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)

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 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

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*

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.

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: Registration 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

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.

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);

- the public records of the registered authentication protocol shall remain until such time as the registrant requests that they be withdrawn subject to the terms of the conditions for application of the Registration Authority;
- subject to the conditions for application of the Registration Authority registration status may be changed to "pending de-registration". The RA shall advise all registrants of any procedures relating to the status change of the protocol".

5.5 Authentication protocol adoption registration

In order for operations, specifications, standards or recommendations to achieve interoperability under ISO/IEC 24727 it is necessary for interchangeable components to utilise standardized authentication protocols and applicable cryptographic algorithms.

This clause provides a procedure for the registration of authentication-protocol-adoption by a party, parties or groups including communities of interest.

5.5.1 Authentication protocol adoption registration procedures

The method 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 authentication-protocol-adoption are as follows and occur in sequence:

- the applicant completes the application form in Annex D and submits it in accordance with the conditions for application of the RA;
- the RA evaluates the application to determine if it is both complete and the documentation provided indicates compliance with this standard. If it meets all requirements then it shall be accepted and the applicant so advised;
- if the RA determines that the application is not complete or does not meet the requirements of this standard then the applicant is advised and given the opportunity to revise and re-apply subject to any additional conditions for application set by the Registration Authority;
- if the application is successful the RA updates a public database (accessible at the RA URL address) with the applicant's details to include the RAP OIDs. The applicant shall be so advised;
- the RA maintains a publicly available and up-to-date copy of the registrants details and adopted RAP OIDs on the Internet in a web based service at the URL address set out in Annex E;
- the public records of the authentication-protocol-adoption will remain current until such time as the registrant requests that they be withdrawn or subject to the conditions for registration of the Registration Authority;
- subject to the conditions for application of the Registration Authority the authentication-protocol-adoption registration status may be changed to "pending de-registration" The Registration Authority shall advise all registrants of any procedures relating to the status change of the authentication-protocol-adoption registration status.

6 Appointment of the registration authority

It is within the mandate of ISO/IEC to organize registration as specified in this standard. In order to do this, ISO/IEC appoints, according to their internal requirements and rules, an organization to act as the RA for this standard.

Contact information for the RA can be found in Annex E.

From time to time RA details may change; consequently ISO also maintains an up-to-date listing of maintenance agencies and registration authorities at the following URL: http://www.iso.org/iso/standards_development/maintenance_agencies.htm

7 Review of applications

7.1 Procedure

In order for an application to be processed, it shall contain sufficient information to enable the applicant to be identified as a bona-fide organization and able to comply with the conditions for application set by the Registration Authority.

The Registration Authority may investigate unclear or incomplete applications which do not follow its conditions for application. If the applicant does not agree to the investigation, the application is rejected.

If the application does not contain the information specified in the conditions for application, the application may be rejected and the applicant notified, citing this sub clause and the specific missing information as the reason for rejection.

If the RA determines that the application is appropriate, then it is put into the confirmation process at clause 7.3.

If the RA determines that the application may not be appropriate, then it shall take any steps contained in its conditions for application.

7.2 Response time

The review of an application under the procedures specified in 7.1 shall normally be completed within 10 working days of the receipt of the application.

7.3 Confirmation process

Details of the successful application shall be recorded on a website maintained by the RA, and the applicant shall be informed of the URL of this site and the OIDs registered.

8 Content of applications

8.1 General

Information required by the RA to conduct the registration process may be submitted by e-mail, facsimile, compact disk or paper copy, or (should the RA chooses to support these options) as a Web-based form or using Web Services protocols. Additional information regarding obligations of the applicants and information regarding applicable laws are contained in the conditions for application of the Registration Authority.

8.2 Applications

The application shall include all the information required by Annexes A, B and C for AP registration and Annex D for AP adoption registration including associated requirements stated in those annexes for the inclusion of documents, indemnities and diagrams.

For AP registration the application forms collect the following information:

1) contact and commercial identification information of the applicant;

2) a completed authentication-protocol-template (derived from ISO/IEC 24727-3 Annex A and B) populated with specific details of the authentication protocol proposed and cryptographic algorithms supported;

3) intellectual property details of the applicant and the AP including patent country and patent number and ownership;

4) an authentication-protocol-test-plan (APTP) populated with specific details required to test the proposed AP according to ISO/IEC 24727-5 [to be published];

5) the Certification form, see Annex C;

6) other comments the applicant requires for publication.

For AP adoption registration the application form collects the following information:

1) contact and commercial information of the applicant;

2) name of the operation, specification, standard or recommendation which uses the RAP OID;

3) the RAP OID to be used;

4) the cryptographic algorithms supported;

5) the ISO/IEC 24727-4 Stack Model supported;

6) other comments the applicant requires for publication.

8.3 Maintenance of a web-based register

The RA shall maintain two registers to include the following:

- registered authentication protocol including the registered OID;
- a register of authentication-protocol-adoption including the OID adopted.

Each entry shall give the identifier information, together with a link to the full details provided in the approved application with the exception of payment related information and signatures.

The RA shall provide a website which displays the contents of the registers. The RA shall be responsible for determining the internal procedures necessary for the maintenance of the register in a timely and appropriate manner.

The RA provides annual reports to the ISO/IEC JTC1/SC 17 Sub-Committee and ISO Secretariat. These are available by request from the Sub-Committee.

Annex A
(normative)

Application for registration of an ISO 24727 registered authentication protocol

To: ISO 24727-6 Authentication Protocol Registration Authority.

Applicants should note that all information provided via this form including all attached details but excluding payments details will be published on the RA web site.

A.1 Contact information of organization requesting RAP

Organization Name:

____

National Business Identification Number:

____

Country and State/Region for business identification purposes:

____

Address:

____

____

____

____

Telephone:

Fax:

E-mail:

A.2 Authorized representative

Name:

Title:

Address:

E-mail:

Signature ____

A.3 Short Identifying name of the RAP proposed

Use the same identifier used in the Registered Authentication-protocol-template.

A.4 Short functional description of the RAP proposed

Full details are separately required in the Registered Authentication-protocol-template.

A.5 Patents applicable to RAP proposed

Is the proposed authentication protocol subject to any patents ?

□ Subject to patent numbers in countries noted below □ Public Domain □ Not subject to patent

□ ISO/IEC Protocol

A.5.1 Patent countries/numbers which apply to the RAP

All known patents should be listed.

A.6 Licence conditions

Are there any conditions which an implementer must comply with in order to utilise the proposed authentication protocol ?

□ See below □ No - Public Domain □ Yes – Contact Licensee □ Yes - Refer ISO/IEC Standard as set out below ☑ Yes – open source – refer details of licence below.

A.6.1 Licence conditions

A.7 Contact for licensing/patent purposes (if different to applicant)

____

____

____

____

____

A.8 Signatories

Signed this day ____________ of the month ______________ of the year __________________________

By: ______________________________ (name) Signature: ______________________________________

Company Seal:

Witnessed by:

By: ______________________________ (name)Signature: ______________________________________

Contact address and phone number of witness

____

____

____

____

Annex B
(normative)

Authentication protocol template

To: ISO 24727-6 Authentication Protocol Registration Authority.

The following APT is derived from ISO/IEC 24727 part 3, Annex A. Applicants should refer to this standard for examples and details of how to complete this template.

B.1 Identification of proposed AP

Suggested short identifying name of the AP proposed.

Use the same identifier used in the Registered Authentication Protocol application form. This should be between 20 and 40 characters. Note that this may be changed by the RA if a name conflict should occur with another previously registered AP.

Short functional description of the AP proposed.

Use the same description used in the Registered Authentication Protocol application form.

Long description of the AP proposed.

This should be informative to the reader so as to assist the selection of AP.

List of other ISO 24727 RAP OID/s used in this proposed AP.

If other ISO/IEC 24727-3 or 24727-6 APs are used within the proposed AP the OID of these should be listed here.

Block diagram of proposed Authentication Protocol.

Attach a JPEG format block sequence diagram, formatted to the style used in ISO/IEC 24727-3, Annex A (an example is provided below). This sequence diagram shall describe the following components:

- client-application;
- ISO/IEC 24727-3 layer implementation;
- card-application component;
- SAL-API interface;
- GCI interface.

This diagram shall set out all significant steps required of the AP to support interoperability.

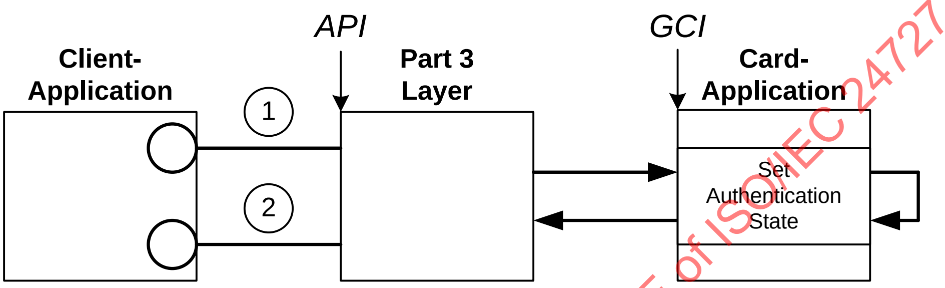

Figure B.1 — Example protocol diagram

B.2 Marker

____

____

Describe the construct using ISO/IEC 24727 part 3 methodology.

B.3 DIDCreate

____

____

Describe the construct using ISO/IEC 24727 part 3 methodology.

B.4 DIDUpdate

____

____

Describe the construct using ISO/IEC 24727 part 3 methodology.

B.5 DIDGet

Describe the construct using ISO/IEC 24727 part 3 methodology.

B.6 Authentication

Describe the protocol in detail using ISO/IEC 24727 part 3 methodology taking care to set out all steps and branches in the protocol as well as clear links to the numbered authentication steps shown in the diagram at B.1.1.

B.7 Encipher

Describe explicitly the expected result of this request.

B.8 Decipher

Describe explicitly the expected result of this request.

B.9 GetRandom

Describe explicitly the expected result of this request.

B.10 Hash

Describe explicitly the expected result of this request.

B.11 Sign

Describe explicitly the expected result of this request.

B.12 Verify Signature

Describe explicitly the expected result of this request.

B.13 VerifyCertificate

Describe explicitly the expected result of this request.

B.14 Testing

Attach either full details of test plans or alternate test methods such as test cards or emulators (including links to supporting material) using the ISO/IEC 24727 part 5 testing methodology for APs.

B.15 Cryptographic algorithm requirement

List the specific cryptographic algorithm/s and their OIDs supported by the protocol.

B.16 Certification

Complete and submit Annex C certification form either as a self-certification or as a certification performed by an independent authority.

For the initial registration of an AP the applicant may self certify. The conditions to meet a registration renewal will be stated in the future amendment to this part of ISO/IEC 24727. In the case of self certification the applicant's assertion shall be based on the assurance that the AP conforms to ISO/IEC 24727.

Annex C
(normative)

Authentication protocol certification form

To: ISO 24727-6 Authentication Protocol Registration Authority.

Applicants should note that all information provided via this form including all attached details but excluding payments details will be published on the RA web site.

C.1 Contact information of certifying organization

Organization Name:

____

National Business Identification Number:

____

Country and State/Region for business identification purposes:

____

Address:

____

____

____

____

Telephone:

____

Fax:

____

E-mail:

____

C.2 Authorized representative

Name:

____

Title:

____

Address:

____

____

____

____

E-mail:

____

Signature ____

C.3 Identifying name of the certified authentication protocol

____

C.4 Certification

Type of certification

<Yes/No> Self Certification (applicant and certifier are the same organization).

<Yes/No> Independent Certification (applicant and certifier are different organizations).

Detail of Certification

<Yes/No> Does the authentication protocol meet the minimum requirements of an authentication protocol as set out in ISO/IEC 24727 part 3.

<Yes/No> Does the test plan in the application for the authentication protocol meet the minimum requirements of an authentication protocol test plan as set out in ISO/IEC 24727 part 5.

<Yes/No > Does the authentication protocol pass the test plans submitted with the application ?

C.5 Signatories

Signed this day ____________ of the month _____________ of the year ___________________________

By: _____________________________ (name) Signature: ______________________________________

Company Seal:

Witnessed by:

By: _____________________________ (name) Signature: ______________________________________

Contact address and phone number of witness.

____

____

____

____

Annex D
(normative)

Registration of authentication protocol adoption application

To: ISO 24727 Authentication Protocol Registration Authority.

Applicants should note that all information provided via this form including all attached details but excluding payments details will be published on the RA web site.

D.1 Contact information of organization

Organization Name:

____

National Business Identification number:

____

Country and State/Region for business identification purposes:

____

Address:

____

____

____

____

Telephone:

____

Fax:

____

E-mail:

____