This is a preview of "ISO/IEC 7816-4:2020". Click here to purchase the full version from the ANSI store.

INTERNATIONAL ISO/IEC

Fourth edition
2020-05

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 7816-4:2020(E)

© ISO/IEC 2020

This is a preview of "ISO/IEC 7816-4:2020". Click here to purchase the full version from the ANSI store.

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2020 – All rights reserved

This is a preview of "ISO/IEC 7816-4:2020". Click here to purchase the full version from the ANSI store.

Contents

Page

Foreword ... **vii**

Introduction ... **viii**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

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 ... 17

6 Data objects ... **19**
6.1 General ... 19
6.2 SIMPLE-TLV data objects ... 19
6.3 BER-TLV data objects ... 20
6.4 Constructed DOs versus primitive DOs ... 20

7 Structures for applications and data ... **20**
7.1 Available structures ... 20
7.2 Validity area ... 22
7.2.1 Definitions and attributes ... 22
7.2.2 Basic rules for VA handling and use ... 22
7.3 Structure selection ... 23
7.3.1 Structure selection methods ... 23
7.3.2 File reference data element and DO ... 24
7.3.3 General reference data element and DO ... 25
7.3.4 Data referencing methods in elementary files ... 25
7.4 File and data control information ... 26
7.4.1 File control information retrieval ... 26
7.4.2 Data control information retrieval ... 26
7.4.3 Control parameters ... 27
7.4.4 Short EF identifier ... 28
7.4.5 File descriptor byte ... 28
7.4.6 Profile indicator ... 29
7.4.7 Data descriptor byte ... 30
7.4.8 DF and EF list data elements ... 30
7.4.9 Instance number data element ... 30
7.4.10 Life cycle status ... 30
7.4.11 Indirect referencing by short EF identifier using DO'A2' ... 31
7.4.12 Interface and life cycle status dependent security attribute template ... 31

8 Specific use of DOs and related concepts ... **33**
8.1 BER-TLV payloads and padding ... 33
8.1.1 General ... 33
8.1.2 Padding conditions ... 33

© ISO/IEC 2020 – All rights reserved

This is a preview of "ISO/IEC 7816-4:2020". Click here to purchase the full version from the ANSI store.

8.1.3 Padding procedure 33
8.2 Template referenced by curConstructedDO and data object generations 34
8.2.1 Template referenced by curConstructedDO and DO referenced by curDO 34
8.2.2 Template extension 34
8.2.3 Data object pruned-tree 35
8.2.4 Data object life cycle 35
8.3 Identification of data elements and data objects 35
8.3.1 Principles 35
8.3.2 Tag interpretation in command and response data fields or payloads 35
8.3.3 Tag allocation 36
8.3.4 Standard tag allocation scheme 36
8.3.5 Compatible tag allocation scheme 36
8.3.6 Coexistent tag allocation scheme 37
8.3.7 Avoidance of independent tag allocation schemes 37
8.4 Referencing and retrieval of DOs and data elements 37
8.4.1 General 37
8.4.2 Element list 38
8.4.3 Tag list 38
8.4.4 Header list 38
8.4.5 Extended header and extended header list 38
8.4.6 Resolving an extended header 39
8.4.7 Resolving an extended header list 40
8.4.8 Wrapper 40
8.4.9 Tagged wrapper 41

9 Security architecture 41
9.1 General 41
9.2 Cryptographic mechanism identifier template 43
9.3 Security attributes 43
9.3.1 General 43
9.3.2 Security attributes targets 43
9.3.3 Compact format 44
9.3.4 Expanded format 48
9.3.5 Access rule references 52
9.3.6 Security attributes for data objects 53
9.3.7 Security parameters template 54
9.3.8 Security attributes for logical channels 59
9.4 Security support data elements 60

10 Secure messaging 61
10.1 General 61
10.2 SM fields and SM DOs 61
10.2.1 SM protection of command payloads 61
10.2.2 SM protection of chained commands and responses 61
10.2.3 SM DOs 62
10.3 Basic SM DOs 63
10.3.1 SM DOs for encapsulating plain values 63
10.3.2 SM DOs for confidentiality 63
10.3.3 SM DOs for authentication 64
10.4 Auxiliary SM DOs 66
10.4.1 General 66
10.4.2 Control reference templates 67
10.4.3 Control reference DOs in control reference templates 67
10.4.4 Security environments 69
10.4.5 Response descriptor template 71
10.5 SM impact on command-response pairs 71

11 Commands for interchange 73
11.1 General 73
11.2 Selection 73

 © ISO/IEC 2020 – All rights reserved

This is a preview of "ISO/IEC 7816-4:2020". Click here to purchase the full version from the ANSI store.

11.2.1 General ... 73
11.2.2 SELECT command ... 73
11.2.3 MANAGE CHANNEL command ... 76
11.3 Data unit handling ... 77
11.3.1 Data units ... 77
11.3.2 General ... 77
11.3.3 READ BINARY command ... 78
11.3.4 WRITE BINARY command ... 78
11.3.5 UPDATE BINARY command ... 79
11.3.6 SEARCH BINARY command ... 79
11.3.7 ERASE BINARY command ... 80
11.3.8 COMPARE BINARY function ... 80
11.4 Record handling ... 80
11.4.1 Records ... 80
11.4.2 General ... 81
11.4.3 READ RECORD (S) command ... 82
11.4.4 WRITE RECORD command ... 84
11.4.5 UPDATE RECORD command ... 85
11.4.6 APPEND RECORD command ... 87
11.4.7 SEARCH RECORD command ... 88
11.4.8 ERASE RECORD (S) command ... 92
11.4.9 ACTIVATE RECORD (S) command ... 93
11.4.10 DEACTIVATE RECORD (S) command ... 94
11.4.11 COMPARE RECORD function ... 95
11.5 Data object handling ... 95
11.5.1 General ... 95
11.5.2 SELECT DATA command ... 96
11.5.3 GET DATA/GET NEXT DATA commands — even INS codes ... 100
11.5.4 GET DATA/GET NEXT DATA commands — odd INS codes ... 102
11.5.5 General properties of PUT DATA/PUT NEXT DATA/UPDATE DATA commands ... 103
11.5.6 PUT DATA command ... 104
11.5.7 PUT NEXT DATA command ... 104
11.5.8 UPDATE DATA command ... 105
11.5.9 COMPARE DATA function ... 106
11.6 Basic security handling ... 106
11.6.1 General ... 106
11.6.2 INTERNAL AUTHENTICATE command ... 107
11.6.3 GET CHALLENGE command ... 108
11.6.4 EXTERNAL AUTHENTICATE command ... 108
11.6.5 GENERAL AUTHENTICATE command ... 109
11.6.6 VERIFY command ... 111
11.6.7 CHANGE REFERENCE DATA command ... 112
11.6.8 ENABLE VERIFICATION REQUIREMENT command ... 112
11.6.9 DISABLE VERIFICATION REQUIREMENT command ... 112
11.6.10 RESET RETRY COUNTER command ... 113
11.6.11 MANAGE SECURITY ENVIRONMENT command ... 114
11.7 Miscellaneous ... 115
11.7.1 COMPARE command ... 115
11.7.2 GET ATTRIBUTE command ... 117
11.8 Transmission handling ... 118
11.8.1 GET RESPONSE command ... 118
11.8.2 ENVELOPE command ... 118

12 Application-independent card services ... 119
12.1 General ... 119
12.2 Card identification ... 119
12.2.1 General ... 119
12.2.2 Historical bytes ... 120
12.2.3 Initial data string recovery ... 124

© ISO/IEC 2020 – All rights reserved

This is a preview of "ISO/IEC 7816-4:2020". Click here to purchase the full version from the ANSI store.

12.2.4 Waiting time management ... 124
12.3 Application identification and selection ... 126
12.3.1 General ... 126
12.3.2 EF.DIR ... 126
12.3.3 EF.ATR/INFO ... 127
12.3.4 Application identifier ... 127
12.3.5 Application template and related data elements ... 129
12.3.6 Application selection ... 129
12.4 Selection by path ... 130
12.5 Data retrieval ... 131
12.6 Card-originated byte string ... 131
12.6.1 General ... 131
12.6.2 Triggering by the card ... 131
12.6.3 Queries and replies ... 132
12.6.4 Formats ... 132
12.7 General feature management ... 132
12.7.1 General ... 132
12.7.2 On-card services ... 132
12.7.3 Interface services ... 133
12.7.4 Profile services ... 133
12.7.5 Provision of additional information ... 133
12.8 APDU management ... 134
12.8.1 Extended length information ... 134
12.8.2 List of supported INS codes ... 134

Annex A (informative) **Examples of object identifiers and tag allocation schemes** ... **135**

Annex B (informative) **Examples of secure messaging** ... **138**

Annex C (informative) **Examples of AUTHENTICATE functions by GENERAL AUTHENTICATE commands** ... **146**

Annex D (informative) **Application identifiers using issuer identification numbers** ... **155**

Annex E (informative) **BER encoding rules** ... **156**

Annex F (informative) **BER-TLV data object handling** ... **158**

Annex G (informative) **Template extension by tagged wrapper** ... **166**

Annex H (informative) **Parsing an extended header against its target DO** ... **170**

Annex I (informative) **Use case of WTX (waiting time extension) procedure and application waiting time procedure** ... **172**

Bibliography ... **176**

© ISO/IEC 2020 – All rights reserved

This is a preview of "ISO/IEC 7816-4:2020". Click here to purchase the full version from the ANSI store.

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and security devices for personal identification*.

This fourth edition cancels and replaces the third edition (ISO/IEC 7816-4:2013), which has been technically revised. It also incorporates the Amendments ISO/IEC 7816-4:2013/Amd.1:2018 and ISO/IEC 7816-4:2013/Amd.2:2018 and the Corrigendum ISO/IEC 7816-4:2013/Cor.1:2014.

The main changes compared to the previous edition are as follows:

— incorporation with the amendments and the corrigendum;

— revision of unclear portions and correction of editorial mistakes.

A list of all parts in the ISO/IEC 7816 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2020 – All rights reserved

This is a preview of "ISO/IEC 7816-4:2020". Click here to purchase the full version from the ANSI store.

Introduction

ISO/IEC 7816 (all parts)[4] 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 (all parts)[11] specifies access by close coupling. ISO/IEC 14443 (all parts)[14] and ISO/IEC 15693 (all parts)[16] specify access by radio frequency. Such cards are also known as contactless cards.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that he/she is willing to negotiate licences — reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from the patent database available at www.iso.org/patents.

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

 © ISO/IEC 2020 – All rights reserved