INTERNATIONAL STANDARD

ISO/IEC 18328-1

First edition
2015-12-15

Identification cards — ICC-managed devices —

Part 1: General framework

Cartes d'identification — Dispositifs contrôlés par carte à circuit intégré (ICC) —
Partie 1: Cadre général

Reference number
ISO/IEC 18328-1:2015(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*.

ISO/IEC 18328 consists of the following parts, under the general title *Identification Cards — ICC-managed Devices*:

— *Part 1: General framework*

— *Part 2: Physical characteristics and test methods for cards with devices*

— *Part 3: Organisation, security and commands for interchange*

Introduction

New upcoming technologies are providing flexible and suitable devices for input and output operations on ICCs and open a wide area of applications and use cases. Interoperability in current developments of new projects underlines the need of standardisation.

Integrated Circuit Card (ICC) consists of a card body with an embedded integrated circuit (or several integrated circuits). International Standards such as ISO/IEC 7816 and ISO/IEC 14443 define the physical and logical requirements of the ICC, e.g. location of the contacts, size of the card, electrical signals and communication protocols, security mechanisms, etc.

A lot of new requirements have to be considered when ICC-managed devices are on an ICC. This also incorporates physical aspects, as well as logical view on this type of card. The needs of useful applications and their environments have to be also taken into account for the ICC-managed devices on or in a card body. The nature of the device type leads to different definitions in physical and logical aspects. The intention of this part of ISO/IEC 18328 is to minimize the technology-dependent differences and to increase interchange.

This part of ISO/IEC 18328 offers a basic framework of different aspects which allows interoperability for application of ICC-managed devices on a card or possibly external off the card.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this part of ISO/IEC 18328 may involve the use of a patent and their 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 this patent right.

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 part of ISO/IEC 18328 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 (www.iso.org/patents) and IEC (http://patents.iec.ch) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

Identification cards — ICC-managed devices —

Part 1: General framework

1 Scope

This part of ISO/IEC 18328 describes the general architecture of an ICC with ICC-managed devices. This part of ISO/IEC 18328 is one of a series of International Standards which outlines the content and the boundaries covered and standardised by the other parts of ISO/IEC 18328. The general principle of this part of ISO/IEC 18328 is that all activities regarding the ICC-managed devices are controlled by the card-IC. This principle also applies when ICC-managed devices are outside the card. This part of ISO/IEC 18328 is applicable for all kind of cards independent from interface technology for communication.

2 Terms and definitions

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

2.1
button
tactile device used as a single input key

2.2
card-IC
integrated circuit with COS

2.3
ICC-managed devices
device or devices whose activities are controlled only by ICC

2.4
keypad
array of several *buttons* (2.1) organized as one entity

2.5
biometric capture device
sensor whose purpose is to acquire biometric data

Note 1 to entry: See also ISO/IEC 17839.

2.6
electronic display
electronic device to show information

3 Symbols and abbreviated terms

CLF contactless frontend

COS card operating system

NOTE COS is a logical element for implementation of functionalities defined in ISO/IEC 7816-4.

eID electronic identification

eSE embedded secure element

HCI host controller interface

IC integrated circuit

ICC integrated circuit card

NOTE An ICC consists of card body (or document, e.g. travel document) and one IC (or several ICs) with implementation of functionalities defined in ISO/IEC 7816-4. This ICC is independent from the physical interface technology.

I^2C inter-integrated circuit

IFD interface device

LED light emitting diode

NFC near field communication

OTP one-time password

PIN personal identification number

SPI serial peripheral interface

SWP single wire protocol

TEE trusted execution environment

UICC universal integrated circuit card

4 Framework for ICC-managed devices

4.1 Device categories of ICC-managed devices

Devices on an ICC mentioned here as ICC-managed devices extend the usage and definitions of a card. First implementations have shown ICCs using extensions, e.g. keypad, electronic displays, etc. Annex A outlines a motivation for having a standard for ICC-managed devices.

In general, an ICC-managed device is defined as an electronic device supplementary to the electronic system on a card, which allows internal transactions and/or transactions with the external world. The following is a general categorisation in groups seen from the perspective of the ICC:

— devices for input purposes, e.g. button, keypad, microphone, and biometric input sensor;

— devices for output purposes, e.g. display and loudspeaker;

— devices for input/output purposes, e.g. touch-screen;

— devices for communication purposes, e.g. LED, optical sensor, loudspeaker, microphone;

— support devices, e.g. power supplying device.

4.2 Targeted subjects in the ISO/IEC 18328 series

Many card-IC of ICC used today have already ICC-managed devices on the card-IC itself. Examples are random number generators (RNG) or crypto coprocessors, etc. These on-board devices support the card-IC and the COS in dedicated use cases. Usually, today, they are proprietarily connected and linked in each

implementation. In this part ISO/IEC 18328, they are out of scope, but it is not excluded in the future to apply the mechanisms, defined in this series of International Standards also to such on-board devices.

Devices in this part ISO/IEC 18328 are always electronic devices linked to the card-IC. Any information from or to the device shall be channelled through and controlled by the ICC operating system.

Physical and logical protocols from the physical interfaces of the card-IC of the ICC to the devices are not covered by this part ISO/IEC 18328. Currently, there are different physical interfaces in ICC in use, e.g. SPI or I^2C interfaces; the definitions applied in this part ISO/IEC 18328shall be independent from any existing or future interfaces. Concrete implementations of the physical and electrical interfaces from ICC to any device or buses to the physical device are also out of the scope of this part ISO/IEC 18328.

The wide range of devices with different purposes and the large number of manufactures offering devices in different technologies and new fast developing technologies require a generic approach which allows easy adapting of new devices, new manufactures and new technologies in the future. The definitions in this part ISO/IEC 18328 shall be as flexible as possible to allow the adaptation of new devices in the future.

This part ISO/IEC 18328 covers all devices connectable to the card-IC including, but not limited to, power supplying devices, displays, all kind of sensors, microphones, loudspeaker, buttons, keypads, etc. The list can be extended due to the fact that future developments and needs will arise. Mechanisms to use electronic devices located outside of the ICC are covered also by this part ISO/IEC 18328. Figure 1 outlines the list of characteristics and mechanisms which shall be standardised within this series of International Standards.

This part ISO/IEC 18328 defines the required functionality of card operating system and other parts of software. It covers physical characteristics and test methods and also aspects of coexistence of technologies for ICC-managed devices.

Definitions of coding required for “trust assessment” of managed data, e.g. warning, font, colour, etc. is also in the scope of this part ISO/IEC 18328.

The mechanisms described in this part ISO/IEC 18328 are independent from internal capabilities of the devices.

NOTE Complex devices may have a separate controller or driver to enable its functionality. For example, an electronic display may have a specific electrical driver which provides and controls the physical signals to the display.

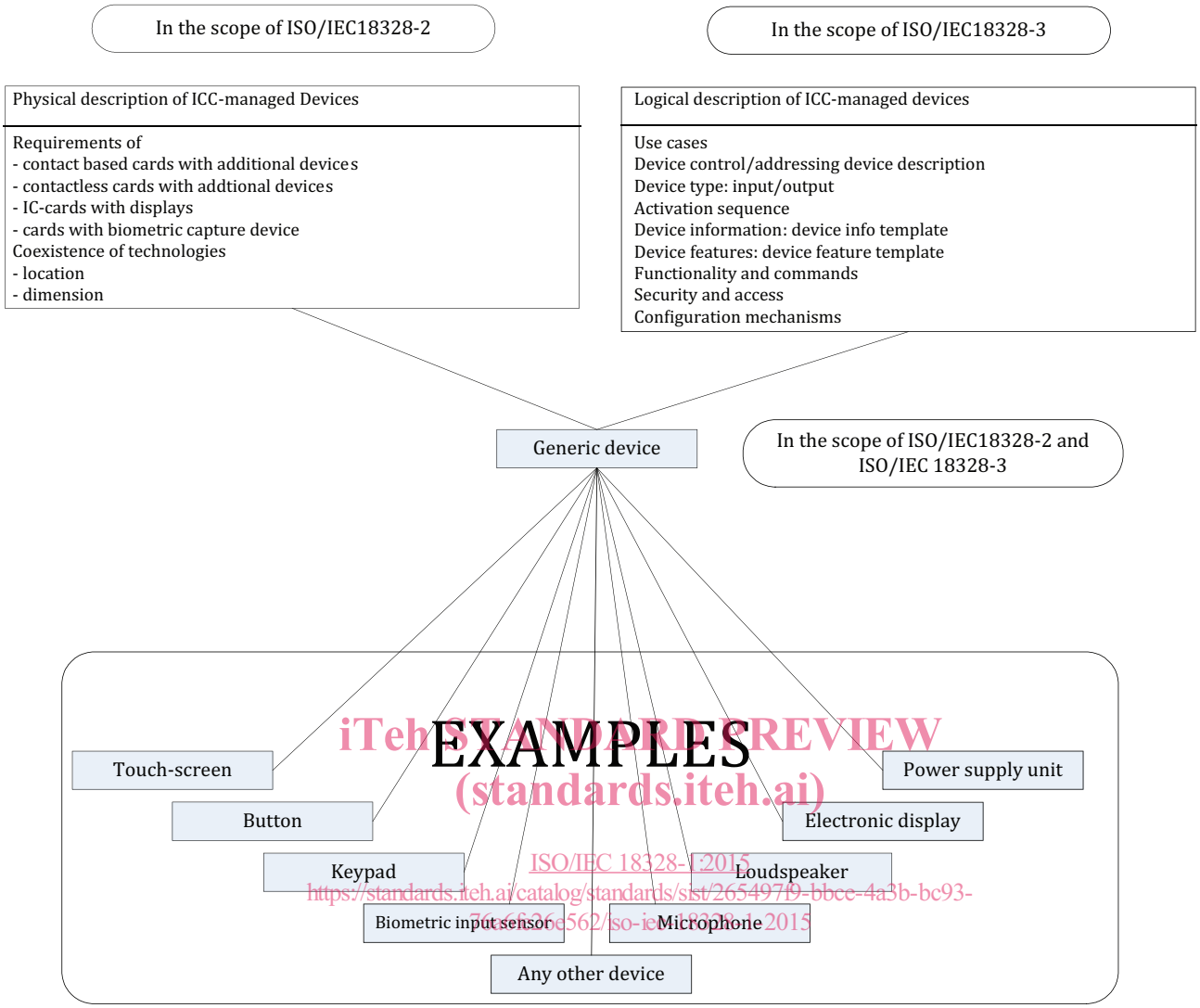

Figure 1 — Subjects in the ISO/IEC 18328 series

4.3 System architecture overview

The integration of devices into the ICC shall not reduce the functionality of the ICC, especially the functionality of proximity cards. Possible impacts are in the scope of the other parts of this part ISO/IEC 18328.

Devices located on different positions on the ICC are always electrically connected to the card-IC. Logical access to any device on the ICC is entirely under the responsibility of the COS. Figure 2 highlights the general architecture of ICC with ICC-managed devices.

Locations, physical and logical access, mechanical and electrical requirements, security-related definitions, etc. are subjects of the other parts of this part ISO/IEC 18328. Some optional features are outlined in Figure 2, e.g. a piece of software in the COS, so called driver, may handle the electrical access and bus activities from and to the device units on the ICC. An alternative for legacy systems to the system architecture on Figure 2 is described in Annex C.

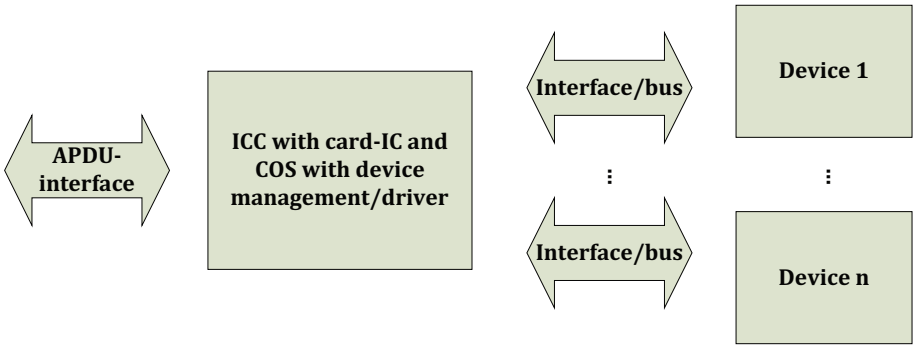

Figure 2 — System architecture of a card-IC with ICC-managed devices

4.4 Logical architecture

The logical framework shall support any ICC-managed devices used by existing or future applications. Mechanisms and templates of the framework shall embed the basic operations and data elements/objects of these applications without restricting their usage or enforcing a redefinition.

Figure 1 outlines some of the projected data templates and mechanisms provided by the operating system with the purpose to use the expanded functionality within the operating system/applications.

The logical architecture shall also include the usage of electrical devices located outside of the card. The interchange and security measures for such are the same as for devices on the card. Any access shall be under the control of the ICC; in case of external devices, an additional functionality for the external world shall be defined. Security is achieved by application of authenticity and confidentiality to transported data.

Logical system architecture is detailed in ISO/IEC 18328-3.

Annex B outlines examples of use cases with ICC-managed devices.