DRAFT AMENDMENT ISO/IEC 24727-3:2008/DAM 1

ISO/IEC JTC **1** Secretariat: **ANSI**

Voting begins on
2012-04-23

Voting terminates on
2012-09-23

Identification cards — Integrated circuit card programming interfaces —

Part 3: Application interface

AMENDMENT 1

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

Partie 3: Interface d'application

AMENDEMENT 1

ICS 35.240.15

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Copyright notice

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

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 24727-3 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*

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 24727-2 standardizes the use of ISO/IEC 7816-15 data structures as "discovery information" that is communicated throughout the ISO/IEC 24727 stack. This proposed amendment shall enhance the definition of the use of ISO/IEC 7816-15 to fully link the entities defined at the Service Access Layer (API) (e.g. Differential Identity, Authentication Protocol) with typical "on-card" entities such as keys, files and Access Control Rules. Examples shall be provided.

XML encodings have become more and more used in the field of IAS [Identity, Authentication and (digital) Signature] Identity Management and general networking communication. To enhance interoperability with existing networking systems and federated identification and authorization systems (e.g. SAML, OpenID, etc.) standardization of an XML representation of the API and data structures of ISO/IEC 24727-3 is essential.

*This new work item proposal is one of three new work item proposals on the ISO/IEC 24727 series of standards that are envisioned to be developed in parallel.

Identification cards — Integrated circuit card programming interfaces —

Part 3: Application interface

AMENDMENT 1

All new or changed text in this amendment is underlined in the clauses being replaced. All removed text will show with a strike-through. When merging all such text into the base standard, the underlining is to be removed and any words showing a strike-through should be removed. In the case of entirely new annexes relative to the base standard will be so indicated by a statement at the beginning of the annex. In that case, the “underline” convention will NOT be used. Rather, it is to be interpreted that the entire annex wording is to be merged into the base document.

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.

ISO/IEC 24727-3 AMD 1 extends the scope of ISO/IEC 24727-3 in the following ways:

1. Make explicit (normative and informative elements, including examples) of the use of the 7816-15-based Registry. ~~ref wg4n2231~~ XML representation of the 24727-3 API including appropriate web service bindings specified as WSDL-structure. ~~ref wg4n2232~~
2. Reaffirm that ASN.1 is the central definition of the API and data structures. All other bindings and representations are derived from ASN.1
3. ASN.1 and XML representations for 24727-3 shall reside in this part, which may necessitate movement of text/annexes from other parts of 24727 (i.e. 24727-2 and 24727-4 and 24727-5).
4. As a result of Amendments under development for other parts of 24727, portions of this standard may be deleted and referenced.
5. Add to this standard the ISO/IEC 7816-13 application management and life cycle concepts.
6. Add a discovery mechanism to the API to indicate messaging is either ASN.1 or XML.
7. Enhance a Registry facility through which the SAL can record its use of the GCI and through which the GCI mechanisms can be conveyed to the SAL.
8. Consider enhancements to the API to resolve technical deficiencies.
9. Remove ambiguities by elaborating and re-specifying concepts that may not be clear in the current standard.
10. Incorporate concepts that are captured in other parts of ISO/IEC 24727 but are more relevant for ISO/IEC 24727-3.
11. Include C and Java bindings in a Normative Annex (C) and an Informative Annex(Java).

12. Pursue additional mechanisms for discovery and (card and application) capability description based e.g. on XML representations as part the development of a more comprehensive Registry. *This XML is restricted to a set of instructions that enable card recognition for legacy cards.*

Annex D
Web Services Interface Description

[Normative]

This annex is a new addition to ISO/IEC 24727-3.

D.1 - 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.

Amendment 1 to ISO/IEC 24727-3:2008 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Identificaation cards - integrated circuit card programming interfaces*, Subcommittee SC 17, *Application interface*.

- **Clause D.2** contains information for the connection establishment for web service based SAL-communication.
- **Clause D.3** contains an XML-based CardInfo-Structure, which facilitates the support of legacy cards.
- **Clause D.4** contains the XML-specification for the XML-based Service Access Layer Interface

D.2 Connection handling for web service based communication

This clause describes the connection handling for web service based communications in an ISO/IEC 24727-based environment.

D 2.1 General security requirements

The security requirements of ISO/IEC 24727 dictate that the TLS protocol in accordance with RFC 4346 shall be used.

Moreover, public server services shall have access to corresponding X.509 certificates.

When it comes to the security of the communication between the different modules realizing the ECC-3 stack consisting of Service Access Layer (SAL) and IFD Layer), however, X.509 certificates shall be used, whereby the associated private keys shall be adequately protected. Alternatively, anonymous TLS cipher suites, such as `TLS_DH_anon` from RFC 4346 or `TLS_ECDH_anon` from RFC 4492, shall be used, although appropriate security measures need to be taken in the operational environment in order to avert man-in-the-middle attacks while the connection is being established.

In both cases there shall be an exclusive binding of the communication context at application level to the TLS channel which has been established in this process. This communication context is established on connection to the IFD-Layer via the function `EstablishContext` and represented by the `ContextHandle`. When connecting to the SAL, this communication context corresponds to a connection to the card application established by means of `CardApplicationConnect`, which is represented by a `ConnectionHandle`.

As such, one single TLS channel shall be sufficient to establish communication between a SAL and the IFD layer — irrespective of the number of card terminals and connected cards — whereas a separate TLS channel shall be required for every connection to a card application for communication to take place between the identity layer or the application layer and the SAL.

D.2.2 Connections for SOAP binding

When using the SOAP binding, the connection shall be established simply by setting up a TLS-protected channel between the user of the web service (service consumer) and the provider of the web service (service provider) via which web service messages can henceforth be exchanged. In this case the service consumer and service provider take the roles of TLS/http client and TLS/http server, respectively.

D.2.3 Connections for PAOS binding

When using the PAOS binding, however, a more complex process shall be required to establish the connection as, in this case, the TLS/http server acts as the user of the web service (service consumer) with eService because the TLS/http client acts as the provider of the web service (service provider) and shall initiate the connection.

Moreover, in this case there are typically two different TLS channels, and appropriate cryptographic mechanisms shall be used to safeguard their logical relationship while the connection is established.

An example general connection sequence is illustrated in Figure D1.

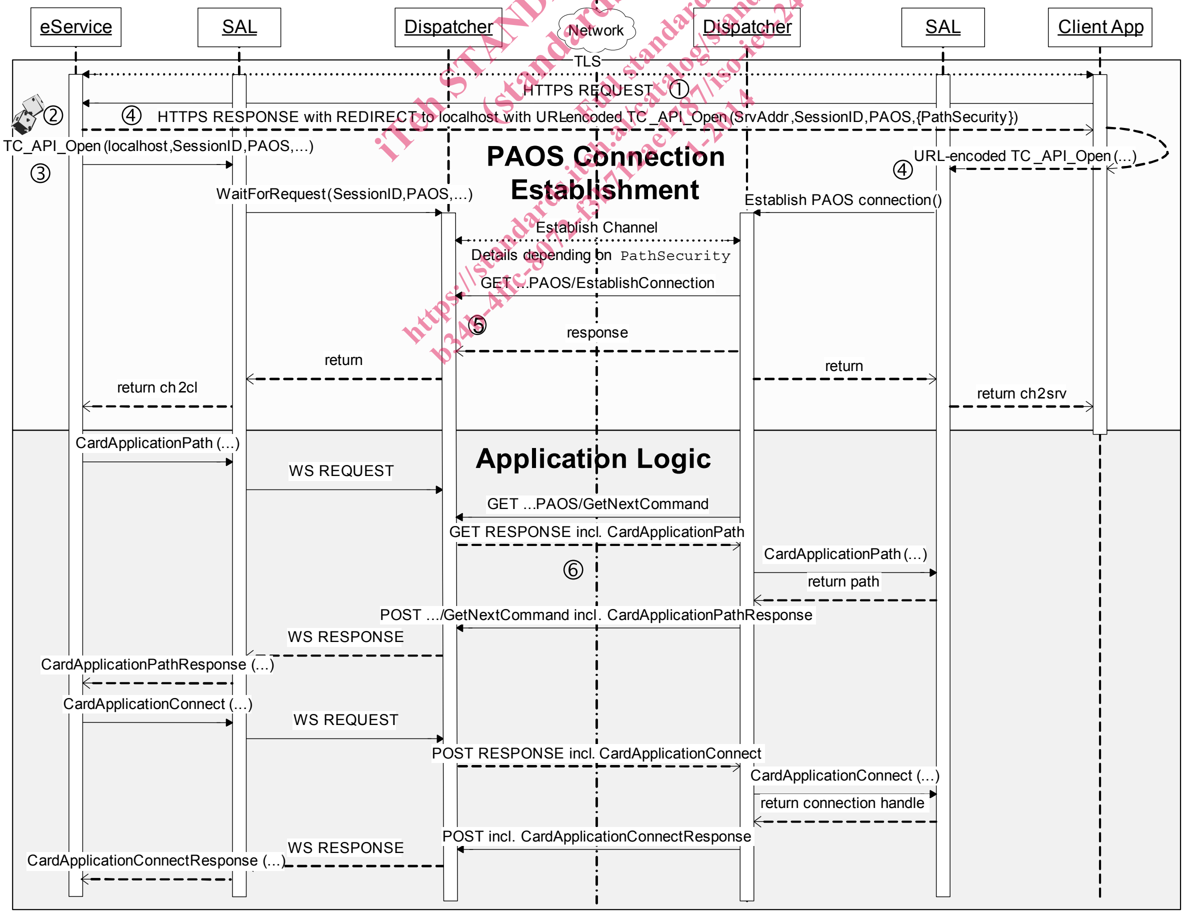
eService
SAL
Dispatcher
Network
Dispatcher
SAL
Client App
TLS
HTTPS REQUEST ①
②
④ HTTPS RESPONSE with REDIRECT to localhost with URL-encoded TC_API_Open (SrvAddr,SessionID,PAOS,{PathSecurity})
TC_API_Open (localhost,SessionID,PAOS,...)
③
PAOS Connection Establishment
④ URL-encoded TC_API_Open (...)
WaitForRequest(SessionID,PAOS,...)
Establish PAOS connection()
Establish Channel
Details depending on PathSecurity
GET ...PAOS/EstablishConnection
⑤
response
return
return
return ch2cl
return ch2srv
Application Logic
CardApplicationPath (...)
WS REQUEST
GET ...PAOS/GetNextCommand
GET RESPONSE incl. CardApplicationPath
⑥
CardApplicationPath (...)
return path
POST .../GetNextCommand incl. CardApplicationPathResponse
WS RESPONSE
CardApplicationPathResponse (...)
CardApplicationConnect (...)
WS REQUEST
POST RESPONSE incl. CardApplicationConnect
CardApplicationConnect (...)
return connection handle
POST incl. CardApplicationConnectResponse
WS RESPONSE
CardApplicationConnectResponse (...)

Figure D1 — Example of a general connection process with PAOS binding

D.3 XML-based CardInfo-Structure for support of legacy cards

D.3.1 Introduction

In order to use the generic Service Access Layer (SAL) interface defined in this standard with legacy cards, it shall be necessary to provide a certain set of information, which allows to map the generic calls at the SAL to card-specific APDUs.

The XML-schema introduced in this clause defines a structure that shall both be used for the specification of card profiles *and* for the mapping of generic calls at the Service Access Interface to card-specific APDUs of legacy cards.

The rest of this annex is structured as follows: Clause D.3.2 provides an overview of the defined structure and explains the top-level element `<CardInfo>`. The following clauses D.3.3 through D.3.7 describe the various child-elements of `<CardInfo>`, Clause E.7 contains the complete XML-schema-definition

D.3.2 Overview

The `CardInfo` structure shall be used for the specification of card profiles *and* for the mapping of generic requests at the Service Access Layer to card-specific APDUs in case of legacy cards, which are not equipped with appropriate ACD and CCD structures according to ISO/IEC 24727-2.

Each card profile shall be described by a `<CardInfo>` element

```
<element name="CardInfo" type="iso:CardInfoType" />
```

of type `CardInfoType` which shall be defined as follows:

```
<complexType name="CardInfoType">
  <sequence>
    <element name="CardType" type="iso:CardTypeType" />
    <element name="CardIdentification" type="iso:CardIdentificationType" />
    <element name="CardCapabilities"
             type="iso:CardCapabilitiesType" maxOccurs="1" minOccurs="0" />
    <element name="ApplicationCapabilities"
             type="iso:ApplicationCapabilitiesType" maxOccurs="1" minOccurs="0" />
    <element name="Signature"
             type="ds:SignatureType" maxOccurs="unbounded" minOccurs="0" />
    </sequence>
    <attribute name="Id" type="ID" use="optional" />
  </complexType>
```

`<CardType> [required]`

Contains a unique identifier for the card type and optionally further links to specification documents. Further details are explained in Clause 0.

`<CardIdentification> [required]`

Allows to determine the type of a given card by traversing an appropriate decision tree and checking whether the characteristic features are as expected. Further details are explained in Clause 0.

`<CardCapabilities> [optional]`

Allows to specify the capabilities of the card. If the card is fully conformant to ISO/IEC 7816 this element MAY be omitted. Further details are explained in Clause 0.

`<ApplicationCapabilities> [optional]`

> Allows to specify the card-applications on the card and shall be used to realize the mapping from SAL-calls to card-specific APDUs. If the necessary information for this mapping is available on the card in adequate CIA-information structures according to ISO/IEC 7816-15 (see Clause 7.5) this element may be omitted. Further details are explained in Clause 0.

`<Signature> [optional]`

Shall be used to protect the integrity and authenticity of (parts of) the `CardInfo`-element. Further details are explained in Clause D.3.3.

D.3.3 CardType

The `<CardType>` element in the `CardInfoType` is of type `CardTypeType` and contains a unique identifier for the card type and optionally further links to specification documents. It is specified as follows:

```
<complexType name="CardTypeType">
  <sequence>
    <element name="ProfilingInfo" maxOccurs="1" minOccurs="0">
      <complexType>
        <sequence>
          <element name="BasisSpecification" type="anyURI" />
          <element name="ProfilingRelation" type="iso:ProfilingType" />
        </sequence>
      </complexType>
    </element>
    <element name="ObjectIdentifier" type="anyURI" />
    <element name="SpecificationBodyOrIssuer"
             type="string" maxOccurs="1" minOccurs="0" />
    <element name="CardTypeName" type="string" maxOccurs="1" minOccurs="0" />
    <element name="Version" maxOccurs="1" minOccurs="0">
      <complexType>
        <sequence>
          <element name="Major" type="string" />
          <element name="Minor" type="string" maxOccurs="1" minOccurs="0" />
          <element name="SubMinor" type="string" maxOccurs="1" minOccurs="0" />
        </sequence>
      </complexType>
    </element>
    <element name="Status" type="string" maxOccurs="1" minOccurs="0" />
    <element name="Date" type="date" maxOccurs="1" minOccurs="0" />
    <element name="CardInfoRepository" type="anyURI" maxOccurs="1" minOccurs="0"/>
           <any namespace="##any" processContents="lax" minOccurs="0"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional" />
</complexType>
```

This type defines the following elements and attributes:

`<ProfilingInfo> [optional]`

> This element shall contain information about a basic specification (`<BasisSpecification>` element) which is extended, profiled or redefined (cf. `<ProfilingRelation>` element below) by the present `CardInfo` structure. Using this element it shall be possible to re-use existing `CardInfo`-structures in a modular approach.

`<ObjectIdentifier> [required]`

> This element shall contain the unique identifier of the card type, which MAY be the object identifier of a profile defined in Part 4 of the present standard.

`<SpecificationBodyOrIssuer> [optional]`

This element may be used to specify the card issuer or the organization, which is responsible for the specification.

`<CardTypeName> [optional]`

This element may contain the name of the card type.

`<Version> [optional]`

This element may contain the version number of the card type.

`<Status> [optional]`

This element may contain information about the state of the present `CardInfo` file (e.g. 'draft').

`<Date> [optional]`

This element may contain the date of creation of the `CardInfo` file.

`<CardInfoRepository> [optional]`

This element may contain the address of a `CardInfo`-repository, which may provide related `CardInfo`-files.

Furthermore there may be some additional element, which structure is defined by some other specification.

The `<ProfilingRelation>` element is of type `ProfilingType` and describes the relation between the basic specification and the present `CardInfo` file.

```
<simpleType name="ProfilingType">
  <restriction base="string">
    <enumeration value="extends" />
    <enumeration value="redefines" />
  </restriction>
</simpleType>
```

The three cases have got the following meaning:

- `extends` – indicates that the present `CardInfo` file is just an extension of the basic specification. All definitions in the basic specification remain valid and the new specifications in the `CardInfo` file just extend them (e.g. a new card application).

- `redefines` – indicates that the elements of the `CardInfo` file overwrite the according elements of the basic specification. Elements of the basic specification not appearing in the `CardInfo` file remain valid.

D.3.4 CardIdentification

The `<CardIdentification>` element, which is part of the `CardInfoType` (cf. Clause 0), allows to determine the type of a given card by traversing the decision tree and checking whether the characteristic features are as expected.

```
<complexType name="CardIdentificationType">
   <sequence>
       <element name="ATR" maxOccurs="unbounded" minOccurs="0"
```