INTERNATIONAL STANDARD

ISO/IEC
7816-13

First edition
2007-03-15

Identification cards — Integrated circuit cards —

Part 13:
Commands for application management in a multi-application environment

Cartes d'identification — Cartes à circuit intégré —

Partie 13: Commandes pour la gestion d'application dans un environnement de plusieurs applications

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 7816-13:2007
https://standards.iteh.ai/catalog/standards/sist/a0f275a7-1b04-4e5e-912b-
c62771c8ffb3/iso-iec-7816-13-2007

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.

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 technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member 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 7816-13 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

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

— *Part 1: Cards with contacts — Physical characteristics*

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

— *Part 3: Cards with contacts — Electrical interface and transmission protocols*

— *Part 4: Organization, security and commands for interchange*

— *Part 5: Registration of application providers*

— *Part 6: Interindustry data elements for interchange*

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

— *Part 8: Commands for security operations*

— *Part 9: Commands for card management*

— *Part 10: Cards with contacts — 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 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 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 of the physical interface technology. They apply to cards accessed by contacts and/or by contactless methods.

— 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 specifies access by close coupling. ISO/IEC 14443 and ISO/IEC 15693 specify access by radio frequency. Such cards are also known as contactless cards.

Identification cards — Integrated circuit cards —

Part 13:
Commands for application management in a multi-application environment

1 Scope

This part of ISO/IEC 7816 specifies commands for application management in a multi-application environment. These commands cover the entire life cycle of applications in a multi-application integrated circuit card, and the commands can be used before and after the card is issued to the cardholder. This part of ISO/IEC 7816 does not cover the implementation within the card and/or the outside world.

2 Normative references

iTeh STANDARD PREVIEW

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 7816-13:2007

ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit cards — Organization, security and commands for interchange*

c62771c8ffb3/iso-iec-7816-13-2007

ISO/IEC 7816-9:2004, *Identification cards — Integrated circuit cards — Commands for card management*

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
application
structures, data elements and program modules needed for performing a specific functionality

[ISO/IEC 7816-4]

3.2
application provider
entity providing the components that make up an application in the card

[ISO/IEC 7816-4]

3.3
card platform
on-card component responsible for basic card functions

3.4
card manager application
card application providing card application management functionality and supervising assignment of the card's resources

4 Abbreviations and notation

AID   application identifier

APP   application

DF   dedicated file

DO   data object

ICC   integrated circuit card

P1-P2   parameter bytes (inserted for clarity, the dash is not significant)

RID   registered application provider identifier

5 Multi-application environment and application life cycle

5.1 Multi-application environment

A multi-application environment in the context of this document has the following characteristics.

a) An application is a uniquely addressable set of functionalities on a multi-application card that provides data storage and computational services.

b) An application may be added to the card before or after the card is issued to the cardholder.

c) More than one application may be added to the card.

d) The card platform provides mechanisms for managing card resources e.g. memory.

e) The card platform provides a security boundary mechanism for each application to prevent unauthorized interaction and security violation from any other application on the card.

f) An application provider is an entity that provides services to the cardholder using a card's application and is responsible for the application's behavior.

g) An application provider for an application on a card may be distinct from the card issuer.

h) The life cycle of an application is independent from the life cycle of any other application in the same card.

i) The life cycle of an application is independent from the life cycle of the card except when the card is in the termination state, as defined in ISO/IEC 7816-9.

j) All applications shall be at least selectable using the SELECT command by specifying its AID as the DF name, as defined in ISO/IEC 7816-4.

k) A card manager application shall be present, unique, and selectable using the SELECT command by specifying its AID as the DF name. Other applications on the card may offer application management functionality.

l)   The default AID of the card manager application is "E8 28 BD 08 0D".

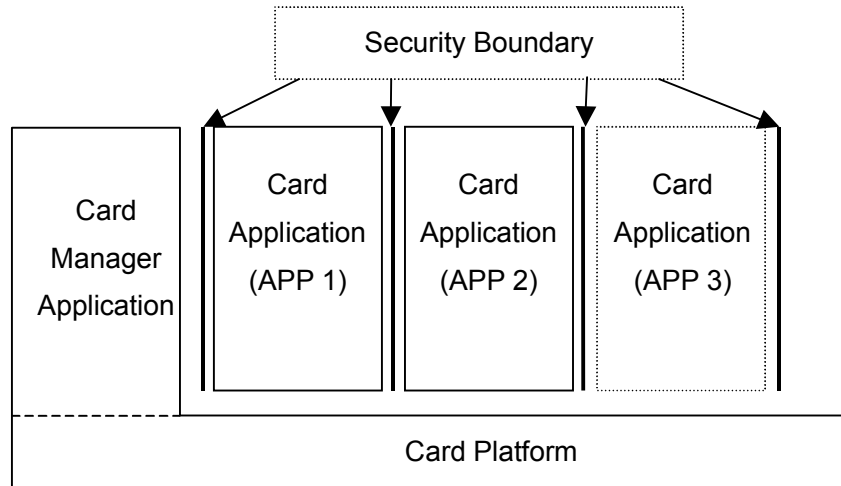Figure 1 is a conceptual representation of a possible structure of a multi-application IC card.

**Figure 1 — Possible structure of a multi-application card**

5.2   Application life cycle

A life cycle status shall be associated with each application. An application may use its life cycle status, in combination with its security attributes, to ensure that any operation it performs complies with that application's security policy. The card manager application shall provide a life cycle transition path from Non Existent to Operational Activated state.

The following commands initiate life cycle state transitions:

— APPLICATION MANAGEMENT REQUEST;

— LOAD APPLICATION;

— REMOVE APPLICATION.

Figure 2 is a conceptual representation of the life cycle states and the commands that invoke each state transition. This diagram shows only the stable (permanent) states an application can reach at the completion of a life cycle transition. Other, intermediate, states may exist during a life cycle transition (e.g. from Non-Existent to Creation state) but are not maintained when the process is interrupted.
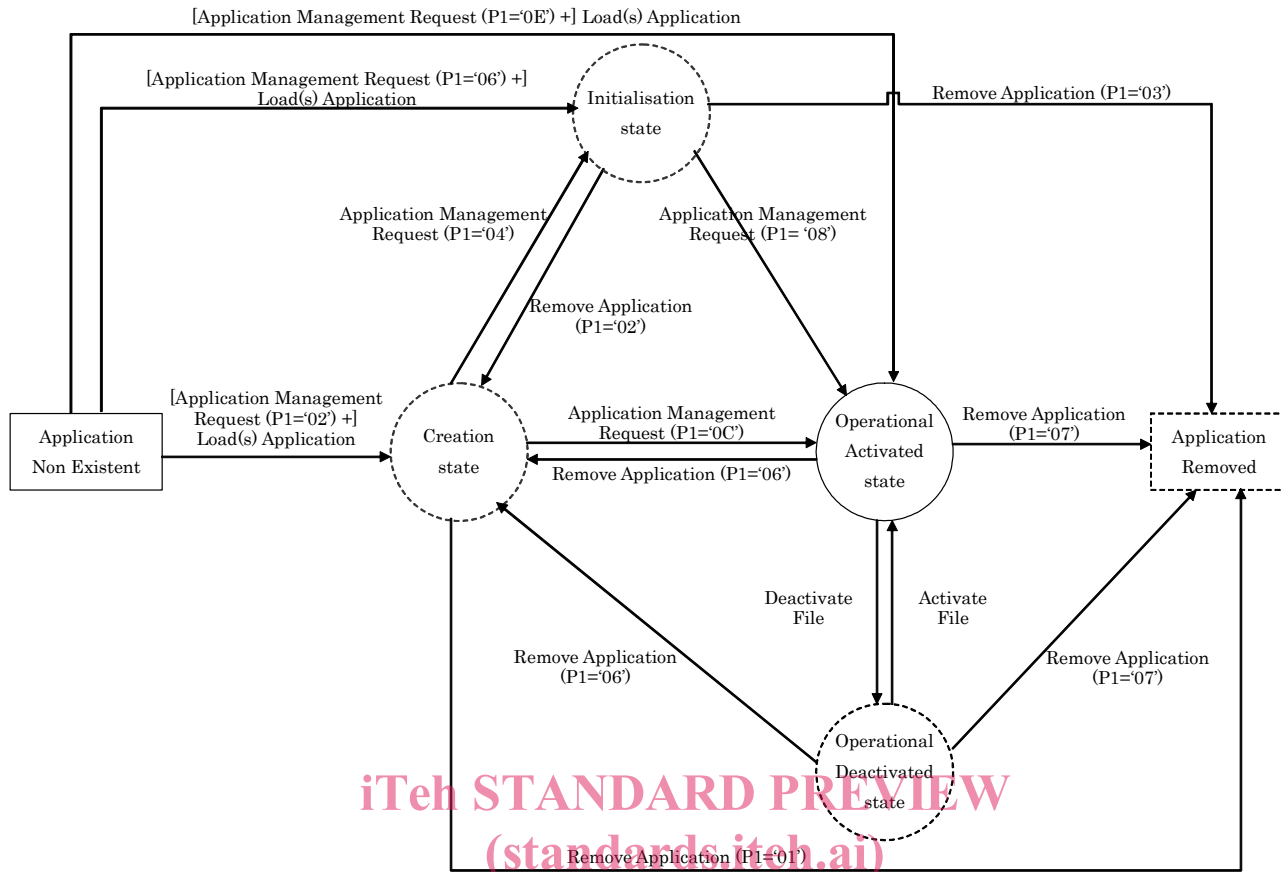
ISO/IEC 7816-13:2007
https://standards.iteh.ai/catalog/standards/sist/0f2d5a7f-4b94-4e5e-912b-
c62771c8ffb3/iso-iec-7816-13-2007

Figure 2 — Application life cycle diagram

NOTE 1 – This diagram reads as follows: for example, after the execution of the APPLICATION MANAGEMENT REQUEST (P1="0E") and LOAD APPLICATION commands, the application is in the Operational Activated life cycle state i.e. executable and selectable.

NOTE 2 – Squares represent states of the card memory, and circles represent application life cycle states. Dotted circles represent optional application life cycle states.

NOTE 3 – The ACTIVATE FILE and DEACTIVATE FILE commands are defined in ISO/IEC 7816-9.

Application life cycle states are defined as in Table 1.

The coding of the application life cycle states shall comply with the coding of the life cycle status byte (LCS byte) defined in ISO/IEC 7816-4.

Table 1 — Application life cycle states

Application Non Existent	Application is, from the point of view of the card manager application, not present.
Creation State	Application is, from the point of view of the card manager application, present, not executable, and not selectable.
Initialisation State	Application is present, executable with limited functionality, and not selectable.
Operational Activated State	Application is present, executable, and selectable.
Operational Deactivated State	Application is present, executable with limited functionality, and the SELECT command returns the warning that the application is deactivated.
Application Removed	Application is not present, not selectable, and not executable. The previously assigned memory resources may be only partially released and reusable.
— Some card platforms may have additional life cycle specific state. Additional states are outside the scope of this document. If the card supports additional life cycle states and state transitions, they shall not interfere with the life cycle states and state transitions described in Figure 2.	
— States in italics represent card memory states. States in regular characters represent application life cycle states.	

5.3 Memory resource assignment data objects for interoperability

A memory resource assignment template (tag "7F65") describing the assignment of memory resources to an application may be associated with each application.

Table 2 specifies the memory resource assignment data objects for each type of memory: persistent or volatile storage, where

— **reserved memory** is the amount of memory exclusively assigned to an application;

— **memory quota** is the maximum amount of memory that an application is allowed to request.

A **memory resource assignment data object** represents an amount of memory resources counted in bytes, coded as an integer value, see ISO/IEC 8825-1.

Table 2 — Memory resource assignment data objects

Tag	Description	Requirement
"80"	Amount of reserved memory in persistent storage for the application's code. If no separation between code and data is requested, then "80" shall be used to indicate the reserved amount of persistent storage memory for both application code and data.	Mandatory
"81"	Amount of reserved volatile memory at the time of application selection for the application's data.	Optional
"82"	Amount of reserved persistent storage memory for the application's data. If "82" is not present, then "80" indicates the sum of persistent storage memory for both application code and data.	Optional
"83"	Amount of memory quota of persistent storage memory for the application's code. If no separation between code and data is requested, then "83" shall be used to indicate the memory quota of persistent storage memory for both application code and data.	Optional
"84"	Amount of memory quota of volatile memory at the time of application selection for the application's data.	Optional
"85"	Amount of memory quota of persistent storage for the application's data. If "85" is not present, then "83" indicates the sum of persistent storage memory for both application code and data.	Optional
— In this context, ISO/IEC JTC1/SC17 reserves any other data object of the context-specific class (first byte from "80" to "BF").		

In using the values of the memory resource assignment data objects, the following rules shall apply.

— The assignment of Reserved Memory to an application reduces the memory resources available to other applications on the card.

— The assignment of Memory Quota to an application does not reduce the memory resources available to other applications on the card.

— The value of Memory Quota is greater than or equal to the value of Reserved Memory.

— At the time of the successful creation of an application (e.g. transition from Non Existent to Operational Activated state), the amount of memory assigned to that application is first charged against the Reserved Memory assigned to that application until it is entirely exhausted. When the application's Reserved Memory is exhausted, the amount of assigned memory reduces the memory resources available to other applications on the card as long as it does not exceed the Memory Quota of that application. When either the Memory Quota is exceeded or the memory resources currently available on the card are exhausted, the creation of the application fails.

— At the time of successful removal of an application (i.e. transition to Application Removed), the memory resources available to other applications on the card are augmented by the amount of memory actually released, and any unused part of the Reserved Memory is reassigned to the memory resources available to other applications on the card.

6 Card management service recognition

6.1 Card management service template

The card management service template (tag"7F64") shall be present. Table 3 defines the contents of the card management service template.

Table 3 — Card management service data objects

Tag	Length/ Format	Description	Requirement
"80"	2 bytes	Card management capabilities supported by the card: the value is a combination of the bits defined in Table 4 and Table 5.	Mandatory
"81"	Variable	Card management scheme name and version: Object Identifier value (see ISO/IEC 8825-1) indicating the scheme name and version (major and minor) used to manage the card and its applications.	Mandatory
"82"	Variable	Card identification procedure indicator: Object Identifier value (see ISO/IEC 8825-1) indicating the procedure used to identify the card uniquely. It defines how to access the local identifier on the card e.g. the ICC serial number, and whether that identifier is globally unique.	Optional
"4F"	Variable	Card manager application AID: Application identifier to select the card manager application, when different from "E8 28 BD 08 0D".	Optional
— In this context, ISO/IEC JTC 1/SC 17 reserves any other data object of the context-specific class (first byte from "80" to "BF").			