SLOVENSKI STANDARD
SIST EN 1546-4:2004

01-maj-2004

Identification card systems - Inter-sector electronic purse - Part 4: Data objects

Identification card systems - Inter-sector electronic purse - Part 4: Data objects

Identifikationskartensysteme - Branchenübergreifende elektronische Geldbörse - Teil 4: Datenobjekte

Systemes de cartes d'identification - Porte-monnaie électronique intersectoriel - Partie 4: Objets de données

Ta slovenski standard je istoveten z: **EN 1546-4:1999**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST EN 1546-4:2004 **en**

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 1546-4

August 1999

ICS 35.240.15

English version

Identification card systems – Inter-sector electronic purse

Part 4: Data objects

Systèmes de cartes d'identification – Portemonnaie électronique intersectoriel – Partie 4: Objets de données

Identifikationskartensysteme – Branchenübergreifende elektronische Geldbörse – Teil 4: Datenelemente

This European Standard was approved by CEN on 1999-07-29.

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.

The European Standards exist 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, the Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, and the United Kingdom.

CEN

European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

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

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 February 2000, and conflicting national standards shall be withdrawn at the latest by February 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 defines the Tag values required and describes the Dictionary mechanisms necessary for their utilisation in order to achieve interoperability between IEP Systems where Data Elements have different lengths and/or the ordering of Data Elements in commands and responses is different from that defined in EN 1546-3. The mechanisms are based on TLV (Tag-length-value) definitions of each Data Element.

Tags and mechanisms are also defined for handling Discretionary Data elements additional to those defined in EN 1546-3. The TLV mechanisms used are in accordance with ASN.1.

Examples of utilisation of Dictionaries are described in an informative Annex.

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

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

EN 1546-3:1995, *Identification card systems - Inter-sector electronic purse - Part 3: Data elements and interchanges.*

EN ISO 3166-1:1997, *Codes for the representation of names of countries and their subdivisions – Part 1 : Country codes (ISO 3166-1:1997).*

EN ISO/IEC 7816-4:1996, *Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange (ISO/IEC 7816-4 :1995).*

EN ISO/IEC 7816-6:1997, *Identification cards - Integrated circuit(s) cards with contacts - Part 6 : Interindustry data elements (ISO/IEC 7816-6:1996).*

ISO/IEC 8825 (all parts), *Information technology - ASN.1 encoding rules.*

ISO 8859-1:1987, Information processing - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1

3 Definitions, symbols and abbreviations

3.1 Terms defined in EN 1546-1

This part of EN 1546 uses the following terms defined in EN 1546-1:

a) acquirer ;

b) card issuer ;

c) currency exchange ;

d) currency exchange log ;

e) identity ;

f) inter-sector electronic purse (IEP) ;

g) IEP balance ;

h) IEP monitor ;

i) IEP system ;

j) load device ;

k) load log ;

l) load SAM; LSAM ;

m) purchase ;

n) purchase device ;

o) purchase log ;

p) purchase SAM; PSAM ;

q) purse provider SAM; PPSAM.

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

3.1.1 Terms defined in EN 1546-2

This part of EN 1546 uses the following terms defined in EN 1546-2 :

a) completion code ;

b) signature.

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

3.1.2 Terms defined in EN 1546-3

This part of EN 1546 uses the following terms defined in EN 1546-3:

a) discretionary data.

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

3.1.3 Terms specific to this part of EN 1546

For the purpose of this standard, the following definitions apply:

3.1.3.1
constructed data object
a data object where the value field itself is a data object (see EN ISO/IEC 7816-4:1996)

3.1.3.2
data element
as defined in EN 1546-3.

NOTE A data element may be presented in the value field of a data object (see EN ISO/IEC 7816-4:1996).

3.1.3.3
data object
a concatenation of the following string of bytes (see EN ISO/IEC 7816-4:1996)

— a mandatory tag field, referenced to as a tag;

— a mandatory length field indicating a length L;

— a conditional value field of L bytes (when L is not equal to '00').

3.1.3.4
dictionary
a set of headerlists defining the fixed formats used by the IEP

3.1.3.5
headerlist
a data element containing a concatenation of tag-length pairs without delimiters

3.1.3.6
primitive data object
a data object where the value field shall not be considered a data object

3.1.3.7
tag
a value identifying a given data element, either uniquely or in conjunction with one or more other tags

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

3.2 Symbols and abbrevations

A	vector (identifier for an ordered set of Data Elements)
n..m	the range from n to m (inclusive)
'0'..'9' and 'A'..'F'	the sixteen hexadecimal digits.

When formats of data elements are described, the following conventions are used :

b	binary
n x	numeric (BCD) coding of x digits, e.g. n 6 means 6 numerical digits (coded on 3 bytes)
an x	alpha-numeric coding of x characters (according to ISO 8859-1:1987)

ASN.1	abstract syntax notation, one
BCD	binary coded decimal
BER	basic encoding rules
DD	discretionary data
IC	integrated circuit
IEP	Inter-sector electronic purse
LDA	load device application
LSAM	load SAM
PDA	purchase device application
PSAM	purchase SAM
SAM	secure application module
TEHL	tag for an extended headerlist
THL	tag for a headerlist
TLV	tag - length - value
TOD	tag for operational data

4 Description of the Dictionary mechanism

When the default fixed message formats defined in EN 1546-3 are not used, the rules laid out in this part on EN 1546 shall be applied.

4.1 Introduction

The use of Dictionaries as defined in this part of EN 1546 is a method for implementing message formats in IEP Systems. It enables other lengths for some Data Elements, a different order of Data Elements in messages and the identification of which Discretionary Data elements (and their lengths) are included in the messages. The mechanism is based on TLV coding.

The IEP indicates whether TLV coding of Data Elements is required according to the value of the application profile of the IEP (AP_{IEP}). The exact details of coding AP_{IEP} are given in 4.2.

If the IEP supports TLV coding, the Data Elements sent in the messages as defined in EN 1546-3 can have lengths and ordering different from that defined in EN 1546-3. For each transaction type and optionally for each logfile, a Headerlist shall be defined and may be stored in the IEP.

Terminals can read the IEP's Headerlists whenever necessary using the Get Data command as defined in 4.7.

The Headerlists give all the information necessary to build and interpret the messages to and from the IEP as they consist of a number of Tag-length pairs, defining the presence and the order of each Data Element in a message/log record as well as its length.

Data Elements transmitted in the application-specific messages are not tagged, i.e. Tag and length fields are not transmitted, but shall conform to the fixed format and order defined in the corresponding Headerlist.

4.2 Indication of the use of TLV coding

The IEP shall indicate to the terminal equipment whether fixed formats, as defined in EN 1546-3 are used or not. Two bits (b4-b3) in the first byte of the Data Element AP_{IEP} are used for this purpose. Normally, the terminal equipment will receive this Data Element as part of the application selection.

The following four possible combinations exist for the coding of bits b4-b3 in AP_{IEP} :

— b4-b3 = 0 0: ASN.1-BER is not used (fixed formats according to EN 1546-3 are used) ;

— b4-b3 = 0 1: Headerlists for commands and responses are present in the IEP ;

— b4-b3 = 1 0: Headerlists for logfile layouts are present in the IEP (fixed formats are used) ;

— b4-b3 = 1 1: Headerlists for commands, responses and logfile layouts are present in the IEP.

4.3 Structure of the Headerlist

A Headerlist defines the list of Data Elements, their length and in which order they are concatenated in a message.

A Headerlist is either simple or extended.

A simple Headerlist comprises:

— a Tag-length pair, THL (Tag for a Headerlist), which identifies the Headerlist and its length ;

— an ordered set of Tag-length pairs, TODs (Tags for Operational Data), one for each Data Element of the message.

A simple Headerlist is a primitive Data Object as defined in ISO/IEC 8825.

An extended Headerlist comprises :

— a Tag-length pair, TEHL, which identifies the Headerlist and its length ;

— a Headerlist (simple or extended).

An extended Headerlist is a constructed Data Object as defined in ISO/IEC 8825.

For example, the Headerlist of the Purchase transaction specifies the Tag-length pairs for all the commands/responses belonging to this transaction. These are :

a) the Tag-length pairs in the Initialize IEP for Purchase command and response ;

b) the Tag-length pairs in the Debit IEP for Purchase command and response, first step ;

c) the Tag-length pairs in the Debit IEP for Purchase command and response, subsequent step ;

d) the Tag-length pairs in the Debit IEP for Purchase Acknowledgement command and response.

Headerlists are coded as shown in figure 1.

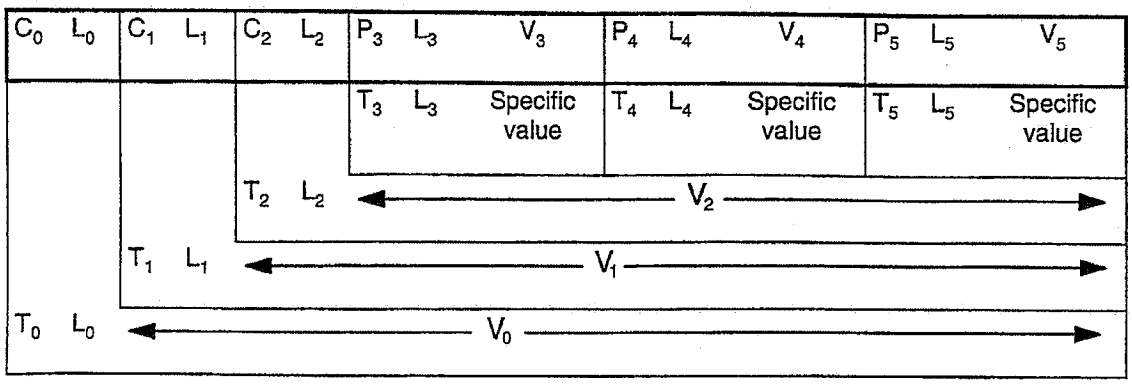

Figure 1 - Coding of a Headerlist

C_0, C_1, C_2 are Tags (T) of Constructed Data Objects with lengths L_0, L_1, L_2, and values V_0, V_1, V_2 respectively which define subsets of an IEP Headerlist and are compatible with ASN.1.

For example C_0 could be the Tag of the full Headerlist ('E5' in this standard), C1 could be the Tag of the type of transaction ('E7' for Purchase), and C_2 could be the Tag of the response message ('F1').

P_3, P_4, P_5 are tags of Primitive Data Objects with lengths L_3, L_4, L_5 and values, V_3, V_4 and V_5 respectively, which are specific to the IEP application Headerlist concept. These Primitive Tags define Data Elements of the IEP System and their origin ('D4' for Data Elements coming from IEP) and are compatible with ASN.1.

The specific values (V_3, V_4, V_5) are structured as follows and are *not* Data Objects.

Each specific value defines a Data Element referenced by a Tag and a length :

T	L

where T=Tag, L=length of the Data Element.

For example, the currency code of the IEP ($CURR_{IEP}$) can be coded as follows :

'5F2A'	'02'

The Tag of this Data Element is '5F2A' and the length is 2 bytes.

A specific value could also define a string of Tag-length pairs belonging to the same data vector and may be coded as follows :

T	L	T_1	L_1	T_2	L_2	...

where T = Tag of the Data Vector, L = length of the following Tag-length pairs, T_1L_1... the string of the individual Tag-length pairs.

For example, the IEP (public) key information vector of the IEP could be coded as follows :

'E0'	'0C'	'E1'	'0A'	'CA'	'03'	'CE'	'8180'	'5F24'	'03'	'CF'	'40'

'E0' is the Tag of the IEP key information vector with a length of 12 bytes and 'E1' is the Tag for a single block of a public key, its certificate and related data (10 bytes).

'CA', 'CE', '5F24', 'CF' are the tags of specific Data Elements: Purse Provider Identity, public key certificate, public key expiry date and public key respectively with the lengths of 3, 128, 3, 64 bytes, i.e. a public key of 512 bits with a certificate of 1024 bits.

For example the Discretionary Data Element vector could be coded as follows:

'E2'	'05'	'9A'	'03'	'9F21'	'03'	'E3'	'03'	'9F01'	'03'

'E2' is the Tag of the "Discretionary Data not to be signed" vector with a length of 6 bytes and 'E3' is the Tag of the "Discretionary Data to be signed" vector with a length of 3 bytes, whilst '9A', '9F21', '9F01' are the Tags of the specific Data Elements: transaction date, transaction time and Acquirer Identity respectively, all with lengths of 3 bytes.

Specific examples of the use of Headerlists are described in Annex A.

4.4 Coding of the Tag field

This subclause defines the rules needed to code the Tag field and lists specific Tag values assigned to Data Objects.

4.4.1 General rules

Tag values are assigned for all Data Objects used in this European Standard. These Tag values define either Primitive or Constructed Data Objects. Where appropriate, Tags assigned by ISO/IEC 7816-6 are used, all other Data Objects specific to the IEP application are defined by this European Standard.

The value of a Tag indicates whether the corresponding Data Object is Primitive or Constructed :

— if bit b6 in the first byte of the Tag is equal to 0, it is associated with a Primitive Data Object ;

— if bit b6 in the first byte of the Tag is equal to 1, it is associated with a Constructed Data Object.

A Tag can be either 1 or 2 bytes long :

— if bits b1-b5 of the first byte of the Tag are all equal to 1, the length is 2 bytes ;

— in all other cases, the length is 1 byte.

The coding of the first byte of the Tag is shown in table 1.

Table 1 - Structure of the first byte of a Tag

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	1	-	-	-	-	-	-	Tags assigned by EN ISO/IEC 7816-6:1997
1	1	-	-	-	-	-	-	Additional Tags defined in this part of EN 1546
-	-	0	-	-	-	-	-	Tags for Primitive Data Objects
-	-	1	-	-	-	-	-	Tags for Constructed Data Objects
-	-	-	1	1	1	1	1	The Tag is 2 bytes long. The value, in the range 31..127, is contained in the second byte
-	-	-	x	x	x	x	x	The Tag is 1 byte long. The value, in the range 0..30, is contained in b1-b5

4.4.2 Primitive Data Objects

The Primitive Data Objects listed in table 2 are the Data Elements defined in EN 1546-3. The format for these Data Elements are further defined in EN 1546-3.

Table 2 - Primitive Data Objects

Tag	Name	Description	Format	Length
'4F'	AID	Application identifier	n 10-32	5-16 bytes
'84'	(AID)	File name, e.g. AID, in File Control Information	b	var.
'C0'	ALG	Algorithm identifier	b	1-5 bytes
'C1'	AM	Authentication mode	bitmap	1 byte
'C2'	AP	Application profile	bitmap	2 bytes
'C3'	BAL	Balance	b	2-8 bytes
'C4'	BALmax	Maximum balance	b	2-8 bytes
'C5'	CC	Completion Code	b	2 bytes
'5F2A'	CURRC	Currency code	n 3	2 bytes
'5F36'	CURRE	Currency exponent	n 1	1 byte
'CE'	$C_nK^P_{(n-1)}$	Certificate for a public key	b	var.
'5F25'	DACT	Application activation date	n 6 YYMMDD	3 bytes
'C6'	DDEA	Application deactivation date	n 6 YYMMDD	3 bytes
'5F24'	DEXP	Application expiry date	n 6 YYMMDD	3 bytes
'C7'	ID	Identifier of the component	b	2-8 bytes
'CF'	K^P_n	Public key	b	var.
'C8'	M	Transaction amount (full or partial)	b	4-8 bytes
'C9'	MTOT	Total transaction amount (Purchase)	b	4-8 bytes
'5F32'	NT	Transaction number	b	2-8 bytes
'CA'	PP	Purse Provider (or key certification authority) id.	n 6	3 bytes
'CB'	R	Random number	b	4-8 bytes
'CC'	S_n	Signature	b	var.
'D2'	TRT	Transaction type and status	bitmap	1 byte
'CD'	VK	Key version	b	1-4 bytes