SLOVENSKI STANDARD
SIST EN 1546-3:2004

01-maj-2004

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

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

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

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

Ta slovenski standard je istoveten z: **EN 1546-3:1999**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST EN 1546-3:2004 **en**

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 1546-3

July 1999

ICS 35.240.15

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

Ref. No. EN 1546-3:1999 E

Contents

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 implement 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 European Standard, 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

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 II 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 S_1 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 $BALmax_{IEP}$.*

6.2.6 $BALmax_{IEP}$ (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.*