INTERNATIONAL STANDARD

ISO/IEC 7816-9

First edition
2000-09-01

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

Part 9: Additional interindustry commands and security attributes

Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 9: Commandes intersectorielles additionnelles et attributs de sécurité

Reference number
ISO/IEC 7816-9:2000(E)

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.ch
Web www.iso.ch

Printed in Switzerland

Contents

Page

Foreword v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols (and abbreviated terms) 2

5 File control parameters 3

6 Life cycle status 4
6.1 Definition and purpose 4
6.2 Principles of use 4
6.3 Life cycle rules 4
6.4 LCS Integer encoding 5

7 Security attributes - general principles 5
7.1 Definition and purpose 5
7.2 Principles of use 5
7.3 Security environments used for access control 6
7.4 Access authorisation coded in certificates 7

8 Security attributes - mechanisms and coding 7
8.1 Coding 7
8.2 Referencing 7
8.2.1 Referencing in the FCI 7
8.2.2 Referencing in SCQL 7
8.2.3 Referencing for data objects 7
8.3 Security attributes for different interface modes 7
8.4 Compact format 8
8.4.1 Introduction 8
8.4.2 Conditions of use 8
8.4.3 Access mode byte 8
8.4.4 Security condition byte 10
8.5 Expanded format 11
8.5.1 Introduction 11
8.5.2 Access Mode data object (AM_DO) 11
8.5.3 Security condition data objects (SC_DO) 12
8.5.4 Access rule references 12

9 Commands 13
9.1 Definition and scope 13
9.2 CREATE FILE command 13
9.2.1 Definition and Scope 13
9.2.2 Conditional usage and security 14
9.2.3 Command message 14
9.2.4 Response message 14
9.2.5 Status conditions 15
9.3 DELETE FILE command 15
9.3.1 Definition and Scope 15
9.3.2 Conditional usage and security 15
9.3.3 Command message 15
9.3.4 Response message 16
9.3.5 Status conditions 16
9.4 DEACTIVATE FILE command 16
9.4.1 Definition and Scope 16

9.4.2 Conditional usage and security 16
9.4.3 Command message 16
9.4.4 Response message 17
9.4.5 Status conditions 17
9.5 ACTIVATE FILE command 17
9.5.1 Definition and Scope 17
9.5.2 Conditional usage and security 17
9.5.3 Command message 18
9.5.4 Response message 18
9.5.5 Status conditions 18
9.6 TERMINATE DF command 18
9.6.1 Definition and Scope 18
9.6.2 Conditional usage and security 19
9.6.3 Command message 19
9.6.4 Response message 19
9.6.5 Status conditions 19
9.7 TERMINATE EF command 19
9.7.1 Definition and Scope 19
9.7.2 Conditional usage and security 19
9.7.3 Command message 20
9.7.4 Response message 20
9.7.5 Status conditions 20
9.8 TERMINATE CARD USAGE command 20
9.8.1 Definition and Scope 20
9.8.2 Conditional usage and security 20
9.8.3 Command message 21
9.8.4 Response message 21
9.8.5 Status conditions 21
9.9 SEARCH BINARY command 21
9.9.1 Definition and Scope 21
9.9.2 Conditional usage and security 21
9.9.3 Command message 22
9.9.4 Response message 22
9.9.5 Status conditions 22
9.10 SEARCH RECORD command 22
9.10.1 Definition and Scope 22
9.10.2 Conditional usage and security 23
9.10.3 Command message 23
9.10.4 Response message 25
9.10.5 Status conditions 25

10 Card originated messages 25
10.1 Definition 25
10.2 Triggering by the card 25
10.3 Message retrieval and reply 26
10.4 Message and reply formats 26
10.5 Conditions of use 26

Annex A (normative) File life cycle states 27
A.1 Commands 27

Annex B (informative) Usage example of security attributes for download 28
B.1 Introduction 28
B.2 Assumptions 28
B.3 Secure downloading 28
B.4 Compact format coding for security attributes of EF 1 29
B.5 Expanded format coding for security attributes of EF 1 30
B.6 Coding of the corresponding Secure Environments (SEs) 31

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 7816 may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 7816-9 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Identification cards and related devices*.

ISO/IEC 7816 consists of the following parts, under the general title *Identification cards — Integrated circuit(s) cards with contacts*:

— *Part 1: Physical characteristics*

— *Part 2: Dimensions and location of the contacts*

— *Part 3: Electronic signals and transmission protocols*

— *Part 4: Interindustry commands for interchange*

— *Part 5: Numbering system and registration procedure for application identifiers*

— *Part 6: Interindustry data elements*

— *Part 7: Interindustry commands for Structured Card Query Language (SCQL)*

— *Part 8: Security related interindustry commands*

— *Part 9: Additional interindustry commands and security attributes*

— *Part 10: Electronic signals and answer to reset for synchronous cards*

Annex A forms a normative part of this part of ISO/IEC 7816. Annex B is for information only.

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

Part 9:
Additional interindustry commands and security attributes

1 Scope

This part of ISO/IEC 7816 specifies

— a description and coding of the life cycle of cards and related objects;

— a description and coding of security attributes of card related objects;

— functions and syntax of additional interindustry commands;

— data elements associated with these commands;

— a mechanism for initiating card-originated messages.

This part of ISO/IEC 7816 does not cover the internal implementation within the card and / or the outside world.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 7816. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 7816 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 7816-4:1995, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange.*

ISO/IEC 7816-7:1999, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 7: Interindustry commands for Structured Card Query Language (SCQL).*

ISO/IEC 7816-8:1999, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands.*

ISO/IEC TR 9577:1996, *Information technology — Protocol identification in the network layer.*

3 Terms and definitions

For the purposes of this part of ISO/IEC 7816, the following terms and definitions apply.

3.1
AND Template
template containing security conditions of which all have to be fulfilled

3.2
access rule
a data element containing an access mode (a reference to an action) and security conditions (to be fulfilled before an action is allowed)

3.3
application
the data structure, data elements and program modules needed for a specific functionality to be satisfied

3.4
OR Template
template containing security conditions of which at least one has to be fulfilled

3.5
security attributes
conditions of use of various resources in the card including stored data and data processing functions, expressed as a data element containing one or several access rules

4 Symbols (and abbreviated terms)

For the purposes of this part of ISO/IEC 7816, the following abbreviations apply:

AM	access mode
AM_DO	access mode data object
APDU	application protocol data unit
ARR	access rule references
AT	authentication template
BER	basic encoding rules (of ASN.1)
CRT	control reference template
DE	data element
DF	dedicated file
DO	data object
EF	elementary file
FCP	file control parameters
File ID	file identifier
IFD	interface device
LCS	life cycle status
LCSI	life cycle status integer
MF	master file
RF	radio frequency
RFU	reserved for future use
SC	security condition
SC_DO	security condition data object
SE	security environment
SE #	security environment number
SM	secure messaging
SW1-SW2	status words
TLV	tag, length, value

5 File control parameters

Table 1 gives the file control parameters (FCP, tag ‘62’) as used in this part of ISO/IEC 7816.

Table 1 - File control parameters

7816 Part-	Tag	L	Value	Applies to
4	‘80’	2	Number of data bytes in the file, excluding structural information	Transparent EFs
4	‘81'	2	Number of data bytes in the file, including structural information if any.	Any file
4	‘82'	1	File descriptor byte	Any file
		2	File descriptor byte followed by data coding byte	Any file
		3	File descriptor byte followed by data coding byte and maximum record length, coded on 1 byte	EFs with record structure
		4	File descriptor byte followed by data coding byte and maximum record length, coded on 2 bytes	EFs with record structure
9		5 or 6	File descriptor byte followed by data coding byte and maximum record length, coded on 2 bytes, and number of records coded on 1 or 2 bytes	EFs with record structure
4	‘83'	2	File identifier	Any file
4	‘84'	1 to 16	DF name	DFs
4	‘85'	var	Proprietary information	Any file
4	‘86'	var	Security attributes, proprietary format	Any file
4	‘87'	2	Identifier of an EF containing an extension of the FCI	Any file
9	‘88'	0 or 1	Short EF identifier, coded from bits b8 to b4. Bits b3, b2, b1 = 000	EFs
9	‘8A'	1	Life Cycle Status Integer (LCSI)	Any file
9	‘8B’	var	Security attributes, reference to expanded format	Any file
9	‘8C’	var	Security attributes, compact format	Any file
9	‘8D’	2	File identifier of file containing SE templates	DFs
9	‘A0’	var	Security attribute template for DOs	Any file
9	‘A1’	var	Security attribute template for interface mode (see 8.3)	Any file
9	‘A2’	var	Short EF identifier / path mapping template, i.e. short EF identifier (tag ‘88’) || path (tag ‘51’) see ISO/IEC 7816-6 || … See note 2	DFs
9	‘A5’	var	Proprietary information, constructed	Any file
9	'AB'	var	Security attributes, expanded format	Any file

NOTE 1 — The meaning of tag ‘82' has been extended in this part of ISO/IEC 7816. Further DOs have been defined.

NOTE 2 — The path to the EF, which can be selected with the short EF identifier, may be an absolute or a relative path.

If selection by short EF identifier is supported but tag ‘88’ is not present, then the 5 least significant bits of the file identifier (tag ‘83’) shall code the short file identifier. If the card supports the short EF identifier mechanism, an empty DO with tag '88' in the FCP indicates that the corresponding EF has no short EF identifier.

6 Life cycle status

6.1 Definition and purpose

The card, files and other objects in the card each have a life cycle, in principle as shown in Annex A.

States in the life cycle may be manipulated by commands. This part of ISO/IEC 7816 defines such commands. Annex A gives a list of these commands.

A life cycle status (LCS) may be associated with files as one of the attributes. It may also be associated with other resources in the card.

To support flexible management of the life cycle as an attribute, a number of life cycle states have been identified, which are defined in this clause. This clause also defines an encoding of the states in the life cycle.

This clause defines a coding of the LCS that allows the card to identify the states. In addition it allows the application to define additional life cycle states. Changes are controlled by the card and may be performed in a pre-defined order, reflecting reversible or irreversible changes in state.

6.2 Principles of use

A card may support a LCS attribute associated with files and, possibly, other objects in the card to indicate the different logical security states of the use of these objects.

Commands may set the value of the LCS attribute when they execute. However the card shall maintain the integrity of this value in accordance with this part of ISO/IEC 7816.

If supported, the current LCS of an object, as expressed by its value, shall be used by the card, possibly in combination with additional security attributes, to determine whether a requested operation with the object is in accordance with the specified security policy.

This standard defines 4 primary states of the life cycle (see 6.3 and Annex A) in the following order:

— creation state;

— initialisation state;

— operational state;

— termination state.

Transitions between the primary states of the life cycle are irreversible and occur in only a top-to-bottom direction.

Each primary state may have reversible secondary states.

6.3 Life cycle rules

The use of objects is governed by the current LCS according to the following rules:

— when an object is in the creation state, any security attributes for that object shall not apply;

— when an object is in the initialisation state, then security attributes specific to this state may apply;

— when an object is in the operational state, then the associated security attributes shall apply;

— when an object is in the termination state, then it shall not allow a modification of its value but it may be used as specified by its associated security attributes e.g. it may be deleted.

See Annex A for an example of the transitions between file life cycle states and associated commands.

The card life cycle status (as defined in ISO/IEC 7816-4) may be present in the historical bytes, in which case the coding shown in Table 2 shall be used.

When the card has a Master file (MF, see ISO/IEC 7816-4), then it is in, at least, the creation state.

6.4 LCS Integer encoding

The LCS Integer (LCSI - tag '8A') encodes the current LCS over one byte. The coding is shown in Table 2.

Table 2 - Coding of the LCSI - tag '8A'

b8..b5	b4	b3	b2	b1	Meaning
'0'	0	0	0	0	no information given
'0'	0	0	0	1	creation state
'0'	0	0	1	1	initialisation state
'0'	0	1	-	1	operational state – activated
'0'	0	1	-	0	operational state – deactivated
'0'	1	1	-	-	termination state
≠ '0'	x	x	x	x	proprietary

7 Security attributes - general principles

7.1 Definition and purpose

The security attributes define the allowed actions, and procedures to be performed to complete such actions (see ISO/IEC 7816-4). In particular, security attributes may:

— specify the security status of the card to be in force before access to data is allowed;

— restrict access to data to certain functions if the card has a particular status;

— define which security functions shall be performed to obtain a specific security status.

Card resources that may be protected with security attributes include:

— files;

— commands;

— tables and views;

— data objects.

7.2 Principles of use

This part of the standard describes the possible content of security attributes as data elements and objects, and the means to retrieve them from the card.

Security attribute definitions may be expressed in a collection of data elements.

A specific resource may be associated with more than one security attribute definition.

A card resource such as an EF or DF may contain in its descriptive data a reference to the security attribute definitions pertaining to it.

Other card resources (e.g. commands and data objects) may be associated with a security attribute definition by a reference contained in the security attribute definition data.

The definition of security attributes shall be specified by use of the following descriptive data elements:

— the set of access rules bound explicitly or implicitly to a resource;

— an access rule combining access modes with security conditions;

— an access mode logically containing a specification of the type of access operation, e.g. read or update. Optionally it specifies the internal function or external command that invokes the appropriate access rule definition;

— a security condition specifying which security mechanisms are necessary to conform to the access rule definition.

See clause 8 for the encoding of these data elements.

7.3 Security environments used for access control

Security environments (SEs, see ISO/IEC 7816-8) used for access control may be stored in the card within a SE Template DO (tag '7B') or in a file (or both).

The SE template DO contains, for every included SE, a SE# DO (tag '80'), an optional LCSI DO (tag '8A') and the corresponding CRTs. The value of the LCSI indicates for which life cycle state the SE is valid. If the SE is used for access control e.g. to a file, then the LCSI of the file and of the SE have to match. If the LCSI is not present, the SE is valid for the operational activated state.

If several DOs with the same tag are present inside a CRT (e.g. DOs specifying a key reference) then only one of the DOs has to be fulfilled (OR condition).

The default SE is always available and is coded under a reserved SE# (#1).

For specifying the usage of a CRT in compliance with the MANAGE SECURITY ENVIRONMENT command, a CRT usage qualifier (tag '95') may be contained in the CRT, see table 3.

Table 3 - Coding of the value of the CRT usage qualifier DO

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1								- verification (DST, CCT) - encipherment (CT) - external authentication (AT)
	1							- computation (DST, CCT) - decipherment (CT) - internal authentication (AT)
		1						- SM response (CCT, CT, DST)
			1					- SM command (CCT, CT, DST)
				1				- User authentication, knowledge based (AT)
					1			- User authentication, biometric based (AT)
						x	x	- RFU (default = 00)