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)

© ISO/IEC 2013
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td></td>
<td>vii</td>
</tr>
<tr>
<td>Introduction</td>
<td></td>
<td>viii</td>
</tr>
<tr>
<td>1</td>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Normative references</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>Terms and definitions</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>Symbols and abbreviated terms</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>Command-Response pairs</td>
<td>8</td>
</tr>
<tr>
<td>5.1</td>
<td>Conditions of operation</td>
<td>8</td>
</tr>
<tr>
<td>5.2</td>
<td>Syntax</td>
<td>9</td>
</tr>
<tr>
<td>5.3</td>
<td>Chaining procedures</td>
<td>10</td>
</tr>
<tr>
<td>5.3.1</td>
<td>General</td>
<td>10</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Payload fragmentation</td>
<td>10</td>
</tr>
<tr>
<td>5.3.3</td>
<td>Command chaining</td>
<td>10</td>
</tr>
<tr>
<td>5.3.4</td>
<td>Response chaining</td>
<td>11</td>
</tr>
<tr>
<td>5.4</td>
<td>Class byte</td>
<td>12</td>
</tr>
<tr>
<td>5.4.1</td>
<td>Coding</td>
<td>12</td>
</tr>
<tr>
<td>5.4.2</td>
<td>Logical channels</td>
<td>13</td>
</tr>
<tr>
<td>5.5</td>
<td>Instruction byte</td>
<td>14</td>
</tr>
<tr>
<td>5.6</td>
<td>Status bytes</td>
<td>14</td>
</tr>
<tr>
<td>6</td>
<td>Data objects</td>
<td>17</td>
</tr>
<tr>
<td>6.1</td>
<td>SIMPLE-TLV data objects</td>
<td>18</td>
</tr>
<tr>
<td>6.2</td>
<td>BER-TLV data objects</td>
<td>18</td>
</tr>
<tr>
<td>6.3</td>
<td>Constructed DOs versus primitive DOs</td>
<td>18</td>
</tr>
<tr>
<td>7</td>
<td>Structures for applications and data</td>
<td>19</td>
</tr>
<tr>
<td>7.1</td>
<td>Available structures</td>
<td>19</td>
</tr>
<tr>
<td>7.2</td>
<td>Validity area</td>
<td>20</td>
</tr>
<tr>
<td>7.2.1</td>
<td>Definitions and attributes</td>
<td>20</td>
</tr>
<tr>
<td>7.2.2</td>
<td>Basic rules for VA handling and use</td>
<td>20</td>
</tr>
<tr>
<td>7.3</td>
<td>Structure selection</td>
<td>21</td>
</tr>
<tr>
<td>7.3.1</td>
<td>Structure selection methods</td>
<td>21</td>
</tr>
<tr>
<td>7.3.2</td>
<td>File reference data element and DO</td>
<td>22</td>
</tr>
<tr>
<td>7.3.3</td>
<td>General reference data element and DO</td>
<td>23</td>
</tr>
<tr>
<td>7.3.4</td>
<td>Data referencing methods in elementary files</td>
<td>23</td>
</tr>
<tr>
<td>7.4</td>
<td>File and data control information</td>
<td>23</td>
</tr>
<tr>
<td>7.4.1</td>
<td>File control information retrieval</td>
<td>23</td>
</tr>
<tr>
<td>7.4.2</td>
<td>Data control information retrieval</td>
<td>24</td>
</tr>
<tr>
<td>7.4.3</td>
<td>Control parameters</td>
<td>24</td>
</tr>
<tr>
<td>7.4.4</td>
<td>Short EF identifier</td>
<td>26</td>
</tr>
<tr>
<td>7.4.5</td>
<td>File descriptor byte</td>
<td>26</td>
</tr>
<tr>
<td>7.4.6</td>
<td>Profile indicator</td>
<td>27</td>
</tr>
<tr>
<td>7.4.7</td>
<td>Data descriptor byte</td>
<td>27</td>
</tr>
<tr>
<td>7.4.8</td>
<td>DF and EF list data elements</td>
<td>27</td>
</tr>
<tr>
<td>7.4.9</td>
<td>Instance number data element</td>
<td>28</td>
</tr>
<tr>
<td>7.4.10</td>
<td>Life cycle status</td>
<td>28</td>
</tr>
<tr>
<td>7.4.11</td>
<td>Indirect referencing by short EF identifier using DO'A2'</td>
<td>28</td>
</tr>
<tr>
<td>7.4.12</td>
<td>Interface and life cycle status dependent security attribute template</td>
<td>29</td>
</tr>
<tr>
<td>8</td>
<td>Specific use of DOs and related concepts</td>
<td>30</td>
</tr>
<tr>
<td>8.1</td>
<td>BER-TLV payloads and padding</td>
<td>30</td>
</tr>
</tbody>
</table>
# ISO/IEC 7816-4:2013(E)

## Contents

- **8.1** Padding conditions .......................................................... 30
  - **8.1.1** 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** Standard tag allocation scheme ..................................... 33
  - **8.3.4** Compatible tag allocation scheme .................................. 33
  - **8.3.5** Coexistent tag allocation scheme .................................. 34
  - **8.3.6** 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
  - **9.4** Access rule references ..................................................... 48
  - **9.5** Security attributes for data objects .................................. 49
  - **9.6** Security parameters template .......................................... 49
  - **9.7** Security attributes for logical channels ......................... 55
  - **9.8** 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
  - **10.4** 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
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.


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
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
— 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:

<table>
<thead>
<tr>
<th>Contact</th>
<th>Patent details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toshiba Corporation&lt;br&gt;Intellectual Property Division&lt;br&gt;1-1, Shibaura 1-Chome&lt;br&gt;Minato-ku, Tokyo&lt;br&gt;105-8001, Japan</td>
<td>JPN 2033906 (priority date: 1986-02-18; publication date: 1996-03-19),&lt;br&gt;FRA 8614996, KOR 44664&lt;br&gt;JPN 2557838 (priority date: 1986-02-18; publication date: 1996-09-05),&lt;br&gt;FRA 8700343, GER 3700504, KOR 42243, USA 4841131&lt;br&gt;JPN 2537199 (priority date: 1986-06-20; publication date: 1996-07-08),&lt;br&gt;FRA 8708646, FRA 8717770, USA 4833595, USA 4901276&lt;br&gt;JPN 2866393 (priority date: 1987-02-17; publication date: 1998-11-27),&lt;br&gt;FRA 8801887, KOR 43929, USA 4847903&lt;br&gt;JPN 2137026 (priority date: 1987-02-20; publication date: 1998-06-26),&lt;br&gt;JPN 3054119, FRA 8802046, KOR 44393, USA 4891506&lt;br&gt;JPN 2831660 (priority date: 1988-08-26; publication date: 1998-09-25),&lt;br&gt;FRA 8911249, KOR 106290, USA 4988855</td>
</tr>
<tr>
<td>Orga Kartensysteme GmbH&lt;br&gt;Am Hoppenhof 33&lt;br&gt;D-33104 Paderborn&lt;br&gt;Germany</td>
<td>DE 198 55 596 (priority date: 1998-12-02; publication date: 2000-06-29)&lt;br&gt;Applications pending in Europe, Russia, Japan, China, USA, Brazil, Australia</td>
</tr>
</tbody>
</table>
Withdrawn
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 7816-6, Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange