BS ISO/IEC 7816-4:2013+A2:2018
Incorporating corrigendum August 2014

BSI Standards Publication

Identification cards — Integrated circuit cards

Part 4: Organization, security and commands for interchange

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

National foreword

This British Standard is the UK implementation of ISO/IEC 7816-4:2013+A2:2018, incorporating corrigendum August 2014. It supersedes BS ISO/IEC 7816-4:2013, which is withdrawn.

The start and finish of text introduced or altered by corrigendum is indicated in the text by tags. Text altered by ISO/IEC corrigendum August 2014 is indicated in the text by [AC1] ⟨AC1⟩.

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 A1 is indicated by [A1] ⟨A1⟩.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and security devices for 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.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 96325 4

ICS 35.240.15

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 30 April 2013.

Amendments/corrigenda issued since publication

Date	Text affected
31 October 2014	Implementation of ISO/IEC corrigendum August 2014
31 October 2018	Implementation of ISO/IEC amendment A1:2018 and A2:2018

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

INTERNATIONAL STANDARD

ISO/IEC 7816-4

Third edition
2013-04-15

Identification cards — Integrated circuit cards —

Part 4: Organization, security and commands for interchange

Cartes d'identification — Cartes à circuit intégré —

Partie 4: Organisation, sécurité et commandes pour les échanges

Reference number
ISO/IEC 7816-4:2013(E)

Documents
Document Sharing Hub
© ISO/IEC 2013

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2013

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

Contents

Page

Foreword vii

Introduction viii

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Symbols and abbreviated terms 7

5 Command-Response pairs 8
5.1 Conditions of operation 8
5.2 Syntax 9
5.3 Chaining procedures 10
5.3.1 General 10
5.3.2 Payload fragmentation 10
5.3.3 Command chaining 10
5.3.4 Response chaining 11
5.4 Class byte 12
5.4.1 Coding 12
5.4.2 Logical channels 13
5.5 Instruction byte 14
5.6 Status bytes 14

6 Data objects 17
6.1 SIMPLE-TLV data objects 18
6.2 BER-TLV data objects 18
6.3 Constructed DOs versus primitive DOs 18

7 Structures for applications and data 19
7.1 Available structures 19
7.2 Validity area 20
7.2.1 Definitions and attributes 20
7.2.2 Basic rules for VA handling and use 20
7.3 Structure selection 21
7.3.1 Structure selection methods 21
7.3.2 File reference data element and DO 22
7.3.3 General reference data element and DO 23
7.3.4 Data referencing methods in elementary files 23
7.4 File and data control information 23
7.4.1 File control information retrieval 23
7.4.2 Data control information retrieval 24
7.4.3 Control parameters 24
7.4.4 Short EF identifier 26
7.4.5 File descriptor byte 26
7.4.6 Profile indicator 27
7.4.7 Data descriptor byte 27
7.4.8 DF and EF list data elements 27
7.4.9 Instance number data element 28
7.4.10 Life cycle status 28
7.4.11 Indirect referencing by short EF identifier using DO'A2' 28
7.4.12 Interface and life cycle status dependent security attribute template 29

8 Specific use of DOs and related concepts 30
8.1 BER-TLV payloads and padding 30

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

8.1.1 Padding conditions 30
8.1.2 Padding procedure 30
8.2 Current template and data object generations 31
8.2.1 Current template and current DO 31
8.2.2 Template extension 31
8.2.3 Data object sub-tree 31
8.2.4 Data object life cycle 32
8.3 Identification of data elements and data objects 32
8.3.1 Principles 32
8.3.2 Tag interpretation in command and response data fields or payloads 32
8.3.3 Tag allocation 32
8.3.4 Standard tag allocation scheme 33
8.3.5 Compatible tag allocation scheme 33
8.3.6 Coexistent tag allocation scheme 34
8.3.7 Avoidance of independent tag allocation schemes 34
8.4 Referencing and retrieval of DOs and data elements 34
8.4.1 General 34
8.4.2 Element list 35
8.4.3 Tag list 35
8.4.4 Header list 35
8.4.5 Extended header and extended header list 35
8.4.6 Resolving an extended header 36
8.4.7 Resolving an extended header list 37
8.4.8 Wrapper 37
8.4.9 Tagged wrapper 38

9 Security architecture 38
9.1 General 38
9.2 Cryptographic mechanism identifier template 39
9.3 Security attributes 40
9.3.1 Security attributes targets 40
9.3.2 Compact format 40
9.3.3 Expanded format 44
9.3.4 Access rule references 48
9.3.5 Security attributes for data objects 49
9.3.6 Security parameters template 49
9.3.7 Security attributes for logical channels 55
9.4 Security support data elements 56

10 Secure messaging 57
10.1 SM fields and SM DOs 57
10.1.1 SM protection of command payloads 57
10.1.2 SM protection of chained commands and responses 57
10.1.3 SM DOs 57
10.2 Basic SM DOs 58
10.2.1 SM DOs for encapsulating plain values 58
10.2.2 SM DOs for confidentiality 59
10.2.3 SM DOs for authentication 60
10.3 Auxiliary SM DOs 61
10.3.1 Control reference templates 61
10.3.2 Control reference DOs in control reference templates 61
10.3.3 Security environments 63
10.3.4 Response descriptor template 65
10.4 SM impact on command-response pairs 65

11 Commands for interchange 67
11.1 Selection 67
11.1.1 SELECT command 67
11.1.2 MANAGE CHANNEL command 69
11.2 Data unit handling 70
11.2.1 Data units 70

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

11.2.2 General 70
11.2.3 READ BINARY command 71
11.2.4 WRITE BINARY command 71
11.2.5 UPDATE BINARY command 72
11.2.6 SEARCH BINARY command 72
11.2.7 ERASE BINARY command 72
11.2.8 COMPARE BINARY function 73
11.3 Record handling 73
11.3.1 Records 73
11.3.2 General 74
11.3.3 READ RECORD (S) command 75
11.3.4 WRITE RECORD command 76
11.3.5 UPDATE RECORD command 78
11.3.6 APPEND RECORD command 79
11.3.7 SEARCH RECORD command 80
11.3.8 ERASE RECORD (S) command 84
11.3.9 ACTIVATE RECORD (s) command 85
11.3.10 DEACTIVATE RECORD (s) command 86
11.3.11 COMPARE RECORD function 86
11.4 Data object handling 86
11.4.1 General 86
11.4.2 SELECT DATA command 88
11.4.3 GET DATA/GET NEXT DATA commands - even INS code 91
11.4.4 GET DATA/GET NEXT DATA command - odd INS codes 92
11.4.5 General properties of PUT/PUT NEXT/UPDATE DATA commands 94
11.4.6 PUT DATA command 94
11.4.7 PUT NEXT DATA command 95
11.4.8 UPDATE DATA command 96
11.4.9 COMPARE DATA function 96
11.5 Basic security handling 96
11.5.1 General 96
11.5.2 INTERNAL AUTHENTICATE command 97
11.5.3 GET CHALLENGE command 97
11.5.4 EXTERNAL AUTHENTICATE command 98
11.5.5 GENERAL AUTHENTICATE command 99
11.5.6 VERIFY command 100
11.5.7 CHANGE REFERENCE DATA command 101
11.5.8 ENABLE VERIFICATION REQUIREMENT command 101
11.5.9 DISABLE VERIFICATION REQUIREMENT command 102
11.5.10 RESET RETRY COUNTER command 102
11.5.11 MANAGE SECURITY ENVIRONMENT command 102
11.6 Miscellaneous 104
11.6.1 COMPARE command 104
11.6.2 GET ATTRIBUTE command 106
11.7 Transmission handling 106
11.7.1 GET RESPONSE command 106
11.7.2 ENVELOPE command 106

12 Application-independent card services 107
12.1 Card identification 107
12.1.1 Historical bytes 107
12.1.2 Initial data string recovery 111
[A2] 12.1.3 Waiting time management ..... 112 [A2]
12.2 Application identification and selection 114
12.2.1 EF.DIR 114
12.2.2 EF.ATR/INFO 114
12.2.3 Application identifier 115
12.2.4 Application template and related data elements 116
12.2.5 Application selection 117
12.3 Selection by path 118
12.4 Data retrieval 118

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

12.5 Card-originated byte strings ... 118
12.5.1 Triggering by the card ... 119
12.5.2 Queries and replies ... 119
12.5.3 Formats ... 119
12.6 General feature management ... 119
12.6.1 On-card services ... 120
12.6.2 Interface services ... 120
12.6.3 Profile services ... 120
12.6.4 Provision of additional information ... 121
12.7 APDU management ... 121
12.7.1 Extended length information ... 121
12.7.2 List of supported INS codes ... 121

Annex A (informative) Examples of object identifiers and tag allocation schemes ... 122
A.1 Object identifiers ... 122
A.2 Tag allocation schemes ... 122

Annex B (informative) Examples of secure messaging ... 124
B.1 Cryptographic checksum ... 124
B.2 Cryptograms ... 128
B.3 Control references ... 128
B.4 Response descriptor ... 128
B.5 ENVELOPE command ... 129
B.6 Synergy between secure messaging and security operations ... 129

Annex C (informative) Examples of AUTHENTICATE functions by GENERAL AUTHENTICATE commands ... 132
C.1 GENERAL AUTHENTICATE using witness-challenge-response triples ... 132
C.2 GENERAL AUTHENTICATE for a multi-step authentication protocol ... 136
NA.1.1 Terminal Authentication protocol ... 138
NA.1.2 Chip Authentication protocol ... 139

Annex D (informative) Application identifiers using issuer identification numbers ... 140
D.1 Background information ... 140
D.2 Format ... 140

Annex E (informative) BER Encoding Rules ... 141
E.1 BER-TLV tag fields ... 141
E.2 BER-TLV length fields ... 142
E.3 BER-TLV value fields ... 142

Annex F (informative) BER-TLV data object handling ... 143
F.1 Generations and templates in a constructed DO ... 143
F.2 Referencing by an extended header ... 144
F.3 Use of the UPDATE DATA command ... 146
F.4 Security attribute for one DO ... 148
F.5 Example of key referencing in a self-controlled DO ... 149

Annex G (informative) Template extension by tagged wrapper ... 151
G.1 General ... 151
G.2 Referencing within the current EF ... 151
G.3 Referencing within the current application DF, first example ... 152
G.4 Referencing in the current application DF, second example ... 153
G.5 Referencing out of the current application DF ... 154
G.6 Warnings ... 154

Annex H (informative) Parsing an extended header against its target DO ... 155

Annex I (informative) Use case of WTX (waiting time extension) procedure and application waiting time procedure ... 155

Bibliography ... 158

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

This third edition cancels and replaces the second edition (ISO/IEC 7816-4:2005), and incorporates the Amendment ISO/IEC 7816-4:2005/Amd.1:2008.

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: 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*

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

Introduction

ISO/IEC 7816 [6] 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 7816-13 specifies commands for handling the life cycle of applications.
  — ISO/IEC 7816-15 specifies cryptographic information application.

ISO/IEC 10536 [15] specifies access by close coupling. ISO/IEC 14443 [18] and ISO/IEC 15693 [20] 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

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

— JPN 2137026, Portable electronic device

— JPN 2831660, Portable electronic device

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

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

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

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

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

Identification cards — Integrated circuit cards —

Part 4:
Organization, security and commands for interchange

1 Scope

This part of ISO/IEC 7816 is intended to be used in any sector of activity. It 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. If the card supports simultaneous use of more than one physical interface, the relationship between what happens on different physical interfaces is out of the scope of this edition of ISO/IEC 7816-4.

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

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

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, also known as Information file

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

3.4
application DF
dedicated file (DF) 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
base template
value field of constructed data object excluding DOs resulting from resolution of indirect referencing

3.11
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)

3.12
command-response pair
set of two messages at the interface: a command APDU followed by a response APDU in the opposite direction

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

3.13
command chaining
means used by the outside world to tell the card that the command data of a sequence of successive command-response pairs must be processed together

3.14
context-specific class
class of a tag with its first or only byte from '80' to 'BF'

3.15
current template
sequence of data objects which can be directly referenced by their sole tag in a command for interchange, i.e. the value field of the current constructed DO (which may be virtual)

3.16
data element
item of information seen at the interface for which are specified a name, a description of logical content, a format and a coding

3.17
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

3.18
data unit
smallest set of bits that can be unambiguously referenced within an EF supporting data units

3.19
dedicated file
structure containing file control information and, optionally, memory available for allocation

3.20
DF name
data element (up to sixteen bytes) that uniquely identifies a DF in the card

3.21
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

3.22
directory file
optional EF containing a list of applications supported by the card and optional related data elements

3.23
elementary file
set of data units or records or data objects sharing the same file identifier

3.24
extended header
data element referencing one or several DOs in a constructed DO

3.25
extended header list
concatenation of extended headers

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

3.26
file
structure for application and/or data in the card, as seen at the interface when processing commands

3.27
file identifier
data element (two bytes) used to address a file

3.28
header list
concatenation of pairs of tag field and length field without delimitation

3.29
information file
optional EF indicating operating characteristics of the card, also known as Answer-to-Reset file

3.30
interindustry
standardized in the ISO/IEC 7816 [6] series of standards

3.31
internal EF
EF for storing data interpreted by the card

3.32
key
sequence of symbols controlling a cryptographic operation (e.g. encipherment, decipherment, a private or a public operation in a dynamic authentication, signature generation, signature verification)

3.33
master file
unique DF representing the root in a card using a hierarchy of DFs

3.34
offset
number sequentially referencing a data unit in an EF supporting data units, or a byte in a record

3.35
oversize payload
payload which exceeds the current size constraints of the APDU

3.36
parent file
DF immediately preceding a given file within a hierarchy of DFs

3.37
password
data that may be required by the application to be presented to the card by its user for authentication purpose

3.38
path
concatenation of file identifiers without delimitation

3.39
payload
data of arbitrary length, to be sent to the card or by the card, in order to be processed together

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

3.40
private key
that key of an entity's asymmetric key pair that should only be used by that entity

[ISO/IEC 9798-1 [10]]

3.41
provider
authority who has or who obtained the right to create a DF in the card

3.42
public key
that key of an entity's asymmetric key pair that can be made public

[ISO/IEC 9798-1 [10]]

3.43
record
string of bytes referenced and handled by the card within an EF supporting records

3.44
record identifier
number used to reference one or more records within an EF supporting records

3.45
record number
sequential number that uniquely identifies each record within an EF supporting records

3.46
registered application provider identifier
data element (five bytes) that uniquely identifies an application provider

3.47
resetting code
data to be presented to a card in order to modify the value of a counter

3.48
response chaining
means used by the card to tell the outside world that the response data of any command-response pair followed by the response data of a sequence of GET RESPONSE command-response pairs should be processed together

3.49
secret key
key used with symmetric cryptographic techniques by a set of specified entities

[ISO/IEC 11770-3 [17]]

3.50
secure messaging
set of means for cryptographic protection of (parts of) command-response pairs

3.51
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

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

3.51
security environment
set of components required by an application in the card for secure messaging or for security operations

3.52
self-controlled DO
constructed DO which nests at least a DO'62' nesting security attributes

3.53
short EF identifier
data element (five bits) used to address an elementary file

3.54
structure
DF, EF, record, DataString or DO

3.55
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)

3.56
tag list
concatenation of tag fields without delimitation

3.57
tagged wrapper
wrapper which provides a tag for local addressing of the DO it references

3.58
template
concatenation of BER-TLV data objects, forming the value field of a constructed BER-TLV data object

3.59
template extension
part of the value field of a constructed DO resulting from automatic resolution of indirect referencing

3.60
transient selection
structure selection needed when performing a C-RP, the success of which will not modify the current validity area

3.61
transient VA
validity area (VA) set transiently during execution of a command which handles DOs

3.62
user
user of the card, also known as cardholder

3.63
validity area
result of all successful selections performed on a logical channel

3.64
virtual root DO
virtual constructed DO'7F70' made current by the selection of a file, a record or a DataString supporting DO handling

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

3.65
wrapper
concatenation of DOs referencing a DO

3.66
working EF
EF for storing data not interpreted by the card

4 Symbols and abbreviated terms

AID	application identifier
AMB	access mode byte
AMF	access mode field
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
CP	control parameter (file control parameter or data object control parameter)
CP DO	control parameter BER-TLV data object
C-RP	command-response pair
DF	dedicated file
DIR	directory
DO	BER-TLV data object
DO'…'	BER-TLV data object, the tag of which is a hexadecimal value given between simple quotes
DST	control reference template for digital signature
EF	elementary file
EF.ARR	access rule reference file
EF.ATR/INFO	Answer-to-Reset file, or Information 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

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

L_c field	length field for coding the number N_c
LCS	Life cycle status
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
OID	object identifier, as defined by ISO/IEC 8825-1
PIX	proprietary application identifier extension
P1-P2	parameter bytes (inserted for clarity, the dash is not significant)
RFU	reserved for future use by ISO/IEC JTC 1/SC 17
RID	registered application provider identifier
SC	security condition
SCB	security condition byte
SCQL	structured card query language
SE	security environment
SEID	security environment identifier
SM	secure messaging
SPT	security parameter template
SW1-SW2	status bytes (inserted for clarity, the dash is not significant)
TLV	tag, length, value
{T-L-V}	data object (inserted for clarity, the dashes and curly brackets are not significant)
VA	validity area
'XY'	notation where any upper case letter from G to Z stands for a hexadecimal digit from '0' to '9' or 'A' to 'F', equal to XY to the base 16. Identical letters do not state that the most and least significant quartets are identical.

5 Command-Response pairs

5.1 Conditions of operation

A physical interface between the card and the outside world shall be enabled to support processing of command-response pairs. The enabling process is defined by interface-specific protocols. With their own words (between double quotes), the following standards define enabling procedures:

— ISO/IEC 7816-3 defines "activation of contacts", "cold reset" or "warm reset", and possible "Protocol and Parameter Selection".

— ISO/IEC 7816-12 defines "electrical connection" of contacts with reference to the USB specification, the "Configured" and "Initial" state of the device, and "ATR".

— ISO/IEC 14443 [18] (all parts) defines how to set a proximity card to an "ACTIVE" state.

Those standards also define procedures and situations which disable the physical interface. A disabled physical interface shall not support processing of command-response pairs.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

5.2 Syntax

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

In any command APDU 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 119, third software function table) in the historical bytes (see 12.1.1) or in EF.ATR/INFO (see 12.2.2), then the card handles short and extended length fields. Otherwise (default value), the card handles only short length fields. In a command APDU longer than 5 bytes, [AC1] the use of extended length fields [AC1] is indicated by the first byte after P2 equal to '00'.

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.

Table 1 — Command-response pair (C-RP)

Field	Description	Number of bytes	Direction
Command header	Class byte denoted CLA	1	To the card
	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)	From the card
Response trailer	Status bytes denoted SW1-SW2	2	

N_e denotes the maximum number of bytes expected in the response data field, regardless of any structure of the data within this 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 C-RP, 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.

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

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 P1 or P2 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 5.4), the instruction byte denoted INS (see 5.5) and the status bytes denoted SW1-SW2 (see 5.6). In those bytes, the RFU bits shall be set to 0 unless otherwise specified.

5.3 Chaining procedures

5.3.1 General

Chaining procedures are used either to support payload fragmentation or for a process involving several consecutive C-RPs.

5.3.2 Payload fragmentation

A command payload is data of arbitrary length to be sent to the card in order to be processed together. A response payload is data of arbitrary length to be received from the card as requested. A payload is oversize if its length is larger than available in a data field (see NOTE); chaining is needed to transmit such a payload:

— Chaining of commands supports the transmission to the card of an oversize command payload. The payload is fragmented; each fragment is a command data field which complies with size limitations.

— Chaining of responses supports the recovery from the card of an oversize response payload. The payload is fragmented; each fragment is a response data field which complies with size limitations.

The receiver shall concatenate the successively transmitted fragments to recover the payload.

NOTE APDU syntax limits the size of data fields. More size limitations may be stated (see 12.7.1); if an Le field ('0000' or '000000') indicates Ne = '010000', then all the required information should be returned, up to 65 536 bytes. Fragmentation will occur with the short format of length fields if the command payload exceeds 255 bytes and/or the response payload exceeds 256 bytes. Fragmentation should not occur with the extended format of length fields if payloads comply with stated size limitations (see 12.7.1).

5.3.3 Command chaining

This clause specifies a mechanism whereby in the interindustry class (CLA < '80', see Table 2 and Table 3) consecutive C-RPs can be chained. If the card supports the mechanism, then it shall indicate it (see

Table 119, third software function table) in the historical bytes (see 12.1.1) or in EF.ATR/INFO (see 12.2.2).

NOTE The contents of this clause do not depend on the transmission protocol. ISO/IEC 7816-3 describes chaining when using protocol T=0.

For chaining in the interindustry class, bit b5 of CLA shall be used while the other seven bits are constant.

— If bit b5 is set to 0, then the command is the only or last command of a chain.

— If bit b5 is set to 1, then the command is not the last command of a chain.

The mechanism may be used:

— to transmit an oversize command payload:

  — all CLA bytes of the commands shall be the same, except for bit b5 (see above).

    — If bit b5 is set to 1, then the L_e field shall be absent.

© ISO/IEC 2013 – All rights reserved
Documents Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

  - If bit b5 is set to 0, then an L_e field may be present.
  - all INS P1 P2 bytes of the commands shall be the same.
- As specified elsewhere in this document (see example in Annex C).
- For any application-defined process involving several consecutive C-RPs
  - bit b5 of CLA shall be used as defined above.
  - the logical channel indicated by CLA shall be the same.
  - there is no constraint on the values of INS P1 P2 bytes of the commands.

This document specifies the card behaviour only in the case where, once initiated, a chain of C-RPs is successfully processed before initiating a C-RP not part of the chain. If this condition is not respected, the card behaviour is out of scope of this document, but may be described in a specification.

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; the use of warning indications is defined in see 5.6; 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.

5.3.4 Response chaining

SW1 = '61' and GET RESPONSE support the transmission of an oversized response payload:

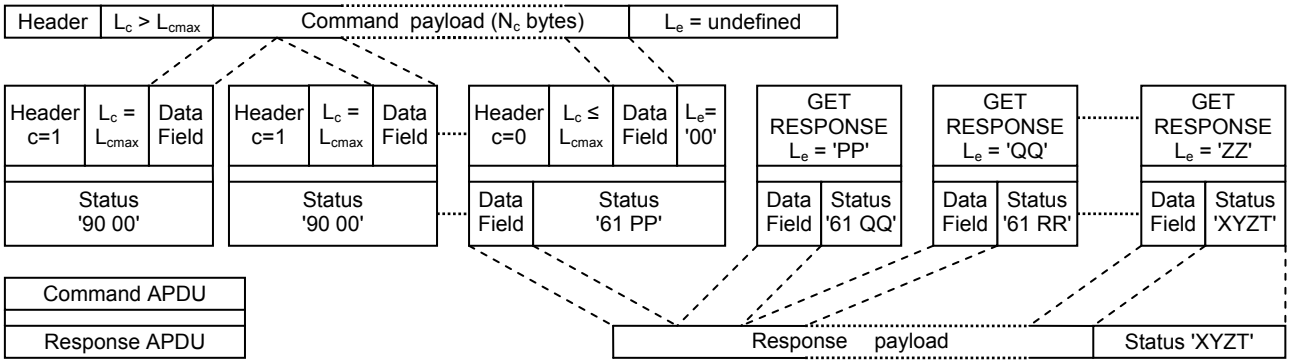
- all CLA bytes of the commands involved in response chaining shall be the same. By definition response chaining starts with that C-RP where SW1 is set to '61'.
- with the exception of the first command APDU of the sequence, all INS P1-P2 bytes of the command APDUs shall be 'C0 00 00' (GET RESPONSE).
- as in command chaining, payload transmission shall be interrupted by any C-RP different from GET RESPONSE, or by any C-RP on another logical channel.
- contrary to command chaining, this possible termination is normal when the outside world considers that it has received enough data: the exchange should continue normally with an arbitrary C-RP.
- however, this document does not define the behaviour of the card if the outside world tries to resume response chaining after e.g. the execution of a command on another logical channel. The behaviour may be defined by the application.

If defined by the application, response chaining may be used for checking the availability of data, which are not necessarily required. The card may indicate availability by SW1-SW2 = '61XY', without sending any response data; the outside world will or will not send (a) GET RESPONSE (s).

In Figure 1, c= 0 and c=1 indicates the value of bit b5 of CLA. Lcmax indicates the maximum value of short or extended Lc field the ICC supports.

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018



WARNING — This is an example where the interface device chooses to send the longest command data fields the card supports, and to recover all data made available by the card. None of those choices is mandated.

Figure 1 — Transmission to the card of an oversize command payload using command chaining, followed by the transmission by the card of an oversize response payload using response chaining.

5.4 Class byte

5.4.1 Coding

CLA indicates the class of the command. Bit b8 of CLA distinguishes between the interindustry class and the proprietary class.

— Bit b8 set to 0 indicates the interindustry class.

— Bit b8 set to 1 indicates the proprietary class, except for the value 'FF' which is invalid due to specifications in ISO/IEC 7816-3. The application-context defines the other bits of CLA in proprietary class.

The values 000x xxxx and 01xx xxxx are specified hereafter. The values 001x xxxx are RFU.

Table 2 specifies 000x xxxx as the first interindustry values.

— Bits b8, b7 and b6 are set to 000.

— Bit b5 controls command chaining (see 5.3.3).

— Bits b4 and b3 indicate secure messaging (see clause 10).

— Bits b2 and b1 encode a logical channel number from zero to three (see 5.4.2).

Table 2 — First interindustry values of CLA

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	**x**	-	-	-	-	**Command chaining control** (see 5.3.3)
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 clause 10, command header not processed according to 10.2.3.1
0	0	0	-	1	1	-	-	— SM according to clause 10, command header authenticated according to 10.2.3.1
0	0	0	-	-	-	**x**	**x**	**Logical channel number from zero to three** (see 5.4.2)

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

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 clause 10, command header not processed according to 10.2.3.1
0	1	-	**x**	-	-	-	-	**Command chaining control** (see 5.3.3)
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 5.4.2)

Table 3 specifies 01xx xxxx as further interindustry values.

— Bits b8 and b7 are set to 01.

— Bit b6 indicates secure messaging (see clause 10).

— Bit b5 controls command chaining (see 5.3.3).

Bits b4 to b1 encode a number from zero to fifteen; this number plus four is the logical channel number from four to nineteen (see 5.4.2).

5.4.2 Logical channels

This clause specifies a mechanism whereby in the interindustry class, C-RPs can refer to logical channels. Each logical channel has its own security status (see 9.3) and validity area (see 7.2). The way to share a security status is out of scope of this document.

If the card supports the mechanism, then it shall indicate the maximum number of available logical channels (see

Table 119, third software function table) in the historical bytes (see 12.1.1) or in EF.ATR/INFO (see 12.2.2).

— 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 number of the logical channel of the C-RP.

— Enabling the physical interface (see 5.1) opens the basic logical channel, which shall remain open until disabling of the physical interface. It may be reset (see below). The number of the basic logical channel is zero.

— Cards not supporting additional logical channel(s) (default value) shall use only the basic logical channel.

— Any additional logical channel shall be opened by completion of either a SELECT or a SELECT DATA command (see 11.1.1 and 11.4.2) where CLA encodes the number of a logical channel not yet in use, or a MANAGE CHANNEL command with open function (see 11.1.2).

— Any additional logical channel can be closed by the completion of a MANAGE CHANNEL command with close function. (see 11.1.2). After closing, the logical channel shall be available for re-use.

— Even if more than one logical channel is opened there shall be no interleaving of C-RPs (see 5.2).

— If sharability is not explicitly excluded by the file descriptor byte (see bit b7 in Table 11), more than one logical channel may be opened to the same structure (see clause 7), i.e. to a DF, possibly an application DF, and also possibly to an EF.

— If sharability is not explicitly excluded by the data descriptor byte (see bit b7 in Table 13) more than one logical channel may be opened to the same DO.

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

— Any logical channel can be reset by the completion of a MANAGE CHANNEL command with reset function (see 11.1.2).

5.5 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 [6] 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.

ISO/IEC 7816 [6] specifies the use of those commands in the interindustry class.

— This document specifies commands for interchange (see clause 11).

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

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

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

— ISO/IEC 7816-13 specifies commands for application management in a multi-application environment.

In the interindustry class, bit b1 of INS indicates a data field format as follows.

— If bit b1 is set to 0 (even INS code), then no indication is provided.

— If bit b1 is set to 1 (odd INS code), payloads (if any) shall be encoded in BER-TLV (see 8.1).

5.6 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', '6701', '6702', '6B00', '6D00', '6E00', '6F00' and '9000' that are interindustry.

Figure 2 shows the structural scheme of the values '9000' and '61XX' to '6FXX' for SW1-SW2.

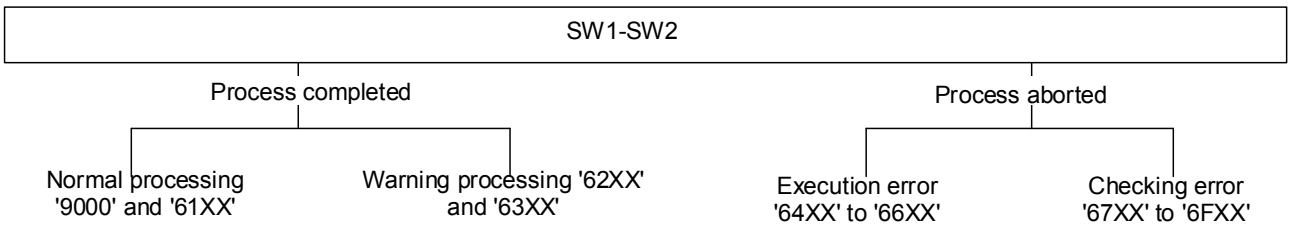


Figure 2 — Structural scheme of values of SW1-SW2

All interindustry values of SW1-SW2 are independent from any transmission protocol. 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 [6]. Table 6 lists all the specific interindustry warning and error conditions used in ISO/IEC 7816 [6] at the time of publication.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

Table 4.1 — Commands in the alphabetic order

Command name	INS	See
ACTIVATE FILE	'44'	Part 9
[AC1] ACTIVATE RECORD (S) [AC1]	'08'	11.3.9
APPEND RECORD	'E2'	11.3.6
APPLICATION MANAGEMENT REQUEST	'40', '41'	Part 13
CHANGE REFERENCE DATA	'24', '25'	11.5.7
COMPARE	'33'	11.6.1
CREATE FILE	'E0'	Part 9
DEACTIVATE FILE	'04'	Part 9
[AC1] DEACTIVATE RECORD (S) [AC1]	'06'	11.3.10
DELETE DATA	'EE'	Part 9
DELETE FILE	'E4'	Part 9
DISABLE VERIFICATION REQUIREMENT	'26'	11.5.9
ENABLE VERIFICATION REQUIREMENT	'28'	[AC1] 11.5.8 [AC1]
ENVELOPE	'C2', 'C3'	11.7.2
ERASE BINARY	'0E', '0F'	11.2.7
ERASE RECORD (S)	'0C'	11.3.8
EXTERNAL (/MUTUAL) AUTHENTICATE	'82'	11.5.4
GENERAL AUTHENTICATE	'86', '87'	11.5.5
GENERATE ASYMMETRIC KEY PAIR	'46', '47'	Part 8
GET ATTRIBUTE	'34','35'	11.6.2
GET CHALLENGE	'84'	11.5.3
GET DATA/GET NEXT DATA	'CA'/'CC'	11.4.3
GET DATA/GET NEXT DATA	'CB'/'CD'	11.4.4
GET RESPONSE	'C0'	11.7.1
INTERNAL AUTHENTICATE	'88'	11.5.2
LOAD APPLICATION	'EA', 'EB'	Part 13
MANAGE CHANNEL	'70'	11.1.2
MANAGE DATA	'CF'	Part 9
MANAGE SECURITY ENVIRONMENT	'22'	11.5.11
PERFORM BIOMETRIC OPERATION	'2E', '2F'	Part 8
PERFORM SCQL OPERATION	'10'	Part 7
PERFORM SECURITY OPERATION	'2A', '2B'	Part 8
PERFORM TRANSACTION OPERATION	'12'	Part 7
PERFORM USER OPERATION	'14'	Part 7
PUT DATA	'DA', 'DB'	11.4.6
PUT NEXT DATA	'D8', 'D9'	11.4.7
READ BINARY	'B0', 'B1'	11.2.3
READ RECORD (S)	'B2', 'B3'	11.3.3
REMOVE APPLICATION	'EC', 'ED'	Part 13
RESET RETRY COUNTER	'2C', '2D'	11.5.10
SEARCH BINARY	'A0', 'A1'	11.2.6
SEARCH RECORD	'A2'	11.3.7
SELECT	'A4'	11.1.1
SELECT DATA	'A5'	11.4.2
TERMINATE CARD USAGE	'FE'	Part 9
TERMINATE DF	'E6'	Part 9
TERMINATE EF	'E8'	Part 9
UPDATE BINARY	'D6', 'D7'	11.2.5
UPDATE DATA	'DE', 'DF'	11.4.8
UPDATE RECORD	'DC', 'DD'	11.3.5
VERIFY	'20', '21'	11.5.6
WRITE BINARY	'D0', 'D1'	[AC1] 11.2.4 [AC1]
WRITE RECORD	'D2'	11.3.4

Table 4.2 — Commands in the numeric order

INS	Command name	See
'04'	DEACTIVATE FILE	Part 9
'06'	[AC1] DEACTIVATE RECORD (S) [AC1]	11.3.10
'08'	[AC1] ACTIVATE RECORD (S) [AC1]	11.3.9
'0C'	ERASE RECORD (S)	11.3.8
'0E', '0F'	ERASE BINARY	11.2.7
'10'	PERFORM SCQL OPERATION	Part 7
'12'	PERFORM TRANSACTION OPERATION	Part 7
'14'	PERFORM USER OPERATION	Part 7
'20', '21'	VERIFY	11.5.6
'22'	MANAGE SECURITY ENVIRONMENT	11.5.11
'24', '25'	CHANGE REFERENCE DATA	11.5.7
'26'	DISABLE VERIFICATION REQUIREMENT	11.5.9
'28'	ENABLE VERIFICATION REQUIREMENT	[AC1] 11.5.8 [AC1]
'2A', '2B'	PERFORM SECURITY OPERATION	Part 8
'2C', '2D'	RESET RETRY COUNTER	11.5.10
'2E', '2F'	PERFORM BIOMETRIC OPERATION	Part 8
'33'	COMPARE	11.6.1
'34','35'	GET ATTRIBUTE	11.6.2
'40', '41'	APPLICATION MANAGEMENT REQUEST	Part 13
'44'	ACTIVATE FILE	Part 9
'46', '47'	GENERATE ASYMMETRIC KEY PAIR	Part 8
'70'	MANAGE CHANNEL	11.1.2
'82'	EXTERNAL (/MUTUAL) AUTHENTICATE	11.5.4
'84'	GET CHALLENGE	11.5.3
'86', '87'	GENERAL AUTHENTICATE	11.5.5
'88'	INTERNAL AUTHENTICATE	11.5.2
'A0', 'A1'	SEARCH BINARY	11.2.6
'A2'	SEARCH RECORD	11.3.7
'A4'	SELECT	11.1.1
'A5'	SELECT DATA	11.4.2
'B0', 'B1'	READ BINARY	11.2.3
'B2', 'B3'	READ RECORD (S)	11.3.3
'C0'	GET RESPONSE	11.7.1
'C2', 'C3'	ENVELOPE	11.7.2
'CA'/'CC'	GET DATA/GET NEXT DATA	11.4.3
'CB'/'CD'	GET DATA/GET NEXT DATA	11.4.4
'CF'	MANAGE DATA	Part 9
'D0', 'D1'	WRITE BINARY	[AC1] 11.2.4 [AC1]
'D2'	WRITE RECORD	11.3.4
'D6', 'D7'	UPDATE BINARY	11.2.5
'D8', 'D9'	PUT NEXT DATA	11.4.7
'DA', 'DB'	PUT DATA	11.4.6
'DC', 'DD'	UPDATE RECORD	11.3.5
'DE', 'DF'	UPDATE DATA	11.4.8
'E0'	CREATE FILE	Part 9
'E2'	APPEND RECORD	11.3.6
'E4'	DELETE FILE	Part 9
'E6'	TERMINATE DF	Part 9
'E8'	TERMINATE EF	Part 9
'EA', 'EB'	LOAD APPLICATION	Part 13
'EE'	DELETE DATA	Part 9
'EC', 'ED'	REMOVE APPLICATION	Part 13
'FE'	TERMINATE CARD USAGE	Part 9

— In the interindustry class, any valid INS code not defined in ISO/IEC 7816 [6] is RFU.

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

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

	SW1-SW2	Meaning
Normal processing	'9000'	No further qualification
	'61XX'	SW2 encodes the number of data bytes still available (see text below)
Warning processing	'62XX'	State of non-volatile memory is unchanged (further qualification in SW2, see Table 6)
	'63XX'	State of non-volatile memory may have changed (further qualification in SW2, see Table 6)
Execution error	'64XX'	State of non-volatile memory is unchanged (further qualification in SW2, see Table 6)
	'65XX'	State of non-volatile memory may have changed (further qualification in SW2, see Table 6)
	'66XX'	Security-related issues (further qualification in SW2 is RFU)
Checking error	'67XX'	Wrong length (further qualification in SW2, see Table 6)
	'68XX'	Functions in CLA not supported (further qualification in SW2, see Table 6)
	'69XX'	Command not allowed (further qualification in SW2, see Table 6)
	'6AXX'	Wrong parameters P1-P2 (further qualification in SW2, see Table 6)
	'6B00'	Wrong parameters P1-P2
	'6CXX'	Wrong L_e field; SW2 encodes the exact number of available data bytes (see text below)
	'6D00'	Instruction code not supported or invalid
	'6E00'	Class not supported
	'6F00'	No precise diagnosis

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 the C-RP which returned '61XY' used the extended length fields, the GET RESPONSE may also use an extended L_e field according to the buffer sizes stated in DO'7F66' (see 12.7.1). This feature is used for response chaining (see 5.3.4).

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.

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

When command chaining is used for payload fragmentation (see 5.3.3), in response to a command that is not the last command of a chain (see 5.3.3), interindustry warning indications are prohibited (see also ISO/IEC 7816-3), i.e. SW1 shall be set to neither '62' nor '63'.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

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 12.5.1)
	'81'	Part of returned data may be corrupted
	'82'	End of file or record reached before reading N_e bytes, or unsuccessful search.
	'83'	Selected file deactivated
	'84'	File or data control information not formatted according to 7.4
	'85'	Selected file in termination state
	'86'	No input data available from a sensor on the card
	'87'	[A1] At least one of the referenced records is not processed for some reason, e.g. record deactivated, security status not satisfied or conditions of use not satisfied. [A1]
'63' (warning)	'00'	No information given
	'40'	Unsuccessful comparison (exact meaning depends on the command)
	'81'	File filled up by the last write
	'CX'	Counter from 0 to 15 encoded by 'X' (exact meaning depends on the command)
'64' (error)	'00'	No information given
	'01'	Immediate response required by the card
	'02' to '80'	Triggering by the card (see 12.5.1)
	'81'	Logical channel shared access denied
	'82'	Logical channel opening denied
'65' (error)	'00'	No information given
	'81'	Memory failure
'66' (error)	'00'	No information given, other values are RFU
'67 (error)	'00'	No information given
	'01'	Command APDU format not compliant with this standard (see 5.1)
	'02'	The value of L_c is not the one expected.
'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 DOs missing
	'88'	Incorrect secure messaging DOs
'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 RFU.		

6 Data objects

This clause specifies two categories of data objects: SIMPLE-TLV data objects and BER-TLV data objects, the latter abbreviated by DOs in this document.

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

6.1 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 11.3.1) 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.

NOTE This standard defines neither tag values nor value fields of ⟦AC1⟩ SIMPLE-TLV ⟨AC1⟧ data objects. Hence, ⟦AC1⟩ SIMPLE-TLV ⟨AC1⟧ data objects addressing cannot be used for interchange.

6.2 BER-TLV data objects

Each BER-TLV data object (DO) 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. Any non empty DO is denoted {T-L-V}.

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. ISO/IEC 7816 [6] supports tag fields of one, two and three bytes; longer tag fields are RFU.

The length field encodes a length, i.e. a number denoted N, according to ISO/IEC 8825-1. If N is zero, there is no value field, i.e. the DO is empty, and noted {T-'00'}. Otherwise (N > 0), the value field consists of N consecutive bytes, and the DO is noted {T-L-V}. ISO/IEC 7816 [6]

a) precludes the use of the “indefinite length” (coded '80'), according to the DER encoding rules;

b) recommends to use the shortest possible coding of the length field, according to DER encoding rules (see ISO/IEC 8825-1);

c) uses length fields consisting of one to five bytes, longer length fields are RFU.

NOTE 1 In order to ascertain the length of the length field, a specification may mandate recommendation b), i.e. the use of shortest length field for the coding of a given length.

NOTE 2 ISO/IEC 7816-4 uses '80' with a specific meaning in the value field of an extended header DO (see 8.4.5).

NOTE 3 Annex E provides the detailed coding of tag and length fields.

6.3 Constructed DOs versus primitive DOs

A constructed, non empty DO is denoted {T-L-{T1-L1-V1} … - {Tn-Ln-Vn}}. Its tag T indicates the structure of its value field (see Annex E). This value field is called a template, which may:

— either consist of one DO, called "nested" in the constructed DO.

— or consist of a concatenation of several nested DOs, (n DOs in the example above), without padding (see 8.1.1).

Unless otherwise specified (e.g. wrapper (see 8.4.8) or tagged wrapper (see 8.4.9), ISO/IEC 7816-15, ISO/IEC 24727 [23]), the order of DOs within a template is not defined in this document.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

See Annex E for the identification of a primitive or constructed data object by the first byte of its tag. A possible structure of the value field of a primitive data object is to be defined elsewhere.

7 Structures for applications and data

7.1 Available structures

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 out of scope of ISO/IEC 7816 [6]. The following structures are supported:

— Dedicated file (DF):
The DFs host applications and/or group files and/or store DOs. An application DF is a DF hosting an application. A DF may be the parent of other structures, whose types shall belong to the following set {DF, EF, DO}. These other structures are said to be immediately under the DF.

— Elementary file (EF):
The EFs store data. An EF may be the parent of other structures, whose types shall belong to the following set {DO, Record, DataString}. These other structures are said to be immediately under the EF. 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.

— Record:
The records store data. A record may be the parent of other structures, whose types shall belong to the following set {DO}. These other structures are said to be immediately under the record.

— DataString:
DataStrings store data. A DataString is a sequence of bytes in a transparent EF. A DataString may be the parent of other structures, whose types shall belong to the following set {DO}. These other structures are said to be immediately under the DataString.

— Data object (DO):
The DOs store data. A DO may be the parent of other structures, whose types shall belong to the following set {DO}. These other structures are said to be immediately under the DO.

Two types of logical organization are provided.

— Figure 3 illustrates a hierarchy of DFs with its corresponding security architecture (see clause 9). 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.

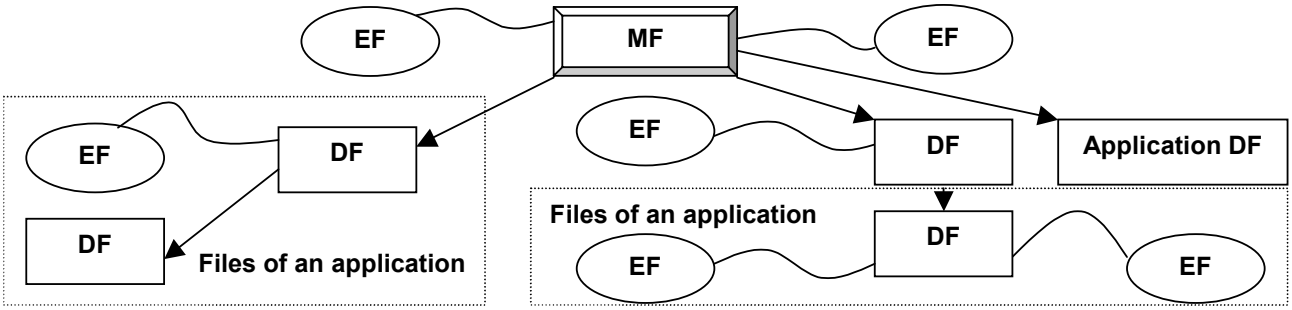


Figure 3 — Example of hierarchy of DFs

— Figure 4 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.

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

Figure 4 — Example of independent application DFs

7.2 Validity area

7.2.1 Definitions and attributes

The validity area (VA) on a logical channel is the result of all successful selections performed on that logical channel. It generalizes the concept of current file defined in the previous version of ISO/IEC 7816-4. The VA determines the resolution of DO tags and file identifiers. The VA consists of:

— curAppDF: a reference either to a DF or an application DF. It is always set.

— curDF: a reference to a DF, which may be an application DF. It is always set.

— curEF: a reference to an EF belonging to the current DF. It is not always set.

— curFile: a reference to a file, it is always set. Its value shall be identical to curDF if curEF is not set, and identical to curEF if curEF is set.

— curRecord: a reference to a record, belonging to a current EF structured in records. It is not always set.

— curDataString: a reference to a sequence of bytes being part of a transparent current EF. It is not always set.

— curConstructedDO: it shall be set for DO handling. When set, it is a reference to a constructed DO. It is not always set.

— curPrimitiveDO: a reference to a primitive DO whose parent is referenced by curConstructedDO. It is not always set.

— curDO: It shall be set for DO handling. When set, it is a reference to a DO, its value shall be identical to curConstructedDO if curPrimitiveDO is not set, and identical to curPrimitiveDO if curPrimitiveDO is set.

NOTE 1 curFile can be calculated from curDF and curEF and vice versa. Thus either curFile is dispensable or curDF and curEF are dispensable. The reason for redundancy is that some functions are easier to describe with curFile (e.g. ACTIVATE, DEACTIVATE) and other functions are easier to describe with curDF and curEF.

NOTE 2 curDO can be calculated from curConstructedDO and curPrimitiveDO and vice versa. Thus either curDO is dispensable or curConstructedDO and curPrimitiveDO are dispensable. The reason for redundancy is that some functions are easier to describe with curDO and other functions are easier to describe with curConstructedDO and curPrimitiveDO.

NOTE 3 The current SE does not belong to the current VA.

7.2.2 Basic rules for VA handling and use

The following list contains a non exhaustive list of rules describing the use of the VA. More rules are given in clauses containing command descriptions:

a) Enabling a physical interface (see 5.1), which opens the basic logical channel, sets the values of curAppDF and curDF to identical values, i.e. they reference either the MF or the implicitly selected application.

b) Resetting a logical channel resets the VA to the same value set when opening that logical channel. See 11.1.2 for other consequences of resetting.

c) Opening a logical channel sets the values of curAppDF and curDF to identical values (see 11.1.1 and 11.1.2).

d) Selecting an application DF sets curDF and curAppDF so that they reference the selected application DF.

AVA Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

e) Selecting a DF which is not an application DF sets curDF so that it references the selected DF. It sets or confirms curAppDF so that curAppDF references either the nearest application DF (if any) in the ancestors (parent, grandparent…) of the selected DF, or the MF if no application DF exists in the ancestors.

f) Selecting an EF sets curEF so that it references the selected EF, and curDF so that it references the parent of the selected EF (see rule e)). When EF selection occurs as a side-effect of a C-RP using referencing by short EF identifier, curEF may change, while curDF does not change.

g) Selecting a record sets curRecord so that it references the selected record as current record, and curEF so that it references the parent of the selected record (see rule f)).

h) Selecting a DataString within a transparent EF sets curDataString so that it references the selected DataString and curEF so that it references the parent of the selected DataString (see rule f)).

i) Selecting a structure containing DOs sets the curConstructedDO so that it references the selected DO according to the specified structure. If the selected structure is a constructed DO, it sets the curConstructedDO so that it references the selected DO. If the specified structure is a {Application DF, DF, EF, record or DataString}, structure selection sets the curConstructedDO so that it references a virtual root DO'7F70' as current Constructed DO. This DO shall be associated with the last encountered structure supporting DOs in the list above.

j) Selecting a primitive DO sets curPrimitiveDO so that it references the specified DO as current PrimitiveDO, and curConstructedDO so that it references the parent of the selected primitive DO.

k) For DO handling, the current template is the value of the DO referenced by curConstructedDO (see rule i).

An explicit selection may modify elements of the VA beyond the explicit selection due to recursion. Such implicit selections shall have the same outcome as an explicit selection.

EXAMPLE The selection of a constructed DO in a record will set curConstructedDO (rule i) explicitly. It will implicitly set or confirm curRecord (rule g)), curEF (rule f)), curDF (rule e)) and curAppDF (rule d)).

7.3 Structure selection

7.3.1 Structure selection methods

Selecting a structure allows access to its data and to structures below, if any. Structures may be selected implicitly, i.e. automatically (see 7.2.2, rules a), g)) after enabling a physical interface (see 5.1). 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 12.2.3) 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 (see 11.4.1.2). The value '3FFF' is reserved (see below and 11.4.1). The value '0000' is reserved (see 11.2.2 and 11.4.1). In order to unambiguously select any file by its identifier, all EFs and DFs immediately under a given DF shall have different file identifiers.

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 12.2.1 and 12.2.2). The path allows an unambiguous selection of any file from the MF or from the current DF (see 12.3).

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

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

binary, references the current EF. At MF level, the number thirty, i.e. 11110 in binary, is reserved (see 12.2.1). Short EF identifiers cannot be used in a path or as an EF identifier (e.g. in a SELECT command). All short EF identifiers of EF immediately under a given DF plus all short EF identifiers indicated in FCP DO'A2' associated with this DF shall be unique.

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

— If the first software function table (see Table 117) is present in the historical bytes (see 12.1.1) or in EF.ATR/INFO (see 12.2.2), then the indication is valid at card level.

— If a short EF identifier DO'88' (see 10.2.3.1 and Table 10) is present in the CPs of an EF, then the indication is valid at EF level.

Selection by tag — A DO may be selected by its sole tag, without further information on the VA, if and only if it belongs to the base template of the current template i.e. the value of the current constructed DO.

Selection by record number — If the EF pointed to by curEF supports records then a record number references a specific record in that EF. A record number is a positive integer.

Selection by offset — If the EF pointed to by curEF is transparent, then an offset references the beginning of a sequence of bytes in that EF. An offset is an integer ≥ 0.

7.3.2 File reference data element and DO

This interindustry DO'51'(see Table 7) references a file. It may have any length.

— An empty DO references the MF.

— If the length is one and if bits b8 to b4 of the data element are not all equal and if bits b3 to b1 are set to 000, then bits b8 to b4 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 11.1.1 and 12.3).

Table 7 — Coding of the file reference DO'51'

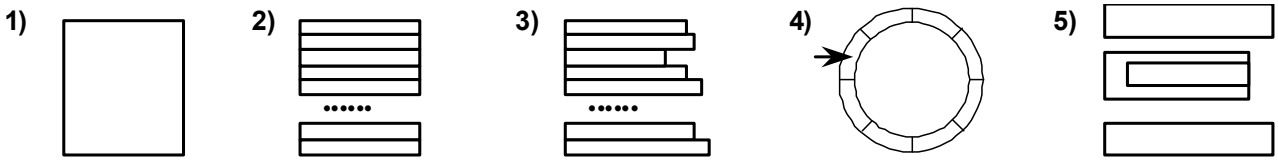
Tag	Length	Value
'51'	0	The empty data object references the MF
	1	Short EF identifier (bits b8 to b4 encode a number from one to thirty; bits b3 to b1 are set to 000)
	2	File identifier
	Even, > 2	Absolute path (the first two bytes are set to '3F00')
		Relative path (the first two bytes are not set to '3F00')
	Odd, > 2	Qualified path (the last byte shall be used as P1 in one or more SELECT commands)

© ISO/IEC 2013 – All rights reserved
Documents Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

7.3.3 General reference data element and DO

This interindustry DO'60' (see Table 86) and DO'7F72' (see Table 37) can reference any structure in a card. The value of DO'60' is used in the command data field of many CR-Ps handling DOs (see 11.4.2). In some cases, those commands temporarily transiently impact the VA; in other cases, they modify the VA.

7.3.4 Data referencing methods in elementary files



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) SIMPLE-TLV or BER-TLV structure

Figure 5 — EF structures

Data referencing method is an EF-dependent feature. An EF shall support at least one of the following structures:

— **Transparent structure —** The EF is seen at the interface as a single continuous, numbered sequence of data units accessible by commands for handling data units (see 11.2). Data unit size is an EF-dependent feature.

— **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 11.3). Record numbering method, SIMPLE-TLV or BER-TLV structure of the records are EF-dependent features. Three attributes are defined: record size, record organization and record LCS.

  — 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 may have a record life cycle. When it does, the record LCS distinguishes at least the following states: ACTIVATED and DEACTIVATED. The coding of a record LCS is out of scope for this part of ISO/IEC 7816 [6]. Within a given EF, either all records have a record life cycle or no record has a record life cycle. The presence of record life cycle is indicated by the CP (see Table 10).

— **SIMPLE-TLV structure** — The EF is seen at the interface as a set of SIMPLE-TLV data objects accessible by commands for handling data objects (see 11.4). This structure precludes BER-TLV structure

— **BER-TLV structure** — The EF is seen at the interface as a set of DOs accessible by commands for handling DOs (see 11.4). This structure precludes SIMPLE-TLV structure.

In DFs or applications, data may be referenced as DOs (see 6.2), the same way as in EFs. If the EF, DF or application supports this referencing, its selection sets the curConstructedDO (see 7.2.2 and 8.2.1).

7.4 File and data control information

7.4.1 File control information retrieval

By definition, the file control information is the byte string available in response to the SELECT command (see 11.1.1); it may be present for any file, i.e. any DF and any EF.

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

— 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 8 shows three interindustry templates:

— The FCP template is a set of CP DOs eligible for files, i.e. logical, structural and security attributes as listed in Table 10 and defined hereafter. Within the FCP template, the context-specific class is reserved for FCPs; tags '85' and 'A5' reference proprietary information.

— The FMD template is a set of file management data, i.e. interindustry DOs such as an application identifier as defined in 12.2.3, an application label as defined in 12.2.4 and an application expiration date as defined in ISO/IEC 7816-6, possibly nested within an application template as defined in 12.2.4. Within the FMD template, tags '53' and '73' reference discretionary data.

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

Table 8 — 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)

The three templates may be retrieved according to selection options of the SELECT command (see Table 62).

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

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

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 CPs. If present within such an EF, file control information shall be introduced by the appropriate tag, either a CP tag, or a FCI tag.

7.4.2 Data control information retrieval

By definition, the data control information is the byte string available in response to a SELECT command with P1='10' or P1='13' (see 11.1.1) or a SELECT DATA command if bit b3 of P2 is set to 1 (see 11.4.2); it may be present for any DO.

Table 9 — Interindustry templates for data control information

Tag	Value
'62'	Set of data control parameters (CP DOs, possibly including a DO'62')

DO'62' nests CP DOs.

— It may be present in the data control information of any structure (files or applications supporting a BER-TLV structure, constructed DO). It belongs and applies to the current template after structure selection.

— When present within the current base template (see 8.2.2) it applies to, it may be retrieved by GET DATA or GET NEXT DATA.

— When it is present in another template, it may be indirectly referenced by a tagged wrapper (see 8.4.8).

7.4.3 Control parameters

Table 10 lists CP DOs for files and data objects, all in the context-specific class. When a CP is present, the table states whether it occurs at most once (explicit indication), or may be repeated (no indication).

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

Table 10 — Control parameter data objects

Tag	Length	Value	Applies to
'80'	Var.	Number of data bytes in the file, excluding structural information	Any EF*
'81'	Var.	Number of data bytes in the file or DO, including structural information if any	File* or DO*
'82'	1	File descriptor byte (see 7.4.5 and Table 11)	File*
	2	File descriptor byte and data coding byte (see Table 118)	
	3 or 4	File descriptor byte, data coding byte and maximum record size on one or two bytes	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 (see NOTE)	
'83'	2	File identifier	File*
'84'	up to 16	DF name	DF
'85'	Var.	Proprietary information not encoded in BER-TLV	File
'86'	Var.	Security attribute in proprietary format	File
'87'	2	Identifier of an EF containing an extension of the file control information	DF*
'88'	0 or 1	Short EF identifier (see 7.4.4)	EF*
'8A'	1	Life cycle status (LCS, see 7.4.10 and Table 14)	File* or DO*
'8B'	Var.	Security attribute referencing the expanded format (see 9.3.3 and Table 38)	File*
'8C'	Var.	Security attribute in compact format, SE oriented (see Table 30)	File*
'8D'	2	Identifier of an EF containing security environment templates [AC1] (see 10.3.3) [AC1]	DF
'8E'	1	Logical channel security attribute (see 9.3.7 and Table 47)	File* or DO*
'8F'	1	Profile indicator (see Table 12)	EF supporting records*
'92'	1	Data descriptor byte (see 7.4.7)	DO* or EF* supporting BER-TLV structure
'96'	Var.	as defined in ISO/IEC 7816-11	see ISO/IEC 7816-11
'97'	Var.	DF list (see 7.4.8)	DF*
'98'	Var.	Instance number (binary coding)	DO*
'99'	Var.	Number of DOs in the current template after file or DO selection (binary coding, see 7.2.2 rule i)).	File* or DO*
'9A'	Var.	Number of EFs within a DF (binary coding)	DF*
'9B'	Var.	EF list (see 7.4.8)	DF*
'9C'	Var.	Security attribute in compact format, SPT oriented (see Table 30). NOTE: It is mainly intended for DO handling.	File* or DO*
'9D'	Var.	Tag of the DO(s) to which DO'62' applies.	DO
'A0'	Var.	Security attribute template for DOs (see 9.3.5)	File* or DO
'A1'	Var.	Security attribute template in proprietary format	File
'A2'	Var.	Template consisting of one or more pairs of DOs: Short EF identifier (DO'88') - File reference (DO'51', L > 2, see 7.3.2)	DF
'A3'	Var.	Interface and LCS dependent security attribute template (see 7.4.12)	File or DO
'A5'	Var.	Proprietary information encoded in BER-TLV	File
'A6'	Var.	as defined in ISO/IEC 7816-11	see ISO/IEC 7816-11
'AB'	Var.	Security attribute template in expanded format (see 9.3.3)	File*
'AC'	Var.	Cryptographic mechanism identifier template (see 9.2)	DF
'AD'	Var.	Security parameters template (see 9.3.6.1)	DO
'AF'	Var.	Template encapsulating one or more DO'06' (OID) relevant to the application.	DF*

* indicates that the DO shall appear at most once under DO'62'.
In the response to a SELECT and under tags '62' and '6F', ISO/IEC JTC 1/SC 17 reserves any other DO of the context-specific class.

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

7.4.4 Short EF identifier

The following rules apply for the use of DO'88' in the CPs of any EF.

— If the card supports selection by short EF identifiers (see 7.3.1) and if DO'88' is absent, then in the second byte of the file identifier (tag '83'), bits b5 to b1 encode the short EF identifier.

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

— If DO'88' is present with a length set to one and if bits b8 to b4 of the data element are not all equal and if bits b3 to b1 are set to 000, then bits b8 to b4 encode the short EF identifier (a number from one to thirty).

7.4.5 File descriptor byte

DO'82' may be present in the CPs of any file (see Table 10).

— The first byte of the value is the file descriptor byte (see Table 11).

— If the value consists of two or more bytes, then the second byte is the data coding byte (see

— Table 118). 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 to that file from:

1) The MF, if present.
2) The DF referred to by curAppDF, if the MF is absent.
3) In the absence of indication in the path, the data unit size is set to the default value (see
4) Table 118).

Table 11 — Coding of the 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	-	1	1	1	0	0	0	**DF**
0	-	Not all set to 1			-	-	-	**EF category**
0	-	0	0	0	-	-	-	— EF for storing data not interpreted by the card (Working EF)
0	-	0	0	1	-	-	-	— EF for storing data interpreted by the card (Internal EF)
0	-	Any other value			-	-	-	— Proprietary categories of EFs
0	-							**EF structure**
0	-	Not all set to 1			0	0	0	— No information given
0	-	Not all set to 1			0	0	1	— Transparent structure
0	-	Not all set to 1			0	1	0	— Linear structure, fixed size, no further information
0	-	Not all set to 1			0	1	1	— Linear structure, fixed size, TLV structure
0	-	Not all set to 1			1	0	0	— Linear structure, variable size, no further information
0	-	Not all set to 1			1	0	1	— Linear structure, variable size, TLV structure
0	-	Not all set to 1			1	1	0	— Cyclic structure, fixed size, no further information
0	-	Not all set to 1			1	1	1	— Cyclic structure, fixed size, TLV structure
0	-	1	1	1	0	0	1	— BER-TLV structure
0	-	1	1	1	0	1	0	— SIMPLE-TLV structure

— Any other value is RFU.
— "Shareable" means that the file ⟨AC1⟩ supports concurrent ⟨AC1⟩ access on different logical channels.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

7.4.6 Profile indicator

The following rules apply for the use of DO'8F' in the file CPs of any EF supporting records:

— If DO'8F' is present, then the value field contains a profile indicator according to Table 12;

— If DO'8F' is absent, then all records in the EF are implicitly in the unchangeable state ACTIVATED.

Table 12 — Coding of the profile indicator

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**Coding of profile indicator defined by ISO/IEC JTC 1/SC 17**
0	–	–	–	–	–	–	x	Record LCS
0	–	–	–	–	–	–	0	All records in this file are in the unchangeable state ACTIVATED
0	–	–	–	–	–	–	1	Each record in this EF has its own record LCS, changeable by the commands ACTIVATE RECORD, DEACTIVATE RECORD and ACTIVATE FILE
1	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**Proprietary coding of profile indicator**
— Any other value is RFU.								

7.4.7 Data descriptor byte

Referenced by tag '92', this interindustry data element is a CP DO, which contains information relevant to DO handling (see Table 13). The information is valid for all instances (if more than 1) of a DO in the relevant template. If a DO is declared "non shareable", only one instance of this DO is accessible on one logical channel.

Table 13 — Coding of the data descriptor byte

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	**x**	-	-	-	-	-	-	**Data accessibility**
0	0	-	-	-	-	-	-	— Not shareable DO
0	1	-	-	-	-	-	-	— Shareable DO
0	-	**x**	**x**	-	-	-	-	**structuring of the DOs in the template**
0	-	0	0	-	-	-	-	— No information given (default).
0	-	0	1	-	-	-	-	— Linear management (see 11.4.7)
0	-	1	0	-	-	-	-	— Cyclic management of instances (see 11.4.7)
0	-	1	1	-	-	-	-	— RFU
0	-	-		**x**	-	-	-	**Instances**
0	-	-	-	0	-	-	-	— A tag shall occur at most once in the template.
0	-	-	-	1	-	-	-	— Tags may occur more than once in the template (default).
0	-	-	-	-	**x**	**x**	**x**	**DO properties**
0	-	-	-	-	0	0	0	— No information given
0	-	-	-	-	-	-	1	— Tag list present (Constructed DO) or present in the tag list (Primitive DO)
0	-	-	-	-	-	1	-	— Base template extendable by wrappers (Constructed DO) or part of the template extension (Primitive DO)
0	-	-	-	-	1	1	-	— Automatic resolution of wrappers
— Any other value is RFU. — "Shareable" means that the DO ⌈AC1⌉ supports concurrent access ⌈AC1⌉ on different logical channels.								

7.4.8 DF and EF list data elements

Referenced by tag '97', the DF list interindustry data element is a file CP which shows the DFs contained in a DF or application DF. It is a concatenation of 2-byte file identifiers.

Referenced by tag '9B', the EF list interindustry data element is a file CP, which contains the identifiers of the elementary files contained in the DF or application DF, and their short EF identifier. The information of each file is coded on three consecutive bytes. The first two bytes contain the file identifier of an EF. The third byte is either the short EF identifier of the EF coded according to 7.4.4 or a byte coded '00' if that elementary file has no short EF identifier.

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

7.4.9 Instance number data element

Referenced by tag '98', this interindustry data element is a CP DO, which may be present only if there are several instances of the DO within its template. Its value shall be a binary coded positive sequence number, as defined by ISO/IEC 8825-1 for the INTEGER type. The numbering scheme for cyclic management of instances is the same as for the management of record numbers (see 11.3.6). See 11.4.7 for further information of numbering schemes.

7.4.10 Life cycle status

The card, files and other objects, each have a life cycle; the life cycle status (LCS) 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 of a file, record or DO as an attribute (see ISO/IEC 7816-9), this clause defines four primary states of the life cycle in the following order.

1) Creation state
2) Initialisation state
3) Operational state: activated or deactivated.
4) Termination state

LCS (1 byte) shall be interpreted according to Table 14.

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

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

The default state shall be Operational state (activated).

Table 14 — Coding of the file or data LCS 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 RFU.								

Under tag '8A', an LCS may be present in the CPs of any file or DO (see Table 10). A card LCS may be present in the historical bytes (see 12.1.1.11). Under tag '48', a card LCS may be present in EF.ATR/INFO (see 12.2.2). When it has an MF, the card is in, at least, the creation state.

NOTE Unless otherwise specified, the security attributes are valid for the operational state of files and ACTIVATED state of DOs.

7.4.11 Indirect referencing by short EF identifier using DO'A2'

A DO'88' under DO'A2' in the FCP of a DF indicates that the nested short EF identifier is valid when the DF is current. A command using it shall transiently select the EF referenced by the path which is nested in DO'51' after that DO'88'. Its success has no impact on curDF and curAppDF (see 7.2.2 rule f)). The impact on curEF is described in sections dealing with commands using short EF identifier (see e.g. 11.2.2 or 11.3.2).

© ISO/IEC 2013 – All rights reserved
Documents Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

7.4.12 Interface and life cycle status dependent security attribute template

DO'A3' may be present in the CPs of any file or DO and in such templates it may occur more than once (see Table 10).

DO'A3' shall contain at most one DO'91' (see 7.4.12.1). If DO'91' is absent then the security attributes contained in DO'A3' apply to all interfaces. If DO'A3' contains a DO'91' it shall be the first DO in the template.

DO'A3' shall contain at most one DO'8A' (see 7.4.12.2). If DO'8A' is absent then the security attributes contained in DO'A3' apply to all life cycle status. If DO'A3' contains a DO'8A' then it shall be

— the first DO in the template if DO'91' is absent, or

— the second DO in the template if DO'91' is present.

DO'A3' may contain any number of DO'8B', DO'8C', DO'9C', DO'A0', DO'AB' in any order having the same meaning and coding as defined by Table 10.

7.4.12.1 Transport type descriptor

Referenced by tag '91' under DO'A3', this data element indicates for which interfaces the security attributes contained in the same DO'A3' apply.

Table 15 — Coding of transport type descriptor (DO'91' under DO'A3')

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	-	-	-	-	-	-	-	0, other values are RFU [a]
-	x	x	-	-	-	-	-	00, other values are RFU
-	-	-	1	-	-	-	-	Communication by contact C6 (see ISO/IEC 7816-3)
-	-	-	-	1	-	-	-	Near-field communication (see ISO/IEC 18092 [22])
-	-	-	-	-	1	-	-	USB interface (see ISO/IEC 7816-12)
-	-	-	-	-	-	1	-	Contactless interface for proximity cards (see ISO/IEC 14443 [18])
-	-	-	-	-	-	-	1	Contact interface (see ISO/IEC 7816-3)

[a] This edition defines the case where one byte is sufficient to reference relevant interfaces. In the future, more than one byte may be necessary.

If in this data element a bit is set to

— 1 then for the corresponding interface the security attributes shall apply.

— 0 then for the corresponding interface the DO'A3' is irrelevant.

7.4.12.2 Indication of life cycle status

Referenced by tag '8A' under DO'A3', this data element indicates for which life cycle status the security attributes contained in the same DO'A3' apply. This data element shall contain one or more bytes and each byte shall be coded and interpreted according to 7.4.10 and Table 14, i.e. each byte encodes a life cycle status and all bytes of the data element build a set of life cycle status. If the life cycle of the file or DO, being given within a DO'8A' in the control parameter template (i.e. the template with tag '62')

— is element of this set then the security attributes shall apply for the file or DO.

— is not element of this set then the DO'A3' is irrelevant for the file or DO.

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

8 Specific use of DOs and related concepts

8.1 BER-TLV payloads and padding

A BER-TLV-encoded data field or payload is a concatenation of BER-TLV DOs, with possible padding before or after any of those DOs.

There are two standard ways of stating BER-TLV-encoding of a command or response data field or payload:

— CLA indicates secure messaging (see clause 10).

— Bit b1 of INS is set to 1 (odd INS code).

Commands with an even INS code may specify BER-TLV-encoding of data fields and payloads.

Within a command payload, this document may define the order of DOs (see e.g. Table 87). In a response payload, the order of DOs is either not defined, or is inherited from the order of the DOs present in the card.

Because of the coding of BER-TLV length fields (see E.2) a DO with a tag of n bytes cannot have a total length of e.g. (n+1+128) bytes or of (n+2+256) bytes or of (n+3+65536) bytes etc. The situation of invalid total length may also occur if several DOs are to be transmitted and the last DO creates the same problem. In all these cases if receiving a command with N_e set to such an invalid total length the card may send within a response data field containing DO(s) the first N_e bytes requested by the command and conclude with a SW1-SW2 set to '61XY', where 'XY' codes the number of remaining bytes. Afterwards response chaining (see 5.3.4) applies.

8.1.1 Padding conditions

The possibility of padding in a data field depends on the command. The terminology "concatenation of DOs" precludes padding. Padding is allowed:

— when handling data structures through data units; e.g. padding may be present in a READ BINARY response data field due to erasure or modification of DOs within an EF supporting data units.

— when handling data structures through records; e.g. padding may be present in a READ RECORD response data field due to the fixed format of records within an EF supporting records.

— when explicitly allowed by a standard C-RP (CLA<'80').

— when explicitly allowed by a specification of a C-RP (CLA>'7F').

If BER-TLV-encoding is explicitly stated, the data payload(s) shall be BER-TLV encoded, without padding. BER-TLV-encoding shall not apply to the individual data fields (a.k.a. payload fragments) of the commands into which the payload is fragmented, because payload fragmentation is entitled to split DOs. Padding is still precluded in payload fragments.

NOTE Secure messaging may require BER-TLV-encoding of payload fragments (see 10.1).

8.1.2 Padding procedure

When padding is allowed in BER-TLV payloads, bytes set to '00' may be present before, between or after DOs.

When present in the historical bytes (see 12.1.1) or in EF.ATR/INFO (see 12.2.2) or in the control information of any file (see tag '82' in Table 10), the data coding byte (see Table 118) 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'.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

8.2 Current template and data object generations

8.2.1 Current template and current DO

If set, the curConstructedDO references a constructed DO. Its value field, as defined in 7.2.2 rule k), is called the current template.

Any DO within the current template can be directly referenced by its sole tag in a command for interchange which does not provide any information on the VA together with this tag.

If any of those DOs is also constructed, the current template does not include any nested DOs within this constructed DO.

The virtual root DO'7F70' belongs to the 0 generation, and is the only DO in that generation. If curConstructedDO references an n^{th} generation constructed DO'XY', the current template is a sequence of $(n+1)^{th}$ generation DOs nested in DO'XY'. The current template does not include DOs possibly nested in any $(n+1)^{th}$ generation DO. Annex F shows examples.

The curDO (see 7.2.1 dash 9) is set by a SELECT command (see 11.1.1) or a SELECT DATA command (see 11.4.2). DO selection also occurs as a side effect of other DO-handling commands, and is described in the relevant clauses, e.g. 11.4.3 and 11.4.4 for the GET DATA command.

In order to support referencing methods defined in this edition of ISO/IEC 7816-4, the card should be able to resolve tag '7F70'.

Immediately after enabling of an interface (see 5.1), thus before any selection, the current template depends on the implicitly selected application or DF (curAppDF in the VA). It may contain specific DOs to support e.g. discovery mechanisms defined in ISO/IEC 24727-2 [24].

Many commands which handle DOs imply one or several internal selections. Those selections are said to be "transient", and set a "transient current file" or a "transient current template", thus a "transient VA". In some cases, a side effect of the command success may validate those internal selections, thus set the transient VA as current VA.

8.2.2 Template extension

The template extension is that part of a template which is accessible only by automatic resolutions of tagged wrappers, whereby extending the base template (see Annex G or examples). All wrapper DO'63' are part of the base template.

If automatic resolution of tagged wrappers is not supported, the template extension is empty. The indirect references are only informative. If needed, the outside world may perform a two-stage procedure:

— selection of the structure where the DO is stored, when this structure is different from the current structure;

— then handling of the DO within the selected structure.

8.2.3 Data object sub-tree

A constructed DO has a tree structure. A sub-tree of this tree structure is obtained by removing nested DOs from the tree. An extended header associated with a constructed DO refers a sub-tree of the DO (see 8.4.6 and 8.4.7).

EXAMPLE A given n^{th} generation DO is denoted {T-L- {T1-L1-{T2-L2-V2}-{T3-L3-V3}}-{T4-L4-V4}-{T5-L5-V5}}. Removing the $(n+2)^{th}$ generation DO T2 and the $(n+1)^{th}$ generation DO T4 yields the sub-tree: {T-L'- {T1-L1'-{T3-L3-V3}}-{T5-L5-V5}}. L and L1 are replaced by L' and L1' because removing a DO from a template impacts its length.

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

8.2.4 Data object life cycle

Any DO stored in the card may have a DO life cycle. When it does, the LCS shall distinguish at least two states: ACTIVATED and DEACTIVATED. The coding of a DO's LCS and the coding of a file's LCS are analogous (see Table 14). The presence of DO's LCS is indicated in the CP template DO'62' (see Table 10).

8.3 Identification of data elements and data objects

8.3.1 Principles

At the interface between the card and the interface device, a data element is generally presented in the value field of a DO. The data element is said to be "under" the tag of the DO.

If the number of bits representing a data element is not a multiple of eight, one may use the BITSTRING universal DO, as e.g. in ISO/IEC 7816-15. If not, the mapping into a byte or a string of bytes should be specified together with the respective data element. Unless otherwise specified, the appropriate number of bits shall be set to 1 in the last byte starting from bit b1.

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.

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.

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

The interindustry commands support multiple instances of the same DO within a template, thus within an application and within a card.

A standard or an application may limit or prohibit multiple instances of the same DO within a template, within a structure or within the application.

8.3.2 Tag interpretation in command and response data fields or payloads

DOs of the universal class (first byte from '01' to '3F', see Annex E) always have their general meaning.

The meaning of DOs of the application class (first byte from '40' to '7F', see Annex E) is defined by standards. The default is the ISO/IEC 7816 [6] and the ISO/IEC JTC 1/SC 17 standards (see 8.3.3). The meanings of those DOs are always the same, though their function is defined by the command where they are used.

The way to interpret DOs of the context-specific class (first byte from '80' to 'BF', see Annex E) is defined:

— generally by its nesting within a constructed DO defined by the standard, e.g. DOs nested in DO'62' (see Table 10). This rule is recursive, and applies e.g. to DOs nested in a DO'A0' nested in a DO'62'.

— by CLA: secure messaging indication (see 5.4 and 10.1)

— by INS: commands may define such DOs of the context-specific class for a specific use.

— In other cases, the interpretation of those DOs is defined by the application.

8.3.3 Tag allocation

This document specifies many interindustry DOs, and allocates tags for the BER-TLV-encoding of those DOs. In addition to defining further interindustry DOs, ISO/IEC 7816-6 maintains an exhaustive list of the tuples (name of the interindustry DO, allocated tag) specified in ISO/IEC 7816 [6] at the time of publication. The tags allocated in ISO/IEC JTC 1/SC 17 standards belong:

— either to the application class;

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

— or to the context-specific class, when the corresponding DOs may be nested in a constructed DO the tag of which has been allocated by the standard.

When a tag is defined by another standard, the national body responsible for the standard shall seek advice of ISO/IEC JTC 1/SC 17/WG 4 for the tag or tags needed, and shall in due time comment in order to add this or those tags in ISO/IEC 7816-6.

Illustrated by Annex A, the subsequent clauses specify tag allocation schemes for identifying interindustry DOs in data fields. When needed, those tag allocation schemes use the interindustry DOs shown in Table 16 for notifying an authority responsible for tag allocation.

Table 16 — Interindustry data objects for tag allocation authority

Tag	Value
'06'	Object identifier (OID), encoding specified in ISO/IEC 8825-1), see examples in Annex A.
'41'	Country code (encoding specified in ISO 3166-1 [3]) and optional national data
'42'	Issuer identification number (encoding and registration specified in ISO/IEC 7812-1 [5]) and optional issuer data
'4F'	Application identifier (AID, encoding specified in 12.2.3)
'5F29'	Interchange profile.

8.3.4 Standard tag allocation scheme

In the application class, ISO/IEC JTC1/SC17 allocates or reserves the use of any application class tag numbers in the range 0-127 or greater than 511 (decimal).

Application class tag numbers in the range 128 to 511 (decimal) may be allocated by any standard or specification referenced by an OID, or by an application referenced by an AID.

In order to identify the tag allocation authority in this range, a constructed DO'78' shall be used. This DO shall nest an empty DO'80' followed by either a DO'06' or a DO'4F'. If DO'78' is present

— in the initial data string (see 12.1.2) or in EF.ATR/INFO (see 12.2.2), then the authority shall be valid for the entire card, except if overruled by another DO'78' in a file or a constructed DO.

— in the management data of an EF or DF, possibly supporting an application (see 7.4), or in the template made current by the selection of any file, then the authority shall be valid within that file or application, except if it is overruled by another DO'78' in a constructed DO.

— in a template, it shall be valid for all DOs in the template, and all objects contained in the constructed DOs, (thus irrespective of their generation), except if it is overruled by another DO'78' in a template.

8.3.5 Compatible tag allocation scheme

These tag allocation schemes use interindustry DOs and further DOs.

These further DOs shall be nested within interindustry DOs referenced by tags '70' to '72', or tags '74' to '77'. In those DOs, the meaning of the application class tags is not defined in ISO/IEC 7816 [6] except for tags '41', '42' and '4F' for identifying tag allocation authorities (see Table 16).

When further DOs use tags of the context-specific class, and belong to the interindustry templates defined above, their meaning is defined by the tag allocation authority.

The use of the context-specific class 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, the interindustry DO'78' may be used. Possible occurrence and overruling are the same as in 8.3.4. If present, its value shall contain one of the interindustry DOs shown in Table 16, for identifying a tag allocation authority.

Documents
Document Sharing Hub

© ISO/IEC 2013 – All rights reserved

Full document details: BS ISO/IEC 7816-4:2013+A2:2018

8.3.6 Coexistent tag allocation scheme

In such a scheme, all the interindustry DOs shall be nested within interindustry DOs'7E'. Moreover, tags '79' and '7E' shall not be given another interpretation, as well as tags '62', '64', '6F' (CP, FMD and FCI templates, see 7.4) and '7D' (SM template, see 10.1).

These tag allocation schemes may use tags with an interpretation not defined in ISO/IEC 7816 [6]. In order to identify a coexistent tag allocation scheme and the authority responsible for the scheme, an interindustry DO'79' shall be used. This DO shall nest one of the interindustry DOs shown in Table 16.

— If an authority is valid for the entire card, then DO'79' shall be present in the initial data string (see 12.1.2) or in EF.ATR/INFO (see 12.2.2).

— If an authority is valid within a file or application, then DO'79' shall be present in the EF, DF or application DF management data (see 7.4), or in the current template set by any file selection.

8.3.7 Avoidance of independent tag allocation schemes

An independent tag allocation scheme uses tags with another interpretation than ISO/IEC 7816 [6], but which does not comply with 8.3.6. Such tag allocation schemes do not comply with this document and do not allow interchange.

Besides a consistent use of compatible and coexistent allocation schemes, there are three ways for an application to avoid such a situation, and remain compliant with this document:

— The use of interindustry discretionary DOs'53' to present discretionary DOs, and DOs'73' to nest proprietary DOs in discretionary templates.

— The use of 3-byte tags reserved for this purpose (see 8.3.4).

— The use of DOs of the context-specific class (see 8.3.2).

8.4 Referencing and retrieval of DOs and data elements

8.4.1 General

A tag 'XY' directly references a data element, which is the value of DO'XY'. For retrieval of DOs before selection of an application see 12.4.

Control parameters and file management data may be retrieved in the answer to a SELECT or SELECT DATA command (see 11.1.1, 11.4.2.1 and Table 87).

Once an application is selected, any DO should be retrieved directly or indirectly:

— In the file management data (see 7.4) of the application DF and from specific EFs within the current DF.

— In the current template (see 8.2) after application selection, using GET DATA or GET NEXT DATA commands (see 11.4.3 and 11.4.4). File management data and/or DO'62' (nesting CPs) should be included in this template, to ensure that those particular DOs are relevant to the application.

Element lists, tag lists, header lists, extended headers and extended header lists, are interindustry DOs which reference indirectly data elements, thus reference DOs within any template. Such a data element instructs the card how to interpret a command data field or to construct a response data field. Computing the concatenation of data elements or the DOs from the indirect reference is called resolving (or resolution of) the indirect reference.

The interpretation of a tag list, a header list, an extended header or an extended header list depends on the template in which they are defined. Nesting one of those DOs within a wrapper (which defines this template), allows referencing wherever in a card. An optional tag within the wrapper allows referencing the result of the resolution of the indirect reference by this tag.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

The command data field syntax in the SELECT DATA, GET DATA, GET NEXT DATA shows the use of those DOs, which may be close to the syntax of a wrapper.

8.4.2 Element list

Under tag '5F41', this interindustry data element denotes that the information to retrieve is not presented as DOs, but under application control. It shall be used only within the wrapper template. Its structure and the returned information are out of scope of ISO/IEC 7816 [6].

8.4.3 Tag list

Referenced by tag '5C', this interindustry data element is a concatenation of tag fields without delimitation. It references a concatenation of DOs with the respective tags, in the same order as in the tag list.

8.4.4 Header list

Under tag '5D', this interindustry data element is a concatenation of tuples (tag field T, length field L) without delimitation. The byte string is as defined as in the tag list except for possible truncation of the values. When L = '00', no truncation occurs. When L > '00', the value shall be right truncated to L bytes, except when it is already shorter or equal to L bytes. The coding of L is a BER length.

WARNING — Within a header list, all referenced DOs to be truncated should be primitive, because a truncated constructed DO is not a DO. For extraction of parts of a constructed DO, one should use an extended header.

8.4.5 Extended header and extended header list

Under tags '4D', '5F60' or '5F61' (see 8.4.8 for the differences between different tags), this interindustry data element is an extended header list.

An extended header list is

— either an extended header

— or a concatenation of extended headers.

An extended header is a concatenation of tuples (tag field T, length field L) without delimitation. An extended header references information within a target DO. ⌈AC1⟩ A complete extended header shall be derived from the target DO by the following procedure: ⟨AC1⌋

a) primitive DO not to be referenced:
If the extended header is to be tagged by
   1) '4D', delete the tag, length and value field.
   2) '5F60' or '5F61', delete the value field and replace the length field by '00'.

b) primitive DO to be referenced without truncation:
Delete the value field. If the extended header is to be tagged by
   1) '4D', replace the length field by '00'.
   2) '5F60' or '5F61', replace the length field by '80'.

c) primitive DO to be referenced with truncation:
Delete the value field and replace the length field by a truncation indication (see 8.4.6)

d) constructed DO not to be referenced at all:
Delete the value field and replace the length field by '00'.

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

e) constructed DO to be referenced entirely:
Delete the value field and replace the length field by '80'.

f) constructed DO where part of the information is to be referenced:
Adjust the value of the length field according to the outcome of applying the procedures above.

As shown in F.2, the explicit referencing of DOs where nothing is referenced is not always necessary, even when several instances of such a DO exist in a given template. Removing useless referencing is entitled by this standard.

8.4.6 Resolving an extended header

To resolve an extended header, one shall build the referenced byte string as follows.

— If a tag indicates a primitive encoding, then the pair of tag field and length field is replaced by data referenced by the tag. If the extended header is tagged by '4D', a length of '00' means that the complete DO/element is included in the byte string. If the extended header is tagged by '5F60' or '5F61', a length of '80' means that the complete DO/element is included in the byte string. A length which is neither '00' in an extended header tagged by '4D', nor '80' in an extended header tagged by '5F60' or '5F61', indicates the maximum number of data bytes to be retrieved and consequently may require truncation as defined in 8.4.4. If the truncation indication indicates more bytes than available in the DO, the behaviour depends on the tagging:

  — Under tag '4D', it is out of the scope of this document.

  — Under tag '5F60' and '5F61' the extended header is invalid. If used in a command APDU, the command shall be rejected by SW1-SW2 = '6985'.

— A tag indicating a constructed encoding followed by a non-zero length, except '80', introduces a subsequent value field that is an extended header list. A tag indicating a constructed encoding followed by a zero length is ignored. A tag indicating a constructed encoding followed by '80' means that the complete constructed DO/complete template is included in the byte string.

— The card shall ignore the elements of the extended header that do not match the target structure.

For security reasons, a card may reject a command with SW1-SW2 = '6985' because of the lack of consistency between the structure used in the command data field and the contents of the card. This may override security attributes.

The byte string consists of either

— the value fields of the primitive DOs, possibly truncated according to the indicated lengths (Case 1), or

— the primitive DOs, possibly truncated according to the indicated lengths, and nested in the respective template, the length of which complies with the BER-TLV rules (Case 2).

— If present, the length '80' shall be replaced by the actual length. The complete constructed DO/complete template is included in the byte string.

The encoding of the referenced byte string, namely, a (possibly constructed) DO(s) or a concatenation of (possibly truncated) data elements, is indicated:

— by an appropriate INS code (odd/even)

— or by an appropriate parameter of the command, e.g., either an appropriate encoding of the data field (either constructed for those containing DOs or primitive for those containing data elements).

— or by tagging the extended header list by another tag than '4D', as shown in 8.4.8 and the PERFORM SECURITY OPERATION command (see ISO/IEC 7816-8).

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

8.4.7 Resolving an extended header list

The byte string referenced by an extended header list is the concatenation of the byte strings referenced by the extended headers, in the same order as in the extended header list. When parsing an extended header list:

— the resolution of one extended header shall be followed by the resolution of the next one if any.

— the order within the byte string is therefore defined by the order of extended headers in the extended header list, which should match the order within the target (template) in order to avoid the following problem: As in the resolution of an extended header, the card shall ignore the elements (extended headers) of the extended header list that do not match the target (template) structure.

8.4.8 Wrapper

Under tag '63', this interindustry DOs shall nest two or more DOs.

a) The first DO is a mandatory indirect reference. Only one indirect reference shall be given in a wrapper. It is a choice between:

   1) an element list (tag '5F41' or '53');
   2) an element list nesting DOs (tag '73');
   3) a tag list (tag '5C')
   4) a header list (tag '5D');
   5) an extended header list (tag '4D');
   6) an extended header list referencing a byte string with no stated structure (tag '5F60');
   7) an extended header list referencing one DO or a concatenation of DOs (tag '5F61');
   8) a byte string identical to the response data of the last command to perform (tag '80', empty DO), see below.

   possibly followed by a filter DO'7F71' (see 11.4.2.3) in the case of tag list or extended header list. The use of DO'5F60' or the use of DO'5F61' entitle skipping indication of primitive DOs according to 8.4.5.

b) The remainder of the wrapper value field shall be:

   1) either an application identifier DO'4F' (see 12.2.3). The indirect reference shall be valid within the current template after application selection.
   2) or a file reference DO'51' (see 7.3.2 and Table 7). The indirect reference shall be valid within the selected file; if it is empty, it shall be valid in the current template.
   3) or a DO'4F' followed by a non-empty DO'51' referencing a file which shall exist in the application. The indirect reference shall be valid within this file.
   4) or one DO'52' (command to perform). The indirect reference shall be valid within the response payload of this command.
   5) or several DO'52'. The commands to perform shall be processed in the presented order. The indirect reference shall be valid within the response payload of the last command or in the transient VA set by this command.

The resolution of a wrapper:

— starts with the resolution of the second part of the wrapper, which is either a standard structure, or a response APDU. It ends there if the indirect reference is a DO'80'.

— if the indirect reference is not a DO'80', it ends with the resolution of the indirect reference, which is defined in 8.4.3, 8.4.4, 8.4.5.

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018

EXAMPLE The following wrapper DO nests a tag list and one command-to-perform.
{'63'-L-{'5C'-L-(Tag1-Tag2-Tag3)}-{'52'-L-Command APDU}}

8.4.9 Tagged wrapper

Under tag '63', this DO extends a template in a card which supports automatic resolution of wrappers.

The first DO in the value filed of a tagged wrapper DO'63' shall be an empty DO'XY'. The tag 'XY' shall be valid in GET DATA or GET NEXT DATA C-RPs when the extended template is the current template; 'XY' shall respect the current tag allocation scheme. The remainder of the value shall be the value of a wrapper DO (see 8.4.8). The outcome of resolving the indirect reference shall be the value of DO'XY' when addressed within the template it extends (see 8.2.2):

— If the wrapper references a DO'ZT', the value of DO'XY' shall be the value of this DO'ZT' (see Annex G for examples). The wrapper shall reference only one DO, possibly constructed.

— If the wrapper references a byte string, the value of DO'XY' shall be that byte string.

NOTE 1 Neither the notation 'XY' nor 'ZT' precludes the use of tags consisting of more than one byte.

NOTE 2 The automatic resolution of the tagged wrapper creates within the current template a virtual DO. The tag of this virtual DO is taken from the first DO in the tagged wrapper. The length field of this DO codes the length of the content of the resolved indirection. The value of the DO is the content itself (see examples in Annex G).

9 Security architecture

9.1 General

This clause describes security status, security attributes and security mechanisms.

Security status — The security status represents the current state possibly achieved on a logical channel after physical interface enabling (see 5.1) or resetting a logical channel and/or ⟦AC1⟩ execution of one or several C-RP(s) on this logical channel possibly performing authentication procedures ⟨AC1⟧. The security status may also result from completion of a security procedure related to the identification of the involved entities, if any, e.g. by proving knowledge of a password (e.g. using a VERIFY command) or knowledge of a key (e.g. using a GET CHALLENGE command followed by an EXTERNAL AUTHENTICATE command, or using a sequence of GENERAL AUTHENTICATE commands), or by secure messaging (e.g. message authentication). Five security statuses are considered.

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

— **Application-specific security status —** It may be modified by completion of an application-related authentication procedure (e.g. entity authentication by a password or a key attached to the application); it may be maintained, recovered or lost by application selection; this modification may be relevant only for the application to which the authentication procedure belongs. If logical channels apply, then the application-specific security status may depend on the logical channel.

— **File-specific security status —** It may be modified by 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; this modification may be relevant only for files within the application to which the authentication procedure belongs. If logical channels apply, then the file-specific security status may depend on the logical channel.

— **DO-specific security status —** It may be modified by completion of a DO-related authentication procedure; it may be maintained, recovered or lost by selections; this modification may be relevant only for DO within the application to which the authentication procedure belongs. If logical channels apply, then the DO-specific security status may depend on the logical channel.

— **Command-specific security status —** It only exists while processing a command using secure messaging and involving authentication; such a command may leave the other security status unchanged.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 7816-4:2013+A2:2018