

---

---

**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*

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

[ISO/IEC 7816-9:2017](https://standards.iteh.ai/catalog/standards/sist/7b04e519-bccb-43a9-8582-b9f7534fc0b1/iso-iec-7816-9-2017)

<https://standards.iteh.ai/catalog/standards/sist/7b04e519-bccb-43a9-8582-b9f7534fc0b1/iso-iec-7816-9-2017>



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

[ISO/IEC 7816-9:2017](https://standards.iteh.ai/catalog/standards/sist/7b04e519-bccb-43a9-8582-b9f7534fc0b1/iso-iec-7816-9-2017)

<https://standards.iteh.ai/catalog/standards/sist/7b04e519-bccb-43a9-8582-b9f7534fc0b1/iso-iec-7816-9-2017>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2017, Published in Switzerland

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

ISO copyright office  
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](mailto:copyright@iso.org)  
[www.iso.org](http://www.iso.org)

# Contents

	Page
<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols and abbreviated terms</b> .....	<b>2</b>
<b>5 Life cycle</b> .....	<b>3</b>
5.1 General properties.....	3
5.2 Generic life cycle status.....	4
5.3 Command-dependent life cycle status transition.....	6
5.4 Life cycle status inheritance and evaluation.....	7
5.4.1 General.....	7
5.4.2 General rules for life cycle status evaluation.....	7
5.4.3 Behaviour for effective LCS.....	8
<b>6 Commands for card management</b> .....	<b>8</b>
6.1 General.....	8
6.2 CREATE FILE command.....	9
6.3 DELETE command.....	10
6.4 DEACTIVATE command.....	10
6.5 ACTIVATE command.....	11
6.6 TERMINATE command.....	11
6.7 TERMINATE EF command.....	12
6.8 MANAGE DATA command.....	12
6.9 CREATE command.....	13
6.10 TERMINATE CARD USAGE command.....	14
6.11 IMPORT CARD SECRET command.....	14
<b>Annex A (informative) Command-dependent LCS transition examples</b> .....	<b>16</b>
<b>Annex B (informative) Life cycle status handling examples</b> .....	<b>18</b>
<b>Bibliography</b> .....	<b>21</b>

## 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](http://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](http://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](http://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.

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

[ISO/IEC 7816-9:2017](#)

<https://standards.iteh.ai/catalog/standards/sist/7b04e519-bccb-43a9-8582-b9f7534fc0b1/iso-iec-7816-9-2017>

# 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 <sub>c</sub> field	length field for coding the number of bytes in the command data field
L <sub>e</sub> field	length field for coding maximum number of bytes expected in the response data field
LCS	life cycle status
MF	master file
N <sub>c</sub>	number of bytes in the command data field
N <sub>e</sub>	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

iTech STANDARD PREVIEW  
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/7b04e519-bccb-43a9-8582-091f534e661/iso-iec-7816-9-2017>



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.

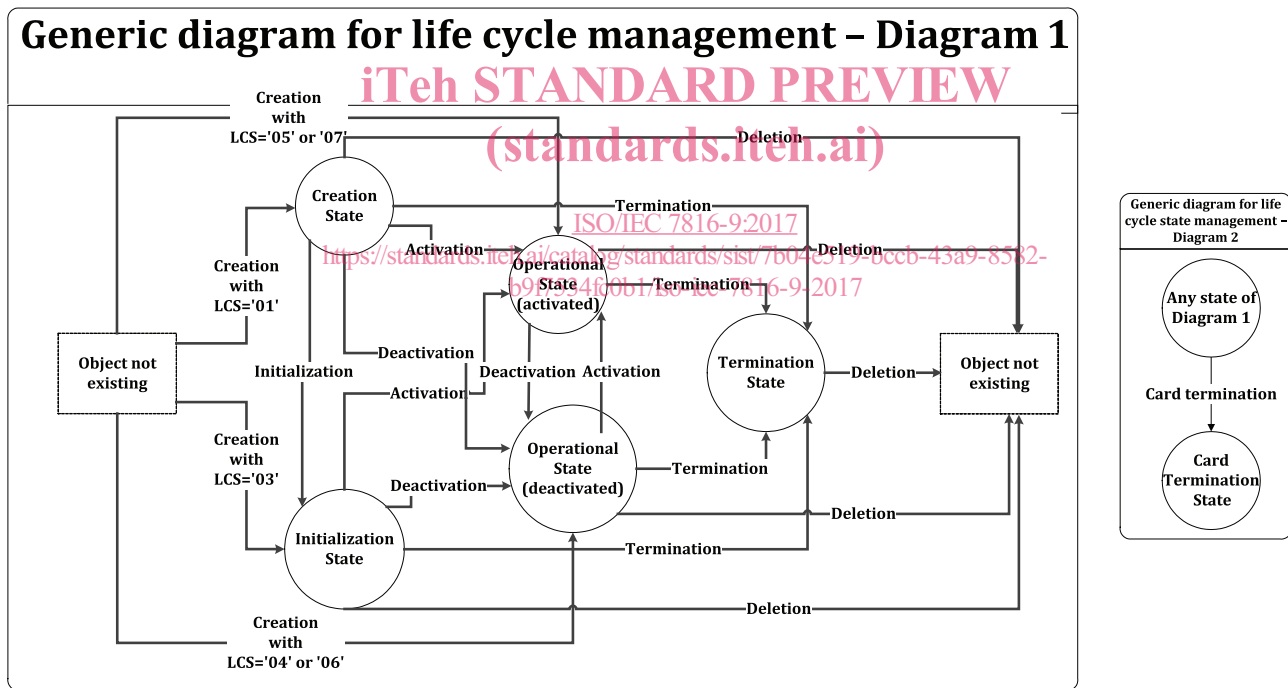


Figure 1 — Generic diagram for life cycle status

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
<b>Object not existing</b>	Creation state	CREATE FILE	CREATE
	Initialization state	CREATE FILE Proprietary command <sup>a</sup>	CREATE Proprietary command <sup>a</sup>
	Operational state (activated)	CREATE FILE	CREATE
	Operational state (deactivated)	CREATE FILE	CREATE
	Card termination state	TERMINATE CARD USAGE	TERMINATE CARD USAGE
<b>Creation state</b>	Operational state (activated)	ACTIVATE (FILE)	ACTIVATE <sup>b</sup> MANAGE DATA
	Operational state (deactivated)	DEACTIVATE (FILE)	DEACTIVATE <sup>b</sup> MANAGE DATA
	Initialization state	Proprietary command <sup>a</sup>	MANAGE DATA Proprietary command <sup>a</sup>
	Termination state	TERMINATE EF TERMINATE (DF)	TERMINATE <sup>b</sup> MANAGE DATA
	Object not existing	DELETE (FILE)	DELETE <sup>b</sup> DELETE DATA
	Card termination state	TERMINATE CARD USAGE	TERMINATE CARD USAGE
<b>Initialization state</b>	Operational state (activated)	ACTIVATE (FILE)	ACTIVATE <sup>b</sup> MANAGE DATA
	Operational state (deactivated)	DEACTIVATE (FILE)	DEACTIVATE <sup>b</sup> MANAGE DATA
	Termination state	TERMINATE EF TERMINATE (DF)	TERMINATE <sup>b</sup> MANAGE DATA
	Object not existing	DELETE (FILE)	DELETE <sup>b</sup> DELETE DATA
	Card termination state	TERMINATE CARD USAGE	TERMINATE CARD USAGE
<b>Operational state (activated)</b>	Operational state (deactivated)	DEACTIVATE (FILE)	MANAGE DATA DEACTIVATE <sup>b</sup>
	Termination state	TERMINATE EF TERMINATE (DF)	TERMINATE <sup>b</sup> MANAGE DATA
	Object not existing	DELETE (FILE)	DELETE <sup>b</sup> DELETE DATA
	Card termination state	TERMINATE CARD USAGE	TERMINATE CARD USAGE

<sup>a</sup> For legacy reasons, proprietary commands can be used for this transition.

<sup>b</sup> Transition applicable to objects other than files referenced as described in 6.1.