INTERNATIONAL STANDARD

ISO/IEC 24727-1

Second edition
2014-06-15

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 24727-1:2014(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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The Committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

This second edition cancels and replaces the first edition (ISO/IEC 24727-1:2007), which has been technically revised.

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 procedures*

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

Introduction

ISO/IEC 24727 specifies a set of programming interfaces and protocols enabling interactions between integrated circuit cards (ICCs) and applications resident on diverse computer platforms. The ICCs provide generic services for multi-sector use aimed preferentially at supporting trusted Identification, Authentication and Signature (IAS) operations. The organization and the operation of the ICCs conform to ISO/IEC 7816-4.

ISO/IEC 24727 makes use of the general principles of the Open Systems Interconnect reference model presented in ISO/IEC 7498-1 | ITU-T Rec. X.200. These principles suggest that the connection of complementary applications on diverse computer platforms be accomplished by well defined procedures accessed through standard interfaces. The procedures encompass both hardware and software facilities that allow the applications to interact, even when separated by complex communication pathways.

The collection of procedures that connect one application to another is referred to as a protocol stack. Each component of such a stack comprises an interface and a layer. The layer comprises the implementation of the procedural functionality that accepts and responds to requests conveyed through the interface. ISO/IEC 24727 specifies interfaces allowing independent layer implementations to be interchangeable. This comprises the basic definition of interoperability: *independent implementations are interchangeable*.

To achieve true interoperability across a wide range of application domains, some of which may pre-date ISO/IEC 24727, requires a variety of mechanisms to be addressed within the relevant implementations. These mechanisms include: common architectures, common semantics, formally defined interfaces, discoverability, extensibility, backward compatibility and conformance testing. The means of realizing these mechanisms are addressed in the following clauses and in the other parts of ISO/IEC 24727.

Identification cards — Integrated circuit card programming interfaces —

Part 1: Architecture

1 Scope

ISO/IEC 24727 specifies a set of programming interfaces and protocols enabling interactions between integrated circuit cards (ICCs) and applications resident on a variety of computer platforms. The ICCs provide generic services for multi-sector use by the applications. The organization and the operation of the ICCs conform to ISO/IEC 7816-4. It is anticipated that some application domains will seek to achieve interoperability through ISO/IEC 24727 facilities even though the applications pre-exist these facilities. To this end, various means of backward compatibility are established through mechanisms specified in ISO/IEC 24727.

This part of ISO/IEC 24727 specifies

— system architecture and principles of operation,

— the means for achieving interoperability among diverse application domains,

— the conceptual service and data models that span the relevant application domains, and

— the rationale for trusted processes enabled under these models.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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

[SOURCE: 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
SAL-lite
Lightweight component which provides a subset of ISO/IEC 24727-3 API for data structure discoverability by a client-application

3.17
service
set of processing functions available at an interface

3.18
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
GCAL	generic card access layer
GCI	generic card interface
ICC	integrated circuit card
IFD	interface device
SAL	service access layer
SAL-lite	service access layer lightweight component
TLV	tag-length-value

5 Interoperability

Interoperability addresses the facilities through which card-application interfaces conforming to ISO/IEC 24727 can be accessed by a client-application conforming to ISO/IEC 24727. ISO/IEC 24727 achieves interoperability through a variety of mechanisms, including:

— common architecture,

— common semantics,

— formally defined interfaces,

— discoverability,

— extensibility,

— backward compatibility, and

— conformance testing.

All of the interfaces in ISO/IEC 24727 are specified through formal languages. This establishes a rigorous expression of grammar and semantics allowing the interfaces to be independently implemented and conveyed throughout a variety of protocol stacks in an interoperable fashion.

As illustrated in Figure 1, for each specified interface the relevant parts of ISO/IEC 24727 shall define the functionality to be supported.

ISO/IEC 24727 applies to an ICC providing directly, or indirectly, a capability description. The capability description is further described in Clause 6.6, and is more rigorously specified in ISO/IEC 24727-2.

Means of extending the various interfaces and protocols addressed by ISO/IEC 24727, including relevant ICC technology, are addressed in the various parts of the standard.

6 Architecture

6.1 General

ISO/IEC 24727 partitions functionality between a client-application running on a host platform and a set of services provided by an ICC resident card-application that can be used by a client-application. Access to such services is provided through a protocol stack that provides 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 discussed in Clause 6.5 and more rigorously addressed in ISO/IEC 24727-3.

The generic card interface implements features discussed in Clause 6.8 and more rigorously addressed in ISO/IEC 24727-2.

The connectivity interface implements features discussed in Clause 6.9 and more rigorously addressed in ISO/IEC 24727-3, ISO/IEC 24727-3 and ISO/IEC 24727-6.

The trusted channel interface implements features discussed in Clause 6.10 and more rigorously addressed in ISO/IEC 24727-4.

Card-applications manage data sets, including establishing a unique name space for data sets and all information contained within 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 and ISO/IEC 24727-4 provide additional detail on access control lists, identities, and actions.

Card-applications are organized on an ICC through an encompassing alpha card-application and one or more contained 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. Each arrow illustrates functionality supported by the standard. The actual format and syntax of a request or a confirmation is detailed in the indicated part of ISO/IEC 24727.

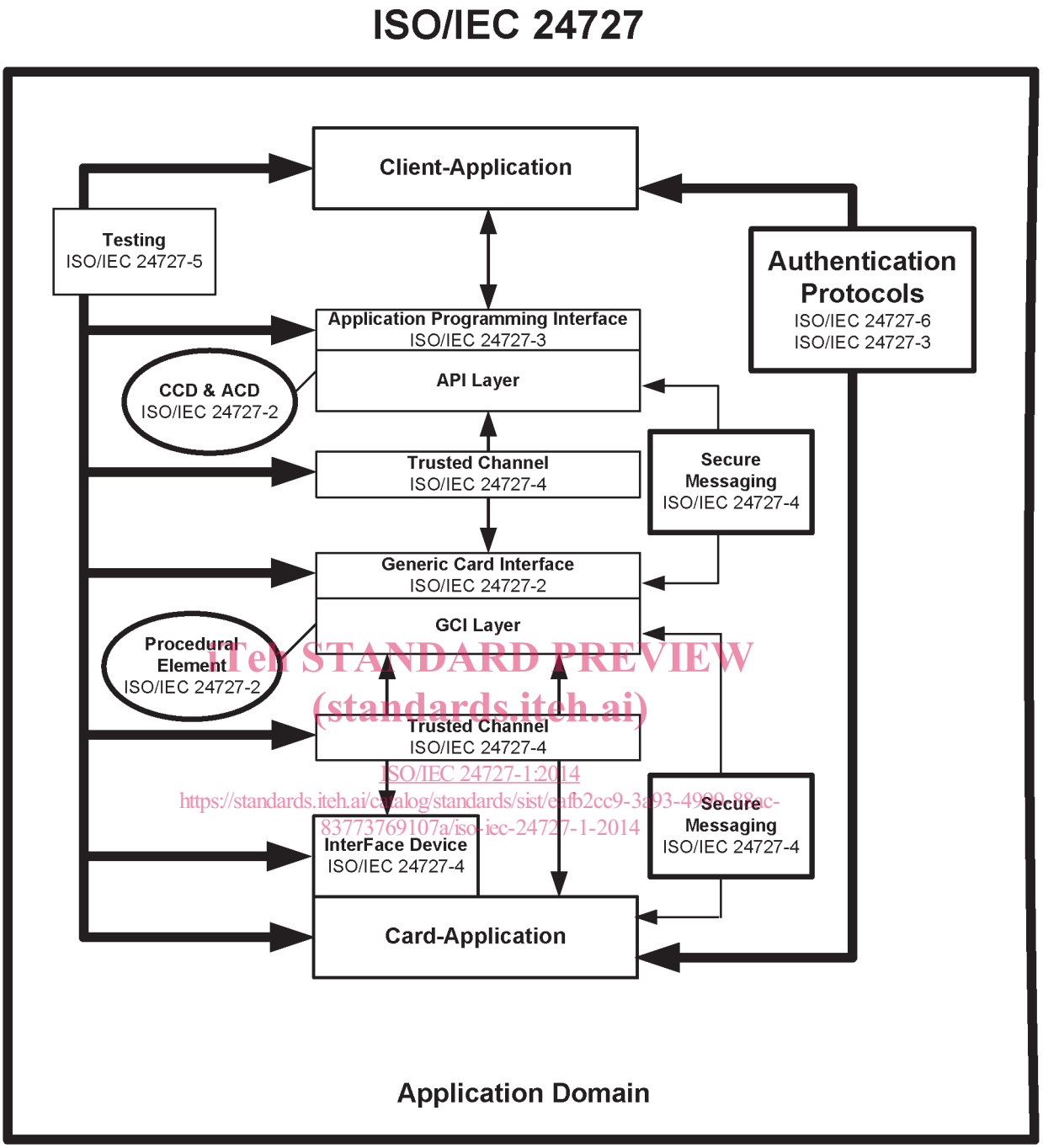

Figure 1 — Logical architecture of ISO/IEC 24727

Functionality of ISO/IEC 24727 can be implemented in multiple ways with interface conformance verified through testing specified by ISO/IEC 24727-5.

6.4 Protocol independence

ISO/IEC 24727 interfaces are specified through ASN.1 description, with subordinate descriptions provided through XML. Interfaces are specified in a manner independent of the protocols required to establish the communication between the client-application and card-application.

Figure 1 illustrates a stack of layers and interfaces necessary to enable connectivity between client-applications and card-applications.