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*