INTERNATIONAL STANDARD

ISO/IEC 18328-3

First edition
2016-10-15

Identification cards — ICC-managed devices —

Part 3: Organization, security and commands for interchange

Cartes d'identification — Dispositifs contrôlés par carte —
Partie 3: Organisation, sécurité et commandes pour les échanges

Reference number
ISO/IEC 18328-3:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

A list of all parts in the ISO 18328 series can be found on the ISO website.

Introduction

The purpose of this document is to establish a normative basis for ICCs with at least an additional device.

Many new developments of electronic displays and keypads offer the technical opportunity to integrate such devices on an ICC. First products are already available and the technical progress driven by mobile devices also enforces the definition of basic standards for these technologies. Upcoming projects require several different standardized aspects.

These different aspects are in the focus of the standardization related to electronic devices on ICC, primarily the physical and electrical aspects, but also in addition the logical, organizational and security definitions.

Physical characteristics for devices on an ICC are handled in ISO/IEC 18328-2. ISO/IEC 18328-3 deals with the logical and security aspects and covers all relevant definitions and mechanisms to logical interfaces, command sets, data structures and security aspects.

Many aspects in this document refer to ISO/IEC 7816 (all parts).

ISO and IEC draw attention to the fact that it is claimed that compliance with this document may involve the usage of the following patents and the foreign counterparts:

— FR99/09818: Smart card architecture incorporating peripherals;

— PCT/EP2011/058914: Bank card with display screen;

— PCT/EP2011/059021: Bank card with display screen;

— EP2001949522A: Contact-free display peripheral device for contact-free portable object;

— WO2009077398, US20100263034, EP2225703, JP2010-538574, KR10-1162443: A method for authorizing a communication with a portable electronic device, such as an access to an electronic memory zone corresponding device and system.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holder of this patent right has assured the ISO and IEC that he/she is willing to negotiate licenses under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

Gemalto

Intellectual Property and Licensing Department

6, Rue de la Verrerie

92197 Meudon Cedex, France

Gemplus

Avenue Pic de Bertagne

Parc d’Activités de Gémenos BP 100

FR-13881 Gémenos Cedex

ASK SA

Les Boullides

15, Traverse des Brucs, Sophia Antipolis

06560 Valbonne, France

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Identification cards — ICC-managed devices —

Part 3: Organization, security and commands for interchange

1 Scope

This document specifies the logical interface of an application supporting the necessary security features in a card-IC which communicates with the external world by a physical interface supporting APDUs. This application supports the usage of electronic devices.

This involves the design of commands, data structures and security mechanisms which are required to handle the data and handling the additional devices itself. The handling of the additional devices is always controlled by the card-IC. External inputs or outputs shall be managed by the existing interfaces. This document deals not with physical characteristics of the card and interface technology, but only with the logical aspects. Management of data for additional devices that is not subdued by the COS or application control is out of the scope of this document.

Definitions of coding requirement for "trust assessment" of the managed data like warning, font, colour etc. is in the scope of this document. A description of the logical internal interface functionality used by the COS or by device drivers, if any, is also part of this document.

Due to the fact that relevant technologies may evolve or be adopted very fast, this document defines commands and structures supporting extensions and adaptations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 7816-4, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
access rule
data element containing an access mode referring to an action and security conditions to fulfil before acting

3.2
application
structures, data elements and program modules needed for performing a specific functionality

3.3
button
tactile device used for a singular input

3.4
card-IC
integrated circuit with COS

3.5
command-response pair
set of two messages at the interface

EXAMPLE A command APDU followed by a response APDU in the opposite direction.

3.6
data element
item of information seen at the interface for which are specified a name, a description of logical content, a format and a coding

3.7
data object
information seen at the interface consisting of the concatenation of a mandatory tag field, a mandatory length field and a conditional value field

3.8
device
additional electronic feature used as an extension of the ICC

3.9
device driver
part of the operating system which provides the required functionality and interfaces to the additional devices on ICC

3.10
device identifier
data element used to reference a device

3.11
device handle
logic data element used to work with a selected device

3.12
device manager
entity in an ICC which controls the device operation

3.13
device unit
electronic system providing all relevant entities to work with the device on the card

EXAMPLE Connections, driver-microcontroller, etc.

3.14
EF.ATR/INFO
optional EF indicating operating characteristics of the card, also known as Information file

3.15
electronic display
electronic device transporting optical information

3.16
file
structure for application and/or data in the card, as seen at the interface when processing commands

3.17
identification card
card identifying its holder and issuer, which may carry data required as input for the intended use of the card and for transactions based thereon

3.18
interindustry
occurring, existing or using between two or more industries

3.19
key
sequence of symbols controlling a cryptographic operation

EXAMPLE Encipherment, decipherment, a private or a public operation in a dynamic authentication, signature generation production, signature verification.

3.20
keypad
array of several buttons organized as one entity

3.21
payload
data of arbitrary length, to be sent to the card or by the card, in order to be processed together

3.22
record
string of bytes stored within EF, referenced and handled as a unit

3.23
secure messaging
set of means for cryptographic protection of (parts of) command-response pairs

3.24
security attribute
condition of use of objects in the card including stored data and data processing functions, expressed as a data element containing one or more access rules

3.25
secure element
tamper-resistant ICC in a different form factor securely hosting applications and their confidential and cryptographic data

3.26
security environment
set of components required by an application in the card for secure messaging or for security operations

3.27
structure
DF, EF, record, Data String or DO

3.28
template
concatenation of BER-TLV data objects, forming the value field of a constructed BER-TLV data object

4 Symbols and abbreviated terms

ACD	application capability description
ADM	additional device management
APDU	application protocol data unit
ATR	answer-to-reset
ATS	answer-to-select
BER	basic encoding rules of ASN.1 (see ISO/IEC 8825-1)
CCD	card capability description
CLA	class byte
COS	card operating system
NOTE	COS is a logical element for implementation of functionalities defined in ISO/IEC 7816-4.
CRT	control reference template
C-RP	command-response-pair
DF	dedicated file
DHN	device handle number
DO	BER-TLV data object
DO'...'	BER-TLV data object, the tag of which is a hexadecimal value given between simple quotes
DVCP	device control parameter
EF	elementary file
EF.ATR/INFO	answer-to-reset file, or information file
FMD	file management data
FCI	file control information
IC	integrated circuit
ICC	integrated circuit card
IFD	interface device
INS	instruction byte
I^2C	inter-integrated circuit
LCD	liquid crystal display
LED	light emitting diode
Le field	length field for coding the number N_e
N_c	number of bytes in the command data field

N_e	maximum number of bytes expected in the response data field
Nr	number of bytes in the response data field
OID	object identifier, as defined by ISO/IEC 8825-1
OLED	organic light emitting diode
RF	radio frequency
RFU	reserved for future use by ISO/IEC JTC 1/SC 17
SPT	security parameter template
SW1-SW2	status bytes (inserted for clarity, the dash is not significant)
TEE	trusted execution environment
TLV	tag length value
UTF	universal character set transformation format

5 Architectural aspects

5.1 General architecture

An ICC comprising additional devices connected to the card IC extends the functionality of existing implementations and applications. The new components require different new physical aspects to the card and the electronic system as well as some new approaches in logical perspective. Architecture, activities, commands and security are aspects which have to be covered in addition to existing standards. The definitions shall be easily extensible for new developments in the future.

An ICC with additional devices consists of an ICC with

— an interface to the external world, e.g. a contact module or an antenna,

— at least an electronic device connected physically to the card IC, or

— logically linked additional off-card devices.

The COS may support the usage of an additional device with an extension or an internal interface to an additional driver which may allow unidirectional or bi-directional information flow.

NOTE Devices referred in this document may consist of additional electronic equipment which allows delivering activity state information or internal device information even in the case of an output device. The ability is defined in the administration data of such devices.

This document deals with the interfaces between the external world and the ICC, and the ICC with the electronic device. A physical interface between the ICC and any input/output device on the card may use different technologies and transmission protocols. This is out of scope of this document. The COS should always enable communication via the implemented interfaces with any device.

An ICC with input/output devices is controlled by means of the COS. The general principle is kept, that the card is the slave, steered by commands of the IFD as the master. The initiative of any operation performed with an additional device shall be caused by the external world or IFD, by the COS or the active ICC application. A direct connection of the outside world to any input/output device on the card is not covered by this document and is finally forbidden.

The principles of access control to any additional devices shall be compliant with the access control syntax to files and data objects defined and described in ISO/IEC 7816-4.

The communication of the external world with the ICC dealing with an additional device consists of APDUs with C-RP according to the definition in ISO/IEC 7816-4. The handling of the APDU is always in the responsibility of the COS and uses the security means defined in ISO/IEC 7816-4.

The physical interfaces to different additional electronical input/output devices use a large variety of electronic protocols, e.g. I^2C, SPI, etc. The definition of a physical interface and related security requirements, e.g. integrity and confidentiality of transferred data to any input/output device and vice versa, is not in the scope of this document. Nevertheless, it is recommended to define generic abstract activities/instructions on a logical level to these interfaces to ease the description of any required activities.

This concept considers additional devices on a card, but also sets a general framework applicable to card or secure element implementing interchanges according to this document and using interfaces to off-card devices, e.g. display, LED and/or button in a handset.

For an informative description of the general system, see D.1.

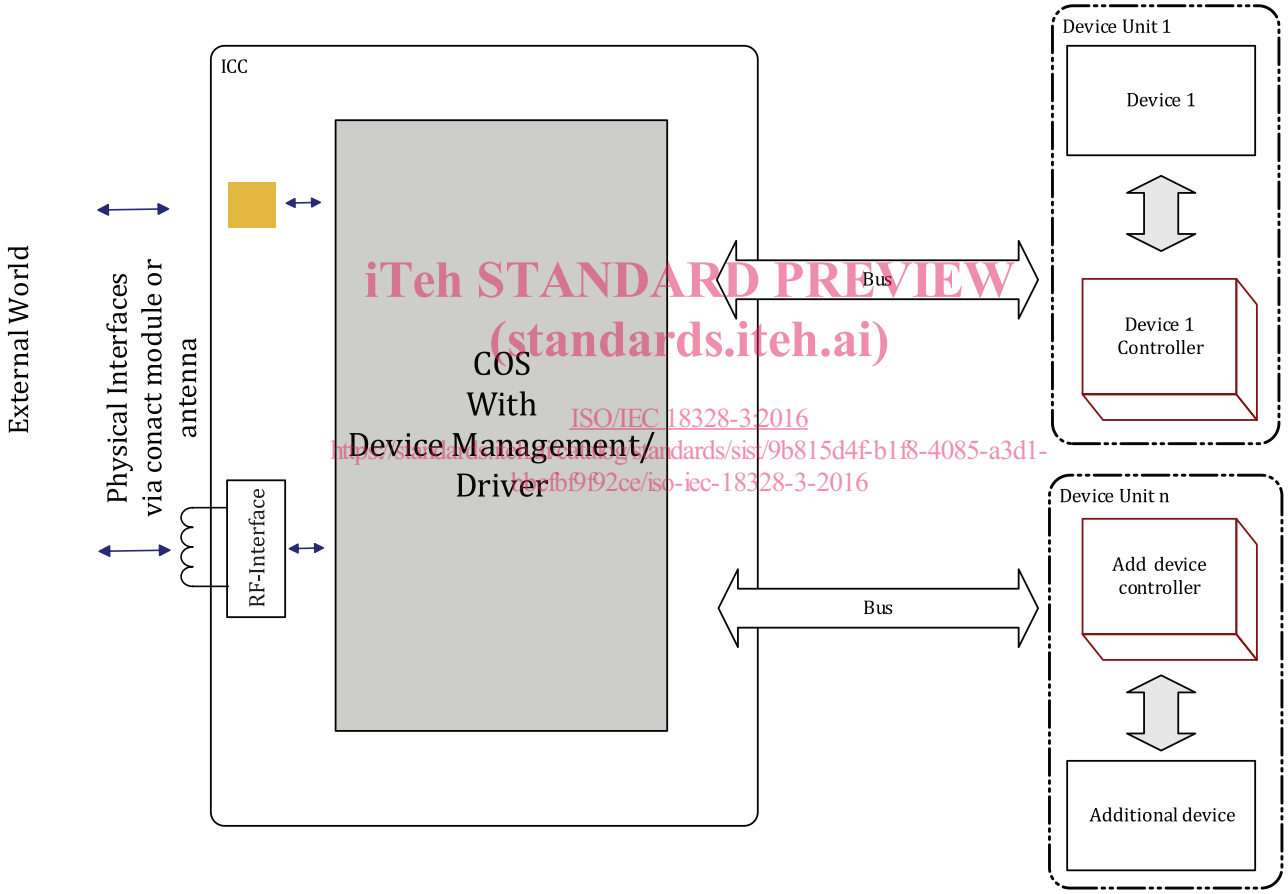

Figure 1 — Schematic ICC system with electronic devices

5.2 Operational conditions

5.2.1 Interfaces

Any transport protocols and interfaces are possible (e.g. according ISO/IEC 7816-3, ISO/IEC 7816-12, ISO/IEC 14443) as far as they allow the transmission of APDU-command-response pairs as defined in ISO/IEC 7816-4.

5.2.2 Identification of additional devices

The external world is able to get the information about the card capabilities. The external world may use different ways to retrieve this information, for example, with the following:

— an analysis of the General Feature Management DO'7F74' in EF.ATR/INFO;

— analysis of the FCI of a selected application to retrieve a general feature management DO'7F74';

— an OID referring the data set of capability description out of the general device information template (see Table 10);

— other identification means of the card, e.g. information according to ISO/IEC 24727 (ACD, CCD, card info file).

5.2.3 Device discovery mechanism

If used for device identification, the general feature management DO'7F74' (see ISO/IEC 7816-4) in EF.ATR/INFO or in the FCI of the selected application shall contain the on-card service DO'81'. This data object contains a bitmap defining the on-card services. An additional DO'83' may denote a device identifiers list in the same order as denoted in the bitmap of on-card services. Multi-occurrences of the same type of devices are represented with a prefixed occurrence number (one byte) followed by the concatenation of device identifier (two bytes each). Each entry of occurrence number and concatenated list of device identifier corresponds to the related bit in the bitmap of DO'81' of the on-card services.

Table 1 — Device identifier list DO'83'

Tag	Length	Value
'83'	var.	Occurrence number byte **n** of on-card service type A || Device identifier A1 || ... || Device identifier An
		Occurrence number byte **m** of on-card service type B || Device identifier B1 || ... || Device identifier Bm
		...

Table 2 defines further entries in the DO'81' of the General Feature Management DO'7F74'. If there is a need to add new devices, the feature list has to be extended.

Table 2 — Extension of feature-list-entries in general feature management DO'7F74'

Tag	Length	Meaning															
'81'	var.	Sub-template identifier for on-card services															
		Feature-List [0..n], expandable															
		Byte 1								Byte 2							
		b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b8**	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Meaning of bits**
		1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Display (defined by ISO/IEC 7816-4)
		—	1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Biometric input sensor (defined by ISO/IEC 7816-4)
		—	—	1	-	—	—	—	—	—	—	—	—	—	—	—	—	Button
		—	—	—	1	—	—	—	—	—	—	—	—	—	—	—	—	Keypad
		—	—	—	—	1	—	—	—	—	—	—	—	—	—	—	—	LED
		—	—	—	—	—	1	—	—	—	—	—	—	—	—	—	—	Loudspeaker
		—	—	—	—	—	—	1	—	—	—	—	—	—	—	—	—	Microphone
		—	—	—	—	—	—	—	1	—	—	—	—	—	—	—	—	Touchscreen
		—	—	—	—	—	—	—	—	1	—	—	—	—	—	—	—	Battery