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

Reference number
ISO/IEC 7816-13:2007(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.org
Web www.iso.org

Published in Switzerland

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

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

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.

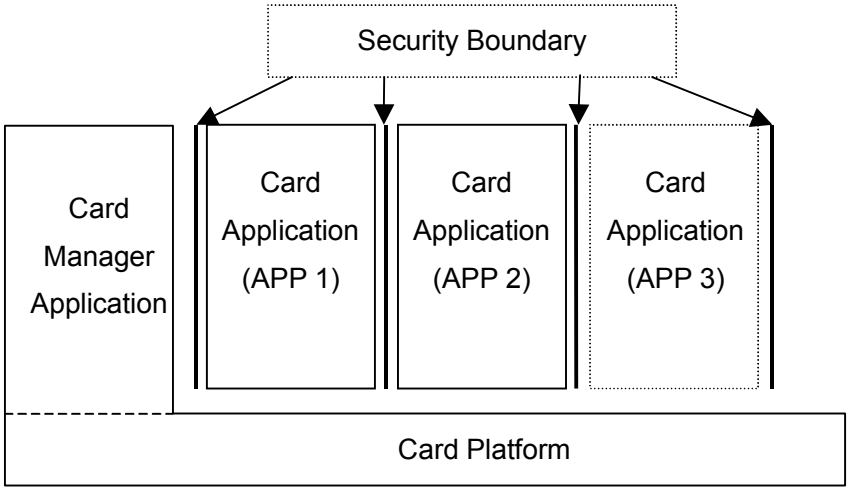

Figure 1 — Possible structure of a multi-application card

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.

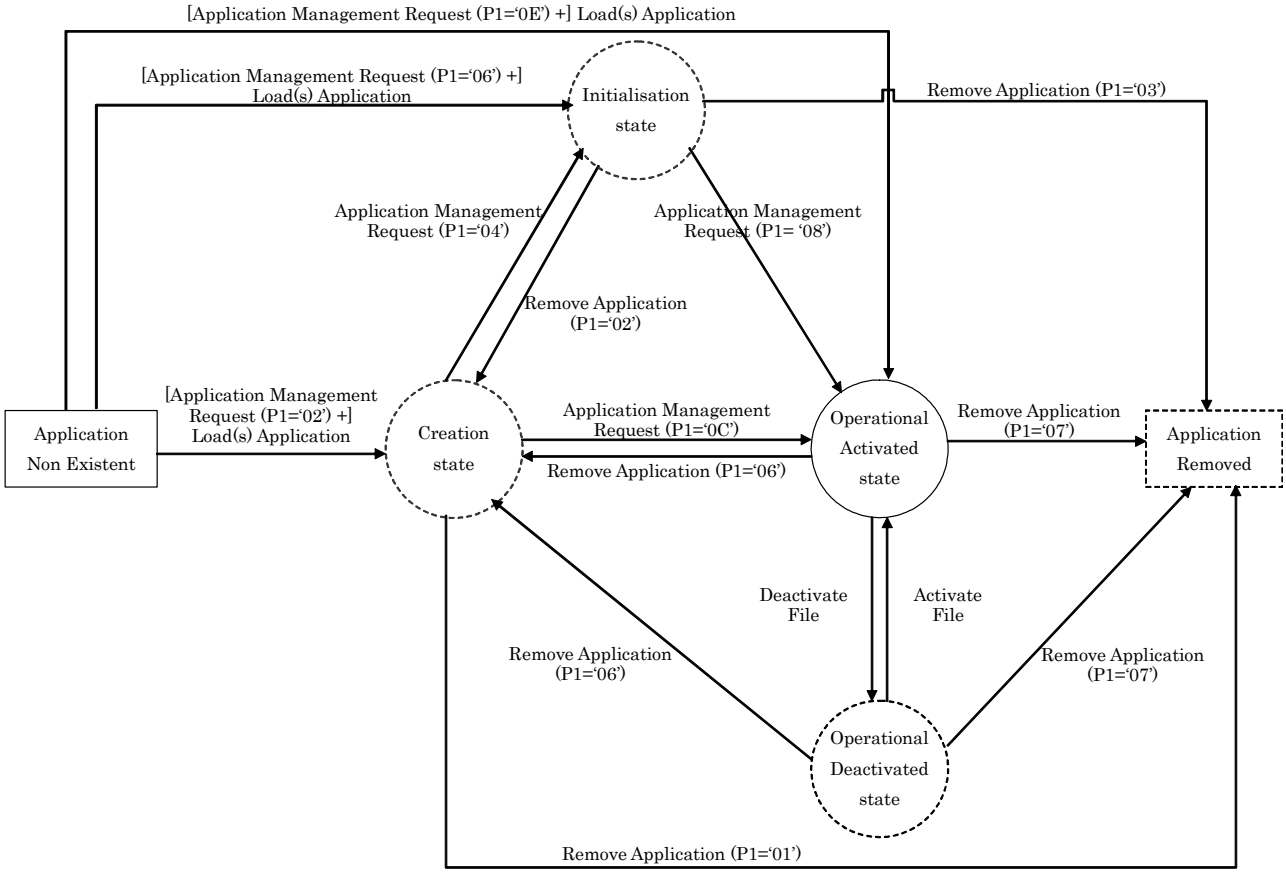

Figure 2 — Application life cycle diagram

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”).			

Table 4 — Card management capabilities: First byte

b8	b7	b6	b5	b4	b3	b2	b1	Value of supported life cycle state transitions
-	-	-	-	-	-	-	1	Non Existent to Creation
-	-	-	-	-	-	1	-	Creation to Initialisation
-	-	-	-	-	1	-	-	Initialisation to Operational Activated
-	-	-	-	1	-	-	-	Creation to Operational Activated
-	-	-	1	-	-	-	-	Non Existent to Operational Activated
-	-	1	-	-	-	-	-	Operational Activated to Operational Deactivated
-	1	-	-	-	-	-	-	Operational Deactivated to Operational Activated
1	-	-	-	-	-	-	-	Operational Activated to Application Removed

Table 5 — Card management capabilities: Second byte

b8	b7	b6	b5	b4	b3	b2	b1	Value of Supported life cycle state transitions
0	0	0	-	-	-	-	1	Creation to Application Removed
0	0	0	-	-	-	1	-	Initialisation to Application Removed
0	0	0	-	-	1	-	-	Initialisation to Creation
0	0	0	-	1	-	-	-	Operational Activated to Creation
0	0	0	1	-	-	-	-	Operational Deactivated to Application Removed
— Any other value is reserved for future use by ISO/IEC JTC 1/SC 17.								

6.2 Card management service template retrieval

Retrieving the card management service template uses the application-independent card services defined by ISO/IEC 7816-4.

The order in which the different retrieval procedures defined in this clause are to be tried is not defined by this document. If all procedures described hereafter fail to return the card management service template, the card does not comply with this document.

Two procedures may apply to retrieve card management service template when the MF or the implicitly selected application DF is selected:

— reading the EF.ATR, where DO “7F64” may be present;

— with a GET DATA command with P1-P2 set to “7F 64”, which may return the card management service template in the response data field.

Another procedure may apply and consists of selecting the application with AID “E8 28 BD 08 0D” followed by a GET DATA command with P1-P2 set to “7F 64”, which may return the card management service template in the response data field.

7 Commands for application management

After selection of the card manager application and optional authentication procedure, a management procedure for an application on the card results from the use of one or more of the following three commands:

— APPLICATION MANAGEMENT REQUEST command;

— LOAD APPLICATION command;

— REMOVE APPLICATION command.

The card manager application shall support at least the first two commands.

If the card manager application supports a command specified in this clause, at least one option of the command shall be supported.

A command for application management can be performed only if the security status satisfies the security conditions defined by the card manager application.

7.1 APPLICATION MANAGEMENT REQUEST command

The APPLICATION MANAGEMENT REQUEST command initiates the management procedure for an application. The card manager application verifies the application management request information present in the command data field. This command may be followed by the LOAD APPLICATION command described in 7.2. If memory resource management is supported, the assignment of memory resources to an application as described in the memory resource assignment template (tag “7F65”) shall comply with the rules defined in clause 5.3.

Table 6 — APPLICATION MANAGEMENT REQUEST command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	“40” or “41”
P1	Application life cycle status control according to Table 7
P2	Application management control according to Table 8
L_c field	Number of bytes in the command data field
Data field	Application management request information whose format and contents are implicitly known by the card manager application (INS=“40”), or coded in the following data objects (INS=“41”): AID (tag “4F”) of the target application (mandatory); Memory resource assignment (tag “7F65”); One or more digital signature block(s) (tag “7F3D”) containing a digital signature DO (tag “9E”) and possibly further DOs, e.g. a hash value DO (tag “90”) with the application's code hash;
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$

Data field	Additional information or absent
SW1-SW2	See ISO/IEC 7816-4:2005, Tables 6 and 7 where relevant, e.g. “6982”, “6985”
— Application management request information may contain other data objects, e.g. issuer identification number (tag “42”), file reference (tag “51”), or discretionary data (tag “53” or “73”). — Coding of the digital signature block (tag “7F3D”) is outside the scope of this document.	

Table 7 — Application life cycle target state control in P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	No information given
0	0	0	0	0	0	1	0	Transition from Non Existent state to Creation state
0	0	0	0	0	1	0	0	Transition from Creation state to Initialisation state
0	0	0	0	0	1	1	0	Transition from Non Existent state to Initialisation state
0	0	0	0	1	0	0	0	Transition from Initialisation state to Operational Activated state
0	0	0	0	1	1	0	0	Transition from Creation state to Operational Activated state
0	0	0	0	1	1	1	0	Transition from Non Existent to Operational Activated state
— Any other value is reserved for future use by ISO/IEC JTC 1/SC 17.								

Table 8 — Application management control in P2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	No information given
0	0	0	0	0	0	0	1	Verify application management request
0	0	0	0	0	0	1	0	Commit application management request
0	0	0	0	0	0	1	1	Verify and commit application management request
— Any other value is reserved for future use by ISO/IEC JTC 1/SC 17.								

7.2 LOAD APPLICATION command

The LOAD APPLICATION command transfers an application to the card. An application may be partitioned into multiple components and each component may be partitioned into multiple blocks for transmission to the card. Each LOAD APPLICATION command transfers one block to the card. This command may be preceded by the APPLICATION MANAGEMENT REQUEST command, see 7.1.

If the LOAD APPLICATION command is preceded by an APPLICATION MANAGEMENT REQUEST command, then memory resource assignment is achieved by the immediately preceding APPLICATION MANAGEMENT REQUEST command. The successful execution of this sequence of commands performs the life cycle transition indicated in the immediately preceding APPLICATION MANAGEMENT REQUEST.

If the LOAD APPLICATION command is not preceded by an APPLICATION MANAGEMENT REQUEST command, then memory resource assignment and setting of the application life cycle state to an appropriate value is done on the basis of information provided by the sequence of LOAD APPLICATION commands.

If memory resource management is supported, the amount of memory assigned to a successfully created application shall comply with the rules defined in 5.3.

Table 9 — LOAD APPLICATION command-response pair

CLA INS P1-P2	As defined in ISO/IEC 7816-4 “EA” or “EB” See Table 10
L_c field	Number of bytes in the command data field
Data field	Application components whose format and contents are implicitly known by the card manager application (INS=“EA”), or coded as individual data objects (INS=“EB”)
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$

Data field	Additional information or absent
SW1-SW2	See ISO/IEC 7816-4:2005, Tables 6 and 7 where relevant, e.g. “6982”, “6985”

Table 10 — Sequence number or offset in P1 and P2

P1								P2	Meaning
b8	b7	b6	b5	b4	b3	b2	b1		
0	0	0	0	0	0	0	0	00	No information given
-	X	X	X	X	X	X	X	XX	Sequence number or offset
-	0	X	X	X	X	X	X	XX	- Offset
-	1	X	X	X	X	X	X	XX	- Sequence number
0	-	-	-	-	-	-	-	-	More block
1	-	-	-	-	-	-	-	-	Last block

— If b7 of P1 is set to 0, then the rest of P1-P2 (fourteen bits) encodes an offset from zero to 16383, and if b7 of P1 is set to 1, then the rest of P1-P2 (fourteen bits) encodes a sequence number of the command.

— If b8 of P1 is set to 0, then a subsequent block is expected, and if b8 of P1 is set to 1, then this command contains the last block.

— The offset is counted in bytes from the beginning of the application transfer.

— The sequence number is incremented by one for each block from the beginning of the application transfer.

7.3 REMOVE APPLICATION command

The REMOVE APPLICATION command deletes an application and possibly reclaims the memory resources that were assigned to the application.

The card manager application verifies the application removing information, when present in the command data field.

If memory resource management is supported, the successful removal of an application shall augment the memory resources available to applications on the card according to the rules defined in 5.3.

Table 11 — REMOVE APPLICATION command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	“EC” or “ED”
P1	Removing state control according to Table 12
P2	“00” no information given. (any other value is reserved for future use by ISO/IEC JTC 1/SC 17)
L_c field	Absent or number of bytes in the command data field
Data field	Absent or application removing information whose format and contents are implicitly known by the card manager application (INS=“EC”) Or application removing information coded in the following data objects (INS=“ED”): AID (tag “4F”) of the target application (mandatory); One or more digital signature block(s) (tag “7F3D”) containing a digital signature DO (tag “9E”).
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$

Data field	Additional information or absent
SW1-SW2	See ISO/IEC 7816-4:2005, Tables 6 and 7 where relevant, e.g. “6982”, “6985”

— Application removing information may contain other data objects, e.g. discretionary data (tag “53” or “73”).

— Coding of the digital signature block (tag “7F3D”) is outside the scope of this document.

Table 12 — Removing state control in P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	No information given
0	0	0	0	0	0	0	1	Transition from Creation state to Application Removed
0	0	0	0	0	0	1	0	Transition from Initialisation state to Creation state
0	0	0	0	0	0	1	1	Transition from Initialisation state to Application Removed
0	0	0	0	0	1	1	0	Transition from Operational (Activated or Deactivated) state to Creation state
0	0	0	0	0	1	1	1	Transition from Operational (Activated or Deactivated) state to Application Removed
— Any other value is reserved for future use by ISO/IEC JTC 1/SC 17.								

7.4 Application management considerations

The card management scheme and/or the card issuer policies specify the type and number of signatures being required, such as

— card issuer's signature,

— application provider's signature,

— card management scheme authority's signature.

The card shall be capable of enforcing those policies and handling the corresponding signature verification keys.

An application management policy between a card issuer and an application provider, and its implementation are outside the scope of this document.

Annex A
(informative)

An example of card application management on an independent card issuer and application provider model

A.1 Introduction

This example shows how to manage an application in the card under an independent card issuer and application provider model. The following assumptions are made.

— An application may be added to the card by an independent application provider after the issuance of the card. The model is shown in Fig. A.1.

— The application creation certificate may be issued during online or offline communication.

NOTE The next generation IC Card System Study Group (NICSS) uses this model.

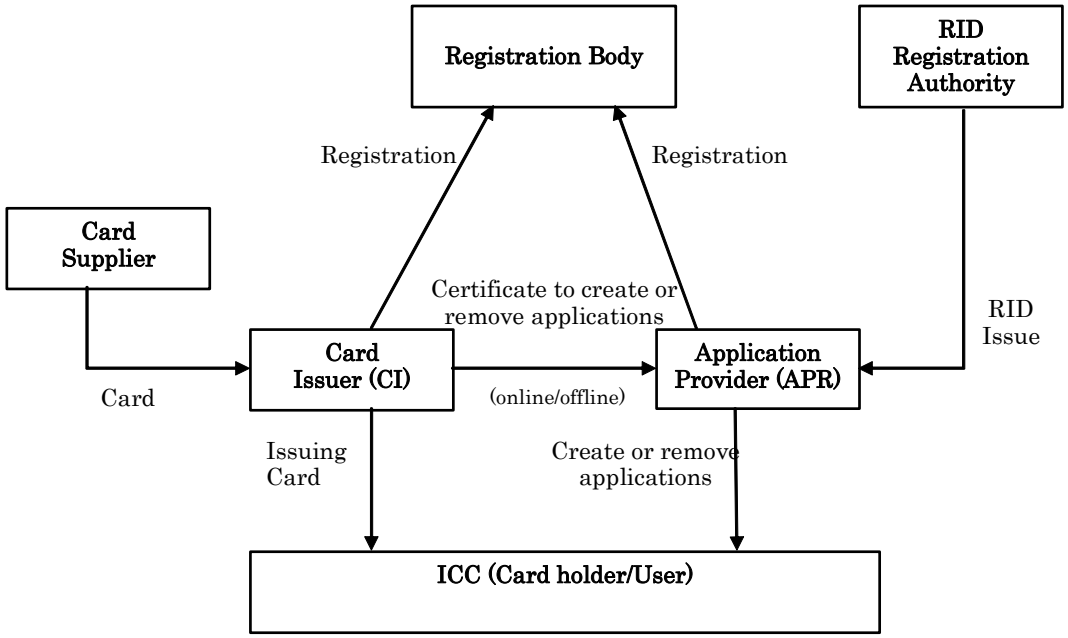

Figure A.1 — A model of independent card issuer and application provider

A.2 Examples of application management procedures

A.2.1 Case of APR independent from CI (remote CI): verify certificate before loading

a) SELECT the application with AID “E8 28 BD 08 0D”.

b) GET DATA to retrieve the card management service template (tag “7F64”).

c) SELECT the card manager application with the AID (tag “4F”) indicated in the card management service template.

d) Mutual authentication.

e) Get an application creation certificate from the card issuer (online/offline). The certificate may contain AID, a hash value of the application, approval ID, Card ID, and digital signature of the card issuer.

f) APPLICATION MANAGEMENT REQUEST with the certificate.

g) Load the application by LOAD APPLICATION.

A.2.2 Case of remote CI: verify certificate after loading

a) SELECT the application with AID “E8 28 BD 08 0D”.

b) GET DATA to retrieve the card management service template (tag “7F64”).

c) SELECT the card manager application with the AID (tag “4F”) indicated in the card management service template.

d) Mutual authentication.

e) Get an application creation certificate from the card issuer.

f) APPLICATION MANAGEMENT REQUEST with no certificate to assign memory.

g) Load the application by LOAD APPLICATION.

h) APPLICATION MANAGEMENT REQUEST with the certificate.

A.3 Examples of removal procedures

A.3.1 Case of remote CI: verify certificate during removing

a) SELECT the application with AID “E8 28 BD 08 0D”.

b) GET DATA to retrieve the card management service template (tag “7F64”).

c) SELECT the card manager application with the AID (tag “4F”) indicated in the card management service template.

d) Mutual authentication.

e) Get an application removal certificate from the card issuer (online/offline). The certificate may contain AID, approval ID, Card ID, and digital signature of the card issuer.

f) REMOVE APPLICATION with the certificate.

A.3.2 Case of remote CI: verify certificate before removing

a) SELECT the application with AID “E8 28 BD 08 0D”.

b) GET DATA to retrieve the card management service template (tag “7F64”).

c) SELECT the card manager application with the AID (tag “4F”) indicated in the card management service template.

d) Mutual authentication.

e) Get an application removal certificate from the card issuer.

f) APPLICATION MANAGEMENT REQUEST with the certificate.

g) REMOVE APPLICATION with no certificate.

Annex B
(informative)

A practical example of card application management

B.1 Introduction

This example shows a two-step model for application creation and activation: load the application's code first, then install and activate an application instance.

NOTE GlobalPlatform (GP) uses this model.

An application is composed of application code and application data. Application code (but not application data) is loaded on the card using a Load Object. The installation of an application creates an instance from the Load Object plus possibly some application data.

In this example, the creation and activation of an application additionally requires

— previous authentication of the Card Application Management System (CAMS),

— protection of commands and responses by secure messaging,

— verification of the card issuer's certificates.

B.2 Commands for application management

B.2.1 APPLICATION MANAGEMENT REQUEST command

The APPLICATION MANAGEMENT REQUEST command is issued to initiate and perform the various steps required for loading a Load Object and installing and activating an application instance.

Table B.1 — APPLICATION MANAGEMENT REQUEST command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	“40”
P1	Application life cycle target state control: see Table B.2
P2	Application management control: see Table B.3
L_c field	Number of bytes in the command data field
Data field	Application management request information
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$

Data field	Absent or application management confirmation information
SW1-SW2	See ISO/IEC 7816-4:2005, Tables 6 and 7 where relevant, e.g. “6982”, “6985”

The parameter P1 of the APPLICATION MANAGEMENT REQUEST command describes the purpose of the command and is coded according to Table B.2.

Table B.2 — Application life cycle target state control in P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	1	1	0	0	Transition from Creation state to Operational Activated state
0	0	0	0	1	0	0	0	Transition from Initialisation state to Operational Activated state
0	0	0	0	0	1	0	0	Transition from Creation state to Initialisation state
0	0	0	0	0	0	1	0	Transition from Non Existent state to Creation state
X	X	X	X	-	-	-	-	RFU

b4 = 1 indicates the activation of the application identified in the command data field. This applies to an application that is only created (current life cycle state = Creation) or that is already initialised (current life cycle state = Initialisation).

b3 = 1 indicates the initialisation of the application identified in the command data field (current life cycle state = Creation).

b2 = 1 indicates the creation of the application identified in the command data field (current life cycle state = Non Existent).

Table B.3 — Application management control in P2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	1	Verify application management request
0	0	0	0	0	0	1	1	Verify and commit application management request

In this example, the APPLICATION MANAGEMENT REQUEST command is issued twice.

— With b2=1 in parameter P1 and P2 set to “01”, to initiate the load of the application's code (Load Object). The command data field contains the identity of the Load Object, the identity of the application provider, memory resource assignment information on the Load Object, the hash of the Load Object and an application creation certificate issued by the card issuer. No response data field is returned in the response message. One or more LOAD APPLICATION commands follow. On the successful execution of the last LOAD APPLICATION command, the creation application management request is implicitly committed and the application life cycle status is set to Creation.

— With a combination of b4=1 and b3=1 in parameter P1 and P2 set to “03”, to simultaneously install and activate an application instance. The command data field contains the identity of the Load Object already loaded, the identity of the application instance, memory resource assigment information on the application instance and an application initialisation-and-activation certificate issued by the card issuer. On the successful execution of the command, the application life cycle status is changed from Creation to Operational Activated. A response data field may be returned in the response message. When present, the content of the response data field contains the length (coded according to the ASN.1 rules defined in ISO/IEC 8825-1) and the value of the application initialisation-and-activation confirmation.

B.2.2 LOAD APPLICATION command

The Load Object is divided into multiple blocks: Load Blocks, for transmission to the card. The LOAD APPLICATION command initiates the transfer of a Load Block to the card. Multiple LOAD APPLICATION commands may be required to transfer a Load Object to the card.

Table B.4 — LOAD APPLICATION command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	"EA"
P1	Load Block sequence number most significant byte, see Table B.5
P2	Load Block sequence number least significant byte, see Table B.6
L_c field	Number of bytes in the command data field
Data field	Load Block
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$

Data field	Absent or application creation confirmation information
SW1-SW2	See ISO/IEC 7816-4:2005, Tables 6 and 7 where relevant, e.g. "6581", "6484"

The parameters P1 and P2 of the LOAD APPLICATION command describes the sequence of Load Blocks and are coded according to Tables B.5 and B.6.

Table B.5 — Sequence number most significant byte in P1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	1	X	X	X	X	X	X	More blocks, sequence number most significant byte
1	1	X	X	X	X	X	X	Last block, sequence number most significant byte

b8 = 0 indicates that more Load Blocks are expected.

b8 = 1 indicates the last Load Block in a sequence.

b7 = 1 indicates a Load Block sequence number coded on fourteen bits, from 0 to16 383.

Table B.6 — Sequence number least significant byte in P2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	X	X	X	X	X	X	Sequence number least significant byte

The first LOAD APPLICATION command is preceded by an APPLICATION MANAGEMENT REQUEST for creation command (b2 of P1 set to 1).

The Load Block sequence number (lower fourteen bits of P1-P2) starts at zero. The Load Block numbering is strictly sequential and increments by one. The card is informed of the last block of the Load Object (b8 of P1 of LOAD APPLICATION command set to 1).

A response data field may be returned in the response message. When present, the content of the response data field contains the length (coded according to the ASN.1 rules defined in ISO/IEC 8825-1) and the value of the application creation confirmation. It is only present in the response data field of the LOAD APPLICATION command transferring the last Load Block (b8 of P1 set to 1).

For LOAD APPLICATION commands other than the last LOAD APPLICATION command transferring the last Load Block (b8 of P1 set to 1), there is no response data field.

B.3 Application management sequence

The typical application management sequence for creating and activating an application in this model is as follows.

a) SELECT the application with AID “E8 28 BD 08 0D”.

b) GET DATA to retrieve the card management service template (tag “7F64”).

c) SELECT the card manager application with the AID (tag “4F”) indicated in the card management service template.

d) APPLICATION MANAGEMENT REQUEST for creation with P1=“02” and P2=“01”.

e) First LOAD APPLICATION with P1=“40” and P2=“00”.

f) Multiple LOAD APPLICATION commands with sequentially incremented P1-P2.

g) Last LOAD APPLICATION with P1=“Cx” and P2=“yz” where “xyz” is the sequence number of the last Load Block (assuming “xyz” is lower than 4 095).

h) APPLICATION MANAGEMENT REQUEST for initialisation and activation with P1=“0C” and P2=“03”.

Annex C
(informative)

A further practical example of card application management

C.1 Introduction

This example shows the three-step model for application creation and activation: assign card resources, load application code and data, and make operational activated.

NOTE MULTOS uses this model.

An initial APPLICATION MANAGEMENT REQUEST command ensures card resources are available and readies the card for subsequent card content management requests. The application is then loaded to the card with the LOAD APPLICATION command. An application is composed of application code and application data, default file control information, directory file entry, digital signature and Key Transformation Unit. All are loaded onto the card as an Application Load Unit. The second and final APPLICATION MANAGEMENT REQUEST command finalises the application creation and activation process, including checking Card Issuer authorisations and the Application Service Provider's digital signature of the Application Load Unit.

C.2 Commands for application management

C.2.1 APPLICATION MANAGEMENT REQUEST command

The APPLICATION MANAGEMENT REQUEST command is issued to initiate and finalise the application loading process

Table C.1 — APPLICATION MANAGEMENT REQUEST command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	“40”
P1	Purpose of the APPLICATION MANAGEMENT REQUEST: see Table C.2
P2	Purpose of the APPLICATION MANAGEMENT REQUEST: see Table C.3
L_c field	Number of bytes in the command data field
Data field	Application Load Certificate
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$

Data field	Absent or Card Public Key Certificate
SW1-SW2	See ISO/IEC 7816-4:2005, Tables 6 and 7 where relevant, e.g. “6982”, “6985”

The parameter P1 of the APPLICATION MANAGEMENT REQUEST command describes the purpose of the command and is coded according to Table C.2.

Table C.2 — Coding of P1 of APPLICATION MANAGEMENT REQUEST command

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	1	1	1	0	Transition from Non Existent state to Operational Activated state

The parameter P2 of the APPLICATION MANAGEMENT REQUEST command describes the purpose of the command and is coded according to Table C.2.

Table C.3 — Coding of P2 of APPLICATION MANAGEMENT REQUEST command

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	1	Verify application management request
0	0	0	0	0	0	1	1	Verify and commit application management request

C.2.2 LOAD APPLICATION command

The Application Load Unit is divided into smaller Components for transmission to the card. The LOAD APPLICATION command initiates the transfer of the Component to the card. Multiple LOAD APPLICATION commands may be used to transfer an Application Load Unit to the card.

Table C.4 — LOAD APPLICATION command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	"EA"
P1	Load Block sequence number most significant byte, see Table C.5
P2	Load Block sequence number least significant byte, see Table C.6
L_c field	Number of bytes in the command data field
Data field	Load Block
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4:2005, Tables 6 and 7 where relevant, e.g. "6581", "6484"

The parameters P1 and P2 of the LOAD APPLICATION command describe the sequence number of Components and are encoded according to Tables C.5 and C.6.

Table C.5 — Coding of P1 of LOAD APPLICATION command

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	1	X	X	X	X	X	X	More blocks, sequence number most significant byte
1	1	X	X	X	X	X	X	Last block, sequence number most significant byte

b8 = 0 indicates more Load Blocks are expected.

b8 = 1 indicates the last Load Block in a sequence.

b7 = 1 indicates a Load Block sequence number coded on fourteen bits, from 0 to 16 383.

Table C.6 — Coding of P2 of LOAD APPLICATION command

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
X	X	X	X	X	X	X	X	Sequence number least significant byte

The first LOAD APPLICATION command is preceded by an APPLICATION MANAGEMENT REQUEST command.

The Load Block sequence number (lower fourteen bits of P1-P2) starts at zero. The Load Block numbering is strictly sequential and increments by one. The card is informed of the last block of the Load Object (b8 of P1 set to 1).

C.3 Application management sequence

The typical application management sequence for creating and activating an application of this model is as follows.

a) SELECT the application with AID “E8 28 BD 08 0D”.

b) GET DATA to retrieve the card management service template (tag “7F64”).

c) SELECT Card Manager Application.

d) APPLICATION MANAGEMENT REQUEST for operational activation request verification with P1 = “0E” and P2 = “01”.

e) First LOAD APPLICATION with P1 = “40” and P2 = “00”.

f) Multiple LOAD APPLICATION commands with sequentially incremented P1-P2.

g) Last LOAD APPLICATION with P1 = “Cx” and P2 = “yz” where “xyz” is the sequence number of the last Load Block.

h) APPLICATION MANAGEMENT REQUEST for operational activation with P1 = “0E” and P2=“03”.

Annex D
(informative)

A further practical example of card application management

The following example shows the usage of the LOAD APPLICATION command as a wrapper of commands for application installation. It allows to control the whole load sequence by a single access rule for the LOAD APPLICATION command, e.g. external authentication with Secure Messaging key agreement required. Such an authentication procedure may be performed by a Card Application Management System (CAMS).

NOTE 1 The command sequence may be sent with secure messaging.

NOTE 2 The command-to-perform in the command data field is coded without secure messaging.

Table D.1 — LOAD APPLICATION command-response pair

CLA	As defined in ISO/IEC 7816-4, bit 5 set to 1 indicates that the command is not the last command of the chain
INS	“EB”
P1-P2	“0000”
L_c field	Number of bytes in the command data field
Data field	Command-to-perform (Tag “52”): “52”-L-.... (CREATE FILE (DF) command)
L_e field	Absent

Data field	Absent
SW1-SW2	“9000” or specific status bytes

Table D.2 — LOAD APPLICATION command-response pair

CLA	As defined in ISO/IEC 7816-4, bit 5 set to 1 indicates that the command is not the last command of the chain
INS	“EB”
P1-P2	“0000”
L_c field	Number of bytes in the command data field
Data field	Command-to-perform (Tag “52”): “52”-L-.... (CREATE FILE (EF) command)
L_e field	Absent

Data field	Absent
SW1-SW2	“9000” or specific status bytes

Table D.3 — LOAD APPLICATION command-response pair

CLA	As defined in ISO/IEC 7816-4, bit 5 set to 1 indicates that the command is not the last command of the chain
INS	“EB”
P1-P2	“0000”
L_c field	Number of bytes in the command data field
Data field	Command-to-perform (Tag “52”): “52”-L-.... (UPDATE BINARY command)
L_e field	Absent

Data field	Absent
SW1-SW2	“9000” or specific status bytes

etc.

Table D.4 — LOAD APPLICATION command-response pair

CLA	As defined in ISO/IEC 7816-4, bit 5 set to 0 indicates that the command is the last command of the chain
INS	“EB”
P1-P2	“0000”
L_c field	Number of bytes in the command data field
Data field	Command-to-perform (Tag “52”): “52”-L-.... (ACTIVATE FILE (DF) command)
L_e field	Absent

Data field	Absent
SW1-SW2	“9000” or specific status bytes

Bibliography

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

[2] GlobalPlatform Card specification V2.1.1 or higher, http://www.globalplatform.org/

[3] NICSS Prerequisites Version 1.20, The Next generation IC Card System Study group, April 24,2001, http://www.nicss.or.jp/

[4] Guide to Loading and Deleting Applications, MAO-DOC-REF-008, MAOSCO, http://www.multos.com/

[5] Guide to Generating Application Load Units, MAO-DOC-REF-009, MAOSCO, http://www.multos.com/

ICS 35.240.15

Price based on 23 pages