SLOVENSKI STANDARD

SIST ISO/IEC 7816-4:2005

01-februar-2005

Identifikacijski dokumenti – Kartice z integriranim vezjem – 4. del: Organizacija, varovanje in ukazi za izmenjavo

Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange

Cartes d'identification -- Cartes à circuit intégré -- Partie 4: Organisation, sécurité et commandes pour les échanges

Ta slovenski standard je istoveten z: ISO/IEC 7816-4:2005

ICS:

35.240.15	Identifikacijske kartice in sorodne naprave	Identification cards and related devices

SIST ISO/IEC 7816-4:2005 en

INTERNATIONAL STANDARD

ISO/IEC 7816-4

Second edition
2005-01-15

Identification cards — Integrated circuit cards —

Part 4: Organization, security and commands for interchange

Cartes d'identification — Cartes à circuit intégré —

Partie 4: Organisation, sécurité et commandes pour les échanges

Reference number
ISO/IEC 7816-4:2005(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

ISO/IEC 7816-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

This second edition cancels and replaces the first edition (ISO/IEC 7816-4:1995), and incorporates material extracted from ISO/IEC 7816-5:1994, ISO/IEC 7816-6:1996, ISO/IEC 7816-8:1999 and ISO/IEC 7816-9:2000. It also incorporates the Amendment ISO/IEC 7816-4:1995/Amd.1:1997.

In addition, material has been extracted from the first edition and moved to the third edition of ISO/IEC 7816-3, so that the transmission protocols T=0 and T=1 are now present only in ISO/IEC 7816-3, no longer in ISO/IEC 7816-4.

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

- *Part 1: Cards with contacts: Physical characteristics*
- *Part 2: Cards with contacts: Dimensions and location of the contacts*
- *Part 3: Cards with contacts: Electrical interface and transmission protocols*
- *Part 4: Organization, security and commands for interchange*
- *Part 5: Registration of application providers*
- *Part 6: Interindustry data elements for interchange*
- *Part 7: Interindustry commands for Structured Card Query Language (SCQL)*
- *Part 8: Commands for security operations*
- *Part 9: Commands for card management*
- *Part 10: Cards with contacts: Electronic signals and answer to reset for synchronous cards*
- *Part 11: Personal verification through biometric methods*
- *Part 12: Cards with contacts: USB electrical interface and operating procedures*
- *Part 15: Cryptographic information application*

Introduction

ISO/IEC 7816 is a series of standards specifying integrated circuit cards and the use of such cards for interchange. These cards are identification cards intended for information exchange negotiated between the outside world and the integrated circuit in the card. As a result of an information exchange, the card delivers information (computation result, stored data), and / or modifies its content (data storage, event memorization).

— Five parts are specific to cards with galvanic contacts and three of them specify electrical interfaces.

  - ISO/IEC 7816-1 specifies physical characteristics for cards with contacts.
  - ISO/IEC 7816-2 specifies dimensions and location of the contacts.
  - ISO/IEC 7816-3 specifies electrical interface and transmission protocols for asynchronous cards.
  - ISO/IEC 7816-10 specifies electrical interface and answer to reset for synchronous cards.
  - ISO/IEC 7816-12 specifies electrical interface and operating procedures for USB cards.

— All the other parts are independent from the physical interface technology. They apply to cards accessed by contacts and / or by radio frequency.

  - ISO/IEC 7816-4 specifies organization, security and commands for interchange.
  - ISO/IEC 7816-5 specifies registration of application providers.
  - ISO/IEC 7816-6 specifies interindustry data elements for interchange.
  - ISO/IEC 7816-7 specifies commands for structured card query language.
  - ISO/IEC 7816-8 specifies commands for security operations.
  - ISO/IEC 7816-9 specifies commands for card management.
  - ISO/IEC 7816-11 specifies personal verification through biometric methods.
  - ISO/IEC 7816-15 specifies cryptographic information application.

ISO/IEC 10536 [13] specifies access by close coupling. ISO/IEC 14443 [15] and ISO/IEC 15693 [17] specify access by radio frequency. Such cards are also known as contactless cards.

ISO and IEC draw attention to the fact that it is claimed that compliance with this document may involve the use of the following patents and the foreign counterparts.

JPN 2033906, *Portable electronic device*

JPN 2557838, *Integrated circuit card*

JPN 2537199, *Integrated circuit card*

JPN 2856393, *Portable electronic device*

JPN 2137026, *Portable electronic device*

JPN 2831660, *Portable electronic device*

DE 198 55 596, *Portable microprocessor-assisted data carrier that can be used with or without contacts*

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applications throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from:

Contact	Patent details
Toshiba Corporation Intellectual Property Division 1-1, Shibaura 1-Chome Minato-ku, Tokyo 105-8001, Japan	JPN 2033906 (priority date: 1986-02-18; publication date: 1996-03-19), FRA 8614996, KOR 44664 JPN 2557838 (priority date: 1986-02-18; publication date: 1996-09-05), FRA 8700343, GER 3700504, KOR 42243, USA 4841131 JPN 2537199 (priority date: 1986-06-20; publication date: 1996-07-08), FRA 8708646, FRA 8717770, USA 4833595, USA 4901276 JPN 2856393 (priority date: 1987-02-17; publication date: 1998-11-27), FRA 8801887, KOR 43929, USA 4847803 JPN 2137026 (priority date: 1987-02-20; publication date: 1998-06-26), JPN 3054119, FRA 8802046, KOR 44393, USA 4891506 JPN 2831660 (priority date: 1988-08-26; publication date: 1998-09-25), FRA 8911249, KOR 106290, USA 4988855
Orga Kartensysteme Gmbh Am Hoppenhof 33 D-33104 Paderborn Germany	DE 198 55 596 (priority date: 1998-12-02; publication date: 2000-06-29) Applications pending in Europe, Russia, Japan, China, USA, Brazil, Australia

Identification cards — Integrated circuit cards —

Part 4:
Organization, security and commands for interchange

1 Scope

This part of ISO/IEC 7816 specifies

- contents of command-response pairs exchanged at the interface,
- means of retrieval of data elements and data objects in the card,
- structures and contents of historical bytes to describe operating characteristics of the card,
- structures for applications and data in the card, as seen at the interface when processing commands,
- access methods to files and data in the card,
- a security architecture defining access rights to files and data in the card,
- means and mechanisms for identifying and addressing applications 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 or the outside world.

This part of ISO/IEC 7816 is independent from the physical interface technology. It applies to cards accessed by one or more of the following methods: contacts, close coupling and radio frequency.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts: Electrical interface and transmission protocols*

ISO/IEC 7816-6, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*

ISO/IEC 8825-1:2002, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
access rule
data element containing an access mode referring to an action and security conditions to fulfil before acting

3.2
Answer-to-Reset file
optional EF indicating operating characteristics of the card

3.3
application
structures, data elements and program modules needed for performing a specific functionality

3.4
application DF
structure hosting an application in a card

3.5
application identifier
data element (up to sixteen bytes) that identifies an application

3.6
application label
data element for use at the man-machine interface

3.7
application provider
entity providing the components that make up an application in the card

3.8
application template
set of application-relevant data objects including one application identifier data object

3.9
asymmetric cryptographic technique
cryptographic technique that uses two related operations: a public operation defined by public numbers or by a public key and a private operation defined by private numbers or by a private key (the two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation)

3.10
certificate
digital signature binding a particular person or object and its associated public key (the entity issuing the certificate also acts as tag allocation authority with respect to the data elements in the certificate)

3.11
command-response pair
set of two messages at the interface: a command APDU followed by a response APDU in the opposite direction

3.12
data element
item of information seen at the interface for which are specified a name, a description of logical content, a format and a coding

3.13
data object
information seen at the interface consisting of the concatenation of a mandatory tag field, a mandatory length field and a conditional value field

3.14
data unit
the smallest set of bits that can be unambiguously referenced within an EF supporting data units

3.15
dedicated file
structure containing file control information and, optionally, memory available for allocation

3.16
DF name
data element (up to sixteen bytes) that uniquely identifies a DF in the card

3.17
digital signature
data appended to, or cryptographic transformation of, a data string that proves the origin and the integrity of the data string and protects against forgery, e.g., by the recipient of the data string

3.18
directory file
optional EF containing a list of applications supported by the card and optional related data elements

3.19
elementary file
set of data units or records or data objects sharing the same file identifier and the same security attribute(s)

3.20
file
structure for application and / or data in the card, as seen at the interface when processing commands

3.21
file identifier
data element (two bytes) used to address a file

3.22
header list
concatenation of pairs of tag field and length field without delimitation

3.23
identification card
card identifying its holder and issuer, which may carry data required as input for the intended use of the card and for transactions based thereon
[ISO/IEC 7810[2]]

3.24
internal elementary file
EF for storing data interpreted by the card

3.25
key
sequence of symbols controlling a cryptographic operation (e.g., encipherment, decipherment, a private or a public operation in a dynamic authentication, signature production, signature verification)

3.26
master file
unique DF representing the root in a card using a hierarchy of DFs

3.27
offset
number sequentially referencing a data unit in an EF supporting data units, or a byte in a record

3.28
parent file
DF immediately preceding a given file within a hierarchy of DFs

3.29
password
data that may be required by the application to be presented to the card by its user for authentication purpose

3.30
path
concatenation of file identifiers without delimitation

3.31
private key
that key of an entity's asymmetric key pair that should only be used by that entity
[ISO/IEC 9798-1[8]]

3.32
provider
authority who has or who obtained the right to create a DF in the card

3.33
public key
that key of an entity's asymmetric key pair that can be made public
[ISO/IEC 9798-1[8]]

3.34
record
string of bytes referenced and handled by the card within an EF supporting records

3.35
record identifier
number used to reference one or more records within an EF supporting records

3.36
record number
sequential number that uniquely identifies each record within an EF supporting records

3.37
registered application provider identifier
data element (five bytes) that uniquely identifies an application provider

3.38
secret key
key used with symmetric cryptographic techniques by a set of specified entities
[ISO/IEC 11770-3[14]]

3.39
secure messaging
set of means for cryptographic protection of [parts of] command-response pairs

3.40
security attribute
condition of use of objects in the card including stored data and data processing functions, expressed as a data element containing one or more access rules

3.41
security environment
set of components required by an application in the card for secure messaging or for security operations

3.42
symmetric cryptographic technique
cryptographic technique using the same secret key for both the originator's and the recipient's operation (without the secret key, it is computationally infeasible to compute either operation)

3.43
tag list
concatenation of tag fields without delimitation

3.44
template
set of BER-TLV data objects forming the value field of a constructed BER-TLV data object

3.45
working elementary file
EF for storing data not interpreted by the card

4 Symbols and abbreviated terms

AID	application identifier
APDU	application protocol data unit
ARR	access rule reference
ASN.1	abstract syntax notation one (see ISO/IEC 8825-1)
AT	control reference template for authentication
ATR	Answer-to-Reset
BER	basic encoding rules of ASN.1 (see ISO/IEC 8825-1)
CCT	control reference template for cryptographic checksum
CLA	class byte
CRT	control reference template
CT	control reference template for confidentiality
DF	dedicated file
DIR	directory
DST	control reference template for digital signature
EF	elementary file
EF.ARR	access rule reference file

EF.ATR	Answer-to-Reset file
EF.DIR	directory file
FCI	file control information
FCP	file control parameter
FMD	file management data
HT	control reference template for hash-code
INS	instruction byte
KAT	control reference template for key agreement
L_c field	length field for coding the number N_c
LCS byte	life cycle status byte
L_e field	length field for coding the number N_e
MF	master file
N_c	number of bytes in the command data field
N_e	maximum number of bytes expected in the response data field
N_r	number of bytes in the response data field
PIX	proprietary application identifier extension
P1-P2	parameter bytes (inserted for clarity, the dash is not significant)
RFU	reserved for future use
RID	registered application provider identifier
SC	security condition
SCQL	structured card query language
SE	security environment
SEID byte	security environment identifier byte
SM	secure messaging
SW1-SW2	status bytes (inserted for clarity, the dash is not significant)
(SW1-SW2)	value of the concatenation of the bytes SW1 and SW2 (the first byte is the most significant byte)
TLV	tag, length, value
{T-L-V}	data object (inserted for clarity, the dashes and curly brackets are not significant)
'XX'	notation using the hexadecimal digits '0' to '9' and 'A' to 'F', equal to XX to the base 16

5 Organization for interchange

For organizing interchange, this clause specifies the following basic features.

1) Command-response pairs
2) Data objects
3) Structures for applications and data
4) Security architecture

5.1 Command-response pairs

Table 1 shows a command-response pair, namely a command APDU followed by a response APDU in the opposite direction (see ISO/IEC 7816-3). There shall be no interleaving of command-response pairs across the interface, i.e., the response APDU shall be received before initiating another command-response pair.

Table 1 — Command-response pair

Field	**Description**	**Number of bytes**
Command header	Class byte denoted CLA	1
	Instruction byte denoted INS	1
	Parameter bytes denoted P1-P2	2
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$	0, 1 or 3
Command data field	Absent if $N_c = 0$, present as a string of N_c bytes if $N_c > 0$	N_c
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$	0, 1, 2 or 3
Response data field	Absent if $N_r = 0$, present as a string of N_r bytes if $N_r > 0$	N_r (at most N_e)
Response trailer	Status bytes denoted SW1-SW2	2

In any command-response pair comprising both L_c and L_e fields (see ISO/IEC 7816-3), short and extended length fields shall not be combined: either both of them are short, or both of them are extended.

If the card explicitly states its capability of handling “extended L_c and L_e fields” (see Table 88, third software function table) in the historical bytes (see 8.1.1) or in EF.ATR (see 8.2.1.1), then the card handles short and extended length fields. Otherwise (default value), the card handles only short length fields.

N_c denotes the number of bytes in the command data field. The L_c field encodes N_c.

— If the L_c field is absent, then N_c is zero.

— A short L_c field consists of one byte not set to '00'.
  - From '01' to 'FF', the byte encodes N_c from one to 255.

— An extended L_c field consists of three bytes: one byte set to '00' followed by two bytes not set to '0000'.
  - From '0001' to 'FFFF', the two bytes encode N_c from one to 65 535.

N_e denotes the maximum number of bytes expected in the response data field. The L_e field encodes N_e.

— If the L_e field is absent, then N_e is zero.

— A short L_e field consists of one byte with any value.
  - From '01' to 'FF', the byte encodes N_e from one to 255.
  - If the byte is set to '00', then N_e is 256.

— An extended L_e field consists of either three bytes (one byte set to '00' followed by two bytes with any value) if the L_c field is absent, or two bytes (with any value) if an extended L_c field is present.
  - From '0001' to 'FFFF', the two bytes encode N_e from one to 65 535.
  - If the two bytes are set to '0000', then N_e is 65 536.

N_r denotes the number of bytes in the response data field. N_r shall be less than or equal to N_e. Therefore in any command-response pair, the absence of L_e field is the standard way for receiving no response data field. If the L_e field contains only bytes set to '00', then N_e is maximum, i.e., within the limit of 256 for a short L_e field, or 65 536 for an extended L_e field, all the available bytes should be returned.