INTERNATIONAL STANDARD

# ISO/IEC 24727-2

First edition
2008-10-01

# Identification cards — Integrated circuit card programming interfaces —

## Part 2:
## Generic card interface

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

*Partie 2: Interface de carte générique*

Reference number
ISO/IEC 24727-2:2008(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 24727-2 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: API administration*

The following parts are under preparation:

— *Part 5: Testing*

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

## Introduction

ISO/IEC 24727 defines interoperable programming interfaces to integrated circuit cards. Programming interfaces are defined for all card lifecycle stages and for use with integrated circuit cards.

ISO/IEC 24727 is written with sufficient detail and completeness that independent implementations of each part are interchangeable and can interoperate with independent implementations of the other parts.

This part of ISO/IEC 24727 specifies a command-level programming interface to contactless integrated circuit cards and cards with contacts that is a concretization of the concepts, data structures and commands found in the following documents:

- 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*
- ISO/IEC 7816-15, *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application*
- ISO/IEC 20060, *Information technology — Open Terminal Architecture (OTA) specification — Virtual machine specification*

The commands and data objects described in this part of ISO/IEC 24727 are consistent with the commands and data objects found in these documents which will be referred to as the base documents.

This part of ISO/IEC 24727 maximizes the fungibility of independent realizations of its prescriptions. This property of this part of ISO/IEC 24727 is realized by positing a minimally sufficient subset of the base standards which realizes their core functionality through the minimization of the number of options provided.

# Identification cards — Integrated circuit card programming interfaces —

# Part 2:
# Generic card interface

## 1 Scope

This part of ISO/IEC 24727 defines a generic card interface for integrated circuit cards. This interface is presented as:

- command-response pairs for interoperability,
- card and application capability description and determination.

This part of ISO/IEC 24727 is based on ISO/IEC 7816-4, ISO/IEC 7816-8, ISO/IEC 7816-9, and ISO/IEC 7816-15.

## 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 24727-1, *Identification cards — Integrated circuit card programming interfaces — Part 1: Architecture*

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*

ISO/IEC 7816-15, *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 24727-1 and the following apply.

**3.1**
**data object**
information seen at the interface consisting of the concatenation of a mandatory ISO/IEC 8825 DER-encoded tag field, a mandatory ISO/IEC 8825 DER-encoded length field and a conditional value field

**3.2**
**file**
structure for application and/or data in the card, as seen at the generic card interface when processing commands

**3.3**
**translation code**
procedural software that transforms commands on the generic card interface to commands implemented on an integrated circuit card

## 4 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 24727-1 and the following apply.

| | |
|---|---|
| ATS | answer to select, as defined in ISO/IEC 14443-3 |
| DF | dedicated file |
| DO | data object |
| FCP | file control parameters |
| FID | file identifier |
| RFU | reserved for further use |

## 5 Organization for interoperability

This clause specifies a subset of the structure, commands and data structure defined in ISO/IEC 7816-4, ISO/IEC 7816-8 and ISO/IEC 7816-9.

The following can not be specified at the generic card interface:

- short file identifiers;
- logical channels;
- files with record structure.

The physical card mapped to the generic card interface by the translation code may use a short EF identifier, logical channels, and record structure files.

### 5.1 Command-response pairs for interoperability

### 5.1.1 Command and response encoding

Requests at the GCI are logically equivalent to command APDUs as specified in ISO/IEC 7816-4, ISO/IEC 7816-8 and ISO/IEC 7816-9.

Confirmations at the GCI are logically equivalent to response APDUs as specified in ISO/IEC 7816-4, ISO/IEC 7816-8 and ISO/IEC 7816-9.

The following interface may be used to send a generic card interface command directly to an implementation of this part of ISO/IEC 24727:

```
sequence-of-bytes ExecuteCommand(sequence-of-bytes command)
```

This interface sends a command to the ISO/IEC 24727-2 implementation and returns as its value the response of the ISO/IEC 24727-2 implementation.

Further interfaces may be defined in other parts of ISO/IEC 24727.

### 5.1.2 Class byte

Table 1 lists the class byte values that shall be used in commands on the generic card interface.

**Table 1 – CLA Values on the GCI**

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Description |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | 0 | - | - | - | - | The command is the last or only command of a chain |
| 0 | - | - | 1 | - | - | - | - | The command is not the last command of a chain |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | The command is for the Part 2 implementation |

This part of ISO/IEC 24727 shall support command chaining only for the transmission of data strings too long for a single command; i.e. constant INS, P1 and P2 across all commands in the chain.

For transmission of requests acted upon by the ISO/IEC 24727-2 implementation, generally without transmission of APDUs to the card, CLA = 'FF' shall be used.

### 5.1.3 Instruction byte

Tables 2 and 3 list the instruction byte values that should be used in commands at the GCI as these commands guarantee the standardized independence of the ISO/IEC 24727-2 and ISO/IEC 24727-3 implementations.

A GCI request with an INS not found in Table 2 shall be sent directly to the card and the card-interface response shall be returned to the entity having made the GCI request.

Commands with instruction bytes listed in Table 3 shall be acted on by the ISO/IEC 24727-2 implementation and shall not be provided to the translation script.

**Table 2 – Requests on the GCI Handled by the Translation Script**

| Command Name | INS | Package | Limitations |
|---|---|---|---|
| SELECT | ‘A4’ | A | SELECT by file identifier (P1-P2 = ’00-04’ or ’00-0C’) and SELECT by DF name (P1-P2 = ’04-04’ or ’04-0C’) with return of FCP data object or no data shall be supported. (See Note) |
| READ BINARY | ‘B0’ | A | Bit 8 of P1 shall be set to 0. |
| READ BINARY | ‘B1’ | A | P1 and P2 shall be set to ‘00’. |
| UPDATE BINARY | ‘D6’ | A | Bit 8 of P1 shall be set to 0. |
| UPDATE BINARY | ‘D7’ | A | P1 and P2 shall be set to ‘00’. |
| GET DATA | ‘CA’<br>‘CB’ | A | None. |
| PUT DATA | ‘DA’<br>‘DB’ | A | When PUT DATA references a data object that already exists it shall be overwritten. |
| GENERATE ASYMMETRIC KEY PAIR | ‘46’<br>‘47’ | B | Out of scope |
| VERIFY | ‘20’ | A | P2 is not zero. |
| VERIFY | ‘21’ | A | P2 is not zero. |
| CHANGE REFERENCE DATA | ‘24’ | A | None. |

| | | | |
|---|---|---|---|
| GET CHALLENGE | ‘84’ | A | None. |
| INTERNAL AUTHENTICATE | ‘88’ | A | None. |
| EXTERNAL AUTHENTICATE | ‘82’ | A | None. |
| MUTUAL AUTHENTICATE | ‘82’ | A | None. |
| GENERAL AUTHENTICATE | ’86’<br>‘87’ | A | None. |
| PERFORM SECURITY OPERATION: COMPUTE DIGITAL SIGNATURE | ‘2A’ | A | P1=’9E’<br>P2=’9A’<br>Command data field:<br>- Absent (hash value provided via PERFORM SECURITY OPERATION:HASH |
| PERFORM SECURITY OPERATION: VERIFY DIGITAL SIGNATURE | ‘2A’ | A | P1=’00’<br>P2=’A8’<br>Command data field:<br>- DO ‘9E’ |
| PERFORM SECURITY OPERATION: HASH | ‘2A’ | A | P1=’90’<br>P2=’80’ or ’9A’<br>Command data field:<br>1) - DO ‘90’ (intermediate hash value \|\| amount of bits already hashed ) \|\| DO ‘80’ (final text block)<br>or<br>2)- DO ‘90’ hash value |
| PERFORM SECURITY OPERATION:VERIFY CERTIFICATE | ‘2A’ | A | P1-‘00’<br>P2=’AE’ or ‘BE’<br>Command data field:<br>- DO ‘7F21’ (card verifiable certificate) |
| PERFORM SECURITY OPERATION: ENCIPHER | ‘2A’ | A | P1=’86’<br>P2=’80’<br>Command data field: data to be enciphered |
| PERFORM SECURITY OPERATION: DECIPHER | ‘2A’ | A | P1=’80’<br>P2=’86’<br>Command data field: data to be deciphered (PI \|\| cryptogram) |
| MANAGE SECURITY ENVIRONMENT | ‘22’ | A | SET (P1=’x1’) and RESTORE (P1=’F3’) |
| CREATE FILE | ‘E0’ | B | Only FCP data objects in Table 9 are supported. The created file becomes the current file. |
| DELETE FILE | ‘E4’ | B | Only P1-P2 = ’00-00’ is supported. After deletion of the file the parent of the deleted file becomes the currently selected dedicated file. |
| ACTIVATE FILE | ‘44’ | B | Only P1-P2 = ‘00-00’ is supported |
| DEACTIVATE FILE | ‘04’ | B | Only P1-P2 = ‘00-00’ is supported |
| RESET RETRY COUNTER | '2C' | A | None |
| GET RESPONSE | 'C0' | A | Only P1-P2 = '00-00' is supported<br>The status word 6985 means there are no data to retrieve |

Note: In the case of SELECT by DF name with return of the FCP (P1-P2=’04-04’), a returned FCP data object may contain a data object with tag ‘87’ indicating the elementary file that contains the card-application capability description.

**Table 3 – INS Values on the GCI Acted on by the ISO/IEC 24727-2 Implementation (CLA='FF')**

| Command Name | INS | P1 P2 | Package | Limitations |
|---|---|---|---|---|
| COLD RESET | '00' | '0000' | A | Lc absent, Le = '00'. |
| WARM RESET | '00' | '00FF' | A | |
| DEACTIVATE CONTACTS | '00' | '0100' | A | Lc and Le absent |
| DEACTIVATE CONTACTS AND EJECT | '00' | '0200' | A | |
| SELECT PROCEDURAL ELEMENT | 'A4' | '0400' | A | Lc in the range 5..16, Le absent.<br>A standard data field shall be an AID containing the OID of an ISO standard defining the implementation, according to ISO/IEC 7816-4. A data field proprietary to the implementation shall start with 'FX' . |
| GET DATA | CA | | A | Unless the DOs to be transmitted have application-class tags defined in ISO/IEC 7816 or ISO/IEC 24727, the tags shall be of the context-dependent class.<br>When PUT DATA references a data object that already exists, it shall be overwritten. Particular tags in a PUT DATA may trigger the execution of a procedure by the called element. If there is more than one parameter to transmit to the procedure, those parameters shall be transmitted within a constructed DO. According to clause 5.2, the status code '0000' indicates proper execution of the procedure. |
| PUT DATA | DA | | A | |
| LIST READERS | CA | '7F64' | A | Lc absent, Le = '00'<br>Returns the value of DO 7F64.<br>This value is a concatenation of DOs encapsulating reader names in UTF8 format. |

The physical card mapped to the generic card interface by the translation code may use other ISO/IEC 7816 compliant commands.

Instruction values received at the GCI including those in Table 2 may trigger a procedural element in a capability description. See 6.3.

Package A shall be required for operational use. Packages A and B shall be required for card management use.

A successful completion of the RESET command shall reset both the ISO/IEC 24727-2 implementation and the card. The reset of the ISO/IEC 24727-2 implementation shall include setting the CCD and all the ACDs to 'undefined'.

The response data in the R-APDU of the RESET C-APDU shall be the historical bytes of the card ATR, ATS or answer to ATTRIB if they are available. The status words shall be '0000' for successful completion and otherwise '0F00'.

### 5.1.4 File descriptor byte

Table 4 lists the file descriptor byte values that shall be used in the FCP on the GCI. Files seen on the GCI are not shareable.

**Table 4 – File Descriptor Byte Values on the GCI**

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Description |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | Dedicated file |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | Working elementary file, transparent structure |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | Working elementary file, TLV structure for BER-TLV data objects |

## 5.2 Card states for interoperability

Tables 5 and 6 list the states that shall be used in implementations of the generic card interface and describes the state transition events between these states.

**Table 5 – Card and Application States and State Transition Events on the GCI**

| State Name | Always Defined | Type of State Change | State Transition Event |
|---|---|---|---|
| Currently selected application | Yes | **Set** | SELECT by DF name; e.g., application identifier |
| Currently selected dedicated file | Yes | **Set** | SELECT by file identifier of a dedicated file |
| | | **Set** | CREATE FILE with the new dedicated file becoming the currently selected dedicated file |
| | | **Set** | DELETE FILE of the currently selected dedicated file with the new dedicated file becoming the parent of the deleted dedicated file |
| Currently selected elementary file | No | **Set** | SELECT by file identifier of an elementary file |
| | | **Set** | CREATE FILE with the newly created elementary file becoming the currently selected elementary file |
| | | **Unset** | SELECT by DF name |
| | | **Unset** | SELECT by file identifier of a dedicated file |
| | | **Unset** | DELETE FILE of the currently selected elementary file or currently selected dedicated file |
| | | **Unset** | CREATE FILE of a dedicated file |

**Table 6 – Currently selected files after the successful execution of commands on the GCI**

| COMMAND | Current application/DF | Current elementary file |
|---|---|---|
| SELECT by DF name | Change to the specified application/DF | Cleared and non existent |
| SELECT DF by file identifier | Change to the specified DF | Cleared and non existent |
| SELECT EF by file identifier | No change | Change to specified EF |
| CREATE FILE of DF | Change to the specified DF | Cleared and non existent |
| CREATE FILE of EF | No change | Change to the specified EF |
| DELETE FILE of DF | Change to the parent DF in the case of deletion of the currently selected DF | Cleared and non existent in the case of deletion of the DF that have currently selected EF |
| DELETE FILE of EF | No change | Clear and non existent |
| Immediately after the RESET command, the currently selected application/DF shall be MF or the default selected application/DF. The currently selected EF is “cleared and non-existent”. | | |

## 5.3 Status words for interoperability

The status words that shall be used on the generic card interface are listed in Table 7.

**Table 7 – Status Words for Interoperability**

| | Symbol | Value | Meaning |
|---|---|---|---|
| Normal | OK | ‘9000’ | Successful completion of command |
| | MORE | ‘61xx’ | Successful completion of command with at least xx bytes of additional response data available |
| Warning | EOP-NOCHANGE | ‘62xx’ | Unexpected end of processing leaving the state of non-volatile memory unchanged from its state immediately before the start of the execution of the command. |
| | EOD | '6282' | End of data reached |
| | EOP-RC | ‘63Cx’ | Wrong reference data – x tries left |
| | EOP-CHANGED | ‘63xx’ other than ‘63Cx’ | Unexpected end of processing leaving the state of non-volatile memory changed from its state immediately before the start of the execution of the command. |
| Execution Error | ABORT-NO CHANGE | ‘64xx’ | End of processing due to error condition leaving the state of non-volatile memory unchanged from its state immediately before the start of the execution of the command. |
| | ABORT-CHANGED | ‘65xx’ | End of processing due to error leaving the state of non-volatile memory changed from its state immediately before the start of the execution of the command. |
| | ABORT-SECURITY | ‘66xx’ | End of processing due to error condition involving a security condition leaving the non-volatile memory in an undefined state. |
| Checking Error | WRONG LENGTH | ‘6700’ | Wrong length |
| | SECURITY CONDITION | ‘6982’ | Security condition not satisfied |
| | REFERENCE DATA BLOCKED | '6983' | Reference data is blocked |
| | CONDITION OF USE | ‘6985’ | Conditions of use not satisfied |
| | DATA FIELD | ‘6A80’ | Incorrect parameters in the command data field |
| | FUNCTION NOT SUPPORTED | ‘6A81’ | Function not supported; e.g. no additional logical channels available |
| | FILE NOT FOUND | ‘6A82’ | File or application not found |
| | P1-P2 | ‘6A86’ | Incorrect parameters P1-P2 |
| | DATA NOT FOUND | ‘6A88’ | Referenced data not found |
| | BAD INS | ‘6D00’ | Instruction is not supported or invalid |
| | BAD CLA | ‘6E00’ | Class code is not supported |
| | UNDEFINED | ‘6F00’ | No precise diagnosis |
| Response produced by Generic Card Access Layer | OK | ‘0000’ | Successful processing by ISO/IEC 24727-2 implementation including CCD and ACD procedural elements |
| | SIGNATURE INVALID | ‘02xx’ | Signature on translation script not verifiable |
| | EXCEPTION | ‘0080’ | Response data contain a language-defined exception |
| | NOT MAPPED | ‘0A81’ | No translation provided by ISO/IEC 24727-2 procedural element |
| | IFD NOT FOUND | ‘0A82’ | Interface device not available |
| | CARD MISSING | ‘0A88’ | Card not found |
| | UNDEFINED | ‘0F00’ | No precise diagnosis |