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

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*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
asymmetric cryptographic technique
cryptographic technique that uses 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 The two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation.

[ISO/IEC 7816-4]

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

NOTE The entity issuing the certificate also acts as tag allocation authority with respect to the data elements in the certificate.

[ISO/IEC 7816-4]

1) To be published.

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 protect against forgery, e.g. by the recipient of the data string

[ISO/IEC 7816-4]

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)

[ISO/IEC 7816-4]

3.5
secure messaging
set of means for cryptographic protection of [parts of] command-response pairs

[ISO/IEC 7816-4]

4 Abbreviations and notation

For the purposes of this document, the following abbreviations apply.

CCT	control reference template for cryptographic checksum
CRT	control reference template
CT	control reference template for confidentiality
DSA	digital signature algorithm
DST	control reference template for digital signature
ECDSA	elliptic curve digital signature algorithm
HT	control reference template for hash-code
MSE	MANAGE SECURITY ENVIRONMENT command
PK	public key
PSO	PERFORM SECURITY OPERATION command
GQ	Guillou and Quisquater
RFU	reserved for future use
RSA	Rivest, Shamir, Adleman
SE	security environment
SEID	security environment identifier

5 Interindustry commands for cryptographic operations

It shall not be mandatory for all cards complying with this document to support all those commands or all the options of a supported command.

5.1 GENERATE ASYMMETRIC KEY PAIR command

The GENERATE ASYMMETRIC KEY PAIR command either initiates the generation and storing of an asymmetric key pair, i.e., a public key and a private key, in the card, or accesses an asymmetric key pair previously generated in the card.

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	Generation control according to Table 2
P2	'00' (no information provided) or reference of the key to be generated
L_c field	Absent for encoding Nc = 0, present for encoding Nc > 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 note)
L_e field	Absent for encoding Ne = 0, present for encoding Ne > 0

Data field	Absent, or Public key as a sequence of data elements or data objects, or Sequence of data objects according to an extended header list
SW1-SW2	See ISO/IEC 7816-4, Tables 5 and 6 where relevant, e.g. 6985

NOTE Several CRTs are present when the key pair is generated for several uses. In a data field, a CRT may have a zero length.

Table 2 — Generation control in P1

b8	b7	b6	b5	b4	b3	b2	b1	Value
0	0	0	0	0	0	0	0	No information given
1	0	0	0	0	x	x	x	Additional information given
1	0	0	0	0	-	-	x	**Key generation**
-	-	-	-	-	x	x	0	- Generate asymmetric key pair
-	-	-	-	-	x	x	1	- Access to an existing public key
1	0	0	0	0	-	x	-	**Format of returned public key data**
-	-	-	-	-	x	0	x	- Proprietary format of public key data
-	-	-	-	-	x	1	x	- Output format of public key data according to an extended headerlist
1	0	0	0	0	x	-	-	**Output indicator**
-	-	-	-	-	0	x	x	- Public key data in response data field
-	-	-	-	-	1	x	x	- No response data if Le field absent or proprietary if Le field present
Any other value is reserved for future use by ISO/IEC JTC1/SC17								

For generating a key pair, in the absence of L_e field, the key pair is stored in the card, possibly in an EF the reference of which is known before issuing the command.

For accessing a key pair (no generation), the command data field may be empty.

Depending on the parity of the INS code (see ISO/IEC 7816-4), a public key in the response data field is either a sequence of data elements ('46') or a sequence of data objects ('47').

If an extended header list describes the response data field, it is implicitly known before issuing the command. It covers public key data objects and other requested data objects.

When bit 1 is set to one in INS, i.e., INS set to '47', and when a public key is returned in the response data field, an interindustry template is used for nesting one appropriate set of public key data objects according to Table 3. 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 the algorithm, 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., 65537)
	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 ECDSA
'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 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 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)
'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).
— 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').	

5.2 PERFORM SECURITY OPERATION command

The PERFORM SECURITY OPERATION command initiates the following security operations, according to the data objects specified in P1-P2.

— Computation of a cryptographic checksum;

— Computation of a digital signature;

— Calculation of a hash-code;

— Verification of a cryptographic checksum;

— Verification of a digital signature;

— Verification of a certificate;

— Encipherment;

— Decipherment.

If the security operation requires several commands to complete, then command chaining shall apply (see ISO/IEC 7816-4).

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

For example, the key reference as well as the algorithm reference shall be either implicitly known or specified in a CRT in a MANAGE SECURITY ENVIRONMENT command.

Such a command can be performed only if the security status satisfies the security attributes for the operation. The successful execution of the command may be subject to successful completion of prior commands (e.g., VERIFY before the computation of a digital signature).

If present, a header list or an extended header list defines the order and the data items that form the input for the security operation.

Table 4 — PERFORM SECURITY OPERATION command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	'2A'
P1	Tag (the response data field is the data element, if present) or '00' (the response data field is always absent); 'FF' is RFU
P2	Tag (the command data field is the data element, if present) or '00' (the command data field is always absent); 'FF' is RFU for ISO/IEC JTC1/SC17
L_c field	Absent for encoding Nc = 0, present for encoding Nc > 0
Data field	Absent or value of the data object specified in P2
L_e field	Absent for encoding Ne = 0, present for encoding Ne > 0

Data field	Absent or value of the data object specified in P1
SW1-SW2	See ISO/IEC 7816-4, Tables 5 and 6 where relevant, e.g. 6985