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.

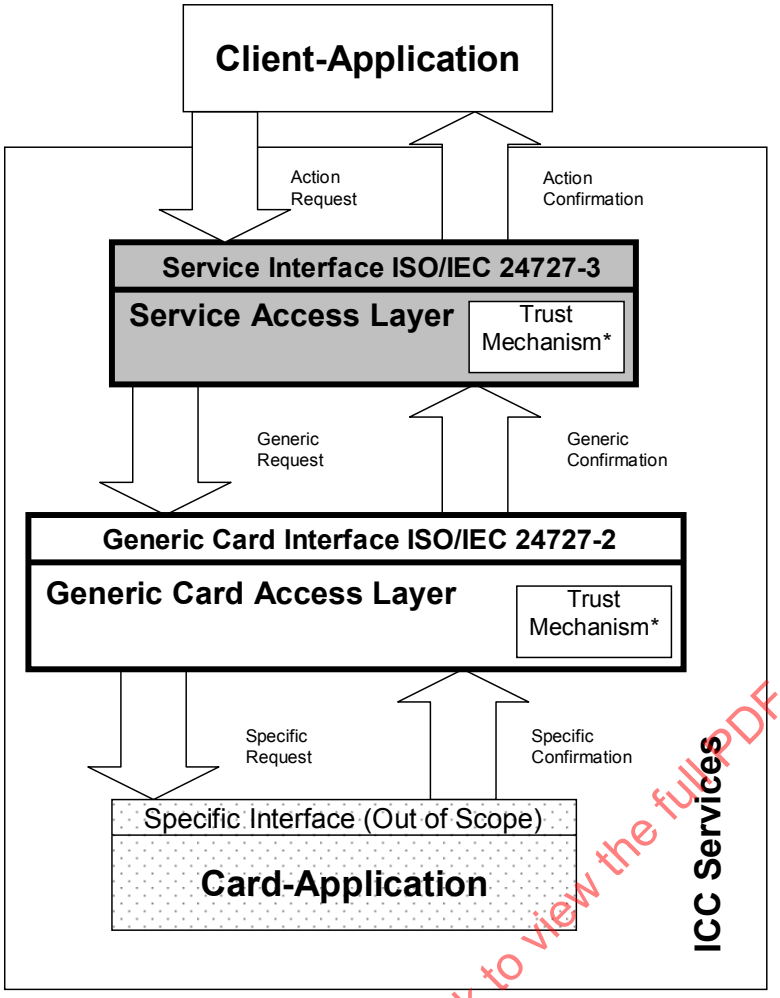
Card-applications manage data sets. Each data set is named and the card-application list of data set names is available to the client-application by direct knowledge or discovery. A client-application uses the data set name when requesting a service to be performed on a data set.

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.



(*)Note: None, one or both of these mechanisms may exist

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,

— translates one or more generic confirmations into an action confirmation.

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 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.

6.7 Data model

Data models define data elements and their interrelationship. Data models are application specific. Data models are intended to be discoverable by client-applications.

6.8 Generic card interface

ISO/IEC 24727-2 defines a means for access to a card-application in 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

A future International Standard (ISO/IEC 24727-4) will provide a detailed description of the connectivity interface available to components. 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

A future International Standard (ISO/IEC 24727-4) will provide a detailed description of the trusted channel interface available to components. An implementation of the trusted channel interface is used to establish a secure communication channel between adjacent components in the communication stack.

7 Security rationale

ISO/IEC 24727 employs the security concepts and mechanisms defined in ISO/IEC 7816-4:2004, 5.4.

ISO/IEC 24727 supports particular modes of secure messaging from ISO/IEC 7816-4.

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

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

— use of capability description,

— use of ISO/IEC 7816-15.

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 each envisioned configuration is detailed in this Annex. The reader is cautioned that this is not an exhaustive list of configurations.

Connectivity to an IFD and other transport layer details are represented in the drawings but are out of scope with respect to enabling communications between the card-application, IFD, one or more ISO/IEC 24727 layers, and the client-application.

Services provided below the client-application may use APDU command-response pairs as the means to make a request and receive a confirmation. This Annex does not detail the syntax or semantics of any interface shown.

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.

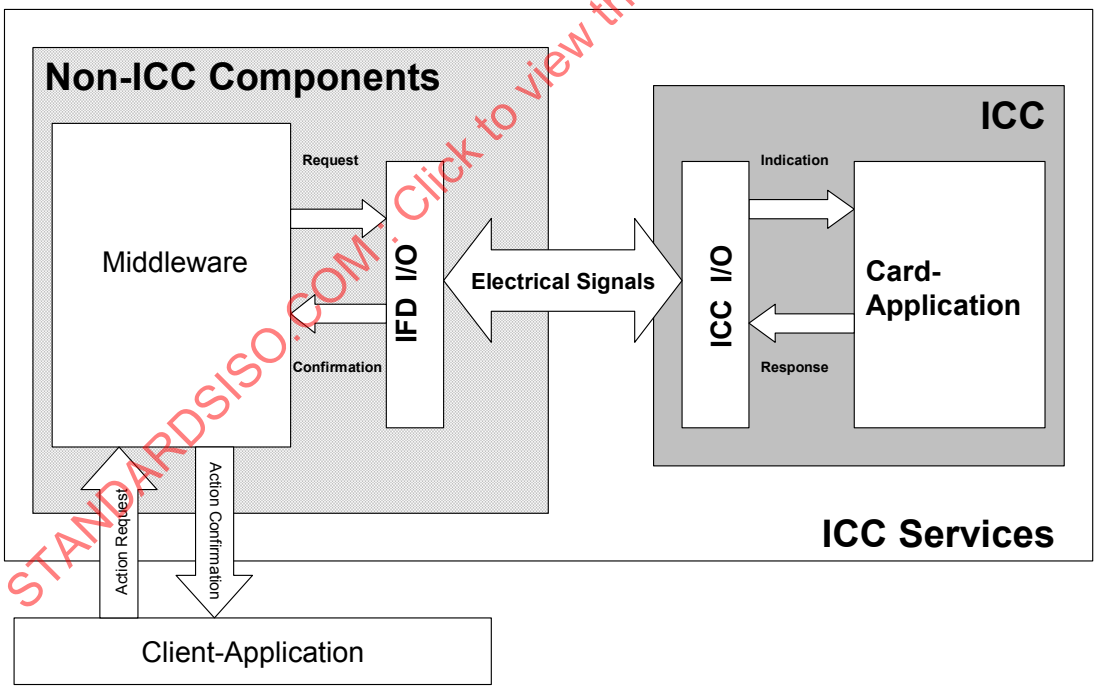


Figure A.1 — Physical architecture

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.

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) are out of scope for ISO/IEC 24727.

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

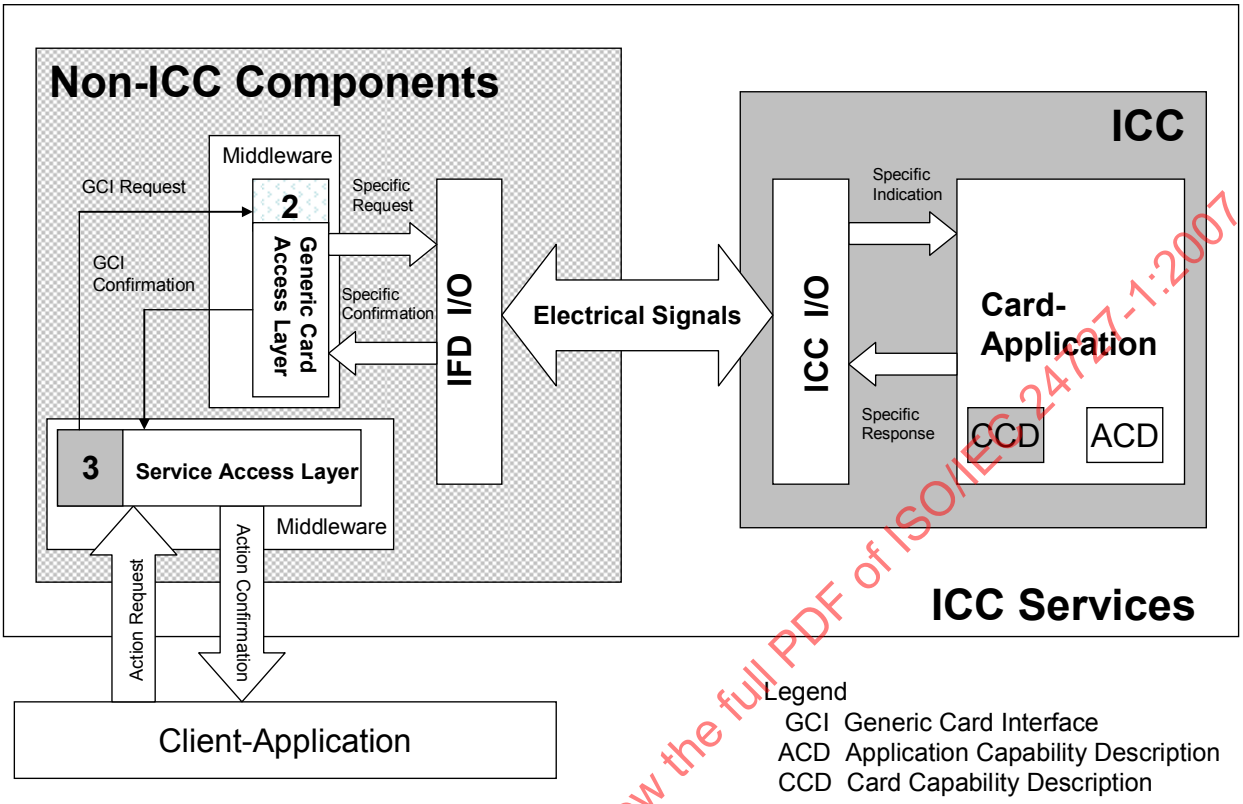


Figure A.2 — Discrete implementation of each interface and layer

This configuration illustrates the implementation of ISO/IEC 24727-2 and ISO/IEC 24727-3 as distinct components.

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

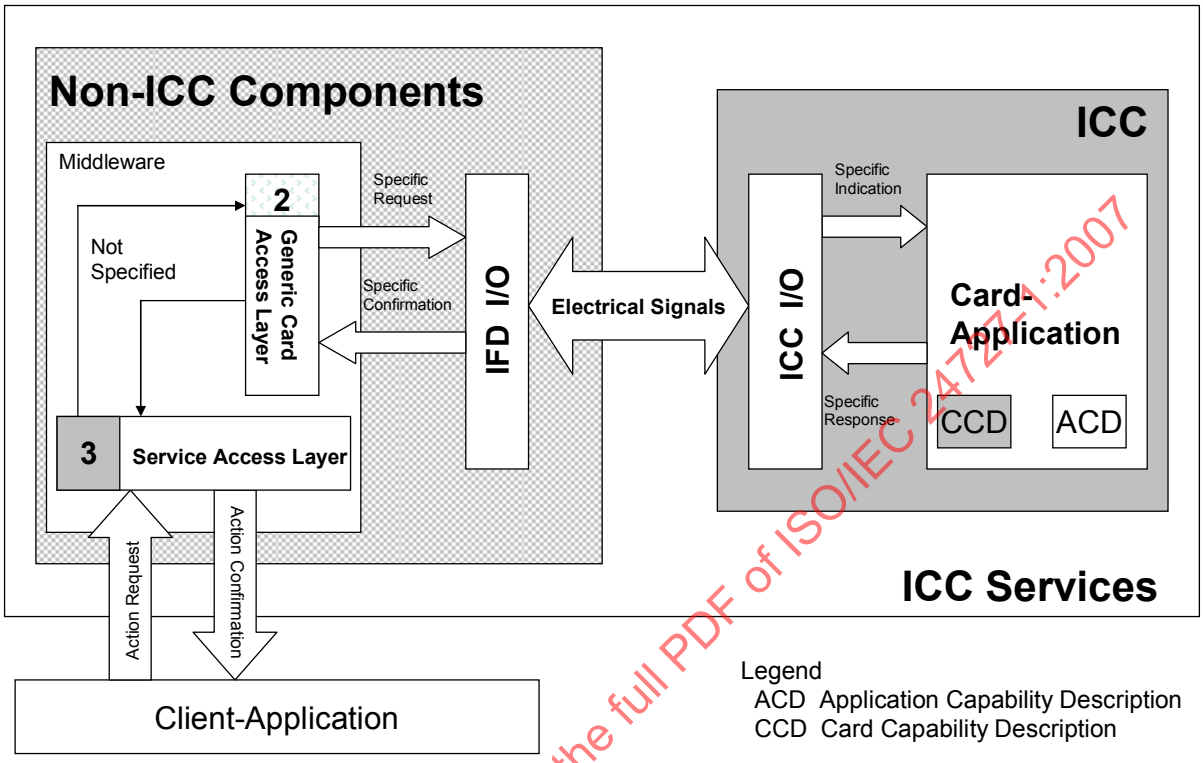


Figure A.3 — Combined implementation

This configuration proposes the service interface, discovery and any APDU translation is 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.

A.4 On-ICC generic card access layer configuration

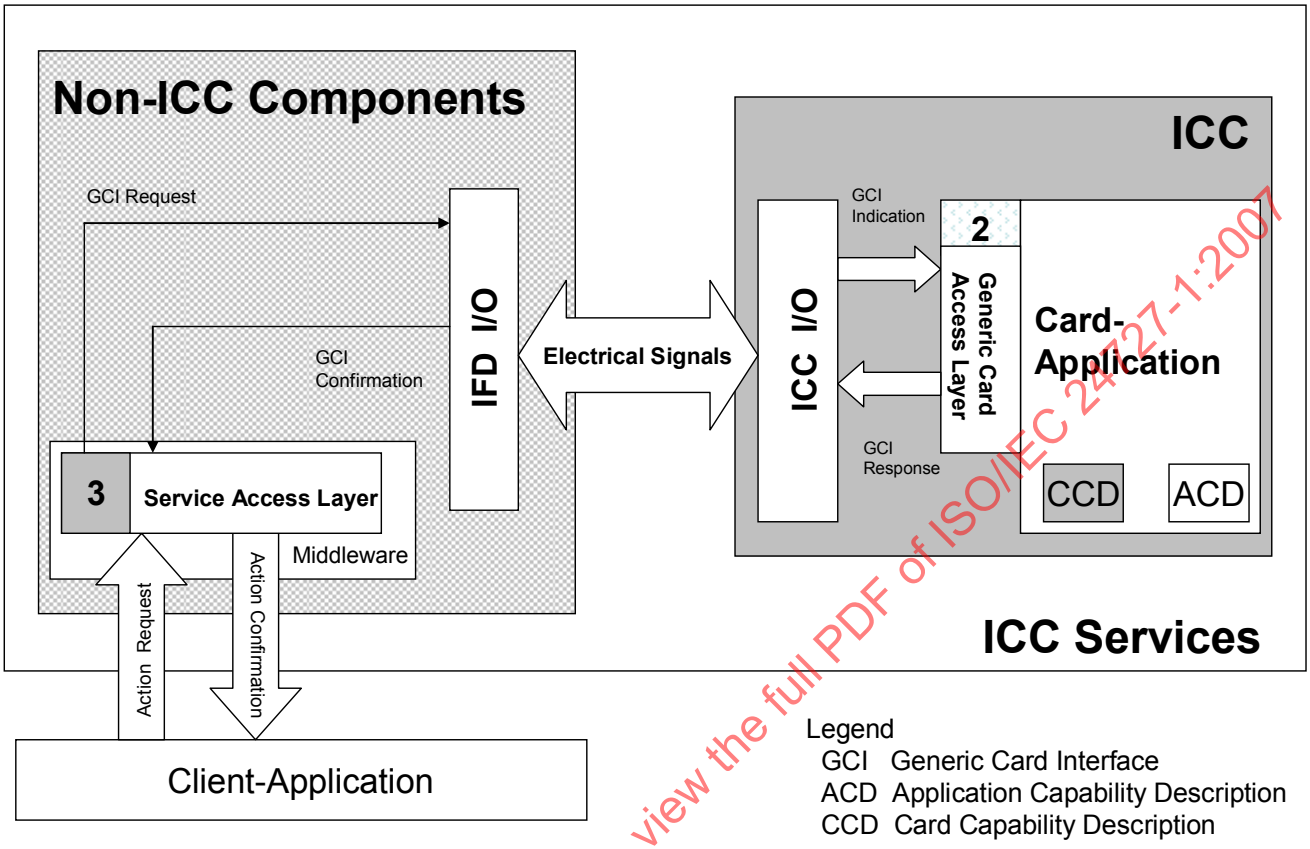


Figure A.4 — Generic card access layer implemented on the ICC

This configuration proposes the generic card interface and access layer is implemented on the ICC. No translation of APDU command-response pairs is anticipated.

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

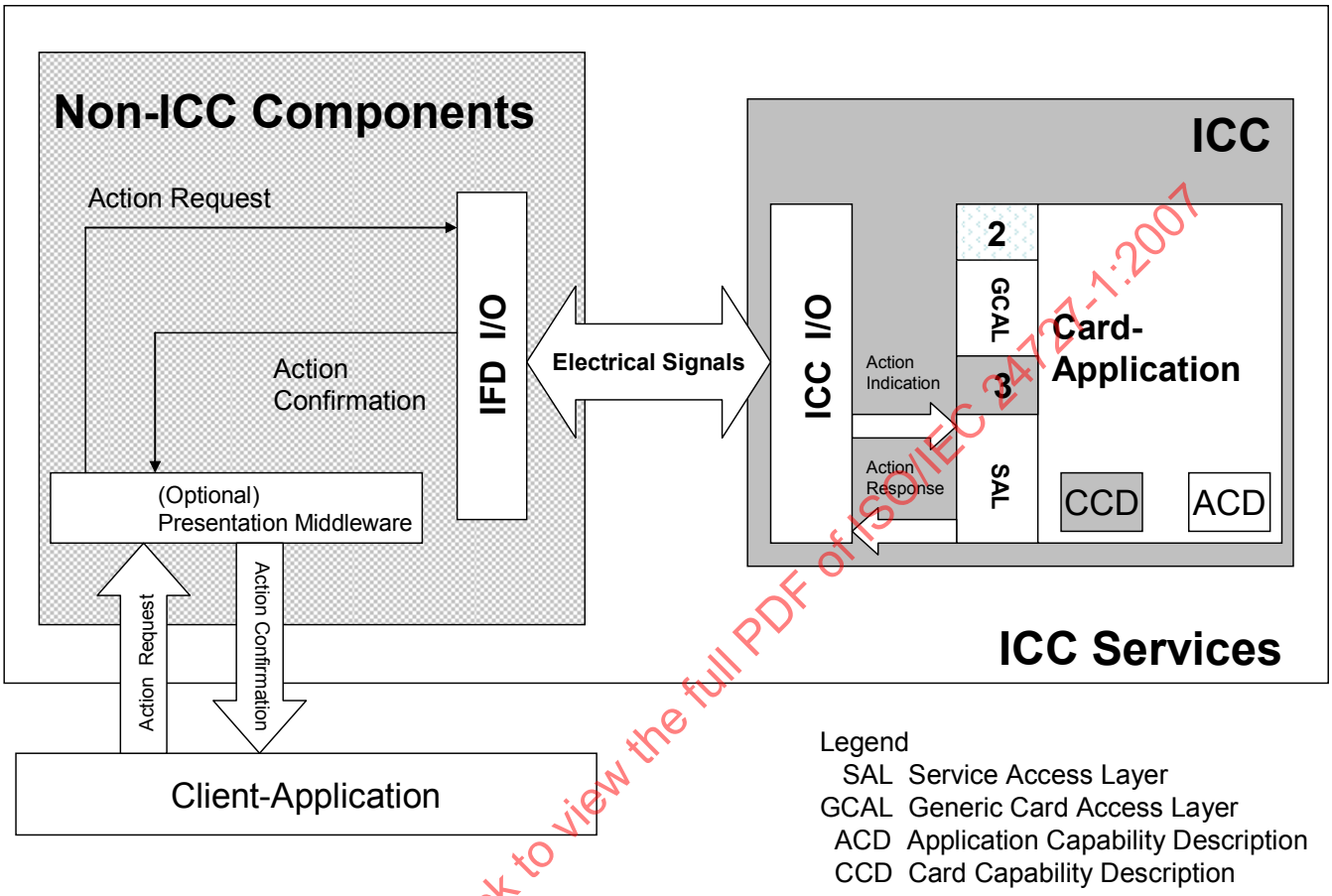


Figure A.5 — Service access and generic card access layers implemented on the ICC

In this configuration, ISO/IEC 7816-4 does not define a standard way to encapsulate actions in standard APDUs.

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

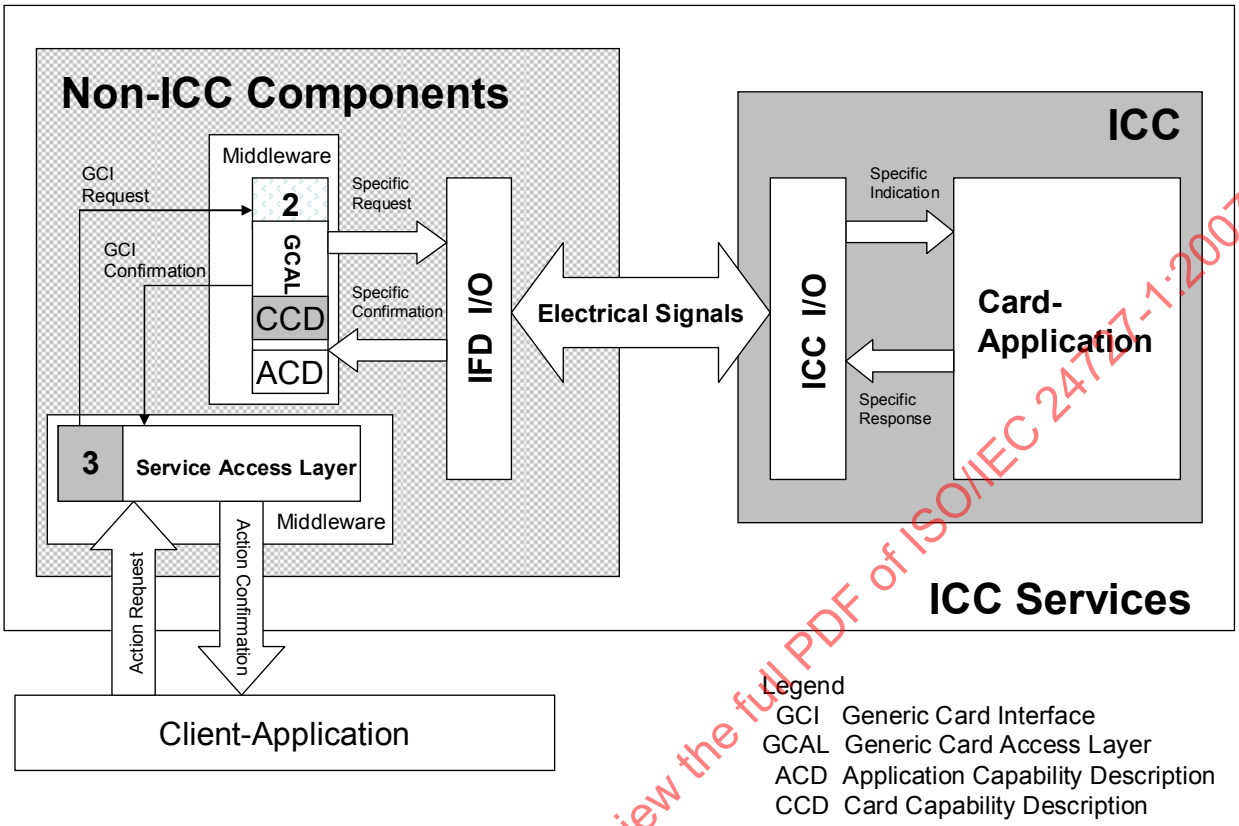


Figure A.6 — Loadable or fixed configuration

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 an unspecified means.

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).

NOTE This particular type of configuration may pose a challenge to achieving interoperability as there are no interoperable, specified means for a Part 2 implementation to discover the CCD/ACD.

A.7 Web service configuration

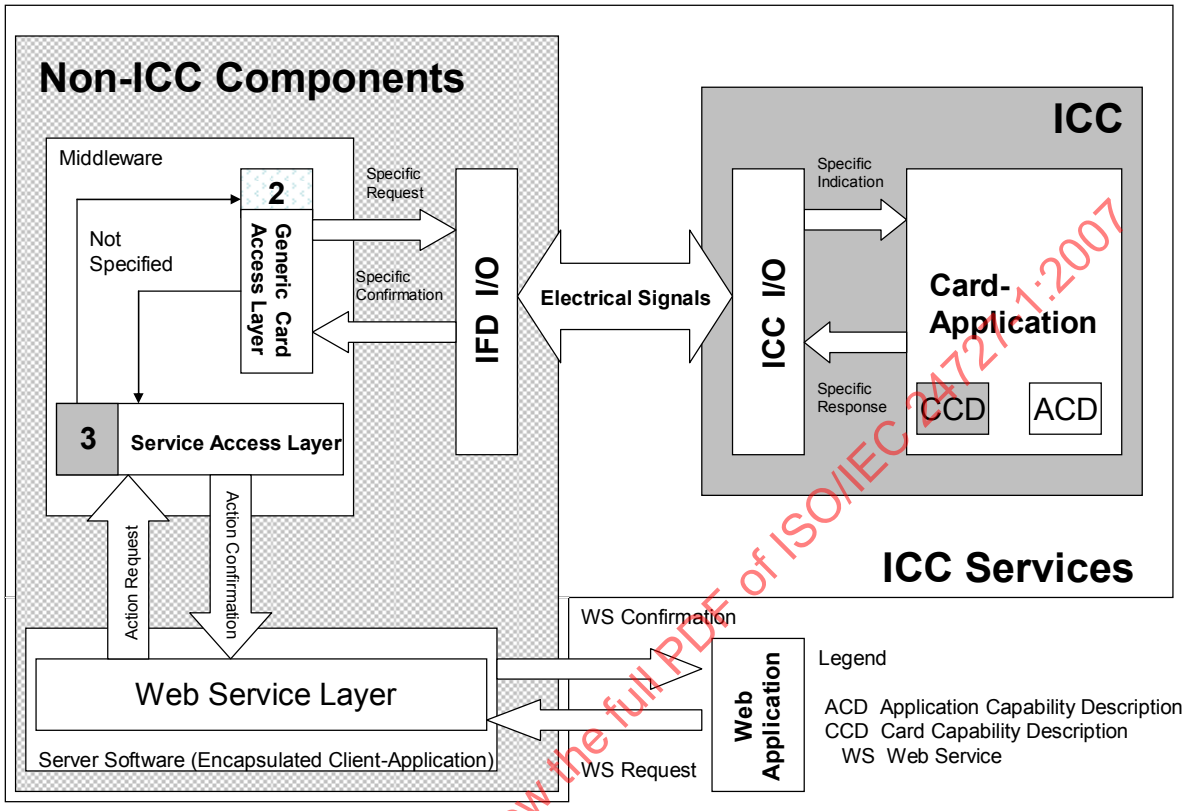


Figure A.7 — Web service configuration

This configuration proposes a Web service Interface which can be accessed from Web applications. The Web service layer can be provided as a local client-application that exposes to web applications either an ISO/IEC 24727-3 service interface or a (non-specified) proprietary interface.

A.8 Multiple application configuration

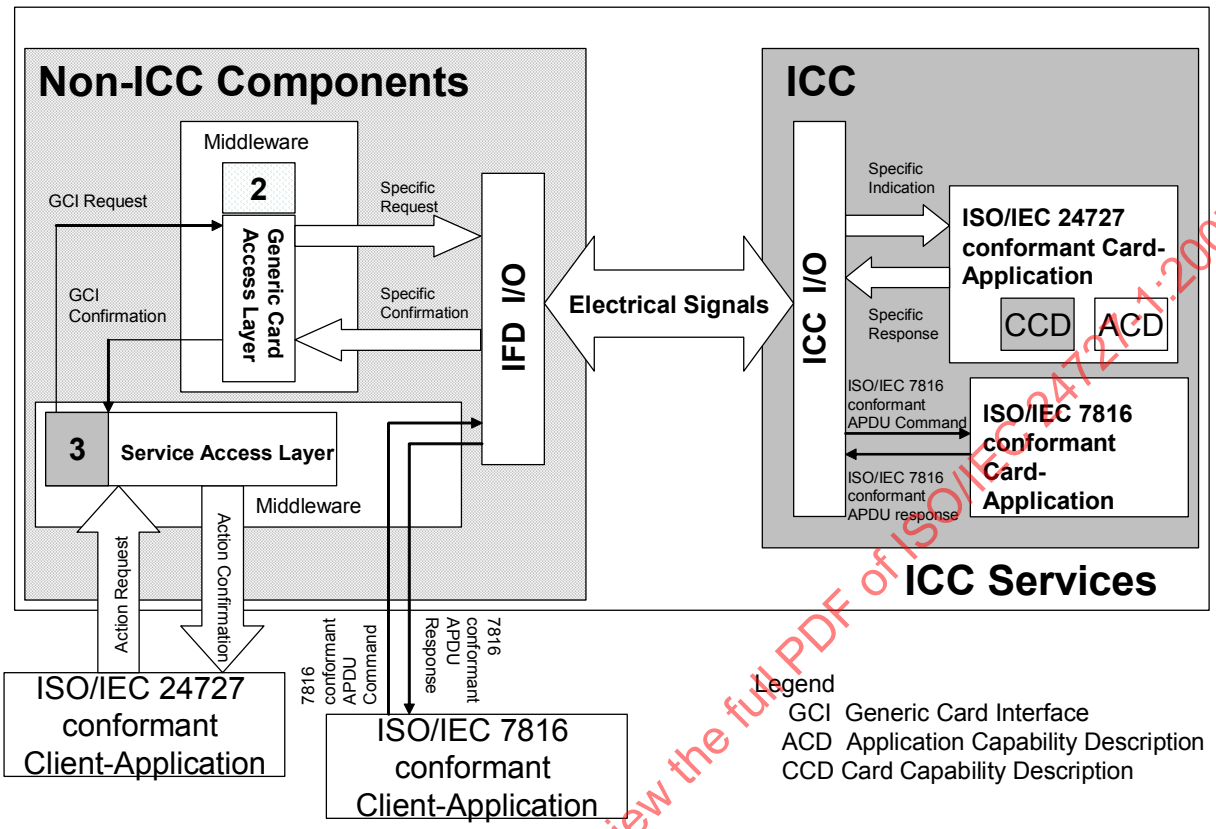


Figure A.8 — Multiple application configuration

This configuration illustrates the co-existence of an ISO/IEC 24727 card-application within an ICC that also supports other ISO/IEC 7816 card-applications.