INTERNATIONAL STANDARD

ISO/IEC 7816-8

Second edition
2004-06-01

Identification cards — Integrated circuit cards —

Part 8: Commands for security operations

Cartes d'identification — Cartes à circuit intégré —

Partie 8: Commandes pour des operations de sécurité

Reference number
ISO/IEC 7816-8:2004(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviations and notation 2

5 Interindustry commands for cryptographic operations 2
5.1 GENERATE ASYMMETRIC KEY PAIR command 2
5.2 PERFORM SECURITY OPERATION command 5
5.3 COMPUTE CRYPTOGRAPHIC CHECKSUM operation 6
5.4 COMPUTE DIGITAL SIGNATURE operation 6
5.5 HASH operation 7
5.6 VERIFY CRYPTOGRAPHIC CHECKSUM operation 8
5.7 VERIFY DIGITAL SIGNATURE operation 8
5.8 VERIFY CERTIFICATE operation 9
5.9 ENCIPHER operation 9
5.10 DECIPHER operation 10

Annex A (informative) **Examples of operations related to digital signature** 11

Annex B (informative) **Examples of certificates interpreted by the card** 14

Annex C (informative) **Examples of asymmetric key import/export** 16

Bibliography 19

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 7816-8 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification.*

This second edition, together with the second editions of ISO/IEC 7816-4, ISO/IEC 7816-5, ISO/IEC 7816-6 and ISO/IEC 7816-9, after an in-depth reorganization of these five parts, cancels and replaces ISO/IEC 7816-4:1995, ISO/IEC 7816-5:1994, ISO/IEC 7816-6:1996, ISO/IEC 7816-8:1999 and ISO/IEC 7816-9:2000. It also incorporates the Amendments ISO/IEC 7816-4:1995/Amd.1:1997, ISO/IEC 7816-5:1994/Amd.1:1996 and ISO/IEC 7816-6:1996/Amd.1:2000 and the Technical Corrigendum ISO/IEC 7816-6:1996/Cor.1:1998.

ISO/IEC 7816 consists of the following parts, under the general title *Identification cards — Integrated circuit cards:*

— *Part 1: Cards with contacts — Physical characteristics*

— *Part 2: Cards with contacts — Dimensions and location of the contacts*

— *Part 3: Cards with contacts — Electrical interface and transmission protocols*

— *Part 4: Organization, security and commands for interchange*

— *Part 5: Registration of application providers*

— *Part 6: Interindustry data elements for interchange*

— *Part 7: Interindustry commands for Structured Card Query Language (SCQL)*

— *Part 8: Commands for security operations*

— *Part 9: Commands for card management*

— *Part 10: Cards with contacts — Electronic signals and answer to reset for synchronous cards*

— *Part 11: Personal verification through biometric methods*

— *Part 15: Cryptographic information application*

Introduction

ISO/IEC 7816 is a series of International 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 7816-15 specifies cryptographic information application.

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

Identification cards — Integrated circuit cards with contacts —

Part 8:
Commands for security operations

1 Scope

This document specifies interindustry commands that may be used for cryptographic operations.

The choice and conditions of use of cryptographic mechanisms 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 referenced documents are indispensable for the application 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:—[1)], *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

1) To be published.