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.

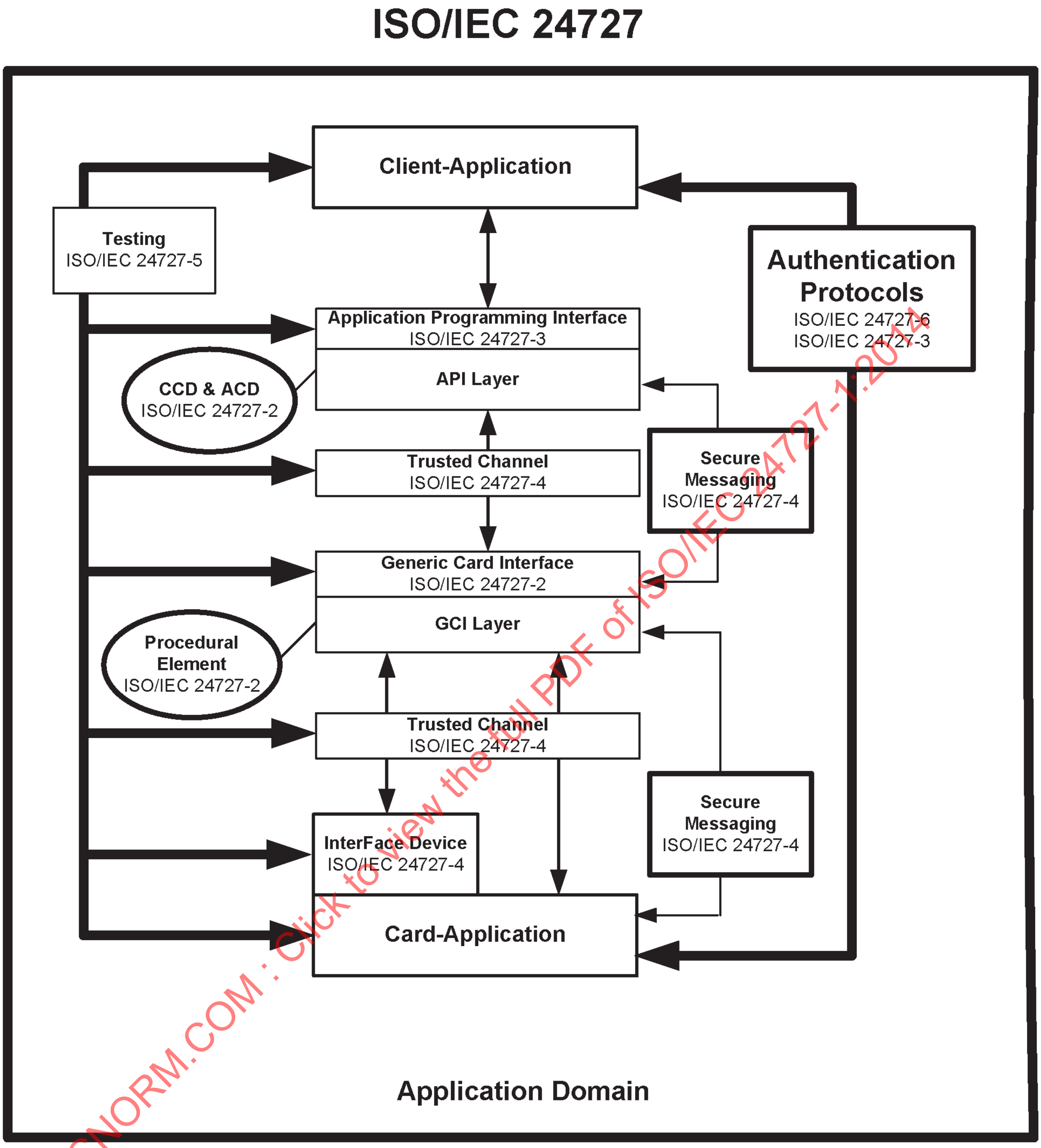

Figure 1 — Logical architecture of ISO/IEC 24727

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.

A proxy-agent mechanism is an implementation of the interface of a stack element that allows the stack element implementation to be split between a proxy and an agent found at some other point within the protocol stack. An interoperable proxy-agent mechanism depends of a formal language specification of the interface and a well defined framing mechanism. This facility is specified in ISO/IEC 24727-4.

Annex A illustrates a number of generically useful configurations. These configurations are considered in more rigorous fashion in ISO/IEC 24727-4.

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 couched in the semantics of the client-application into one or more generic requests couched in the semantics of the ICC-resident card-application,
- translates one or more generic confirmations from the card-application into an action confirmation destined for the client-application.

The service interface includes

- client-application to card-application connectivity using the generic card interface,
- client-application to card-application security in accordance with the security rationale,
- cryptographic service,
- differential-identity service.

6.6 Capability description

The service interface and generic card interface are specified in a manner that facilitates discovery of the capabilities of one or more card-applications resident on an ICC. The information structure for enabling this discovery mechanism is the Capability Description.

Two levels of Capability Description are detailed in ISO/IEC 24727.

- A Card Capability Description (CCD) is used to discover one or more card-applications resident on the ICC. The CCD resides in the alpha card-application. The CCD provides APDU translation information.
- An Application Capability Description (ACD) may be provided with a card-application. The ACD, if present, is used to inform the requesting entity of additional or revised capability from what is provided in the CCD.

ISO/IEC 24727-2 details both levels of Capability Description. The purpose of the capability description is to enable discovery at both the generic card interface and service interface. Any command-response pair translation between the generic card interface and the service interface may be specified using a capability description.

ISO/IEC 24727-2 further details the capability description methodology relating to how information is organized, protected, retrieved, and updated using card-applications resident on an ICC.

A subset of API called SAL-lite implemented exclusively on a local host supports card-application discoverability.

6.7 Data model

The service interface specified in ISO/IEC 24727-3 is predicated on a data model structure that defines data elements and their interrelationship. While they are application specific, the data elements and their relationships are presented consistently through this data model structure. Thus, the application specific data models are discoverable by client-applications through the service interface.

6.8 Generic card interface

ISO/IEC 24727-2 defines a means for access to a card-application present on an ICC. The generic card interface detailed in ISO/IEC 24727-2 provides a fixed set of functionality.

An implementation of the generic card interface

— translates a generic request into one or more specific requests,

— translates one or more specific confirmations into a generic confirmation.

ISO/IEC 24727-2 defines the functionality available for data processing, security management, and administration.

6.9 Connectivity interface

ISO/IEC 24727-3 provides a detailed description of the connectivity interface available to components. Mechanisms to effect this connectivity is specified in ISO/IEC 24727-4. An implementation of the connectivity interface is used to establish a communication channel between adjacent components in the communication stack.

6.10 Trusted channel interface

ISO/IEC 24727-4 provides a detailed description of the trusted channel interface available to stack components. An implementation of the trusted channel interface is used to establish a secure communication channel between adjacent components in the protocol stack.

7 Security rationale

ISO/IEC 24727 employs the security concepts and mechanisms defined in ISO/IEC 7816-4:2005.

ISO/IEC 24727 utilizes secure messaging consistent with ISO/IEC 7816-4 specified in ISO/IEC 24727-4.

Security in an ISO/IEC 24727 implementation depends on the ability to map the security architecture mechanisms defined in ISO/IEC 24727-3 and ISO/IEC 24727-4 onto the security architecture mechanisms supported by the ICC as specified by ISO/IEC 7816-4.

Cryptographic information discovery may be implemented in more than one form, e.g.

— use of capability description,

— use of ISO/IEC 7816-15 as specified in ISO/IEC 24727-2 and ISO/IEC 24727-4.

ISO/IEC 24727-3 details the mechanics of the security rationale from a client-application perspective.

Annex A
(informative)

Implementation configuration examples

A.1 General

A discussion of anticipated stack configurations is detailed in this Annex. More detailed specifications of these various stack configurations is presented in ISO/IEC 24727-4. The set of stack configurations presented addresses all of the use cases thus far identified. However, it should be noted that specializations of these configurations is not precluded by ISO/IEC 24727. Indeed, such specialization is an essential element necessary to achieve the desired levels of interoperability.

Each diagram represents a physical architectural perspective of a single client-application communicating with a single card-application as illustrated in Figure A.1. The possible expansion of request/confirmation exchanges at the card-application interface is not shown in these drawings.

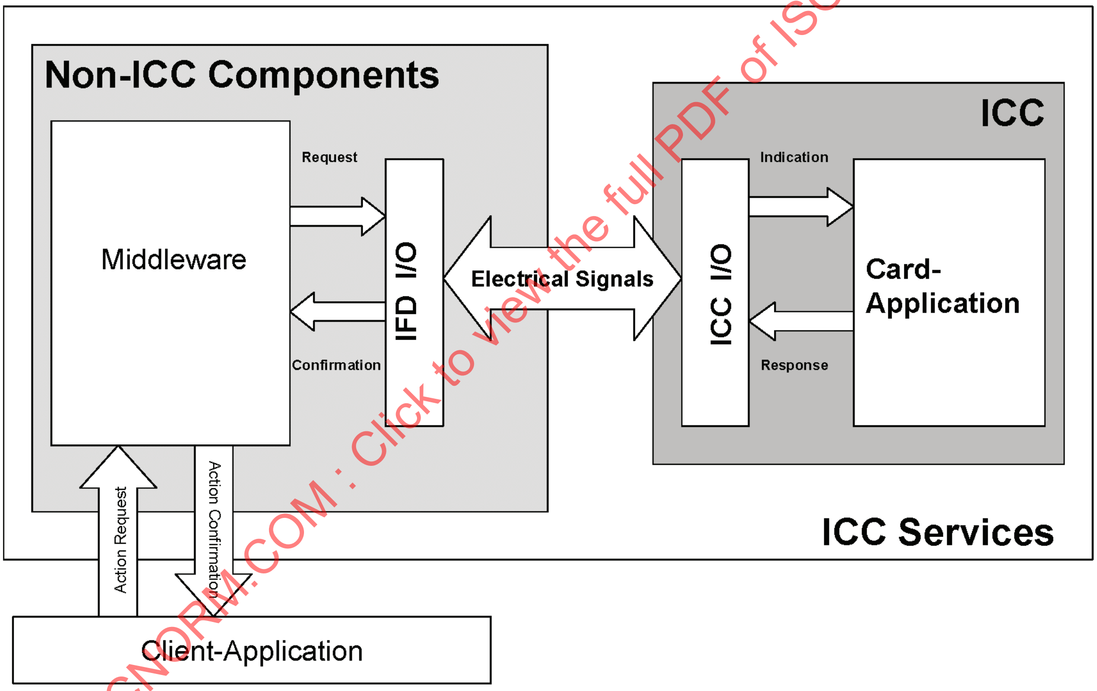

Figure A.1 — Physical architecture

Figure 1 in Clause 6 and Figure A.1 show the same system but from different perspectives. Figure 1 illustrates a logical view of the architecture whereas Figure A.1 illustrates a physical view. The mapping of components between the logical and physical perspectives depends on the chosen implementation configuration as outlined in further clauses of this Annex and addressed specifically in ISO/IEC 24727-4.

Hereinafter follows a brief description of the physical architecture shown in Figure A.1.

ICC Services: An implementation that provides services to a client-application and employs an ICC.

ICC: An element of ICC Services. The component is identical to a physical ICC.

Non-ICC Components: This element represents all other functionality provided within ICC Services. This element is complementary to the ICC.

Electrical Signals: The two major functional partitions of ICC Services communicate through a channel called “Electrical Signals”. The specific type of electrical signals (e.g. ISO/IEC 7816-3 (T=0, T=1), ISO/IEC 7816-12 USB, ISO/IEC 14443 contactless, and Transport Layer Security) are addressed in the relevant standards.

ICC I/O: This is a component of ICC. Its purpose is to transform messages received by the channel “Electrical Signals” into requests which are sent to the Card-Application. Furthermore, this component transforms confirmations received from the Card-Application into electrical signals and sends them via the channel “Electrical Signals”. ICC I/O is out of scope for ISO/IEC 24727.

IFD I/O: This functionality, contained in “non-ICC components”, has a similar responsibility as ICC I/O. IFD I/O is out of scope for ISO/IEC 24727.

Card-Application: As defined in Clause 3.

Middleware: As defined in Clause 3.

A.2 Discrete layer configuration

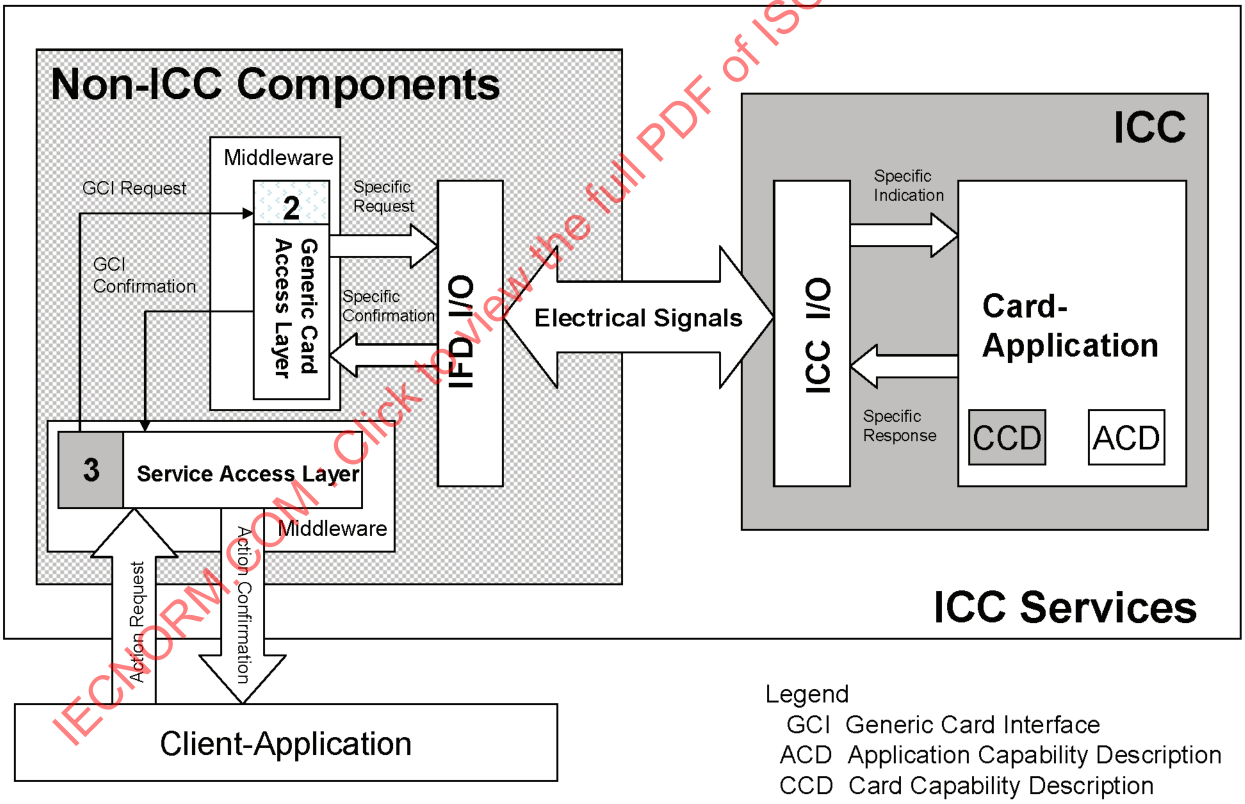

Figure A.2 — Discrete implementation of each interface and layer

This configuration illustrates the implementation of ISO/IEC 24727-2 and ISO/IEC 24727-3 as distinct components. As illustrated in ISO/IEC 24727-4, this class of implementation can present as an Opaque ICC Stack or as a Full-network Stack.

This configuration is proposed for evolving requirements. The generic card access layer, serving as an ICC proxy, can provide the necessary translation required for an existing, deployed ICC.

A.3 Combined configuration

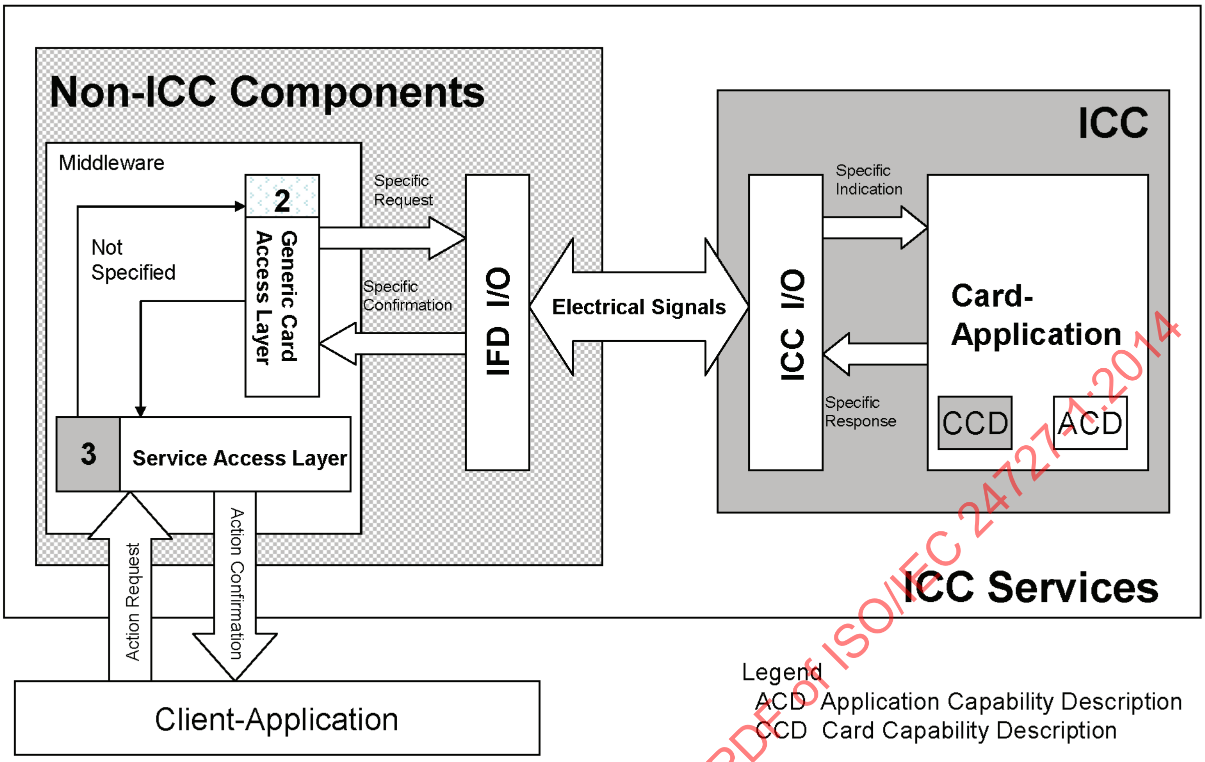

Figure A.3 — Combined implementation

This configuration proposes the service interface, discovery and any APDU translation are implemented as a single software component. The interaction between the ISO/IEC 24727-2 generic card interface and the ISO/IEC 24727-3 service access layer is not specified in this case. As illustrated in ISO/IEC 24727-4, this class of stack configuration can present as a Loyal Stack, a Remote Loyal Stack, a Remote ICC Stack, or an ICC Resident Stack.

A.4 On-ICC generic card access layer configuration

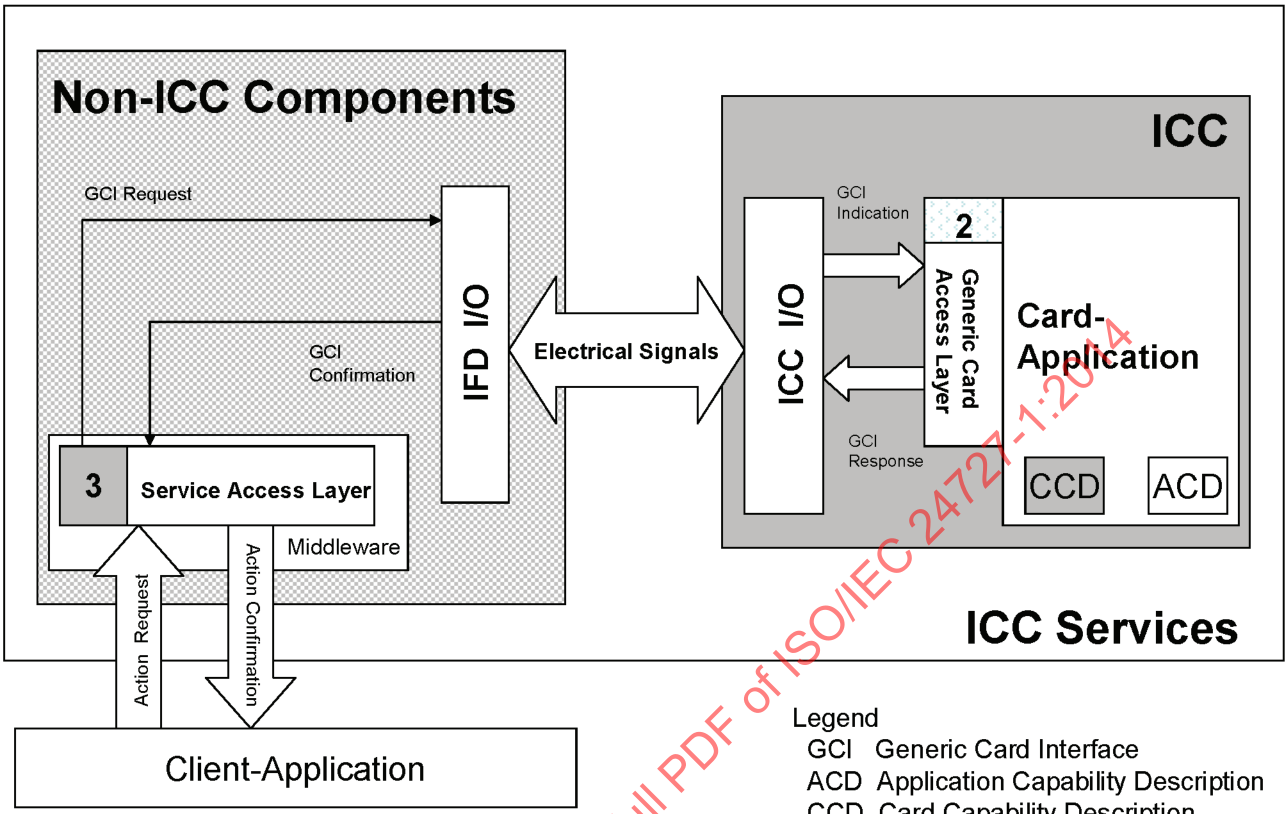

Figure A.4 — Generic card access layer implemented on the ICC

This configuration proposes the generic card interface and access layer is implemented on the ICC. In ISO/IEC 24727-4 this is presented as an ICC Resident Stack. In this stack configuration, access to the card application can be provided through an APDU-based connection via the ENVELOPE APDU indicated in ISO/IEC 24727-2 and/or directly through a TLS message structure if the ICC has direct network connectivity. Supporting TLS through direct network connection is not specified by the ISO/IEC 7816 series of standards.

A.5 On-ICC implementation of service access and generic card access layers

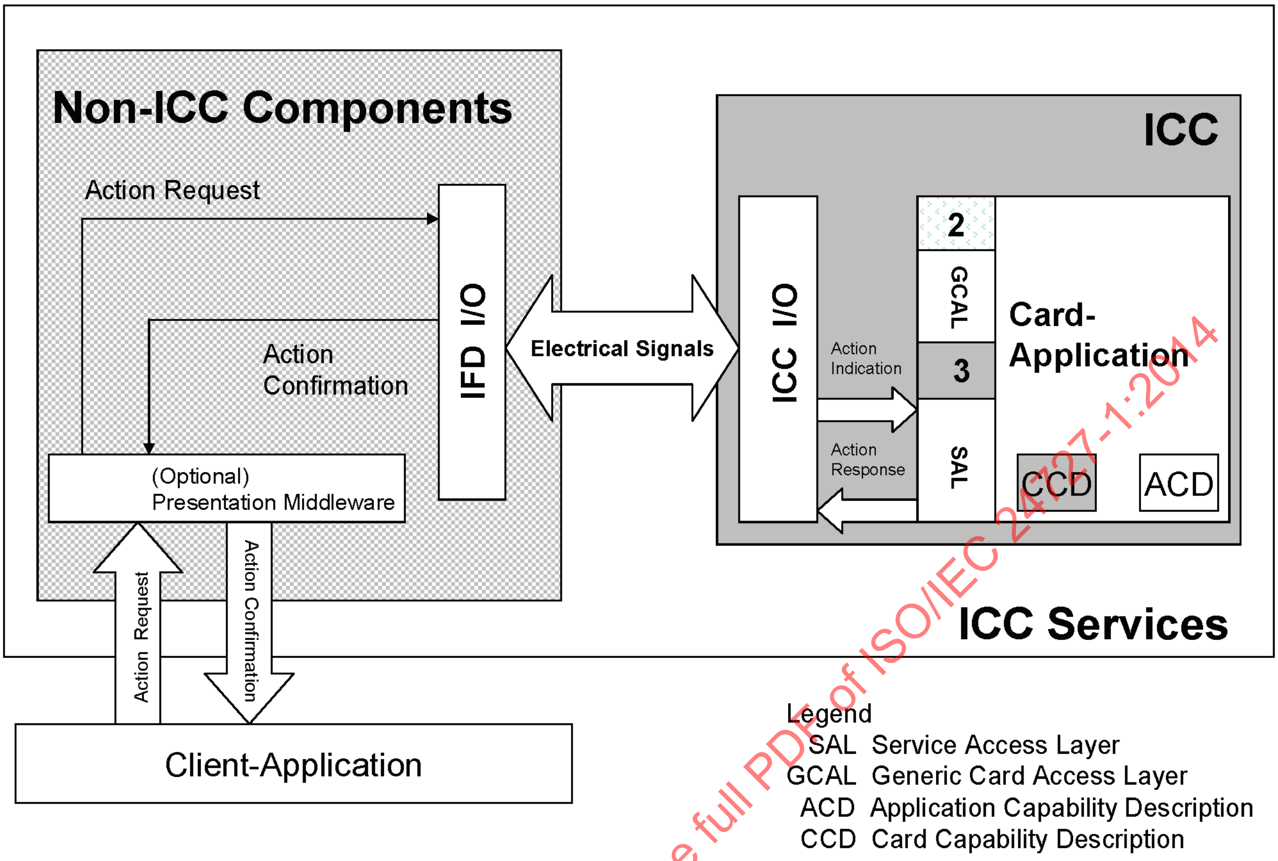

Figure A.5 — Service access and generic card access layers implemented on the ICC

In this configuration, ISO/IEC 7816-4 addresses the encapsulation of actions through ASN.1 data objects in the form of BER-TLV structures.

A.6 Loadable/fixed non-ICC components hosting of capability description

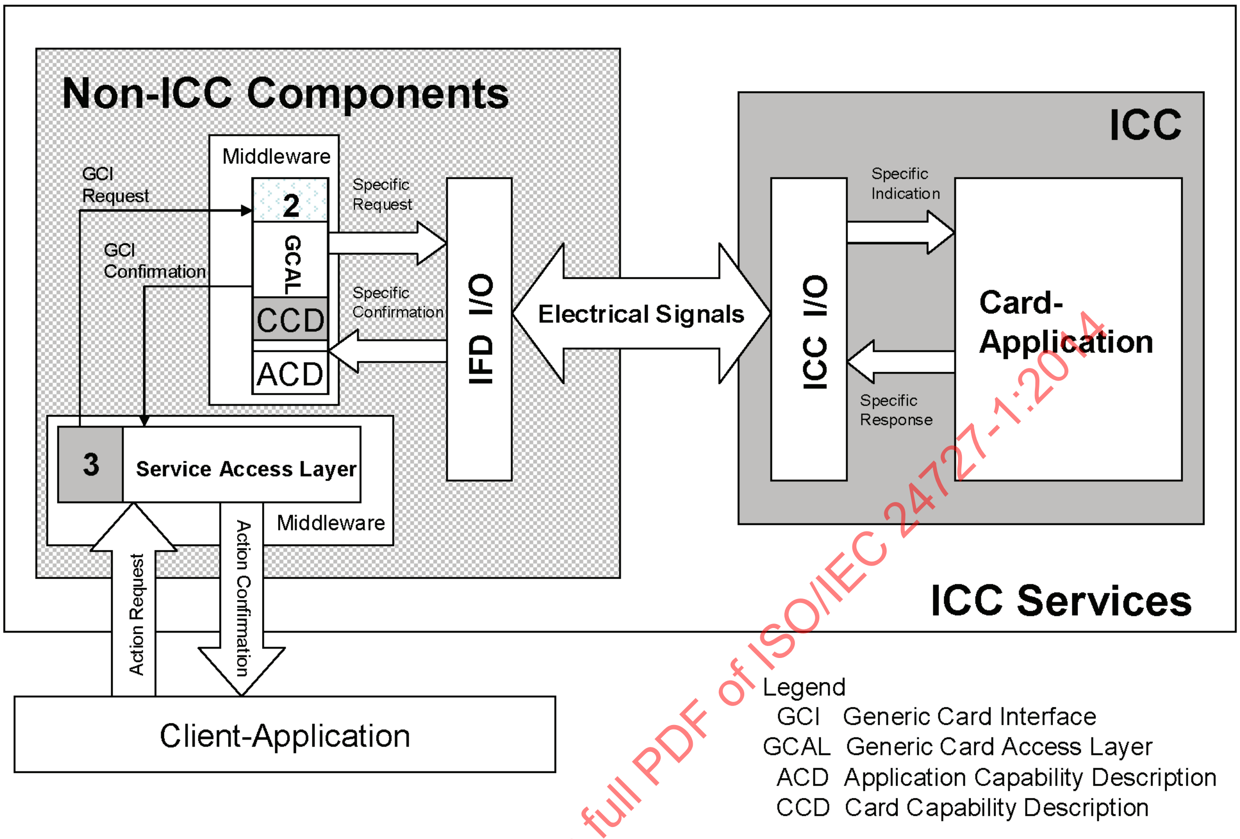

Figure A.6 — Loadable or fixed configuration

Loadable configuration is proposed for accommodating an ICC that cannot support the loading of a capability description. The CCD and ACD are provided by the middleware using off-ICC facilities. ISO/IEC 24727-2 specifies specific signalling mechanisms through which middleware can address these facilities.

Fixed configuration is proposed for accommodating an ICC that cannot support the loading of a capability description. Further, the middleware supports a known set of ICC implementations. The capability description may be explicitly provided or is implied in the functionality of the middleware (e.g.; a loadable API).

A.7 Web service configuration

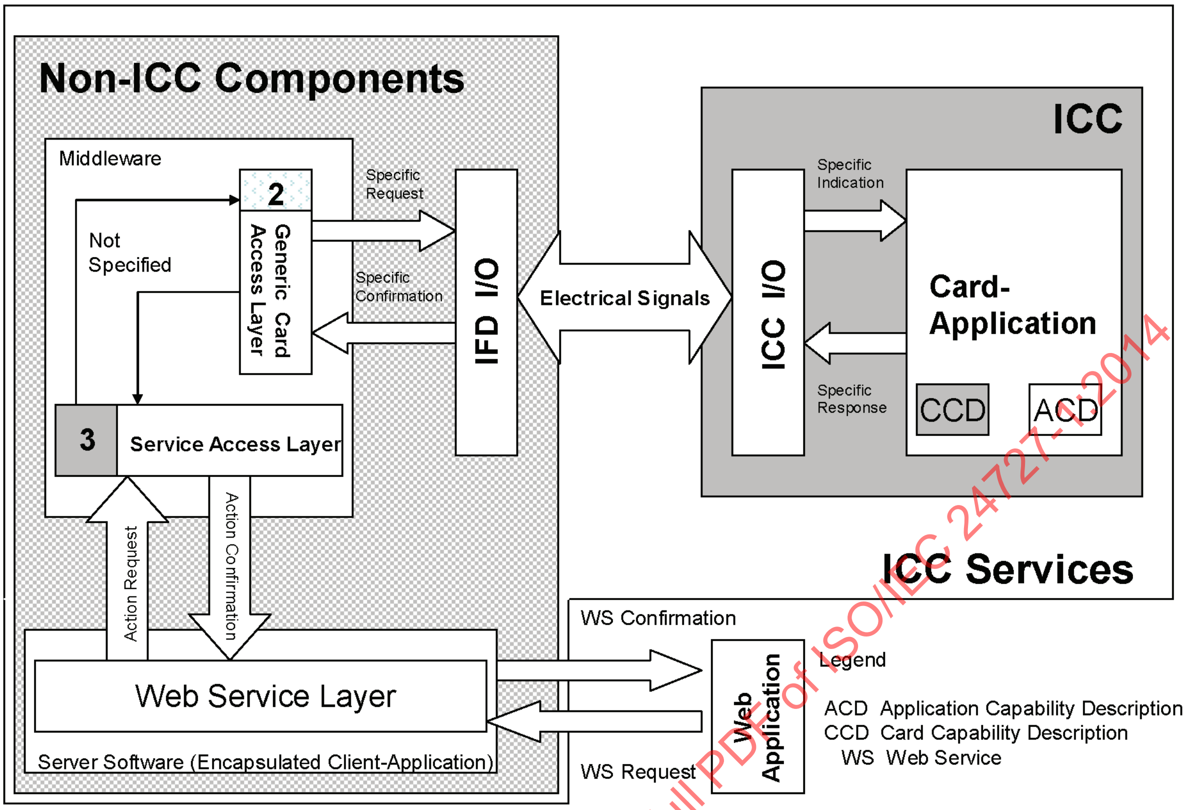

Figure A.7 — Web service configuration

This configuration proposes a Web service Interface which can be accessed from Web applications. All interfaces in ISO/IEC 24727 are formally specified preferentially through ASN.1, but secondarily through XML descriptions found respectively in ISO/IEC 24727-3 and ISO/IEC 24727-4.