrated circuit(s) cards with contacts. Part 6: Inter-industry data elements.*

ISO/IEC 9797, *Data cryptographic techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.*

3 Definitions

For the purposes of this **Error! Reference source not found.**, the following definitions apply:

3.1

activation

see prEN 1546-1

3.2

completion code

see EN 1546-2

3.3

deactivation

see prEN 1546-1

3.4

discretionary data

optional data elements added to messages as defined by the Purse Provider

3.5

IEP balance

see prEN 1546-1

3.6

IEP system

see prEN 1546-1

3.7

load

see prEN 1546-1

3.8

load device

see prEN 1546-1

3.9

load log

see prEN 1546-1

3.10

load SAM

see prEN 1546-1

3.11

message authentication code

see EN 1546-2

3.12

negative file

see prEN 1546-1

3.13

purchase

see prEN 1546-1

3.14

purchase device

see prEN 1546-1

© BSI 01-2000

3.15
purchase log
see prEN 1546-1

3.16
purchase SAM
see prEN 1546-1

3.17
purse provider
see prEN 1546-1

3.18
purse provider SAM
see prEN 1546-1

3.19
secure application module
see prEN 1546-1

3.20
signature
see EN 1546-2

3.21
total
see prEN 1546-1

In order to emphasize terms specific to a general IEP System, throughout this European Standard, these terms commence with capital letters, e.g. Purse Provider.

4 Symbols and abbreviations

k concatenation (of data elements)
A vector (identifier for an ordered set of data elements)

'0'..'9' and 'A'..'F' : The sixteen hexadecimal digits.

AID application identifier
ALG algorithm
AM authentication mode
AP application profile
APDU application protocol data unit (see ISO/IEC 7816-4)
ATR answer to reset
BAL balance
BALmax maximum balance
BCD binary coded decimal
CC completion code
CURR currency

DACT	activation date
DD	discretionary data
DDEA	deactivation date
DES	data encryption standard (cryptographic algorithm)
DEXP	expiry date
DSS	digital signature standard (cryptographic algorithm)
FCI	file control information
IC	integrated circuit
ICC	IC card
ID	identifier
IEP	inter-sector electronic purse
IK	key information
LDA	load device application
LSAM	load SAM
LSB	least significant byte
M	amount
MAC	message authentication code
MSB	most significant byte
MTOT	total amount
NT	transaction number
PAR	parameter
PDA	purchase device application
PIN	personal identification number
PIX	proprietary application identifier extension
PP	purse provider
PPSAM	purse provider SAM
PSAM	purchase SAM
R	random number
RFU	reserved for future use
RID	registered identifier
RSA	Rivest, Shamir and Adleman (cryptographic algorithm)

SAM	secure application module
SW	status word
TPDU	transmission protocol data unit (see ISO/IEC 7816-4)

5 General information

5.1 Introduction

All definitions of data elements and messages used for IEP applications only concern what can be seen on the interface level, as this is necessary to obtain interoperability between different IEP Systems.

Other data elements, as for example encipherment keys, are needed, but as there is no need to send these on the interface of the ICC hosting the IEP application during normal operation, the coding and possible placing in one or more internal files is left open for different implementations.

5.2 Discretionary Data

In order to allow additional data to be used in certain implementations of IEP Systems, commands and responses may contain Discretionary Data within the message.

The handling of such Discretionary Data, e.g. how to update Discretionary Data in files based on Discretionary Data received in commands, is outside the scope of this standard.

For interoperability reasons, no device should depend on such Discretionary Data being sent to it, e.g. if an IEP is used in a Purchase Device not sending any Discretionary Data, it should still be able to perform normal Purchase transactions. In the same way, the PDA/PSAM shall discard any Discretionary Data if it cannot be handled, and still be able to perform the transaction.

6 IEP data elements

6.1 General remarks

For each data element, the following descriptors may be present:

- reference (if present, it refers to an existing standard defining a similar data element);
- purpose (a short description of the use of the given data element);
- format (giving the recommended default size of the data element and possibly a symbolic format used to describe the content);
- content (the exact definition for the coding of the data element);
- remarks (other information).

6.2 List of data elements

This subclause defines data elements used to support the IEP and which may be transmitted to or from the IEP. Data elements not used in mandatory commands are optional.

Data elements can optionally be managed as data objects using ASN.1-BER (abstract syntax notation one, basic encoding rules). This mechanism is described in prEN 1546-4.

6.2.1 AID_{IEP} (Application identifier for an IEP)

Reference: ISO/IEC 7816-5 and ISO/IEC 7816-6 (tag '4F').

Purpose: To enable the PDA to select the IEP application prior to performing the transactions defined in this European standard, e.g. Purchase and Load. If the card uses implicit selection, the AID is included in the historical bytes of the answer to reset message.

Format: 5-16 bytes.

Content: RID || PIX where RID is the 5 byte global registered identifier as specified in ISO/IEC 7816-5 and PIX (0-11 bytes) is for free use by the Purse Provider.

Remarks: AID_{IEP} is used as the file name for DF_{IEP} in order to facilitate easy selection of the IEP application in multi-application components.

6.2.2 ALG_{IEP} (Cryptographic algorithm used by an IEP)

Purpose: A value stored in the IEP, identifying the cryptographic algorithm used by the IEP (including the modes of operation etc.) used for authentication and/or encipherment between IEP, PSAM, LSAM and PPSAM.

Format: 1 byte.

Content: The coding is at the discretion of the Purse Provider.

Remarks: Each value shall implicitly include all the information needed to implement the algorithm, e.g. the algorithm type (if several exist) and the key length.

6.2.3 AM_{IEP} (Authentication Mode required by an IEP)

Purpose: To identify the authentication mode required by the IEP for Purchase transactions. Additionally, it specifies the requirement for S₁ and a signed acknowledgement from the PSAM at the end of the transaction.

Format: 1 byte.

Content: The possible values are defined by table 1.

Table 1 - Coding of AM_{IEP}

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	-	-	-	-	-	-	-	Usage of S ₁ :
0	-	-	-	-	-	-	-	- S ₁ is not sent by the IEP
1	-	-	-	-	-	-	-	- S ₁ is sent by the IEP
-	x	-	-	-	-	-	-	Requirement for a signed ack.:
-	0	-	-	-	-	-	-	- Signed ack. not required
-	1	-	-	-	-	-	-	- Signed ack. Required
-	-	-	-	-	-	x	x	Authentication mode required by the IEP:
-	-	-	-	-	-	0	0	- RFU
-	-	-	-	-	-	0	1	- One-way authentication
-	-	-	-	-	-	1	0	- Two-way authentication
-	-	-	-	-	-	1	1	- Dual-mode authentication
-	-	x	x	x	x	-	-	RFU

Remarks: The reserved bits (b6-b3) shall be set to zero.

6.2.4 AP_{IEP} (Application Profile of an IEP)

Purpose: To identify the following optional functions implemented in an IEP:

- possibility of performing incremental Purchase transactions;
- purchase Cancellation/IEP Balance Recovery;
- currency Conversion;
- update of application parameters;
- use of ASN.1-BER formats.

Format: 2 bytes.

Content: The possible values for the first byte are defined by table 2. All bits in the second byte are reserved for future use.

Table 2 - Coding of AP_{IEP}

b8	b7	b6	b5	B4	b3	b2	b1	Meaning
x	-	-	-	-	-	-	-	Incremental step Purchase:
0	-	-	-	-	-	-	-	- incremental steps not allowed
1	-	-	-	-	-	-	-	- incremental steps allowed
-	x	-	-	-	-	-	-	Purchase Cancellation/IEP Balance Recovery function:
-	0	-	-	-	-	-	-	- Cancellation not allowed
-	1	-	-	-	-	-	-	- Cancellation allowed
-	-	x	-	-	-	-	-	Currency Conversion function:
-	-	0	-	-	-	-	-	- Curr. Conversion not allowed
-	-	1	-	-	-	-	-	- Curr. Conversion allowed
-	-	-	x	-	-	-	-	Update IEP Parameters function:
-	-	-	0	-	-	-	-	- Update not allowed
-	-	-	1	-	-	-	-	- Update allowed
-	-	-	-	x	x	X	-	Use of ASN.1-BER format:
-	-	-	-	0	0	0	-	- Fixed formats
-	-	-	-	0	0	1	-	- See prEN 1546-4
-	-	-	-	0	1	0	-	- See prEN 1546-4
-	-	-	-	0	1	1	-	- See prEN 1546-4
-	-	-	-	1	0	0	-	- See prEN 1546-4
-	-	-	-	1	0	1	-	- See prEN 1546-4
-	-	-	-	1	1	0	-	- See prEN 1546-4
-	-	-	-	1	1	1	-	- See prEN 1546-4
-	-	-	-	-	-	-	x	RFU

Remarks: The reserved bit (b1) shall be set to zero.

6.2.5 BAL_{IEP} (Balance of an IEP)

Reference: ISO 4217 concerning currency code and currency exponent.

Purpose: Defines the actual Value in the IEP. It can only be interpreted in combination with CURR_{IEP}.

Format: 4 bytes.

Content: An unsigned binary integer defining the actual Balance. The Balance is represented in the smallest unit of the corresponding currency as specified in the currency code (CURR_{IEP}).

Remarks: This data element may be limited by BAL_{maxIEP}.

6.2.6 BAL_{maxIEP} (Maximum Balance of an IEP)

Reference: ISO 4217 concerning currency code and currency exponent.

Purpose: Defines the maximum value of a given IEP up to which a Load is allowed. It can only be interpreted in combination with CURR_{IEP}. May be necessary due to national legislation or Purse Holder requirements. Can be read out using IEP Monitoring. It may be updated by use of the Update IEP Parameter transaction and shall be updated as part of the Currency Conversion transaction.

Format: 4 bytes.

Content: An unsigned binary integer defining the Maximum Balance.

6.2.7 CC_{IEP} (Completion Code of an IEP)

Reference: ISO/IEC 7816-3 and ISO/IEC 7816-4.

Purpose: The result of the actions within an IEP executing a given command. It is transmitted in the response to indicate whether error(s) occurred (and which).

Format: The two status bytes SW1 and SW2 are used.

Content: The possible values for each command are defined in subclause 7.3 and an overview is given in Annex D (Informative).

6.2.8 CURR_{IEP} / CURR_{LDA} / CURR_{PDA} (Actual currency for an IEP, LDA or PDA)

Reference: ISO 4217 and ISO/IEC 7816-6 (tag '5F2A' and '5F36').

Purpose: To identify the currency of the balance of a given IEP or currency specified by the LDA or PDA in combination with an Amount in a Load or Purchase transaction. Additionally, to indicate the number of decimals in amount fields.

Format: 3+1 digits (2+1 bytes).

Content: According to ISO 4217: The first two bytes contain the numeric currency code and the last byte indicates the position of the decimal point (the number of decimals).

Remarks: The 4 most significant bits in the currency code shall be set to zero. The two parts of this data element may be accessed separately.

6.2.9 DACT_{IEP} (Activation date of an IEP)

Reference: ISO/IEC 7816-6 (tag '5F25').

Purpose: To be able to verify (using IEP Monitoring) at which date the IEP was activated.

Format: 6 digits (3 bytes) in the format YYMMDD.

Content: YY : The two least significant digits of the year of Activation, coded in BCD. MM : The number of the month of Activation, coded in BCD (January is month number 1). DD : The day number of the month for the Activation, coded in BCD.

Remarks: The default value '000000' indicates that the IEP has not yet been activated.
To avoid problems around the year 2000, the following conventions shall apply:

- a) If the year is in the range 1990-1999, YY shall be in the range '90'-'99'.
- b) If the year is in the range 2000-2089, YY shall be in the range '00'-'89'.
- c) If the year is outside these two ranges, it cannot be represented by this data element.

6.2.10 DD (Discretionary Data)

Purpose: To allow implementation dependent data to be added to commands and responses.

Format: n bytes.

Content: At the discretion of the Purse Provider.

6.2.11 DDEA_{IEP} (Deactivation date of an IEP)

Purpose: To be able to identify at which date the IEP was deactivated.

Format: As for DACT_{IEP} (see 6.2.9).

Content: As for DACT_{IEP} (see 6.2.9).

Remarks: As for DACT_{IEP} (see 6.2.9).

6.2.12 DEXP_{IEP} (Expiry date of an IEP)

Reference: ISO/IEC 7816-6 (tag '5F24').

Purpose: The expiry date may be checked by the respective PSAM or PPSAM in the initialisation phase of a Load or a Purchase transaction to prevent transactions using an expired component.

Format: As for DACT_{IEP} (see 6.2.9).

Content: As for DACT_{IEP} (see 6.2.9).

Remarks: As for DACT_{IEP} (see 6.2.9).

6.2.13 ID_{IEP} (Identifier for an IEP)

Purpose: To uniquely identify each IEP belonging to the Purse Provider.

Format: 5 bytes.

Content: At the discretion of the Purse Provider.

Remarks: The IEP identifier shall be unique for the given Purse Provider and shall not be changed during the lifetime of the IEP.

6.2.14 ID_{LDA} (Identifier for an LDA)

Purpose: To uniquely identify each Load Device.

Format: 4 bytes.

Content: At the discretion of the Purse Provider.

Remarks: The LDA identifier should be unique.

6.2.15 ID_{PPSAM} (Identifier for a PPSAM)

Purpose: To uniquely identify each PPSAM belonging to the Purse Provider.

Format: 4 bytes.

Content: At the discretion of the Purse Provider.

Remarks: The PPSAM identifier shall be unique for the given Purse Provider.
This data element shall not be changed during the lifetime of the PPSAM.

6.2.16 ID_{PSAM} (Identifier for a PSAM)

- Purpose:* To uniquely identify each PSAM belonging to the Purse Provider.
- Format:* 4 bytes.
- Content:* At the discretion of the Purse Provider.
- Remarks:* The PSAM identifier shall be unique for the given Purse Provider.
This data element shall not be changed during the lifetime of the PSAM.

6.2.17 IK_{IEP} / IK_{PSAM} / IK_{PPSAM} (Key information for an IEP, PSAM or PPSAM)

- Purpose:* To give to another component the necessary information to verify or compute Signatures.
- Format:* Algorithm dependent.
- Content:* Algorithm dependent.
- Remarks:* The size and content of IK_{COMP} depends on the algorithm and Key Management scheme used.
Examples are given in annexes E, F and G for the DES, RSA and DSS algorithms respectively.

6.2.18 M_{PDA} / M_{LDA} (Transaction amount of a PDA or LDA)

- Reference:* ISO 4217 concerning use of the currency exponent.
- Purpose:* To inform the involved components of the transaction amount (Load, Purchase and Purchase Cancellation/IEP Balance Recovery transactions).
- Format:* 4 bytes.
- Content:* The transaction amount coded as an unsigned binary integer.
- Remarks:* The transaction amount is always associated with a currency code and currency exponent.

6.2.19 MTOT_{IEP} (Total transaction amount for a Purchase)

- Reference:* ISO 4217 concerning use of the currency exponent.
- Purpose:* To accumulate the amounts of incremental Purchase steps into one total value for the Purchase transaction.
- Format:* 4 bytes.
- Content:* The amount in the currency given by CURR_{IEP}, modified by the currency exponent also defined in CURR_{IEP}. It is coded as an unsigned binary integer.

6.2.20 NT_{IEP} / NT_{PSAM} (Transaction number for an IEP, PSAM)

- Reference:* ISO/IEC 7816-6 (tag '5F32').
- Purpose:* To serve as an identifier for a specific transaction (in combination with PP_{IEP} and IEP, or PP_{PSAM} and PSAM respectively). Furthermore, to serve as a challenge parameter to other components, e.g. PSAMs.
- Format:* NT_{IEP}: 2 bytes.
NT_{PSAM}: 4 bytes.

Content: The 16 or 32 bit transaction number, coded as an unsigned binary integer.

Remarks: NT_{IEP} is incremented in each transaction initiated in the IEP and shall never repeat.
NT_{PSAM} has to change in consecutive transactions and may be implemented at the discretion of the Purse Provider.

6.2.21 PAR (Parameter identifier for updates)

Purpose: To identify the data element to be updated.

Format: 2 bytes.

Content: At the discretion of the Purse Provider.

6.2.22 PP_{IEP} (Purse Provider identifier for an IEP)

Reference: ISO/IEC 7812-1.

Purpose: To uniquely identify which Purse Provider issued the IEP.

Format: 6 digits (3 bytes).

Content: As defined by ISO/IEC 7812-1, subclause 4.2, coded as BCD digits.

Remarks: If the issuer identifier consists of less than 6 digits, the identifier shall be left justified and padded with trailing hexadecimal 'F's.

6.2.23 R_{PPSAM} / R_{LDA} (Random number computed by a PPSAM or LDA)

Purpose: To serve as a challenge from the PPSAM or an LDA to an IEP.

Format: 4 bytes.

Content: Random bits.

Remarks: The algorithm and device selected for computing R are outside the scope of this standard.

7 IEP commands and responses

7.1 General remarks

7.1.1 Conformance to ISO/IEC 7816-4

The message structure etc. used throughout this subclause conforms to ISO/IEC 7816-4, subclauses 5.3, 5.4 and 5.5 in the following ways:

- an IEP shall always respond to a command using the corresponding response message (also defined in this standard). In case the processing of the command is not successful, the response may consist of only two bytes (SW1 and SW2) indicating the reason why the command was rejected;
- the messages in this standard define the APDUs (Application Protocol Data Unit) as used in ISO/IEC 7816-4. These APDUs shall be mapped on to the TPDUs (Transmission Protocol Data Unit) according to the rules listed in Annex A (for T=0) and Annex B (for T=1) of ISO/IEC 7816-4;
- the class byte selected for IEP commands ('80') indicates that the command message is proprietary, i.e. not covered by ISO/IEC 7816-4. However, the same message structure is used;
- a number of instruction bytes (INS) have been assigned in order to identify the application specific commands. The values have been selected outside the ranges of codes already defined by ISO and ETSI;
- the parameter bytes P1 and P2 are not restricted by ISO/IEC 7816-4 and are used in some of the application specific commands as further qualifiers for the instruction byte;
- the coding of the status bytes (SW1 and SW2) conforms to ISO/IEC 7816-4 concerning general error situations. Additional values of the status bytes are defined in ranges outside the scope of ISO/IEC 7816-4;
- secure messaging as defined in ISO/IEC 7816-4 is not used by IEPs as security is an integrated part of the transaction protocols.

7.1.2 Length fields

ISO/IEC 7816-4 defines short and long length fields in the commands to indicate the length of the parameters transmitted in the command (if any) as well as the expected length of the response. These length fields are called L_C and L_E respectively.

Where the amount of Discretionary Data is large, the short (1 byte) length fields may not be sufficient, but as very long messages would impose a large penalty on the transaction time, this standard limits most commands to use only short length fields.

Where public keys and corresponding public key certificates are transmitted, long length fields are allowed, as the amount of data could exceed 255 bytes, e.g. if the public key of an IEP is certified by several levels of authorities.

Several data elements in the commands and responses defined by this part of EN 1546 have lengths which depend on other parameters, e.g. the algorithm used. Such data elements are described with a length equal to "variable". However, the devices involved are able to parse the messages, as they are informed of the parameters affecting the actual lengths.

7.1.3 Common Completion Codes

An IEP shall either return on an IEP command the appropriate responses SW1 and SW2 as defined in ISO/IEC 7816-4, clause 5.4.5, or the IEP application specific ones as defined for some commands in the following subclauses of this standard.

Table 3 - Common Completion Codes

SW1	SW2	Meaning
'91'	'01'	Application is not active
'91'	'06'	Application has been deactivated
'92'	'01'	Application is not open ¹⁾
'95'	'8X'	Command out of sequence, actual state is X
1) This Completion Code may be used if the IEP has been closed by use of a PIN or a similar mechanism.		

7.1.4 IEP response message formats

A rejection message to a command consists solely of a Completion Code with one exception: The rejection message to a Credit IEP for Load command contains, in addition to the Completion Code, a Signature.

The rejection messages are not defined here.

7.2 Application selection

The following two methods exist for selecting the IEP application before performing the transactions defined in EN 1546:

- a) direct application selection which shall be supported by all cards;
- b) implicit application selection which may additionally be supported by mono-application cards.

The use of implicit selection for mono-application cards can lead to lower transaction times in some cases as described in subclause 7.2.2.

Further application selection methods which may be supported by the ICC hosting the IEP application(s) are outside the scope of this part of EN 1546.

7.2.1 Direct application selection

The ICC shall at least support direct application (as defined in ISO/IEC 7816-4, subclause 9.3.2) where either the full AID or the RID (the first five bytes of the AID) is used as the file name as parameter for a Select File command. File control information (FCI) shall be returned by the ICC in the response to this command.

The operating system of the ICC shall keep track of the application currently selected and only allow the commands applicable to that particular application while it is selected.

The response to Select File when the selected file is DF_{IEP} shall be coded according to table 4.

Table 4 - Coding of the response to Select File command for selecting DF_{IEP}

Field	Value	Mandatory/ optional	Length (bytes)
Tag	'6F' (FCI)	M	1
Length	Depends on the number of data objects included	M	1
Tag	'84' (DF name)	M	1
Length	'05'-'10'	M	1
AID _{IEP}	Application identifier of the IEP	M	5-16
Tag	'A5' (proprietary data)	M	1
Length	Depends on the number of data objects included	M	1
Tag	'87' (Application priority indicator)	O	1
Length	'01'	O	1
API	Application priority indicator	O	1
Tag	'9F38' (Processing options data object list)	O	2
Length	Depends on the number of data objects included	O	1
PDOL	Processing options Data Object Data List	O	<i>n</i>
Tag	'BF0C' (FCI issuer discretionary data)	M	2
Length	Depends on the number of data objects included	M	1
Tag	'C1' (Purse Provider identifier)	M	1
Length	'03'	M	1
PP _{IEP}	Purse Provider identifier	M	3
Tag	'C9' (application profile)	M	1
Length	'02'	M	1
AP _{IEP}	Application profile of the IEP	M	2
Tag	'5F2A' (currency code)	O	2
Length	'02'	O	1
CURR _{IEP}	Currency code (first 2 bytes)	O	2
Tag	'5F36' (currency exponent)	O	2
Length	'01'	O	1
CURR _{IEP}	Currency code (last byte)	O	1
Tag	'C3' (IEP Balance)	O	1
Length	'04'	O	1
BAL _{IEP}	IEP Balance	O	4
Tag	'C4' (Maximum Balance)	O	1
Length	'04'	O	1
BAL _{maxIEP}	Maximum Balance	O	4
SW1-SW2	Status bytes	M	2

NOTE The order of the data objects included in the response may vary and further data objects may optionally be added.

7.2.2 Implicit application selection

The AID of the IEP application shall be included in the historical bytes of the ATR as defined in ISO/IEC 7816-4, subclause 8.3 and ISO/IEC 7816-5, subclause 6.3.3. Other data objects which may be needed by the PDA/LDA, such as PP_{IEP} and AP_{IEP}, may not be present as the number of historical bytes is limited to 15.

Implicit application selection may be offered by mono-application cards to speed up transactions in PDAs/LDAs knowing the Purse Provider and application profile associated with a given AID ("local" cards). Such devices may initiate IEP transactions immediately after reset without sending a Select File command.

PDAs/LDAs not knowing the related data (or if there is not a fixed relationship) will have to issue the Select File command described in subclause 7.2.1. The file name to use is the AID received in the historical bytes of the ATR.

7.3 Application specific commands to the IEP

7.3.1 List of default commands

Table 5 summarises the application specific commands an IEP has to perform in an IEP System in order to handle all defined transaction types.

Table 5 - List of IEP commands

Command	INS	P1	P2	Mandatory/ optional
Initialize IEP	'50'			
a) for Load		'00'	'00'	O
b) for Purchase		'01'	'00'	M
c) for Purchase Cancellation/IEPBalance Recovery		'02'	'00'	O
Credit IEP	'52'			
a) for Load		'00'	'00'	O
b) for Purchase Cancellation/IEPBalance Recovery		'01'	'00'	O
Debit IEP	'54'			
a) Purchase - first step		'00'	'00'	M
b) Purchase - subsequent steps		'01'	'00'	O
c) Purchase Acknowledgement		'02'	'00'	O
Get previous IEP Signature	'5A'	'00'	'00'	O
Monitor IEP ¹⁾	----- Out of scope of EN 1546-3 -----			

1) Depending on the implementation, the monitoring functionality may be implemented using one or more of the ISO defined commands: Read Binary, Read Record(s) and Get Data, or by using an application specific command not defined in this part of EN 1546.

7.3.2 Initialize IEP

7.3.2.1 Definition and scope

This command is used to initiate a new transaction with the IEP. Different formats are described as each transaction initialisation requires different data either for input or for output.

The following three variants exist:

- Initialize IEP for Load;
- Initialize IEP for Purchase;
- Initialize IEP for Purchase Cancellation/IEP Balance Recovery.

7.3.2.2 Command message

The command message for Initialize IEP for Load shall be coded according to table 6.

Table 6 - Command message for Initialize IEP for Load

Field	Value	Length (bytes)
CLA	'80'	1
INS	'50'	1
P1	'00'	1
P2	'00'	1
L _c	DD dependent	1
M _{LDA}	Amount to be loaded	4
CURRLDA	Currency Code	3
IDPPSAM / IDLDA ¹⁾	PPSAM identifier / LDA identifier	4
RPPSAM / RLDA ¹⁾	Random number from the PPSAM or an LDA	4
DD	Discretionary Data	variable
L _e	Maximum number of data bytes expected in the response	1 or 2

¹⁾ Data elements coming from the PPSAM or from an LDA if the transaction is initiated by the LDA without connection to the Purse Provider Host.

NOTE PP_{PPSAM} is not included because PP_{IEP} has already been exchanged during application selection and PP_{IEP} is implicitly equal to PP_{PPSAM}.

The command message for Initialize IEP for Purchase shall be coded according to table 7.

Table 7 - Command message for Initialize IEP for Purchase

Field	Value	Length (bytes)
CLA	'80'	1
INS	'50'	1
P1	'01'	1
P2	'00'	1
L _c	DD dependent (absent if no Discretionary Data is sent)	1 or absent
DD	Discretionary Data	variable
L _e	Maximum number of data bytes expected in the response	1 or 3

The command message for Initialize IEP for Purchase Cancellation/IEP Balance Recovery shall be coded according to table 8.

Table 8 - Command message for Initialize IEP for Purchase Cancellation/IEP Balance Recovery

Field	Value	Length (bytes)
CLA	'80'	1
INS	'50'	1
P1	'02'	1
P2	'00'	1
L _c	DD dependent (absent if no Discretionary Data is sent)	1 or absent
DD	Discretionary Data	variable
L _e	Maximum number of data bytes expected in the response	1 or 3

7.3.2.3 Response messages (nominal case)

The response message for Initialize IEP for Load shall be coded according to table 9.

Table 9 - Response message for Initialize IEP For Load

Field	Value	Length (bytes)
PP _{IEP}	Purse Provider identifier	3
ID _{IEP}	IEP identifier	5
ALG _{IEP}	Algorithm used by the IEP	1
DEXP _{IEP}	Expiry Date	3
BAL _{IEP}	Balance of the IEP	4
MT _{IEP}	Transaction number of the IEP	2
IK _{IEP}	Key information (algorithm dependent)	variable
S ₁	Signature of the IEP	variable
SW1-SW2	Status bytes (= CC _{IEP})	2

The response message for Initialize IEP for Purchase shall be coded according to table 10.

Table 10 - Response message for Initialize IEP For Purchase

Field	Value	Length (bytes)
PP _{IEP}	Purse Provider identifier	3
ID _{IEP}	IEP identifier	5
ALG _{IEP}	Algorithm used by the IEP	1
DEXP _{IEP}	Expiry date	3
BAL _{IEP}	Balance of the IEP	4
CURR _{IEP}	Currency Code	3
AM _{IEP}	Authentication mode of the IEP	1
NT _{IEP}	Transaction number of the IEP	2
IK _{IEP}	Key information (algorithm dependent)	variable
S ₁	Signature of the IEP (algorithm and AM dependent)	variable
SW1-SW2	Status bytes (= CC _{IEP})	2

The response message for Initialize IEP for Purchase Cancellation/IEP Balance Recovery shall be coded according to table 11.

Table 11 - Response message for Initialize IEP For Purchase Cancellation/IEP Balance Recovery

Field	Value	Length (bytes)
PP _{IEP}	Purse Provider identifier	3
ID _{IEP}	IEP identifier	5
ALG _{IEP}	Algorithm used by the IEP	1
DEXP _{IEP}	Expiry date	3
NT _{IEP}	Transaction number of the IEP	2
MTOT _{IEP(log)}	Total amount of the Purchase	4
MPDA(log)	Amount to be cancelled	4
CURRPDA(log)	Currency code	3
IDPSAM(log)	PSAM identifier of the latest Purchase	4
NTPSAM(log)	Transaction number of PSAM	4
IK _{IEP}	Key information (algorithm dependent)	variable
S ₁	Signature of the IEP	variable
SW1-SW2	Status bytes (= CC _{IEP})	2

7.3.2.4 Status conditions

The status conditions listed in table 12 may occur when handling the Initialize IEP for Load command.

Table 12 - Status conditions for Initialize IEP For Load

SW1	SW2	Meaning
'91'	'02'	NT has reached its limit
'94'	'01'	Currency not supported
'94'	'02'	Amount is too high for credit

The status conditions listed in table 13 may occur when handling the Initialize IEP for Purchase command.

Table 13 - Status conditions for Initialize IEP For Purchase

SW1	SW2	Meaning
'91'	'02'	NT has reached its limit

The status conditions listed in table 14 may occur when handling the Initialize IEP for Purchase Cancellation/IEP Balance Recovery command.

Table 14 - Status conditions for Initialize IEP For Purchase Cancellation/IEP Balance Recovery

SW1	SW2	Meaning
'91'	'02'	NT has reached its limit
'94'	'02'	Amount is too high for credit
'94'	'09'	Last transaction was not a Purchase
'95'	'04'	Corresponding Purchase was not successful
'95'	'05'	Corresponding Purchase has been cancelled

7.3.3 Credit IEP

7.3.3.1 Definition and scope

This command increments the IEP Balance during a Load IEP transaction or a Purchase Cancellation/IEP Balance Recovery transaction.

7.3.3.2 Command message

The command message for Credit IEP for Load shall be coded according to table 15.

Table 15 - Command message for Credit IEP for Load

Field	Value	Length (bytes)
CLA	'80'	1
INS	'52'	1
P1	'00'	1
P2	'00'	1
L _c	ALG and DD dependent	1 or 3
IK _{PPSAM}	PPSAM Key Information (algorithm dependent)	variable
S ₂ ¹⁾	Signature of the PPSAM (algorithm dependent)	variable
ID _{PPSAM} ²⁾	PPSAM identifier	4
R _{PPSAM} ²⁾	Random number computed by the PPSAM	4
DD	Discretionary Data	variable
L _e	Maximum number of data bytes expected in the response	1

1) Called S₃' in the Load with an LSAM as defined in EN 1546-2.

2) These data elements are only transmitted if initialization of the Load transaction is executed without connection to a PPSAM. In this case, the certificate (S₂) and the signed acknowledgement (S₃) will contain the data elements ID_{PPSAM} and R_{PPSAM}.

The command message for Recredit IEP for Purchase Cancellation/IEP Balance Recovery shall be coded according to table 16.

Table 16 - Command message for Recredit IEP for Purchase Cancellation/IEP Balance Recovery

Field	Value	Length (bytes)
CLA	'80'	1
INS	'52'	1
P1	'01'	1
P2	'00'	1
L _c	ALG dependent	1 or 3
IK _{PSAM}	PSAM Key Information (algorithm dependent)	variable
S ₂	Signature of the PSAM (algorithm dependent)	variable
DD	Discretionary Data	variable

7.3.3.3 Response messages (nominal case)

The response message for Credit IEP for Load shall be coded according to table 17.

This format shall also be used in the error conditions listed in table 19.