
**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)*

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

Contents

Page

Foreword.....	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions.....	2
4 Abbreviated terms	3
5 Architecture specialization	4
5.1 Full-network-stack	6
5.2 Loyal-stack	8
5.3 Opaque-ICC-stack.....	9
5.4 Remote-loyal-stack	10
5.5 ICC-resident-stack	11
5.6 Remote-ICC-stack	12
6 Security architecture	12
6.1 Path-protection-policy	12
6.2 ACL – ACR mapping.....	14
6.3 Secure messaging	14
6.4 Trusted-channel key administration	15
7 Connection components.....	15
7.1 Action request and response semantics.....	15
7.2 Proxy – Agent Architecture	15
7.3 Trusted-channel Interface.....	16
7.3.1 TC_API_Open request	17
7.3.2 TC_API_Close request	18
7.3.3 TC_API_Read request	19
7.3.4 TC_API_Write request	20
7.3.5 TC_API_Reset request	21
7.3.6 TC_API_GetStatus request	22
7.4 Interface Device API	23
7.4.1 Establish Context.....	24
7.4.2 ReleaseContext	25
7.4.3 ListIFDs	26
7.4.4 GetIFDCapabilities	27
7.4.5 GetStatus	30
7.4.6 Wait.....	32
7.4.7 Cancel	33
7.4.8 ControlIFD	34
7.4.9 Connect.....	35
7.4.10 Disconnect.....	36
7.4.11 BeginTransaction.....	37
7.4.12 EndTransaction	38
7.4.13 Transmit.....	39
7.4.14 VerifyUser	40
7.4.15 ModifyVerificationData	43
7.4.16 Output	45
7.4.17 SignalEvent	47

Annex A (normative) Path-protection Mechanisms	48
Annex B (normative) IFD - API: Web Service Binding	55
Annex C (normative) IFD-Callback-API - Web Service Binding	78
Bibliography	81

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*