

**Implementation of
EN ISO/IEC 7816-4:1996**

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

**Part 4: Interindustry commands for
interchange**

The European Standard EN ISO/IEC 7816-4:1996 has the status of a
British Standard

ICS 35.240.15

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

Committees responsible for this British Standard

The preparation of this British Standard was entrusted to Technical Committee IST/17, upon which the following bodies were represented:

- APACS (Barclaycard)
- APACS (Co-operative Bank)
- APACS (Lloyds Bank)
- APACS (Midland Bank)
- APACS (NatWest Bank)
- Association for Payment Clearing Services (APACS)
- BT Laboratories
- Cellnet
- Consumer Policy Committee of BSI
- Electricity Association
- GPT Card Technology
- HMSO
- Mondex International
- Motorola Ltd.
- Rochford Thompson Equipment
- Shell UK
- Thorn Transit Systems International
- Vodafone Ltd.
- Westinghouse Cubic Ltd.

This British Standard, having been prepared under the direction of the Information Systems Technology Assembly, was published under the authority of the Standards Board and comes into effect on 15 December 1996

© BSI 11-1998

The following BSI references relate to the work on this standard:
Committee reference IST/17
Draft for comment 94/646721 DC

ISBN 0 580 26838 1

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
Foreword	2
Text of EN ISO/IEC 7816-4	1
Annex ZA (normative) Normative references to international publications with their relevant European publications	Inside back cover

National foreword

This Part of BS EN ISO/IEC 7816 is the English language version of EN ISO/IEC 7816-4:1996 and implements it as the UK national standard.

This Part of BS EN ISO/IEC 7816 is published under the direction of the Information Systems Technology Assembly whose Technical Committee IST/17 has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on interpretation, or proposals for change, and keep UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

NOTE International and European Standards, as well as overseas standards, are available from Customer Services, BSI, 389 Chiswick High Road, London, W4 4AL.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the EN title page, pages 2 to 4, the ISO/IEC title page, page ii, pages 1 to 44, an inside back cover and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

ICS 35.240.40

Descriptors: Data processing, information interchange, identification cards, IC cards, messages, security techniques, authentication

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.

This European Standard exists 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

© 1996 Copyright reserved to CEN members

Ref. No. EN ISO/IEC 7816-4:1995 E
 **Documents**
Document Sharing Hub

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.

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

Contents

	Page
Foreword	2
Introduction	1
1 Scope	1
2 Normative references	1
3 Definitions	1
4 Abbreviations and notation	3
5 Basic organizations	3
5.1 Data structures	3
5.2 Security architecture of the card	6
5.3 APDU message structure	7
5.4 Coding conventions for command headers, data fields and response trailers	9
5.5 Logical channels	13
5.6 Secure messaging	13
6 Basic interindustry commands	17
6.1 READ BINARY command	17
6.2 WRITE BINARY command	18
6.3 UPDATE BINARY command	18
6.4 ERASE BINARY command	19
6.5 READ RECORD(S) command	20
6.6 WRITE RECORD command	21
6.7 APPEND RECORD command	22
6.8 UPDATE RECORD command	23
6.9 GET DATA command	24
6.10 PUT DATA command	25
6.11 SELECT FILE command	26
6.12 VERIFY command	27
6.13 INTERNAL AUTHENTICATE command	27
6.14 EXTERNAL AUTHENTICATE command	28
6.15 GET CHALLENGE command	29
6.16 MANAGE CHANNEL command	29
7 Transmission-oriented interindustry commands	30
7.1 GET RESPONSE command	30
7.2 ENVELOPE command	31
8 Historical bytes	31
9 Application-independent card services	33
Annex A (normative) Transportation of APDU messages by T=0	36
Annex B (normative) Transportation of APDU messages by T=1	39
Annex C (informative) Record pointer management	40
Annex D (informative) Use of the basic encoding rules of ASN.1	41
Annex E (informative) Examples of card profiles	42
Annex F (informative) Use of secure messaging	43
Figure 1 — Logical file organisation (example)	3
Figure 2 — EF structures	4
Figure 3 — Command APDU structure	8
Figure 4 — The 4 structures of command APDUs	8
Figure 5 — Not empty body	8
Figure 6 — Response APDU structure	9
Figure 7 — Structural scheme of status bytes	11
Table 1 — Templates relevant to FCI	5
Table 2 — File control parameters	6
Table 3 — File descriptor type	6
Table 4 — Data within a command-response pair	7
Table 5 — Decoding of the command APDUs	8
Table 6 — Command APDU contents	9
Table 7 — Response APDU contents	9
Table 8 — Coding and meaning of CLA	10
Table 9 — Coding and meaning of nibble 'X' when CLA = "0X", "8X", "9X" or "AX"	10
Table 10 — Invalid INS codes	10
Table 11 — INS codes defined in this part of ISO/IEC 7816	10
Table 12 — Coding of SW1–SW2	12
Table 13 — Coding of SW2 when SW1 = "62"	12

	Page		Page
Table 14 — Coding of SW2 when SW1 = “63”	12	Table 57 — select file command APDU	26
Table 15 — Coding of SW2 when SW1 = “65”	12	Table 58 — Coding of the selection control P1	26
Table 16 — Coding of SW2 when SW1 = “68”	12	Table 59 — Coding of the selection control P2	27
Table 17 — Coding of SW2 when SW1 = “69”	12	Table 60 — SELECT FILE response APDU	27
Table 18 — Coding of SW2 when SW1 = “6A”	12	Table 61 — VERIFY command APDU	27
Table 19 — Plain value data objects	14	Table 62 — Coding of the reference control P2	27
Table 20 — Cryptographic checksum data object	15	Table 63 — VERIFY response APDU	27
Table 21 — Digital signature related data objects	15	Table 64 — INTERNAL AUTHENTICATE command APDU	28
Table 22 — Data objects for confidentiality	15	Table 65 — Coding of the reference control P2	28
Table 23 — Padding indicator byte	15	Table 66 — INTERNAL AUTHENTICATE response APDU	28
Table 24 — Control reference templates	16	Table 67 — EXTERNAL AUTHENTICATE command APDU	28
Table 25 — Control reference data objects	16	Table 68 — Coding of the reference control P2	29
Table 26 — Response descriptor template	17	Table 69 — EXTERNAL AUTHENTICATE response APDU	29
Table 27 — READ BINARY command APDU	17	Table 70 — GET CHALLENGE command APDU	29
Table 28 — READ BINARY response APDU	17	Table 71 — GET CHALLENGE response APDU	29
Table 29 — WRITE BINARY command APDU	18	Table 72 — MANAGE CHANNEL command APDU	30
Table 30 — WRITE BINARY response APDU	18	Table 73 — MANAGE CHANNEL response APDU	30
Table 31 — UPDATE BINARY command APDU	19	Table 74 — GET RESPONSE command APDU	30
Table 32 — UPDATE BINARY response APDU	19	Table 75 — GET RESPONSE response APDU	30
Table 33 — ERASE BINARY command APDU	19	Table 76 — ENVELOPE command APDU	31
Table 34 — ERASE BINARY response APDU	19	Table 77 — ENVELOPE response APDU	31
Table 35 — READ RECORD (S) command APDU	20	Table 78 — Coding of the category indicator	31
Table 36 — Coding of the reference control P2	20	Table 79 — Coding of the country/issuer indicator	31
Table 37 — READ RECORD (S) response APDU	20	Table 80 — Card-profile for application-independent card services	32
Table 38-1 — Data field of the response when reading for one record	20	Table 81 — Coding of the command when length = “1”	32
Table 38-2 — Data field of the response when reading for several record	21	Table 82 — Structure of the first byte	32
Table 39 — WRITE RECORD command APDU	21	Table 83 — Coding of the command when b8=0	32
Table 40 — Coding of the reference control P2	22	Table 84 — Coding of the command when b8=0	32
Table 41 — Data field of the command	22	Table 85 — First software function table	33
Table 42 — WRITE RECORD response APDU	22	Table 86 — Second software function table (data coding byte)	33
Table 43 — WRITE RECORD command APDU	22	Table 87 — Third software function table	33
Table 44 — Coding of the reference control P2	22	Table 88 — Coding of the command for direct application selection	34
Table 45 — Data field of the command	22	Table 89 — Coding of the command to select a DF using a file identifier	35
Table 46 — APPEND RECORD response APDU	23	Table 90 — Coding of the command to select an EF	35
Table 47 — UPDATE RECORD command APDU	23	Table 91 — Coding of the command to read a transparent file	35
Table 48 — Coding of the reference control P2	23	Table 92 — Coding of the command to read a record-oriented file	35
Table 49 — Data field of the command	23		
Table 50 — UPDATE RECORD response APDU	23		
Table 51 — GET DATA command APDU	24		
Table 52 — Coding of the parameters P1–P2	24		
Table 53 — GET DATA response APDU	24		
Table 54 — PUT DATA command APDU	25		
Table 55 — Coding of the parameters P1–P2	25		
Table 56 — PUT DATA response APDU	25		

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)

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).

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 8825:1990²⁾, *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

¹⁾ To be published

²⁾ Currently under revision.

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

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
$B_1 B_2$	Concatenation of bytes B_1 (the most significant byte) and B_2 (the least significant byte)
$(B_1 B_2)$	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).

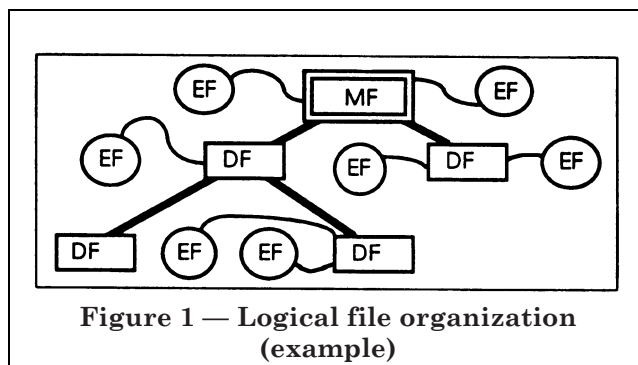
The logical organization of data in a card consists of the following structural hierarchy of dedicated files.

- 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.



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 FE may be referenced by a short FE identifier coded on 5 bits valued in the range from 1 to 30. The value 0 used as a short FE identifier references the currently selected FE. Short FE 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.

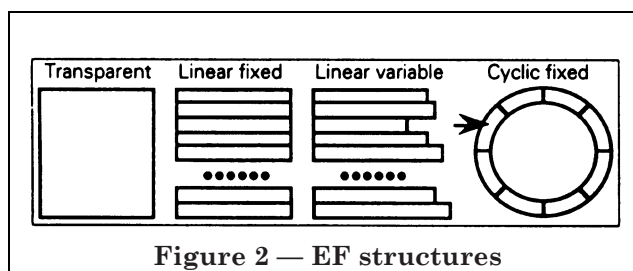


Figure 2 — EF structures

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.

NOTE 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.

NOTE 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.

Table 2 — File control parameters

Tag	L	Value	Applies to
“80”	2	Number of data bytes in the file, excluding structural information	Transparent EFs
“81”	2	Number of data bytes in the file, including structural information if any	Any file
“82”	1	File descriptor byte (see Table 3)	Any file
	2	File descriptor byte followed by data coding byte (see Table 86)	Any file
	3 or 4	File descriptor byte followed by data coding byte and maximum record length	EFs with record structure
“83”	2	File identifier	Any file
“84”	1 to 16	DF name	DFs
“85”	var.	Proprietary information	Any file
“86”	var.	Security attributes (coding outside the scope of this part of ISO/IEC 7816)	Any file
“87”	2	Identifier of an EF containing an extension of the FCI	Any file
“88” to “9E”		RFU	
“9FXY”		RFU	

Table 3 — File descriptor byte

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	—	—	—	—	—	—	File accessibility
0	0	—	—	—	—	—	—	— Not shareable file
0	1	—	—	—	—	—	—	— Shareable file
0	—	x	x	x	—	—	—	File type
0	—	0	0	0	—	—	—	— Working EF
0	—	0	0	1	—	—	—	— Internal EF
0	—	0	1	0	—	—	—	— Reserved
0	—	0	1	1	—	—	—	for
0	—	1	0	0	—	—	—	proprietary
0	—	1	0	1	—	—	—	types
0	—	1	1	0	—	—	—	of EFs
0	—	1	1	1	—	—	—	— DF
0	—	—	—	—	x	x	x	EF structure
0	—	—	—	—	0	0	0	— No information given
0	—	—	—	—	0	0	1	— Transparent
0	—	—	—	—	0	1	0	— Linear fixed, no further info
0	—	—	—	—	0	1	1	— Linear fixed, SIMPLE-TLV
0	—	—	—	—	1	0	0	— Linear variable, no further info
0	—	—	—	—	1	0	1	— Linear variable, simple-tlv
0	—	—	—	—	1	1	0	— Cyclic, no further info
0	—	—	—	—	1	1	1	— Cyclic, SIMPLE-TLV
1	x	x	x	x	x	x	x	RFU
“Shareable” means that the file supports at least concurrent access on different logical channels.								

5.2 Security architecture of the card

This clause describes the following features:

- security status,
- security attributes,
- security mechanisms.

Security attributes are compared with the security status to execute commands and/or to access files.

5.2.1 Security status

Security status represents the current state possibly achieved after completion of

- answer to reset (ATR) and possible protocol type selection (PTS) and/or
- a single command or a sequence of commands, possibly performing authentication procedures.

The security status may also result from the completion of a security procedure related to the identification of the involved entities, if any, e.g.,

- by proving the knowledge of a password (e.g., using a VERIFY command),
- by proving the knowledge of a key (e.g., using a GET CHALLENGE command followed by an EXTERNAL AUTHENTICATE command).

— by secure messaging (e.g., message authentication).

Three security statuses are considered.

— **Global security status** — It may be modified by the completion of an MF-related authentication procedure (e.g., entity authentication by a password or by a key attached to the MF).

— **File-specific security status** — It may be modified by the completion of a DF-related authentication procedure (e.g., entity authentication by a password or by a key attached to the specific DF); it may be maintained, recovered or lost by file selection (see 6.10.2); this modification may be relevant only for the application to which the authentication procedure belongs.

— **Command-specific security status** — It only exists during the execution of a command involving authentication using secure messaging (see 5.6); such a command may leave the other security status unchanged.

If the concept of logical channels is applied, the file specific security status may depend on the logical channel (see 5.5.1).

5.2.2 Security attributes

The security attributes, when they exist, define the allowed actions and the procedures to be performed to complete such actions.

Security attributes may be associated with each file and fix the security conditions that shall be satisfied to allow operations on the file. The security attributes of a file depend on

- its category (DF or EF),
- optional parameters in its file control information and/or in that of its parent file(s).

NOTE Security attributes may also be associated to other objects (e.g., keys).

5.2.3 Security mechanisms

This part of ISO/IEC 7816 defines the following security mechanisms.

— **Entity authentication with password** — The card compares data received from the outside world with secret internal data. This mechanism may be used for protecting the rights of the user.

— **Entity authentication with key** — The entity to be authenticated has to prove the knowledge of the relevant key in an authentication procedure (e.g., using a GET CHALLENGE command followed by an EXTERNAL AUTHENTICATE command).

— **Data authentication** — Using internal data, either secret or public, the card checks redundant data received from the outside world. Alternately, using secret internal data, the card computes a data element (cryptographic checksum or digital signature) and inserts it in the data sent to the outside world. This mechanism may be used for protecting the rights of a provider.

— **Data encipherment** — Using secret internal data, the card deciphers a cryptogram received in a data field. Alternately, using internal data, either secret or public, the card computes a cryptogram and inserts it in a data field, possibly together with other data. This mechanism may be used to provide a confidentiality service, e.g., for key management and conditional access. In addition to the cryptogram mechanism, data confidentiality can be achieved by data concealment. In this case, the card computes a string of concealing bytes and adds it by exclusive-or to data bytes received from or sent to the outside world. This mechanism may be used for protecting privacy and for reducing the possibilities of message filtering.

The result of an authentication may be logged in an internal EF according to the requirements of the application.

5.3 APDU message structure

A step in an application protocol consists of sending a command, processing it in the receiving entity and sending back the response. Therefore a specific response corresponds to a specific command, referred to as a command-response pair.

An application protocol data unit (APDU) contains either a command message or a response message, sent from the interface device to the card or conversely.

In a command-response pair, the command message and the response message may contain data, thus inducing four cases which are summarized by Table 4.

Table 4 — Data within a command-response pair

Case	Command data	Expected response data
1	No data	No data
2	No data	Data
3	Data	No data
4	Data	Data