SLOVENSKI STANDARD
SIST EN ISO/IEC 7816-4:1998

01-junij-1998

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

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

Informationtechnologie - Identifikationskarten - Karten mit integrierten Schaltkreisen und Kontakten - Teil 4: Interindustrielle Kommandos (ISO/IEC 7816-4:1995)

Technologies de l'information - Cartes d'identification - Cartes a circuit(s) intégré(s) a contacts - Partie 4: Commandes intersectorielles pour les échanges (ISO/IEC 7816-4:1995)

Ta slovenski standard je istoveten z: **EN ISO/IEC 7816-4:1996**

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST EN ISO/IEC 7816-4:1998 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 7816-4

July 1996

ICS 35.240.40

Descriptors: See ISO document

English version

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

Technologies de l'information - Cartes d'identification - Cartes à circuit(s) intégré(s) à contacts - Partie 4: Commandes intersectorielles pour les échanges (ISO/IEC 7816-4:1995)

Informationstechnologie - Identifikationskarten - Karten mit integrierten Schaltkreisen und Kontakten - Teil 4: Interindustrielle Kommandos (ISO/IEC 7816-4:1995)

This European Standard was approved by CEN on 1996-05-22. 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, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CEN

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

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

Foreword

The text of the International Standard from Technical Committee ISO/IEC/JTC 1 "Information technology" of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) has been taken over as an European Standard by the Technical Board of CEN.

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 1997, and conflicting national standards shall be withdrawn at the latest by January 1997.

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

Endorsement notice

The text of the International Standard ISO/IEC 7816-4:1995 has been approved by CEN as a European Standard without any modification.

NOTE: Normative references to International Standards are listed in annex ZA (normative).

Annex ZA (normative)
Normative references to international publications with their relevant European publications

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.

Publication	Year	Title	EN	Year
ISO/IEC 7816-5	1994	Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers	EN ISO/IEC 7816-5	1996

INTERNATIONAL STANDARD

ISO/IEC 7816-4

First edition
1995-09-01

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

Part 4: Interindustry commands for interchange

Technologies de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts —

Partie 4: Commandes intersectorielles pour les échanges

Reference number
ISO/IEC 7816-4:1995(E)

Contents

Annexes

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 JTC 1. Draft International Standards adopted by the joint technical committee are circulated to 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 7816-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

ISO/IEC 7816 consists of the following parts, under the general title *Information technology — 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.*

Annexes A and B form an integral part of this part of ISO/IEC 7816. Annexes C, D, E and F are for information only.

Introduction

This part of ISO/IEC 7816 is one of a series of standards describing the parameters for integrated circuit(s) cards with contacts and the use of such cards for international interchange.

These cards are identification cards intended for information exchange negotiated between the outside and the integrated circuit in the card. As a result of an information exchange, the card delivers information (computation results, stored data), and/or modifies its content (data storage, event memorization).

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

Part 4:
Interindustry commands for interchange

1 Scope

This part of ISO/IEC 7816 specifies

— the content of the messages, commands and responses, transmitted by the interface device to the card and conversely,

— the structure and content of the historical bytes sent by the card during the answer to reset,

— the structure of files and data, as seen at the interface when processing interindustry commands for interchange,

— access methods to files and data in the card,

— a security architecture defining access rights to files and data in the card,

— methods for secure messaging,

— access methods to the algorithms processed by the card. It does not describe these algorithms.

It does not cover the internal implementation within the card and/or the outside world.

It allows further standardization of additional interindustry commands and security architectures.

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 IEC and ISO maintain registers of currently valid International Standards.

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

ISO/IEC 7812-1 : 1993, *Identification cards — Identification of issuers — Part 1 : Numbering system.*

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

Amendment 1 : 1992 to ISO/IEC 7816-3 : 1989, *Protocol type T=1, asynchronous half duplex block transmission protocol.*

Amendment 2 : 1994 to ISO/IEC 7816-3 : 1989, *Revision of protocol type selection.*

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

ISO/IEC 7816-6 : —[1], *Identification cards — Integrated circuit(s) cards with contacts — Part 6 : Interindustry data elements.*

ISO/IEC 8825 : 1990 [2], *Information technology — Open Systems Interconnection — Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

ISO/IEC 9796 : 1991, *Information technology — Security techniques — Digital signature scheme giving message recovery.*

ISO/IEC 9797 : 1994, *Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.*

ISO/IEC 9979 : 1991, *Data cryptographic techniques — Procedures for the registration of cryptographic algorithms.*

ISO/IEC 10116:1991, *Information technology — Modes of operation for an n-bit block cipher algorithm.*

ISO/IEC 10118-1 : 1994, *Information technology — Security techniques — Hash-functions — Part 1 : General.*

ISO/IEC 10118-2 : 1994, *Information technology — Security techniques — Hash-functions — Part 2 : Hash-functions using an n-bit block cipher algorithm.*

3 Definitions

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

3.1 Answer-to-Reset file : Elementary file which indicates operating characteristics of the card.

3.2 command-response pair : Set of two messages : a command followed by a response.

3.3 data unit : The smallest set of bits which can be unambiguously referenced.

3.4 data element : Item of information seen at the interface for which are defined a name, a description of logical content, a format and a coding.

3.5 data object : Information seen at the interface which consists of a tag, a length and a value (i.e., a data element). In this part of ISO/IEC 7816, data objects are referred to as BER-TLV, COMPACT-TLV and SIMPLE-TLV data objects.

3.6 dedicated file : File containing file control information and, optionally, memory available for allocation. It may be the parent of EFs and/or DFs.

3.7 DF name : String of bytes which uniquely identifies a dedicated file in the card.

3.8 directory file : Elementary file defined in part 5 of ISO/IEC 7816.

3.9 elementary file : Set of data units or records which share the same file identifier. It cannot be the parent of another file.

3.10 file control parameters : Logical, structural and security attributes of a file.

3.11 file identifier : A 2-bytes binary value used to address a file.

3.12 file management data : Any information about a file except the file control parameters (e.g., expiration date, application label).

3.13 internal elementary file : Elementary file for storing data interpreted by the card.

3.14 master file : The mandatory unique dedicated file representing the root of the file structure.

3.15 message : String of bytes transmitted by the interface device to the card or vice-versa, excluding transmission-oriented characters as defined in part 3 of ISO/IEC 7816.

3.16 parent file : The dedicated file immediately preceding a given file within the hierarchy.

3.17 password : Data which may be required by the application to be presented to the card by its user.

3.18 path : Concatenation of file identifiers without delimitation. If the path starts with the identifier of the master file, it is an absolute path.

3.19 provider : Authority who has or who obtained the right to create a dedicated file in the card.

3.20 record : String of bytes which can be handled as a whole by the card and referenced by a record number or by a record identifier.

3.21 record identifier : Value associated with a record that can be used to reference that record. Several records may have the same identifier within an elementary file.

3.22 record number : Sequential number assigned to each record which uniquely identifies the record within its elementary file.

3.23 working elementary file : Elementary file for storing data not interpreted by the card.

[1] To be published.
[2] Currently under revision.

4 Abbreviations and notation

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

APDU	Application protocol data unit
ATR	Answer to reset
BER	Basic encoding rules of ASN.1 (see annex D)
CLA	Class byte
DIR	Directory
DF	Dedicated file
EF	Elementary file
FCI	File control information
FCP	File control parameter
FMD	File management data
INS	Instruction byte
MF	Master file
P1-P2	Parameter bytes
PTS	Protocol type selection
RFU	Reserved for future use
SM	Secure messaging
SW1-SW2	Status bytes
TLV	Tag, length, value
TPDU	Transmission protocol data unit

For the purposes of this part of ISO/IEC 7816, the following notation applies.

'0' to '9' and 'A' to 'F'	The sixteen hexadecimal digits
(B_1)	Value of byte B_1
$B_1 \parallel B_2$	Concatenation of bytes B_1 (the most significant byte) and B_2 (the least significant byte)
$(B_1 \parallel B_2)$	Value of the concatenation of bytes B_1 and B_2
#	Number

5 Basic organizations

5.1 Data structures

This clause contains information on the logical structure of data as seen at the interface, when processing interindustry commands for interchange. The actual storage location of data and structural information beyond what is described in this clause are outside the scope of ISO/IEC 7816.

5.1.1 File organization

This part of ISO/IEC 7816 supports the following two categories of files.

— Dedicated file (DF).

— Elementary file (EF).

The logical organization of data in a card consists of the following structural hierarchy of dedicated files.

— The DF at the root is called the master file (MF). The MF is mandatory.

— The other DFs are optional.

The following two types of EFs are defined.

— Internal EF — Those EFs are intended for storing data interpreted by the card, i.e., data analyzed and used by the card for management and control purposes.

— Working EF — Those EFs are intended for storing data not interpreted by the card, i.e., data to be used by the outside world exclusively.

Figure 1 illustrates an example of the logical file organization in a card.

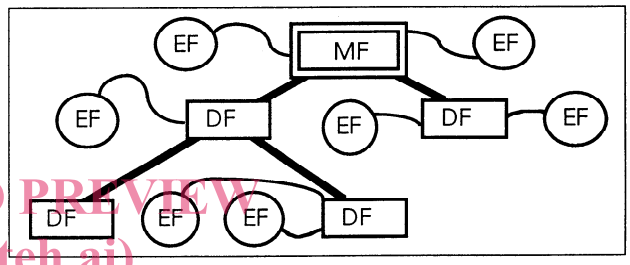

Figure 1 — Logical file organization (example)

5.1.2 File referencing methods

When a file cannot be implicitly selected, it shall be possible to select it by at least one of the following methods.

— **Referencing by file identifier** — Any file may be referenced by a file identifier coded on 2 bytes. If the MF is referenced by a file identifier, '3F00' shall be used (reserved value). The value 'FFFF' is reserved for future use. The value '3FFF' is reserved (see referencing by path). In order to select unambiguously any file by its identifier, all EFs and DFs immediately under a given DF shall have different file identifiers.

— **Referencing by path** — Any file may be referenced by a path (concatenation of file identifiers). The path begins with the identifier of the MF or of the current DF and ends with the identifier of the file itself. Between those two identifiers, the path consists of the identifiers of the successive parent DFs if any. The order of the file identifiers is always in the direction parent to child. If the identifier of the current DF is not known, the value '3FFF' (reserved value) can be used at the beginning of the path. The path allows an unambiguous selection of any file from the MF or from the current DF.

— **Referencing by short EF identifier** — Any EF may be referenced by a short EF identifier coded on 5 bits valued in the range from 1 to 30. The value 0 used as a short EF identifier references the currently selected EF. Short EF identifiers cannot be used in a path or as a file identifier (e.g., in a SELECT FILE command).

— **Referencing by DF name** — Any DF may be referenced by a DF name coded on 1 to 16 bytes. In order to select unambiguously by DF name (e.g., when selecting by means of application identifiers as defined in part 5 of ISO/IEC 7816), each DF name shall be unique within a given card.

5.1.3 Elementary file structures

The following structures of EFs are defined.

— Transparent structure — The EF is seen at the interface as a sequence of data units.

— Record structure — The EF is seen at the interface as a sequence of individually identifiable records.

The following attributes are defined for EFs structured in records.

— Size of the records : either fixed or variable.

— Organization of the records: either as a sequence (linear structure) or as a ring (cyclic structure).

The card shall support at least one of the following four methods for structuring EFs.

— Transparent EF.

— Linear EF with records of fixed size.

— Linear file with records of variable size.

— Cyclic EF with records of fixed size.

Figure 2 shows those four EF structures.

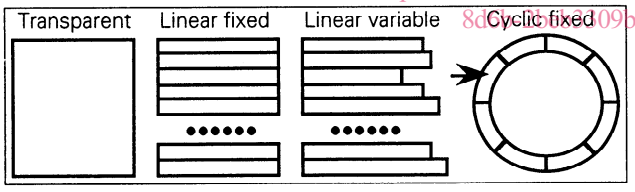

Figure 2 — EF structures

NOTE — The arrow on the figure references the most recently written record.

5.1.4 Data referencing methods

Data may be referenced as records, as data units or as data objects. Data is considered to be stored in a single continuous sequence of records (within an EF of record structure) or of data units (within an EF of transparent structure). Reference to a record or to a data unit outside an EF is an error.

Data referencing method, record numbering method and data unit size are EF-dependent features. The card can provide indications in the ATR, in the ATR file and in any file control information. When the card provides indications in several places, the indication valid for a given EF is the closest one to that EF within the path from the MF to that EF.

5.1.4.1 Record referencing

Within each EF of record structure, each record can be referenced by a record identifier and/or by a record number. Record identifiers and record numbers are unsigned 8-bit integers with values in the range from '01' to 'FE'. The value '00' is reserved for special purposes. The value 'FF' is RFU.

Referencing by record identifier shall induce the management of a record pointer. A reset of the card, a SELECT FILE and any command carrying a valid short EF identifier can affect the record pointer. Referencing by record number shall not affect the record pointer.

— **Referencing by record identifier** — Each record identifier is provided by an application. If a record is a SIMPLE-TLV data object in the data field of a message (see 5.4.4), then the record identifier is the first byte of the data object. Within an EF of record structure, records may have the same record identifier, in which case data contained in the records may be used for discriminating between them.

Each time a reference is made with a record identifier, an indication shall specify the logical position of the target record : the first or last occurrence, the next or previous occurrence relative to the record pointer.

— Within each EF of linear structure, the logical positions shall be sequentially assigned when writing or appending, i.e., in the order of creation. Therefore the first created record is in the first logical position.

— Within each EF of cyclic structure, the logical positions shall be sequentially assigned in the opposite order, i.e., the most recently created record is in the first logical position.

The following additional rules are defined for linear structures and for cyclic structures.

— The first occurrence shall be the record with the specified identifier and in the first logical position ; the last occurrence shall be the record with the specified identifier and in the last logical position.

— When there is no current record, the next occurrence shall be equivalent to the first occurrence ; the previous occurrence shall be equivalent to the last occurrence.

— When there is a current record, the next occurrence shall be the closest record with the specified identifier but in a greater logical position than the current record ; the previous occurrence shall be the closest record with the specified identifier but in a smaller logical position than the current record.

— The value '00' shall refer to the first, last, next or previous record in the numbering sequence, independently from the record identifier.

— **Referencing by record number** — Within each EF of record structure, the record numbers are unique and sequential.

— Within each EF of linear structure, the record numbers shall be sequentially assigned when writing or appending, i.e., in the order of creation. Therefore the first record (record number one, # 1) is the first created record.

— Within each EF of cyclic structure, the record numbers shall be sequentially assigned in the opposite order, i.e., the first record (record number one, # 1) is the most recently created record.

The following additional rule is defined for linear structures and for cyclic structures.

— The value '00' shall refer to the current record, i.e., that record fixed by the record pointer.

5.1.4.2 Data unit referencing

Within each EF of transparent structure, each data unit can be referenced by an offset (e.g., in READ BINARY command, see 6.1). It is an unsigned integer, limited to either 8 or 15 bits according to an option in the respective command. Valued to 0 for the first data unit of the EF, the offset is incremented by 1 for every subsequent data unit.

By default, i.e., if the card gives no indication, the size of the data unit is one byte.

NOTES

1 An EF of record structure may support data unit referencing and, in case it does, data units may contain structural information along with data, e.g., record numbers in a linear structure.

2 Within an EF of record structure, data unit referencing may not provide the intended result because the storage order of the records in the EF is not known, e.g., storage order in a cyclic structure.

5.1.4.3 Data object referencing

Each data object (as defined in 5.4.4) is headed by a tag which references it. Tags are specified in this part and other parts of ISO/IEC 7816.

5.1.5 File control information

The file control information (FCI) is the string of data bytes available in response to a SELECT FILE command. The file control information may be present for any file.

Table 1 introduces 3 templates intended for conveying file control information when coded as BER-TLV data objects.

— The FCP template is intended for conveying file control parameters (FCP), i.e., any BER-TLV data objects defined in table 2.

— The FMD template is intended for conveying file management data (FMD), i.e., BER-TLV data objects specified in other clauses of this part or in other parts of ISO/IEC 7816 (e.g., application label as defined in part 5 and application expiration date as defined in part 6).

— The FCI template is intended for conveying file control parameters and file management data.

Table 1 — Templates relevant to FCI

Tag	Value
'62'	File control parameters (FCP template)
'64'	File management data (FMD template)
'6F'	File control information (FCI template)

The 3 templates may be retrieved according to selection options of the SELECT FILE command (see table 59). If the FCP or FMD option is set, then the use of the corresponding template is mandatory. If the FCI option is set, then the use of the FCI template is optional.

Part of the file control information may additionally be present in a working EF under control of an application and referenced under tag '87'. The use of the FCP or FCI template is mandatory for the coding of file control information in such an EF.

File control information not coded according to this part of ISO/IEC 7816 may be introduced as follows.

— '00' or any value higher than '9F' — The coding of the subsequent string of bytes is proprietary.

— Tag = '53' — The value field of the data object consists of discretionary data not coded in TLV.

— Tag = '73' — The value field of the data object consists of discretionary BER-TLV data objects.