INTERNATIONAL STANDARD

ISO/IEC 24727-4

First edition
2008-11-01

Identification cards — Integrated circuit card programming interfaces —

Part 4: Application programming interface (API) administration

Cartes d'identification — Interfaces programmables de cartes à puce — Partie 4: Administration d'interface de programmation (API)

Reference number
ISO/IEC 24727-4:2008(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 24727-4 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 ICCs conform to ISO/IEC 7816-4.

ISO/IEC 24727 is relevant to ICC applications desiring interoperability among diverse application domains. ISO/IEC 7498-1:1994 is used as the layered architecture of the client-application to card-application connectivity. That is, the client-application, through the application interface, assumes that there is a protocol stack through which it will exchange information and transactions among card-applications using commands conveyed through the message structures defined in ISO/IEC 7816. The semantics of action requests through the interface defined in ISO/IEC 24727-3 refers to application protocol data units (APDUs) as characterized through the interface defined in ISO/IEC 24727-2, and in the following International Standards:

— ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

— ISO/IEC 7816-8:2004, *Identification cards — Integrated circuit cards — Part 8: Commands for security operations*

— ISO/IEC 7816-9:2004, *Identification cards — Integrated circuit cards — Part 9: Commands for card management*

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

By conforming to this part of ISO/IEC 24727, interoperable implementations of ISO/IEC 24727-3 and ISO/IEC 24727-2 can be realized. Implementation details are not defined within this part of ISO/IEC 24727; it is assumed that an implementation conforms to an accepted security policy. The specific security policy is outside the scope of ISO/IEC 24727.

Identification cards — Integrated circuit card programming interfaces —

Part 4:
Application programming interface (API) administration

1 Scope

ISO/IEC 24727 defines a set of programming interfaces for interactions between integrated circuit cards and external applications to include generic services for multi-sector use.

This part of ISO/IEC 24727 standardizes the connectivity and security mechanisms between the client-application and the card-application.

It specifies API-Administration of service-independent and implementation-independent ISO/IEC 24727 compliant modules, including security, that enables action requests to a specific card-application of an ICC such that, when coupled to data model and content discovery operations, the card-application can be used by a variety of client-applications.

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*

ISO/IEC 9797-1:1999, *Information technology — Security techniques —Message Authentication Codes (MACs) —Part 1: Mechanisms using a block cipher*

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*

ISO/IEC 24727-3, *Identification cards — Integrated circuit card programming interfaces — Part 3: Application interface*

IETF RFC 2246, *The TLS Protocol Version 1.0*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 24727-1, ISO/IEC 24727-2, ISO/IEC 24727-3 and the following apply.

3.1
channel
physical pathway allowing movement of information bits between a client-application and a card-application

3.2
component
executable code comprising a processing layer accessed with ISO/IEC 24727 defined application programming interfaces

3.3
confidentiality
access restricted to some defined level of differential-identity authentication

3.4
dubious-channel
channel that might allow information messages to be altered, dropped, replayed or overheard by eavesdroppers

3.5
instantiation
operational component implementation or communication channel implementation

3.6
integrity
state of immutability of information

3.7
ISO/IEC 24727 protocol stack
series of processing components connected by communication channels that connect a client-application to a card-application

3.8
loyal-channel
channel that intrinsically maintains the integrity of channel end-points along with the confidentiality, integrity and authenticity of information

3.9
loyal-platform
computing platform that is trusted to perform data transformations and communication while maintaining confidentiality, integrity and authenticity of information

3.10
loyal-stack
ISO/IEC 24727 stack in which the full stack from client-application to the integrated circuit card that contains the card-application is implemented on a single loyal-platform

3.11
path-protection-policy
specification of the security characteristics of all platforms and channels using ISO/IEC 24727 that connect the client-application to the card-application

3.12
proxy
application programming interface implementation that conveys action requests and parameters to a layer implementation located elsewhere

3.13
TC_API
application programming interface used by components of an ISO/IEC 24727 stack to effect the stack's instantiation in a network environment

3.14
trusted-channel
channel that explicitly assures the confidentiality, integrity and authenticity of information during the transfer process, independent of the characteristics of the transfer mechanism or media

3.15
trusted-path
connection between a client-application and a card-application in which all platforms and channels have security characteristics as defined by the client-application

4 Abbreviated terms

TLS	-	transport layer security
CC	-	cryptographic checksum
CG	-	cryptogram
D	-	decipher
DES	-	data encryption standard
DO	-	data object
E	-	encipher
K	-	key
Le	-	expected length
MAC	-	message authentication code
SSC	-	send sequence counter
API	-	application programming interface
APDU	-	application protocol data unit

5 Architecture specialization

ISO/IEC 24727-1, ISO/IEC 24727-2 and ISO/IEC 24727-3 define an architecture, application programming interface and a command-set communication message structure and protocol through which a client-application can access information and computation services from a card-application. The objective of ISO/IEC 24727 is to achieve interoperability among diverse implementations of card-applications and client-applications. ISO/IEC 24727-1 specifies the overarching architecture of ISO/IEC 24727. ISO/IEC 24727-2 specifies a generic request set through which card-application services may be accessed. ISO/IEC 24727-3 specifies the application interface through which client-applications shall access services provided by card-applications. The architectural overview of ISO/IEC 24727 as illustrated in Figure 1 envisions a variety of implementations that can satisfy the standard in sufficient detail to successfully conform to the testing procedures which will be specified in ISO/IEC 24727-5.

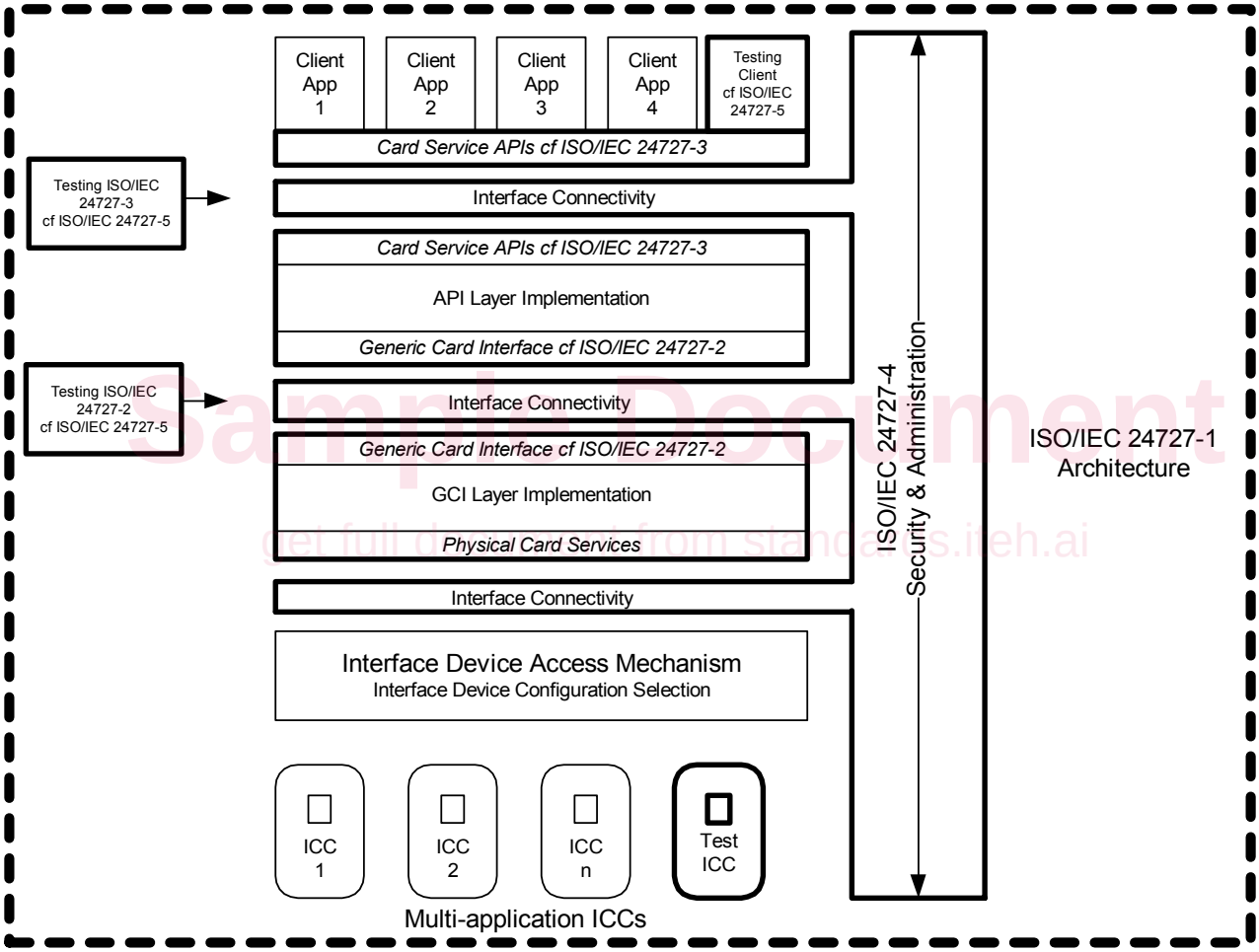


Figure 1 — Specialization of the ISO/IEC 24727 Architecture

This part of ISO/IEC 24727 details the stack instantiation and operational procedures that provide for the preparation and use of a card-application to provide information storage, retrieval and associated processing for client-applications.

This part of ISO/IEC 24727 does not mandate a specific implementation methodology, but it does provide a detailed definition of information organization and content to be supported by any conformant implementation. An ISO/IEC 24727 conformant stack shall instantiate at least one of the configurations defined in Clause 5.

This clause specifies a variety of instantiation configurations of the ISO/IEC 24727 protocol stack. The spectrum of configurations range from the full-network-stack to the loyal-stack. The opaque-ICC-stack is a

configuration in which the ISO/IEC 24727-2 instantiation shall be tightly coupled to the card-applications that it can support; tightly coupled meaning that the connection to the card-application containing ICC through operating system specific code for accessing an interface device is encompassed by the ISO/IEC 24727-2 instantiation. The remote-loyal-stack considers a configuration in which a loyal-stack shall be utilized on a platform that is remote from the client-application. The ICC-resident-stack considers a card-application that shall support the ISO/IEC 24727-3 layer implementation. Finally, the remote-ICC-stack discusses a stack in which the physical connection of the ICC shall be made to a different platform from the rest of the stack.

It is noted that all parts of ISO/IEC 24727 are neutral with respect to the physical interconnection mechanism used to complete a communication channel(s) from the client-application to the card-application. Consequently, references to ICC should be interpreted as being equally applicable to PICC or to non-card resident card-applications and that references to IFD are equally applicable to PCD or other card-application containing platform interfaces.

Figure 2 illustrates the generic elements of an ISO/IEC 24727 protocol stack.

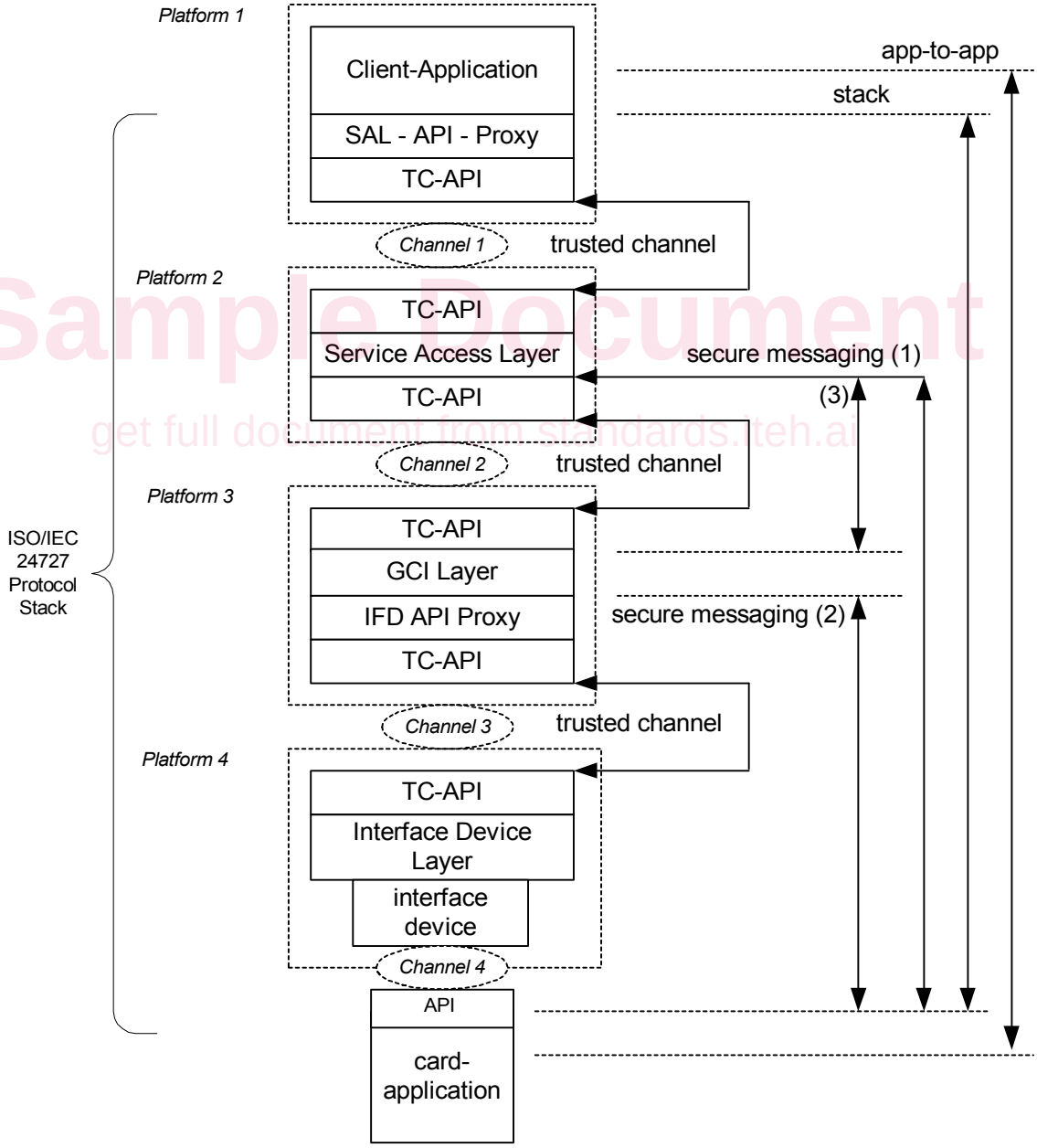


Figure 2 — Generic Elements of the ISO/IEC 24727 Stack

These elements define a general stack configuration. This general stack configuration allows a full ISO/IEC 24727 compliant stack to be segmented across a range of one to four distinct computer platforms. In Figure 2, these platforms are designated as Platform 1, 2, 3 & 4 respectively.

In a fully segmented stack, four distinct communication channels are required to connected the components that comprised the stack. These channels are designated as Channel 1, 2, 3 & 4 respectively. In Clause 5.1 through Clause 5.6, six distinct stack configurations are specified. These comprise the set of allowed ISO/IEC 24727 conformant stacks. A conformant ISO/IEC 24727 stack instantiation shall encompass at least one of these six stack specifications. A conformant ISO/IEC 24727 stack instantiation may encompass more than one of these six stack configurations.

Figure 3 provides a descriptive legend to be used in interpreting the details of the remaining figures in Clause 5.

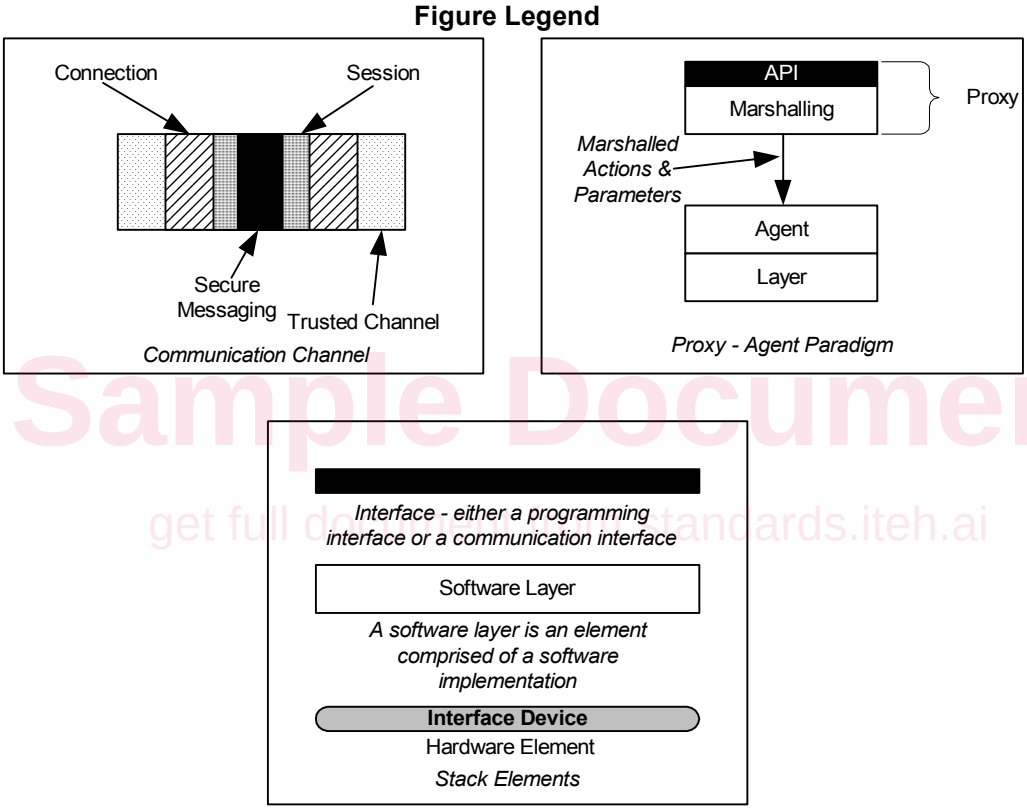


Figure 3 — Legend for Following Figures

A proxy and agent pair (of processes) allow the extension of an API from one point in a stack to a different point by conveying the action requests and associated parameters through a standard description; a procedure known as "marshalling".

5.1 Full-network-stack

A general interconnection between a client-application and a card-application allows each component of the stack to be connected to its adjacent components by way of a network connection, as illustrated in Figure 4.

The full-network-stack configuration of ISO/IEC 24727 entails a segmentation of the ISO/IEC 24727 stack into its interoperable constituent components. While it may be unlikely that such a stack configuration shall be used in a routine operational setting, by testing conformance of this configuration, a fine level of granularity of component interoperability can be confirmed.

Realization of a full-network-stack shall be effected through static network configurations of the various components. Dynamic process invocation of the components is not required by ISO/IEC 24727. The establishment of end-to-end security characteristics shall be effected through parameters passed through the ISO/IEC 24727-3 API. Stack instantiation and operation may subsequently entail out-of-band parameter passing with respect to the ISO/IEC 24727-2 interface, particular in establishing the appropriate keys to enable subsequent secure messaging between the ISO/IEC 24727-2 layer implementation and the card-application.

Corresponding stack establishment and connection (and session) security characteristics establishment shall be met by instantiations of all other stack configurations specified in the various sub-clauses of Clause 5.

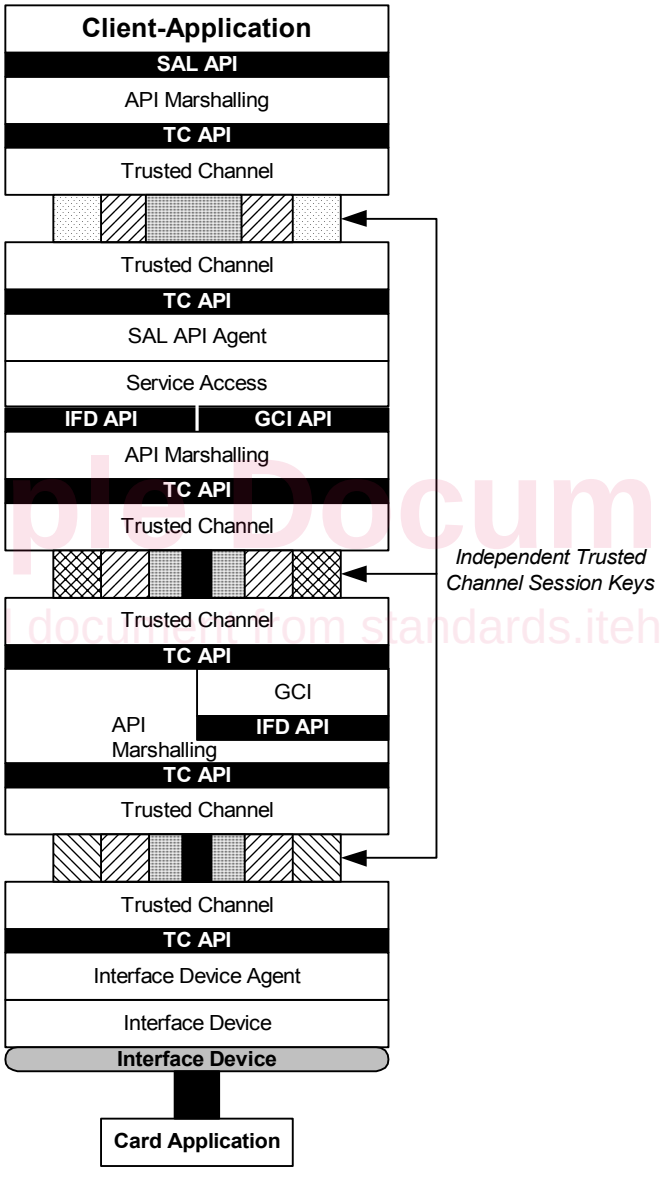


Figure 4 — Networked Connections Between Client-Application and Card-Application

In Figure 4, the client-application to SAL-API proxy connection is effected by a loyal-channel. All other communication channels indicated in the figure are dubious-channels. If the path-protection-policy invoked by the client-application specifies an increased level of security beyond a dubious-channel for any communication channel, then this level shall be achieved through the use of trusted-channels or, if applicable, through the use of secure messaging.

The ISO/IEC 24727-3 implementation, ISO/IEC 24727-2 implementation and card broker implementations all comprise components that shall be effected on trusted platforms if the entire stack is to be viewed as a secure category beyond a level of intrinsic security and discussed in Clause 6.

5.2 Loyal-stack

As illustrated in Figure 5, a loyal-stack is an implementation of the complete ISO/IEC 24727 stack on a loyal-platform, hence using loyal-channels for all connections except for any connection to an ICC via an interface device. For the operating system specific interface device API layer, an enhanced security category shall be achieved for communication via the interface device to the card-application through the use of secure messaging.

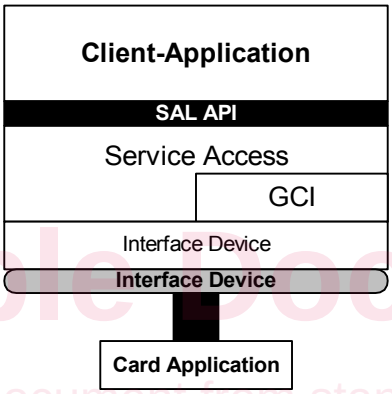
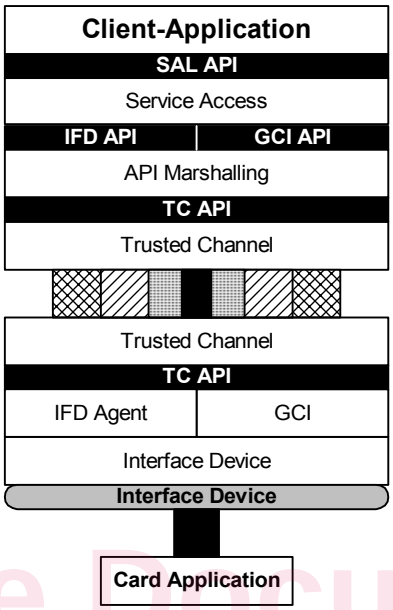


Figure 5 — Proprietary Implementations of ISO/IEC 24727-2 & ISO/IEC 24727-3 Layers

A loyal-stack shall effect either an intrinsic path-protection-policy category, as defined in Clause 6, or be completely instantiated in a loyal environment with the only possible dubious-channel being the connection of the stack to the card-application via an interface device using secure messaging as noted above. The use of the TC_API is not mandatory when running a secure channel within a Loyal Stack.

5.3 Opaque-ICC-stack

An opaque-ICC-stack incorporates the ISO/IEC 24727-2 layer instantiation and the interface device layer instantiation into a single component. This component encompasses the operating system specific connection via an interface device with the card-application. This component shall exist as a static network accessible process in which its trusted-channel layer shall present itself as the server component (see IETF RFC 2246) in the negotiation of a trusted-channel.



Stack Configuration

Figure 6 — Opaque ICC Stack

The keys through which to effect secure messaging between the ISO/IEC 24727-2 layer instantiation and the card-application shall be obtained through the procedural element invoked during the ISO/IEC 24727-2 layer's bootstrap operation as specified in ISO/IEC 24727-2.