

Teil 4

CT-BCS

Anwendungsunabhngiger CardTerminal Basic Command Set fr Chipkartenanwendungen

Version 0.9

28.07.95

TeleTrust Deutschland e.V.

Project Editor:

GMD - Forschungszentrum Informationstechnik GmbH

Die Weitergabe des Dokuments an Dritte ist ausdrcklich erlaubt.
nderungen und Ergnzungen sind TeleTrust Deutschland vorbehalten.
Gewhrleistung und Haftung sind ausgeschlossen.

Inhalt

1. Zweck	3
2. Referenzen	3
3. Abkürzungen	3
4. CT-Kommando-Konventionen	3
4.1 CT-Kommando-Struktur	3
4.2 CT-Kommando-Übersicht und allgemeine Return-Codes	4
4.3 Functional Units	4
5. Allgemeine CT-Kommandos	5
5.1 RESET CT	5
5.2 REQUEST ICC	5
5.3 GET STATUS	6
5.4 EJECT ICC	7
6. Zusätzliche CT-Kommandos für CTs mit Display und Tastatur	8
6.1 INPUT	8
6.2 OUTPUT	9
6.3 PERFORM VERIFICATION	10
6.4 MODIFY VERIFICATION DATA	12
7. Display-Anzeigetexte	13
Anhang (informativ)	
Download-Mechanismus	14

Adressen:

TeleTrusT Deutschland e.V.
Eichendorffstr.16
99096 Erfurt

GMD - Forschungszentrum Informationstechnik
L. Eckstein, B. Struif
Rheinstr. 75
64295 Darmstadt

RID German National Registration Authority
c/o GMD
Bruno Struif
Rheinstr.75
64295 Darmstadt
Tel. 06151-869-206
Fax 06151-869-224

1. Zweck

Diese Spezifikation beschreibt den CardTerminal Basic Command Set (CT-BCS) zur Steuerung von Kartenterminals unterschiedlichster Ausprägung:

- integrierte Kartenterminals mit einer oder mehreren Chipkarten-Schnittstellen (z.B. in die Tastatur integrierter Kartenleser, Kartenleser im Diskettenschacht, PCMCIA-Kartenleser)
- externe Kartenterminals mit einer oder mehreren Chipkarten-Schnittstellen und optionalen Funktionseinheiten wie z.B. Display und Eingabetastatur.

Die CT-Kommandos sind anwendungsneutral und können von beliebigen Chipkarten-orientierten Anwendungssystemen benutzt werden. Sie sind nach dem Konstruktionsprinzip der ISO/IEC 7816-4 Inter-industry commands aufgebaut und werden an der CT-API-Schnittstelle (CardTerminal Application Programming Interface) unter Verwendung der CT_data-Funktion (siehe CT-API-Spezifikation) zur Steuerung von Kartenterminals benutzt.

In der hier definierten CT-BCS-Version ist kein CT-orientiertes File-Konzept und auch nicht die Integration von Sicherheitsmodulen im Kartenterminal vorgesehen.

2. Referenzen

Deutsche Telekom, GMD, RWT+V, TeleTrust Deutschland: 1995

CT-API 1.1 - Anwendungsunabhängiges CardTerminal Application Programming Interface für Chipkartenanwendungen

DIN NI-17: 1995

Chipkarten mit synchroner Übertragung:
Teil 1: ATR und Datenbereiche

DIN NI-17.4: 1995

Chipkarten mit synchroner Übertragung:
Teil 2: Übertragungsprotokolle

DIN NI-17.4: 1995

Chipkarten mit synchroner Übertragung:
Teil 3: Anwendung von 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

(Verwendung findet der WD vom Oktober 1994, in dem AM 1 und AM 2 integriert sind)

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 (DIS)

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)

DIN 66003: 1974

Deutsche Referenzversion mit Umlauten

3. Abkürzungen

ASN.1 = Abstract Syntax Notation One

ATR = Answer-to-Reset

BCD = Binary Coded Digits

BER = Basic Encoding Rules

CHV = Card Holder Verification

CT = CardTerminal

CT-API=CT Application 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-Kommando-Konventionen

4.1 CT-Kommando-Struktur

Für die CT-Kommandos gilt derselbe Aufbau wie für die inter-industry commands nach ISO/IEC 7816-4.

Abb. 1: CT-Kommando-Struktur (identisch mit Kommando-Struktur in ISO/IEC 7816-4)

Als CLA-Codierung wird für CT-BCS-Kommandos aus Kompatibilitätsgründen zu den bereits eingeführten CT-Kommandos «20» verwendet.

Als Destination Address (DAD) wird an der CT-API-Schnittstelle für alle CT-BCS-Kommandos der Adresswert «01» (siehe CT-API-Spezifikation) verwendet.

4.2 CT-Kommando-übersicht und allgemeine Return-Codes

Folgende allgemeinen CT-Kommandos sind von allen Kartenterminals zu unterstützen:

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: Allgemeine CT-Kommandos

Von Kartenterminals mit Display und Tastatur sind die Kommandos in Tabelle 2 ebenfalls zu unterstützen.

CardTerminal Command (mandatory for all CTs with display and keyboard)	INS-Code
INPUT	«16»
OUTPUT	«17»
PERFORM VERIFICATION	«18»
MODIFY VERIFICATION DATA	«19»
Proprietary	«50»-«99»
All other values	F
	RFU

Tab. 2: Zusätzliche CT-Kommandos für Kartenterminals mit Display und Tastatur

Bei den Kommando-Beschreibungen sind nur die speziellen Return-Codes angegeben. Darüber hinaus können noch folgende allgemeine Return-Codes auftreten:

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

Hinweis:

Kann ein ICC-Kommando nicht zur Chipkarte übertragen werden, weil diese entnommen wurde, defekt ist oder sich in einem Zustand befindet, in dem sie nicht mehr reagiert, dann ist als Return-Code «6F00» zurückzugeben und als Sender der Antwort (SAD-Adresse) das Kartenterminal zu benennen.

4.3 Functional Units

In einem CT-Kommando können Funktionseinheiten («Functional Units») eines Kartenterminals adressiert werden. In Tabelle 3 sind diese Einheiten und die Kennungen, wie sie im CT-Kommando-Parameter P1 vorkommen können, aufgelistet.

Functional Unit	Coding	Support
CT-Kernel	«00»	mandatory
CT/ICC-Interface1	«01»	mandatory
CT/ICC-Interface2	«02»	conditional
...
CT/ICC-Interface14	«0E»	conditional
CT-Display	«40»	conditional
CT-Keyboard	«50»	conditional

Tab. 3: CT-Funktionseinheiten und ihre Codierung

5. Allgemeine CT-Kommandos

5.1 RESET CT

5.1.1 Funktion

Das RESET CT-Kommando veranlaßt das Kartenterminal, ein Reset bei der angegebenen Einheit (CT oder CT-Funktionseinheiten) durchzuführen. Soll ein Software-Reset bei dem Kartenterminal selbst vorgenommen werden (Functional Unit = «00»), dann ist der Grundzustand herzustellen (Rücksetzen aller Zustandsinformationen, Deaktivierung der Kontakte).

Optional kann der gesamte ATR oder ein Teil des ATR (die Historical Bytes) angefordert werden, falls für die betreffende Einheit ein ATR definiert wurde.

5.1.2 Anwendungsbedingungen

Ein Reset des Kartenterminals sollte nur

- nach der Initialisierung des Kommunikationskanals durch CT_init (siehe CT-API-Spezifikation) und
- nach Auftreten einer Kommunikationsstörung zwischen Anwendungssystem und Kartenterminal

gegeben werden.

Ein Reset zur Chipkarte kann vom Anwendungssystem veranlaßt werden, wenn dies auf Anwendungsebene erforderlich ist (z.B. bei einer Kommunikationsstörung).

5.1.3 Kommando-Struktur

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 Antwort-Struktur

Data SW1-SW2	Empty or ATR or HB Status bytes
--------------	------------------------------------

Tab. 5: RESET CT-Response

5.1.5 Status-Kodierungen

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 Funktion

Mit dem REQUEST ICC-Kommando wird eine Chipkarte angefordert, wobei optional die Zeit für die Einführung der Chipkarte überwacht wird. Nach Einführung der Chipkarte wird automatisch ein Reset bei der Chipkarte durchgeführt. Bei Kartenterminals mit Display kann eine Chipkarten-Eingabeanforderung angezeigt werden.

5.2.2 Anwendungsbedingungen

Keine Restriktionen.

5.2.3 Kommando-Struktur

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-Instruktionen

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: Mögliche Datenobjekte im Datenfeld des REQUEST ICC-Kommandos

Bei Kartenterminals mit Display beginnt die Ausführung des Kommandos mit der Ausgabe eines Anzeigetextes, falls die entsprechende Option gesetzt ist (Standard-Anzeigetext: «Bitte Karte einführen«, s. Kap. 7).

Danach wird auf die Einföhrung der Chipkarte entsprechend der Timer-Angabe gewartet. Das Kommando kann auch im Polling-Betrieb genutzt werden (Timer-Angabe fehlt oder Timer = «00«), d.h. es wird eine unmittelbare Rückantwort gewünscht (bei wiederholtem Aufruf des REQUEST ICC-Kommandos muß der Anzeigetext nicht erneut ausgegeben werden, da ein Text am Display bis zur expliziten Änderung erhalten bleibt).

Nach Einföhrung der Chipkarte wird diese aktiviert und der Reset ausgeföhrt.

Falls die Chipkarte

- defekt,
- falsch eingeföhrt oder
- nicht kommunikationsfähig mit dem Kartenterminal z.B. wegen Unverträglichkeiten im ATR oder bei den Übertragungsprotokollen ist,

dann soll der Standard-Anzeigetext «Karte unlesbar. Falsche Lage?» (s. Kap. 7) am Display ausgegeben werden, falls ein Display vorhanden ist.

Besitzt das Kartenterminal Display und Tastatur und wurde die Abbruch-Taste gedröckt, dann ist als Returncode SW1-SW2 = «6401« zurückzugeben und der Standard-Anzeigetext «Abbruch« (s. Kap. 7) auszugeben.

5.2.4 Antwort-Struktur

Data SW1-SW2	Empty or ATR or HB Status bytes
-----------------	------------------------------------

Tab. 9: REQUEST ICC-Response

Der Aufbau eines ICC-ATR ergibt sich aus ISO/IEC 7816-3 und 7816-4 für ICCs mit asynchroner Übertragung. Für ICCs mit synchroner Übertragung gelten die Festlegungen im DIN NI-17-Papier «Chipkarten mit synchroner Übertragung, Teil 1: ATR und Datenbereiche«.

5.2.5 Status-Kodierungen

- «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 Funktion

Das GET STATUS-Kommando erlaubt die Abfrage von Zustands-Informationen, die als BER-TLV-codierte Datenobjekte (DO) zurückgeliefert werden.

5.3.2 Anwendungsbedingungen

Keine Restriktionen.

5.3.3 Kommando-Struktur

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 Antwort-Struktur

Data	Status information (only value)
------	---------------------------------

SW1-SW2	field of DO) Status bytes
---------	------------------------------

Tab. 11: GET STATUS-Response

Aufbau und Inhalt der Status-Information ist von der Funktionseinheit abhängig, über die Status-Information abgefragt werden soll.

a) CardTerminal Manufacturer Data Object

Das CardTerminal Manufacturer Data Object beinhaltet

- CardTerminal Manufacturer
- CardTerminal Type
- CardTerminal Software Version
- Discretionary Data.

Abb. 2: CT Manufacturer Data Object

Die einzelnen Felder sind in ASCII und ggf. mit führenden Blanks angegeben. CTT und CTSV sind hexadezimal. Die Codierung für CTM stimmt mit der RID German Registration Authority festgelegt überein. Sie besteht aus

- 2 byte country code in alpha-2, entsprechend ISO 3166 (DE für Deutschland, FR für Frankreich)
- 3 byte Herstelleracronym.

Die Discretionary Data können für weitere Informationen genutzt werden.

b) ICC Status Data Object

Das ICC-Status-DO beinhaltet an der Schnittstelle ein Statusbyte mit dem folgenden Aufbau:

- 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

Abb. 3: ICC Status Data Object

5.3.5 Status-Kodierungen

«9000» = Command successful

5.4 EJECT ICC

5.4.1 Funktion

Das EJECT ICC-Kommando bewirkt die Deaktivierung des elektrischen Interfaces und veranlaßt die Ausführung optionaler Zusatzfunktionen:

- Setzen eines akustischen Signals
- Setzen eines optischen Signals
- Auswurf der Chipkarte
- Setzen eines Timers

5.4.2 Anwendungsbedingungen

Das Kommando sollte in der Regel nur am Ende der Kommunikation mit der Chipkarte gegeben werden. Tritt ein nicht behebbare Fehler in der Kommunikation mit der Chipkarte auf, kann mit dem Kommando auch die Kommunikation mit derselben abgebrochen werden.

5.4.3 Kommando-Struktur

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 Instruktionen fŸr das Kartenterminal

5.4.4 Antwort-Struktur

Data SW1-SW2	Empty Status bytes
--------------	--------------------

Tab. 14: EJECT ICC-Response

5.4.5 Status-Kodierungen

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

6. ZusŠtzliche CT-Kommandos fŸr CTs mit Display und Tastatur

6.1 INPUT

6.1.1 Funktion

Das INPUT-Kommando dient dazu, eine Eingabe Ÿber das Keyboard im Datenfeld der Response zurŸckzuliefern. Zur Eingabeanforderung kann ein Anzeigetext am Display ausgegeben werden.

6.1.2 Anwendungsbedingungen

Das INPUT-Kommando ist nur zulŠssig, wenn Display und Tastatur vorhanden sind.

6.1.3 Kommando-Struktur

CLA	«20«
INS	«16« (= INPUT)
P1	Functional unit: «50« = Keyboard
P2	Command qualifier: «00« = No meaning «01« = Indication of input as characters «02« = Indication of input as asterics
Lc field	Empty or length of subsequent data
Data field	Empty or

Le field	ASN.1 data objects, see table 16 «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: Mšgliche Datenobjekte im Datenfeld des INPUT-Kommandos

Die HinzufŸgung weiterer Datenobjekte (z.B. ein Verweis-DO auf einen in einem CT-File abgelegten Text) ist fŸr eine spŠtere Ausbaustufe vorgesehen.

AusfŸhrung des Kommandos:

Fehlt das DO mit Tag «50« im Datenfeld, ist der Standard-Anzeigetext «Bitte Dateneingabe (s. Kap. 7) zu verwenden. Wird im Le-Feld als LŠnge «00« angegeben, dann handelt es sich um eine variabel lange Eingabe, die mit der BestŠtigungstaste abzuschlieŸen ist. Ist Le = n, dann gilt die Eingabe nach der n-ten Ziffer als abgeschlossen (das DrŸcken der BestŠtigungstaste ist dann zwar erlaubt, aber nicht nŠtig). Der Ablauf ist zeitmŠssig zu Ÿberwachen (Default-Dauer bis zur Ersteingabe max. 15 sec, Dauer zwischen zwei Eingaben max. 5 sec).

1. Fehlerfreier Ablauf

Wird die Eingabe ordnungsgemŠŸ abgewickelt, dann werden die eingegebenen Ziffern als Zeichen im Datenfeld der Antwort mit Return-Code «9000« zurŸckgeliefert. Vor Absenden ist der Eingabepuffer zu lšschen.

2. Ablauf bei ZeitŸberschreitung

Vergehen bis zur Eingabe der ersten Ziffer mehr als n Sekunden (Default-Wert 15) oder zwischen zwei Ziffern mehr als 5 Sekunden, dann ist der Vorgang wegen ZeitŸberschreitung abzubrechen (Returncode «6400«). Am Display wird dies mit Standard-Anzeigetext «Abbruch« (s. Kap.7) angezeigt.

Handelte es sich um eine Eingabe mit Bestätigung und hat der Benutzer das Drücken der Bestätigungstaste vergessen, dann ist er mit dem Standard-Anzeigetext «Bitte Eingabe bestätigen» (s. Kap. 7) hierzu aufzufordern. Erfolgt keine Bestätigung innerhalb von 5 sec, dann wird der Vorgang wie oben dargestellt abgebrochen.

3. Ablauf bei Abbruch

Der Vorgang kann auch vom Benutzer durch Drücken der Abbruchtaste abgebrochen werden. In diesem Fall wird der Standard-Anzeigetext «Abbruch» (s. Kap. 7) am Display ausgegeben und als Return-Code «6401» zurückgeliefert.

6.1.4 Antwort-Struktur

Data SW1-SW2	Input (character coded) Status bytes
-----------------	---

Tab. 17: INPUT-Response

6.1.5 Status-Kodierungen

«9000» = Command successful
 «6400» = No or incomplete input in time
 «6401» = Process aborted by pressing of cancel key

6.2 OUTPUT

6.2.1 Funktion

Mit dem OUTPUT-Kommando können Daten an einer «Functional Unit» (Display) ausgegeben werden. Die Anzeige bleibt erhalten, bis ein neuer Text gesetzt wird.

6.2.2 Anwendungsbedingungen

Das OUTPUT-Kommando ist nur zulässig, wenn ein Display vorhanden ist.

6.2.3 Kommando-Struktur

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 Le field	ASN.1 data objects, see table 19 Empty
------------------------	---

Tab. 18: OUTPUT-Command

Tag	Length	Value
«50»	«XX»	Application label for information used at the man-machine inter-face: Message to be displayed

Tab. 19: Mögliche Datenobjekte im Datenfeld des OUTPUT-Kommandos

6.2.4 Antwort-Struktur

Data SW1-SW2	Empty Status bytes
-----------------	-----------------------

Tab. 20: OUTPUT-Response

6.2.5 Status-Kodierungen

«9000» = Command successful
 «6700» = Message too long

6.3 PERFORM VERIFICATION

6.3.1 Funktion

Dieses Kommando bewirkt die PIN-Abfrage an einem Kartenterminal mit Display und PIN-Tastatur und die entsprechende Interaktion mit der Chipkarte.

6.3.2 Anwendungsbedingungen

Das PERFORM VERIFICATION-Kommando ist nur zulässig, wenn Display und PIN-Tastatur vorhanden sind.

6.3.3 Kommando-Struktur

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

Im Datenfeld können folgende Datenobjekte vorkommen (siehe hierzu auch ISO/IEC 7816-6):

- Inter-industry data object «Command-to-perform»
(es enthält das zur Chipkarte zu übertragende Kommando sowie Steuerungsinformationen für das PIN-Handling)
- Inter-industry data object «Application label» (es enthält einen Display-Anzeigetext zur Steuerung der Mensch-Maschine-Schnittstelle)

Weitere DOs können nach Bedarf hinzugefügt werden, z.B. DO für Message-Id, DO für Key-Id, falls PIN chiffriert übertragen werden soll. Tab. 22 zeigt die bisher definierten Datenobjekte mit ihren Datenobjekt-Kennzeichen («Tag«).

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: Mögliche Datenobjekte im Datenfeld des PERFORM VERIFICATION-Kommandos

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-Instruktionen für das Kartenterminal

Das ICC-Kommando im «Command-to-perform» kann je nach Anwendung in einem der beiden nachfolgenden Formen auftreten:

- Command Header (4 Bytes), falls im Datenfeld des ICC-Kommandos nur der PIN ohne Padding eingetragen wird
- Command Header mit Längenfeld Lc und mit Paddingbytes vorformatiertem Datenfeld

Die Codierung des Value-Feldes des Command-to-perform soll an zwei Beispielen verdeutlicht werden:

1. VERIFY-command nach ISO/IEC 7816-4 mit 4-stelliger PIN 4712 und PIN-Codierung in BCD-Form.

Value field von DO «52»: «400600200000»
Insertion position für die PIN ist «06», also sechstes Byte nach Beginn des VERIFY-Kommandos. Es hat folgende Codierung: «00200000024712»
Auf Position «05» ist das Längenbyte Lc, im Beispiel mit dem Wert «02», durch das Kartenterminal einzutragen.

2. VERIFY CHV-command nach CEN 726-3 mit 4-stelliger PIN 4712 und PIN-Codierung als Zeichen.

Value field von DO «52»: «4106A020000108FFFFFFFFFFFFFFFF»
Insertion position «06», also sechstes Byte nach Beginn des VERIFY CHV-Kommandos. Es hat folgende Codierung: «A02000010834373132FFFFFFFF»

Ausführung des Kommandos für Prozessor-Chipkarten:

Die Ausführung des PERFORM VERIFICATION-Kommandos im Kartenterminal beginnt normalerweise mit der Ausgabe des Standard-Anzeigetextes «Bitte Geheimzahl eingeben» (s. Kap. 7). Falls kein Standard-Anzeigetext

zur Bedienerführung verwendet wird, ist der Anzeigetext mit Datenobjekt «50» (s. Tab. 22) im Datenfeld anzugeben. Das Datenobjekt «52» (Command-to-perform) sollte immer als letztes DO im Datenfeld stehen. Im folgenden werden die verschiedenen Ablaufvarianten beschrieben:

1. Fehlerfreier Ablauf

Die abgefragte PIN (üblicherweise min. 4, max. 8 Ziffern) wird am Display mit einem Sternchen pro eingegebener Ziffer angezeigt. Die Länge der PIN ist dem Control byte (siehe Tab. 23) zu entnehmen. Die PIN wird dann in das Datenfeld des ICC-Kommandos eingetragen, das sich im Datenfeld des PERFORM VERIFICATION-Kommandos befindet (Command-to-perform, siehe Tab. 22; falls dort nur der Command Header angegeben, ist vor der PIN das Lc-Feld einzutragen). Anschließend wird das ICC-Kommando zur Chipkarte übertragen. Die in der Antwort des ICC-Kommandos zurückgelieferten Status-Bytes (bei korrekter PIN-Eingabe ist SW1-SW2 = «9000») werden als Status-Bytes des PERFORM VERIFICATION-Kommandos an das Anwendungssystem weitergereicht und am Display der Standard-Anzeigetext «Aktion erfolgreich» (s. Kap. 7) ausgegeben. Vor Senden der Rückantwort an das Anwendungssystem ist der PIN-Eingabepuffer zu löschen.

2. Ablauf bei inkorrektter PIN-Eingabe

Der Ablauf ist derselbe wie bei der korrekten PIN-Eingabe, doch kommt als Returncode von der Chipkarte SW1-SW2 «9000». In diesem Fall ist der Standard-Anzeigetext «Geheimzahl falsch /gesperrt» (s. Kap. 7) auszugeben, der Eingabepuffer zu löschen und der Returncode an das Anwendungssystem zurückzuliefern.

3. Ablauf bei Abbruch der PIN-Eingabe durch den Benutzer

Drückt der Benutzer vor Abschluß der PIN-Eingabe die Abbruch-Taste, dann wird kein Kommando zur Chipkarte geschickt, am Display der Standard-Anzeigetext «Abbruch» (s. Kap. 7) ausgegeben, der Eingabepuffer gelöscht und als Returncode SW1-SW2 = «6401» zurückgegeben.

4. Ablauf bei Zeitüberschreitung bei der PIN-Eingabe

Erfolgt nach Eingabeaufforderung nicht innerhalb von 15 sec (Default-Wert) die Eingabe der ersten Ziffer oder verstreicht mehr Zeit als 5 sec bis zur Eingabe der jeweils nächsten Ziffer, dann wird kein Kommando zur Chipkarte geschickt, der Eingabepuffer gelöscht, am Display der Standard-Anzeigetext «Abbruch» (s. Kap. 7) ausgegeben und als Returncode SW1-SW2 = «6400» zurückgegeben. Hat der Benutzer bei variabler PIN-Eingabe nur das Drücken der Bestätigungstaste (validation key) vergessen, dann soll das Kartenterminal mit Standard-Anzeigetext «Bitte Eingabe bestätigen» (s. Kap. 7) den Benutzer um Bestätigung der eingegebenen Geheimzahl auffordern.

Ausführung des Kommandos für Speicherchipkarten:

Die Ausführung des Kommandos entspricht der Umsetzung des ISO/IEC 7816-4-VERIFY-Kommandos für Speicherchipkarten und ist in dem Papier «Inter-industry Commands für Speicherchipkarten» beschrieben. Als PIN-Codierung sollte die BCD-Codierung verwendet werden, da nur 3 Bytes an Reference Data in der Karte zur Verfügung stehen, die meisten Anwendungen jedoch mit 4-stelligen PINs arbeiten. Ansonsten gelten dieselben Ausführungsbedingungen des PERFORM VERIFICATION-Kommandos wie für Prozessor-Chipkarten.

6.3.4 Antwort-Struktur

Data	Empty
SW1-SW2	Status bytes

Tab.24: PERFORM VERIFICATION-Response

6.3.5 Status-Kodierungen

- «9000» = Verification successful
- «6400» = No or incomplete input in time
- «6401» = Process aborted by pressing of cancel key

Fehler-Codierungen des ICC-Kommandos: siehe ICC-Kommando-Spezifikation.

6.4 MODIFY VERIFICATION DATA

6.4.1 Funktion

Dieses Kommando bewirkt die Abfrage der alten PIN (bzw. der PUK oder der Super-PIN) und der neuen PIN an einem Kartenterminal mit Display und PIN-Tastatur und die entsprechende Interaktion mit der Chipkarte.

6.4.2 Anwendungsbedingungen

Das MODIFY VERIFICATION DATA-Kommando ist nur zulässig, wenn Display und PIN-Tastatur vorhanden sind.

6.4.3 Kommando-Struktur

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

Tab. 26: Mögliche Datenobjekte im Datenfeld des MODIFY VERIFICATION DATA-Kommandos

Die Codierung des Value-Feldes des Command-to-perform soll am Beispiel des CHANGE CHV-Kommandos nach CEN 726-3 mit 4-stelliger PIN (alte PIN 4712, neue PIN 2315) und BCD-Codierung verdeutlicht werden:

Value field von DO «52«:

```
«40060EA024000110FFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFF«
```

Insertion position für erste PIN: «06«, also sechstes Byte nach Beginn des CHANGE CHV-Kommandos, Insertion position für neue PIN: Byte «0E«, also vierzehntes Byte nach Beginn des CHANGE VD-Kommandos. Es hat folgende Codierung:

```
«A0240001104712FFFFFFFFFFFFFFFF2315FFFF
FFFFFFFFFFFF«
```

Ausführung des Kommandos für Prozessor-Chipkarten:

Die Ausführung des MODIFY VERIFICATION DATA-Kommandos im Kartenterminal beginnt normalerweise mit der Ausgabe des Standard-Anzeigetextes «Bitte Geheimzahl eingeben» (s. Kap. 7). Falls kein Standard-Anzeigetext zur Bedienerführung verwendet wird, ist der Anzeigetext mit Datenobjekt «50» (s. Tab. 25) im Datenfeld anzugeben. Das Datenobjekt «52» (Command-to-perform) sollte immer als letztes DO im Datenfeld stehen. Im folgenden werden die verschiedenen Ablaufvarianten beschrieben:

1. Fehlerfreier Ablauf

Nach Abfrage der alten PIN bzw. der PUK ist der Standard-Anzeigetext «Neue Geheimzahl eingeben» (s. Kap. 7) auszugeben. Nach Eingabe der neuen PIN ist der Standard-Anzeigetext «Eingabe wiederholen» (s. Kap. 7) anzuzeigen. Nach Wiederholung der PIN-Eingabe und Überprüfung auf Gleichheit sind dann im Datenfeld des zur Chipkarte zu sendenden ICC-Kommandos die beiden PINs an den entsprechenden Insertion Positionen einzutragen. Die in der Antwort des ICC-Kommandos zurückgelieferten Status-Bytes SW1-SW2 = «9000» werden als Status-Bytes des MODIFY VERIFICATION DATA-Kommandos an das Anwendungssystem weitergereicht und der Standard-Anzeigetext «Aktion erfolgreich» am Display ausgegeben. Vor Senden der Rückantwort an das Anwendungssystem ist der PIN-Eingabepuffer zu löschen.

2. Ablauf bei fehlerhafter Eingabe der alten PIN bzw. PUK

Der Ablauf entspricht dem fehlerfreien Ablauf, doch kommt von der Chipkarte ein Returncode SW1-SW2 «9000» zurück. In diesem Fall ist der Standard-Anzeigetext «Geheimzahl falsch / gesperrt» (s. Kap. 7) auszugeben, der

Eingabepuffer zu löschen und die betreffenden Status-Bytes an das Anwendungssystem zurückzuliefern.

3. Ablauf bei fehlerhafter Eingabe der neuen PIN

Ist die Eingabe bei der Wiederholung der neuen PIN nicht mit der vorherigen Eingabe identisch, dann wird der Standard-Anzeigetext «Geheimzahl nicht gleich. Abbruch» am Display ausgegeben, der Eingabepuffer gelöscht und als Status-Bytes SW1-SW2 = «6402» an das Anwendungssystem zurückgeliefert.

4. Ablauf bei Zeitüberschreitung oder Abbruch

Hier gelten dieselben Regeln wie für das PERFORM VERIFICATION-Kommando.

Ausführung des Kommandos für Speicherchipkarten:

Die Ausführung des Kommandos entspricht der Umsetzung des ISO/IEC 7816-7-CHANGE VD-Kommandos (in Ausarbeitung, kompatibel zu ETSI command CHANGE CHV) und ist in dem Papier «Inter-industry Commands für Speicherchipkarten» beschrieben. Als PIN-Codierung sollte in diesem Fall die BCD-Codierung verwendet werden, da nur 3 Bytes an Reference Data in der Karte zur Verfügung stehen, die meisten Anwendungen jedoch mit 4-stelligen PINs arbeiten.

Hinweis:

Ist eine Korrekturtaste vorhanden und wird sie vom Benutzer gedrückt, dann ist die gesamte Eingabe zu löschen.

6.4.4 Antwort-Struktur

Data SW1-SW2	Empty Status bytes
-----------------	-----------------------

Tab. 27: MODIFY VERIFICATION DATA-Response

6.4.5 Status-Kodierungen

«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

Fehler-Codierungen des ICC-Kommandos:
 siehe ICC-Kommando-Spezifikation

7. Display-Anzeigetexte

Für Anzeigetexte wird von einer Display-Größe von mindestens 2x16 Zeichen ausgegangen. Als Zeichensatz sind das Alphabet (mit Umlaute) in Groß- und Kleinschreibung sowie die Ziffern und die üblichen Sonderzeichen insbesondere inklusive Stern zu unterstützen. Als Steuerzeichen ist in einem Anzeigetext nur CR zulässig. Bei Anzeigetexten mit nachfolgender Tastatur-Eingabe soll ein blinkendes Cursor-Zeichen die Position des Cursors anzeigen.

Folgende Standardtexte werden festgelegt:

Nr.	Text
1	Bitte Karte einführen
2	Bitte Karte entnehmen
3	Karte unlesbar. Falsche Lage?
4	Bitte Geheimzahl eingeben
5	Aktion erfolgreich
6	Geheimzahl falsch / gesperrt
7	Neue Geheimzahl eingeben
8	Eingabe wiederholen
9	Geheimzahl nicht gleich. Abbruch
10	Bitte Eingabe bestätigen
11	Bitte Dateneingabe
12	Abbruch

Tab. 28: Standard-Anzeigetexte

Anhang (informativ)

Download-Mechanismus

Zur Abwicklung eines Ladevorgangs wird empfohlen, ein Ladeprogramm zu entwickeln, das auf der CT-API-Schnittstelle aufsetzt und die Ladedaten aus einer Datei liest. Der Ladevorgang darf nur durch Software des Kartenterminal-Herstellers erfolgen und muß abgesichert werden. Hierzu wird die Verwendung des ISO/IEC 7816-4-Kommandos VERIFY empfohlen. Die im Kommando mitgelieferten Verification Data sind vom Download-Modul im Kartenterminal mit den dort abgelegten Reference Data zu vergleichen. Bei Übereinstimmung wird in den Ladezustand umgeschaltet. Die Formatierung der Ladedaten und deren Sicherung z.B. durch Prüfsummen ist vom Hersteller festzulegen.