INTERNATIONAL STANDARD

ISO/IEC 7816-9

Second edition
2004-06-01

Identification cards — Integrated circuit cards —

Part 9: Commands for card management

Cartes d'identification — Cartes à circuit intégré —

Partie 9: Commandes pour la gestion des cartes

Reference number
ISO/IEC 7816-9:2004(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 7816-9 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 7816-8, 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 —

Part 9:
Commands for card management

1 Scope

This document specifies interindustry commands for card and file management. These commands cover the entire life cycle of the card and therefore some commands may be used before the card has been issued to the cardholder or after the card has expired.

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 — Organization, security and commands for interchange*

3 Terms and definitions

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

3.1
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.

APDU application protocol data unit

FCP file control parameters

LCS life cycle status

1) To be published.

5 Life cycle

A life cycle status may be associated with any object in the card and with the card itself. The card shall use the life cycle status in combination with additional security attributes, to determine whether an operation on an object is in accordance with a security policy. The life cycle status reflects the use of objects according to the following rules.

— If an object is in creation state, then no security attribute for that object shall apply.

— If an object is in initialisation state, then any security attribute specific to this state may apply.

— If an object is in operational state, then every associated security attribute shall apply.

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

Transitions between primary life cycle states are irreversible and occur only from creation to termination. In addition, the application may define secondary life cycle states: each primary state may have reversible secondary states. Changes are controlled by the card and may be performed in a pre-defined order, reflecting reversible or irreversible changes in states. The following commands for card and file management may be used for initiating a life cycle state transition.

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

Commands may set the value of the life cycle status when they execute. However the card shall maintain the integrity of this value in accordance with this document.

5.1 File life cycle

Figure 1 is a conceptual representation of the file life cycle states and the commands that invoke a transition upon successful completion. It does not show the conditions of execution of those commands (see ISO/IEC 7816-4).

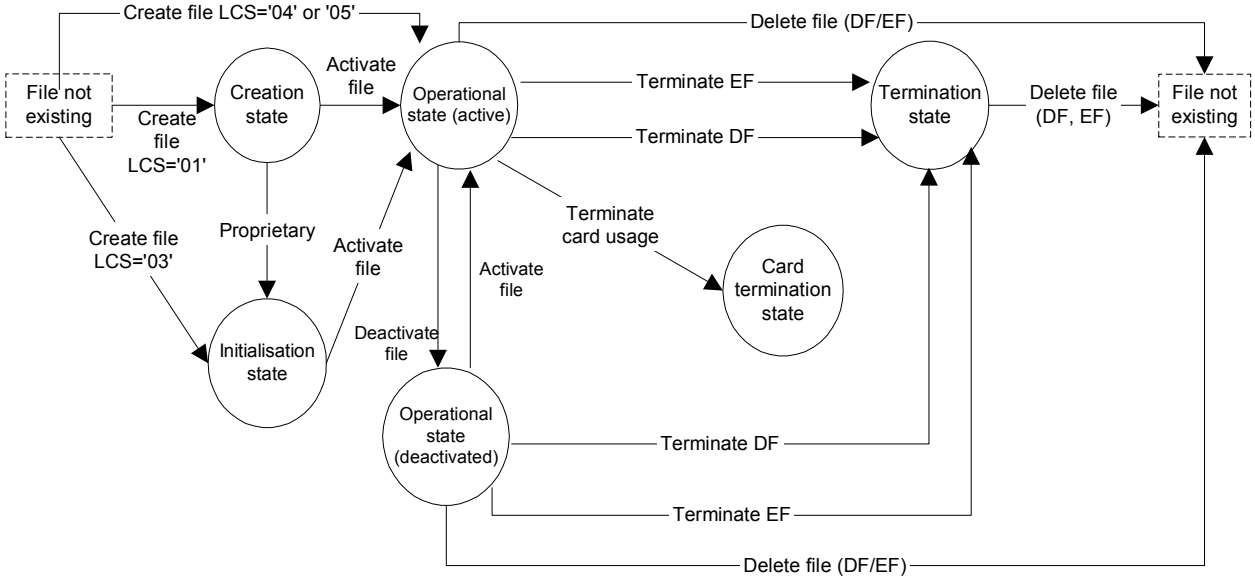

Figure 1 — Diagram for file life cycle

6 Commands for card management

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.

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

For these commands, bits 4 and 3 have no meaning and shall be ignored.

For each command, a non-exhaustive list of status conditions is provided, (see also ISO/IEC 7816-4).

6.1 CREATE FILE command

The CREATE FILE command initiates the creation of a file (DF or EF) placed immediately under the current DF. The command may allocate memory to the file it creates. The created file shall be set as the current file, unless otherwise specified.

When more than one EF with a given short EF identifier exists in the same DF, the behaviour of the card is not defined in this document.

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

The file descriptor byte is mandatory. It indicates whether a DF or an EF is to be created.

— If a DF is created, then a DF name and / or a file identifier shall be specified.

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

Table 1 — CREATE FILE command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	'E0'
P1-P2	'0000' File identifier and file parameters encoded in the command data field P1 not equal to '00': File descriptor byte P2 Short EF identifier on bits 8 to 4; bits 3 to 1 proprietary
Lc field	Absent for encoding Nc = 0, present for encoding Nc > 0
Data field	FCP template (tag '62') and possible further templates or absent
Le field	Absent for encoding Ne = 0

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4, Tables 5 and 6 where relevant, e.g. 6982, 6A84, 6A89, 6A8A

NOTE — If number N_c is zero, then the created file has default file control parameters.

6.2 DELETE FILE command

The DELETE FILE command initiates the deletion of a referenced EF immediately under the current DF, or of a DF with its complete sub-tree. After successful completion of this command, the deleted file can no longer be selected. 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. 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 deletion of the file may additionally depend on the file life status. The MF shall not be deleted.

If P1-P2 = '0000' and the command data field is absent, then the command applies to a file that has been selected by the command executed directly before. Furthermore, if the selected file is selected on another logical channel the execution of the command is aborted and an appropriate error is returned in the response.

Other meanings of P1-P2, including the rules defining the uniqueness of file identifiers, are defined in the SELECT command.

Table 2 — DELETE FILE command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	'E4'
P1-P2	'0000' Deletes current file
	Other values: as defined for the SELECT command (see ISO/IEC 7816-4)
L_c field	Absent for encoding Nc = 0, present for encoding Nc > 0
Data field	As defined for the SELECT command (see ISO/IEC 7816-4)
L_e field	Absent for encoding Ne = 0

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4, Tables 5 and 6 where relevant, e.g. 6982, 6985

6.3 DEACTIVATE FILE command

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

When applied to a deactivated file, the SELECT command will select the file and return SW1-SW2 = '6283' as a warning status: selected file invalidated, i.e., deactivated.

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

If P1-P2 = '0000' and if the command data field is absent, 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 identifiers, are defined in the SELECT command.

Secure messaging should be used. 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.

Table 3 — DEACTIVATE FILE command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	'04'
P1-P2	'0000' Deactivates current file
	Other values: as defined for the SELECT command (see ISO/IEC 7816-4)
L_c field	Absent for encoding Nc = 0, present for encoding Nc > 0
Data field	As defined for the SELECT command (see ISO/IEC 7816-4)
L_e field	Absent for encoding Ne = 0

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4, Tables 5 and 6 where relevant, e.g. 6982, 6A80

6.4 ACTIVATE FILE command

The ACTIVATE FILE command initiates the transition of a file state from either the creation state or the initialisation state or the operational state (deactivated) to the operational state (activated).

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 by secure messaging, 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 command data field is absent, 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 identifiers, are defined in the SELECT command.

Table 4 — ACTIVATE FILE command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	'44'
P1-P2	'0000' Activates current file
	Other values: as defined for the SELECT command (see ISO/IEC 7816-4)
L_c field	Absent for encoding Nc = 0, present for encoding Nc > 0
Data field	As defined for the SELECT command (see ISO/IEC 7816-4)
L_e field	Absent for encoding Ne = 0

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4, Tables 5 and 6 where relevant, e.g. 6400, 6982

6.5 TERMINATE DF command

The TERMINATE DF command initiates the irreversible transition of a DF into the termination state. After a successful completion of the command, the DF is in a terminated state and the functionality available from the DF and its sub-tree 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.

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

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

If P1-P2 = '0000' and if the command data field is absent, 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 identifiers, are defined in the SELECT command.

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

Table 5 — TERMINATE DF command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	'E6'
P1-P2	'0000' Terminates current DF Other values as defined for the SELECT command (see ISO/IEC 7816-4)
L_c field	Absent for encoding Nc = 0, present for encoding Nc > 0
Data field	As defined for the SELECT command (see ISO/IEC 7816-4)
L_e field	Absent for encoding Ne = 0

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4, Tables 5 and 6 where relevant, e.g. 6982, 6985

NOTE — In commands where P1P2 are encoded according to the SELECT command (see ISO/IEC 7816-4), bits 3 and 4 of P2 have no meaning and shall be ignored.

6.6 TERMINATE EF command

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

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

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

If P1-P2 = '0000' and if the command data field is absent, 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 identifiers, are defined in the SELECT command.

Table 6 — TERMINATE EF command-response pair

CLA	As defined in ISO/IEC 7816-4
INS	'E8'
P1-P2	'0000' Terminates current EF Other values: as defined for the SELECT command (see ISO/IEC 7816-4)
L_c field	Absent for encoding Nc = 0, present for encoding Nc > 0
Data field	As defined for the SELECT command (see ISO/IEC 7816-4)
L_e field	Absent for encoding Ne = 0

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4, Tables 5 and 6 where relevant, e.g. 6982, 6985

6.7 TERMINATE CARD USAGE command

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 Answer-to-Reset.

After a successful completion of the command, the card shall not support the SELECT command.

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.

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

Table 7 — TERMINATE CARD USAGE command-response pair

CLA INS P1-P2	As defined in ISO/IEC 7816-4 'FE' '0000'
L_c field	Absent for encoding Nc = 0
Data field	Absent
L_e field	Absent for encoding Ne = 0

Data field	Absent
SW1-SW2	See ISO/IEC 7816-4, Tables 5 and 6 where relevant, e.g. 6982, 6985

Annex A
(informative)

Examples of security attributes used for download

A.1 Introduction

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

The following assumptions are made:

— File system according to this document;

— Command structure, life cycle and access control according to this document;

— Current DF already in operational state (LCS = 4);

— Data to load into a subsidiary transparent file 1 (DF/EF in initialisation state (LCS = 3));

— SEID = 2 for LCS = 3, initialisation state, and online communication, present in the current DF;

— SEID = 3 for LCS = 3, initialisation state, and offline communication, present in the current DF;

— SEID = 4 for LCS = 4, operational state, present in the current DF;

— Data protected for authentication (and optionally enciphered) by secure messaging data objects;

— In an online communication (SEID = 2), an asymmetric authentication process has been successfully executed before, e.g., with session key exchange to use to protect the loading by secure messaging. The data to load are protected by a cryptographic checksum data object and optionally by a cryptogram data object.

— In an offline communication (SEID = 3), the data to load are protected by a digital signature data object and optionally enciphered by a cryptogram data object.

— Authorisation information (certificate holder authorisation) may be present inside a card-verifiable certificate binding the loading entity to the authentication key (SEID = 2, online communication) or to the digital signature key (SEID = 3, offline communication) and to its access rights.

A.2 Secure downloading

Secure downloading is described below, under online and offline communications.

Online communication

1. Select the current DF (SELECT (DF name = AID))

2. Set initialisation state for online communication (MSE: RESTORE SEID = 2)

3. External authentication (verify certificate, external authenticate)

4. Select file 1 (SELECT (file identifier))

5. Load data into the file (e.g., WRITE BINARY) with SM, protected by cryptographic checksum data object

6. Activation of file (ACTIVATE FILE)
7. Set operational state (MSE: RESTORE SEID = 4)
8. Verify user authentication (VERIFY (password))
9. Select file 1 (SELECT (file identifier))
10. Read information (READ BINARY)

Offline communication

1. Select the current DF (SELECT (DF name = AID))
2. Set initialisation state for offline communication (MSE: RESTORE SEID = 3)
3. Verification of certificate (VERIFY CERTIFICATE)
4. Select file 1 (SELECT (file identifier))
5. Load data into the file with SM (e.g., WRITE BINARY) protected by digital signature data object
6. Activation of file (ACTIVATE FILE)
7. Set operational state (MSE: RESTORE SEID = 4)
8. Verify user authentication (VERIFY (password))
9. Select file 1 (SELECT (file identifier))
10. Read information (READ BINARY)

A.3 Compact format coding for security attributes

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

Online communication

If a WRITE BINARY and (after successful completion) an ACTIVATE FILE are allowed in the initialisation state and a READ BINARY in the operational state for a certain security state, then the coding of the AM byte and SC bytes are as follows.

— **Initialisation state**

- AM byte (ACTIVATE FILE (bit 5 = 1), WRITE BINARY (bit 3 = 1))
- SC byte 1 (All conditions (bit 8 = 1), secure messaging for ACTIVATE FILE (bit 7 = 1))
- SC byte 2 (All conditions (bit 8 = 1), external authentication and secure messaging for WRITE BINARY (bits 7 to 6 = 11))

— **Operational** state

- AM byte (READ BINARY (bit 1 = 1))
- SC byte (User authentication (bit 5 = 1))

Either:

- bits 4 to 1 code a SE identifier (2 as 0010, 4 as 0100) in the SC bytes
- or the corresponding SE is identified as the current SE (0000); in this case the security attributes are coded in expanded format.

Offline communication

If a WRITE BINARY and (after successful completion) an ACTIVATE FILE are allowed in the initialisation state and a READ BINARY is allowed in the operational state for a certain security state, then the coding of the AM byte and SC bytes are as follows.

— **Initialisation state**

- AM byte (ACTIVATE FILE (bit 5 = 1), WRITE BINARY (bit 3 = 1))
- SC byte 1 (All conditions (bit 8 = 1), secure messaging for ACTIVATE FILE (bit 7 = 1))
- SC byte 2 (All conditions (bit 8 = 1), secure messaging for WRITE BINARY (bit 7 = 1))

— **Operational state**

- AM byte (READ BINARY (bit 1 = 1))
- SC byte (User authentication (bit 5 = 1))

Either:

- bits 4 to 1 code a SE identifier (3 as 0011, 4 as 0100) in the SC bytes
- or the corresponding SE is identified as the current SE (0000); in this case the security attributes are coded in expanded format.

A.4 Expanded format coding for security attributes

Online communication

If a WRITE BINARY and (after successful completion) an ACTIVATE FILE are allowed in the initialisation state and a READ BINARY in the operational state for a certain security state, then the coding of the AM data objects and SC data objects may be as follows.

— **Initialisation state**

- AM data object 1 conveys an AM byte (WRITE BINARY (bit 3 = 1))
- SC data object 1 conveys an AT including a key reference data object and a CRT usage qualifier data object for external authentication (bit 8 = 1).
- SC data object 2 conveys a CCT including a key reference data object and a CRT usage data object for secure messaging (bits 5 to 6 = 11).
- AM data object 2 conveys an AM byte (ACTIVATE FILE (bit 5 = 1))
- SC data object 3 conveys a CCT including a key reference data object and a CRT usage data object for secure messaging (bits 5 to 6 = 11)

— **Operational state**

- AM data object conveys an AM byte (READ BINARY (bit 1 = 1)).

- SC data object conveys an AT including a key reference data object and a CRT usage qualifier data object indicating user authentication (bit 4 = 1).

The corresponding SE is identified as the current SE (bits 4 to 1 = 0000). In this case the security attributes are coded in expanded format.

Offline communication

If a WRITE BINARY and (after successful completion) an ACTIVATE FILE are allowed in the initialisation state and a READ BINARY in the operational state for a certain security state, then the coding of the AM data objects and SC data objects are as follows.

— **Initialisation state**

- AM data object 1 conveys an AM byte (WRITE BINARY (bit 3 =1), ACTIVATE FILE (bit 5 = 1))
- SC data object 1 conveys a DST including a key reference data object and a CRT usage qualifier data object for secure messaging (bits 5 to 6 = 11)

— **Operational state**

- AM data object conveys an AM byte (READ BINARY (bit 1 = 1))
- SC data object conveys an AT including a key reference data object and a CRT usage qualifier data object indicating user authentication (bit 4 = 1)

The corresponding SE is identified as the current SE. In this case the security attributes are coded in expanded format.

A.5 Coding of the corresponding security environments

SEID = 2 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'}}

SEID = 3 inside the template (´7B´)

{'80' - L - '03'} - {'8A' - L - '03'} - {'B6' - L - {'83' - L - Key reference} - {'95' - '01' - '30'}}

SEID = 4 inside the template ('7B')

{'80' - L - '04'} - {'8C' - L - '04'} - {'A4' - L - {'83' - L - Key reference} - {'95' - '01' - '08'}}

Bibliography

[1] ISO/IEC 7816 (all parts), *Identification cards — Integrated circuit cards*

[2] ISO/IEC 10536 (all parts), *Identification cards — Contactless integrated circuit(s) cards — Close-coupled cards*

[3] ISO/IEC 14443 (all parts), *Identification cards — Contactless integrated circuit(s) cards — Proximity cards*

[4] ISO/IEC 15693 (all parts), *Identification cards — Contactless integrated circuit(s) cards — Vicinity cards*

ICS 35.240.15

Price based on 12 pages