BS ISO/IEC 24727-6:2010

BSI Standards Publication

Identification cards — Integrated circuit card programming interfaces

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

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 24727-6:2010

National foreword

This British Standard is the UK implementation of ISO/IEC 24727-6:2010.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2011

ISBN 978 0 580 62871 9

ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 February 2011.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24727-6:2010

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)

Documents
Document Sharing Hub

© ISO/IEC 2010

Full document details: BS ISO/IEC 24727-6:2010

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 2010

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 2010 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24727-6:2010

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols (and abbreviated terms) 2

5 General 2
5.1 Purpose 2
5.2 Dependencies 2
5.3 Authentication protocol OID arcs 3
5.4 Authentication protocol registration 3
5.5 Authentication protocol adoption registration 4

6 Appointment of the registration authority 4

7 Review of applications 5
7.1 Procedure 5
7.2 Response time 5
7.3 Confirmation process 5

8 Content of applications 5
8.1 General 5
8.2 Applications 5
8.3 Maintenance of a web-based register 6

Annex A (normative) **Application for registration of an ISO 24727 registered authentication protocol** 7

Annex B (normative) **Authentication protocol template** 11

Annex C (normative) **Authentication protocol certification form** 15

Annex D (normative) **Registration of authentication protocol adoption application** 18

Annex E (informative) **Registration Authority** 22

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24727-6:2010

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*

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24727-6:2010

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.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24727-6:2010

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24727-6:2010

INTERNATIONAL STANDARD ISO/IEC 24727-6:2010(E)

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: R egistration procedures for OSI document types*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 24727-3, and the following, apply.

3.1
applicant
organization or person requesting registration

3.2
authentication-protocol-adoption
use of ISO/IEC 24727-3 or ISO/IEC 24727-6 APs (either in operations or referenced in dependent specifications or standards or recommendations)

3.3
registration authority
organization nominated and appointed by the ISO/IEC Technical Management Board to prepare and maintain ISO/IEC 24727-6 registers

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24727-6:2010

3.4
registrant
organization or person that has either registered an authentication protocol or registered the adoption of an authentication protocol

4 Symbols (and abbreviated terms)

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 24727-3, and the following, apply.

AP authentication protocol

APDU application protocol data unit

APT authentication protocol template

APTP authentication protocol test plan

OID object identifier

RA registration authority

RAP registered authentication protocol

URL uniform resource locator

5 General

5.1 Purpose

This part of ISO/IEC 24727 defines the ISO procedures for:

— the registration of new or revised APs in accordance with ISO/IEC 24727-3 and this part. These APs are extensions to the ISO/IEC 24727-3, Annex A suite of APs;

— registration of related cryptographic algorithms, APTP and conformance assessment criteria;

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

5.2 Dependencies

This part of ISO/IEC 24727 relies on two other parts of the ISO/IEC 24727 standards suite:

— ISO/IEC 24727-3:

  — a standardized method for the un-ambiguous description of a range of differing APs;

  — a standardized method for the un-ambiguous description of a range of differing cryptographic algorithms used by the APs.

— ISO/IEC 24727-5: [to be published]

  — a standardized method for the conformance testing of a range of differing APs;

  — the testing requirements for an authentication protocol.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24727-6:2010

5.3 Authentication protocol OID arcs

The OID method set out in ISO/IEC 24727-3 is limited to the standards arc of ISO/IEC 9834-2 and does not support the extension of the arc by registration authority procedures.

This part extends these capabilities using a registration authority arc in order to manage the full extensibility and interoperability requirements for new ISO/IEC 24727 APs under the ISO/IEC 9834-2 registration authority arc.

The ISO 24727-6 Registration Authority arc is {iso(1) registration-authority (1) iso24727(24727) part6(6) *new-protocol-short-name* (*new-protocol-number*)}

5.4 Authentication protocol registration

In order for implementations of ISO/IEC 24727 using different APs to achieve interoperability, there is a need to unambiguously identify the implemented APs.

In order to achieve interoperability with a range of APs, implementers require the details of APs to be published in a form which may be referenced. This clause provides a procedure for the registration of APs, and for those registration details to be made publicly available at a URL, in a format managed by an ISO/IEC RA.

5.4.1 Authentication protocol registration procedures

The procedure supported by this part is compliant with the ISO/IEC 9834-2 ASN.1 Object Identifier (OID) method. The registration and procedural requirements for registration of APs are as follows and occur in sequence:

— the applicant duly completes all documents which form part of the AP registration;

— the RA checks the AP registration for completeness and that the documentation provided indicates compliance with this standard. The RA is only responsible for the administrative operations for the purpose of maintenance of the register which does not include technical content contained in the applicant' s application;

— should there be doubt about any data submitted, or the completeness or accuracy or consistency or ownership of the application then the RA shall initiate an investigation where any doubt exists. The RA should initially consult with the applicant;

— if all requirements are met then the application is accepted and the applicant so advised by the RA;

— if the RA determines that the AP application is not complete or does not meet the requirements of this standard then the applicant is so advised and given the opportunity to revise and re-apply subject to conditions set out in the conditions for application set by the Registration Authority;

— when the application is successful the RA allocates an OID using ISO/IEC 9834 procedures and advises the applicant that they are the formal registrant of the allocated OID from the date of first publication;

— the RA includes the new AP and registrant details in a publicly available and up-to-date database of registered OIDs and ISO/IEC 24727-6 APs on the Internet in a web based service. Details are provided in Annex E;

— once the registration has been successful, the registrant may optionally flag the registration as " Draft Only" , for a period determined by the registrant. In this case, details of the AP set out in Annex B may be changed by the registrant until such time that the registrant advises the RA that the AP should be published as " Final" . Once the AP been published as " Final" there shall be no further changes to the applicants technical representation of the AP (as set out in Annex B);

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24727-6:2010