

---

---

**Identification cards — Integrated circuit  
card programming interfaces —**

**Part 5:  
Testing procedures**

*Cartes d'identification — Interfaces programmables de cartes à puce —  
Partie 5: Essais*

**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 2011

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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

Foreword .....	vi
Introduction.....	vii
1 Scope .....	1
2 Normative references .....	1
3 Terms and definitions .....	2
4 Symbols and abbreviated terms .....	3
5 Testing methodology .....	4
5.1 Terms of testing .....	4
5.1.1 Purpose of testing .....	4
5.1.2 Testing objective .....	4
5.1.3 Testing Principles.....	4
5.1.4 GCI under test:.....	6
5.1.5 SAL under test:.....	6
5.1.6 Conformance attainment .....	7
5.2 Conformance vector.....	8
5.3 Structure of tests .....	10
5.4 Test environment.....	12
5.4.1 Stack configurations .....	12
5.4.2 Card-application emulators .....	12
5.4.3 Verification and logging capability of components .....	12
5.4.4 Procedural element .....	12
6 Components.....	12
6.1 Service access layer API .....	12
6.1.1 Basic tests .....	12
6.1.2 Discoverability tests.....	12
6.2 Generic card interface.....	15
6.2.1 Basic test.....	15
6.2.2 Processing tests .....	15
6.2.3 Discoverability tests.....	17
6.2.4 Generic card interface acted on ISO/IEC 24727-2 implementation (i.e. CLA = "FF") .....	18
6.3 Interface device API .....	19
6.4 Trusted channel API.....	19
6.4.1 TC_API_Open.....	19
6.4.2 TC_API_Close .....	19
6.4.3 TC_API Write .....	19
6.4.4 TC_API Read .....	19
6.5 SAL on-card implementation component testing .....	20
7 Authentication protocols .....	20
7.1 General .....	20
7.2 SAL security test sequences .....	21
7.2.1 Cryptographic operations .....	22
7.2.2 Simple assertion.....	26
7.2.3 Asymmetric internal authenticate.....	27
7.2.4 Asymmetric external authenticate.....	28
7.2.5 Symmetric internal authenticate.....	30
7.2.6 Symmetric external authenticate .....	31
7.2.7 Compare .....	33
7.2.8 PIN compare.....	35

7.2.9	Biometric compare .....	36
7.2.10	Mutual authentication with key establishment .....	37
7.2.11	Client-application mutual authentication with key establishment .....	39
7.2.12	Client-application asymmetric external authenticate .....	41
7.2.13	Modular extended access control protocol (M-EAC) .....	43
7.2.14	Key transport with mutual authentication based on RSA .....	45
7.2.15	Age attainment .....	47
7.2.16	Asymmetric session key establishment .....	48
7.2.17	Secure PIN compare .....	49
7.2.18	EC key agreement with card-application authentication .....	51
7.2.19	EC key agreement with mutual authentication .....	52
7.2.20	Simple EC-DH key agreement .....	54
7.2.21	GP asymmetric authentication .....	55
7.2.22	GP symmetric authentication (explicit mode) .....	56
7.2.23	GP symmetric authentication (implicit mode) .....	58
8	Secure messaging .....	60
9	Marshalling .....	61
9.1	ASN.1 representation .....	61
9.2	Web-services representation .....	61
10	Stack configuration testing .....	61
10.1	Testable interface definitions .....	61
10.1.1	Full-network-stack .....	63
10.1.2	Loyal-stack .....	64
10.1.3	Opaque-ICC-stack .....	65
10.1.4	Remote-loyal-stack .....	66
10.1.5	ICC-resident-stack .....	67
10.1.6	Remote-ICC-stack .....	68
11	Operational testing .....	68
11.1	SAL test sequences .....	69
12	Operational test reporting .....	69
13	ISO/IEC 24727-6 authentication protocol testing .....	69
13.1	SAL test sequences .....	70
13.1.1	ISO/IEC 24727-6 defined authentication protocol .....	70
13.2	Reference model implementations .....	70
13.2.1	Off card-application .....	70
13.2.2	Card-application emulator or test card use .....	70
Annex A	(normative) SAL operational test sequence descriptions .....	71
A.1	Application management – alpha card-application data structure construction .....	71
A.2	Application management – first application data structure construction .....	92
A.3	Application management – application data structure construction error conditions .....	148
A.4	Application management – second application data structure construction .....	163
A.5	Data manipulation - card application path .....	207
A.6	Data manipulation – general .....	215
A.7	Data manipulation - global authentication .....	255
A.8	Application management - data structure destruction .....	282
Annex B	(informative) Envelope APDU implementation ICC-Resident stack expected component test inputs and outputs .....	326
B.1	Application management - alpha card-application data structure construction .....	326
B.2	Application management - first application data structure construction .....	434
B.3	Application management - application data structure construction error conditions .....	755
B.4	Application management - second application data structure construction .....	907
B.5	Data manipulation - card application path .....	1156
B.6	Data manipulation – general .....	1271
B.7	Data manipulation - global authentication .....	1633
B.8	Application management - data structure destruction .....	1913

<b>Annex C</b> (informative) <b>Non ICC-Resident stack expected component test inputs and outputs</b> .....	<b>2346</b>
<b>C.1</b> Application management - alpha card-application data structure construction.....	<b>2346</b>
<b>C.2</b> Application management - first application data structure construction .....	<b>2443</b>
<b>C.3</b> Application management - application data structure construction error conditions .....	<b>2734</b>
<b>C.4</b> Application management - second application data structure construction.....	<b>2884</b>
<b>C.5</b> Data manipulation - card application path.....	<b>3112</b>
<b>C.6</b> Data manipulation – general .....	<b>3228</b>
<b>C.7</b> Data manipulation - global authentication.....	<b>3579</b>
<b>C.8</b> Application management - data structure destruction.....	<b>3855</b>
<b>Annex D</b> (informative) <b>TLS implementation ICC-Resident stack expected component test inputs and outputs</b> .....	<b>4277</b>
<b>D.1</b> Application management - alpha card-application data structure construction.....	<b>4277</b>
<b>D.2</b> Application management - first application data structure construction .....	<b>4329</b>
<b>D.3</b> Application management - application data structure construction error conditions .....	<b>4501</b>
<b>D.4</b> Application management - second application data structure construction.....	<b>4578</b>
<b>D.5</b> Data manipulation – general .....	<b>4711</b>
<b>D.6</b> Data manipulation - global authentication.....	<b>4908</b>
<b>D.7</b> Application management - data structure destruction.....	<b>5060</b>
<b>Annex E</b> (informative) <b>WSDL encoded IFD data structures</b> .....	<b>5307</b>
<b>E.1</b> Establish Context .....	<b>5307</b>
<b>E.2</b> ReleaseContext.....	<b>5308</b>
<b>E.3</b> ListIFDs .....	<b>5308</b>
<b>E.4</b> GetIFDCapabilities.....	<b>5309</b>
<b>E.5</b> GetStatus.....	<b>5310</b>
<b>E.6</b> Wait .....	<b>5312</b>
<b>E.7</b> Cancel.....	<b>5314</b>
<b>E.8</b> ControlIFD .....	<b>5315</b>
<b>E.9</b> Connect .....	<b>5315</b>
<b>E.10</b> Disconnect .....	<b>5316</b>
<b>E.11</b> BeginTransaction .....	<b>5317</b>
<b>E.12</b> EndTransaction .....	<b>5317</b>
<b>E.13</b> Transmit .....	<b>5318</b>
<b>E.14</b> VerifyUser.....	<b>5319</b>
<b>E.15</b> ModifyVerificationData.....	<b>5320</b>
<b>E.16</b> Output.....	<b>5321</b>
<b>E.17</b> SignalEvent.....	<b>5322</b>
<b>Annex F</b> (informative) <b>ISO/IEC 24727-3 C language binding for common definitions</b> .....	<b>5323</b>
<b>Annex G</b> (informative) <b>ISO/IEC 24727-4 C language binding for algorithm definitions</b> .....	<b>5326</b>
<b>Annex H</b> (informative) <b>ISO/IEC 24727-4 C language binding for API and authentication protocol data</b> .....	<b>5329</b>
<b>Annex I</b> (informative) <b>ISO/IEC 24727-4 C language binding for TC-API</b> .....	<b>5374</b>
<b>Annex J</b> (informative) <b>ISO/IEC 24727-4 C language binding for IFD-API</b> .....	<b>5379</b>
<b>Annex K</b> (informative) <b>ISO/IEC 24727 Java language binding for common definitions</b> .....	<b>5396</b>
<b>Annex L</b> (informative) <b>ISO/IEC 24727-3 Java language binding for API and authentication protocol data</b> .....	<b>5398</b>
<b>Annex M</b> (informative) <b>ISO/IEC 24727-3 Java language binding for algorithms</b> .....	<b>5590</b>
<b>Annex N</b> (informative) <b>ISO/IEC 24727-4 Java language binding for TC-API</b> .....	<b>5592</b>
<b>Annex O</b> (informative) <b>ISO/IEC 24727-4 Java language binding for IFD-API</b> .....	<b>5614</b>
<b>Bibliography</b> .....	<b>5656</b>

## 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 24727-5 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 (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, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*, 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 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 specifies an application-independent and implementation-independent testing regimen through which conformance of specific implementations to the relevant part of ISO/IEC 24727 can be confirmed. It is assumed that such testing will be performed through test environments and procedures developed in accordance with this part of ISO/IEC 24727.

# Identification cards — Integrated circuit card programming interfaces —

## Part 5: Testing procedures

### 1 Scope

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.

This part of ISO/IEC 24727 specifies conformance testing procedures designed to determine if interfaces developed with the ISO/IEC 24727 series meet the requirement of ISO/IEC 24727. By conforming to this part of ISO/IEC 24727, interoperable implementations of ISO/IEC 24727 can be realized.

Test procedures for ISO/IEC 24727-2, ISO/IEC 24727-3 and ISO/IEC 24727-4 are described with sufficient detailing in support of ISO/IEC 24727 interoperability requirements, i.e. the connectivity, ISO/IEC 24727 security mechanisms and discovery mechanisms between the client-application and the card-application. This part of ISO/IEC 24727 defines calls on ISO/IEC 24727-3 in an ordered sequence. It also defines the confirmation of integrity of transmitted data by an implementation under test, as well as the syntax of that data received from the implementation under test for the marshalling procedures defined in ISO/IEC 24727-3 and ISO/IEC 24727-4.

For each test procedure, the conditions required for its execution are defined, along with the conditions under which it has to be executed and the expected results. Structures and entities used for the tests, as well as a common set of recurring sequences used for the various procedures, are identified and documented in this part of ISO/IEC 24727.

### 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 24727-2:2008, *Identification cards — Integrated circuit card programming interfaces — Part 2: Generic card interface*

ISO/IEC 24727-3:2008, *Identification cards — Integrated circuit card programming interfaces — Part 3: Application interface*

ISO/IEC 24727-4:2008, *Identification cards — Integrated circuit card programming interfaces — Part 4: Application programming interface (API) administration*