INTERNATIONAL STANDARD

ISO/IEC 7816-6

First edition
1996-05-15

Identification cards — Integrated circuit(s) cards with contacts —

Part 6:
Interindustry data elements

Cartes d'identification — Cartes à circuit(s) intégré(s) avec contacts —

Partie 6: Éléments de données interindustrielles

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC1. Draft International Standards adopted by the joint technical committee are circulated to the national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 7816-6 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Identification cards and related devices*.

ISO/IEC 7816 consists of the following parts, under the general title *Identification cards — Integrated circuit(s) cards with contacts*:

— *Part 1 : Physical characteristics*

— *Part 2 : Dimensions and location of the contacts*

— *Part 3 : Electronic signals and transmission protocols*

— *Part 4 : Interindustry commands for interchange*

— *Part 5 : Numbering system and registration procedure for application identifiers*

— *Part 6 : Interindustry data elements*

Annex A forms an integral part of this part of ISO/IEC 7816. Annex B is for information only.

Identification cards - Integrated circuit(s) cards with contacts -

Part 6:
Interindustry data elements

1 Scope

This part of ISO/IEC 7816 specifies directly or by reference the Data Elements (DE), including composite DEs, used in interindustry interchange, based on integrated circuit cards (ICCs).

It identifies the following characteristics of each DE:

— Identifier

— Name

— Description and ISO reference

— Format and coding (if not available in other ISO standards or parts of ISO/IEC 7816).

The layout of each DE is described as seen at the interface between the interface device (IFD) and the ICC. This part of ISO/IEC 7816 defines the means of retrieval of the DEs in the card (historical bytes, reset command(s) to perform and commands defined in this international standard).

This part of ISO/IEC 7816 provides the definition of DEs without consideration of any restrictions on the usage of the DEs.

It is intended that new interindustry data objects be incorporated into this standard; see clause 7 for the procedure to be followed.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 7816. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 7816 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of the IEC and ISO maintain registers of currently valid International Standards.

ISO 639: 1988, *Code for the representation of names of languages.*

ISO/IEC 646: 1991, *Information technology - ISO 7-bit coded character set for information interchange.*

ISO 3166: 1993, *Codes for the representation of names of countries.*

ISO 4217: 1995, *Codes for the representation of currencies and funds.*

ISO 4909: 1987, *Bank cards - Magnetic stripe data content for track 3.*

ISO/IEC 7501-1: 1993, *Identification cards - Machine readable travel documents - Part 1: Machine readable passport.*

ISO/IEC 7813: 1995, *Identification cards - Financial transaction cards.*

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

ISO/IEC 7816-5: 1994, *Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers.*

ISO 8583: 1993, *Financial transaction card originated messages - Interchange message specifications.*

ISO/IEC 8825-1: 1995, *Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*

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

ISO 9992-2:—[1], *Financial transaction cards - Messages between the Integrated Circuit Card and the Card Accepting Device - Part 2: Functions, messages (commands and responses), data elements and structures.*

ISO/IEC 10918-1: 1994, *Information technology - Digital compression and coding of continuous-tone still images: Requirements and guidelines.*

ISO/IEC 11544: 1993, *Information technology - Coded representation of picture and audio information - Progressive bi-level image compression.*

3   Definitions, abbreviations and notations

3.1 Definitions

For the purposes of this part of ISO/IEC 7816, the following definitions apply.

---

[1] To be published.

3.1.1 composite data element: a data element made up of a concatenation of zero, one or more data element(s).

3.1.2 data element: as defined in ISO/IEC 7816-4.

3.1.3 data object: as defined in ISO/IEC 7816-4.

3.1.4 element list: items of information concerning DEs.

3.1.5 headerlist: a concatenation of tag/length pairs without delimiters.

3.1.6 interindustry data element: data element for use in interindustry interchange.

3.1.7 interindustry data object: data object for use in interindustry interchange.

3.1.8 taglist: a concatenation of tag/length pairs without delimiters.

3.1.9 template: value field of a constructed data object, defined to give a logical grouping of data objects.

3.2 Abbreviations

For the purposes of this part of ISO/IEC 7816, the following abbreviations apply.

ASN.1	Abstract syntax notation one
ATR	Answer-to-reset
DE	Data element
DF	Dedicated file
DO	Data object
EF	Elementary file
FCI	File control information
ICC	Integrated circuit card
IDE	Interindustry data element
IDO	Interindustry data object
LRC	Longitudinal redundancy check
PIN	Personal identification number

3.3 Notations

a	alphabetic character
n	numeric, coded in binary coded decimal format
s	special character
an	alphanumeric character
ans	alphanumeric and special characters
...	between 2 numbers denotes a range of values.

Any number following the notations denotes the number of digits or characters. For example:

a3 means 3 alphabetic characters

n...3 means up to 3 binary coded decimal digits

n2...4 means 2, 3 or 4 binary coded decimal digits

4 Identification of Data Elements

4.1 Principles

The following principles apply to the identification of DEs:

4.1.1 For the purposes of this part of ISO/IEC 7816 a data element is generally presented in the value field of a data object.

4.1.2 For the purposes of this part of ISO/IEC 7816 a data object is a concatenation of the following string of bytes:

— a mandatory tag field, referred 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').

4.1.3 For purposes of retrieval and referencing in interchange:

— a DE shall be associated with the tag of a DO;

— the DE may be encapsulated in this DO.

4.1.4 The context according to which a DO is identified depends:

— either on the nesting of the DO in a template or;

— on the application currently selected.

4.1.5 When no application is selected all DOs shall be interpreted according to ISO/IEC 7816.

4.1.6   A DE may be referenced directly by its associated tag. It may be associated with another DE which indicates the context to which it belongs.

4.1.7   A DE may be referenced indirectly by one or more command to perform DOs.

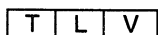**4.1.8** The DOs are described as seen at the interface between the ICC and the interface device.

4.1.9 Within ISO/IEC 7816 a tag denotes a type of DE.

4.1.10 There may be multiple occurrences of the same IDO in a card.
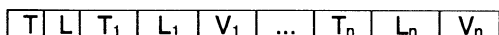
4.2 Data object structure

The following DO structures are supported:

— primitive DO

| T | L | V |

where T = Tag, L = Length, V = Value

— constructed DO

| T | L | T₁ | L₁ | V₁ | ... | Tₙ | Lₙ | Vₙ |

T	=	tag of constructed DO
L	=	length of the string (template) T_1 to V_n
$T_{1...n}$	=	tag of a $DO_{1...n}$
$L_{1...n}$	=	length of $V_{1...n}$
$V_{1...n}$	=	value of a $DO_{1...n}$

4.2.1 Structure of the tag

The tag consists of one or two bytes. The coding of these bytes shall be consistent with the basic encoding rules of ASN.1. Table 1 defines the first byte.

Table 1 - Structure of the first byte of the tag

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	-	-	-	-	-	-	Not defined in this part of ISO/IEC 7816
0	1	-	-	-	-	-	-	Defined in this part of ISO/IEC 7816. Application class, unambiguous identification
1	0	-	-	-	-	-	-	Defined in this part of ISO/IEC 7816 and only to be used within a template - see note below
1	1	-	-	-	-	-	-	Not defined in this part of ISO/IEC 7816. Reserved for private use
-	-	0	-	-	-	-	-	Primitive DO
-	-	1	-	-	-	-	-	Constructed DO
-	-	-	1	1	1	1	1	Tag number contained in the next byte - range 31..127
-	-	-	x	x	x	x	x	Tag number - range 0..30 Not all equal to 1

NOTE — Context dependent class tags (b8b7=10) are used out of templates for the file control information and secure messaging, see ISO/IEC 7816-4.

The coding of the second byte, when present, is:

b8   = 0

b7 to b1 = binary value of the tag number in the range 31..127

4.2.2 Structure of the length

All lengths are expressed in bytes.

The length consists of one or more bytes. The coding of these bytes shall be consistent with the basic encoding rules of ASN.1 and shall be as defined in table 2.

Table 2 - Coding of the length value

Range	# of bytes	1st byte	2nd byte	3rd byte
0..127	1	binary value	none	none
0..255	2	'81'	binary value	none
0..65,535	3	'82'	binary value ms byte	value ls byte

ms = most significant; ls = least significant

4.2.3 Format of the value

The format of the value depends on the type of the DE.

When the length of the DE is not expressed as a number of bytes, the mapping onto a byte string should be defined in the context of the respective DE (see clause 8). If not specified otherwise, the appropriate number of least significant bits of the last byte shall be set to 1.

4.3 Indirect DE referencing

The following IDOs are used:

— the wrapper, tag '63', constructed as described in 5.6;

— the DO taglist, tag '5C', the value of which is a (concatenation of) tag(s) without delimiter;

— the DO headerlist, tag '5D', the value of which is a concatenation of tag/lengths without delimiter;

— the element list, tag '5F41', only to be used within the wrapper, tag '63';

— the Command to Perform, tag '52', used as defined in ISO/IEC 7816-4;

— the path, tag '51', used as defined in ISO/IEC 7816-4.

4.4 Tag allocation schemes

ISO/IEC 7816-6 allocates some ASN.1-BER application class tags (context independent) as indicated in table 1. The default tag allocation scheme for IDOs in an ICC is defined in this part of ISO/IEC 7816 (see table 8).

4.4.1 Compatible tag allocation schemes

These tag allocation schemes use IDOs as defined in ISO/IEC 7816, and further DOs which

— either shall use context-dependent class tags (starting with 8 ,9, A, B) within templates defined in this part of ISO/IEC 7816 (templates '65', '66', '67', '6E');

— or shall be nested within templates with tags in the range '70' to '77'. Within these templates the meaning of application class tags is not defined in ISO/IEC 7816 except for the tags defined in table 4.

In order to identify a compatible tag allocation scheme and the authority responsible for the scheme, a Tag Allocation Authority DO with a tag of '78' (defined in 4.4.4) may be used.

If the tag allocation authority is only valid for data within a DF, then the FCI of the DF may contain the Tag Allocation Authority DO.

If the tag allocation authority is valid for the entire card then the DO may be present in the initial data string of the ATR file (as defined in ISO/IEC 7816-4).

An IDO listed in 4.4.4 may be included in the templates '70' to '77' indicating the authority responsible for the allocation of tags used in that template.

NOTE — the use of these schemes is either implicit (use of context dependent tags) or explicit (presence of the IDO with tag '78').

4.4.2 Coexistent tag allocation schemes

For these tag allocation schemes, DOs may use tags with another interpretation than ISO/IEC 7816.

In order to identify a coexistent tag allocation scheme, a Tag Allocation Authority DO with a tag of '79' (defined in 4.4.4) identifying the authority responsible for the scheme shall be used.

If the tag allocation authority is only valid for data within a DF then the FCI of the DF shall contain the Tag Allocation Authority DO.

If the tag allocation authority is valid for the entire card then the DO shall be present in the initial data string of the ATR file (as defined in ISO/IEC 7816-4).

All IDOs shall be nested within templates, tag '7E'. In such a scheme tags '79' and '7E' shall not be given another interpretation.

Besides '79' and '7E' the tags in table 3, defined in ISO/IEC 7816, shall not be reallocated by a coexistent tag allocation scheme:

Table 3 - Tags reserved for ISO/IEC

Tag	IDO
62	denotes file control parameters (FCP) template, as defined in ISO/IEC 7816-4
64	denotes file management data (FMD) template, as defined in ISO/IEC 7816-4
6F	denotes FCI template, as defined in ISO/IEC 7816-4
7D	reserved for secure messaging template of ISO/IEC 7816

4.4.3 Independent tag allocation schemes

For these tag allocation schemes DOs may use tags with another interpretation than ISO/IEC 7816, but which do not comply with 4.4.2. Such tag allocation schemes do not allow interindustry interchange and are not in compliance with ISO/IEC 7816-6.

A consistent use of the IDOs discretionary data, tag '53' and discretionary DOs, tag '73', allows the use of proprietary objects whilst remaining compliant to ISO/IEC 7816-6.

4.4.4 Tag allocation authority

Within templates '78' or '79' the IDOs shown in table 4 indicate which authority is responsible for tag allocation:

Table 4 - Tags for allocation of authorities

Tag	IDO
06	object identifier, as defined in ISO/IEC 8825, see example of coding in Annex B
41	defined in ISO/IEC 7816-4 and used to indicate at least a country
42	defined in ISO/IEC 7816-4 and used to indicate an issuer
4F	indicates an Application Identifier (AID), as defined in ISO/IEC 7816-5.

4

5 Retrieval of data

This clause defines standard retrieval procedures of DEs.

5.1 Principles

Before selecting an application, IDOs should be retrieved directly or indirectly from :

— the historical bytes;

— the initial data string;

— the ATR file;

— the Directory file (DIR file)

in the above order, when present.

These IDOs shall be interpreted according to clause 4.

Once an application is selected, IDOs should be retrieved directly or indirectly from:

— the FCI of the DF;

— other specific Elementary Files (EFs) within the current DF.

In this case these IDOs may also be retrieved by use of GET DATA command(s).

5.2 Retrieval of DOs after ATR

If indicated in the Historical Bytes, DOs may be retrieved after reset and possible Protocol Type Selection (PTS) by the use of the initial access data, according to ISO/IEC 7816-4.

All these DOs shall have tags complying with 4.4.

5.3 Retrieval of data in files

DOs may be retrieved in reserved files (DIR file and ATR file). This may be indicated in the historical bytes. Selection and reading of these files is defined in ISO/IEC 7816-4. The content of the DIR file is defined in ISO/IEC 7816-5. Information on the content of the ATR file is given in ISO/IEC 7816-4. All these DOs shall have tags defined by ISO/IEC 7816.

DEs may be retrieved in other files denoted by their path in a wrapper DE (see 5.6). Selection and reading of an EF known by its path is defined in ISO/IEC 7816-4.

5.4 Retrieval of data in FCI

Data may be present in the FCI according to ISO/IEC 7816-4.

5.5 Retrieval of data using the GET DATA command

DOs may be retrieved by use of the GET DATA command as defined in ISO/IEC 7816-4.

5.6 Indirect retrieval of DEs

For indirect referencing the wrapper DO is used. The wrapper DO has the tag '63', is constructed and shall consist of two parts:

the first part contains either

— the IDO taglist, tag '5C', denoting that the DEs to be retrieved are presented as DOs or;

— the IDO headerlist, tag '5D', denoting that the DEs to be retrieved are presented as a string of values, in the same order as in the taglist;

— the IDO element list, tag '5F41', denoting that the elements to be retrieved are not presented as DOs, but under application control. The structure of the element list as well as the information returned are outside the scope of ISO/IEC 7816.

the second part contains

— a path to an EF, tag '51';

— and/or one (or more) 'command to perform' DOs, tag '52', as defined in ISO/IEC 7816-5.

The following diagram is an example of a wrapper containing a taglist and one 'command to perform':

63	L	5C	L	Tag1, Tag2, Tag3...	52	L	CTP 1
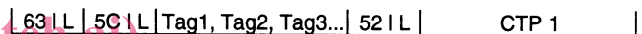
Only one indirect reference shall be given in a wrapper. There may be more than one wrapper.

A DO referenced according to ISO/IEC 7816 in the tag list, or a DE referenced another way in the DE list, shall be either

— contained in a file denoted by its path, see 5.3 for the retrieval or

— be (part of) the response to the last 'command to perform' indicated in the wrapper. The commands shall be executed in the order presented.

6 Coding of specific DEs

6.1 IDO 5B Name (of an individual)

A composite DE of variable length up to 39 characters, made up of:

— Surname (family name);

— Given name(s) (forename(s));

— Name suffix (e.g. Jr, number...);

— Filler(s)

as defined and used in ISO/IEC 7501-1. They shall be coded according to ISO/IEC 8859-1.

National languages with non-Latin characters shall be transliterated or transcribed into the Latin alphabet using the appropriate ISO standard.

In cases where:

— names cannot be shown in full;

— or a special alphabet is needed;

— or the transliteration or transcription is not sufficient

the IDO "qualified name" should be used.

6.2 IDO 6B Qualified name

A constructed DO of variable length, made up of:

— one or several object identifiers, tag '06', referring to the standards defining the presentation of the qualified name;

— a name tag '80' (primitive) or 'A0' (constructed), the value and coding of which is defined by the aforementioned standards;

— other related optional information, (e.g. sex, nationality, place of birth).

6.3 IDO 6A Log-in template

A log-in template is a constructed object of variable length. The value shall consist of one or more primitive objects such as qualifiers, numbers, text and times, as specified hereafter.

6.3.1 Qualifier

The tag shall be '80'. The value (1 to 9 bytes) shall consist of a mandatory first byte coding a rank followed by, at most, 8 optional bytes coding a mnemonic. This shall qualify the subsequent objects in a template, until the next qualifier, if any.

The rank is an integer valued from 0 to 255. If two or more qualifiers have the same rank within the same context, then only the set of objects qualified by the most recent one is valid.

The mnemonic is a string of 7-bit characters (b8 set to 0, see ISO/IEC 646) to be displayed at the man-machine interface.

6.3.2 Number

The tag shall be '81'. The value of the variable length shall consist of an even number of nibbles where each nibble codes one character for representing a telephone number, according to table 5.

Table 5 - Nibble decoding

Nibble	Character	Meaning
'0' to '9'	0 to 9	Decimal digits
'A'	(	Opening bracket
'B'	)	Closing bracket
'C'	C	Requirement for connecting to the line before continuing
'D'	+	Introduction of an international telephone number
'E'	-	If first, introduction of a number to be used without prefix; if not first, requirement for a delay (2 seconds) before continuing
'F'		Reserved for padding

6.3.3 Text

The tag shall be '82'. The value of the variable length shall consist of one or more bytes where each byte codes one character. The bit b8 sets the difference between data characters (b8 set to 0) and control characters (b8 set to 1). The string of bytes consists of one or more strings of data characters (7-bit character, see ISO/IEC 646) separated by strings of control characters. The following control characters are defined:

— '80' A message has to be received before sending the next character;

— 'C0' A modulation has to be present before sending the next character;

— '8X' X characters have to be received in echo before waiting for a message.

6.3.4 Time for end of message detection

The tag shall be '83'. The value shall consist of a single byte coding a time according to table 6. That time shall be used for detecting an end of message. The default value shall be 2 seconds.

6.3.5 Time for start of message detection

The tag shall be '84'. The value shall consist of a single byte coding a time according to table 6. That time shall be used for detecting an absence of response. The default value shall be 60 seconds.

Table 6 - Time decoding

b8	b7	b6	b5	b4	b3	b2	b1
⇐ RFU ⇒		⇐ Unit of ⇒		⇐ Number of units ⇒			

Time

b8-b7	Reserved for future use (RFU)
	(00 when not used)
b6-b5	Value of the unit of time
	00 = 100 ms
	01 = 1 second
	10 = 10 seconds
	11 = 100 seconds
b4-b1	Number of units

Moreover log-in data may be present with proprietary structures not specified by this International Standard. The tag '5E' is reserved for nesting such proprietary log-in data.

6.4 IDO 5F2F Coding of the PIN usage policy

The PIN usage policy DE consists of 2 bytes which indicate the tests to be performed by the terminal in order to determine whether a PIN is applicable to the current transaction, and, therefore, whether the terminal should prompt for the PIN to be entered. Bit 8 of the first byte, if set to 1, specifies that a PIN applies to this application and the terminal should prompt for the PIN. The meaning of the other 15 bits is application dependent. If all bits are set to 0, then the terminal should not prompt for the PIN.

If bit 8 of the first byte is on or if any of the tests performed indicate that a PIN applies, but the PIN cannot be presented, the action to be taken is application dependent.

6.5 IDO 6C Cardholder images

This constructed IDO contains at least one IDO as defined in this clause. An authority indicator (see 4.4.4) may precede such an IDO identifying the authority responsible for the data format of the IDO.

6.5.1 IDO 5F2E Cardholder biometric data

This IDO contains biometric data relating to the cardholder. Biometric data is designed to provide a means of verifying the claimed identity of the person presenting the card. Examples of biometric data are finger prints, palm prints, voice prints, dynamic signatures etc.

6.5.2 IDO 5F40 Cardholder portrait image

The format of the cardholder portrait image shall be as defined in ISO/IEC 10918-1, unless otherwise specified and/or requested by an authority.

6.5.3 IDO 5F43 Cardholder handwritten signature image

The format of the cardholder handwritten signature image shall be as defined in ISO/IEC 11544, unless otherwise specified and/or requested by an authority.

NOTE — It is recommended that the use of this IDO should be associated with appropriate security measures.

6.6 IDO 6D Application image template

This IDO contains at least an application image, tag 5F44. It may also contain an authority indicator (see 4.4.4) identifying the body responsible for the data format of the application image. When no authority is present the format shall be as defined in ISO/IEC 10918-1.

6.7 Magnetic stripe data

Tags '5F21', '5F22' and '5F23' are defined to be the card track 1, track 2 and track 3 DOs respectively. These tags shall be used when the data content of these DOs are identical to the data content of the corresponding tracks on the magnetic stripe of the card.

Tags '56', '57' and '58' are defined to be the application track 1, track 2 and track 3 DOs. These tags shall be used when the data format is as defined in ISO/IEC 7813 and ISO 4909 but the content may differ from that contained on the magnetic stripe of the card.

6.8 IDO 7F20 Display control

One or more IDOs may be contained in this template. The value of any IDO contained in this template, either directly or indirectly through constructed DOs, is not intended to be displayed and should only be used, when relevant, for processing of transmission.

6.9 Interchange profile

The specification of IDOs associated with the interchange profile of an ICC (eg available security functions and authentication methods) may be further detailed in future parts of ISO/IEC 7816.

The tags shown in table 7 are reserved for this purpose: