INTERNATIONAL STANDARD

ISO/IEC 7816-9

First edition
2000-09-01

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

Part 9: Additional interindustry commands and security attributes

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

Partie 9: Commandes intersectorielles additionnelles et attributs de sécurité

Reference number
ISO/IEC 7816-9:2000(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.ch
Web www.iso.ch

Printed in Switzerland

Contents

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

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.

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

International Standard ISO/IEC 7816-9 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*

Annex A forms a normative part of this part of ISO/IEC 7816. Annex B is for information only.

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

Part 9: Additional interindustry commands and security attributes

1 Scope

This part of ISO/IEC 7816 specifies

— a description and coding of the life cycle of cards and related objects;

— a description and coding of security attributes of card related objects;

— functions and syntax of additional interindustry commands;

— data elements associated with these commands;

— a mechanism for initiating card-originated messages.

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

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. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

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

ISO/IEC 7816-7:1999, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 7: Interindustry commands for Structured Card Query Language (SCQL).*

ISO/IEC 7816-8:1999, *Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands.*

ISO/IEC TR 9577:1996, *Information technology — Protocol identification in the network layer.*

3 Terms and definitions

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

3.1
AND Template
template containing security conditions of which all have to be fulfilled

3.2
access rule
a data element containing an access mode (a reference to an action) and security conditions (to be fulfilled before an action is allowed)

3.3
application
the data structure, data elements and program modules needed for a specific functionality to be satisfied

3.4
OR Template
template containing security conditions of which at least one has to be fulfilled

3.5
security attributes
conditions of use of various resources in the card including stored data and data processing functions, expressed as a data element containing one or several access rules

4 Symbols (and abbreviated terms)

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

AM	access mode
AM_DO	access mode data object
APDU	application protocol data unit
ARR	access rule references
AT	authentication template
BER	basic encoding rules (of ASN.1)
CRT	control reference template
DE	data element
DF	dedicated file
DO	data object
EF	elementary file
FCP	file control parameters
File ID	file identifier
IFD	interface device
LCS	life cycle status
LCSI	life cycle status integer
MF	master file
RF	radio frequency
RFU	reserved for future use
SC	security condition
SC_DO	security condition data object
SE	security environment
SE #	security environment number
SM	secure messaging
SW1-SW2	status words
TLV	tag, length, value

5 File control parameters

Table 1 gives the file control parameters (FCP, tag '62') as used in this part of ISO/IEC 7816.

Table 1 - File control parameters

7816 Part-	Tag	L	Value	Applies to
4	'80'	2	Number of data bytes in the file, excluding structural information	Transparent EFs
4	'81'	2	Number of data bytes in the file, including structural information if any.	Any file
4	'82'	1	File descriptor byte	Any file
		2	File descriptor byte followed by data coding byte	Any file
		3	File descriptor byte followed by data coding byte and maximum record length, coded on 1 byte	EFs with record structure
		4	File descriptor byte followed by data coding byte and maximum record length, coded on 2 bytes	EFs with record structure
9		5 or 6	File descriptor byte followed by data coding byte and maximum record length, coded on 2 bytes, and number of records coded on 1 or 2 bytes	EFs with record structure
4	'83'	2	File identifier	Any file
4	'84'	1 to 16	DF name	DFs
4	'85'	var	Proprietary information	Any file
4	'86'	var	Security attributes, proprietary format	Any file
4	'87'	2	Identifier of an EF containing an extension of the FCI	Any file
9	'88'	0 or 1	Short EF identifier, coded from bits b8 to b4. Bits b3, b2, b1 = 000	EFs
9	'8A'	1	Life Cycle Status Integer (LCSI)	Any file
9	'8B'	var	Security attributes, reference to expanded format	Any file
9	'8C'	var	Security attributes, compact format	Any file
9	'8D'	2	File identifier of file containing SE templates	DFs
9	'A0'	var	Security attribute template for DOs	Any file
9	'A1'	var	Security attribute template for interface mode (see 8.3)	Any file
9	'A2'	var	Short EF identifier / path mapping template, i.e. short EF identifier (tag '88') || path (tag '51') see ISO/IEC 7816-6 || ... See note 2	DFs
9	'A5'	var	Proprietary information, constructed	Any file
9	'AB'	var	Security attributes, expanded format	Any file

NOTE 1 — The meaning of tag '82' has been extended in this part of ISO/IEC 7816. Further DOs have been defined.

NOTE 2 — The path to the EF, which can be selected with the short EF identifier, may be an absolute or a relative path.

If selection by short EF identifier is supported but tag '88' is not present, then the 5 least significant bits of the file identifier (tag '83') shall code the short file identifier. If the card supports the short EF identifier mechanism, an empty DO with tag '88' in the FCP indicates that the corresponding EF has no short EF identifier.

6 Life cycle status

6.1 Definition and purpose

The card, files and other objects in the card each have a life cycle, in principle as shown in Annex A.

States in the life cycle may be manipulated by commands. This part of ISO/IEC 7816 defines such commands. Annex A gives a list of these commands.

A life cycle status (LCS) may be associated with files as one of the attributes. It may also be associated with other resources in the card.

To support flexible management of the life cycle as an attribute, a number of life cycle states have been identified, which are defined in this clause. This clause also defines an encoding of the states in the life cycle.

This clause defines a coding of the LCS that allows the card to identify the states. In addition it allows the application to define additional life cycle states. Changes are controlled by the card and may be performed in a pre-defined order, reflecting reversible or irreversible changes in state.

6.2 Principles of use

A card may support a LCS attribute associated with files and, possibly, other objects in the card to indicate the different logical security states of the use of these objects.

Commands may set the value of the LCS attribute when they execure. However the card shall maintain the integrity of this value in accordance with this part of ISO/IEC 7816.

If supported, the current LCS of an object, as expressed by its value, shall be used by the card, possibly in combination with additional security attributes, to determine whether a requested operation with the object is in accordance with the specified security policy.

This standard defines 4 primary states of the life cycle (see 6.3 and Annex A) in the following order:

— creation state;

— initialisation state;

— operational state;

— termination state.

Transitions between the primary states of the life cycle are irreversible and occur in only a top-to-bottom direction.

Each primary state may have reversible secondary states.

6.3 Life cycle rules

The use of objects is governed by the current LCS according to the following rules:

— when an object is in the creation state, any security attributes for that object shall not apply;

— when an object is in the initialisation state, then security attributes specific to this state may apply;

— when an object is in the operational state, then the associated security attributes shall apply;

— when an object is in the termination state, then it shall not allow a modification of its value but it may be used as specified by its associated security attributes e.g. it may be deleted.

See Annex A for an example of the transitions between file life cycle states and associated commands.

The card life cycle status (as defined in ISO/IEC 7816-4) may be present in the historical bytes, in which case the coding shown in Table 2 shall be used.

When the card has a Master file (MF, see ISO/IEC 7816-4), then it is in, at least, the creation state.

6.4 LCS Integer encoding

The LCS Integer (LCSI - tag '8A') encodes the current LCS over one byte. The coding is shown in Table 2.

Table 2 - Coding of the LCSI - tag '8A'

b8..b5	b4	b3	b2	b1	Meaning
'0'	0	0	0	0	no information given
'0'	0	0	0	1	creation state
'0'	0	0	1	1	initialisation state
'0'	0	1	-	1	operational state – activated
'0'	0	1	-	0	operational state – deactivated
'0'	1	1	-	-	termination state
≠ '0'	x	x	x	x	proprietary

7 Security attributes - general principles

7.1 Definition and purpose

The security attributes define the allowed actions, and procedures to be performed to complete such actions (see ISO/IEC 7816-4). In particular, security attributes may:

— specify the security status of the card to be in force before access to data is allowed;

— restrict access to data to certain functions if the card has a particular status;

— define which security functions shall be performed to obtain a specific security status.

Card resources that may be protected with security attributes include:

— files;

— commands;

— tables and views;

— data objects.

7.2 Principles of use

This part of the standard describes the possible content of security attributes as data elements and objects, and the means to retrieve them from the card.

Security attribute definitions may be expressed in a collection of data elements.

A specific resource may be associated with more than one security attribute definition.

A card resource such as an EF or DF may contain in its descriptive data a reference to the security attribute definitions pertaining to it.
Other card resources (e.g. commands and data objects) may be associated with a security attribute definition by a reference contained in the security attribute definition data.

The definition of security attributes shall be specified by use of the following descriptive data elements:

— the set of access rules bound explicitly or implicitly to a resource;

— an access rule combining access modes with security conditions;

— an access mode logically containing a specification of the type of access operation, e.g. read or update. Optionally it specifies the internal function or external command that invokes the appropriate access rule definition;

— a security condition specifying which security mechanisms are necessary to conform to the access rule definition.

See clause 8 for the encoding of these data elements.

7.3 Security environments used for access control

Security environments (SEs, see ISO/IEC 7816-8) used for access control may be stored in the card within a SE Template DO (tag '7B') or in a file (or both).

The SE template DO contains, for every included SE, a SE# DO (tag '80'), an optional LCSI DO (tag '8A') and the corresponding CRTs. The value of the LCSI indicates for which life cycle state the SE is valid. If the SE is used for access control e.g. to a file, then the LCSI of the file and of the SE have to match. If the LCSI is not present, the SE is valid for the operational activated state.

If several DOs with the same tag are present inside a CRT (e.g. DOs specifying a key reference) then only one of the DOs has to be fulfilled (OR condition).

The default SE is always available and is coded under a reserved SE# (#1).

For specifying the usage of a CRT in compliance with the MANAGE SECURITY ENVIRONMENT command, a CRT usage qualifier (tag '95') may be contained in the CRT, see table 3.

Table 3 - Coding of the value of the CRT usage qualifier DO

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1								- verification (DST, CCT) - encipherment (CT) - external authentication (AT)
	1							- computation (DST, CCT) - decipherment (CT) - internal authentication (AT)
		1						- SM response (CCT, CT, DST)
			1					- SM command (CCT, CT, DST)
				1				- User authentication, knowledge based (AT)
					1			- User authentication, biometric based (AT)
						x	x	- RFU (default = 00)

7.4 Access authorisation coded in certificates

In public key based authentication procedures, card verifiable certificates may be applied. In such a certificate, a certificate holder authorisation (e.g. a role identifier) may be contained coded in a DE or DO with tag '5F4B'. If this certificate holder authorisation is used in the security conditions to be fulfilled for access to data or functions, then the DO, tag '5F4B', shall be present in the related authentication template (AT) describing the public key oriented authentication procedure.

8 Security attributes - mechanisms and coding

8.1 Coding

The coding structure presented here aims to provide a tiered approach to binding objects and their respective security attributes. Two codings are defined:

— a compact coding based on bitmaps (see 8.4);

— an expanded coding which is an extension of the compact coding with intermediate scope containing bitmaps and TLV list management (see 8.5).

8.2 Referencing

8.2.1 Referencing in the FCI

The File Control Information (FCI, see ISO/IEC 7816-4) may contain security attributes.

Relevant data objects are listed in table 1.

8.2.2 Referencing in SCQL

In an SCQL environment (see ISO/IEC 7816-7), security attributes can be specified in SCQL operations e.g. CREATE TABLE and CREATE VIEW.

If security attributes based on this part of ISO/IEC 7816 are used, then they shall be conveyed in a DO with tag '8C', '8B' or 'AB' in the security attribute parameters of an SCQL operation.

8.2.3 Referencing for data objects

Security attributes for data objects may be stored in the FCI of the corresponding DF (see table 1). The security attribute template for DOs, tag 'A0', is the concatenation of a security attribute DO and a taglist DO (giving the relevant DOs).

8.3 Security attributes for different interface modes

If the security attribute template for interface mode (tag 'A1') is present, it is used for indicating access conditions for radio frequency (RF) interface and / or contact interface.

The template contains one or more pairs consisting of an interface mode DO (see tables 4 and 5) followed by any of the DOs '86', '8B', '8C', 'A0' or 'AB', containing the corresponding security attributes.

Table 4 — Interface mode DO

Tag	L	Value
'91'	1	Interface mode DE

Table 5 — Interface mode DE

b8..b3	b2..b1	Meaning
000000		RFU (0 is default value)
		Access is restricted to interface mode:
	00	- RFU
	01	- contacts (default in ICC with contact interface)
	10	- RF (default in ICC with RF interface)
	11	- contacts and RF (default in ICC with dual interface)

8.4 Compact format

8.4.1 Introduction

Access control to an object in this coding is managed by binding the access rules to the related object.

An access rule is encoded with:

— an Access Mode (AM) byte, as defined in table 6 to table 9;

— one or more Security Condition (SC) bytes, as defined in table 10.

8.4.2 Conditions of use

The AM byte is followed by a number of SC bytes equal to the number of bits set to 1 in the AM byte (excluding b8). Each SC byte codes the conditions relevant to a (set of) command(s), in the same order (b7 to b1) as in the AM byte.

When several access rules are present in the value field of the DO, tag '8C' (see table 1), they represent an OR condition.

8.4.3 Access mode byte

Table 6 to table 9 define an AM byte for:

— DFs;

— EFs;

— Tables and views;

— DOs.

If, in an AM byte, a '1' is set within the range b7..b1, then an SC byte applies. If a '0' is set within the same range, then no SC byte applies.

Table 6 - AM byte for DFs

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	-	-	-	-	-	-	-	b7..b1 according to this table
1	-	-	-	-	-	-	-	b3..b1 according to this table; b7..b4 proprietary
-	1	-	-	-	-	-	-	DELETE FILE (self)
-	-	1	-	-	-	-	-	TERMINATE CARD USAGE (MF), TERMINATE DF
-	-	-	1	-	-	-	-	ACTIVATE FILE
-	-	-	-	1	-	-	-	DEACTIVATE FILE
-	-	-	-	-	1	-	-	CREATE FILE – DF creation
-	-	-	-	-	-	1	-	CREATE FILE – EF creation
-	-	-	-	-	-	-	1	DELETE FILE (child)

Table 7 - AM byte for EFs

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	-	-	-	-	-	-	-	b7..b1 according to this table
1	-	-	-	-	-	-	-	b3..b1 according to this table; b7..b4 proprietary
-	1	-	-	-	-	-	-	DELETE FILE
-	-	1	-	-	-	-	-	TERMINATE EF
-	-	-	1	-	-	-	-	ACTIVATE FILE
-	-	-	-	1	-	-	-	DEACTIVATE FILE
-	-	-	-	-	1	-	-	WRITE BINARY, WRITE RECORD, APPEND RECORD
-	-	-	-	-	-	1	-	UPDATE BINARY, UPDATE RECORD, ERASE BINARY
-	-	-	-	-	-	-	1	READ BINARY, READ RECORD, SEARCH BINARY, SEARCH RECORD

Table 8 - AM byte for Tables & Views

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	-	-	-	-	-	-	-	b7..b1 according to this table
1	-	-	-	-	-	-	-	b3..b1 according to this table; b7..b4 proprietary
-	1	-	-	-	-	-	-	CREATE USER, DELETE USER
-	-	1	-	-	-	-	-	GRANT, REVOKE
-	-	-	1	-	-	-	-	CREATE TABLE, CREATE VIEW, CREATE DICTIONARY
-	-	-	-	1	-	-	-	DROP TABLE, DROP VIEW
-	-	-	-	-	1	-	-	INSERT
-	-	-	-	-	-	1	-	UPDATE, DELETE
-	-	-	-	-	-	-	1	FETCH

Table 9 - AM byte for DOs

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	-	-	-	-	-	-	-	b7..b1 according to this table
1	-	-	-	-	-	-	-	b3..b1 according to this table; b7..b4 proprietary
-	x	-	-	-	-	-	-	0 (1 = RFU)
-	-	x	-	-	-	-	-	0 (1 = RFU)
-	-	-	x	-	-	-	-	0 (1 = RFU)
-	-	-	-	x	-	-	-	0 (1 = RFU)
-	-	-	-	-	1	-	-	MANAGE SECURITY ENVIRONMENT
-	-	-	-	-	-	1	-	PUT DATA
-	-	-	-	-	-	-	1	GET DATA

Additional commands e.g. application specific commands may be added to the grouping of the commands presented in tables 6 to 9.

8.4.4 Security condition byte

The SC byte specifies which security mechanisms are necessary to conform to the access rules.

The 4 most significant bits indicate the required security conditions.

A SE may be specified in bits b4..b1. If a SE is specified, the mechanisms that may be defined in it for external authentication, user authentication and command protection shall be used, if indicated by bits b8..b5.

The coding of the SC byte is given in table 10.

Table 10 - Security condition byte

b8	b7	b6	b5	b4..b1	Meaning
0	0	0	0	0000	No condition
1	1	1	1	1111	Never
-	-	-	-	0000	No reference to SE
-	-	-	-	0001..1110	SE#
-	-	-	-	1111	RFU
0	-	-	-	-	At least one condition
1	-	-	-	-	All conditions
-	1	-	-	-	Secure messaging
-	-	1	-	-	External authentication
-	-	-	1	-	User authentication (e.g. password presentation)

If bit b8 = 1, all conditions set in bits b7..b5 shall be satisfied.

If bit b8 = 0, at least one of the conditions set in bits b7..b5 shall be satisfied.

If b7 =1, the CRT of the SE indicated in bits b4..b1 describes whether SM shall apply to the command APDU, the response APDU or both (see table 3).

8.5 Expanded format

8.5.1 Introduction

Access control to an object in this format is managed by referencing the access rules from the related object.

An access rule consists of:

— an AM_DO, as defined in table 11, followed by a sequence of

— SC_DOs, as defined in table 13.

Access rules with this encoding may be present in the value field of the DO with tag 'AB' (see table 1).

8.5.2 Access Mode data object (AM_DO)

An AM_DO contains either:

— an AM byte (see table 6 to table) or

— a list of command descriptions or

— a proprietary state machine description.

Subsequent SC_DOs are relevant for all commands indicated in the AM_DO. Table 11 shows the coding of AM_DOs.

Table 11 - AM_DOs

Tag	L	Value	Meaning
'80'	1	AM byte	See table 6 to table 9
'81'..'8F'	x	Command description (e.g. INS-P2 || INS-P2)	List of CLA-INS-P1-P2, the existence of which in the list is determined by the bits b4..b1 of the tag byte according to table 12
'9C'	x		Proprietary state machine description

If the tag ranges from '81' to '8F' then the value field of the AM_DO represents a list of possible combinations of CLA-INS-P1-P2 to be compared to the command header. Depending on b4..b1 of the tag the list contains only the indicated reference values as described in table 12. The existing byte groups may appear repeatedly in order to define a set of commands being protected.

Table 12 - Coding of b4..b1 of the AM_DO tag byte

b4	b3	b2	b1	Meaning
1	x	x	x	CLA exists in definition list
x	1	x	x	INS exists in definition list
x	x	1	x	P1 exists in definition list
x	x	x	1	P2 exists in definition list

In the CLA byte, if used in the command description, the logical channel number shall be set to 0 with the meaning that the description is independent from the particular logical channel being applied.

8.5.3 Security condition data objects (SC_DO)

The SC_DO defines the required security actions in order to access an object being protected through the particular AM_DO:

— to be performed before accessing an object (e.g. authentication);

— to protect commands or responses by secure messaging.

Table 13 shows the coding of SC_DOs.

Table 13 - SC_DOs

Tag T_{SC_DO}	L	Value	Description of access condition
'90'	'00'	-	Always
'97'	'00'	-	Never
'A4'	x	CRT value	Authentication (external authentication or user authentication) depending on the CRT usage
'B4' 'B6' 'B8'	x	CRT value	CRTs for command and/or response with SM depending on CRT usage
'9E'	x	SC byte according to table 10	Security Condition byte
'A0'	x	SC_DOs	OR template
'AF'	x	SC_DOs	AND template

Several SC_DOs may be attached to a particular operation:

— if the SC_DOs are encapsulated in an OR template, then only one of the security conditions has to be fulfilled for the operation to be allowed;

— if the SC_DOs are not to be encapsulated in an OR template or if the SC_DOs are encapsulated in an AND template, then all security conditions shall be fulfilled before the operation is allowed.

8.5.4 Access rule references

Access rules in expanded format (AM_DOs and SC_DOs) may be stored in a linear variable EF, each record containing one or more rules (see table 14). The access rule file may be an internal file, referenced implicitly, or may be referenced explicitly, e.g. by a File ID (File Identifier, see ISO/IEC 7816-4).

In the FCP an access rule stored in a file may be referenced in a DO with tag '8B' (See table 1). The value of this DO contains at least one record number, called Access Rule Reference (ARR). It may be:

— three bytes containing two bytes with the File ID of the access rule file followed by one byte with the record number for the access rule or

— a single byte containing the record number of the rule, valid if the access rule file is (implicitly) known.

NOTE — The access rule file may be known after a reference in the FCP (in DO tag '8B') of a DF, e.g. an application DF.

Table 14 - Layout of EF_{ARR} showing access rules

Record Number (ARR)	Record Content (Access Rules)
'01'	AM_DO || SC_DO_1 || SC_DO_2 || AM_DO || ...
'02'	AM_DO || SC_DO_1 ...

The ARR represents the value of the security attributes (tag '8B', see table 1).

Table 15– Security attribute DO referencing expanded format

Tag	Length	Value
'8B'	'01'	<ARR>
	'03'	<File ID><ARR>
	'02' + n x '02'	<File ID><$SEID_1$><ARR_1>..<$SEID_n$><ARR_n>

If the value field is coded with a length '01' it represents the ARR.

If the value field is coded with a length '03' it represents the File ID together with an ARR, whereby the File ID denotes the file containing the access rules referenced by the ARR.

If the value field is coded with a length '02' + n x '02', for n>1, it contains one or more SEID/ARR pairs, where the SEID codes the SE# on one byte. For each SE, the access rules indicated in the ARR following its SE# are valid.

The ARR of the current SE indicates the access rules, valid for the current access to the file.

NOTE — if no SE# is set in a former MANAGE SECURITY ENVIRONMENT command, then the SEID = '01' (default SE) is the current SE.

9 Commands

9.1 Definition and scope

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

Unless specifically stated, status conditions are as defined in ISO/IEC 7816-4.

Transitions between the file life cycle states defined in clause 6 may be achieved using dedicated commands.

9.2 CREATE FILE command

9.2.1 Definition and Scope

The CREATE FILE command initiates the creation of a file (DF or EF) placed immediately under the current DF. Upon successful completion of the command the created file shall be set as the current file, unless otherwise specified by e.g. proprietary options of the CREATE FILE command.

This command may allocate memory to the file it creates.

The behaviour of a card if more than one EF with a given short EF identifier exists in the same DF is not defined in this part of ISO/IEC 7816.

9.2.2 Conditional usage and security

The command can be performed only if the security status satisfies the security attributes for the current DF.

If a DF is created, a filename and / or a file identifier shall be specified. If an EF is created, a file identifier and / or a short EF identifier shall be specified.

The file descriptor byte is mandatory.

NOTE — This byte indicates whether a DF or an EF is to be created.

9.2.3 Command message

Table 16 - CREATE FILE command APDU

CLA	As defined in ISO/IEC 7816-4
INS	'E0'
P1-P2	P1-P2 = '0000': File ID and file parameters encoded in data field
	P1 ≠ '00': File descriptor
	P2
	- 5 most significant bits = short EF identifier
	- 3 least significant bits = proprietary
Lc field	Empty or length of the subsequent data field
Data field	FCP template, tag '62' with DOs according to table 1, and possible further templates (see ISO/IEC 7816-4, file control information)
Le field	Empty

NOTE — When Lc is empty the created file has default file control parameters.

9.2.4 Response message

Table 17 - CREATE FILE response APDU

Data field	Empty
SW1-SW2	Status bytes

9.2.5 Status conditions

The following specific error conditions may occur:

— SW1 = '69' with SW2 =

• '82': Security status not satisfied

— SW1 = '6A' with SW2 =

• '84': not enough memory space;

• '89': file already exists;

• '8A': DF name already exists.

9.3 DELETE FILE command

9.3.1 Definition and Scope

This command initiates the deletion of a referenced EF immediately under the current DF, or a DF with its complete subtree. After successful completion of this command, the deleted file can no longer be selected. The resources held by the file shall be released and the memory used by this file shall be set to the logical erased state.

The current file after deletion of an EF is the current DF. The current DF after deletion of a DF is the parent DF, if not otherwise defined.

9.3.2 Conditional usage and security

The command can be performed only if the security status satisfies the security attributes for the command. The deletion of the file may additionally depend on the file life status.

If P1-P2 = '0000' and if the data field is empty, then the command applies to the file that has been selected by the command executed directly before.

Other meanings of P1-P2 including the rules defining the uniqueness of File IDs, are defined in the SELECT FILE command in ISO/IEC 7816-4.

The command shall not be executed if there is more than one logical channel open.

The MF shall not be deleted.

9.3.3 Command message

Table 18 - DELETE FILE command APDU

CLA	As defined in ISO/IEC 7816-4
INS	'E4'
P1-P2	as defined for the SELECT FILE command (see ISO/IEC 7816-4)
Lc field	Empty or length of subsequent data
Data field	as defined for the SELECT FILE command (see ISO/IEC 7816-4)
Le field	Empty

9.3.4 Response message

Table 19 - DELETE FILE response APDU

Data field	Empty
SW1-SW2	Status bytes

9.3.5 Status conditions

The following specific error conditions may occur:

— SW1 = '69' with SW2 =

• '82': Security status not satisfied

9.4 DEACTIVATE FILE command

9.4.1 Definition and Scope

This command initiates a reversible deactivation of a file. After a successful completion of the command, only the SELECT FILE, ACTIVATE FILE, DELETE FILE, TERMINATE EF and, in the case of a DF, TERMINATE DF commands shall be allowed.

The SELECT FILE command selecting a deactivated file will select the file and return the warning status SW1-SW2 = '6283' (selected file invalidated i.e. deactivated) according to ISO/IEC 7816-4.

If an EF is selected then the command shall only be applied to the EF and not to the parent DF.

9.4.2 Conditional usage and security

The command can be performed only if the security status satisfies the security attributes defined for this command.

If P1-P2 = '0000' and if the data field is empty, then the command applies to the file that has been selected by the command executed directly before.

Other meanings of P1-P2 including the rules defining the uniqueness of File IDs, are defined in the SELECT FILE command in ISO/IEC 7816-4.

The command APDU should be protected by secure messaging (SM). If the response APDU is not protected, then the way to check that the function has been properly executed is not defined within the scope of ISO/IEC 7816.

For security reasons, the same functionality may be achieved by proprietary means.

9.4.3 Command message

Table 20 - DEACTIVATE FILE command APDU

CLA	As defined in ISO/IEC 7816-4
INS	'04'
P1-P2	as defined for the SELECT FILE command (see ISO/IEC 7816-4)
Lc field	Empty or length of subsequent data field
Data field	as defined for the SELECT FILE command (see ISO/IEC 7816-4)
Le field	Empty

9.4.4 Response message

Table 21 - DEACTIVATE FILE response APDU

Data field	Empty
SW1-SW2	Status bytes

9.4.5 Status conditions

The following specific error conditions may occur:

— SW1 = '69' with SW2 =

• '82': Security status not satisfied

— SW1 = '6A' with SW2 =

• '80': Incorrect parameters in data field (e.g. selected file and file specified in the command don't match)

9.5 ACTIVATE FILE command

9.5.1 Definition and Scope

This command initiates the transition of a file from

— the creation state or

— the initialisation state or

— the operational state (deactivated)

to the operational state (activated).

9.5.2 Conditional usage and security

Activating a correctly created file is always allowed. Activating a deactivated file can only be performed if the security status satisfies the security attributes defined for this file for the activation function.

If the response APDU is not protected, then the way to check that the function has been properly executed is not defined within the scope of ISO/IEC 7816.

If P1-P2 = '0000' and if the data field is empty, then the command applies to the file that has been selected by the command executed directly before.

Other meanings of P1-P2 including the rules defining the uniqueness of File IDs, are defined in the SELECT FILE command in ISO/IEC 7816-4.

9.5.3 Command message

Table 22 - ACTIVATE FILE command APDU

CLA	As defined in ISO/IEC 7816-4
INS	'44'
P1-P2	as defined for the SELECT FILE command (see ISO/IEC 7816-4)
Lc field	Empty or length of subsequent data
Data field	as defined for the SELECT FILE command (see ISO/IEC 7816-4)
Le field	Empty

9.5.4 Response message

Table 23 - ACTIVATE FILE response APDU

Data field	Empty
SW1-SW2	Status bytes

9.5.5 Status conditions

The following specific error conditions may occur:

— SW1 = '64' with SW2 =

• '00': Execution error (e.g. created file could not be activated);

— SW1 = '69' with SW2 =

• '82': Security status not satisfied.

9.6 TERMINATE DF command

9.6.1 Definition and Scope

The TERMINATE DF command initiates the irreversible transition of the currently selected DF into the termination state.

Following a successful completion of the command, the DF is in a terminated state and the functionality available from the DF and its subtree is reduced. The DF shall be selectable and if selected the warning status SW1-SW2 = '6285' (selected file in termination state) shall be returned.

Further possible actions are not defined in ISO/IEC 7816.

For security reasons, the same functionality may be achieved by proprietary means.

If P1-P2 = '0000' and if the data field is empty, then the command applies to the file that has been selected by the command executed directly before.

Other meanings of P1-P2 including the rules defining the uniqueness of File IDs, are defined in the SELECT FILE command in ISO/IEC 7816-4.

NOTE — the intent of DF termination is generally to make the application unusable by the cardholder.

9.6.2 Conditional usage and security

The command APDU should be protected by secure messaging (SM). If the response APDU is not protected, then the way to check that the function has been properly executed is not defined within the scope of ISO/IEC 7816.

9.6.3 Command message

Table 24 - TERMINATE DF command APDU

CLA	As defined in ISO/IEC 7816-4
INS	'E6'
P1-P2	as defined for the SELECT FILE command (see ISO/IEC 7816-4)
Lc field	Empty or length of subsequent data
Data field	as defined for the SELECT FILE command (see ISO/IEC 7816-4)
Le field	Empty

9.6.4 Response message

Table 25 - TERMINATE DF response APDU

Data field	Empty
SW1-SW2	Status bytes

9.6.5 Status conditions

The following specific error conditions may occur:

— SW1 = '69' with SW2 =

• '82': Security status not satisfied

9.7 TERMINATE EF command

9.7.1 Definition and Scope

The TERMINATE EF command initiates the irreversible transition of the specified EF into the termination state.

9.7.2 Conditional usage and security

The EF to be terminated shall be in an activated or deactivated state.

The command can be performed only if the security status satisfies the security attributes defined for this command.

For security reasons, the same functionality may be achieved by proprietary means.

If P1-P2 = '0000' and if the data field is empty, then the command applies to the file that has been selected by the command executed directly before.

Other meanings of P1-P2 including the rules defining the uniqueness of File IDs, are defined in the SELECT FILE command in ISO/IEC 7816-4.

9.7.3 Command message

Table 26 - TERMINATE EF command APDU

CLA	As defined in ISO/IEC 7816-4
INS	'E8'
P1-P2	as defined for the SELECT FILE command (see ISO/IEC 7816-4)
Lc field	Empty or length of subsequent data
Data field	as defined for the SELECT FILE command (see ISO/IEC 7816-4)
Le field	Empty

9.7.4 Response message

Table 27 - TERMINATE EF response APDU

Data field	Empty
SW1-SW2	Status bytes

9.7.5 Status conditions

The following specific error conditions may occur:

— SW1 = '69' with SW2 =

• '82': Security status not satisfied

9.8 TERMINATE CARD USAGE command

9.8.1 Definition and Scope

The TERMINATE CARD USAGE command initiates the irreversible transition of the card into the termination state. Use of this command gives an implicit selection of the MF.

For cards supporting this command, the termination state should be indicated in the ATR (see ISO/IEC 7816-4) using the coding shown in table 2.

Following a successful completion of the command, the SELECT FILE command shall not be supported by the card.

For security reasons, the same functionality may be achieved by proprietary means.

NOTE — The intent of terminating card usage is to make the card unusable by the cardholder.

9.8.2 Conditional usage and security

The command APDU should be protected by secure messaging (SM). If the response APDU is not protected, then the way to check that the function has been properly executed is not defined within ISO/IEC 7816.

9.8.3 Command message

Table 28 - TERMINATE CARD USAGE command APDU

CLA	As defined in ISO/IEC 7816-4
INS	'FE'
P1-P2	'0000'
Lc field	Empty
Data field	Empty
Le field	Empty

9.8.4 Response message

Table 29 - TERMINATE CARD USAGE response APDU

Data field	Empty
SW1-SW2	Status bytes

9.8.5 Status conditions

The following specific error conditions may occur:

— SW1 = '69' with SW2 =

• '82': Security status not satisfied

9.9 SEARCH BINARY command

9.9.1 Definition and Scope

The SEARCH BINARY command initiates a search within transparent files.

The SEARCH BINARY response message gives the offset in a transparent EF of a data unit. The value of the byte in the EF at the offset returned shall be identical to the data field in the command message. The search starts with the offset given in P1-P2.

When the data field of the command message is empty the SEARCH BINARY response message gives the offset of the first data unit in a logically erased state.

9.9.2 Conditional usage and security

The command can be performed only if the security status satisfies the security attributes defined for this command.

When the command contains a valid short EF identifier, it sets the file as the current EF.

The command is processed on the currently selected EF.

The command shall be aborted if it is applied to a non-transparent EF.

9.9.3 Command message

Table 30 - SEARCH BINARY command APDU

CLA	As defined in ISO/IEC 7816-4
INS	'A0'
P1-P2	See text below
Lc field	Empty or length of the subsequent data field
Data field	Empty or search string
Le field	Empty or '02'

If b8 = 1 in P1 then:

— b7 and b6 of P1 are set to 0 (RFU bits);

— b5 to b1 are a short EF identifier;

— P2 is the offset of the first byte from which to start searching, in data units from the beginning of the file.

If b8 = 0 in P1 then P1-P2 is the offset of the first byte from which to start searching, in data units from the beginning of the file.

9.9.4 Response message

Table 31 - SEARCH BINARY response APDU

Data field	offset of the data unit, the contents of which match the command data field, in units from the beginning of the file
SW1-SW2	Status bytes

NOTE — the data field is empty either if the Le field is empty or if no match is found.

9.9.5 Status conditions

The following specific warning conditions may occur:

— SW1 = '62' with SW2 =

• '82': End of file reached before finding matching string

— SW1 = '69' with SW2 =

• '82': Security status not satisfied

9.10 SEARCH RECORD command

9.10.1 Definition and Scope

The SEARCH RECORD command initiates a simple search, an enhanced search or a proprietary search on stored data within a linear or a cyclic EF.

The search can be limited to records with a given identifier or to those having a higher / lower record number than a given value. It can be executed in increasing / decreasing order of record numbers.

The search starts either:

— at the first byte of the record(s) (simple search) or

— from a given offset in the record(s) (enhanced search) or

— from the first occurrence of a given byte in the record(s) (enhanced search).

The SEARCH RECORD response message gives the record number(s) which match the search criteria, within a linear or cyclic EF.

NOTE — Record identifier(s) are not given in a response message since they may not be unique.

9.10.2 Conditional usage and security

The command can be performed only if the security status satisfies the security attributes defined for this command.

In variable record length files, if the search pattern is longer than the record length, the appropriate record shall not be included in the search.

If the length of the search pattern exceeds the record length of a linear fixed file, the card shall abort the operation with an appropriate error code.

If one or more matches are found the record pointer shall be set to the first record where the search pattern was found.

9.10.3 Command message

Table 32 - SEARCH RECORD command APDU

CLA	As defined in ISO/IEC 7816-4
INS	'A2'
P1	Record number or record identifier ('00' indicates the current record
P2	See table 33
Lc	Length of subsequent data field
Data field	If P2 is not equal to 'xxxxx11x' (simple search): search string If P2 equals 'xxxxx110' (enhanced search): search indication (2 bytes) followed by search string If P2 equals 'xxxxx111' (proprietary search): data field is proprietary
Le	Empty or maximum length of response data

Table 33 - Coding of P2

b8..b4	b3..b1	Description
0 0 0 0 0	- - -	- Currently selected EF
x x x x x (not all equal)	- - -	- Short EF Identifier
1 1 1 1 1		RFU
		Simple Search
	0 x x	Use of P1 as a record identifier
	0 0 0	Search forward from first occurrence
	0 0 1	Search backward from last occurrence
	0 1 0	Search forward from next occurrence
	0 1 1	Search backward from previous occurrence
	1 0 x	Use of P1 as record number
	1 0 0	Search forward from record indicated in P1
	1 0 1	Search backward from record indicated in P1
		Other search modes
	1 1 0	Enhanced search (See table 34 for search indication)
	1 1 1	Proprietary search

Table 34 – Coding of first byte of the search indication for enhanced search mode

b8..b5	b4	b3..b1	Description
00000	0	x x x	The search starts in the record from the offset (absolute position) given in the second byte of the search indication
	1	x x x	The search starts in the record after the first occurrence of the value contained in the second byte of the search indication
		0 x x	Use of PI as a record identifier
		0 0 0	Search forward from first occurrence
		0 0 1	Search backward from last occurrence
		0 1 0	Search forward from next occurrence
		0 1 1	Search backward from previous occurrence
		1 x x	Use of P1 as a record number
		1 0 0	Search forward from record indicated in P1
		1 0 1	Search backward from record indicated in P1
		1 1 0	Search forward from next record
		1 1 1	Search backward from previous record
All other values are RFU			

9.10.4 Response message

Table 35 – SEARCH RECORD response APDU

Data field	- Empty or record number(s)
SW1 – SW2	Status bytes

NOTE – the data field is empty either if the Le field is empty or if no match is found.

9.10.5 Status conditions

The following specific error may occur:

Le > Response data length

— SW1 = '6C' with SW2 = 'XX' : wrong length Le: SW2 indicates the exact length.

The following specific warnings may occur :

— SW1 = '62' with SW2 = '82' : End of file reached before finding matching string ;

— SW1 = '69' with SW2 = '82' : Security status not satisfied.

10 Card originated messages

10.1 Definition

This clause describes a service whereby it is the card, not the IFD, that originates a message. This allows both card to IFD communication and card to card communication. In addition this communication may be carried out over a network.

This clause covers the definition of:

— SW1-SW2 values acting as a trigger indicating that a card wants to issue a message and expects a reply;

— The particular use of the GET DATA command, which retrieves this message;

— The particular use of the PUT DATA command, which transmits a reply, if any, to the message;

— The format of the messages sent and of the replies received by the card.

10.2 Triggering by the card

When SW1 is equal to '62', SW2 = 'XY' in the range '02'..'80' warns that the IFD should retrieve a message of 'XY' bytes, for which the card possibly expects a reply (see 10.3).

When SW1 is equal to '64', SW2 = 'XY' in the range '02'..'80' indicates that the command has been rejected, and that a possible execution of the command is conditional on the recovery of a message of 'XY' bytes, for which the card possibly expects a reply.

If present in the ATR (see ISO/IEC 7816-4), SW1 SW2 have the same meaning as defined above.

The rejection of the reply with SW1 equal to '64', SW2 in the range '02'..'80' means that the card wants to send at least one more message.

The rejection of a command with SW1 equal to '64', SW2 = '01' means that the card is expecting an immediate reply.

10.3 Message retrieval and reply

The message available in the card is retrieved by the IFD through a GET DATA command with P1 P2 = '0000', Lc = 'XY'.

— When SW1 SW2 warns that the IFD should retrieve a message, further messages should be concatenated to the received message before processing in the outside world.

— When SW1 SW2 = '9000' the completed message may be processed by the outside world.

The reply, if any, shall be transmitted by the IFD to the card in the data field of a PUT DATA command with P1 P2 = '0000'.

Command chaining, as defined in ISO/IEC 7816-8, applies when the reply is too long for one PUT DATA command.

10.4 Message and reply formats

All messages retrieved from the card are coded as follows:

— if the first byte of the message is not equal to 'FF', then the message is a command APDU, as defined in ISO/IEC 7816-4;

— if the first byte of the message is equal to 'FF', then the following bytes of the message code an initial protocol identifier, according to ISO/IEC TR 9577.

The replies to the message(s) retrieved from the card shall be either:

— a response APDU, as defined in ISO/IEC 7816-4 or

— a reply in compliance with the protocol indicated in the message retrieved from the card.

10.5 Conditions of use

All conditions are relevant to the protocol indicated in the message, except for the proper use of:

— SW1-SW2 values;

— GET DATA and PUT DATA commands.

In particular, this standard does not make any assumptions:

— on the need for a reply;

— on the entity responsible for the contents of the possible reply.

Annex A
(normative)

File life cycle states

A.1 Commands

The following dedicated commands may be used for initiating a life cycle state transition:

CREATE FILE	TERMINATE CARD USAGE
ACTIVATE FILE	TERMINATE DF
DEACTIVATE FILE	TERMINATE EF
	DELETE FILE

Figure A.1 is a conceptual representation of the file life cycle states and the commands which invoke a transition upon successful completion. It does not show the conditions of execution of those commands.

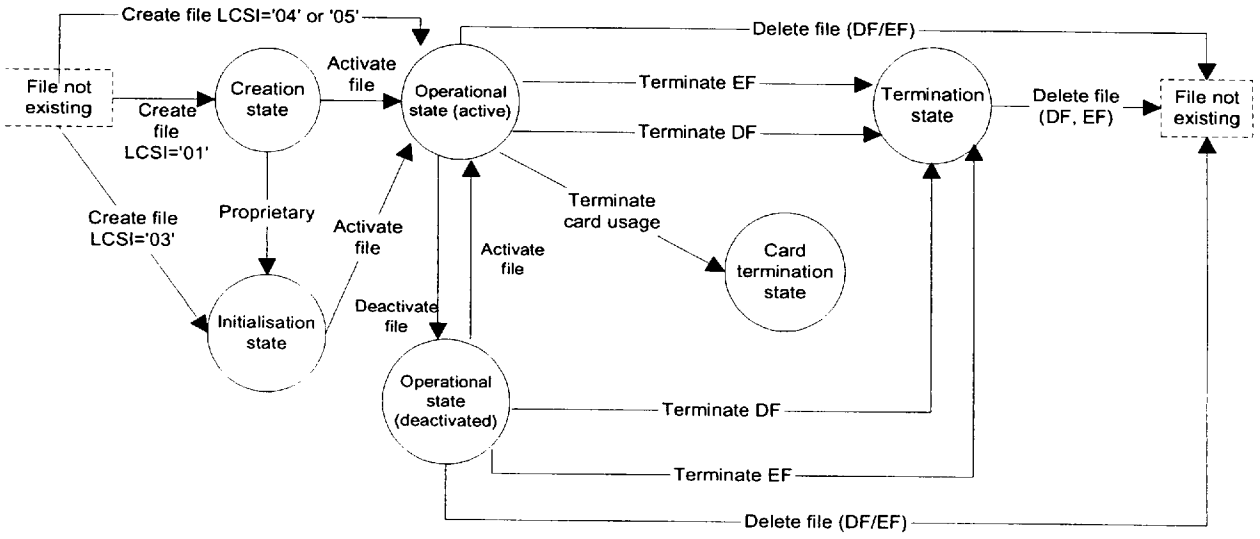

Figure A.1 - Diagram for file life cycle states

Annex B
(informative)

Usage example of security attributes for download

B.1 Introduction

This example shows how to control the loading of data (secure download) into the card or into an EF or DF, by means of verifying the access rights of the loading entity and protection of the transmitted data with secure messaging. The loading data may contain e.g. code, keys and applets.

B.2 Assumptions

- ISO/IEC 7816-4 file system
- Command structure, life cycle and access control according to ISO/IEC 7816-4 and ISO/IEC 7816-8 and this part of the standard.
- Current DF is already in operational state (LCSI = 4).
- Data to be loaded into a subsidiary transparent file 1 (DF/EF in initialisation state (LCSI = 3)).
- SE #2 for LCSI = 3, initialisation state, and online communication, present in the current DF.
- SE #3 for LCSI = 3, initialisation state, and offline communication, present in the current DF.
- SE #4 for LCSI = 4, operational state, present in the current DF.
- The data are protected authentically and may be enciphered optionally by secure messaging data objects (see ISO/IEC 7816-4).
  - In an online communication (SE #2) an asymmetric authentication process has been successfully executed before, e.g. with session key exchange to be used to protect the loading by secure messaging. The data to be loaded are protected by a cryptographic checksum DO and optionally by a cryptogram DO (see ISO/IEC 7816-4).
  - In an offline communication (SE #3) the data to be loaded are protected by a digital signature DO and optionally enciphered by a cryptogram DO (see ISO/IEC 7816-4).
- Authorisation information (certificate holder authorisation) may be present inside a corresponding CV Certificate (see ISO/IEC 7816-8, Annex A), binding the loading entity to the authentication key (SE #2, online communication) or to the digital signature key (SE #3, offline communication) and to its access rights (see 7.4).

B.3 Secure downloading

Secure downloading under online and offline conditions is described below.

B.3.1 Online communication

- Select the current DF (SELECT FILE (DF AID))
- Set initialisation state for online communication (MSE: RESTORE SE #2)
- External authentication (PSO: VERIFY CERTIFICATE, EXTERNAL AUTHENTICATE)
- Select file 1 (SELECT FILE (File ID))
- Load data into the file (e.g. WRITE BINARY) with SM, protected by cryptographic checksum DO

— Activation of file (ACTIVATE FILE)
— Set operational state (MSE:RESTORE SE #4)
— Verify user authentication (VERIFY (password))
— Select file 1 (SELECT FILE (File ID))
— Read information (READ BINARY)

B.3.2 Offline communication

— Select the current DF (SELECT FILE (DF AID))
— Set initialisation state for offline communication (MSE: RESTORE SE #3)
— Verification of certificate (PSO: VERIFY CERTIFICATE)
— Select file 1 (SELECT FILE (File ID))
— Load data into the file with SM (e.g. WRITE BINARY) protected by digital signature DO
— Activation of file (ACTIVATE FILE)
— Set operational state (MSE: RESTORE SE #4)
— Verify user authentication (VERIFY (password))
— Select file 1 (SELECT FILE (File ID))
— Read information (READ BINARY)

B.4 Compact format coding for security attributes of EF 1

The following coding illustrates that the access in the operational state may be different from the access in the initialisation state.

B.4.1 Online communication

According to table 5, table 7 and table 10, if a WRITE BINARY and (after successful completion) an ACTIVATE FILE is allowed in the initialisation state and a READ BINARY is allowed in the operational state for a certain security state, the coding of the AM Byte and SC Bytes are the following:

Initialisation state:

— AM Byte (ACTIVATE FILE (b5 =1), WRITE BINARY (b3 =1))
— SC Byte 1 (All conditions (b8 =1), Secure Messaging for ACTIVATE FILE (b7 =1))
— SC Byte 2 (All conditions (b8 =1), External authentication and Secure Messaging for WRITE BINARY (b7 =1, b6 =1))

Operational state:

— AM Byte (READ BINARY (b1 =1))
— SC Byte (User authentication (b5 =1))

The SE #2 and SE #4 may be coded in the bits b4-b1 (SE #2: b4...b1 = '0010', SE #4: b4..b1 = '0100') of the SC bytes.

Or the corresponding SE may be coded as the current SE (b4..b1 = '0000'). In this case the security attributes are coded in accordance to table 15 (expanded format).

B.4.2 Offline communication

According to table 6 and table 10, if a WRITE BINARY and (after successful completion) an ACTIVATE FILE is allowed in the initialisation state and a READ BINARY is allowed in the operational state for a certain security state, the coding of the AM Byte and SC Bytes are the following:

Initialisation state:

— AM Byte (ACTIVATE FILE (b5 =1), WRITE BINARY (b3 =1))
— SC Byte 1 (All conditions (b8 =1), Secure Messaging for ACTIVATE FILE (b7 =1))
— SC Byte 2 (All conditions (b8 =1), Secure Messaging for WRITE BINARY (b7 =1))

Operational state:

— AM Byte (READ BINARY (b1 =1))
— SC Byte (User authentication (b5 =1))

The SE #3 and SE #4 may be coded in the bits b4-b1 (SE #3: b4...b1 = '0011', SE #4: b4..b1 = '0100') of the SC bytes.

Or the corresponding SE may be coded as the current SE (b4..b1 = '0000'). In this case the security attributes are coded in accordance to table 15 (expanded format).

B.5 Expanded format coding for security attributes of EF 1

B.5.1 Online communication

According to table 11 and table 13, if a WRITE BINARY and (after successful completion) an ACTIVATE FILE is allowed in the initialisation state and a READ BINARY is allowed in the operational state for a certain security state the coding of the AM_DOs and SC_DOs may be the following:

Initialisation state:

— AM_DO 1 contains as DE the AM Byte (WRITE BINARY (b3 =1)).
— SC_DO 1 contains as DE CRT for authentication AT including the key reference DO and the CRT usage qualifier DO for external authentication (b8 =1).
— SC_DO 2 contains as DE the CRT for cryptographic checksum CCT including the DO for key reference and the CRT usage DO for secure messaging (b5 =1, b6 =1).
— AM_DO 2 contains as DE the AM Byte (ACTIVATE FILE (b5 =1)).
— SC_DO 3 contains as DE the CRT for cryptographic checksum CCT including the DO for key reference and the CRT usage DO for secure messaging (b5 =1, b6 =1).

Operational state:

— AM_DO contains as AM Byte (READ BINARY (b1 =1)).
— SC_DO contains the CRT AT including the key reference DO and the CRT usage qualifier DO indicating user authentication (b4 =1).

The corresponding SE is coded as the current SE (b4..b1 = '0000'). In this case the security attributes are coded in accordance to table 15 (expanded format).

B.5.2 Offline communication

According to table 11 and table 13, if a WRITE BINARY and (after successful completion) an ACTIVATE FILE is allowed in the initialisation state and a READ BINARY is allowed in the operational state for a certain security state the coding of the AM_DOs and SC_DOs are the following:

Initialisation state:

— AM_DO 1 contains as DE the AM Byte (WRITE BINARY (b3 =1), ACTIVATE FILE (b5 =1)).

— SC_DO 1 contains as DE CRT DST including the key reference DO and the CRT usage qualifier DO for secure messaging (b5 =1, b6 =1).

Operational state:

— AM_DO contains as AM Byte (READ BINARY (b1 =1)).

— SC_DO contains the CRT AT including the key reference DO and the CRT usage qualifier DO indicating user authentication (b4 =1).

The corresponding SE is coded as the current SE. In this case the security attributes are coded in accordance to table 15 .

B.6 Coding of the corresponding Secure Environments (SEs)

Coding of SE #2 (see 7.3) inside the template ('7B')

('80' - L - '02') || ('8A' - L - '03') || ('A4' - L - ('83' - L - key reference) || ('95' - 01 - 80) || ('5F4B' - L - certificate holder authorisation)) || ('B4' - L - (('83' - L - key reference) || ('95' - 01 - 30))

Coding of SE #3 (see 7.3) inside the template ('7B')

('80' - L - '03') || ('8A' - L - '03') || ('B6' - L - ('83' - L - key reference) || ('95' - 01 - 30))

Coding of SE #4 (see 7.3) inside the template ('7B')

('80' - L - '04') || ('8C' - L - '04') || ('A4' - L - ('83' - L - key reference) || ('95' - 01 - 08))

ICS 35.240.15
Price based on 31 pages