INTERNATIONAL STANDARD

ISO/IEC 7816-8

First edition
1999-10-01

Identification cards — Integrated circuit(s) cards with contacts —

Part 8:
Security related interindustry commands

Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts —

Partie 8: Commandes intersectorielles de sécurité

Reference number
ISO/IEC 7816-8:1999(E)

Contents

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Symbols (and abbreviated terms) 2

5 Security environments 2

6 Extended headerlist DE 4

7 Security support 5

8 Secure messaging extensions 7

9 Command chaining 9

10 MANAGE SECURITY ENVIRONMENT command 9

11 PERFORM SECURITY OPERATION command 11

12 Manage verification process 15

13 GENERATE PUBLIC KEY PAIR command 18

14 MUTUAL AUTHENTICATE function 18

15 Tags defined in ISO/IEC 7816-8 19

Annex A (informative) **Structure and usage of certificates interpreted by the card** 20

Annex B (informative) **Usage of digital signature relevant operations** 22

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

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. 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.

International Standard ISO/IEC 7816-8 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Identification cards and related devices*.

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

- *Part 1: Physical characteristics*
- *Part 2: Dimensions and location of the contacts*
- *Part 3: Electronic signals and transmission protocols*
- *Part 4: Interindustry commands for interchange*
- *Part 5: Numbering system and registration procedure for application identifiers*
- *Part 6: Interindustry data elements*
- *Part 7: Interindustry commands for Structured Card Query Language (SCQL)*
- *Part 8: Security related interindustry commands*
- *Part 9: Additional interindustry commands and security attributes*
- *Part 10: Electronic signals and answer to reset for synchronous cards*

Annexes A and B of this part of ISO/IEC 7816 are for information only.

Introduction

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 7816 may involve the use of a patent concerning smart cards and terminals given in the body of the text.

The ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

Director of Intellectual Property
BULL CP8, S.A.
68, route de Versailles
B.P. 45
78431 Louveciennes Cédex
France

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 7816 may be subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Identification cards - Integrated circuit(s) cards with contacts - Part 8: Security related interindustry

1 Scope

This part of ISO/IEC 7816 specifies:

- security protocols for use in cards;
- secure messaging extensions;
- the mapping of the security mechanisms on to the card’s security functions/services, including a description of the in-card security mechanisms;
- data elements for security support;
- the use of algorithms implemented on the card (though the algorithms themselves are not described in detail);
- the use of certificates;
- security related commands.

This part of ISO/IEC 7816 does not cover the internal implementation within the card and/or the outside world.

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 part of ISO/IEC 7816.

It shall not be mandatory for cards complying to this part of ISO/IEC 7816 to support all the described commands or all the options of supported commands.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 7816. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However parties to agreements based on this part of ISO/IEC 7816 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 7816-3:1997, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocols.*

ISO/IEC 7816-4:1995, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange.*

ISO/IEC 7816-4:1995/Amd.1:1997, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange — Amendment 1: Impact of secure messaging on the structures of APDU messages.*

ISO/IEC 7816-6:1996, *Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements.*

ISO/IEC 9796:1991, *Information technology — Security techniques — Digital signature scheme giving message recovery.*

ISO/IEC 9798-2:1994, *Information technology — Security techniques — Entity authentication mechanisms — Part 2: Mechanism using symmetric encipherment algorithms.*

ISO/IEC 9798:1991, *Information technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public-key algorithm.*

ISO/IEC 9979:1991, *Data cryptographic techniques — Procedures for the registration of cryptographic algorithms.*

3 Terms and definitions

For the purposes of this part of ISO/IEC 7816, the following definitions apply.

3.1
Certification Authority
CA
a trusted third party that establishes a proof that links a public key and other relevant information to its owner

3.2
cryptographic mechanisms
functions provided by the card as a result of its implementation of cryptographic algorithms with a specific set of operational parameters e.g. the mode of operation and the size of data or keys

3.3
secure messaging
provides a means for cryptographic protection on the data exchanged during a command (as described in ISO/IEC 7816-4)

3.4
security environment
a mechanism to specify to the card system the security functions that are available to provide protection to commands for a specific application of the card

4 Symbols (and abbreviated terms)

For the purposes of this part of ISO/IEC 7816, the following abbreviations apply

APDU	Application protocol data unit
AT	Authentication template
BER-TLV	Basic Encoding Rules - Tag Length Value
CA	Certification authority
CC	Cryptographic checksum
CCT	Cryptographic checksum template
CK	Common key
CRDO	Control reference data object
CRT	Control reference template
CT	Confidentiality template
DE	Data element
DF	Dedicated file
DO	Data object
DS	Digital signature
DSI	Digital signature input
DST	Digital signature template
EF	Elementary file
HT	Hash template
IFD	Interface device
PK	Public key
PSO	PERFORM SECURITY OPERATION command
RFU	Reserved for future use
SE	Security environment
SK	Secret key
SM	Secure messaging
SST	Security support template

5 Security environments

5.1 Description

The security environment (SE) in a card is the logical container of a set of fully specified security mechanisms which are available for reference in security related commands and in secure messaging (SM) as defined in this part of ISO/IEC 7816 and in ISO/IEC 7816-4.

Any SE shall specify references to the cryptographic algorithm(s) to be executed, the mode(s) of operation, the key(s) to be used and any additional data needed by a security mechanism. It may specify a template describing data elements (DEs) stored in the card or resulting from some computation, to be included by the algorithms specified in the security environment definition. It also may provide directions for handling the data resulting from the computation, e.g. storage in the card memory. Any relative references to files (keys or data) specified with a mechanism in the environment definition shall be resolved with respect to the dedicated file (DF) selected at the time the mechanism is used to perform a computation.

Absolute references (e.g. absolute path) need not be resolved.

NOTE — ISO maintains a register of cryptographic algorithms (see ISO/IEC 9979) and, separately, provides protocol standards.

5.2 Activation of a security environment

At any time during operation of the card a current SE shall be active, either by default or as a result of commands from the interface device (IFD). The default SE may be empty. The content of the default SE is not defined in this part of ISO/IEC 7816.

The current SE may explicitly be set or replaced with the MANAGE SECURITY ENVIRONMENT command (see clause 10). An SE may contain a mechanism to perform initialisation of non-persistent data used by mechanisms in the environment, e.g. a session key.

In SM, data objects transmitted in a control reference data object (CRDO) shall take precedence over any corresponding data object (DO) present in the current SE.

Definitions of associated SE's may be grouped into the following sets:

- One global SE set, which may be provided by the card. The first SE of this set is the default SE;
- One or more application specific SE sets which are provided by applications.

The global SE set shall be active by default, unless otherwise specified. A SE or set of SEs may be associated with a DF or EF such that after selecting the DF or EF the associated SE or a specific SE in the set is implicitly set. The method of specifying this functional association between a file and a set of SEs is outside the scope of this part of ISO/IEC 7816.

The current SE is valid until there is a change of context (e.g. by selecting a different application with the SELECT FILE command), a MANAGE SECURITY ENVIRONMENT command, a warm reset or deactivation of the contacts (see ISO/IEC 7816-3).

5.3 Components

Control Reference Templates (CRT) may be used to describe the various components of a SE (see Table 2).

Five such templates are defined for:

- cryptographic checksum;
- digital signature;
- confidentiality;
- hash;
- authentication.

Within the SE, components may have two aspects; one being valid for the protection of command APDUs (application protocol data units) and the other for the protection of response APDUs.

SEs may be numbered for storing, restoring (see clause 10) and referencing, in which case the numbering is context specific.

SE numbers represented by:

- all zeroes (0) denote an empty environment, where no authentication no SM procedure is defined;
- all ones (1) denote that no operation can be performed in this environment;
- 11101111 is Reserved for Future Use (RFU).

The current SE contains one or more:

- components belonging to the default stored SE associated with the current DF;
- components transmitted in SM commands (see ISO/IEC 7816-4);
- components transmitted in MANAGE SECURITY ENVIRONMENT commands (see clause 10);
- all the components of a stored SE, invoked by its number in a MANAGE SECURITY ENVIRONMENT command.

5.4 Algorithm referencing

The Algorithm Object Identifier DO is a data object which identifiers the cryptographic algorithm associated with an algorithm reference, as defined in ISO/IEC 7816-4. One or more such DOs may be present in the file control information (FCI) of a DF with a tag ‘AC’.

This DO encapsulates two mandatory DOs and an optional DO, in the following sequence:

— the first mandatory DO is the algorithm reference DO, tag ‘80’, as used in Table 3;

— the second mandatory DO is an ASN.1 DO Identifier, tag ‘06’, referencing the algorithm uniquely;

— the optional DO (tag dependent on the Object Identifier) indicates the algorithm parameters.

Example coding (see ISO/IEC 7816-6, Annex B) -

AC II 09 II 80-01-01 II 06-04-28CC4701

This Object Identifier (28CC4701) refers to algorithm 1 in ISO/IEC 9979, with no parameter.

6 Extended headerlist DE

6.1 Construction and use

An extended headerlist DE is a concatenation of tag/lengths without delimiters.

An extended headerlist is normally used for referencing DOs to be signed.

An extended headerlist references a byte string built as follows:

— each tag/length is replaced by data referenced by the tag when the DO is primitive;

— when a tag/length denotes a constructed DO, its value is interpreted as an extended headerlist DE.

According to the conditions of use of an extended headerlist, the data to include in the byte string are

— either the values of the referenced primitive DOs, truncated according to the length indicated in the extended headerlist (Case 1) or

— the primitive DOs themselves, truncated according to the length indicated in the extended headerlist, and nested in the respective template, the length of which is adjusted according to BER-TLV (Basic Encoding Rules - Tag length Value) rules (Case 2).

indicated by the appropriate parameter of the command (e.g. ‘AC’, ‘BC’ in PERFORM SECURITY OPERATION, see 11.7.3) or by the appropriate

A constructed tag followed by a length = 00 is ignored.

A primitive tag followed by a length = 00 indicates that the complete DO or DE is to be included in the byte string.

A DO, the value of which is an extended headerlist, uses tag '4D'. According to their use, other DOs may have the implicit type 'extended headerlist'.

6.2 Examples of extended headerlists

Given an extended headerlist:

Primitive T_1	00	Const . tag	L = 4	Primitive T_2	00	Primitive T_3	L = 5

describing 3 primitive DOs:

Primitive T_1	L_1	$Value_1$

Primitive T_2	L_2	$Value_2$

Primitive T_3	L_3 (≥5)	$Value_3$

Result in Case 1 (the headerlist referring to the concatenation of the DEs)

$Value_1$	$Value_2$	$Value_3$ truncated at 5 bytes

Result in Case 2 (the headerlist referring to the concatenation of the DOs)

Primitive T_1	L_1	$Value_1$	Const. tag	L = L_2 + 9	Primitive T_2

—

L_2	$Value_2$	Primitive T_3	5	$Value_3$ truncated at 5 bytes

structure of the data field: constructed for those containing DOs; primitive for those containing DEs).

7 Security support

7.1 Description and rules

The security support data elements are a collection of specially defined DEs with rules governing the way their values are handled. These DEs may be provided by the card as generic support to cryptographic protection mechanisms performed by an application.

The security support DEs may be referenced by applications for inclusion in operations executed by the card when performing commands e.g. in secure messaging or in the PERFORM SECURITY OPERATION command. The security support DEs extend and refine the auxiliary data elements for secure messaging as defined in ISO/IEC 7816-4.

The rules for maintenance and use of the value of security support DEs shall be governed by the card. They are based on the following principles:

— update is done with new values computed by the card or provided by the outside world, in accordance with the specific rule for a specific type of security support DE;

— update is performed before any output is produced for a command which causes an update. The update is independent of the completion status of the command;

— if the value is to be used by the application in an operation that causes an update, the update is performed before the value is used;

— access to application specific security support DEs is restricted to functions performed by the specific application.

NOTE — the actual security achieved in a data exchange ultimately depends on the algorithms and protocols specified by the application, the card only provides support with these DEs and associated usage rules.

7.2 Data elements

The card may support security of data exchanges with data elements having values that are different each time the card is activated. They include the following:

— A card session counter, that is incremented once during card activation;

— A session identifier, that may be computed from the card session counter and possibly data provided by the outside world.

Cryptographic protection of data exchanges may be supported with data elements, called progression values. Their values are increased at specific events throughout the life of the card.

Two progression value types are specified:

— Internal Progression Values which, if so specified for an application, register the number of times specific events are performed. The data element shall be incremented after the event has occurred; the card may provide a reset function for these counters which if so specified for an application sets its value to zero. Internal progression values cannot be controlled by the outside world and are suitable for use as secured in-card approximate representations of real time. Their values can be used in cryptographic computations.

— External Progression Values which, if so specified for an application, shall only be updated by a data value from the outside world. The new value shall be numerically larger than its current stored value.

7.3 Data element referencing

Access to the value of security support data elements may be provided in a card by:

— an EF contained in the master file (MF), e.g. for card session counter;

— an EF contained in a DF associated with an application, e.g. for application specific progression values;

— a reference as a data object with BER-TLV encoding as defined in the first column of Table 1;

— a reference as auxiliary data (tags '88', '92', '93') in a control reference template (CRT, see Table 3). These tags can be used if the SE supports unambiguous use of these data elements.

Characteristics of the security support data elements, e.g. length of the data, and the algorithms which alter their value are not defined in this part of ISO/IEC 7816.

Table 1 — Tags for security support data objects

Tag	Meaning
'7A'	Security Support Template (SST), to encapsulate DOs with the following tags
'80'	Card session counter
'81'	Session identifier
‘82’ - ‘8E’	File selection counter
‘93’	Digital signature counter
'9F2X'	Internal progression value
'9F3Y'	External progression value

The coding of 'X' in Table 1 is an index of a specific internal progression value e.g. a counter of file selections.

The coding of 'Y' in Table 1 is an index of a specific external progression value e.g. an external time stamp.

8 Secure messaging extensions

8.1 Secure messaging data objects

Table 2 lists the SM data objects defined in ISO/IEC 7816-4 and Amendment 1, and the SM data objects defined in this part of ISO/IEC 7816.

Table 2 - Secure messaging data objects

ISO/IEC 7816 Part-	Tag	Value
4	'80' '81'	Plain value (non BER-TLV coded data)
4	'B0', 'B1'	Plain value (BER-TLV, including SM related data objects)
4	'B2', 'B3'	Plain value (BER-TLV, but not SM related data objects)
4	'96', '97'	Value of Le in an unsecured command (see ISO/IEC 7816-4, Amendment 1)
4	'99'	Status information (e.g. SW1-SW2)
4	'82' '83'	Cryptogram, the plain value consisting of BER-TLV including SM related data objects
4	'84' '85'	Cryptogram, the plain value consisting of BER-TLV, but not SM related data objects
4	'86' '87'	Padding indicator byte (see ISO/IEC 7816-4) followed by cryptogram (plain value not coded in BER-TLV)
4	'8E'	Cryptographic checksum (at least 4 bytes)
4	'9E'	Digital signature
8	‘90’	Hash Code
4	'9A'	Input for Digital Signature (non BER-TLV coded data)
8	'A0'	Input template for Hash Code
8	'A2'	Input template for cryptographic checksum verification
8	'A8'	Input template for DS verification
8	'AC'	Input template for DS (BER-TLV coded data, the concatenation of the value fields are signed)
8	'BC'	Input template for DS (BER-TLV coded data, TLV data are signed)
8	‘92’	Certificate (non BER-TLV coded data)
8	'AE'	Input template for certificate verification (signed signature input consisting of non BER-TLV coded data)
8	'BE'	Input template for certificate verification (signed signature input consisting of BER-TLV coded data)
8	'A4', 'A5'	CRT for authentication (AT)
8	'AA', 'AB'	CRT for hash code (HT)
4	'B4', 'B5'	CRT for cryptographic checksum (CCT)
4	'B6', 'B7'	CRT for digital signature (DST)
4	'B8', 'B9'	CRT for confidentiality (CT)
4	'BA', 'BB'	Response descriptor

8.2 Control reference data objects

Table 3 lists the CRDOs defined in ISO/IEC 7816-4 and this part of ISO/IEC 7816. The table indicates to which CRT they are relevant: cryptographic checksum template (CCT), digital signature template (DST), confidentiality template (CT), hash template (HT) and authentication template (AT).

Table 3 - Data objects within control reference templates

Tag	Value	CCT	DST	CT - Asym	CT - Sym	HT	AT
		'B4', 'B5'	'B6', 'B7'	'B8', 'B9'	'B8', 'B9'	'AA', 'AB'	'A4', 'A5'
'4D'	L≠0, extended headerlist of DOs as defined in clause 6		x			x	
'5D'	L≠0, Headerlist, as defined in ISO/IEC 7816-6		x			x	
'80'	Algorithm reference *	x	x	x	x	x	x
	File reference *						
'81'	- file identifier or path	x	x	x	x	x	
'82'	- DF name	x	x	x	x	x	
	Key reference *						
'83'	- for direct use in symmetric cases	x			x	x (CK)	x
	- for referencing a public key in asymmetric cases		x	x		x	x
'84'	- for computing a session key in symmetric cases	x			x		x
	- for referencing a private key in asymmetric cases		x	x			
	Initial check block *						
'85'	L=0, null block	x			x	x	
'86'	L=0, chaining block	x			x	x	
'87'	L=0, e.g. previous initial value block + 1	x			x		
	L=k, initial value block (IV block)						
	Auxiliary data						
'88'	L=0, previous challenge + 1	x	x	x	x		
	L≠0, reference data object not specified						
'90'	L=0, hash code provided by the card		x			x	
'91'	L=0, random no. provided by the card	x	x	x			
	L≠0, random number		x	x			
'92'	L=0, time stamp provided by the card		x	x		x	
	L≠0, time stamp		x	x			
'93'	L=0, previous counter + 1**		x	x	x	x	
	L≠0, counter		x	x	x		
'89' to	L=0, index of a proprietary data item				x		
'8D'	L≠0, value of a proprietary data item						
'8E'	Cryptogram contents reference *			x	x		
'94'	Challenge or data item for deriving a key	x			x		x

* = as defined in ISO/IEC 7816-4

** = Digital signature counter.