INTERNATIONAL STANDARD

ISO/IEC 7816-9

Third edition
2017-12

Identification cards — Integrated circuit cards —

Part 9: Commands for card management

Cartes d'identification — Cartes à circuit intégré —

Partie 9: Commandes pour la gestion des cartes

Reference number
ISO/IEC 7816-9:2017(E)

COPYRIGHT PROTECTED DOCUMENT

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

Contents

Page

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.

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 ISO documents 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 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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

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

This third edition cancels and replaces the second edition (ISO/IEC 7816-9:2004), which has been technically revised.

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

— a template 'AE' has been proposed for the configuration of command-dependent LCS transitions (see CREATE command);

— Figure 1 (generic LCS transition diagram) has been modified;

— DELETE, ACTIVATE, DEACTIVATE, TERMINATE commands have been redesigned with a common generic P1 parameter, and existing commands have remained unchanged for legacy reasons; 6.1 describes generic or legacy command options and Table 3 describes the bitmap of P1 and P2 for legacy commands and extended command (generic ones);

— MANAGE DATA and DELETE DATA commands have been reserved for DO only; enquiry on DELETE DATA usefulness has been confirmed and the command maintained but declared as likely to be deprecated in future revisions of this document;

— dedicated subclauses have been provided addressing LCS inheritance and LCS evaluation;

— new terminology and rules for evaluated LCS category have been provided: directly assigned or effective, with addition of a recursive table for effective LCS allotment to the child object;

— the command CREATE DATA has been renamed CREATE and assigned a P1 parameter borrowed from generic commands for the sake of harmonization.

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

Introduction

ISO/IEC 7816 is a series of International 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 in the series 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 in the series 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 application management in a multi-application environment.

  — ISO/IEC 7816-15 specifies cryptographic information application.

ISO/IEC 10536 (all parts) specifies access by close coupling. ISO/IEC 14443 (all parts) and ISO/IEC 15693 (all parts) specify access by radio frequency. Such cards are also known as contactless cards.

Identification cards — Integrated circuit cards —

Part 9: Commands for card management

1 Scope

This document specifies interindustry commands for card, file and other structure management, i.e. data object and security object. These commands cover the entire life cycle of the card and therefore some commands are used before the card has been issued to the cardholder or after the card has expired. For details on record life cycle status, refer to ISO/IEC 7816-4.

It is not applicable to the internal implementation within the card and/or the outside world.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1
object
structure (according to ISO/IEC 7816-4) or *security object* (3.3)

3.2
secure messaging
set of means for cryptographic protection of (parts of) command-response pairs

[SOURCE: ISO/IEC 7816-4:2013, 3.50]

3.3
security object
standalone *object* (3.1) nested in an EF, a record, a data object, a DataString or a combination thereof that endorses security handling according to ISO/IEC 7816-4

4 Symbols and abbreviated terms

AID	application identifier
AMF	access mode field
AT	control reference template for authentication
CCT	control reference template for cryptographic checksum
CLA	class byte
CP	control parameter
CP DO	control parameter data object (bearing the tag '62')
CRT	control reference template
DF	dedicated file
DO	BER-TLV data object
DST	control reference template for digital signature
EF	elementary file
EF.ATR/INFO	Answer-to-Reset file or Information file
FCP	file control parameter
FID	file identifier
GAKP	GENERATE ASYMMETRIC KEY PAIR command
ICC	integrated circuit card
IFD	interface device
INS	instruction byte
L_c field	length field for coding the number of bytes in the command data field
L_e field	length field for coding maximum number of bytes expected in the response data field
LCS	life cycle status
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
OID	object identifier
P1-P2	parameter bytes
RFU	reserved for future use by ISO/IEC JTC 1/SC 17
SE	security environment
SEID	security environment identifier

SCB	security condition byte
SM	secure messaging
SPT	security parameter template (using DO'AD' under DO'62')
SW1-SW2	status bytes
TLV	tag, length, value
VA	validity area

5 Life cycle

5.1 General properties

A life cycle status (see coding in ISO/IEC 7816-4:2013, 7.4.10) may be associated with any object in the card and with the card itself. The card shall use the life cycle status in combination with additional security attributes when present and applicable, unless defined otherwise by the application, to determine whether an operation on an object is in accordance with a security policy. The life cycle status determines the use of objects when the card supports life cycle status dependent security attributes according to the following rules.

— If an object is in creation state, then no security attribute shall apply unless otherwise specified.

— If an object is in initialization state, then any security attribute specific to this state may apply.

— If an object is in operational state, then any associated security attribute specific to this state shall apply.

— If an object is in termination state, then the value of the object shall not be accessed unless determined otherwise by its associated security attributes, e.g. it can be deleted.

In addition to the behaviour described above, distinguishing characteristics for primary states of life cycle are defined as follows.

— Creation state — an object is newly created (e.g. by CREATE or CREATE FILE command) or appended (e.g. UPDATE DATA, PUT DATA commands) to an existing object. These operations may fit the created item with its control parameters and may provision it with data elements.

— Initialization state — a newly created object or an existing object in creation state may be initialized. The object is not active but selectable and may be provisioned with data.

— Operational state comprises two secondary states: operational activated and operational deactivated. When activated, the object and its contents may be accessed according to its security attributes. When deactivated, the object is logically reduced with restricted capabilities or functionality but selectable and the access to its content depends on the application. From these states, the object can be terminated.

— Termination state — the object is logically reduced with restricted capabilities or functionality but selectable. The only applicable command is for object deletion unless determined otherwise by the application. Upon selection of a selectable terminated object, the warning status SW1-SW2 = '6285' shall be returned; otherwise, i.e. not selectable object, an error code shall be returned. Further possible actions are not defined in ISO/IEC 7816 (all parts).

— Card Termination state — after a successful completion of the TERMINATE CARD USAGE command, the card shall reject the SELECT command.

After creation, the object is either in creation state or in initialization state or operational (activated or deactivated) state. Transitions between primary life cycle statuses are irreversible and occur only

from creation to termination. In addition, the application may define secondary life cycle status: each primary state may have reversible secondary states. Changes are controlled by the card and may be performed in a pre-defined order, reflecting reversible or irreversible changes in states. Commands that may be used for initiating a life cycle status transition for either card and file management or for data object or further object management are listed in Table 1.

Commands may set the value of the life cycle status when they execute. However, the card shall maintain the integrity of this value in accordance with this document.

For all the life cycle status above, their supported transitions are described in a generic diagram applying to all objects (see Figure 1). For further transition alternatives that may be applied to all objects, see 5.3 for command-dependent LCS transitions. Other commands applicable to the objects in these states, including for the discoverability of their related state, are determined by the application.

Examples of life cycle status handling are provided for information on Annex B.

5.2 Generic life cycle status

Figure 1 provides a generic representation of life cycle status and transitions applying to files, data objects or any further object of which the card management is according to this document. The transitions on Figure 1 are performed upon successful completion of card management commands that are listed in Table 1. The condition of execution of those commands is according to ISO/IEC 7816-4.

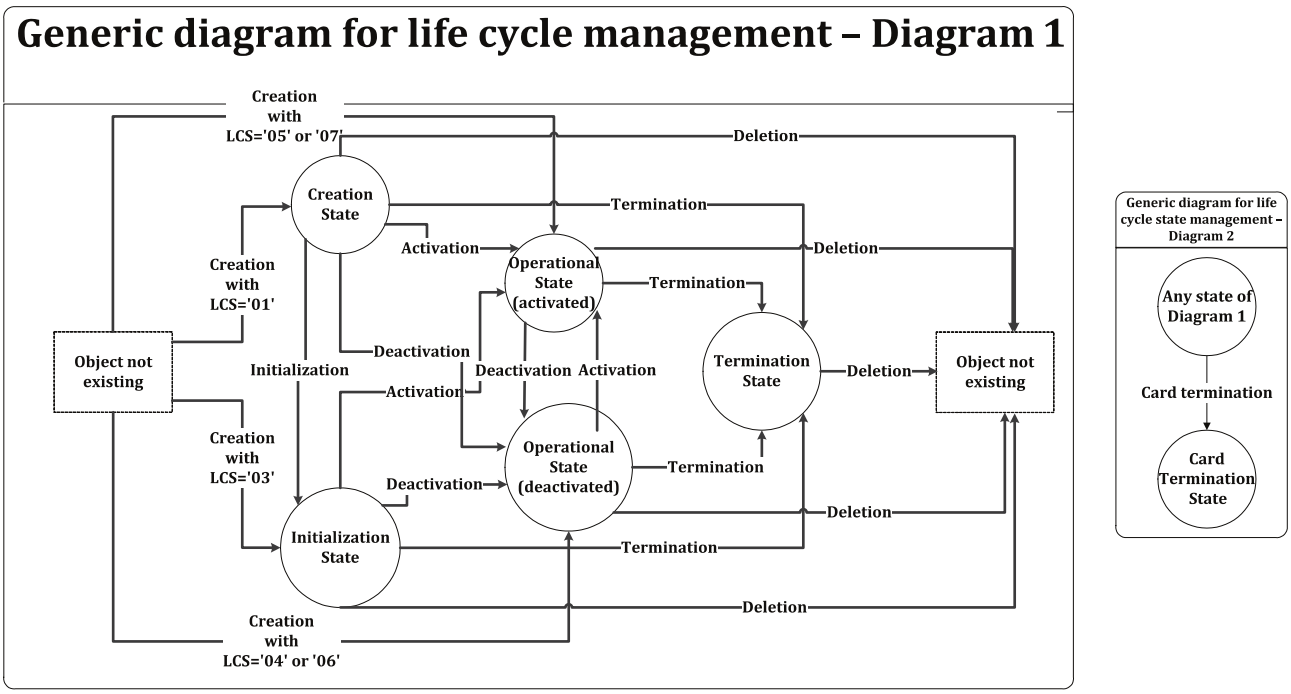

Figure 1 — Generic diagram for life cycle status

NOTE ISO/IEC 7816-4 allows proprietary values for life cycle status that are addressed by this document.

Table 1 — Commands entailing explicit life cycle status transition

Transition		Object	
From	**To**	**File**	**Other objects**
Object not existing	Creation state	CREATE FILE	CREATE
	Initialization state	CREATE FILE Proprietary command[a]	CREATE Proprietary command[a]
	Operational state (activated)	CREATE FILE	CREATE
	Operational state (deactivated)	CREATE FILE	CREATE
	Card termination state	TERMINATE CARD USAGE	TERMINATE CARD USAGE
Creation state	Operational state (activated)	ACTIVATE (FILE)	ACTIVATE[b] MANAGE DATA
	Operational state (deactivated)	DEACTIVATE (FILE)	DEACTIVATE[b] MANAGE DATA
	Initialization state	Proprietary command[a]	MANAGE DATA Proprietary command[a]
	Termination state	TERMINATE EF TERMINATE (DF)	TERMINATE[b] MANAGE DATA
	Object not existing	DELETE (FILE)	DELETE[b] DELETE DATA
	Card termination state	TERMINATE CARD USAGE	TERMINATE CARD USAGE
Initialization state	Operational state (activated)	ACTIVATE (FILE)	ACTIVATE[b] MANAGE DATA
	Operational state (deactivated)	DEACTIVATE (FILE)	DEACTIVATE[b] MANAGE DATA
	Termination state	TERMINATE EF TERMINATE (DF)	TERMINATE[b] MANAGE DATA
	Object not existing	DELETE (FILE)	DELETE[b] DELETE DATA
	Card termination state	TERMINATE CARD USAGE	TERMINATE CARD USAGE
Operational state (activated)	Operational state (deactivated)	DEACTIVATE (FILE)	MANAGE DATA DEACTIVATE[b]
	Termination state	TERMINATE EF TERMINATE (DF)	TERMINATE[b] MANAGE DATA
	Object not existing	DELETE (FILE)	DELETE[b] DELETE DATA
	Card termination state	TERMINATE CARD USAGE	TERMINATE CARD USAGE

[a] For legacy reasons, proprietary commands can be used for this transition.

[b] Transition applicable to objects other than files referenced as described in 6.1.

Table 1 *(continued)*

Transition		Object	
From	**To**	**File**	**Other objects**
Operational state (deactivated)	Operational state (activated)	ACTIVATE (FILE)	MANAGE DATA ACTIVATE[b]
	Termination state	TERMINATE EF TERMINATE (DF)	TERMINATE[b] MANAGE DATA
	Object not existing	DELETE(FILE)	DELETE[b] DELETE DATA
	Card termination state	TERMINATE CARD USAGE	TERMINATE CARD USAGE
Termination state	Object not existing	DELETE (FILE)	DELETE[b] DELETE DATA
	Card termination state	TERMINATE CARD USAGE	TERMINATE CARD USAGE

[a] For legacy reasons, proprietary commands can be used for this transition.

[b] Transition applicable to objects other than files referenced as described in 6.1.

5.3 Command-dependent life cycle status transition

A command-dependent LCS transition for an object is an LCS transition triggered by a command according to the execution rules applicable for the object.

The security handling or operation commands GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR, RESET RETRY COUNTER and CHANGE REFERENCE DATA, and commands initiating the modification of the current template contents as PUT/PUT NEXT/UPDATE DATA may have a command-dependent LCS transition effect of initiating an LCS transition. Unlike the rest of the transitions initiated by other commands and that are said explicit (see Table 1), these transitions are provided as optional functionality.

In the last step of command processing onto an object featuring CP, the assigned CP shall be evaluated to check for the requirement to perform a command-dependent LCS transition.

To be applicable, command-dependent LCS transition functionality shall conform to the following rules:

— for an existing object, all transitions from Figure 1 could be triggered by a command-dependent LCS transition;

— the command-dependent LCS transition applicable for the object shall be executed after successful execution of the command, i.e. the response trailer indicates “normal processing” (see ISO/IEC 7816-4:2013, Table 5);

— such a transition shall be declared during object creation phase with the use of CREATE command only; the use of any other command to achieve the same goal is out of scope of this document;

— the payload of CREATE shall contain within CP template (DO‘62’) a data object ‘AE’ nesting one or more context-specific configuration DO‘A1’, each of which features a value field describing the conditions for a command-dependent LCS transition and is comprised of:

  — an LCS DO‘8A’ according to ISO/IEC 7816-4:2013, Table 14 denoting the starting LCS for the transition;

  — one or more access mode DO from ‘81’ to ‘8F’ according to ISO/IEC 7816-4:2013, Tables 31 and 32, optionally followed by security condition data objects according to ISO/IEC 7816-4:2013, Table 33; access mode and security condition compose an access rule; the LCS transition occurs if and only if this access rule is fulfilled**;**

  — an LCS DO‘8A’ denoting the targeted LCS for the transition.

Whenever it occurs under CREATE (INS code 'E1'), the template 'AE' nested in CP DO'62' is meant for command-dependent transition configuration. See DO'AE' application examples in Annex A.

5.4 Life cycle status inheritance and evaluation

5.4.1 General

This subclause describes the general rules for life cycle status inheritance and evaluation applicable to objects.

Life cycle status are defined herein either as directly assigned LCS or effective LCS.

The life cycle status of a file, a data object or a further object is said to be

— directly assigned LCS when it is configured in the object's CP as the explicit value of DO'8A', or

— effective LCS when it results from the evaluation rules set in Table 2 (see 5.4.2) and it derives from the effective life cycle status of its parent structure.

The effective LCS of an object shall match one among the LCSs of LCS-dependent security attributes for those attributes to be applicable; as a general rule, for LCS-dependent security attributes, the effective LCS shall apply (see ISO/IEC 7816-4:2013, 7.4.12.2). As a general rule, a command can be performed only if the security status satisfies the security attributes defined for the function.

5.4.2 General rules for life cycle status evaluation

Table 2 reads as follows: when a child's directly assigned LCS valuates to a row's value from Table 2, it is assigned the effective LCS as read at the intersection with its parent's effective LCS. At any point of time, before an evaluation is made, the child LCS subject to evaluation is either directly assigned or effective, i.e. resulting from a previous evaluation.

Table 2 — Evaluation matrix for effective LCS of Child in a hierarchy

		Effective LCS of Parent structure				
		Creation state	Initialization state	Operational state (activated)	Operational state (deactivated)	Termination state
Directly assigned LCS of Child object	Creation state	Creation state	Creation state	Creation state	Operational state deactivated	Termination state
	Initialization state	Creation state or Initialization state	Initialization state	Initialization state	Operational state (deactivated)	Termination state
	Operational state (activated)	Creation state or Operational state (activated)	Initialization state or Operational state (activated)	Operational state (activated)	Operational state (deactivated)	Termination state
	Operational state (deactivated)	Creation state or Operational state (deactivated)	Initialization state or Operational state (deactivated)	Operational state (deactivated)	Operational state (deactivated)	Termination state
	Termination state	Out of scope	Out of scope	Termination state	Termination state	Termination state

The following principles are consistent with evaluation rules from Table 2.

— When derived effective LCS, i.e. resulting from the evaluation according to Table 2 matrix, is different from directly assigned LCS, the updating of directly assigned LCS is not required.

— When requested, the LCS DO'8A' (included in CP DO) that is returned shall be the directly assigned one.

— As LCS DO'8A' (included in CP DO) is optional, if an object does not have a directly assigned LCS, then the default value Operational state (activated) is used during the calculation of the effective LCS; see ISO/IEC 7816-4:2013, 7.4.10.

— If a child object is accessed by an IFD, e.g. through SELECT, GET DATA or GET ATTRIBUTE command, with its effective LCS in Operational state (deactivated) or terminated state, the application shall either return

  — checking or execution error status bytes, or

  — a warning processing, for example, SW1-SW2='6200' or '6283' or '6285' or '6287', even though the security attributes of the object aforementioned are assigned an ALWAYS security condition.

5.4.3 Behaviour for effective LCS

Once its effective LCS is evaluated, a child object is allowed the entire set of transitions determined for this resulting LCS as described in Figure 1; if the CP of this child object includes command-dependent LCS transition indicator DO'AE' (see 5.3), some transition(s) may be forbidden for its effective LCS or controlled by security rules.

6 Commands for card management

6.1 General

It shall not be mandatory for all cards complying with this document to support all those commands or all the options of a supported command.

The commands can be performed only if the security status satisfies the security attributes for the command.

For each command, a non-exhaustive list of status bytes is provided (see also ISO/IEC 7816-4).

When using P1 parameters from Table 3:

— bit b5 and bit b6 set to 0, the commands for deletion, activation, deactivation and termination work on files;

— bit b5 set to 1 and bit b6 set to 0, the commands for deletion, activation, deactivation and termination work on passwords;

— bit b5 set to 0 and bit b6 set to 1, the commands for deletion, activation, deactivation and termination work on keys;

— bit b5 and bit b6 set to 1, the commands for deletion, activation, deactivation and termination work on any other structure.

For parameter P2 values, see Table 3.

Table 3 — Coding of P1 in DELETE, ACTIVATE, DEACTIVATE, TERMINATE commands

b8	b7	b6	b5	b4	b3	b2	b1	Meaning	Command data field
0	0	0	0	x	x	x	x	**File operations (EF or DF) P2='00'**[a]	
0	0	0	0	0	0	0	0	Target file is the most recently selected file (EF or DF)	Absent
0	0	0	0	0	0	0	1	Target DF under the current DF	FID indicating DF
0	0	0	0	0	0	1	0	Target EF under the current DF	FID indicating EF
0	0	0	0	0	1	0	0	Target DF by DF name	Full DF name
0	0	0	0	1	0	0	0	Target file indicated with path from the MF	Path without the MF file identifier
0	0	0	0	1	0	0	1	Target file indicated with path from the current DF	Path without the current DF file identifier
0	0	0	1	x	x	x	x	**Password operations**	
0	0	0	1	0	0	0	0	Password reference in P2	Absent
0	0	0	1	0	0	0	1	Further DO in command data field, P2='00'	Further DO with password reference
0	0	1	0	x	x	x	x	**Key operations**	
0	0	1	0	0	0	0	0	Key reference in P2	Absent
0	0	1	0	0	0	0	1	Further DO in command data field, P2='00'	Further DO with key reference
0	0	1	1	x	x	x	x	**Other structure operations**	
0	0	1	1	0	0	0	0	Structure reference in P2, or current structure (P2='00')	Absent
0	0	1	1	0	0	0	1	Further DO in command data field, P2='00'	Further DO with other structure reference

[a] P2='0C' may be used for legacy reasons.

6.2 CREATE FILE command

The CREATE FILE command (see Table 4) initiates the creation of a file (DF or EF) placed immediately under the current DF. The command may allocate memory to the file it creates. The created file shall be set as the current file, unless otherwise specified. MF generation is out of scope of this command.

When a short EF identifier is given that already exists in the current DF, the behaviour of the card is not defined in this document.

The command can be performed only if the security status satisfies the security attributes for the current DF.

The file descriptor byte is mandatory. It indicates whether a DF or an EF is to be created.

— If a DF is created, then a DF name and/or a file identifier shall be specified.

— If an EF is created, then a file identifier and/or a short EF identifier shall be specified.

Table 4 — CREATE FILE command-response pair

CLA	As defined in ISO/IEC 7816-4:2013, 5.4.1
INS	'E0'
P1-P2	'0000' File identifier and file parameters, i.e. file descriptor byte, encoded in the command data field P1 not equal to '00': File descriptor byte as defined in ISO/IEC 7816-4:2013, Table 11 P2 short EF identifier on bits b8 to b4; bits b3 to b1 proprietary
L_c field	Absent for encoding N_c[a] = 0, present for encoding $N_c > 0$
Data field	FCP template (DO'62') and possible further DO, or absent
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4:2013, Tables 5 and 6 where relevant, e.g. '6982', '6A84', '6A86', '6A89', '6A8A'

[a] If number N_c is zero, then the file control parameters of the created file are out of scope of this document.

6.3 DELETE command

The DELETE command (see Table 5) initiates the deletion of a referenced object. In case the referenced object is a DF, it is deleted with its complete sub-tree. After successful completion of this command, the deleted object can no longer be selected, referenced or used. If a file is referenced by this command, the following rule applies in general: if the current file is deleted, its parent becomes the current file. If a file is deleted which is not the current file, the current file may remain the same. Current DF deletion for DF without parent is out of scope of this document.

The deletion of the object may additionally depend on the object LCS. The deletion of MF is out of scope of this document.

NOTE 1 DELETE DATA command with INS='EE' was reserved by ISO/IEC 7816-4; however, the complete functionality is fulfilled by generic DELETE command.

NOTE 2 See 6.1 for generic or legacy command options.

Table 5 — DELETE command-response pair

CLA	As defined in ISO/IEC 7816-4:2013, 5.4.1
INS	'E4'
P1-P2	See Table 3, other value is RFU
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$
Data field	See Table 3
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4:2013, Tables 5 and 6 where relevant, e.g. '9000', '6982', '6985'

6.4 DEACTIVATE command

The DEACTIVATE command (see Table 6) initiates the transition to the Operational state (deactivated) of an object referenced by P1, P2 or by further information in command data field, according to Table 3. When applied to a deactivated file, the SELECT command will select the file and return SW1-SW2 = '6283' as a warning processing status for selected file deactivated.

The command shall only apply to the referenced object (see Table 3).

The successful execution of the command shall not change the VA.

NOTE See 6.1 for generic or legacy command options.

Table 6 — DEACTIVATE command-response pair

CLA	As defined in ISO/IEC 7816-4:2013, 5.4.1
INS	'04'
P1-P2	See Table 3, other value is RFU
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$
Data field	See Table 3
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4:2013, Tables 5 and 6 where relevant, e.g. '6982', '6A80'

6.5 ACTIVATE command

The ACTIVATE command (see Table 7) initiates the transition to the Operational state (activated) of an object referenced by P1, P2 or by further information in command data field, according to Table 3.

The successful execution of the command shall not change the VA.

NOTE See 6.1 for generic or legacy command options.

Table 7 — ACTIVATE command-response pair

CLA	As defined in ISO/IEC 7816-4:2013, 5.4.1
INS	'44'
P1-P2	See Table 3, other value is RFU
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$
Data field	See Table 3
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4:2013, Tables 5 and 6 where relevant, e.g. '6400', '6982'

6.6 TERMINATE command

The TERMINATE command (see Table 8) initiates the irreversible transition to the termination state of an object referenced by P1, P2 or by further information in data field, according to Table 3. In case of a terminated DF, the DF shall be selectable and if selected, the warning status SW1-SW2 = '6285' (selected file in termination state) shall be returned. Further possible actions are not defined in ISO/IEC 7816 (all parts).

The successful execution of the command shall not change the VA.

NOTE 1 The intent of DF termination is generally to make the application unusable by the cardholder.

NOTE 2 See 6.1 for generic or legacy command options.

Table 8 — TERMINATE command-response pair

CLA	As defined in ISO/IEC 7816-4:2013, 5.4.1
INS	'E6'
P1-P2	See Table 3, other value is RFU
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$
Data field	See Table 3
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4:2013, Tables 5 and 6 where relevant, e.g. '6982', '6985'

6.7 TERMINATE EF command

The TERMINATE EF command (see Table 9) initiates the irreversible transition to the termination state of an EF referenced by P1, P2 or by further information in command data field, according to Table 3.

The successful execution of the command shall not change the VA.

Table 9 — TERMINATE EF command-response pair

CLA	As defined in ISO/IEC 7816-4:2013, 5.4.1
INS	'E8'
P1-P2	See Table 3, other value is RFU
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$
Data field	See Table 3
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4:2013, Tables 5 and 6 where relevant, e.g. '6982', '6985'

6.8 MANAGE DATA command

The MANAGE DATA command (see Table 10) initiates LCS transition of the indicated DO according to direction indicated in Figure 1. P2 indicates the target LCS for the transition. Coding of P1 is the same as that of SELECT DATA command (see ISO/IEC 7816-4). Command data field is either absent or features the general reference DO'60' (see ISO/IEC 7816-4). For MANAGE DATA command, DO'60' includes one DO only such as tag list DO'5C', extended header DO'4D' or DO'5F61'. If several DOs correspond to general reference DO's indication, P1='01' to 'EF' denotes occurrence number of target DO.

— If several instances of a DO fit the target definition, P1= '00' to 'EF' denotes occurrence number of instance and allows for successive management of all instances.

— When executed with empty command data field, MANAGE DATA does not select the DO to be managed, i.e. it does not modify the current VA; when selecting the DO, the effect of this command on the current VA is according to ISO/IEC 7816-4.

Table 10 — MANAGE DATA command-response pair

CLA	As defined in ISO/IEC 7816-4:2013, 5.4.1
INS	'CF'
P1	'00' to 'EF' for occurrence number of instance (numbered in Data Field) 'F0' parent of curConstructedDO if it exists. >'F0' RFU
P2	See Table 11
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$
Data field	Absent or general reference DO'60' (see ISO/IEC 7816-4:2013, Table 86)
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4:2013, Table 5 and Table 6 where relevant, e.g. '6202' to '6280', '6281', '6700', '6981', '6982', '6985', '6A81', '6A88' (DOs not found, i.e. referenced data not found)

Table 11 — Coding of P2 in MANAGE DATA command

Value	Meaning
'03'	Initialize DO
'04'	Deactivate DO
'05'	Activate DO
'0C'	Terminate DO

6.9 CREATE command

The CREATE command (see Table 12) generates a new object in the logical context defined by the object related VA references. The command data field may comprise a CP DO'62' including a command-dependent LCS transition indicator DO'AE' (see 5.3), along with further DO. The created object shall be set as the current object unless otherwise specified.

Table 12 — CREATE command-response pair

CLA	As defined in ISO/IEC 7816-4:2013, 5.4.1
INS	'E1'[a]
P1-P2	See Table 13
L_c field	Present for coding $N_c > 0$
Data field	CP DO'62' when needed, optionally including command-dependent LCS management template DO'AE' (see 5.3) and/or further DO
L_e field	Absent

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4:2013, Table 5 and Table 6 where relevant, e.g. '6981', '6982', '6986', '6A82', '6A83'

[a] The INS code of this command is not defined in ISO/IEC 7816-4.

Table 13 — Coding of P1 for generic CREATE command

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	P2='00', no information given, creation of an object of arbitrary type
0	0	0	1	**0**	**0**	**0**	**x**	**Creation of a password**
				0	0	0	0	Password reference in P2
				0	0	0	1	P2='00', further DO in command data field
0	0	1	0	**0**	**0**	**0**	**x**	**Creation of a key**
				0	0	0	0	Key reference in P2
				0	0	0	1	P2='00', further DO in command data field
0	0	1	1	**0**	**0**	**0**	**x**	**Creation of other structures**
				0	0	0	0	Structure reference in P2
				0	0	0	1	P2='00', further reference DO in command data field
Any other value is RFU.								

6.10 TERMINATE CARD USAGE command

The TERMINATE CARD USAGE command (see Table 14) initiates the irreversible transition of the card into the termination state. Use of this command gives an implicit selection of the MF.

For cards supporting this command, the termination state should be indicated in the Answer-to-Reset.

NOTE The intent of terminating card usage is to make the card unusable by the cardholder.

Table 14 — TERMINATE CARD USAGE command-response pair

CLA	As defined in ISO/IEC 7816-4:2013, 5.4.1
INS	'FE'
P1-P2	'0000'
L_c field	Absent for encoding $N_c = 0$
Data field	Absent
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4:2013, Tables 5 and 6 where relevant, e.g. '6982', '6985'

6.11 IMPORT CARD SECRET command

The IMPORT CARD SECRET command (see Table 15) initiates the import of card secret data related to a key or password or biometric reference object placed under the current DF.

The relevant security object is referred by P1, P2 or by further information in the data field, according Table 3. The card secret data are transmitted using a DO or template depending on the type of the card secret data.

The command can be performed only if the security status satisfies the security attributes for the security object.

Table 15 — IMPORT CARD SECRET command-response pair

CLA	As defined in ISO/IEC 7816-4:2013, 5.4.1
INS	'48'[a]
P1-P2	See Table 3, other value is RFU
L_c field	Present for encoding $N_c > 0$
Data field	DO with reference to the security object according Table 3 (conditional), followed by a data object transmitting the secret data. '5F48' or '7F48': private key '5F49' or '7F49': public key '53' or '73': secret key '53': password reference data '5F2E' or '7F2E': biometric reference data '7F61' or '7F60': biometric information template(s)
L_e field	Absent for encoding $N_e = 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4:2013, Table 5 and Table 6 where relevant, e.g. '6982', '6A80', '6A88'

[a] The INS code of this command is not defined in ISO/IEC 7816-4.

Annex A
(informative)

Command-dependent LCS transition examples

A.1 General

The combination allowed by DO'AE' may achieve a variety of use cases as described in the following examples.

A.2 Example of key generation or update

The newly created object's LCS may be respectively changed into Operational state (activated) or Operational state (deactivated) upon successful execution of either GENERATE ASYMMETRIC KEY PAIR or GENERAL AUTHENTICATE command, e.g. an object hosting a key is deactivated every time its content is renewed through GENERATE ASYMMETRIC KEY PAIR command, then an administrator has to authorize the activation of this key object with ACTIVATE command to allow its use by the cardholder.

A.3 Example of provision of content

Once an object is created with its LCS set at Creation state, this LCS may transit to initialization state by provisioning its content, e.g. by nesting further data or by generating DO of further generation upon successful execution of PUT DATA, PUT NEXT DATA or UPDATE DATA command.

A.4 Example of a password administration

Every time the value of a password/PIN or its attribute of authorized tries is changed (e.g. with CHANGE REFERENCE DATA or RESET RETRY COUNTER), the object hosting this password/PIN, or the password/PIN itself, is deactivated, i.e. its LCS becomes Operational state (deactivated), e.g. this process may be employed to require from an administrator to confirm the authorization of use to the cardholder, e.g. by an ACTIVATE command.

A.5 Example of key initialization

Once an object is created and its LCS set at either Creation state, Operational state (activated) or Operational state (deactivated), this LCS may transit upon successful execution of either GENERATE ASYMMETRIC KEY PAIR or GENERAL AUTHENTICATE command, e.g. an object intended to host a key pair is created as an empty container, and once provisioned with keys through GENERATE ASYMMETRIC KEY PAIR, its LCS moves from its Creation state to its Initialization state.

A.6 Example of digital signature control

An ICC featuring digital signature functionality may be set up by an administrator with a password object and assigned attributes but no content (i.e. no password value set) and LCS state Operational state (deactivated). A user applies the CHANGE REFERENCE DATA command according to the access rules to set an initial password value. The command triggers the LCS transition of the password object into Operational state (activated), which saves the user one command.

A.7 Example of object behaviour after LCS evaluation

When its effective LCS is evaluated for a child object (see 5.4.2), the transition(s) from this resulting LCS may be controlled by the application. In case that such object includes command-dependent LCS transition indicator DO'AE' within its CP DO (see 5.3), some transition(s) may be forbidden.

Annex B
(informative)

Life cycle status handling examples

B.1 General

This annex provides further clarifications on file or data object life cycle status handling.

B.2 LCS interdependencies issue

If the security parameter template DO'AD' is expanded with an additional DO'7B' encapsulating a Security Environment template, i.e. set of control reference templates (CRT), and featuring an LCS (DO'8A'), this LCS, if any, shall match LCS DO occurring immediately under interface and LCS dependent security attribute template DO(DO'A3'); otherwise, the Security Environment is not applicable (see Table B.1).

Table B.1 — Interdependencies between Physical interface, LCS, security attributes and SE

DO generation				Value	
1st	2nd	3rd	4th		
'62'				CP DO	
	'8A'			LCS (Life Cycle Status), optional	
	'A3'			Interface and LCS dependent security attribute template	
		'91'		**Physical interface** (contact/contactless, etc.)	
		'8A'		**LCS**	
		'9C'		AMF || SCB (ref#n)	Alternatively Tag '9D' under tag 'AB' when using expanded format
		'5C'		Tag list	
	'AD'			Security parameters template #n	
		'80'		AD sequence number (AD #n)	
		'AX'		Security attributes extension (X from 0 to 4)	
		'7B'		Security Environment template	
			'80'	SEID	
			'8A'	**LCS**, optional	
			'AC'	Cryptographic mechanism identifier template, optional	
			'A4', 'A6', 'AA', 'B4', 'B6', 'B8'	CRTs	
		'83'		OID related information, optional	
		'63'		Wrapper pointing, e.g. to the security object involved in AX, optional	

B.3 Retrieval of LCS value

The directly assigned life cycle status of a file or a DO may be retrieved by either (non-exhaustive list) of the following.

— COMPARE command (see ISO/IEC 7816-4:2013, 11.6.1) may be applied to check whether a data object LCS belongs to a set of input LCS values, i.e. it may be necessary to ask the card whether the LCS of a given DO is either Operational state (activated) or Operational state (deactivated); accordingly, the response to such a question (COMPARE command) may be either YES (SW1-SW2='90 00') or NO (SW1-SW2='63 40').

  For this purpose, two values of parameter P2 are possible:

  — '07' which means that the reference value shall belong to the set of finite values defined by the command;

  — '08' which means that the reference value shall not belong to the set of finite values defined by the command.

  The target of such COMPARE command shall be the value of the primitive DO'8A' standing for reference data.

— GET ATTRIBUTE command (see ISO/IEC 7816-4:2013, 11.6.2).

— SELECT, SELECT DATA, or GET DATA command with a parameter specifying to return CP DOs, then DO'8A' immediately under DO'62' in the response data field is extracted by IFD.

When required by bit b5 set to 1 in parameter P2 of SELECT DATA command, this command returns a tag list DO'5C' nesting the same concatenation of tags as in the DIR function but, according to its needs, an application may exclude the tags that do not fulfil some conditions; unless specified otherwise by the application, the default condition that applies on DO, security objects and files for the VIEW function is LCS valuating to Operational state (activated).

B.4 Life cycle status handling for DO with same tag in same generation

For DO(s) with same tag in the same template (thus in the same generation), the handling of one among those DOs for the purpose of reading or setting or updating its LCS may use DO ordering within this template; a proper selection of the targeted DO is required, e.g. SELECT DATA, GET NEXT DATA with odd INS code or PUT DATA, PUT NEXT DATA, or UPDATE DATA using a pointer set by the command and not by the template allowing pointing the DO before to set its LCS.

B.5 Life cycle status of tagged wrapper extension

Primary DO LCS influences the view on extensions possibly targeted by the primary DO, i.e. wrapper extension. The LCS of a tagged wrapper does not impact any property of the referenced object if any, but may impact the view on the targeted object. Besides, when the outside world sets the LCS of a DO belonging to the parent template, it does not impact the LCS of the template extension, e.g. even in case the LCS of the parent template becomes TERMINATED, the DO belonging to the extension template remains in its former state with its life cycle unchanged.

B.6 Life cycle status handling for DO hosted in files

When not featuring their CP DO, data objects nested in files may have their related security attributes encoded within the file header under security attribute template DO'A0' as described on Table B.2; such implementation complies with ISO/IEC 7816-4 rules.

Table B.2 — Example of CP DO contents for DOs nested in File

DO generation				Value	
1st	2nd	3rd	4th		
'62'				CP DO	
	'8A'			LCS (Life Cycle status)	
	'A3'			Interface and LCS dependent security attribute template	
		'91'		**Physical interface**	
		'8A'		**LCS**	
		'A0'		Security attributes template **for DOs**	
			'8C'	AMF associated to **DO** handling commands	Alternatively Tag '9C' or '9D' with SPT oriented security attributes
			'5C'	Tag list	
	'A3'			Interface and LCS dependent security attribute template	
		'91'		**Physical interface**	
		'8A'		LCS	
		'8C'		AMF associated to **Application DF/ DF/EF** handling commands	Alternatively Tag '9C' or '9D' with SPT oriented security attributes

Bibliography

[1] ISO/IEC 7816 (all parts), *Identification cards — Integrated circuit cards*

[2] ISO/IEC 10536 (all parts), *Identification cards — Contactless integrated circuit(s) cards — Close-coupled cards*

[3] ISO/IEC 14443 (all parts), *Identification cards — Contactless integrated circuit cards — Proximity cards*

[4] ISO/IEC 15693 (all parts), *Identification cards — Contactless integrated circuit cards — Vicinity cards*

ICS 35.240.15

Price based on 21 pages