INTERNATIONAL STANDARD

ISO/IEC 24727-3

First edition
2008-12-01

Identification cards — Integrated circuit card programming interfaces —

Part 3: Application interface

Cartes d'identification — Interfaces programmables de cartes à puce —

Partie 3: Interface d'application

Reference number
ISO/IEC 24727-3:2008(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 joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this 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 24727-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

ISO/IEC 24727 consists of the following parts, under the general title *Identification cards — Integrated circuit card programming interfaces*:

— *Part 1: Architecture*

— *Part 2: Generic card interface*

— *Part 3: Application interface*

— *Part 4: Application programming interface (API) administration*

— *Part 5: Testing*

— *Part 6: Registration authority procedures for the authentication protocols for interoperability*

Introduction

ISO/IEC 24727 is a set of programming interfaces for interactions between integrated circuit cards (ICCs) and external applications to include generic services for multi-sector use. The organization and the operation of the ICC conform to ISO/IEC 7816-4.

ISO/IEC 24727 is relevant to ICC applications desiring interoperability among diverse application domains. This part of ISO/IEC 24727 specifies a language-independent and implementation-independent application level interface that allows information and transaction interchange with a card. ISO/IEC 7498-1 is used as the layered architecture of the application interface. That is, the application interface assumes that there is a protocol stack through which it will exchange information and transactions among cards using commands conveyed through the message structures defined in ISO/IEC 7816. The semantics of commands accessed by the application interface refers to application protocol data units (APDUs) as characterized in ISO/IEC 24727-2, and in the following standards:

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

— ISO/IEC 7816-8, *Identification cards — Integrated circuit cards — Part 8: Commands for security operations*

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

The goal of this part of ISO/IEC 24727 is to maximize the applicability and solution space of software tools that provide application interface support to card-aware applications. This effort includes supporting the evolution of card systems as the cards become more powerful, peer-level partners with existing and future applications while minimizing the impact to existing solutions conforming to this part of ISO/IEC 24727.

Identification cards — Integrated circuit card programming interfaces —

Part 3: Application interface

1 Scope

This part of ISO/IEC 24727 defines services as representations of action requests and action responses to be supported at the client-application service interface. The services are described in a programming-language-independent way.

This part of ISO/IEC 24727 is the application interface of the Open Systems Interconnection Reference Model defined in ISO/IEC 7498-1. It provides a high-level interface for a client-application making use of information storage and processing operations of a card-application as viewed on the generic card interface.

This part of ISO/IEC 24727 does not mandate a specific implementation methodology for this interface.

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 7816-11, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 24727-1, *Identification cards — Integrated circuit card programming interfaces — Part 1: Architecture*

ISO/IEC 24727-2, *Identification cards — Integrated circuit card programming interfaces — Part 2: Generic card interface*

IETF RFC 2141, *URN Syntax,* May 1997

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 24727-1, ISO/IEC 24727-2 and the following apply.

3.1
access control list
set of access rules

3.2
access permission
granted capability to perform an action

3.3
access rule
association of an action and a security condition in the context of a card-application

3.4
action
operation that a client-application can request of a card-application at the ISO/IEC 24727-3 application interface

3.5
alpha card-application
administrative card-application, specific to ISO/IEC 24727, providing card and application discoverability and administrative services

3.6
card-application-path
ordered set of protocol termination points in the network that connects the client-application to the card-application

3.7
card-application-service
set of actions

3.8
channel
physical pathway allowing movement of bits of information between a client-application and a card-application

3.9
client-application
software component running on a platform that uses data storage and computational services offered by a card-application

3.10
connection
logically referenced channel

3.11
global differential-identity
differential-identity recognized in all card-applications that are managed by the same alpha card-application

3.12
local differential-identity
differential-identity recognized only within a specific card-application in which it is defined

3.13
parameter
information required to define or effect an action

3.14
return code
information, including status, returned as a consequence of an action

3.15
security condition
boolean expression in terms of differential-identity authentication states

3.16
session
connection used under a particular security context

3.17
target
persistent entity that shall be manipulated through the actions of a card-application-service

4 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 24727-1 and the following apply.

ACL	access control list
AR	access rule
DID	differential-identity
DSI	data structure for interoperability

5 Organization for interoperability

5.1 General

A client-application and a card-application comprise two peer-level entities that interact through well-defined transaction and communication mechanisms. The ISO/IEC 24727-3 application interface shall be the sole mechanism through which a client-application interacts with a card-application.

This clause defines the model of computation and persistent entities on the ISO/IEC 24727-3 application interface by which the client-application and the card-application interact. A security model governs the security mechanisms through which trust in this interaction is achieved.

Clause 5.2 introduces the conceptual entities on the ISO/IEC 24727-3 application interface and describes their operational behavior and relationships. Clause 5.3 specifies the entities and relationships presented on the ISO/IEC 24727-3 application interface. Clause 5.4 specifies the security model provided on the ISO/IEC 24727-3 application interface.

5.2 Computation model

Using the terminology defined in ISO/IEC 24727-1:

5.2.1 A *client-application* may know a *card-application-path* to a *card-application.* Using this card-application-path, a client-application can initiate a *connection* to a card-application. The card-application shall be known as the *current card-application* for the connection.

5.2.2 The ISO/IEC 24727-3 *application interface* is the set of *card-application-services* provided to the client-application. Each card-application-service shall be comprised of *actions* that may be *requested* by a client-application and *confirmations* returned by the SAL.

5.2.3 If the client-application does not know a card-application-path to a card-application, it may make a request at the ISO/IEC 24727-3 application interface to discover a card-application-path to the requested card-application.

5.2.4 A card-application shall be uniquely identified by an AID.

5.2.5 The *alpha card-application* provides the basis for trusted management of card-applications by the client-application.

5.2.6 A client-application may open more than one connection. A client-application may open more than one connection with the same card-application, each connection being referenced by a different *connection handle*.

5.2.7 Using an open connection, a client-application may initiate a *session* with a card-application.

5.2.8 A client-application may open more than one session. Only one session may be open within a connection.

5.2.9 The *current state* is the current state of a connection defined by the current card-application, current data-set, authentication state of recognized differential-identities, and the presence of a session on the connection.

5.2.10 A card-application contains one or more card-application-services.

5.2.11 A specific card-application-service, the *Named Data Service*, provides access to zero or more *data-sets*.

5.2.12 A data-set contains zero or more *data structures for interoperability* (DSI). A data-set shall provide naming scope and access rules for the DSIs it contains.

5.2.13 Every data-set shall be accessible according to the *access rules* governing the actions available from the *Named Data Service*.

5.2.14 The currently selected data-set in a card-application shall be known as the *current data-set*.

5.2.15 A single *action request* at the ISO/IEC 24727-3 application interface may translate into multiple generic requests at the ISO/IEC 24727-2 generic card interface.

5.2.16 A card-application may support multiple actions that may be requested by the client-application through the ISO/IEC 24727-3 application interface.

5.2.17 An action request shall produce an *action confirmation*.

5.2.18 An *access rule* consists of the name of an action and a *security condition*. The security condition is said to be associated with the action by the access rule.

5.2.19 An *access control list* is a collection of zero or more access rules. An access control list shall be associated with each *target*.

5.2.20 An action involving a target may be successfully performed if and only if the security condition associated with the action by an access rule in the access control list of the target evaluates to TRUE.

5.2.21 An *authentication protocol* is the process by which a *differential-identity* demonstrates possession of a *marker*.

5.2.22 *Authentication* is the successful execution of an authentication protocol. In this case the differential-identity is said to be authenticated.

5.2.23 The *authentication state* of a differential-identity shall be a boolean variable that is TRUE if the differential-identity is authenticated and FALSE otherwise.

5.2.24 A client-application may learn about information, status or services provided by a card-application through a discovery process effected through the various List, Get, and Describe actions offered at the 24727-3 application interface.

5.2.25 Access rules are discoverable at the ISO/IEC 24727-3 application interface.

5.2.26 In general, the degree of interoperability of a card-application with client-applications depends on the discoverable information presented by the card-application at the ISO/IEC 24727-3 application interface.

5.3 Entity relationships on the application interface

5.3.1 General

This clause describes the entities accessible through a card-application, specifically the alpha card-application and card-applications it manages. Entities more directly involved in the security model are described in Clause 5.4.

Figure 1 illustrates the client-application to card-application paradigm that underlies the ISO/IEC 24727 standard. The ISO/IEC 24727-3 application interface facilitates the connection and session mechanisms shown in this figure.

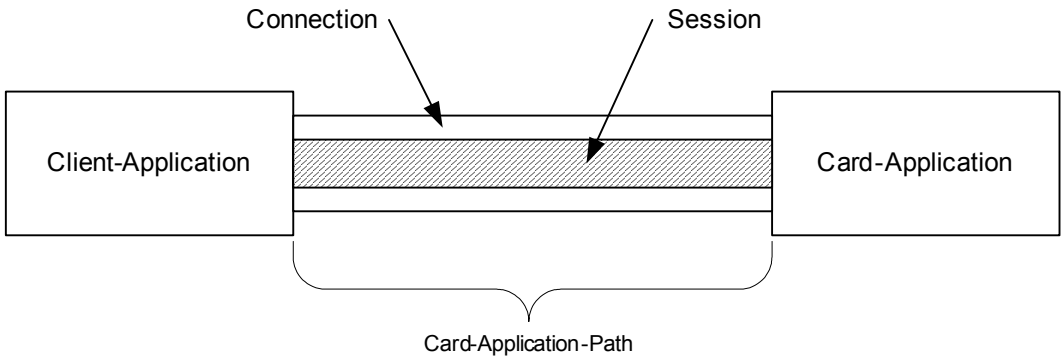

Figure 1 — Application Connection Paradigm

A card-application-path can be specified to allow a client-application to be connected to a specific card-application. Through such a connection, the client-application can access card-application-services using the ISO/IEC 24727-3 application interface. A session adds a security context to a connection in addition to its intrinsic security characteristics that can be used to protect the data flowing between the client-application and the card-application.

Figure 2 illustrates the entities defined in the model of computation and establishes the relationships among these entities. This entity-relationship diagram is elaborated below to describe individual card-application-services. The type of target applicable to each action is shown in the rounded boxes associated with each action.

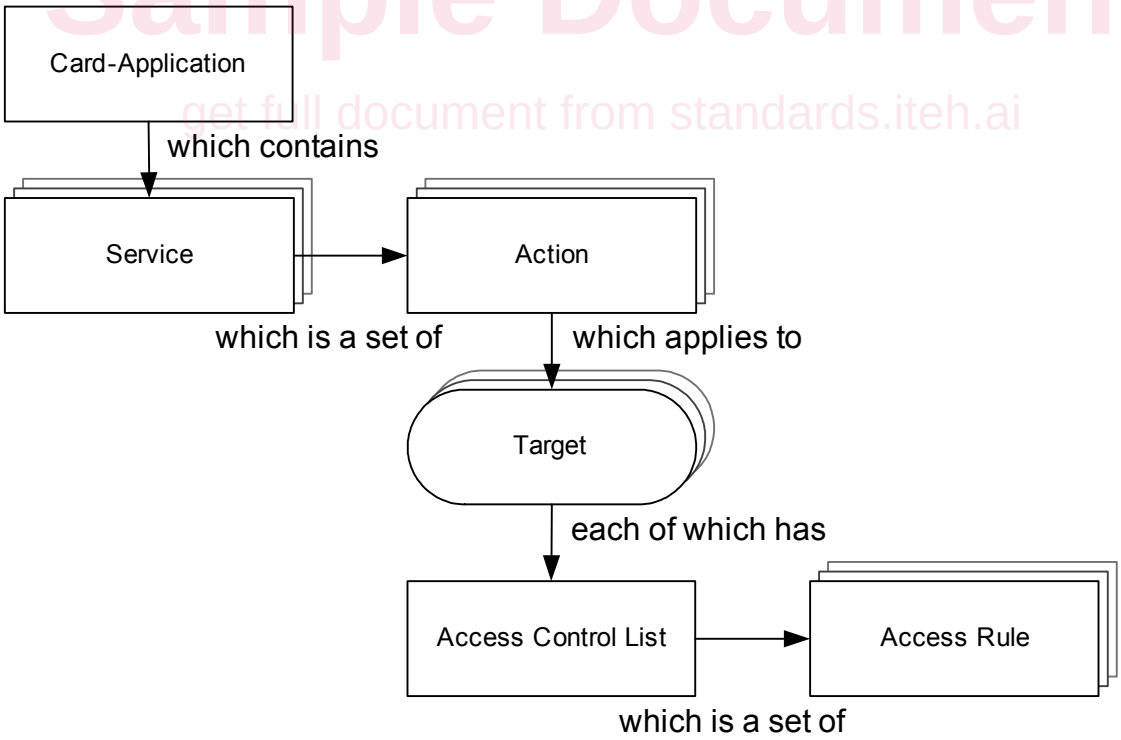

Figure 2 — Model of Computation Entities and Relationships

A card-application is a collection of targets and services. A service is a collection of actions. An action is an operation which is applied to a target. The actions and services of a card-application are accessed by a client-application using the ISO/IEC 24727-3 application interface.

5.3.2 Alpha Card-Application

The alpha-card-application shall be available at the application interface. It may either be present in the ICC or emulated by the SAL or GCAL implementation. In all cases, a connection by the client application to the alpha-card-application grants the availability of the card application list.

5.3.3 Accessing Card-Application-Services

A client-application uses the Initialize and CardApplicationPath entry points on the ISO/IEC 24727-3 application interface to gain access to card-application-services. A client-application uses the Terminate entry point to terminate access to card-application-services.

Before accessing card-application-services, a client-application must request the Initialize entry point on the ISO/IEC 24727-3 application interface. After the Initialize confirmation, the client-application may open connections and request actions with multiple card-applications, simultaneously or sequentially. The client-application should request the Terminate entry point when use of card-application-services is no longer needed.

5.3.4 Connection Service Interface

This card-application-service provides actions for the establishment of a connection between a client-application and a card-application. Once a connection is established, a session may be effected through this connection in order to enhance the security characteristics of the communication between the client-application and the card-application. Figure 3 illustrates the entity relationships of the Connection Service.

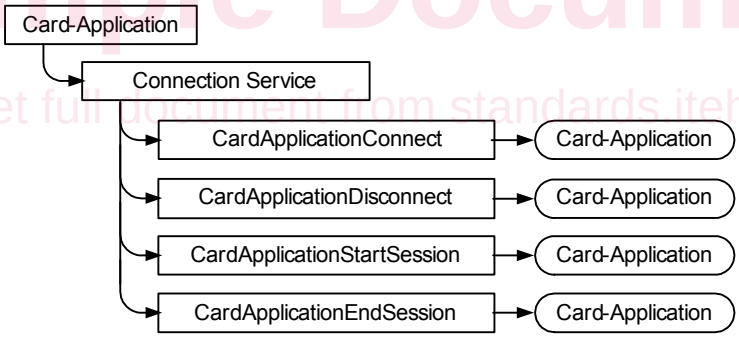

Figure 3 — Connection Service

The target of each of these actions, as specified in the diagram above, is the current card-application, or the card-application to which the client-application is attempting to connect.

5.3.5 Card-Application Service Interface

This card-application-service provides actions for the creation and manipulation of card-applications. Figure 4 illustrates the entity relationships of the Card-Application Service.

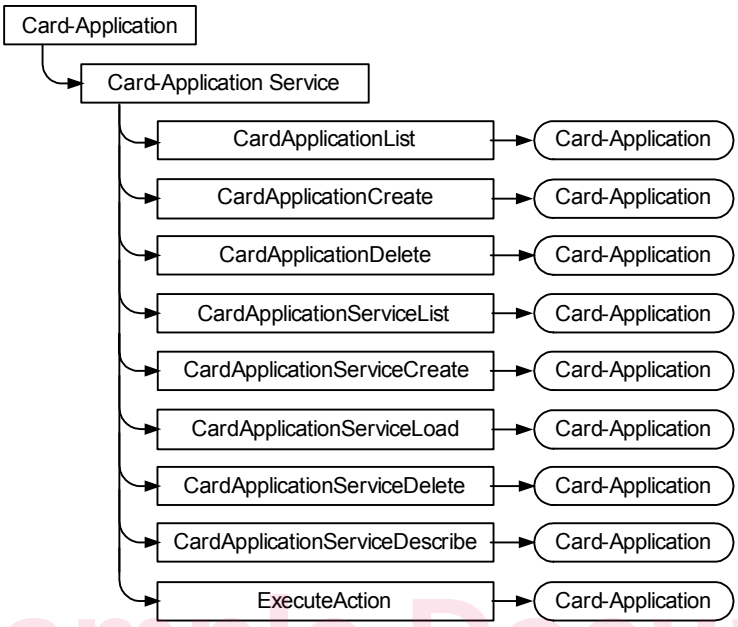

Figure 4 — Card-Application Service

The target of the CardApplicationCreate and CardApplicationDelete actions is the alpha card-application. The current card-application shall be the alpha card-application when requesting these actions.

The target of each of the remaining actions is the current card-application.

5.3.6 Named Data Service Interface

This card-application-service provides actions for the creation and manipulation of data-sets, a containment mechanism that allows for the establishment of common access rules for data contained in data structures for interoperability. Data-sets may contain any number of DSIs. Figure 5 illustrates the entity relationships of the Named Data Service.

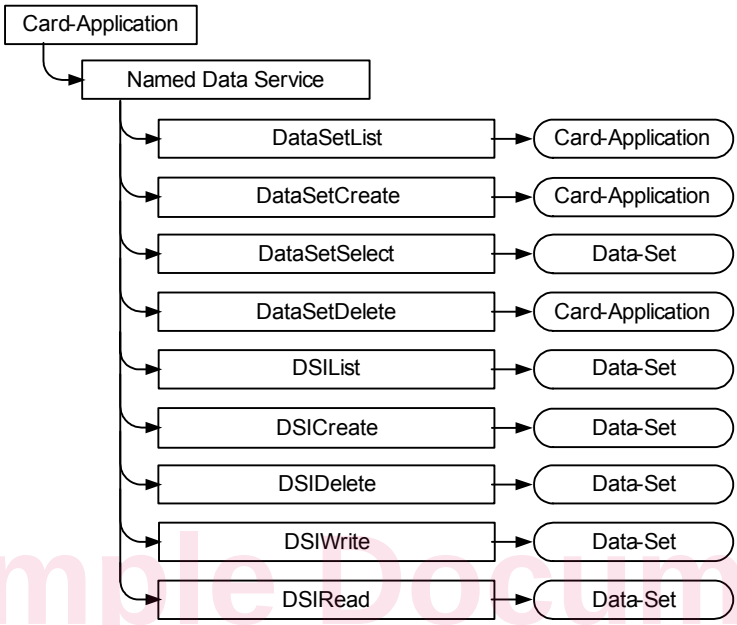

Figure 5 — Named Data Service

The target of each of these actions, as specified in the diagram above, is the current card-application, the current data-set, or the data-set which the client-application is attempting to select.