INTERNATIONAL STANDARD

ISO/IEC 24727-1

First edition
2007-02-15

Identification cards — Integrated circuit card programming interfaces —

Part 1: Architecture

Cartes d'identification — Interfaces programmables de cartes à puce — Partie 1: Architecture

Reference number
ISO/IEC 24727-1:2007(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 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 24727-1 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*

API administration and testing will form the subjects of the future Parts 4 and 5, respectively.

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.

ISO/IEC 24727 defines interfaces such that independent implementations are interoperable.

Services may be discoverable through mechanisms detailed in ISO/IEC 24727. ISO/IEC 24727 discovery methods include provisions for a client-application to discover

— card-applications available for selection on the ICC,

— information about each card-application.

ISO/IEC 24727-1 specifies the conceptual framework. It provides essential background information for the subsequent parts. Developers using ISO/IEC 24727 are encouraged to read this introductory part of ISO/IEC 24727. The other parts provide technical details of the concepts specified in ISO/IEC 24727-1.

ISO/IEC 24727-2 details the functionality and related information structures available to the implementation of the interface defined in ISO/IEC 24727-3.

ISO/IEC 24727-3 details service access mechanisms to initiate their use by a client-application.

ISO/IEC 24727-4 will detail trust mechanisms and connectivity mechanisms between adjacent components in the communication stack.

ISO/IEC 24727-5 will detail test mechanisms.

Functionality for ISO/IEC 24727-3 usually resides outside of the ICC. Functionality for ISO/IEC 24727-2 may reside inside the ICC.

Identification cards — Integrated circuit card programming interfaces —

Part 1: Architecture

1 Scope

ISO/IEC 24727 is a set of programming interfaces for interactions between integrated circuit cards 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.

This part of ISO/IEC 24727 specifies

— system architecture and principles of operation,

— a capabilities discovery mechanism,

— security rationale.

ISO/IEC 24727-1 is independent of physical interface technology.

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

3 Terms and definitions

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

3.1
authentication
process of assessing a level of confidence in identity or identification

3.2
authentication protocol
specific process for authentication

3.3
card
integrated circuit card

3.4
card-application
uniquely addressable set of functionalities on an ICC that provide data storage and computational services to a client-application

3.5
client-application
processing software needing access to one or more card-application(s)

3.6
data element
item of information seen at the interface for which are specified a name, a description of logical content, a format and a coding

[ISO/IEC 7816-4]

3.7
data set
named collection of data structures for interoperability

3.8
data structure for interoperability
ISO/IEC 7816-4 file identified by a two-byte file identifier or an ISO/IEC 8825 BER-TLV data object identified by an octet string encoding an ASN.1 tag

3.9
differential-identity
set of information that comprises a name, a marker, and an authentication protocol

3.10
generic card access layer
component which provides an ISO/IEC 24727-2 interface to a service access layer

3.11
identification
collective aspect of a set of characteristics and processes by which an entity is recognizable or known

3.12
interface
point at which independent and often unrelated systems meet and act on or communicate with each other

3.13
interoperability
ability for any card-application interface that conforms to ISO/IEC 24727 to be used by any client-application conforming to ISO/IEC 24727

3.14
marker
item of information within a differential-identity representing a unique characteristic of an entity

3.15
middleware
software that connects two otherwise separate applications

3.16
service
set of processing functions available at an interface

3.17
service access layer
component which provides an ISO/IEC 24727-3 API to a client-application

4 Abbreviated terms

AID application identifier

ACD application capability description

APDU application protocol data unit

API application programming interface

BER basic encoding rules

CCD card capability description

DSI data structure for interoperability

GCAL generic card access layer

GCI generic card interface

IAS identity, authentication, and (digital) signature services

ICC integrated circuit card

IFD interface device

OID object identifier

PKI public key infrastructure

RFU reserved for future use by ISO/IEC

SAL service access layer

TLV tag-length-value

URL uniform resource locator

5 Interoperability

Interoperability is the ability for any card-application interface that conforms to ISO/IEC 24727 to be used by any client-application conforming to ISO/IEC 24727. ISO/IEC 24727 defines a set of interfaces and discovery mechanisms such that independent implementations are functionally equivalent as verifiable by testing.

ISO/IEC 24727 defines interfaces at two levels

— between the client-application and a service interface,

— between a service access layer and a generic card interface.

For each specified interface, the relevant parts of ISO/IEC 24727 shall define which functionality shall be supported.

ISO/IEC 24727 applies to an ICC providing directly, or indirectly, a capability description. Capability description is described in 6.6.

The service interface, generic card interface, and capability descriptions may be extended according to the future development of ICC technologies.

6 Architecture

6.1 General

ISO/IEC 24727 partitions functionality between a client-application running on a host platform and a layered set of services that can be used by a client-application. The organization of services is further defined into a service interface, a generic card interface, and one or more card-applications resident on an ICC.

6.2 Architectural attributes

The service interface implements features given in 6.5.

The generic card interface implements features given in 6.8.

The connectivity interface implements features given in 6.9.

The trusted channel interface implements features given in 6.10.

Card-applications manage data sets. Each data set is named and the card-application list of data set names is available to the client-application by direct knowledge or discovery. A client-application uses the data set name when requesting a service to be performed on a data set.

Access to data sets is controlled through an access control list. The access control list describes the security conditions that shall be satisfied in order to perform an action on the data set. ISO/IEC 24727-3 provides additional detail on access control lists, identities, and actions.

Card-applications are organized on an ICC as an alpha card-application and one or more card-applications. Card-applications are selectable by AID at the service interface.

6.3 Logical architecture

Figure 1 illustrates the relationships between a client-application, the layers and interfaces defined in ISO/IEC 24727, and a card-application resident on an ICC. The flow of requests from the client-application to the card-application is shown as directional arrows indicating either a request or a confirmation. The naming of each arrow conveys functionality being supported by the standard. The actual format and syntax of a request or a confirmation is not detailed in this part of ISO/IEC 24727.

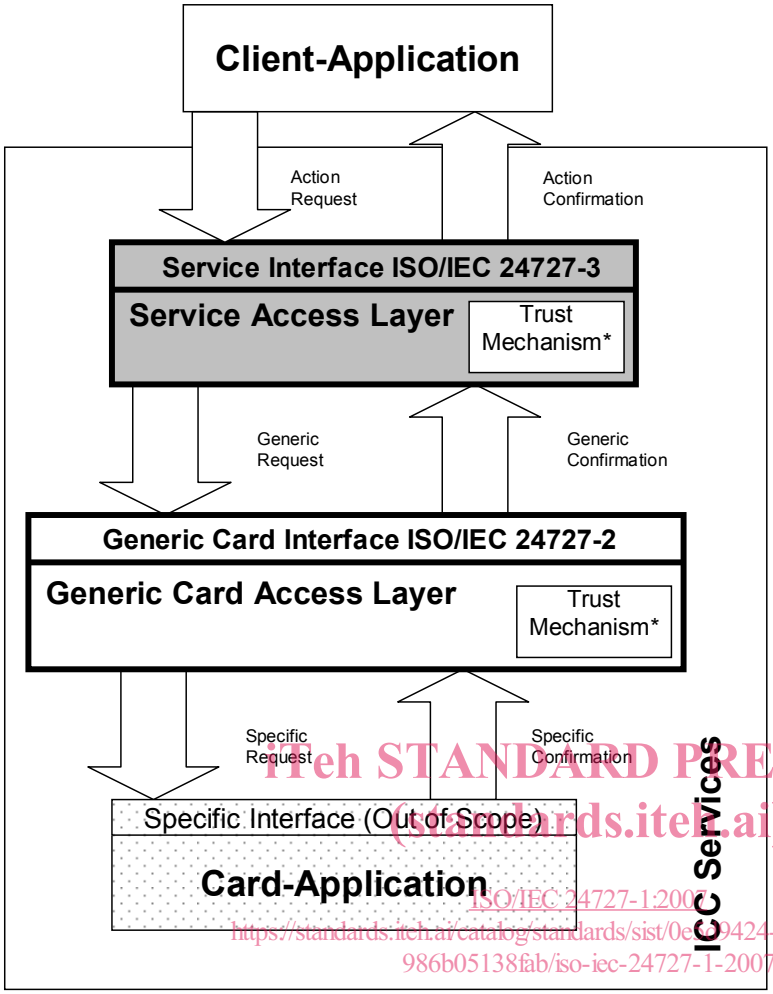

Figure 1 — Logical architecture of ISO/IEC 24727

Functionality of ISO/IEC 24727 can be implemented in more than one manner.

6.4 Protocol independence

ISO/IEC 24727 defined interfaces are specified in a manner independent of the protocols required to establish the communication between the client-application and card-application.

Figure 1 shows a stack of layers and interfaces.

A proxy is an implementation of the interface of a stack element to allow the stack element implementation to be split. For example, card-application in Figure 1 is a proxy for the actual card.

See Annex A for details on the configurations of implementations of the stack.

6.5 Client-application service access layer interface

ISO/IEC 24727-3 provides a detailed description of the service interface available to a client-application.

An implementation of the service interface

— translates an action request into one or more generic requests,