BRITISH STANDARD

BS ISO/IEC 7816-4:2005 +A1:2008

Identification cards — Integrated circuit cards —

Part 4: Organization, security and commands for interchange

ICS 35.240.15

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSI Documents Document Sharing Hub British Standards

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

National foreword

This British Standard is the UK implementation of ISO/IEC 7816-4:2005+A1:2008. It supersedes BS ISO/IEC 7816-4:2005 which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to ISO/IEC text carry the number of the ISO/IEC amendment. For example, text altered by ISO/IEC amendment 1 is indicated by ⟩A1⟨ ⟨A1⟩.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2008

© BSI 2009

ISBN 978 0 580 65671 2

Amendments/corrigenda issued since publication

Date	Comments
31 August 2009	Implementation of ISO/IEC amendment 1:2008

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

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

AMENDEMENT 1: Activation et désactivation d'enregistrement

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

Contents

Page

Foreword ... iv
Introduction ... v
1 Scope ... 1
2 Normative references ... 1
3 Terms and definitions ... 2
4 Symbols and abbreviated terms ... 5
5 Organization for interchange ... 7
5.1 Command-response pairs ... 7
5.2 Data objects ... 13
5.3 Structures for applications and data ... 17
5.4 Security architecture ... 23
6 Secure messaging ... 29
6.1 SM fields and SM data objects ... 29
6.2 Basic SM data objects ... 30
6.3 Auxiliary SM data objects ... 32
6.4 SM impact on command-response pairs ... 36
7 Commands for interchange ... 37
7.1 Selection ... 37
7.2 Data unit handling ... 40
7.3 Record handling ... 42
7.4 Data object handling ... 51
7.5 Basic security handling ... 53
7.6 Transmission handling ... 60
8 Application-independent card services ... 60
8.1 Card identification ... 61
8.2 Application identification and selection ... 64
8.3 Selection by path ... 67
8.4 Data retrieval ... 68
8.5 Data element retrieval ... 68
8.6 Card-originated byte strings ... 70
Annex A (informative) Examples of object identifiers and tag allocation schemes ... 72
Annex B (informative) Examples of secure messaging ... 74
Annex C (informative) Examples of AUTHENTICATE functions by GENERAL AUTHENTICATE commands ... 81
Annex D (informative) Application identifiers using issuer identification numbers ... 85
Bibliography ... 86

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

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 13: Commands for application management in a multi-application environment*

— *Part 15: Cryptographic information application*

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

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,

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2005+A1:2008

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)*

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2005+A1:2008

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)

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2005+A1:2008

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2005+A1:2008

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.

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

If the process is aborted, then the card may become unresponsive. However if a response APDU occurs, then the response data field shall be absent and SW1-SW2 shall indicate an error.

P1-P2 indicates controls and options for processing the command. A parameter byte set to '00' generally provides no further qualification. There is no other general convention for encoding the parameter bytes.

General conventions are specified hereafter for encoding the class byte denoted CLA (see 5.1.1), the instruction byte denoted INS (see 5.1.2) and the status bytes denoted SW1-SW2 (see 5.1.3). In those bytes, the RFU bits shall be set to 0 unless otherwise specified.

5.1.1 Class byte

CLA indicates the class of the command. Due to specifications in ISO/IEC 7816-3, the value 'FF' is invalid. Bit 8 of CLA distinguishes between the interindustry class and the proprietary class.

Bit 8 set to 0 indicates the interindustry class. The values 000x xxxx and 01xx xxxx are specified hereafter. The values 001x xxxx are reserved for future use by ISO/IEC JTC 1/SC 17.

— Table 2 specifies 000x xxxx as the first interindustry values.
- Bits 8, 7 and 6 are set to 000.
- Bit 5 controls command chaining (see 5.1.1.1).
- Bits 4 and 3 indicate secure messaging (see 6).
- Bits 2 and 1 encode a logical channel number from zero to three (see 5.1.1.2).

Table 2 — First interindustry values of CLA

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	x	-	-	-	-	**Command chaining control** (see 5.1.1.1)
0	0	0	0	-	-	-	-	— The command is the last or only command of a chain
0	0	0	1	-	-	-	-	— The command is not the last command of a chain
0	0	0	-	x	x	-	-	**Secure messaging indication**
0	0	0	-	0	0	-	-	— No SM or no indication
0	0	0	-	0	1	-	-	— Proprietary SM format
0	0	0	-	1	0	-	-	— SM according to 6, command header not processed according to 6.2.3.1
0	0	0	-	1	1	-	-	— SM according to 6, command header authenticated according to 6.2.3.1
0	0	0	-	-	-	x	x	**Logical channel number from zero to three** (see 5.1.1.2)

— Table 3 specifies 01xx xxxx as further interindustry values.
- Bits 8 and 7 are set to 01.
- Bit 6 indicates secure messaging (see 6).
- Bit 5 controls command chaining (see 5.1.1.1).
- Bits 4 to 1 encode a number from zero to fifteen; this number plus four is the logical channel number from four to nineteen (see 5.1.1.2).

Table 3 — Further interindustry values of CLA

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	1	x	-	-	-	-	-	**Secure messaging indication**
0	1	0	-	-	-	-	-	— No SM or no indication
0	1	1	-	-	-	-	-	— SM according to 6, command header not processed according to 6.2.3.1
0	1	-	x	-	-	-	-	**Command chaining control** (see 5.1.1.1)
0	1	-	0	-	-	-	-	— The command is the last or only command of a chain
0	1	-	1	-	-	-	-	— The command is not the last command of a chain
0	1	-	-	x	x	x	x	**Logical channel number from four to nineteen** (see 5.1.1.2)

Bit 8 set to 1 indicates the proprietary class, except for the value 'FF' which is invalid. The application-context defines the other bits.

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

5.1.1.1 Command chaining

This clause specifies a mechanism whereby in the interindustry class, consecutive command-response pairs can be chained. The mechanism may be used when executing a multi-step process, e.g., transmitting a data string too long for a single command.

If the card supports the mechanism, then it shall indicate it (see Table 88, third software function table) in the historical bytes (see 8.1.1) or in EF.ATR (see 8.2.1.1).

This document specifies the card behaviour only in the case where, once initiated, a chain is terminated before initiating a command-response pair not part of the chain. Otherwise the card behaviour is not specified.

For chaining in the interindustry class, bit 5 of CLA shall be used while the other seven bits are constant.

— If bit 5 is set to 0, then the command is the last or only command of a chain.

— If bit 5 is set to 1, then the command is not the last command of a chain.

In response to a command that is not the last command of a chain, SW1-SW2 set to '9000' means that the process has been completed so far; warning indications are prohibited (see 5.1.3); moreover, the following specific error conditions may occur.

— If SW1-SW2 is set to '6883', then the last command of the chain is expected.

— If SW1-SW2 is set to '6884', then command chaining is not supported.

5.1.1.2 Logical channels

This clause specifies a mechanism whereby in the interindustry class, command-response pairs can refer to logical channels.

If the card supports the mechanism, then it shall indicate the maximum number of available channels (see Table 88, third software function table) in the historical bytes (see 8.1.1) or in EF.ATR (see 8.2.1.1).

— If the indicated number is four or less, then only Table 2 applies.

— If the indicated number is five or more, then Table 3 also applies.

For referring to logical channels in the interindustry class, the following rules apply.

— CLA encodes the channel number of the command-response pair.

— The basic channel shall be permanently available, i.e., it cannot be closed. Its channel number is zero.

— Cards not supporting the mechanism (default value) shall use only the basic channel.

— Any other channel shall be opened by completion of either a SELECT command (see 7.1.1) where CLA encodes a channel number not yet in use, or a MANAGE CHANNEL command with open function (see 7.1.2).

— Any other channel can be closed by the completion of a MANAGE CHANNEL command with close function. After closing, the channel shall be available for re-use.

— Only one channel shall be active at a time. The use of logical channels does not remove the prohibition of interleaving command-response pairs across the interface, i.e., the response APDU shall be received before initiating another command-response pair (see 5.1).

— If not explicitly excluded by the file descriptor byte (see Table 14), more than one channel may be opened to the same structure (see 5.3), i.e., to a DF, possibly an application DF, and also possibly to an EF.

Each logical channel has its own security status (see 5.4). The way to share a security status is outside the scope of this document.

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

5.1.2 Instruction byte

INS indicates the command to process. Due to specifications in ISO/IEC 7816-3, the values '6X' and '9X' are invalid.

Table 4 lists all the commands specified in ISO/IEC 7816 at the time of publication.

— Table 4.1, i.e., the left side, lists the command names in the alphabetic order.

— Table 4.2, i.e., the right side, lists the INS codes in the numeric order.

Table 4.1 — Commands in the alphabetic order

Command name	INS	See
ACTIVATE FILE	'44'	Part 9
APPEND RECORD	'E2'	7.3.7
CHANGE REFERENCE DATA	'24'	7.5.7
CREATE FILE	'E0'	Part 9
DEACTIVATE FILE	'04'	Part 9
DELETE FILE	'E4'	Part 9
DISABLE VERIFICATION REQUIREMENT	'26'	7.5.9
ENABLE VERIFICATION REQUIREMENT	'28'	7.5.8
ENVELOPE	'C2', 'C3'	7.6.2
ERASE BINARY	'0E', '0F'	7.2.7
ERASE RECORD (S)	'0C'	7.3.8
EXTERNAL (/ MUTUAL) AUTHENTICATE	'82'	7.5.4
GENERAL AUTHENTICATE	'86', '87'	7.5.5
GENERATE ASYMMETRIC KEY PAIR	'46'	Part 8
GET CHALLENGE	'84'	7.5.3
GET DATA	'CA', 'CB'	7.4.2
GET RESPONSE	'C0'	7.6.1
INTERNAL AUTHENTICATE	'88'	7.5.2
MANAGE CHANNEL	'70'	7.1.2
MANAGE SECURITY ENVIRONMENT	'22'	7.5.11
PERFORM SCQL OPERATION	'10'	Part 7
PERFORM SECURITY OPERATION	'2A'	Part 8
PERFORM TRANSACTION OPERATION	'12'	Part 7
PERFORM USER OPERATION	'14'	Part 7
PUT DATA	'DA', 'DB'	7.4.3
READ BINARY	'B0', 'B1'	7.2.3
READ RECORD (S)	'B2', 'B3'	7.3.3
RESET RETRY COUNTER	'2C'	7.5.10
SEARCH BINARY	'A0', 'A1'	7.2.6
SEARCH RECORD	'A2'	7.3.7
SELECT	'A4'	7.1.1
TERMINATE CARD USAGE	'FE'	Part 9
TERMINATE DF	'E6'	Part 9
TERMINATE EF	'E8'	Part 9
UPDATE BINARY	'D6', 'D7'	7.2.5
UPDATE RECORD	'DC', 'DD'	7.3.5
VERIFY	'20', '21'	7.5.6
WRITE BINARY	'D0', 'D1'	7.2.4
WRITE RECORD	'D2'	7.3.4

Table 4.2 — Commands in the numeric order

INS	Command name	See
'04'	DEACTIVATE FILE	Part 9
'0C'	ERASE RECORD (S)	7.3.8
'0E', '0F'	ERASE BINARY	7.2.7
'10'	PERFORM SCQL OPERATION	Part 7
'12'	PERFORM TRANSACTION OPERATION	Part 7
'14'	PERFORM USER OPERATION	Part 7
'20', '21'	VERIFY	7.5.6
'22'	MANAGE SECURITY ENVIRONMENT	7.5.11
'24'	CHANGE REFERENCE DATA	7.5.7
'26'	DISABLE VERIFICATION REQUIREMENT	7.5.9
'28'	ENABLE VERIFICATION REQUIREMENT	7.5.8
'2A'	PERFORM SECURITY OPERATION	Part 8
'2C'	RESET RETRY COUNTER	7.5.10
'44'	ACTIVATE FILE	Part 9
'46'	GENERATE ASYMMETRIC KEY PAIR	Part 8
'70'	MANAGE CHANNEL	7.1.2
'82'	EXTERNAL (/ MUTUAL) AUTHENTICATE	7.5.4
'84'	GET CHALLENGE	7.5.3
'86', '87'	GENERAL AUTHENTICATE	7.5.5
'88'	INTERNAL AUTHENTICATE	7.5.2
'A0', 'A1'	SEARCH BINARY	7.2.6
'A2'	SEARCH RECORD	7.3.7
'A4'	SELECT	7.1.1
'B0', 'B1'	READ BINARY	7.2.3
'B2', 'B3'	READ RECORD (S)	7.3.3
'C0'	GET RESPONSE	7.6.1
'C2', 'C3'	ENVELOPE	7.6.2
'CA', 'CB'	GET DATA	7.4.2
'D0', 'D1'	WRITE BINARY	7.2.6
'D2'	WRITE RECORD	7.3.4
'D6', 'D7'	UPDATE BINARY	7.2.5
'DA', 'DB'	PUT DATA	7.4.3
'DC', 'DD'	UPDATE RECORD	7.3.5
'E0'	CREATE FILE	Part 9
'E2'	APPEND RECORD	7.3.6
'E4'	DELETE FILE	Part 9
'E6'	TERMINATE DF	Part 9
'E8'	TERMINATE EF	Part 9
'FE'	TERMINATE CARD USAGE	Part 9

— In the interindustry class, any valid INS code not defined in ISO/IEC 7816 is reserved for future use by ISO/IEC JTC 1/SC 17.

ISO/IEC 7816 specifies the use of those commands in the interindustry class.

— This document (see 7) specifies commands for interchange.

— ISO/IEC 7816-7[4] specifies commands for structured card query language (SCQL).

— ISO/IEC 7816-8[4] specifies commands for security operations.

— ISO/IEC 7816-9[4] specifies commands for card management.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2005+A1:2008

In the interindustry class, bit 1 of INS indicates a data field format as follows.

— If bit 1 is set to 0 (even INS code), then no indication is provided.

— If bit 1 is set to 1 (odd INS code), then BER-TLV encoding (see 5.2.2) shall apply as follows.

- In unchained commands with SW1 not set to '61', data fields, if any, shall be encoded in BER-TLV.
- Command chaining and / or the use of SW1 set to '61' allow the transmission of data strings too long for a single command. Such a process may split data objects in data fields consecutively sent as a sequence in one direction, i.e., while sending no data field in the opposite direction. When chaining commands and / or using SW1 set to '61', the concatenation of all the consecutive data fields in the same direction in the same sequence shall be encoded in BER-TLV.

5.1.3 Status bytes

SW1-SW2 indicates the processing state. Due to specifications in ISO/IEC 7816-3, any value different from '6XXX' and '9XXX' is invalid; any value '60XX' is also invalid.

The values '61XX', '62XX', '63XX', '64XX', '65XX', '66XX', '68XX', '69XX', '6AXX' and '6CXX' are interindustry. Due to specifications in ISO/IEC 7816-3, the values '67XX', '6BXX', '6DXX', '6EXX', '6FXX' and '9XXX' are proprietary, except the values '6700', '6B00', '6D00', '6E00', '6F00' and '9000' that are interindustry.

Figure 1 shows the structural scheme of the values '9000' and '61XX' to '6FXX' for SW1-SW2.

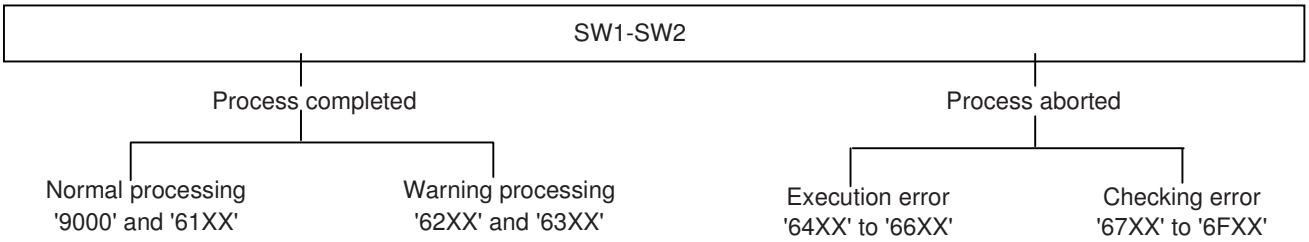

Figure 1 — Structural scheme of values of SW1-SW2

Table 5 lists all the interindustry values of SW1-SW2 and shows their general meaning. ISO/IEC JTC 1/SC 17 reserves for future use any interindustry value of SW1-SW2 not defined in ISO/IEC 7816.

Table 5 — General meaning of the interindustry values of SW1-SW2

	SW1-SW2	Meaning
Normal processing	'9000' '61XX'	No further qualification SW2 encodes the number of data bytes still available (see text below)
Warning processing	'62XX' '63XX'	State of non-volatile memory is unchanged (further qualification in SW2) State of non-volatile memory has changed (further qualification in SW2)
Execution error	'64XX' '65XX' '66XX'	State of non-volatile memory is unchanged (further qualification in SW2) State of non-volatile memory has changed (further qualification in SW2) Security-related issues
Checking error	'6700' '68XX' '69XX' '6AXX' '6B00' '6CXX' '6D00' '6E00' '6F00'	Wrong length; no further indication Functions in CLA not supported (further qualification in SW2) Command not allowed (further qualification in SW2) Wrong parameters P1-P2 (further qualification in SW2) Wrong parameters P1-P2 Wrong L_e field; SW2 encodes the exact number of available data bytes (see text below) Instruction code not supported or invalid Class not supported No precise diagnosis

If the process is aborted with a value of SW1 from '64' to '6F', then the response data field shall be absent.

If SW1 is set to '63' or '65', then the state of the non-volatile memory has changed. If SW1 is set to '6X' except for '63' and '65', then the state of the non-volatile memory is unchanged.

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

In response to a command that is not the last command of a chain (see 5.1.1.1), interindustry warning indications are prohibited (see also ISO/IEC 7816-3), i.e., SW1 shall be set to neither '62' nor '63'.

Two interindustry values of SW1 are independent from any transmission protocol.

— If SW1 is set to '61', then the process is completed and before issuing any other command, a GET RESPONSE command may be issued with the same CLA and using SW2 (number of data bytes still available) as short L_e field.

— If SW1 is set to '6C', then the process is aborted and before issuing any other command, the same command may be re-issued using SW2 (exact number of available data bytes) as short L_e field.

Table 6 lists all the specific interindustry warning and error conditions used in ISO/IEC 7816 at the time of publication.

Table 6 — Specific interindustry warning and error conditions

SW1	SW2	Meaning
'62' (warning)	'00'	No information given
	'02' to '80'	Triggering by the card (see 8.6.1)
	'81'	Part of returned data may be corrupted
	'82'	End of file or record reached before reading N_e bytes
	'83'	Selected file deactivated
	'84'	File control information not formatted according to 5.3.3
	'85'	Selected file in termination state
	'86'	No input data available from a sensor on the card
	〚A1〛 '87'	At least one of the referenced records is deactivated 〚A1〛
'63' (warning)	'00'	No information given
	'81'	File filled up by the last write
	'CX'	Counter from 0 to 15 encoded by 'X' (exact meaning depending on the command)
'64' (error)	'00'	Execution error
	'01'	Immediate response required by the card
	'02' to '80'	Triggering by the card (see 8.6.1)
'65' (error)	'00'	No information given
	'81'	Memory failure
'68' (error)	'00'	No information given
	'81'	Logical channel not supported
	'82'	Secure messaging not supported
	'83'	Last command of the chain expected
	'84'	Command chaining not supported
'69' (error)	'00'	No information given
	'81'	Command incompatible with file structure
	'82'	Security status not satisfied
	'83'	Authentication method blocked
	'84'	Reference data not usable
	'85'	Conditions of use not satisfied
	'86'	Command not allowed (no current EF)
	'87'	Expected secure messaging data objects missing
	'88'	Incorrect secure messaging data objects
'6A' (error)	'00'	No information given
	'80'	Incorrect parameters in the command data field
	'81'	Function not supported
	'82'	File or application not found
	'83'	Record not found
	'84'	Not enough memory space in the file
	'85'	N_c inconsistent with TLV structure
	'86'	Incorrect parameters P1-P2
	'87'	N_c inconsistent with parameters P1-P2
	'88'	Referenced data or reference data not found (exact meaning depending on the command)
	'89'	File already exists
	'8A'	DF name already exists
— Any other value of SW2 is reserved for future use by ISO/IEC JTC 1/SC 17.		

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2005+A1:2008

5.2 Data objects

If encoded in TLV, any data field, or concatenation of data fields, is a sequence of data objects. This clause specifies two categories of data objects: SIMPLE-TLV data objects and BER-TLV data objects.

5.2.1 SIMPLE-TLV data objects

Each SIMPLE-TLV data object shall consist of two or three consecutive fields: a mandatory tag field, a mandatory length field and a conditional value field. A record (see 7.3.1) may be a SIMPLE-TLV data object.

— The tag field consists of a single byte encoding a tag number from 1 to 254. The values '00' and 'FF' are invalid for tag fields. If a record is a SIMPLE-TLV data object, then the tag may be used as record identifier.

— The length field consists of one or three consecutive bytes.
  - If the first byte is not set to 'FF', then the length field consists of a single byte encoding a number from zero to 254 and denoted N.
  - If the first byte is set to 'FF', then the length field continues on the subsequent two bytes with any value encoding a number from zero to 65 535 and denoted N.

— If N is zero, there is no value field, i.e., the data object is empty. Otherwise (N > 0), the value field consists of N consecutive bytes.

5.2.2 BER-TLV data objects

Each BER-TLV data object consists of two or three consecutive fields (see the basic encoding rules of ASN.1 in ISO/IEC 8825-1): a mandatory tag field, a mandatory length field and a conditional value field.

— The tag field consists of one or more consecutive bytes. It indicates a class and an encoding and it encodes a tag number. The value '00' is invalid for the first byte of tag fields (see ISO/IEC 8825-1).

— The length field consists of one or more consecutive bytes. It encodes a length, i.e., a number denoted N.

— If N is zero, there is no value field, i.e., the data object is empty. Otherwise (N > 0), the value field consists of N consecutive bytes.

5.2.2.1 BER-TLV tag fields

ISO/IEC 7816 supports tag fields of one, two and three bytes; longer tag fields are reserved for future use.

Bits 8 and 7 of the first byte of the tag field indicate a class.

— The value 00 indicates a data object of the universal class.

— The value 01 indicates a data object of the application class.

— The value 10 indicates a data object of the context-specific class.

— The value 11 indicates a data object of the private class.

Bit 6 of the first byte of the tag field indicates an encoding.

— The value 0 indicates a primitive encoding of the data object, i.e., the value field is not encoded in BER-TLV.

— The value 1 indicates a constructed encoding of the data object, i.e., the value field is encoded in BER-TLV.

If bits 5 to 1 of the first byte of the tag field are not all set to 1, then they encode a tag number from zero to thirty and the tag field consists of a single byte.

Otherwise (bits 5 to 1 all set to 1), the tag field continues on one or more subsequent bytes.

— Bit 8 of each subsequent byte shall be set to 1, unless it is the last subsequent byte.

— Bits 7 to 1 of the first subsequent byte shall not be all set to 0.

— Bits 7 to 1 of the first subsequent byte, followed by bits 7 to 1 of each further subsequent byte, up to and including bits 7 to 1 of the last subsequent byte encode a tag number.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

Table 7 shows the first byte of the tag field. The value '00' is invalid.

Table 7 — First byte of BER-TLV tag fields in ISO/IEC 7816

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	-	-	-	-	-	-	Universal class, not defined in ISO/IEC 7816
0	1	-	-	-	-	-	-	Application class, identification defined in this document
1	0	-	-	-	-	-	-	Context-specific class, defined in ISO/IEC 7816
1	1	-	-	-	-	-	-	Private class, not defined in ISO/IEC 7816
-	-	0	-	-	-	-	-	Primitive encoding
-	-	1	-	-	-	-	-	Constructed encoding
-	-	-	Not all set to 1					Tag number from zero to thirty (short tag field, i.e., a single byte)
-	-	-	1	1	1	1	1	Tag number greater than thirty (long tag field, i.e., two or three bytes)

In data fields encoded in BER-TLV, bytes set to '00' may be present before, between or after data objects (e.g., due to erasure or modification of data objects within an EF supporting data units). Such padding is prohibited within value fields of constructed data objects, called “templates” in ISO/IEC 7816.

When present in the historical bytes (see 8.1.1) or in EF.ATR (see 8.2.1.1) or in the control information of any file (see tag '82' in Table 12), the data coding byte (see Table 87) indicates whether the value 'FF' is

— valid for the first byte of long tag fields of the private class, constructed encoding (explicit statement), or

— invalid for the first byte of tag fields (default value), i.e., used for the same purpose (padding) and under the same conditions as the value '00'.

In tag fields of two or more bytes, the values '00' to '1E' and '80' are invalid for the second byte.

— In two-byte tag fields, the second byte consists of bit 8 set to 0 and bits 7 to 1 encoding a number greater than thirty. The second byte is valued from '1F' to '7F; the tag number is from 31 to 127.

— In three-byte tag fields, the second byte consists of bit 8 set to 1 and bits 7 to 1 not all set to 0; the third byte consists of bit 8 set to 0 and bits 7 to 1 with any value. The second byte is valued from '81' to 'FF' and the third byte from '00' to '7F'; the tag number is from 128 to 16 383.

5.2.2.2 BER-TLV length fields

In short form, the length field consists of a single byte where bit 8 is set to 0 and bits 7 to 1 encode the number of bytes in the value field. One byte can thus encode any number from zero to 127.

NOTE Any number from one to 127 is encoded in the same way in BER-TLV length field as in L_c and L_e fields. The encoding differs for zero, 128 and more. See for example, the coding of data objects in the GET DATA command in 7.4.2.

In long form, the length field consists of two or more bytes. Bit 8 of the first byte is set to 1 and bits 7 to 1 are not all equal, thus encoding the number of subsequent bytes in the length field. Those subsequent bytes encode the number of bytes in the value field.

ISO/IEC 7816 does not use the “indefinite length” specified by the basic encoding rules of ASN.1.

ISO/IEC 7816 supports length fields of one, two, … up to five bytes (see Table 8). In ISO/IEC 7816, the values '80' and '85' to 'FF' are invalid for the first byte of length fields.

Table 8 — BER-TLV length fields in ISO/IEC 7816

	1st byte	2nd byte	3rd byte	4th byte	5th byte	N
1 byte	'00' to '7F'	-	-	-	-	0 to 127
2 bytes	'81'	'00' to 'FF'	-	-	-	0 to 255
3 bytes	'82'	'0000' to 'FFFF'		-	-	0 to 65 535
4 bytes	'83'	'000000' to 'FFFFFF'			-	0 to 16 777 215
5 bytes	'84'	'00000000' to 'FFFFFFFF'				0 to 4 294 967 295

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

5.2.3 Data fields, value fields, data objects and data elements

Any command or response data field may be encoded in BER-TLV, e.g., in a command-response pair where CLA indicates secure messaging (see 6) or where bit 1 of INS is set to 1 (odd INS code, see 5.1.2).

— Any BER-TLV data object is denoted {T-L-V} with a tag field followed by a length field encoding a number. Depending on whether the number is zero or not, the value field is absent (empty data object) or present.

— Any constructed BER-TLV data object is denoted {T-L- {T1-L1-V1} … - {Tn-Ln-Vn}} with a tag field followed by a length field encoding a number. If the number is not zero, then the value field of the constructed data object, i.e., the template, consists of one or more BER-TLV data objects, each one consisting of a tag field, a length field encoding a number and if the number is not zero, a value field.

Some data fields, e.g., commands for handling data units (see 7.2), the value fields of SIMPLE-TLV data objects and the value fields of some primitive BER-TLV data objects consist of data elements according to the specifications of the command or according to the tag of the data object.

Some data fields, e.g., commands for handling records (see 7.3) and the value fields of some primitive BER-TLV data objects consist of SIMPLE-TLV data objects.

Some data fields, e.g., commands for handling data objects (see 7.4) and the value fields of constructed BER-TLV data objects, i.e., the templates, consist of BER-TLV data objects.

5.2.4 Identification of data elements

The identification of data elements relies on the following principles.

1) If the number of bits representing a data element is not a multiple of eight, then the mapping into a byte or a string of bytes should be specified in the context of the respective data element. Unless otherwise specified, the appropriate number of bits shall be set to 1 in the last byte starting from bit 1.

2) At the interface between the card and the interface device, a data element is generally presented in the value field of a BER-TLV data object.

3) For purposes of retrieval and referencing in interchange, a data element shall be associated with the tag of a BER-TLV data object and the data element may be encapsulated in this data object.

4) A data element may be referenced directly by its associated BER-TLV tag. It may be associated with another data element that sets the context to which it belongs.

5) One or more command-to-perform data objects may indirectly reference a data element.

6) When present, data objects of the universal class (first byte from '01' to '3F') have their general meaning.

7) All the data objects of the application class (first byte from '40' to '7F') are interindustry, unless otherwise specified. This part and other parts of ISO/IEC 7816 allocate tags of the application class. Every application class tag not defined in ISO/IEC 7816 is reserved for ISO/IEC JTC 1/SC 17.

8) This document specifies many interindustry data elements. In addition to defining further interindustry data elements, ISO/IEC 7816-6 maintains an exhaustive list of the interindustry data elements specified in ISO/IEC 7816 at the time of publication.

9) There may be multiple occurrences of the same interindustry data object within the card.

10) In command and response data fields, all the data objects of the context-specific class (first byte from '80' to 'BF') shall be nested within interindustry templates, except for file control information (see 5.3.3) and secure messaging (see 6).

11) Illustrated by annex A, the subsequent clauses specify tag allocation schemes for identifying interindustry data objects in data fields. When needed, those tag allocation schemes use the interindustry data objects shown in Table 9 for notifying an authority responsible for tag allocation.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

Table 9 — Interindustry data objects for tag allocation authority

Tag	Value
'06'	Object identifier (encoding specified in ISO/IEC 8825-1, see examples in annex A)
'41'	Country code (encoding specified in ISO 3166-1[1]) and optional national data
'42'	Issuer identification number (encoding and registration specified in ISO/IEC 7812-1[3]) and optional issuer data
'4F'	Application identifier (AID, encoding specified in 8.2.1.2)

5.2.4.1 Compatible tag allocation scheme

These tag allocation schemes use interindustry data objects and further data objects.

These further data objects shall be nested within interindustry templates referenced by tags '70' to '77' (except for tag '73' reserved for nesting proprietary data objects, see 5.2.4.3) where the meaning of the application class tags is not defined in ISO/IEC 7816 except for tags '41', '42' and '4F' for identifying tag allocation authorities as shown in Table 9.

The use of the context-specific class (first byte from '80' to 'BF') within interindustry templates with tags '65' (cardholder-related data), '66' (card data), '67' (authentication data) and '6E' (application-related data) is deprecated.

In order to identify a compatible tag allocation scheme and the authority responsible for the scheme, an interindustry template referenced by tag '78' may be used. If present, such a template shall contain one of the interindustry data objects shown in Table 9, for identifying a tag allocation authority.

— If tag '78' is present in the initial data string (see 8.1.2) or in EF.ATR (see 8.2.1.1), then the authority is valid for the entire card.

— If tag '78' is present in DF management data (see 5.3.3), then the authority is valid within that DF.

5.2.4.2 Coexistent tag allocation scheme

These tag allocation schemes may use tags with an interpretation not defined in ISO/IEC 7816. In order to identify a coexistent tag allocation scheme and the authority responsible for the scheme, an interindustry template referenced by tag '79' shall be used. If present, such a template shall contain one of the interindustry data objects shown in Table 9, for identifying a tag allocation authority.

— If an authority is valid for the entire card, then tag '79' shall be present in the initial data string (see 8.1.2) or in EF.ATR (see 8.2.1.1).

— If an authority is valid within a DF, then tag '79' shall be present in the DF management data (see 5.3.3).

In such a scheme, all the interindustry data objects shall be nested within interindustry templates referenced by tag '7E'. Moreover, tags '79' and '7E' shall not be given another interpretation, as well as tags '62', '64', '6F' (FCP, FMD and FCI templates, see 5.3.3) and '7D' (SM template, see 6).

5.2.4.3 Independent tag allocation scheme

These tag allocation schemes may use tags with another interpretation than ISO/IEC 7816, but which does not comply with 5.2.4.2. Such tag allocation schemes do not allow interchange and do not comply with this document.

The use of interindustry discretionary data objects with tags '53' for presenting discretionary data elements and '73' for nesting proprietary data objects in discretionary templates allows the use of proprietary data elements and data objects while remaining compliant with this document.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2005+A1:2008

5.3 Structures for applications and data

This clause specifies structures for applications and data, as seen at the interface when processing commands in the interindustry class. The actual storage location of data and structural information beyond what is described in this clause is outside the scope of ISO/IEC 7816.

Two categories of structures are supported: dedicated file (DF) and elementary file (EF).

— The DFs host applications and / or group files and / or store data objects. An application DF is a DF hosting an application. A DF may be the parent of other files. These other files are said to be immediately under the DF.

— The EFs store data. An EF cannot be the parent of another file. Two categories of EFs are specified.
  - An internal EF stores data interpreted by the card, i.e., data used by the card for management and control purposes.
  - A working EF stores data not interpreted by the card, i.e., data used by the outside world exclusively.

Two types of logical organization are provided.

— Figure 2 illustrates a hierarchy of DFs with its corresponding security architecture (see 5.4). In such a card organization, the DF at the root is called the master file (MF); any DF may be an application DF, with or without its own hierarchy of DFs.

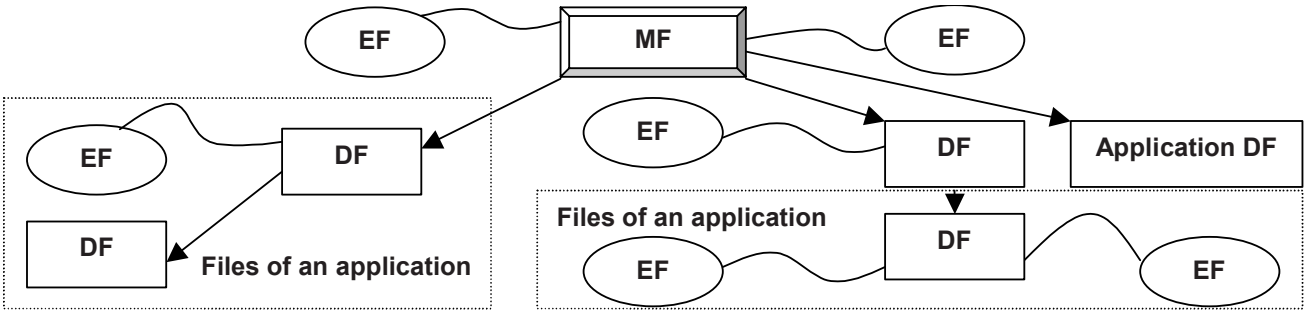

Figure 2 — Example of hierarchy of DFs

— Figure 3 illustrates application DFs in parallel, with no MF seen at the interface, i.e., without any apparent hierarchy of DFs. Such an organization supports independent applications in the card where any application DF may have its own hierarchy of DFs with its corresponding security architecture.

Figure 3 — Example of independent application DFs

5.3.1 Structure selection

5.3.1.1 Structure selection methods

Selecting a structure allows access to its data and, if the structure is a DF, its sub-structure. Structures may be selected implicitly, i.e., automatically after reset and possible protocol and parameter selection (see ISO/IEC 7816-3). When a structure cannot be implicitly selected, it shall be selected explicitly, i.e., by at least one of the following four methods.

Selection by DF name — A DF name may reference any DF. It is a string of up to sixteen bytes. Any application identifier (AID, see 8.2.1.2) may be used as DF name. In order to select unambiguously by DF name, e.g., when selecting by means of application identifiers, each DF name shall be unique within a given card.

Selection by file identifier — A file identifier may reference any file. It consists of two bytes. The value '3F00' is reserved for referencing the MF. The value 'FFFF' is reserved for future use. The value '3FFF' is reserved (see below and 7.4.1). The value '0000' is reserved (see 7.2.2 and 7.4.1). In order to unambiguously select any file by its identifier, all EFs and DFs immediately under a given DF shall have different file identifiers.

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

Selection by path — A path may reference any file. It is a concatenation of file identifiers. The path begins with the identifier of a DF (the MF for an absolute path or the current DF for a relative path) 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, then the value '3FFF' (reserved value) can be used at the beginning of the path. The values '3F002F00' and '3F002F01' are reserved (see 8.2.1.1). The path allows an unambiguous selection of any file from the MF or from the current DF (see 8.3).

Selection by short EF identifier — A short EF identifier may reference any EF. It consists of five bits not all equal, i.e., any number from one to thirty. When used as short EF identifier, the number zero, i.e., 00000 in binary, references the current EF. At MF level, the number thirty, i.e., 11110 in binary, is reserved (see 8.2.1.1). Short EF identifiers cannot be used in a path or as an EF identifier (e.g., in a SELECT command).

If supported, selection by short EF identifier shall be indicated.

— If the first software function table (see Table 86) is present in the historical bytes (see 8.1.1) or in EF.ATR (see 8.2.1.1), then the indication is valid at card level.

— If a short EF identifier (tag '88', see Table 12) is present in the control parameters (see 5.3.3) of an EF, then the indication is valid at EF level.

5.3.1.2 File reference data element

Referenced by tag '51', this interindustry data element references a file. It may have any length.

— An empty data object references the MF.

— If the length is one and if bits 8 to 4 of the data element are not all equal and if bits 3 to 1 are set to 000, then bits 8 to 4 encode a number from one to thirty that is a short EF identifier.

— If the length is two, then the data element is a file identifier.

— If the length is more than two, then the data element is a path.
  - If the length is even and if the first two bytes are set to '3F00', then the path is absolute. The data element is a concatenation of at least two file identifiers starting with the MF identifier.
  - If the length is even and if the first two bytes are not set to '3F00', then the path is relative. The data element is a concatenation of at least two file identifiers starting with the identifier of the current DF.
  - If the length is odd, then the path is qualified. The data element is either an absolute path without '3F00', or a relative path without the identifier of the current DF, followed by a byte to use as P1 in one or more SELECT commands (see 7.1.1 and 8.3).

Table 10 shows the file reference data object.

Table 10 — File reference data object

Tag	Length	Value
'51'	0	The empty data object references the MF
	1	Short EF identifier (bits 8 to 4 encode a number from one to thirty; bits 3 to 1 are set to 000)
	2	File identifier
	Even, > 2	Absolute path (the two first bytes are set to '3F00')
		Relative path (the first two bytes are not set to '3F00')
	Odd, > 2	Qualified path (the last byte shall be used as P1 in one or more SELECT commands)

5.3.2 Data referencing methods

In DFs, data may be referenced as data objects (see 5.2). The DF is seen at the interface as a set of data objects accessible by commands for handling data objects (see 7.4).

In EFs, data may be referenced as data units (see 7.2.1), as records (see 7.3.1) or as data objects (see 5.2). Data referencing method is an EF-dependent feature. Three structures of EFs are defined.

— **Transparent structure —** The EF is seen at the interface as a single continuous sequence of data units accessible by commands for handling data units (see 7.2). Data unit size is an EF-dependent feature.

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

— **Record structure —** The EF is seen at the interface as a single continuous sequence of individually identifiable records accessible by commands for handling records (see 7.3). Record numbering method is an EF-dependent feature. Three attributes are defined.

- The size of the records is either fixed, or variable.
- The organization of the records is either a sequence (linear structure) or a ring (cyclic structure).
- A record life cycle state distinguishing at least the following states: ACTIVATED and DEACTIVATED. The coding of a record life cycle state is out of scope for this part of ISO/IEC 7816. Within a certain EF, either all records have a record life cycle state or no record has a record life cycle state. The presence of record life cycle states is indicated in the FCP (see Table 12).

— **TLV structure —** The EF is seen at the interface as a set of data objects accessible by commands for handling data objects (see 7.4). The type of data objects in the EF, namely, either SIMPLE-TLV, or BER-TLV, is an EF-dependent feature.

For referencing data in EFs, the card shall support at least one of the five structures shown in Figure 4.

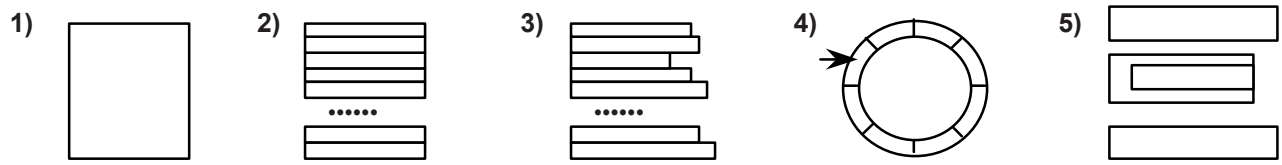

Figure 4 — EF structures

1) Transparent structure
2) Linear structure with records of fixed size
3) Linear structure with records of variable size
4) Cyclic structure with records of fixed size (the arrow references the most recently written record)
5) TLV structure

5.3.3 File control information

By definition, the file control information is the byte string available in response to the SELECT command (see 7.1.1); it may be present for any structure, i.e., any DF and any EF.

— If the first byte is valued from '00' to 'BF', then the byte string shall be BER-TLV encoded. ISO/IEC JTC 1/SC 17 reserves for future use all the values in the range '00' to 'BF' that are not defined in this document.

— If the first byte is valued from 'C0' to 'FF', then the byte string is not encoded according to this document.

Table 11 shows three interindustry templates for nesting file control information BER-TLV data objects.

— The FCP template is a set of file control parameters, i.e., logical, structural and security attributes as listed in Table 12 and defined hereafter. Within the FCP template, the context-specific class (first byte from '80' to 'BF') is reserved for file control parameters; tags '85' and 'A5' reference discretionary data.

— The FMD template is a set of file management data, i.e., interindustry data objects such as an application identifier as defined in 8.2.1.2, an application label as defined in 8.2.1.4 and an application expiration date as defined in ISO/IEC 7816-6, possibly nested within an application template as defined in 8.2.1.3. Within the FMD template, tags '53' and '73' reference discretionary data.

— The FCI template is a set of file control parameters and file management data.

Table 11 — Interindustry templates for file control information

Tag	Value
'62'	Set of file control parameters (FCP template)
'64'	Set of file management data (FMD template)
'6F'	Set of file control parameters and file management data (FCI template)

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

The three templates may be retrieved according to selection options of the SELECT command (see Table 40).

— If the FCI option is set, then the FCI tag is optional for introducing the template in the response data field.

— If the FCP or FMD option is set, then the corresponding tag is mandatory for introducing the template.

Table 12 lists the file control parameters, all in the context-specific class. When a control parameter is present for a file, the Table says whether it occurs only once (explicit indication), or it may be repeated (no indication).

Table 12 — File control parameter data objects

Tag	Length	Value	Applies to
'80'	Var.	Number of data bytes in the file, excluding structural information	Any EF, Once
'81'	2	Number of data bytes in the file, including structural information if any	Any file, Once
'82'	1	File descriptor byte (see 5.3.3.3 and Table 14)	Any file
	2	File descriptor byte and data coding byte (see Table 87)	
	3 or 4	File descriptor byte, data coding byte and maximum record size on one or two bytes	Any EF supporting records
	5 or 6	File descriptor byte, data coding byte, maximum record size on two bytes and number of records on one or two bytes	
'83'	2	File identifier	Any file
'84'	up to 16	DF name	Any DF
'85'	Var.	Proprietary information not encoded in BER-TLV	Any file
'86'	Var.	Security attribute in proprietary format	Any file
'87'	2	Identifier of an EF containing an extension of the file control information	Any DF, Once
'88'	0 or 1	Short EF identifier (see 5.3.3.1)	Any EF, Once
'8A'	1	Life cycle status byte (LCS byte, see 5.3.3.2 and Table 13)	Any file, Once
'8B'	Var.	Security attribute referencing the expanded format (see 5.4.3.3 and Table 25)	Any file, Once
'8C'	Var.	Security attribute in compact format (see 5.4.3.1)	Any file, Once
'8D'	2	Identifier of an EF containing security environment templates (see 6.3.4)	Any DF
'8E'	1	Channel security attribute (see 5.4.3 and Table 15)	Any file, Once
'8F'	1	Profile indicator, see Table Amd.1-1	EF supporting records, once
'A0'	Var.	Security attribute template for data objects (see 5.4.3)	Any file, Once
'A1'	Var.	Security attribute template in proprietary format	Any file
'A2'	Var.	Template consisting of one or more pairs of data objects: Short EF identifier (tag '88') - File reference (tag '51', L > 2, see 5.3.1.2)	Any DF
'A5'	Var.	Proprietary information encoded in BER-TLV	Any file
'AB'	Var.	Security attribute template in expanded format (see 5.4.3.2)	Any file, Once
'AC'	Var.	Cryptographic mechanism identifier template (see 5.4.2)	Any DF
— In this context, ISO/IEC JTC 1/SC 17 reserves any other data object of the context-specific class (first byte from '80' to 'BF').			

Part of the control information of a DF may additionally be present in an EF under the control of an application and referenced by tag '87' in the file control parameters. If present within such an EF, file control information shall be introduced by the appropriate tag, either a FCP tag, or a FCI tag.

5.3.3.1 Short EF identifier

The following rules apply for the use of tag '88' in the control parameters of any EF.

— If the card supports selection by short EF identifiers (see 5.3.1.1) and if tag '88' is absent, then in the second byte of the file identifier (tag '83'), bits 5 to 1 encode the short EF identifier.

— If tag '88' is present with a length set to zero, then the EF supports no short identifier.

— If tag '88' is present with a length set to one and if bits 8 to 4 of the data element are not all equal and if bits 3 to 1 are set to 000, then bits 8 to 4 encode the short EF identifier (a number from one to thirty).

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2005+A1:2008

5.3.3.2 Life cycle status byte

The card, files and other objects, each have a life cycle; the life cycle status allows the card and the interface device to identify the different logical security states of the use of the card, files and other objects in the card. To support flexible management of the life cycle as an attribute (see ISO/IEC 7816-9[4]), this clause defines four primary states of the life cycle in the following order.

1) Creation state
2) Initialisation state
3) Operational state
4) Termination state

The life cycle status byte (LCS byte) shall be interpreted according to Table 13.

— The values '00' to '0F' are interindustry.

— The values '10' to 'FF' are proprietary.

Table 13 — Life cycle status byte

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	No information given
0	0	0	0	0	0	0	1	Creation state
0	0	0	0	0	0	1	1	Initialisation state
0	0	0	0	0	1	-	1	Operational state (activated)
0	0	0	0	0	1	-	0	Operational state (deactivated)
0	0	0	0	1	1	-	-	Termination state
Not all zero				x	x	x	x	Proprietary
— Any other value is reserved for future use by ISO/IEC JTC 1/SC 17.								

Referenced by tag '8A', a file LCS byte may be present in the control parameters of any file (see Table 12).

A card LCS byte may be present in the historical bytes (see 8.1.1.3). Referenced by tag '48', a card LCS byte may be present in EF.ATR (see 8.2.1.1). When it has a MF, the card is in, at least, the creation state.

NOTE Unless otherwise specified, the security attributes are valid for the operational state.

5.3.3.3 File descriptor byte

Referenced by tag '82', a data element may be present in the control parameters of any file (see Table 12).

— The first byte of the data element is the file descriptor byte (see Table 14).

— If the data element consists of two or more bytes, then the second byte is the data coding byte (see Table 87). If the card provides data coding bytes in several places, then the indication valid for a given file is in the closest position to that file within the path from the MF to that file.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2005+A1:2008