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/IEC 2014



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **3**
5 Interoperability ... **3**
6 Architecture ... **4**
6.1 General ... 4
6.2 Architectural attributes ... 4
6.3 Logical architecture ... 4
6.4 Protocol independence ... 5
6.5 Client-application service access layer interface ... 6
6.6 Capability description ... 6
6.7 Data model ... 6
6.8 Generic card interface ... 7
6.9 Connectivity interface ... 7
6.10 Trusted channel interface ... 7
7 Security rationale ... **7**
Annex A (informative) **Implementation configuration examples** ... **8**
Bibliography ... **18**

© ISO/IEC 2014 – All rights reserved

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*

 © ISO/IEC 2014 – All rights reserved

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.

© ISO/IEC 2014 – All rights reserved

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

© ISO/IEC 2014 – All rights reserved