DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 7816-8

ISO/IEC JTC **1**/SC **17** Secretariat: **BSI**

Voting begins on:
2020-10-13

Voting terminates on:
2021-01-05

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

ICS: 35.240.15

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 7816-8:2020(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

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.

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) or the IEC list of patent declarations received (see https://patents.iec.c).

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.

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

This fourth edition cancels and replaces the third edition (ISO/IEC 7816-8:2016), 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, P1P2 value of MSE command has been corrected.

— In Table A.11, P1P2 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 website.

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.

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 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

Editor's note: The source indications of the normative references will be aligned with the actual value until the final draft is released. 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:—,[1] *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:

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

— IEC Electropedia: available at http://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) (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:—, 3.11]

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:—, 3.20]

3.4
key
sequence of symbols controlling a cryptographic operation (e.g. encipherment, decipherment, a private or a public operation in a dynamic authentication, signature production, signature verification)

[SOURCE: ISO/IEC 7816-4:—, 3.31]

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
set of means for cryptographic protection of (parts of) command-response pairs

[SOURCE: ISO/IEC 7816-4:—, 3.50]

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
ECC	elliptic curve cryptography

ECDH	elliptic curve Diffie–Hellman key exchange
ECDSA	elliptic curve digital signature algorithm
EF	elementary file
GQ2	modified Guillou-Quisquater protocol for zero knowledge proof
HT	control reference template for hash-code
ICAO	international civil aviation organization
ICC	integrated circuit card
IS	inspection system
KAT	control reference template for key agreement
LDS	logical data structure
MRTD	machine readable travel document
MSE	MANAGE SECURITY ENVIRONMENT command
OID	object identifier, as defined by ISO/IEC 8825-1
PSO	PERFORM SECURITY OPERATION command
RFU	reserved for future use for ISO/IEC JTC 1/SC 17
RSA	Rivest, Shamir, Adleman
SE	security environment
SEID	security environment identifier
TLV	tag, length, value

5 Interindustry commands for security operations

5.1 General

An ICC compliant with this document may support any of the commands and/or options provided in the following clauses and subclauses.

NOTE In addition to the use of logical channels, there are other alternatives that can be used for switching the security context. Annex D provides information about this functionality.

5.2 Generate asymmetric key pair command

The GENERATE ASYMMETRIC KEY PAIR command, which shall be as specified in Table 1, initiates either

— the generation and storing of an asymmetric key pair, i.e. a public key and a private key, in the card,

— the generation, storing of an asymmetric key pair and extracting generated public key, or

— the extracting previously generated public key.

The command may be preceded by a MANAGE SECURITY ENVIRONMENT command in order to set key generation related parameters (e.g. algorithm reference). The command may be performed in one or several steps, possibly using command chaining (see ISO/IEC 7816-4).

Table 1 — GENERATE ASYMMETRIC KEY PAIR command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	'46' or '47'
P1	See Table 2
P2	'00' (no information provided) or reference of the private key to be generated coded according to ISO/IEC 7816-4:—, Table 102
L_c field	Absent for encoding $N_c = 0$, present for encoding $N_c > 0$
Data field	Absent, or Proprietary data if P1-P2 set to '0000', or One or more CRTs associated to the key generation if P1-P2 different from '0000' (see notes) A CRT may include an extended header list
L_e field	Absent for encoding $N_e = 0$, present for encoding $N_e > 0$

Data field	Absent, or Public key as a sequence of data elements (INS = '46'), or Public key as a sequence of data objects (INS = '47'), or Public key as a sequence of data objects according to an extended header list (INS = '47')
SW1-SW2	See ISO/IEC 7816-4:—, Tables 6 and 7 where relevant, e.g. 6985

NOTE 1 Several CRTs are present when the key pair is generated for several uses. In the command data field, a CRT possibly has a zero length.

Table 2 — P1 coding

b8	b7	b6	b5	b4	b3	b2	b1	Value
0	0	0	0	0	0	0	0	No information given
1	—	—	—	—	x	x	x	Additional information given
1	—	—	—	—	—	—	x	**Key generation**
1	—	—	—	—	—	—	0	— Generate asymmetric key pair
1	—	—	—	—	—	—	1	— Access to an existing public key
1	—	—	—	—	—	x	—	**Format of returned public key data**
1	—	—	—	—	—	0	—	— Proprietary format
1	—	—	—	—	—	1	—	— Output format according to extended header list
1	—	—	—	—	x	—	—	**Output indicator**
1	—	—	—	—	0	—	—	— Public key data in response data field
1	—	—	—	—	1	—	—	— No response data if Le field absent or proprietary if Le field present
—	x	x	x	x	—	—	—	0000, other values are RFU

NOTE 2 The private key can be stored in an internal EF the reference of which is known before issuing the command or in a DO'7F48' as cardholder private key template.

NOTE 3 The public part can be stored for example in a DO'7F49' as cardholder public key template.

For extracting a previously generated public key (i.e. no generation), the command data field shall be empty or shall contain a CRT, possibly including an extended header list.

NOTE 4 In those cases when only access to a previously generated public key is requested, P2 is either '00' or references the private key.

The response data field shall be either

— absent,

— a public key as a sequence of data elements (INS = '46'),

— a public key as a sequence of data objects (INS = '47') from Table 3, or

— a public key as a DO'7F49' (INS = '47') nesting data objects from Table 3.

If the command data field does not indicate any format of public key data, it shall be implicitly known before issuing the command (e.g. as part of the security environment). When the command data field indicates an extended header list within a CRT, it covers public key data objects and other requested data object.

EXAMPLE Annex E provides a set of examples on the use of this command.

If the algorithm is not indicated in the command, then the algorithm is known before issuing the command. In the public key template, the context-specific class (first byte from '80' to 'BF') is reserved for public key data objects.

Table 3 — Public key data objects

Tag		Value
'7F49'		Interindustry template for nesting one set of public key data objects with the following tags
	'06'	Object identifier of any further information, optional
	'80'	Algorithm reference as used in control reference data objects for secure messaging, optional
		Set of public key data objects for RSA
	'81'	Modulus (a number denoted as n coded on x bytes)
	'82'	Public exponent (a number denoted as v, e.g. 65 537)
		Set of public key data objects for DSA
	'81'	First prime (a number denoted as p coded on y bytes)
	'82'	Second prime (a number denoted as q dividing p-1, e.g. 20 bytes)
	'83'	Basis (a number denoted as g of order q coded on y bytes)
	'84'	Public key (a number denoted as y equal to g to the power x mod p where x is the private key coded on y bytes)
		Set of public key data objects for ECC
	'81'	Prime (a number denoted as p coded on z bytes)
	'82'	First coefficient (a number denoted as a coded on z bytes)
	'83'	Second coefficient (a number denoted as b coded on z bytes)
	'84'	Generator (a point denoted as PB on the curve, coded on 2z + 1 or 2z or z + 1 bytes)
	'85'	Order (a prime number denoted as q, order of the generator PB, coded on z bytes)
	'86'	Public key (a point denoted as PP on the curve, equal to x times PB where x is the private key, coded on 2z + 1 or 2z or z + 1 bytes)
	'87'	Co-factor
		Set of public key data objects for GQ2
	'81'	Modulus (a number denoted as n coded on x bytes)
	'83'	Number of basic numbers (a number denoted as m coded on 1 byte. If tag '83' is present, then tag 'A3' shall be absent and the m basic numbers denoted as g, g_2..g_m are the first m prime numbers 2, 3, 5, 7, 11...)
	'84'	Verification parameter (a number denoted as k coded on 1 byte)

NOTE In this context, ISO/IEC JTC 1/SC 17 reserves any other data object of the context-specific class (first byte in the range '80' to 'BF').

[a] The RSA Okamoto-Schnorr signature scheme, is considered a blind signature process, which is an interactive procedure between a signer and a recipient. It allows a recipient to obtain a signature of a message of the recipient's choice without giving the signer any information about the actual message or the resulting signature[8][9][10][11]. DO'73' may be used in the data field for returning a multi-part digital signature response comprised of concatenation of context-specific data objects defined by the application.

Table 3 *(continued)*

Tag	Value
'A3'	Set of m basic numbers denoted as g, g_2..g_m, each one coded on 1 byte with tag '80' (If tag 'A3' is present, then tag '83' shall be absent)
	Set of public key data objects for RSA Okamoto-Schnorr signature scheme[a]
'81'	p the first large prime number
'82'	q the second large prime number such that q|(p − 1), with q a divisor of (p − 1)
'83'	Zp* the set of integers U modulo p such as 0 < U < p and gcd (U,p) = 1, gcd() being the greatest common divisor
'84'	Zq* the set of integers U' modulo q such as 0 < U' < q and gcd (U',q) = 1
'85'	g the first element of Zp* of order q such as g is a generator of Gq and Gq a cyclic group of prime order q
'86'	h the second element of Zp* of order q different from g
'87'	y the public key, an integer denoted as $y=g^{-r}\ h^{-s}$ mod p where (s,r) is the secret key, and s and r are two elements of (Zq*), and h of (Zp*)

NOTE In this context, ISO/IEC JTC 1/SC 17 reserves any other data object of the context-specific class (first byte in the range '80' to 'BF').

[a] The RSA Okamoto-Schnorr signature scheme, is considered a blind signature process, which is an interactive procedure between a signer and a recipient. It allows a recipient to obtain a signature of a message of the recipient's choice without giving the signer any information about the actual message or the resulting signature[8][9][10][11]. DO'73' may be used in the data field for returning a multi-part digital signature response comprised of concatenation of context-specific data objects defined by the application.

NOTE 5 For other Blind Signature schemes, e.g. Blind RSA signature (with data objects related to RSA), Blind Schnorr signature (with data objects related to DSA and/or ECDSA), Okamoto-Guillou-Quisquater blind signature scheme (with data objects related to GQ2), the OID under template '7F49' determines the nature and meaning of any further or different data objects, i.e. the following indications are possibly denoted by the OID

— blind signature type, e.g. RSA, Schnorr, Okamoto-Schnorr, Okamoto-Guillou-Quisquater),

— cryptographic Hash function,

— generic description of the token/credential (message) to be signed,

— attributes generic structure, and/or

— type of control upon signed message, i.e. partially blind, fully blind or restrictive blind signature (in some mechanisms, the signer does not totally lose control over the signed message since the signer can include explicit information in the resulting signature based on some agreement with the recipient. Such blind signatures are called partially blind signatures. Other mechanisms allow a recipient to receive a blind signature on a message not known to the signer but the choice of the message is restricted and conforms to certain rules. Such schemes are called restrictive blind signature mechanisms).

For the coding of the DO stating information about the private part of the key pair, Table 4 applies.

Table 4 — Private key data objects

Tag	Value
'7F48'	Interindustry template for nesting one set of private key data object with the following tags
'82'	public exponent (optional)
'92'	parameter p
'93'	parameter q
'94'	parameter 1/q mod p

NOTE In this context, ISO/IEC JTC 1/SC 17 reserves any other data object of the context-specific class (first byte in the range '80' to 'BF').

Table 4 *(continued)*

Tag	Value
'95'	parameter d mod (p – 1)
'96'	parameter d mod (q –1)
'7F48'	Interindustry template for nesting one set of ECDSA/ECDH private key data object with the following tags
'92'	Private key
'06'	object identifier of related curve (optional)
or	
	curve information (optional):
'93'	— p is the prime specifying the base field;
'94'	— A 1st coefficient of the equation y^2 = x^3 + A*x + mod p defining the elliptic curve;
'95'	— B 2nd coefficient of the equation y^2 = x^3 + A*x + B mod p;
'96'	— G = (x,y) base point, i.e., a point in E of prime order, with x and y being its x- and y-coordinates;
'97'	— q prime order of the group generated by G;
'98'	— h cofactor of G in E, i.e. #E[GF(p)]/q.
NOTE In this context, ISO/IEC JTC 1/SC 17 reserves any other data object of the context-specific class (first byte in the range '80' to 'BF').	

Annex C provides examples of exporting a public key and importing a private key.

5.3 Perform security operation command

5.3.1 General

The PERFORM SECURITY OPERATION command, which shall be as specified in Table 5, initiates the following security operations:

— computations, such as

— computation of a cryptographic checksum,

— computation of a digital signature, or

— computation of a hash-code;

— verifications, such as

— verification of a cryptographic checksum,

— verification of a digital signature, or

— verification of a certificate;

— encipherment; or

— decipherment.

P1 defines output data of the security operation (see Table 6). P2 defines input data to the security operation (see Table 7). Values of tag of SM data object defined in ISO/IEC 7816-4 are used for P1 and P2.

P1 and P2 also define operation of this command. It depends on each operation defined in subsequent subclauses which value is used for P1 and P2. If the security operation requires several commands to complete, then command chaining may apply (see ISO/IEC 7816-4).

The PERFORM SECURITY OPERATION command may be preceded by a MANAGE SECURITY ENVIRONMENT command.