INTERNATIONAL STANDARD

ISO/IEC 24727-6

First edition
2010-12-15

Identification cards — Integrated circuit card programming interfaces —

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

Cartes d'identification — Interfaces programmables de cartes à puce —

Partie 6: Procédures de l'autorité d'enregistrement des protocoles d'authentification pour l'interopérabilité

Reference number
ISO/IEC 24727-6:2010(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 24727-6 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 procedures*

— *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 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. This document specifies a language independent and implementation independent application level interface that allows information and transaction interchange with a card. The Open Systems Interconnect Reference Model [ISO/IEC 7498-1:1994] is used as the layered architecture of the Application Interface. That is, the Application Interface assumes that there is a protocol stack through which it will exchange information and transactions among cards using commands conveyed through the message structures defined in ISO 7816. The semantics of commands accessed by the Application Interface refers to application protocol data units (APDUs) as characterized 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 purpose of this part of ISO/IEC 24727 is to maximize the applicability and solution space of software tools that provide Application Interface support to card-aware applications. This effort includes supporting the evolution of card systems as the cards become more powerful peer-level partners with existing and future applications while minimizing the impact to existing solutions conforming to this part of ISO/IEC 24727.

This part of ISO/IEC 24727 extends the function of ISO/IEC 24727-3, Annex A authentication protocols (APs), by providing a means for publication and management of an interoperable framework for new or modified APs using a standardized ISO/IEC registration authority (RA).

APs submitted carry no warranty or guarantee in regard to their fitness for any purpose including security. It is incumbent on the end user to ascertain the APs suitability for the purpose proposed, including the validity of any claims made by the applicant.

Identification cards — Integrated circuit card programming interfaces —

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

1 Scope

This part of ISO/IEC 24727 defines the procedures for

— registration of APs, including related cryptographic algorithms, test methods and conformance assessment criteria, and

— registration of the adoption of ISO/IEC 24727 APs by parties desiring to advertise AP interoperability.

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

ISO/IEC 9834-2, *Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities — Part 2: Registration procedures for OSI document types*