INTERNATIONAL STANDARD

ISO/IEC 7816-8

Third edition
2016-11-01

Identification cards — Integrated circuit cards —

Part 8:
Commands and mechanisms for security operations

Cartes d'identification — Cartes à circuit intégré —

Partie 8: Commandes et mécanismes pour les opérations de sécurité

Reference number
ISO/IEC 7816-8:2016(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*.

This third edition cancels and replaces the second edition (ISO/IEC 7816-8:2004), which has been technically revised.

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

Introduction

ISO/IEC 7816 is a series of standards specifying integrated circuit cards and the use of such cards for interchange. These cards are identification cards intended for information exchange negotiated between the outside world and the integrated circuit in the card. As a result of an information exchange, the card delivers information (computation result, stored data), and/or modifies its content (data storage, event memorization).

- Five parts are specific to cards with galvanic contacts and three of them specify electrical interfaces:
  - ISO/IEC 7816-1 specifies physical characteristics for cards with contacts;
  - ISO/IEC 7816-2 specifies dimensions and location of the contacts;
  - ISO/IEC 7816-3 specifies electrical interface and transmission protocols for asynchronous cards;
  - ISO/IEC 7816-10 specifies electrical interface and answer to reset for synchronous cards;
  - ISO/IEC 7816-12 specifies electrical interface and operating procedures for USB cards.
- All the other parts are independent from the physical interface technology. They apply to cards accessed by contacts and/or by radio frequency:
  - ISO/IEC 7816-4 specifies organization, security and commands for interchange;
  - ISO/IEC 7816-5 specifies registration of application providers;
  - ISO/IEC 7816-6 specifies interindustry data elements for interchange;
  - ISO/IEC 7816-7 specifies commands for structured card query language;
  - ISO/IEC 7816-8 specifies commands for security operations;
  - ISO/IEC 7816-9 specifies commands for card management;
  - ISO/IEC 7816-11 specifies personal verification through biometric methods;
  - ISO/IEC 7816-13 specifies commands for handling the life cycle of applications;
  - ISO/IEC 7816-15 specifies cryptographic information application.

ISO/IEC 10536 (all parts) specifies access by close coupling. ISO/IEC 14443 (all parts) and ISO/IEC 15693 (all parts) specify access by radio frequency. Such cards are also known as contactless cards.

Identification cards — Integrated circuit cards —

Part 8:
Commands and mechanisms for security operations

1 Scope

This document specifies interindustry commands that may be used for security operations. This document also provides informative directives on how to construct security mechanisms with ISO/IEC 7816-4 defined commands.

The choice and conditions of use of cryptographic mechanism in security operations may affect card exportability. The evaluation of the suitability of algorithms and protocols is outside the scope of this document. It does not cover the internal implementation within the card and/or the outside world.

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 7816-4:2013, *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
asymmetric key pair
pair of elements belonging to cryptographic techniques that use two related operations: a public operation defined by public numbers or by a public key and a private operation defined by private numbers or by a private key

Note 1 to entry: The two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation.

3.2
certificate
digital signature (3.3) binding a particular person or object and its associated public key

Note 1 to entry: The entity issuing the certificate also acts as tag allocation authority with respect to the data elements in the certificate.

[SOURCE: ISO/IEC 7816-4:2012, 3.11, modified]