

---

---

**Identification cards — Integrated circuit  
cards —**  
**Part 4:**  
**Organization, security and commands for  
interchange**

**iTeh STANDARD PREVIEW**  
*Cartes d'identification — Cartes à circuit intégré —*  
*(standards.iteh.ai)* **Partie 4: Organisation, sécurité et commandes pour les échanges**

ISO/IEC 7816-4:2013

<https://standards.iteh.ai/catalog/standards/sist/5000cd1a-7aae-48bf-922a-a04642ecfcac/iso-iec-7816-4-2013>

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 7816-4:2013](https://standards.iteh.ai/catalog/standards/sist/5000cd1a-7aae-48bf-922a-a04642ecfcac/iso-iec-7816-4-2013)

<https://standards.iteh.ai/catalog/standards/sist/5000cd1a-7aae-48bf-922a-a04642ecfcac/iso-iec-7816-4-2013>



### **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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

Foreword .....	vii
Introduction.....	viii
<b>1 Scope .....</b>	<b>1</b>
<b>2 Normative references .....</b>	<b>1</b>
<b>3 Terms and definitions .....</b>	<b>2</b>
<b>4 Symbols and abbreviated terms .....</b>	<b>7</b>
<b>5 Command-Response pairs .....</b>	<b>8</b>
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
<b>6 Data objects .....</b>	<b>17</b>
6.1 SIMPLE-TLV data objects .....	18
6.2 BER-TLV data objects .....	18
6.3 Constructed DOs versus primitive DOs .....	18
<b>7 Structures for applications and data .....</b>	<b>19</b>
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
<b>8 Specific use of DOs and related concepts.....</b>	<b>30</b>
8.1 BER-TLV payloads and padding.....	30

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

iTeh STANDARD PREVIEW

(standards.iteh.ai)

ISO/IEC 7816-4:2013

<https://standards.iteh.ai/catalog/standards/sist/5000cd1a-7aac-48bf-922a->

[a04042cc1cac/iso-iec-7816-4-2013](https://standards.iteh.ai/catalog/standards/sist/5000cd1a-7aac-48bf-922a-a04042cc1cac/iso-iec-7816-4-2013)

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.....	74
11.3.4	WRITE RECORD command.....	76
11.3.5	UPDATE RECORD command .....	77
11.3.6	APPEND RECORD command .....	77
11.3.7	SEARCH RECORD command.....	78
11.3.8	ERASE RECORD (s) command .....	79
11.3.9	ACTIVATE RECORD (s) command .....	80
11.3.10	DEACTIVATE RECORD (s) command .....	80
11.3.11	COMPARE RECORD function.....	81
11.4	Data object handling .....	81
11.4.1	General .....	81
11.4.2	SELECT DATA command .....	82
11.4.3	GET DATA/GET NEXT DATA commands - even INS code.....	86
11.4.4	GET DATA/GET NEXT DATA command - odd INS codes.....	87
11.4.5	General properties of PUT/PUT NEXT/UPDATE DATA commands .....	89
11.4.6	PUT DATA command.....	89
11.4.7	PUT NEXT DATA command.....	90
11.4.8	UPDATE DATA command.....	91
11.4.9	COMPARE DATA function.....	91
11.5	Basic security handling .....	91
11.5.1	General .....	91
11.5.2	INTERNAL AUTHENTICATE command.....	92
11.5.3	GET CHALLENGE command.....	92
11.5.4	EXTERNAL AUTHENTICATE command.....	93
11.5.5	GENERAL AUTHENTICATE command.....	94
11.5.6	VERIFY command .....	95
11.5.7	CHANGE REFERENCE DATA command.....	96
11.5.8	ENABLE VERIFICATION REQUIREMENT command .....	96
11.5.9	DISABLE VERIFICATION REQUIREMENT command .....	97
11.5.10	RESET RETRY COUNTER command .....	97
11.5.11	MANAGE SECURITY ENVIRONMENT command .....	97
11.6	Miscellaneous .....	99
11.6.1	COMPARE command.....	99
11.6.2	GET ATTRIBUTE command .....	101
11.7	Transmission handling .....	101
11.7.1	GET RESPONSE command.....	101
11.7.2	ENVELOPE command.....	101
12	Application-independent card services .....	102
12.1	Card identification .....	102
12.1.1	Historical bytes.....	102
12.1.2	Initial data string recovery.....	106
12.2	Application identification and selection .....	107
12.2.1	EF.DIR.....	107
12.2.2	EF.ATR/INFO .....	107
12.2.3	Application identifier.....	108
12.2.4	Application template and related data elements.....	109
12.2.5	Application selection .....	110
12.3	Selection by path.....	111
12.4	Data retrieval.....	111

12.5	Card-originated byte strings.....	111
12.5.1	Triggering by the card.....	112
12.5.2	Queries and replies .....	112
12.5.3	Formats.....	112
12.6	General feature management .....	112
12.6.1	On-card services.....	113
12.6.2	Interface services.....	113
12.6.3	Profile services .....	113
12.6.4	Provision of additional information .....	114
12.7	APDU management .....	114
12.7.1	Extended length information .....	114
12.7.2	List of supported INS codes.....	114
Annex A	(informative) Examples of object identifiers and tag allocation schemes.....	115
A.1	Object identifiers.....	115
A.2	Tag allocation schemes .....	115
Annex B	(informative) Examples of secure messaging .....	117
B.1	Cryptographic checksum.....	117
B.2	Cryptograms.....	121
B.3	Control references .....	121
B.4	Response descriptor .....	121
B.5	ENVELOPE command .....	122
B.6	Synergy between secure messaging and security operations.....	122
Annex C	(informative) Examples of AUTHENTICATE functions by GENERAL AUTHENTICATE commands .....	125
C.1	GENERAL AUTHENTICATE using witness-challenge-response triples .....	125
C.2	GENERAL AUTHENTICATE for a multi-step authentication protocol.....	129
NA.1.1	Terminal Authentication protocol.....	131
NA.1.2	Chip Authentication protocol.....	132
Annex D	(informative) Application identifiers using issuer identification numbers .....	133
D.1	Background information .....	133
D.2	Format.....	133
Annex E	(informative) BER Encoding Rules .....	134
E.1	BER-TLV tag fields .....	134
E.2	BER-TLV length fields .....	135
E.3	BER-TLV value fields.....	135
Annex F	(informative) BER-TLV data object handling.....	136
F.1	Generations and templates in a constructed DO .....	136
F.2	Referencing by an extended header.....	137
F.3	Use of the UPDATE DATA command.....	139
F.4	Security attribute for one DO.....	141
F.5	Example of key referencing in a self-controlled DO .....	142
Annex G	(informative) Template extension by tagged wrapper .....	144
G.1	General.....	144
G.2	Referencing within the current EF .....	144
G.3	Referencing within the current application DF, first example .....	145
G.4	Referencing in the current application DF, second example .....	146
G.5	Referencing out of the current application DF .....	147
G.6	Warnings.....	147
Annex H	(informative) Parsing an extended header against its target DO.....	148
Bibliography	.....	149

## 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*

## Introduction

ISO/IEC 7816<sup>[6]</sup> 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<sup>[15]</sup> specifies access by close coupling. ISO/IEC 14443<sup>[18]</sup> and ISO/IEC 15693<sup>[20]</sup> 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:

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

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC 7816-4:2013](#)

<https://standards.iteh.ai/catalog/standards/sist/5000cd1a-7aae-48bf-922a-a04642ecfcac/iso-iec-7816-4-2013>

# 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)*

### 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

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

ISO/IEC 7816-4:2013  
<https://standards.iteh.ai/catalog/standards/sist/5000cd1a-7aae-48bf-922a-a04642ecfcac/iso-iec-7816-4-2013>

**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

**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<sup>[6]</sup> 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

<https://standards.iteh.ai/catalog/standards/sist/5000cd1a-7aae-48bf-922a-a04642ec1cac/iso-iec-7816-4-2013>

**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

**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<sup>[10]</sup>]

**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<sup>[10]</sup>]

**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<sup>[17]</sup>]

**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