Part 4

CT - BCS

Application independent
CardTerminal Basic Command Set
for ICC applications

Version 0.9

28.07.1995

TeleTrusT **Deutschland e.V.**

Project Editor:
GMD - Forschungszentrum Informationstechnik GmbH

Contents

Addresses:

TeleTrusT Deutschland e.V.
Eichendorffstr.16
D-99096 Erfurt
Germany

GMD
L. Eckstein, B. Struif
Rheinstr. 75
D-64295 Darmstadt
Germany

1. Scope

This specification describes the CardTerminal Basic Command Set (CT-BCS) used to control different types of CardTerminals:

- integrated CardTerminals with one or more ICC interfaces (e.g. a card reader integrated in the keyboard or in a disc slot, a PCMCIA card reader)

- external CardTerminals with one or more ICC interfaces and optional functional units such as display and key pad

The CT commands are application independent and may be used by any ICC orientated application system. They are constructed in compliance with the ISO/IEC 7816-4 inter-industry commands and used to control CardTerminals at the CardTerminal Application Programming Interface (CT-API) utilising the CT_data function (see CT-API specification).

The CT-BCS version defined here is open for further extension, e.g. a CT orientated file concept or the integration of security modules in the CardTerminal.

2. Normative references

Deutsche Telekom, GMD, RWTÜV, TeleTrusT Deutschland: 1995
CT-API 1.1 - Application independent CardTerminal Application Programming Interface for ICC applications

DIN NI-17: 1995
ICCs with synchronous transmission,
Part 1: ATR and data sections

DIN NI-17: 1995
ICCs with synchronous transmission,
Part 2: Transmission protocols

DIN NI-17.4: 1995
ICCs with synchronous transmission,
Part 3: Usage of inter-industry commands

ISO 3166: 1994
Codes for the representation of names of countries

ISO/IEC 7816-3: 1989
Identification cards - Integrated circuit(s) cards with contacts
Part 3 - Electronic Signals and transmission protocols
AM 1: Clause 9: Protocol T=1, asynchronous half duplex block transmission protocol
AM 2: Protocol type selection
(The WD October 1994 in which AM 1and AM 2 are integrated is used)

ISO/IEC 7816-4: 1995
Identification cards - Integrated circuit(s) cards with contacts
Part 4 - Inter-industry commands for interchange

ISO/IEC 7816-6: 1995
Identification cards - Integrated circuit(s) cards with contacts
Part 6 - Inter-industry data elements

CEN 1257-3: 1995 (Draft)
Identification card systems - Rules for Personal Identification Number handling in intersector environments - Part 3: PIN verification

CCITT Rec. T.50:
International Alphabet No. 5
(ISO 646: 1983, Information processing - ISO 7-bits coded character set for information interchange)

3. Abbreviations

ASN.1	= Abstract Syntax Notation One
ATR	= Answer-to-Reset
BCD	= Binary Coded Digits
BER	= Basic Encoding Rules
CHV	= Card Holder Verification
CR	= Carriage return
CT	= CardTerminal
CT-API	= CT Appl. Programming Interface
CT-BCS	= CT Basic Command Set
DAD	= Destination address
DO	= Data Object
FU	= Functional Unit
HB	= Historical Bytes
ICC	= Integrated Circuit(s) Card
PIN	= Personal Identification Number
PUK	= Personal Unblocking Key
RID	= Registered application provider ID
SAD	= Source address
TLV	= Tag, Length, Value
VD	= Verification Data

4. CT Command conventions

4.1 CT Command structure

CT commands are constructed in compliance with the ISO/IEC 7816-4 Inter-industry commands.

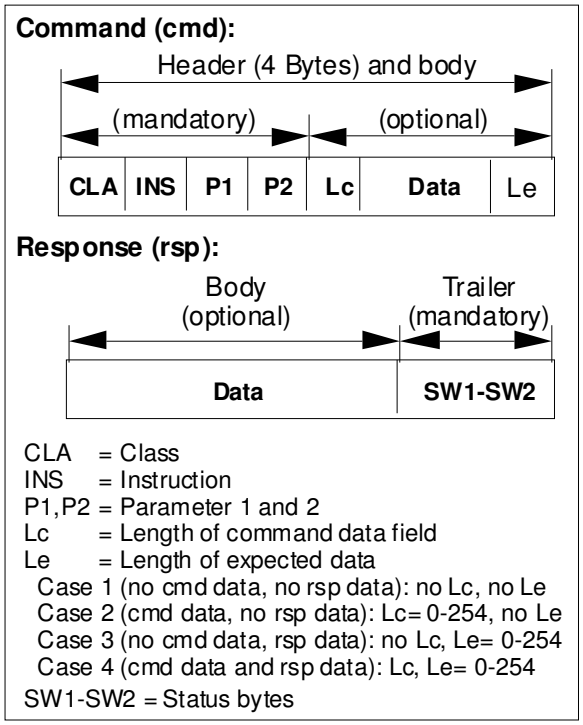

Fig. 1: CT command structure (identical with command structure in ISO/IEC 7816-4)

The CLA value used for CT-BCS commands is '20' to ensure compatibility with CT commands already being used.

The address value '01' (address of the CardTerminal) shall be used as destination address (DAD) at the CT-API for all CT-BCS commands (see CT-API specification).

4.2 CT command overview and general return codes

The following general CT commands are mandatory for all CardTerminals:

CardTerminal Command (mandatory for all CTs)	**INS-Code**
Reserved for Telekom command	´10´
RESET CT	´11´
REQUEST ICC	´12´
GET STATUS	´13´
Reserved for Telekom command	´14´
EJECT ICC	´15´

Tab. 1: General CT commands

The commands in Tab. 2 are only mandatory for CardTerminals with display and key pad.

CardTerminal Command (mandatory for all CTs with display and key pad)	**INS-Code**
INPUT	´16´
OUTPUT	´17´
PERFORM VERIFICATION	´18´
MODIFY VERIFICATION	´19´
Proprietary	´50´-´9F´
All other values	RFU

Tab. 2: Additional CT commands for CardTerminals with display and keypad

In the command descriptions only the special return codes are given. Further to these the following general return codes (status bytes) may occur:

´6700´ = Wrong length
´6900´ = Command not allowed
´6A00´ = Wrong parameters P1, P2
´6D00´ = Wrong instruction
´6E00´ = Class not supported

Note:
If an ICC command cannot be transmitted from the CT to the ICC because the ICC has been removed, is defective, or is in a state in which it no longer reacts, '6F00' is to be sent as return code and the CT to be named as sender of the response (SAD address).

4.3 Functional units

Functional units of a CT may be addressed in a CT command. The units and their coding as they may appear in CT command parameter P1 are listed in tab. 3.

Functional Unit	**Coding**	**Support**
CT kernel	´00´	mandatory
CT/ICC interface1	´01´	mandatory
CT/ICC interface2	´02´	conditional
...	...	...
CT/ICC interface14	´0E´	conditional
Display	´40´	conditional
Key pad	´50´	conditional

Tab. 3: CT functional units and their coding

5. General CT commands

5.1 RESET CT

5.1.1 Function

The RESET CT command causes the CardTerminal to carry out a reset of the specified unit (CT or CT functional units). If a software reset is to be carried out at the CardTerminal itself (functional unit = '00'), then the basic state has to be recovered (i.e. reset of all status information, deactivation of the contacts).
Optionally the complete ATR or a part of the ATR (the historical bytes) can be requested, if for the unit addressed an ATR has been defined.

5.1.2 Usage conditions

A reset of the CardTerminal should only be initiated

- after initialization of the communication channel by CT_init (see CT-API specification) and
- after the occurence of a communication error between the application system and the CardTerminal.

A reset to the ICC can also be made by the application system, if this should be necessary on the application level.

5.1.3 Command structure

CLA	´20´
INS	´11´ (= RESET CT)
P1	Functional unit: ´00´ = CT ´01´ - ´0E´ = ICC-Interface1 - 14
P2	Command qualifier: In case P1 = ´00´: ´00´ = No response In case P1 = ´01´, ´02´: ´00´ = No response data ´01´ = Return complete ATR ´02´ = Return Historical Bytes
Lc field	Empty
Data field	Empty
Le field	Empty or ´00´ = Return full length of requested information

Tab. 4: RESET CT command

5.1.4 Response structure

Data	Empty or ATR or HB
SW1-SW2	Status bytes

Tab. 5: RESET CT response

5.1.5 Status bytes

a) Functional Unit = CT

´9000´ = Reset successful
´6400´ = Reset not successful

b) Functional Unit = ICC

´9000´ = Synchronous ICC, reset successful
´9001´ = Asynchronous ICC, reset successful
´6400´ = Reset not successful

5.2 REQUEST ICC

5.2.1 Function

An ICC is requested with the REQUEST ICC command, whereby optionally the time allowed for the insertion of the card can be specified. After insertion of the IC card a reset of the card is automatically carried out. CardTerminals with display may display a request message for the user.

5.2.2 Usage conditions

No restrictions.

5.2.3 Command structure

CLA	´20´
INS	´12´ (= REQUEST ICC)
P1	Functional unit: ´01´ - ´0E´ = ICC-Interface1 - 14
P2	Command qualifier: Request handling instructions for

	the CT, see table 7
Lc field	Empty or length of subsequent data field
Data field	Empty (= immediate response required) or max. waiting time in seconds (1 byte, binary coding) for presenting the ICC or ASN.1 data objects, see table 8
Le field	Empty or ´00´ = Return full length of requested information

Tab. 6: REQUEST ICC command

Bits	Request handling instructions. Meaning of the bits of P2:
b8-b5	CT without display: ´0´= No meaning CT with display: ´0´ = standard message (text no. 1, tab. 28) or message in data field to be displayed ´F´ = no message to be displayed Other values RFU
b4-b1	´0´ = No response data ´1´ = Return complete ATR ´2´ = Return Historical Bytes

Tab. 7: Request handling instructions

Tag	Length	Value
´50´	´XX´	Application label for information used at the man-machine-inter-face: Message to be displayed
´80´	´XX´	Max. waiting time in seconds, binary coding

Tab. 8: Possible data objects in the data field of the REQUEST ICC command

The execution of the command begins on CardTerminals with display by showing of a request message, if the appropriate option has been set (standard display message: 'Please insert card' - see section 7).
The insertion of the card is then expected within the specified time. The command can also be used in polling mode. If a time limit is not specified or timer = '00', then an immediate response is desired (when the REQUEST ICC command is repeated the display message may not be sent again as it remains displayed until an explicit change is made).

After insertion, the IC card is activated and the reset executed.

If the IC card is

- defective,
- wrongly inserted or
- not able to communicate with the CardTerminal because of for example incompatibilities in the ATR or transmission protocols

the standard display message 'Card illegible. Wrong position?' should appear in the display if a display is available.
If the CardTerminal has display and keypad and the cancellation key is pressed, SW1-SW2 = '6401' has to be returned as return code, and the standard display message 'Abort' shall be shown.

5.2.4 Response structure

Data	Empty or ATR or HB
SW1-SW2	Status bytes

Tab. 9: REQUEST ICC response

The structure and coding of an ICC-ATR is specified in ISO/IEC 7816-3 and with respect to the historical bytes also in 7816-4 for ICCs with asynchronous transmission. The structure and coding for ICCs with synchronous transmission is specified in 'ICCs with sychronous transmission, part1: ATR and data sections'.

5.2.5 Status bytes

´9000´ = Synchronous ICC presented, reset successful
´9001´ = Asynchronous ICC presented, reset successful
´6200´ = Warning: no card presented within specified time
´6201´ = Warning: ICC already present and activated
´6400´ = Reset not successful
´6401´ = Process aborted by pressing of cancel key
´6900´ = Command with timer not supported

5.3 GET STATUS

5.3.1 Function

The GET STATUS command allows the retrieval of status information which is returned as BER-TLV encoded data objects (DO).

5.3.2 Usage conditions

No restrictions.

5.3.3 Command structure

CLA	´20´
INS	´13´ (= GET STATUS)
P1	Functional unit: ´00´ = CT
P2	Command qualifier: Tag of data element to be returned (see 5.3.4)
Lc field	Empty
Data field	Empty
Le field	´00´ = Return full length of requested information

Tab. 10: GET STATUS command

5.3.4 Response structure

Data	Status information (only value field of DO)
SW1-SW2	Status bytes

Tab. 11: GET STATUS response

Structure and content of the status information is dependent on the functional unit for which status information is requested.

a) CardTerminal Manufacturer data object

The CardTerminal Manufacturer data object contains

- CardTerminal manufacturer

- CardTerminal type

- CardTerminal software version

- Discretionary data.

Fig. 2: CT Manufacturer data object

The data elements are to be encoded in ASCII and, where necessary, to be padded with leading blanks. The information CTT and CTSV are manufacturer specific. The encoding for CTM is shall be determined in cooperation with a national registration authority (e.g. the national standardisation body or its agent) and registered there.
It consists of

- 2 byte country code in alpha coding acc. to ISO 3166 (e.g. DE for Germany, FR for France)

- 3 byte manufacturer acronym.

The discretionary data can be used for supplementary information.

b) ICC status data object

The ICC status DO contains per ICC interface a status byte with the following structure:

b8 - b1 = 0 : no ICC inserted
b1 =1 : ICC inserted
b3-b2 = 00 : no information
01 : ICC electrically not connected
10: ICC electrically connected
11: RFU
b4 - b8 = RFU

Fig. 3: ICC status data object

5.3.5 Status bytes

´9000´ = Command successful

5.4 EJECT ICC

5.4.1 Function

The EJECT ICC command effects the deactivation of the electric interface and the execution of optional additional functions:

- Setting of an acoustic signal
- Setting of an optical signal
- Ejection of the ICC
- Setting of a timer

5.4.2 Usage conditions

The command should usually only be given at the end of the communication with the ICC. If an irreparable error occurs in the communication with the ICC, then the communication with the ICC may be aborted with this command.

5.4.3 Command structure

CLA	´20´
INS	´15´ (= EJECT ICC)
P1	Functional unit: ´01´ - ´0E´ = ICC-Interface1 - 14
P2	Command qualifier: Eject handling instructions for the CT, see table 13
Lc field	Empty or length of subsequent data
Data field	Empty or time in seconds for removing the ICC
Le field	Empty

Tab. 12: EJECT ICC command

Bits	Eject handling instructions. Meaning of the bits of P2:
b8-b5	CT without display: ´0´= No meaning CT with display: ´0´ = standard message (text no. 2, tab. 28) or message in data field to be displayed ´F´ = no message to be displayed Other values RFU
b4-b1	Option setting (a bit set to 0 means no, 1 means yes)
b4	0 (RFU)
b3	Delivery (0 = throwout, 1 = keep)
b2	Optical signal
b1	Acoustic signal

Tab. 13: Eject handling instructions for the CardTerminal

5.4.4 Response structure

Data	Empty
SW1-SW2	Status bytes

Tab. 14: EJECT ICC response

5.4.5 Status bytes

´9000´ = Command successful
´9001´ = Command successful, card removed
´6200´ = Warning: card not removed within specified time

6. Additional CT commands for CTs with display and keypad

6.1 INPUT

6.1.1 Function

The INPUT command allows an input entered at the keypad to be returned in the data field of the response. To request the input a display message shall be shown.

6.1.2 Usage conditions

The INPUT command is only applicable if display and keypad are available.

6.1.3 Command Structure

CLA	´20´
INS	´16´ (= INPUT)
P1	Functional unit: ´50´ = Key pad
P2	Command qualifier: ´00´ = No meaning ´01´ = Indication of input as characters ´02´ = Indication of input as asteriks
Lc field	Empty or length of subsequent data
Data field	Empty or ASN.1 data objects, see table 16
Le field	´00´ (= return full length of input) or number of expected bytes

Tab. 15: INPUT command

Tag	Length	Value
´50´	´XX´	Application label for information used at the man-machine-inter-face: Message to be displayed
´80´	´XX´	Max. waiting time in seconds (binary coding) for presenting the first input

Tab. 16: Possible data objects in the data field of the INPUT command

The addition of further data objects (e.g. a reference DO to a text stored in a CT File) is subject of further extensions of this specification.

Execution of the command

If the DO with tag '50' is missing in the data field, the standard display message 'Please enter data' (see section 7) is to be used. If '00' is given as length in the Le field it denotes a variable long input which shall be confirmed with the validation key. When Le = n, the input is assumed to be completed after entry of the n-th digit (use of the validation key is permissible but not required). The input process shall be timed (default period to first input max. 15 sec, period between 2 inputs max. 5 sec).

1. Errorfree operation

When the input is carried out properly the digits entered will be returned as characters in the data field of the response with status bytes '9000'. Before sending, the input buffer shall be erased.

2. Actions when the time limit is exceeded

If more than n seconds (default value 15) pass before input of the first digit or more than 5 seconds elapse between entering 2 digits, the procedure must be aborted because of exceeding the time limit (return code '6400'). The display shows the standard message 'Abort' (see section 7).
If it concerns an input with confirmation and the user has forgotten to press the validation key, the standard display message 'Please confirm input' is shown. Should no confirmation be entered within 5 sec, the procedure will be aborted as described above.

3. Actions when the enter process is aborted

The entering of digits can also be stopped by the user by pressing the cancel key. In this case the standard display message 'Abort' (see section 7) is shown and the status bytes '6401' returned.

6.1.4 Response structure

Data	Input (character coded)
SW1-SW2	Status bytes

Tab. 17: INPUT response

6.1.5 Status bytes

´9000´ = Command successful
´6400´ = No or incomplete input in time
´6401´ = Process aborted by operating the cancel key

6.2 OUTPUT

6.2.1 Function

With the OUTPUT command data can be displayed on a functional unit (display). The display message remains displayed until a new message is set.

6.2.2 Usage conditions

The OUTPUT command is only applicable if a display is available.

6.2.3 Command structure

CLA	´20´
INS	´17´ (= OUTPUT)
P1	Functional unit: ´40´ = Display
P2	Command qualifier: RFU (default value ´00´)
Lc field	Length of subsequent data field
Data field	ASN.1 data objects, see table 19
Le field	Empty

Tab. 18: OUTPUT command

Tag	Length	Value
´50´	´XX´	Application label for information used at the man-machine interface: Message to be displayed

Tab. 19: Possible DOs in the data fields of the OUTPUT command

6.2.4 Response structure

Data	Empty

SW1-SW2	Status bytes

Tab. 20: OUTPUT response

6.2.5 Status bytes

´9000´ = Command successful
´6700´ = Message too long

6.3 PERFORM VERIFICATION

6.3.1 Function

This command effects the PIN request at a CardTerminal with display and PIN keypad and the appropriate interaction with the ICC.

6.3.2 Usage conditions

The PERFORM VERIFICATION command is only applicable when display and PIN keypad are available.

6.3.3 Command Structure

CLA	´20´
INS	´18´ (= PERFORM VERIFICATION)
P1	Functional unit: ´01´ - ´0E´ = ICC-Interface1 - 14
P2	Command qualifier: RFU (default value ´00´)
Lc field	Length of subsequent data field
Data field	ASN.1 data objects, see table 22
Le field	Empty

Tab. 21: PERFORM VERIFICATION command

The following DOs may appear in the data field (see ISO/IEC 7816-6):

- Inter-industry data object ´Command-to-perform´ (it contains the command to be transmitted to the ICC and control information for the PIN handling)

- Inter-industry data object ´Application label´ (it contains a display message to control the man-machine interface)

Further DOs can be added if required, e.g. DO for message Id, DOs for managing the transmission of the PIN in enciphered form.

Tab. 22 shows the data objects defined until now.

Tag	Length	Value
´52´	´XX´	Command-to-perform: Control byte (see table 23), insertion position byte, command to be sent to the ICC (e.g. VERIFY, DISABLE, ENABLE)
´50´	´XX´	Application label for information used at the man-machine-inter-face: Message to be displayed
´80´	´XX´	Waiting time in seconds, binary coding

Tab. 22: Possible data objects in the data field of the PERFORM VERIFICATION command

Bits	Control byte with PIN handling instructions for the CT
b8-b5	Length of PIN to be presented. If length = 0 (value for variable length), then pressing of validation key is required.
b4-b2	000 = RFU
b1	PIN coding 0 = BCD 1 = characters according to T.50 with b8=0 (i.e. digit 0 is coded ´30´, digit 1 is coded ´31´ etc.)

Tab. 23: PIN handling instructions for the Card-Terminal

The ICC command in the ´Command-to-perform´ may appear in one of the two following forms:

- Command header (4 bytes), if only the PIN without padding is entered in the data field of the ICC command

- Command header with length field Lc and the data field pre-formatted with padding bytes

The coding of the value field of the command-to-perform can be clarified with two examples:

1. VERIFY-command according to ISO/IEC 7816-4 with PIN 4712 and PIN in BCD coding.

Value field of DO ´52´: ´400600200000´

Insertion position for the PIN is ´06´, i.e. sixth byte after the beginning of the VERIFY command. The coding of the VERIFY command is as follows:
'00200000024712'
The length byte Lc (in the example Lc has the value '02') is to be inserted at position '05' by the CardTerminal.

2. VERIFY CHV-command according to CEN 726-3 with PIN 4712 and PIN coding as character.

Value field of DO ´52´:
´4106A020000108FFFFFFFFFFFFFFFF´
Insertion position ´06´, i.e. sixth byte after the beginning of the VERIFY CHV command. The coding of the VERIFY CHV command is as follows:
'A02000010834373132FFFFFFFF'

Execution of the command for processor IC cards:

The execution of the PERFORM VERIFICATION command normally begins with the display of the standard display message 'Please enter PIN' (see section 7). If no standard display message is utilised for user guidance, the display message shall be given with DO '50' (see Tab. 22) in the data field. The DO '52' (command-to-perform) should always be the last DO in the data field. The different cases are described below:

1. Errorfree operation

The requested PIN (usually min. 4, max. 8 digits) is shown on the display with an asterisk per entered digit. The length of the PIN can be seen from the control byte (see Tab. 23). The PIN is then entered into the data field of the ICC command that is located in the data field of the PERFORM VERIFICATION (command-to-perform, see Tab.22; if only the command header is specified, the Lc field must be inserted before the PIN). Subsequently the ICC command is transmitted to the ICC. The status bytes returned in the response of the ICC command (if the PIN input is correct SW1-SW2 = '9000') are passed on as status bytes of the PERFORM VERIFICATION command to the application system, and the standard display message 'Action successful' (see section 7) is shown on the display. Before sending the response to the application system the PIN input buffer shall be erased.

2. Handling with erroneous PIN input

The actions are the same as with an errorfree PIN input, however, SW1-SW2 ≠ '9000' comes as return code from the ICC. In this case the standard display message 'PIN wrong or blocked' (see section 7) shall be shown, the input buffer erased and the status bytes returned to the application system.

3. Handling of cancellation of the PIN input by the user

If the user presses the cancel key before completing the PIN input, no command shall be sent to the ICC, and the display shall show the standard display message 'Abort' (see section 7). The input buffer shall be erased and SW1-SW2 = '6401' returned as status bytes.

4. Handling when time limit for PIN input is exceeded

If the input of the first digit is not made within 15 sec (default value) after insertion request, or if more than 5 sec elapse before input of each next digit, no command shall be sent to the ICC, the input buffer shall be erased, and the standard display message 'Abort' shall be shown. As status bytes, SW1-SW2 = '6400' shall be returned to the application system.
If the user has forgotten to press the validation key after entering the PIN, the CardTerminal shall remind the user to confirm the entered PIN with the standard display message 'Please confirm PIN' (see section 7).

Execution of the command for memory cards:

The execution of the command complies with that of the ISO/IEC 7816-4 VERIFY command for memory cards and is described in ´ICCs with synchronous transmission, Part 3: Usage of inter-industry commands´. BCD coding should be used for the PIN as normally only 3 bytes reference data are available on the card, but most applications work with 4 number PINs. Beside of this the same conditions for executing the PERFORM VERIFICATION commands shall apply as for processor IC cards.

6.3.4 Response structure

Data	Empty
SW1-SW2	Status bytes

Tab.24: PERFORM VERIFICATION response

6.3.5 Status bytes

´9000´ = Verification successful
´6400´ = No or incomplete input in time
´6401´ = Process aborted by operating the cancel key

Error codings of the ICC command: see ICC command specification

6.4 MODIFY VERIFICATION DATA

6.4.1 Function

This command effects the request for the old PIN (or PUK or Super PIN) and the new PIN at a display CardTerminal with PIN keypad and the appropriate interaction with the ICC.

6.4.2 Usage conditions

The MODIFY VERIFICATION DATA command is only applicable, if display and PIN keypad are available.

6.4.3 Command structure

CLA	´20´
INS	´19´ (= MODIFY VERIFIC. DATA)
P1	Functional unit: ´01´ - ´0E´ = ICC-Interface1 - 14
P2	Command qualifier: RFU (default value ´00´)
Lc field	Length of subsequent data field
Data field	ASN.1 data objects, see table 26
Le field	Empty

Tab. 25: MODIFY VERIFICATION DATA command

Tag	Length	Value
´52´	´XX´	Command-to-perform: Control byte (see table 23), insertion position byte for first PIN, insertion position byte for new PIN, command to be sent to the ICC
		(e.g. CHANGE, UNBLOCK)
´50´	´XX´	Application label for information used at the man-machine-inter-face: Message to be displayed
´80´	´XX´	Waiting time in seconds, binary coding

Table 26: Possible data objects in the data field of the MODIFY VERIFICATION DATA command

The coding of the value field of the Command to perform can be seen from the example CHANGE CHV command acc. to CEN 726-3 with PIN length 4 and BCD coding (old PIN 4712 and new PIN 2315):

Value field von DO ´52´:
´40060EA024000110FFFFFFFFFFFFFFFFFF
FFFFFFFFFFFF´
Insertion position for first PIN: ´06´, i.e. sixth byte after beginning of the CHANGE CHV command, insertion position for new PIN: byte '0E', i.e. fourteenth byte after beginning of the CHANGE CHV command. The coding is as follows:
´A0240001104712FFFFFFFFFFF2315FFFFF
FFFFFF´

Execution of the command for processor ICCs

The execution of the MODIFY VERIFICATION DATA command normally begins with the display of the standard display message 'Please enter PIN' (see section 7). If no standard display messages are utilised for user guidance, the display message with the DO '50' (see tab. 25) shall be given in the data field. The DO '52 (command-to-perform) should always be the last DO in the data field. The different cases are described below:

1. Errorfree operation

After the request for the old PIN or PUK the standard display message ´Please enter new PIN´ (see section 7) is shown. After the new PIN has been entered the standard display message 'Repeat input' (see section 7) shall be shown. After the repeat entry of the PIN and checking that the numbers are identical the 2 PINs are placed in the appropriate insertion positions in the data field of the ICC command which is sent to the ICC. The status bytes returned in the ICC

command response SW1-SW2 = '9000' are transferred as status bytes of the MODIFY VERIFICATION DATA command to the application system and the standard display message ´Action successful´ is shown. The PIN input buffer shall be erased before sending the response to the application system.

2. Handling with erroneous input of the old PIN or PUK

The sequence is the same as with an errorfree PIN input, however, SW1-SW2 ≠ '9000' was sent as return code from the ICC. In this case the standard display message 'PIN wrong/blocked' (see section 7) shall be shown, the input buffer erased and the status bytes given by the ICC returned to the application system.

3. Handling with erroneous input of the new PIN

If the second input of the new PIN is not identical with the first, the standard display message 'PIN not identical. Abort' is shown on the display, the input buffer shall be erased and SW1-SW2 = '6402' returned to the application system as status bytes.

4. Handling on exceeding the time limit or on cancellation

The same procedure as with the PERFORM VERIFICATION DATA command applies.

Execution of the command for memory cards:

The execution of the command complies with that of the ISO/IEC 7816-7 CHANGE VD command (at present being drafted, compatible with ETSI command CHANGE CHV) and is described in ´ICCs with synchronous transmission, Part 3: Usage of inter-industry commands´. BCD coding should be used for the PIN as normally only 3 bytes reference data are available on the card, but most applications work with 4 number PINs.

Note:
If the keypad has a correction key and this is operated by the user, the complete input shall be cancelled.

6.4.4 Response structure

Data	Empty
SW1-SW2	Status bytes

Tab. 27: MODIFY VERIFICATION DATA response

6.4.5 Status bytes

´9000´ = Change of verification data successful
´6400´ = No or incomplete input in time
´6401´ = Process aborted by pressing of cancel key
´6402´ = Process unsuccessful, new PINs not identical

Error codings of the ICC command: see ICC command specification

7. Display messages

The display shall consist of at least two lines with 16 characters each.
The character set for the display shall include

- the alphabet (upper and lower case),
- the numerals and
- the usual special characters, especially the asterisk.

Only CR (carriage return) is allowed as control character in the display message. Display messages requiring user keypad input shall have a blinking cursor character to indicate the position of the cursor.

The following standard display messages have been established:

Nr.	Text
1	Please insert card
2	Please remove card
3	Card illegible. Wrong position?
4	Please enter PIN
5	Action successful
6	PIN wrong or

	blocked
7	Please enter new PIN
8	Repeat input
9	PIN not iden- tical. Abort
10	Please confirm input
11	Please enter data
12	Abort

Tab. 28: Standard display messages

Annex (informative)

Download mechanism

For downloading (in local or remote mode) it is recommended to work with a download program which uses the CT-API - functions (see CT-API specification) and which reads the data to be loaded from a file. The download procedure may work only through software from the Card-Terminal manufacturer and shall be protected. For this the use of the ISO/IEC 7816-4 command VERIFY is recommended. The verification data from the command shall be compared by the download module in the CardTerminal with the reference data stored there. When the verification is positve, downloading is started. The format of the data and its protection, e.g. by checksums is up to the manufacturer.