INTERNATIONAL STANDARD

ISO/IEC 7816-4

Fourth edition
2020-05

AMENDMENT 1
2023-10

Identification cards — Integrated circuit cards —

Part 4: Organization, security and commands for interchange

AMENDMENT 1: Support of multiple logical security devices

Cartes d'identification — Cartes à circuit intégré —

Partie 4: Organisation, sécurité et commandes pour les échanges

AMENDEMENT 1: Prise en charge de plusieurs dispositifs de sécurité logiques

Reference number
ISO/IEC 7816-4:2020/Amd. 1:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and security devices for personal identification*.

A list of all parts in the ISO/IEC 7816 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Identification cards — Integrated circuit cards —

Part 4: Organization, security and commands for interchange

AMENDMENT 1: Support of multiple logical security devices

Clause 3

Add the following term and definition at the end of Clause 3:

3.68
logical security device
collection of resources of the physical ICC, build for a logical view as a virtual ICC

Table 4

Add the following new entry after `MANAGE DATA` entry:

MANAGE LOGICAL SECURITY DEVICE	'7C'	11.9

Table 5

Add the following new entry after `MANAGE CHANNEL` entry:

'7C'	MANAGE LOGICAL SECURITY DEVICE	11.9

Clause 7

Add the following subclauses after the last subclause in Clause 7:

7.5 Multiple logical security device

7.5.1 Concept of logical security devices

Logical resources are the collection of resources of the physical ICC, described in Clause 5 to Clause 11 (except 7.5), assigned to the logical security device as a virtual ICC on the physical ICC. This collection contains, e.g. the set of data structures with its own security architecture, security attributes and security status, its own logical channels and a set of commands for interchange. An ICC supporting logical security device offers at least the basic logical security device. Multiple logical security devices may exist in parallel on one physical ICC. Each logical security device is identified by its logical security device number.

NOTE 1 The assignment of logical resources to a logical security device in the opening process is implementation dependent and can use configuration data on the physical ICC, addressed by the logical security device number. This can also apply in particular for the security conditions to be fulfilled for opening a new logical security device.

For an ICC supporting logical security devices, the following rules apply:

— Enabling the physical interface (see 5.1) opens and selects the basic logical security device automatically, which shall remain open until disabling of the physical interface. The VA on the basic logical channel for the basic logical security device is as defined in 7.2. The logical security device number of the basic logical security device is '00'.

NOTE 2 An ICC which does not support the logical security devices concept has only one security device represented by the physical ICC. A basic logical security device and its numbering can be available but is agnostic to the external world. Only the support of `MANAGE LOGICAL SECURITY DEVICE` command, defined in 11.9, enables access to the logical security device concept.

— An ICC shall support the basic logical security device and may support supplemental logical security devices. Opening with selecting, selecting, resetting and closing of a logical security device is executed by the `MANAGE LOGICAL SECURITY DEVICE` command defined in 11.9.

— `MANAGE LOGICAL SECURITY DEVICE` command shall be applicable in each logical security device.

— The first selection of a logical security device other than the basic logical security device opens the logical security device, allocates the assigned collection of logical resources and selects the logical security device.

— Logical security devices shall be separated in respect to each logical resource, shall be distinguished by its unique logical security device number and shall act independently from each other.

— The logical security device number of a logical security device, other than the basic logical security device, is determined by the external world using it in the (first) selection of the logical security device with the `MANAGE LOGICAL SECURITY DEVICE` command. After the selection of a logical security device, all sub-sequent APDUs to the ICC are handled by this logical security device, until a `MANAGE LOGICAL SECURITY DEVICE` command selects another one.

— Logical security devices use all common services of the ICC, e.g. the physical interface and its transmission protocol, the application independent card services (described in Clause 12) and the card life cycle state and its related commands.

— Resetting of an opened logical security device sets the state of the logical security device to the same state right after opening with selecting.

— Closing of an opened logical security device sets the state of the logical security device to the same state before opening with selecting, and releases the collection of all logical resources allocated to this logical security device.

— After closing, the released logical security device number shall be available for re-use by the external world.

— Closing of a logical security device which is currently selected performs a selection of the basic logical security device automatically.

7.5.2 Data related to logical security devices

The logical security device number is defined and assigned by the external world and is used to address the logical security device in the `MANAGE LOGICAL SECURITY DEVICE` command. Each logical security device administrates its own VA, logical channels and security status, independently to other logical security devices.

The reset of a logical security device may return a reset string which can be used by the external world for identification or set-up purposes. The content and structure are out of scope of this document.

NOTE Some environments expect an ATR like data structure after a reset of a logical security device. Since the transmission protocols and other common resources are used by all logical security devices, the conveyed data are only for information.