INTERNATIONAL STANDARD

ISO/IEC 24727-3

First edition
2008-12-01

Identification cards — Integrated circuit card programming interfaces —

Part 3: Application interface

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

Partie 3: Interface d'application

Reference number
ISO/IEC 24727-3:2008(E)

© ISO/IEC 2008

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing 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

 © ISO/IEC 2008 – All rights reserved

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 3

5 Organization for interoperability 4
5.1 General 4
5.2 Computation model 4
5.3 Entity relationships on the application interface 5
5.4 Security model 13

6 Card-application-service access 16
6.1 General 16
6.2 Initialize 16
6.3 Terminate 17
6.4 CardApplicationPath 18

7 Connection service 19
7.1 General 19
7.2 CardApplicationConnect 20
7.3 CardApplicationDisconnect 21
7.4 CardApplicationStartSession 22
7.5 CardApplicationEndSession 23

8 Card-application service 24
8.1 General 24
8.2 CardApplicationList 25
8.3 CardApplicationCreate 26
8.4 CardApplicationDelete 27
8.5 CardApplicationServiceList 28
8.6 CardApplicationServiceCreate 29
8.7 CardApplicationServiceLoad 30
8.8 CardApplicationServiceDelete 31
8.9 CardApplicationServiceDescribe 32
8.10 ExecuteAction 33

9 Named data service 34
9.1 General 34
9.2 DataSetList 35
9.3 DataSetCreate 36
9.4 DataSetSelect 37
9.5 DataSetDelete 38
9.6 DSIList 39
9.7 DSICreate 40
9.8 DSIDelete 41
9.9 DSIWrite 42
9.10 DSIRead 43

10 Cryptographic service 44
10.1 General 44
10.2 Encipher 45

© ISO/IEC 2008 — All rights reserved

10.3 Decipher 46
10.4 GetRandom 47
10.5 Hash 48
10.6 Sign 49
10.7 VerifySignature 50
10.8 VerifyCertificate 51

11 Differential-identity service 52
11.1 General 52
11.2 DIDList 53
11.3 DIDCreate 54
11.4 DIDGet 55
11.5 DIDUpdate 56
11.6 DIDDelete 57
11.7 DIDAuthenticate 58

12 Authorization service 59
12.1 General 59
12.2 ACLList 60
12.3 ACLModify 61

Annex A (normative) **Authentication protocols** 62
A.1 General 62
A.2 Common Definitions 63
A.3 Simple Assertion 64
A.4 Asymmetric Internal Authenticate 66
A.5 Asymmetric External Authenticate 69
A.6 Symmetric Internal Authenticate 72
A.7 Symmetric External Authenticate 75
A.8 Compare 78
A.9 PIN Compare 81
A.10 Biometric Compare 84
A.11 Mutual Authentication with Key Establishment 87
A.12 Client-Application Mutual Authentication with Key Establishment 90
A.13 Client-Application Asymmetric External Authenticate 93
A.14 Modular Extended Access Control Protocol (M-EAC) 96
A.15 Key Transport with mutual authentication based on RSA 100
A.16 Age Attainment 104
A.17 Asymmetric Session Key Establishment 107
A.18 Secure PIN Compare 114
A.19 EC Key Agreement with Card-Application Authentication 118
A.20 EC Key Agreement with Mutual Authentication 122
A.21 Simple EC-DH Key Agreement 128
A.22 GP Asymmetric Authentication 132
A.23 GP Symmetric Authentication (Explicit Mode) 138
A.24 GP Symmetric Authentication (Implicit Mode) 142

Annex B (normative) **Cryptographic algorithms** 145
B.1 Interoperability requirements 145
B.2 Symmetric Algorithms 146
B.3 Asymmetric Algorithms 149
B.4 Elliptic Curve Algorithms 150
B.5 Hash Functions 151
B.6 Message Authentication Codes 152
B.7 Key Establishment 153

Annex C (normative) **ASN.1 Representation** 154
C.1 General 154

Bibliography 193

 © ISO/IEC 2008 — 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.

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 24727-3 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*

© ISO/IEC 2008 — All rights reserved

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. This part of ISO/IEC 24727 specifies a language-independent and implementation-independent application level interface that allows information and transaction interchange with a card. ISO/IEC 7498-1 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/IEC 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 standards:

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

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

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

The goal 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.

© ISO/IEC 2008 — All rights reserved

Identification cards — Integrated circuit card programming interfaces —

Part 3: Application interface

1 Scope

This part of ISO/IEC 24727 defines services as representations of action requests and action responses to be supported at the client-application service interface. The services are described in a programming-language-independent way.

This part of ISO/IEC 24727 is the application interface of the Open Systems Interconnection Reference Model defined in ISO/IEC 7498-1. It provides a high-level interface for a client-application making use of information storage and processing operations of a card-application as viewed on the generic card interface.

This part of ISO/IEC 24727 does not mandate a specific implementation methodology for this interface.

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 7816-11, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

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*

IETF RFC 2141, *URN Syntax,* May 1997

© ISO/IEC 2008 — All rights reserved