INTERNATIONAL STANDARD

ISO/IEC 7816-8

Fifth edition
2021-08

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 7816-8:2021(E)

© ISO/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **2**
5 Interindustry commands for security operations ... **3**
5.1 General ... 3
5.2 GENERATE ASYMMETRIC KEY PAIR command ... 3
5.3 PERFORM SECURITY OPERATION command ... 7
5.3.1 General ... 7
5.3.2 COMPUTE CRYPTOGRAPHIC CHECKSUM operation ... 10
5.3.3 COMPUTE DIGITAL SIGNATURE operation ... 10
5.3.4 HASH operation ... 10
5.3.5 VERIFY CRYPTOGRAPHIC CHECKSUM operation ... 11
5.3.6 VERIFY DIGITAL SIGNATURE operation ... 11
5.3.7 VERIFY CERTIFICATE operation ... 12
5.3.8 ENCIPHER operation ... 13
5.3.9 DECIPHER operation ... 13
Annex A (informative) **Examples of operations related to digital signature** ... **14**
Annex B (informative) **Examples of certificates interpreted by the card** ... **20**
Annex C (informative) **Examples of asymmetric key transfer** ... **24**
Annex D (informative) **Alternatives to achieve the reversible change of security context** ... **27**
Annex E (informative) **Examples of uses for GENERATE ASYMMETRIC KEY PAIR command** ... **29**
Bibliography ... **35**

© ISO/IEC 2021 – 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.

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).

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) or the IEC list of patent declarations received (see patents.iec.ch).

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 personal identification*.

This fifth edition cancels and replaces the fourth edition (ISO/IEC 7816-8:2019), which has been technically revised.

The main changes compared to the previous edition are as follows:

— in Table A.9, A.10 and A.11, P1-P2 value of MSE command has been corrected;

— in Table A.11, P1-P2 value of PSO command with HASH operation has been corrected.

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.

© ISO/IEC 2021 – All rights reserved

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.

© ISO/IEC 2021 – All rights reserved

Identification cards — Integrated circuit cards —

Part 8: Commands and mechanisms for security operations

1 Scope

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

The choice and conditions of use of cryptographic mechanism in security operations can 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, *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 terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

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* (3.4) 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* (3.4)

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 7816-4:2020, 3.11]

© ISO/IEC 2021 – All rights reserved

3.3
digital signature
data appended to, or cryptographic transformation of, a data string that proves the origin and the integrity of the data string and protects against forgery, e.g. by the recipient of the data string

[SOURCE: ISO/IEC 7816-4:2020, 3.20]

3.4
key
sequence of symbols controlling a cryptographic operation

EXAMPLE Encipherment, decipherment, a private or a public operation in a dynamic authentication, signature production, signature verification.

[SOURCE: ISO/IEC 7816-4:2020, 3.30]

3.5
non-self-descriptive certificate
certificate (3.2) consisting of a concatenation of data elements associated to a header list or extended header list, describing the structure of the certificate

3.6
self-descriptive certificate
certificate (3.2) consisting of a concatenation of data objects

3.7
secure messaging
SM
set of means for cryptographic protection of (parts of) command-response pairs

[SOURCE: ISO/IEC 7816-4:2020, 3.49]

4 Abbreviated terms

BCD	binary-coded decimal
BER	basic encoding rules of ASN.1 (see ISO/IEC 8825-1)
CA	certification authority
CCT	control reference template for cryptographic checksum
CRT	control reference template
CT	control reference template for confidentiality
CVCA	country verifying CA
DG3	data group 3
DO	BER-TLV data object
DO'...'	BER-TLV data object, the tag of which is a hexadecimal value given between single quotation marks
DSA	digital signature algorithm
DST	control reference template for digital signature
DV	document verifier

© ISO/IEC 2021 – All rights reserved