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/IEC 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Symbols and abbreviated terms **4**

5 Architectural aspects **5**
5.1 General architecture 5
5.2 Operational conditions 6
5.2.1 Interfaces 6
5.2.2 Identification of additional devices 7
5.2.3 Device discovery mechanism 7
5.2.4 Logical activation of additional devices 8
5.2.5 Activation sequence 8
5.2.6 Activity states of additional devices 8
5.2.7 Exclusive usage attribute 10
5.2.8 General functionality 11
5.2.9 Timer control 12
5.3 Energy depending activation 12
5.4 Addressing of an additional device 12
5.4.1 General 12
5.4.2 Device identifier 12
5.4.3 Device handle 13
5.5 Device control information 13
5.5.1 Administration of additional devices 13
5.5.2 Device control parameter DVCP 13
5.5.3 General device information template 15

6 Functions of the ADDITIONAL DEVICE MANAGEMENT command **17**
6.1 General 17
6.2 Specific status bytes for ADDITIONAL DEVICE MANAGEMENT 18
6.3 Functions of ADDITIONAL DEVICE MANAGEMENT command 18
6.3.1 General command handling 18
6.3.2 GENERAL DEVICE RESET function 18
6.3.3 LOGICAL DEVICE RESET function 19
6.3.4 OPEN DEVICE function 19
6.3.5 DEACTIVATE DEVICE function 20
6.3.6 REACTIVATE DEVICE function 20
6.3.7 EXCLUSIVE DEVICE USAGE function 20
6.3.8 GENERAL DEVICE USAGE function 21
6.3.9 GET FROM DEVICE function 21
6.3.10 PUT TO DEVICE function 22
6.3.11 GET DEVICE INFORMATION function 23
6.3.12 ERASE DEVICE CONTENT function 23
6.3.13 MANAGE DEVICE CONFIGURATION function 24

7 Usage of off-card devices **24**
7.1 General 24
7.2 Transmission mechanism 26
7.3 Device handle 27
7.4 Secure channel 27

8 Command structures with ADM functions in applications **28**

9 Security aspects **28**

© ISO/IEC 2016 – All rights reserved

9.1 Security attributes 28
9.1.1 Access mode field for ADM command 28
9.1.2 Security conditions 29
9.2 Data integrity and confidentiality 29
9.3 Security with off-card-devices 30
9.4 Trust assessment 30
10 Device configuration template 30
10.1 Configuration template 30
10.2 Usage of device configuration templates 31
Annex A (informative) **Activity sequences 32**
Annex B (informative) **Examples for information templates 34**
Annex C (informative) **Example of command sequences with additional devices 38**
Annex D (informative) **General system description 41**
Bibliography 42

 © ISO/IEC 2016 – All rights reserved

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.

© ISO/IEC 2016 – All rights reserved

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

© ISO/IEC 2016 – All rights reserved

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.

© ISO/IEC 2016 – All rights reserved

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

© ISO/IEC 2016 – All rights reserved

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

© ISO/IEC 2016 – All rights reserved

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

© ISO/IEC 2016 – All rights reserved