INTERNATIONAL STANDARD

ISO/IEC 24727-5

First edition
2011-03-15

Identification cards — Integrated circuit card programming interfaces —

Part 5: Testing procedures

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

Partie 5: Essais

Reference number
ISO/IEC 24727-5:2011(E)

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 24727-5 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*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
certification
formal confirmation of successful conformance testing by a certified party

3.2
component
executable code comprising a processing layer accessed with ISO/IEC 24727 defined application programming interfaces

[ISO/IEC 24727-4:2008]

3.3
component-under-test
ISO/IEC 24727 component being tested

3.4
conformance-testing
formal demonstration that a component complies with specified critera established by a standard

3.5
conformance-vector
concatenation of the tuple element values

3.6
dimension-of-conformance
tuple element of a conformance-vector

3.7
native-implementation
on-card implementation connected to ISO/IEC 24727-2 layer either directly or via a procedural element

3.8
card-application emulator
processing component accessed through the interface device application programming interface (IFD-API) that simulates the behaviour of a smart card-application

3.9
card emulator
processing component accessed through the interface device application programming interface (IFD-API) that simulates the behaviour of a card

3.10
stack-configuration
series of processing components connected by communication channels that connect a client-application to a card-application as specified by the ISO/IEC 24727-4 protocol stacks

3.11
test-component
ISO/IEC 24727 trusted component that is provided and used by the testee

3.12
test-environment
systems, personnel and standard procedures to perform conformance-testing

3.13
test-implementation
ISO/IEC 24727 stack including the component(s) under test and testing components

3.14
testing-body
organization providing a test-environment, test-implementation and means to perform conformance-testing

4 Symbols and abbreviated terms

ACA	alpha card application
ACD	application capability description
ACL	access control list
AK	asymmetric key
APDU	application protocol data unit
API	application programming interface
AR	access rule
CA	card application
CCD	card capability description
CIA	cryptographic information application
CUT	component under test
DER-TLV	distinguished encoding rules – tag length value
DF	dedicated file
DID	differential identity
DS	data set
DSI	data structure for interoperability
EF	elementary file
GCI	generic card interface
IFD	interface device
MF	master file
PC/SC	personal computer / smart card consortium
RMI	reference model implementation
RFU	reserved for future use
SAL	service access layer

SE security environment

TC test component

TLS transport layer security

5 Testing methodology

ISO/IEC 24727 establishes the facilities for interoperability through the specification of a number of interfaces. Independent implementations of each interface shall be interchangeable and thus provide for interoperability at each interface. Consequently, ISO/IEC 24727 enables a wide variety of interoperability. This part of ISO/IEC 24727 shall provide a methodology for conformance-testing such that distinct interface implementations can be affirmed as being interchangeable with other independent implementations.

The testing methodology assumes a test-environment that presents standard characteristics that include:

1) Equipment configuration interfaces

2) Test-implementations

3) Test-specifications

Given these standard characteristics a testing-body can make use of this test-environment to confirm the behaviour of the various interfaces through which interoperability is enabled.

This part of ISO/IEC 24727 does not test the following:

1) Tests for quality, performance, robustness

2) Testing of standards and protocols that are referenced within

3) Testing of proprietary card application services, their creation and execution

4) Error conditions that cannot be produced by a correctly functioning implementation

5.1 Terms of testing

5.1.1 Purpose of testing

The purpose of ISO/IEC 24727-5 is to provide testing specifications at a level that allow independent testing bodies to conduct testing with the assurance of independent equivalent results.

5.1.2 Testing objective

The objective of ISO/IEC 24727-5 is to specify a testing regimen that enables independent, equivalent implementations. Independent testing bodies can thereby evaluate conformance to ISO/IEC 24727 with equivalent results. Levels of certification can then indicate which component or set of components is ISO/IEC 24727 conformant.

5.1.3 Testing Principles

The testing principles are derived from the ISO/IEC 24727 objective of interoperability. Interoperability is achieved by specifying interfaces and behaviour through which a component is accessed. Since each component is tested independently there will be varying levels of conformance and a distinct set of certification levels will be defined that address single components as well as a concatenation of components that form ISO/IEC 24727 component-configurations.

ISO/IEC 24727-5 defines test configurations and unique parameters to be applied uniformly to each component for different implementations to assure conformance.

It is assumed that automated testing tools can be used for:

- the generation of test data that is used as input and output during testing to ensure that all user data is differs for each test execution;
- consistent definition;
- performance of tests; and
- result reporting.

ISO/IEC 24727 certification is enabled through ISO/IEC 24727-5 tests that can be administered by testing bodies.

Table 1 —Testing Principles

	Principle
1.	To attain conformance, all aspects of the ISO/IEC 24727 interfaces for the Component-under-test shall comply with ISO/IEC 24727.
2.	ISO/IEC 24727-5 testing shall only include behavioural testing at the component interfaces.
3.	Testing shall encompass one or more of the following ISO/IEC 24727 components: i. ASN.1 DER-TLV defined APIs; ii. communication interfaces; iii. C language bindings for API marshalling and binding of the APIs; iv. stack configurations; v. authentication protocols.
4.	A test facility shall provide a reference test implementation that permits a component under test to be tested in a complete stack test configuration.
5.	The use of automated testing tools is assumed for generating tests and to aid the certification process.
6.	ISO/IEC 24727-5 should enable the development of conformance and certification testing abilities to be derived in a consistent manner.
7.	Every component under test shall be subject to tests defined at the ISO/IEC 24727-3 API.
8.	Only services and actions as defined by ISO/IEC 24727-3 shall be tested. The testing of proprietary services, actions and the associated creation and loading of these is out of scope.
9.	Test inputs and results shall vary each time a test is performed in order to ascertain that tests are not predictable.
10.	ISO/IEC 24727-3 testing verifies the request and response of the interface and the APDUs it generates.
11.	ISO/IEC 24727-3 proxy testing verifies the request and response of the interface plus the DER-TLV that it generates.
12.	ISO/IEC 24727-3 (including proxy) tests shall be run against blank and populated (partially provisioned) smart cards.
13.	Interoperability is only fully tested in the C language implementation (until other language binding is provided)
14.	Any other languages shall use an agent to translate the messages (e.g. DER-TLV) into language

	Principle
	specific bindings.
15.	Data transfer over communication channels is intercepted by a "man in the middle" and compared to the test data (protocol analysers).
16.	The only testable interface at the card application is the ISO/IEC 24727-3 on-card implementation.
17.	Only IFD API syntax (i.e. the structure and not the containing data) shall be tested. The testing of data contained within the IFD API syntax is out of scope.
18.	Only TC API syntax shall be tested. The testing of data contained within the TC API syntax is out of scope.
19.	Testing of procedural element low-level coding and functions is out of scope
20.	Testing of other standards that are referenced within ISO/IEC 24727 is out of scope
21.	Testing of other protocols (i.e. not ISO/IEC 24727 authentication protocols) that are referenced within ISO/IEC 24727 is out of scope
22.	Testing of error conditions that cannot be produced by a correctly functioning implementation is out of scope
23.	Testing of proprietary services, actions and the associated creation and loading of these is out of scope.
24.	The standard shall not test application specific software module.
25.	Checking of CIA updates is out of scope.

5.1.4 GCI under test:

The GCI under test shall be submitted to test that shall confirm the following minimum set features:

- Whenever procedural elements are present, all the incoming APDUs that are part of the GCI shall be submitted to these procedural elements. Therefore, the GCI under test capability to handle the request and response APDUs shall be tested. The GCI under test shall pass on the request APDU from SAL to Procedural Elements, and the response APDU from the ICC to procedural elements. The procedural elements testing component shall require a “probe” to prove such APDU processing.

- GCI under test shall be capable to parse CCD and to ensure availability of interoperability data to the SAL. The CCD content shall be retrieved according to the bootstrap mechanism. Some CCD data object values may be loaded from remote location specified in the CCD.

- GCI under test capability to deliver upon request the CCD content to the SAL.

- ISO/IEC 24727-2 interface (request and response) (only for C language binding).

- GCI under test capability to handle request APDUs with CLA=’FF’ (packageA) intended for GCI internal/resources management

- GCI under test capability to forward any APDU that is neither part of ISO/IEC 24727-2 Table 2 nor Table 3 directly to ICC without any processing.

- GCI under test capability to call IFD-API functions.

5.1.5 SAL under test:

The SAL under test shall be submitted to test that shall confirm the following minimum set features:

- SAL shall be able to recover the whole data mapping between off-card data representation an on-card data representation using the CIA containing within the ACD.

- SAL shall be enabled to parse the CIA values and to generate all the discovery data and to encode it according to ISO/IEC 24727-3, Annex C ASN.1 normative definitions.

- Upon or prior to the call to CardApplicationEndSession action, any change impacting the CIA entries (as per ISO/IEC 24727-2) that occurred during the transaction shall be updated in the CIA that is either stored or referenced in the ACD.

- The retrieved (by ISO/IEC 24727-3) CIA must reflect the card implementation and any changes that have been applied.

- ISO/IEC 24727-3 interface (request and response) (only for C language binding), generated APDUs and ASN.1 DER-TLV (for proxies)

- The off-card SAL shall be enabled to act on client-application requests according to the related ACL (e.g denied actions shall not be translated into APDUs)

- SAL claiming compatibility with a given Authentication Protocol shall prove capability to translate generic requests into specific set of request APDUs according to the Protocol OID description and the rest of information provided in the DID bearing this Protocol.

- Authentication protocols that are internal to ISO/IEC 24727-3 are tested using a trusted test implementation below the ISO/IEC 24727-3 layer.

- Authentication protocols that are internal to ISO/IEC 24727-3 are tested using a trusted test ISO/IEC 24727-3 implementation.

- Specified authentication protocol algorithms and their use are verified by the trusted test components.

- DIDCreate and DIDUpdate requests shall uniquely be executed by the SAL according to existing specification of these requests parameters in ISO/IEC 24727-3, Annex A.

- SAL shall be enabled to translate ExecuteAction requests into IFD-API calls without resorting to GCI under test layer. The SAL shall be able to extract the parameter “request” from within ExecuteAction call and to deliver it unchanged as InputAPDU parameter to the Transmit command from IFD-API.

- SAL shall be enabled to process post-issuance personalization data as a separate package of requests. This package is comprised of the following SAL-API calls:

    i) DIDCreate

    ii) DIDUpdate

    iii) DataSetCreate

    iv) DSICreate

5.1.6 Conformance attainment

For a component-under-test to attain conformance all its mandatory features, as defined in all other parts of ISO/IEC 24727, shall be implemented.

All tests contained within ISO/IEC 24727-5 shall be mandatory for each relevant component-under-test.

Distinct tests shall identify the component-under-test interface behaviour.