

Teil 4

CT-BCS

**Anwendungsunabhängiger
CardTerminal Basic Command Set**

MKT-Version 1.0

15.04.1999

Inhalt

1	Zweck.....	1
2	Referenzen.....	1
3	Abkürzungen	1
4	CT-Kommando-Konventionen	2
4.1	CT-Kommando-Struktur.....	2
4.2	CT-Kommando-Übersicht und allgemeine Return-Codes	2
4.3	Functional Units.....	3
4.4	Kodierung von Display-Texten.....	3
5	Allgemeine CT-Kommandos.....	3
5.1	RESET CT.....	3
5.2	REQUEST ICC.....	4
5.3	GET STATUS.....	7
5.4	EJECT ICC.....	8
6	CT-Kommandos für MKTs mit speziellen Funktionseinheiten.....	10
6.1	INPUT	10
6.2	OUTPUT	12
6.3	PERFORM VERIFICATION.....	12
6.4	MODIFY VERIFICATION DATA	16
7	Display-Anzeigetexte.....	19
	Anhang A (normativ): Kodierung von Biometrical Units	14
	Anhang B (normativ): Format 2 PIN Block.....	15
	Anhang C (informativ): B1-Kommandos	16
	Anhang D (informativ): Download-Mechanismus	17

1 Zweck

Dieser Teil der 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 Interindustry commands aufgebaut und werden an der CT-API-Schnittstelle (CardTerminal Application Programming Interface) unter Verwendung der CT_data-Funktion (siehe MKT-Teil 3: CT-API) zur Steuerung von Kartenterminals benutzt.

Zur Erreichung der Kompatibilität mit B1-Lesern wird zusätzlich die Unterstützung einer Teilmenge der B1-Leser-Kommandos (siehe Anhang C) empfohlen.

2 Referenzen

MKT-Teil 3: CT-API 1.1 – Anwendungsunabhängiges CardTerminal Application Programming Interface

MKT-Teil 5: Chipkarten mit synchroner Übertragung – ATR und Datenbereiche

MKT-Teil 7: Chipkarten mit synchroner Übertragung - Anwendung von Interindustry Commands

ISO 3166: 1993 (4th edition)
Codes for the representation of names of countries

ISO/IEC 7816-3: 1997 (2nd edition)
Identification cards - Integrated circuit(s) cards with contacts
Part 3 - Electronic signals and transmission protocols

ISO/IEC 7816-4: 1995

Identification cards - Integrated circuit(s) cards with contacts
Part 4 - Interindustry commands for inter-change

ISO/IEC 7816-6: 1995

Identification cards - Integrated circuit(s) cards with contacts
Part 6 - Interindustry data elements

ISO/IEC 7816-8: 1998 (FDIS)

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

ISO/IEC 7816-10: 1998 (FDIS)

Identification cards - Integrated circuit(s) cards with contacts
Part 6 – Electronic signals and answer-to-reset for synchronous cards

ISO 10202-6:

Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards
Part 6: Cardholder verification

CEN 1257-3: 1995

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

Deutsche Telekom / PZ Telesec
B0 / B1 HTSI - Programmer's Manual
Release 2.1, 03.03.1996

3 Abkürzungen

ASN.1 = Abstract Syntax Notation One
ATR = Answer-to-Reset
BCD = Binary Coded Digit (4 bits)
BER = Basic Encoding Rules
BU = Biometrical Unit
CHV = Card Holder Verification
CR = Carriage Return
CT = CardTerminal

CT-API = CT Application Programming Interf.

CT-BCS=CT Basic Command Set

DAD = Destination Address

DO = Data Object

FU = Functional Unit

HB = Historical Bytes

HBCI = Homebanking Computer Interface

ICC = Integrated Circuit(s) Card

PIN = Personal Identification Number

PUK = Personal Unblocking Key

RD = Reference Data

RID = Registered application provider ID

SAD = Source Address

TLV = Tag, Length, Value

VD = Verification Data

VR = Verification Requirement

|| = Concatenation

Als Destination Address (DAD) wird an der CT-API-Schnittstelle für alle CT-BCS-Kommandos der Adresswert '01' (siehe MKT-Teil 3: CT-API) verwendet.

4.2 CT-Kommando-Übersicht und allgemeine Return-Codes

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

4 CT-Kommando-Konventionen

4.1 CT-Kommando-Struktur

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

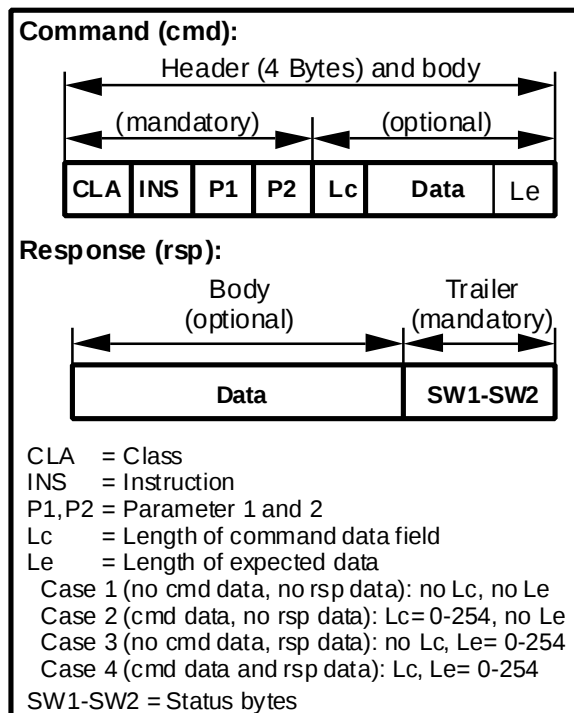


Abb. 1: CT-Kommando-Struktur (identisch mit Kommando-Struktur in ISO/IEC 7816-4)

Als CLA-Kodierung wird für CT-BCS-Kommandos aus Kompatibilitätsgründen zu den bereits eingeführten CT-Kommandos '20' verwendet.

CardTerminal Command (mandatory for all CTs)	INS-Code
Reserved for B1command	'10'
RESET CT	'11'
REQUEST ICC	'12'
GET STATUS	'13'
Reserved for B1 command	'14'
EJECT ICC	'15'

Tab. 1: Allgemeine CT-Kommandos

Von Kartenterminals mit Functional Units wie z.B. Display, Tastatur und biometrischer Sensor sind die Kommandos in Tabelle 2 ebenfalls zu unterstützen, soweit sie relevant für die betreffenden FUs sind.

CardTerminal Command (to be supported by CTs with related functional units such as display and keyboard)	INS-Code
INPUT	'16'
OUTPUT	'17'
PERFORM VERIFICATION	'18'
MODIFY VERIFICATION DATA	'19'
Proprietary	'50'-'9F'
All other values	RFU

Tab. 2: Zusätzliche CT-Kommandos für Kartenterminals mit speziellen Functional Units

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

'64A1' = No card present
 '64A2' = Card not activated
 '6700' = Wrong length
 '6900' = Command not allowed
 '6A00' = Wrong parameters P1, P2
 '6C00' = Wrong length Le
 '6D00' = Wrong instruction
 '6E00' = Class not supported
 '6F00' = Communication with ICC not possible

Der Return-Code '6F00' ist zurückzugeben, wenn ein ICC-Kommando nicht zur Chipkarte übertragen werden kann, weil diese defekt ist oder sich in einem Zustand befindet, in dem sie nicht mehr reagiert. Als Sender der Antwort (SAD-Adresse) ist 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. Zu den Functional Units gehören auch biometrische Identifikationseinheiten (Biometrical Units BU).

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
Printer	'60'	conditional
Biometrical Unit, see annex A	'7x'	conditional

Tab. 3: CT-Funktionseinheiten und ihre Kodierung

4.4 Kodierung von Display-Texten

Display-Texte (siehe z.B. DO '50' in Tab. 8) sind in ASCII zu codieren (nationale Referenz-Version). Der Zeichensatz, der unterstützt werden muß, sofern das MKT über ein Display verfügt, umfaßt mindestens

- die Buchstaben (Groß/Kleinschreibung)
- die Ziffern
- die Sonderzeichen . , | : | ? | - | + | =
- das Leerzeichen.

Bei internationalem Einsatz eines MKT ist der jeweils gebräuchliche Zeichensatz zu verwenden.

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 MKT-Teil 3: CT-API) 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' = CT/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

Bei einer Chipkarte kann je nach MKT-Ausprägung entweder sofort nach Einführung oder erst bei Eintreffen des REQUEST ICC-Kommandos ein Reset ausgeführt werden. An der CT-API wird jedoch die Chipkarte in jedem Fall erst nach erfolgreichem REQUEST ICC-Kommando „sichtbar“. Wird eine Karte herausgezogen und durch eine andere ersetzt, dann wird diese an der CT-API ebenfalls erst nach REQUEST ICC wahrgenommen, d.h. das MKT darf nur Kommandos an Karten senden, zu denen ein ordnungsgemäßer REQUEST ICC ausgeführt wurde.

5.2.3 Kommando-Struktur

CLA	'20'
INS	'12' (= REQUEST ICC)
P1	Functional unit: '01' - '0E' = CT/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', siehe Kap. 7).

Danach wird auf die Einführung 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 Einführung der Chipkarte wird diese aktiviert und der Reset ausgeführt. Falls die Chipkarte

- defekt,
 - falsch eingeführt oder
 - nicht kommunikationsfähig mit dem Kartenterminal z.B. wegen Unverträglichkeiten im ATR oder beim Übertragungsprotokoll ist,
- dann soll der Standard-Anzeigetext 'Karte unlesbar. Falsche Lage?' (siehe Kap. 7) am Display (falls vorhanden) ausgegeben werden. Besitzt das Kartenterminal Display und Tastatur und wurde die Abbruch-Taste gedrückt, dann ist als Returncode SW1-SW2 = '6401' zurückzugeben und der Standard-Anzeigetext 'Abbruch' (siehe Kap. 7) auszugeben.

Hinweis: Ist schon eine Karte eingeführt und aktiviert, dann bleibt die Karte in ihrem Zustand.

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 MKT-Teil 5: 'Chipkarten mit synchroner Übertragung - 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-kodierte 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 '01'-'0E' = CT/ICC-Interface 1-14
P2	Command qualifier: If P1 = '00': '46' = Card Manufacturer DO '80' = ICC Status DO (all ICC interfaces) '81' = Functional Unit DO If P1 ≠ '00': '80' = ICC Status DO (status of ICC interface as specified in P1)
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
SW1-SW2	Status bytes

Tab. 11: GET STATUS-Response

Hinweis: Wie in 5.3.1 beschrieben, soll das angeforderte DO inclusive Tag und Länge zurückgeliefert werden. Um die Abwärtskompatibilität zu Version 0.9 sicherzustellen, ist jedoch auch die Rückgabe des Value-Teils ohne Tag und Länge zulässig.

a) CardTerminal Manufacturer Data Object

Das CardTerminal Manufacturer Data Object beinhaltet

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

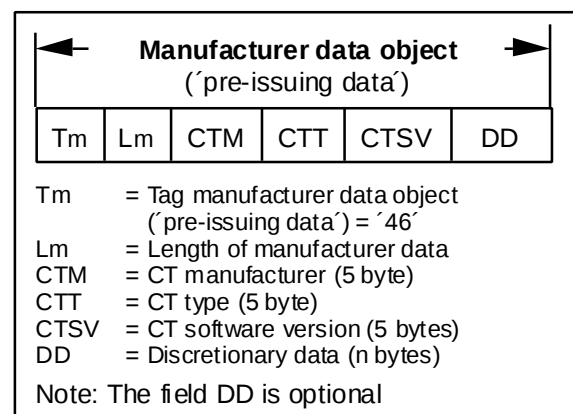


Abb. 2: CT Manufacturer Data Object

Die einzelnen Felder sind in ASCII zu codieren und ggf. mit führenden Blanks aufzufüllen. Die Angaben CTT und CTSV sind herstellerspezifisch. Die Kodierung für CTM wird in Abstimmung mit der RID German National Registration Authority festgelegt und dort registriert. Sie besteht aus

- 2 byte country code in alpha-Kodierung entsprechend ISO 3166 (z.B. DE für Deutschland, FR für Frankreich)
- 3 byte Hersteller-Acronym.

Die Discretionary Data können für ergänzende Informationen genutzt werden.

b) ICC Status Data Object

Das ICC-Status-DO beinhaltet pro ICC-Schnittstelle ein Statusbyte mit folgendem 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

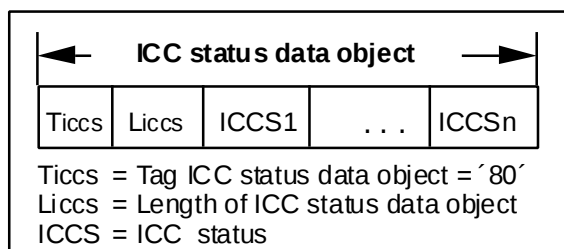


Abb. 3: ICC Status Data Object

c) Functional Unit Data Object

Das FU Data Object beinhaltet Informationen, welche FUs im MKT vorhanden sind.

TFU = '81'

FU = Kodierung entsprechend Tab. 3

FU Data Object						
TFU	LFU	'01'	'02'	'40'	'50'	'70'
'81'	'05'	ICC1	ICC2	Display	Key-board	Finger print

Abb. 4: FU Data Object (Beispiel)

In der Liste fehlt '00' (=CT), weil diese FU immer vorhanden ist.

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 behebbarer 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’ = CT/ ICC-Interface1-
P2	14 Command qualifier:
Lc field	Eject handling instructions for the CT, see table 13
Data field	Empty or length of subsequent data field Empty (= immediate response required) or max. waiting time in seconds (1 byte, binary coding) for removing the ICC or
Le field	ASN.1 data objects, see table 8 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 für das
Kartenterminal**5.4.4 Antwort-Struktur**

Data	Empty
SW1-SW2	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 CT-Kommandos für MKTs mit speziellen Funktionseinheiten

6.1 INPUT

6.1.1 Funktion

Das INPUT-Kommando dient dazu, eine Eingabe des Benutzers über eine Eingabeeinheit (Keyboard oder biometrische Einheit) im Datenfeld der Response zurückzuliefern. Zur Eingabeanforderung kann ein Anzeigetext am Display ausgegeben und ein Timer gesetzt werden.

6.1.2 Anwendungsbedingungen

Das INPUT-Kommando ist nur zulässig, wenn das MKT mit entsprechenden Functional Units ausgestattet ist. Das Abrufen biometrischer Meßdaten soll nur dann zulässig sein, wenn der Feature-Extraction-Algorithmus nicht im MKT selbst abläuft, sondern von der Software-Einheit ausgeführt wird, die das INPUT-Kommando sendet.

6.1.3 Kommando-Struktur

CLA	'20'
INS	'16' (= INPUT)
P1	Functional unit: '50' = Keyboard '7x' = Biometrical Unit
P2	Command qualifier: If P1 = '50': '00' = No input indication '01' = Input indication: characters '02' = Input indication: asterics If P1 = '7x': '00' = No meaning
Lc field	Empty or length of subsequent data field
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: Mögliche Datenobjekte im Datenfeld des INPUT-Kommandos

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

Ausführung des Kommandos für FU = Keyboard:

Fehlt das DO mit Tag '50' im Datenfeld, ist der Standard-Anzeigetext 'Bitte Dateneingabe' (s. Kap. 7) zu verwenden (falls Display am MKT vorhanden). Wird im Le-Feld als Länge '00' angegeben, dann handelt es sich um eine variabel lange Eingabe, die mit der Bestätigungstaste abzuschließen ist. Ist Le = n, dann gilt die Eingabe nach der n-ten Ziffer als abgeschlossen (das Drücken der Bestätigungstaste ist dann zwar erlaubt, aber nicht nötig). Der Ablauf ist zeitmäßig zu überwachen (Default-Dauer bis zur Ersteingabe max. 15 sec, Dauer zwischen zwei Eingaben max. 5 sec).

1. Fehlerfreier Ablauf

Wird die Eingabe ordnungsgemäß abgewickelt, dann werden die eingegebenen Ziffern als Zeichen im Datenfeld der Antwort mit Return-Code '9000' zurückgeliefert. Vor Absenden ist der Eingabepuffer zu löschen.

2. Ablauf bei Zeitüberschreitung

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 Zeitüberschreitung abzubrechen (Returncode '6400'). Am Display wird dies mit Standard-Anzeigetext 'Abbruch' (siehe 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' (siehe 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' (siehe Kap. 7) am Display ausgegeben und als Return-Code '6401' zurückgeliefert.

6.1.4 Antwort-Struktur

Data	Input: - ASCII characters in case of keyboard - biometrical measure data in case of biometrical unit
SW1-SW2	Status bytes

Tab. 17: INPUT-Response

Hinweis: Um die Nutzung des INPUT-Kommandos für PIN-Abfragen auszuschließen, sollte die max. Anzahl der bei diesem Kommando eingebaren Ziffern auf 3 beschränkt werden.

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 einer 'Functional Unit' übergeben werden:

- Text für Display (die Anzeige bleibt erhalten, bis ein neuer Text gesetzt wird oder der Timer für die Ausgabe abgelaufen ist)
- Druckdaten für einen am MKT angeschlossenen Drucker
- Daten zur Konfigurierung einer biometrischen Einheit.

Der Aufbau der Druckdaten ist druckerabhängig, der Aufbau und der Inhalt für Daten zur Konfigurierung einer biometrischen Einheit ist abhängig von deren Ausprägung.

6.2.2 Anwendungsbedingungen

Das OUTPUT-Kommando ist nur zulässig, wenn die adressierte Functional Unit (Display, Drucker bzw. biometrischer Sensor) vorhanden ist.

6.2.3 Kommando-Struktur

CLA	'20'
INS	'17' (= OUTPUT)
P1	Functional unit: '40' = Display '60' = Printer '7x' = Biometrical Unit
P2	Command qualifier: RFU (default value '00')
Lc field	Length of subsequent data field
Data field	- if P1 = '40': ASN.1 data objects, see table 19 - if P1 = '60': data to be printed - if P1 = '7x': configuration data
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
'80'	'XX'	Max. display time in seconds, binary coding

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

6.2.4 Antwort-Struktur

Data	Empty
SW1-SW2	Status bytes

Tab. 20: OUTPUT-Response

6.2.5 Status-Kodierungen

'9000' = Command successful
 '6410' = FU unable to process the output data

6.3 PERFORM VERIFICATION

6.3.1 Funktion

Dieses Kommando bewirkt die Anzeige von Texten zur Bedienerführung (falls Display vorhanden), die Entgegennahme der PIN-Eingabe an einem Kartenterminal mit PIN-Tastatur, und die entsprechende Interaktion mit der Chipkarte. MKTs mit biometrischen Sensor erlauben auch die Erfassung und Aufbereitung

der biometrischer Meßdaten und die entsprechende Interaktion mit der Chipkarte.

Die Interaktion mit der Chipkarte besteht

- in dem Senden des im Datenfeld des PERFORM VERIFICATION-Kommandos übergebenen Kommandos, wobei entweder die PIN, der Resetting Code oder aufbereitete biometrische Meßdaten vom MKT an der im DO 'Command-to-perform' angegebenen Insertion Position einzusetzen sind und
- der Entgegennahme der Chipkarten-Antwort.

der Default-Wert benutzt werden soll)

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').

6.3.2 Anwendungsbedingungen

Das PERFORM VERIFICATION-Kommando ist nur zulässig, wenn PIN-Tastatur und/oder eine biometrische Identifizierungseinheit vorhanden sind.

6.3.3 Kommando-Struktur

CLA	'20'
INS	'18' (= PERFORM VERIFICATION)
P1	Functional unit: '01' - '0E' = CT/ICC-Interface1 - 14
P2	Command qualifier: '00' = User authentication via PIN-pad '01' = User authentication via biometric sensor
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 (s. hierzu auch ISO/IEC 7816-6):

- Interindustry data object 'Command-to-perform'
(es enthält das zur Chipkarte zu übertragende Kommando sowie Steuerungsinformationen für das PIN-Handling, falls PIN-Eingabe gefordert; DO mandatory)
- Interindustry data object 'Application label'
(es enthält einen Display-Anzeigetext zur Steuerung der Mensch-Maschine-Schnittstelle)
- DO zur Angabe der Wartezeit für den ersten Input
(DO nur nötig, falls ein anderer Wert als

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 - CHANGE RD (only with new RD, see ISO/IEC 7816-8, option P1 = '01') - DISABLE / ENABLE VR - RESET RETRY COUNTER (only with resetting code)
'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) for presenting the first input

Tab. 22: Mögliche Datenobjekte im Datenfeld
des PERFORM VERIFICATION-Kommandos

Bits	Control byte for user authentication
b8-b5	Length of PIN to be presented. If length = 0 (value for variable length), then pressing of validation key is required.
b4-b3	00 = RFU
b2-b1	PIN coding 00 = BCD 01 = characters according to T.50 with b8=0 (i.e. digit 0 is coded '30', digit 1 is coded '31' etc.) 10 = Format 2 PIN Block, see annex B 11 = RFU
b8-b1	'FF' in case of biometric identifica- tion

Tab. 23: Benutzer-Authentisierungs-Instruktionen
für das Kartenterminal

a) Benutzer-Authentisierung mit PIN

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

- Command Header (CLA, INS, P1 P2 = 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 Kodierung des Value-Feldes des Command-to-perform soll an zwei Beispielen verdeutlicht werden:

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

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

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

Value field von DO '52':
'4106A020000108FFFFFFFFFFFFFFFF'
Insertion position '06', also sechstes Byte nach Beginn des VERIFY CHV-Kommandos. Es hat folgende Kodierung: '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' (siehe Kap. 7). Falls kein Standard-Anzeigetext zur Bedienerführung verwendet wird, ist der Anzeigetext mit Datenobjekt '50' (siehe Tab. 22) im Datenfeld anzugeben (Wiederholung des DOs zulässig, wobei dann der Ersatz für die Texte 4, 5 und 6 in dieser Reihenfolge anzugeben ist). 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' (siehe 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' (siehe 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' (siehe 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' (siehe 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' (siehe 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-Kodierung sollte die BCD-Kodierung 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.

b) Biometrische Benutzer-Authentisierung

Im Datenfeld werden die biometrischen Verifikationsdaten (aufbereitete biometrische Meßdaten) übergeben.

6.3.4 Antwort-Struktur

Data SW1-SW2	Empty 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-Kodierungen 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. des Resetting Codes, siehe ISO/IEC 7816-8, oder des Unblocking Keys, siehe EN 726-3) und der neuen PIN an einem Kartenterminal mit Display und PIN-Tastatur und die entsprechende Interaktion mit der Chipkarte. MKTs mit biometrischem Sensor ermöglichen - falls dies für das betreffende Verfahren sinnvoll ist - auch einen Wechsel der biometrischen Daten (z.B. statt Daumen soll der Zeigefinger bei der Fingerabdruck-Verifikation verwendet werden).

6.4.2 Anwendungsbedingungen

Das MODIFY VERIFICATION DATA-Kommando ist nur zulässig, wenn Display und PIN-Tastatur und/oder eine biometrische Identifizierungseinheit vorhanden sind.

6.4.3 Kommando-Struktur

CLA	'20'
INS	'19' (= MODIFY VERIFIC. DATA)
P1	Functional unit: '01' - '0E' = CT/ICC-Interface1 - 14
P2	Command qualifier: '00' = User authentication via PIN-pad '01' = user authentication via biometric sensor
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 old reference data (or resetting code), insertion position byte for new reference data, command to be sent to the ICC (e.g. CHANGE REFERENCE DATA, RESET RETRY COUNTER)
'50'	'XX'	Application label for information used at the man-machine-interface: Message to be displayed
'80'	'XX'	Waiting time in seconds (binary coding) for presenting the first input

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

Die Bedeutung und Nutzung der DOs entspricht dem PERFORM VERIFICATION-Kommando (siehe 6.3.3).

a) Benutzer-Authentisierung mit PIN

Die Kodierung des Value-Feldes des Command-to-perform soll an 2 Beispielen verdeutlicht werden:

1. CHANGE REFERENCE DATA nach ISO/IEC 7816-8 mit alten Referenz-Daten (4-stellige PIN) und neuen Referenz-Daten (6-stellige PIN), d.h. PINs mit variabler Länge und Darstellung als ASCII-Zeichen. Der Wert der alten Referenz-Daten ist im Beispiel 4712, der Wert der neuen Referenz-Daten 231546:

Value field von DO '52': '01060000240000'
 Insertion position für die alten Referenzdaten:
 '06', also sechstes Byte nach Beginn des
 CHANGE REFERENCE DATA-Kommandos,
 Insertion position für neue Referenz-Daten:
 Byte '00', d.h. unmittelbar im Anschluß an die
 alten Referenz-Daten. Das Längenbyte Lc wird
 von dem Kartenterminal an Position 05 nach
 Kommandobeginn eingesetzt. Das an die
 Chipkarte gesandte Kommando hat folgende
 Kodierung:

'002400000A34373132323331353436'

Anm.: Bei ISO/IEC 7816-8 wird davon ausge-
 gangen, daß die Chipkarte die Länge der alten
 Referenz-Daten kennt und daher weder feste
 Felder von 8 Byte noch Delimiter benötigt.

2. CHANGE CHV-Kommandos nach CEN
 726-3 mit 4-stelliger PIN (alte PIN 4712, neue
 PIN 2315) und BCD-Kodierung:

Value field von DO '52':

'40060EA024000110FFFFFFFFFFFFFFFFFFFFF
 FFFFFFFFFFFFFFFF'

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 Kodierung:

'A0240001104712FFFFFFFFFFFFFF2315FFFF
 FFFFFFFF'

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'
 (siehe Kap. 7). Falls kein Standard-An-
 zeigetext zur Bedienerführung verwendet wird,
 ist der Anzeigetext mit Datenobjekt '50' im
 Datenfeld anzugeben (Wiederholung des DOs
 zulässig, wobei dann der Ersatz für die Texte
 4 bis 9 in dieser Reihenfolge anzugeben ist).
 Das Datenobjekt '52' (Command-to-perform)
 sollte immer als letztes DO im Datenfeld
 stehen. Im folgenden werden die verschiede-
 nen Ablaufvarianten beschrieben:

1. Fehlerfreier Ablauf

Nach Abfrage der alten PIN bzw. des Reset-
 ting Codes ist der Standard-Anzeigetext
 'Neue Geheimzahl eingeben' (siehe Kap. 7)
 auszugeben. Nach Eingabe der neuen PIN ist

der Standard-Anzeigetext 'Eingabe wieder-
 holen' (siehe Kap. 7) anzuzeigen. Nach Wie-
 derholung 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 wei-
 tergereicht und der Standard-Anzeigetext 'Ak-
 tion erfolgreich' am Display ausgegeben. Vor
 Senden der Rückantwort an das Anwendungs-
 system 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' (siehe Kap. 7) auszugeben, der Ein-
 gabepuffer zu löschen und die betreffenden
 Status-Bytes an das Anwendungssystem zu-
 rückzuliefern.

3. Ablauf bei fehlerhafter Eingabe der neuen PIN

Ist die Eingabe bei der Wiederholung der neu-
 en PIN nicht mit der vorherigen Eingabe iden-
 tisch, 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 PER-
 FORM VERIFICATION-Kommando.

Ausführung des Kommandos für Speicherchip-
 karten:

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 im
 MKT-Teil 7 beschrieben. Als PIN-Kodierung
 sollte in diesem Fall die BCD-Kodierung ver-
 wendet 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.

b) Biometrische Benutzer-Authentisierung

Im Datenfeld werden die alten und neuen biometrischen Verifikationsdaten übergeben.

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-Kodierungen 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 A (normativ)

Kodierung von Biometrical Units

Die folgende Tabelle zeigt die Kodierung von Functional Units vom Typ „biometrische Einheit“ (z.B. Sensor-Chip), die in ein MKT integriert sein können.

Functional Unit	Coding
Fingerprint Unit	'70'
Voiceprint Unit	'71'
Dynamic Signature Verification Unit	'72'
Face Recognition Unit	'73'
Iris Unit	'74'
RFU	'75' - '7F'

Tab. A.1: Biometrische Funktionseinheiten und ihre Kodierung

Anhang B (normativ)

Format 2 PIN Block

Der Format 2 PIN Block (Verwendung u.a. bei HBCI) wird gemäß Anhang A von ISO 10202-6 aus der PIN gebildet. Sie hat eine Mindestlänge von 5 Ziffern und darf maximal 12 Ziffern lang sein. Die 8 Byte sind wie folgt belegt:

C	L	P	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F
---	---	---	---	---	---	---	-----	-----	-----	-----	-----	-----	-----	---	---

Abb. B.1: Kodierung des Format 2 PIN Blocks

Jedes Feld repräsentiert ein Halbbyte:

C:	Kontrollfeld, binär kodiert	hat immer den Wert '2'
L:	PIN-Länge, binär kodiert	mögliche Werte von '5' bis 'C'
P:	PIN-Ziffer, BCD-kodiert	
F:	Filler, binär kodiert	hat immer den Wert 'F'
P/F:	PIN/Filler	abhängig von der PIN-Länge

Anhang C (informativ)

B1-Kommandos

Zur Erreichung von Kompatibilität zwischen MKTs und B1-Lesegeräten sollten die Kommandos RESET und DEACTIVATE ICC unterstützt werden.

1 RESET

1.1 Funktion

Das RESET-Kommando veranlaßt das Kartenterminal, ein Reset bei der angegebenen Einheit (Device) durchzuführen. Optional kann der gesamte ATR oder nur die Historical Bytes angefordert werden. Das RESET-Kommando ist eine Untermenge des RESET CT-Kommandos.

1.2 Kommando-Struktur

CLA	'20'
INS	'10' (= RESET)
P1	Functional unit (Device): '00' = CT '01' = ICC1 '02' = ICC2
P2	Command qualifier: '00' = No response '01' = Return complete ATR '02' = Return Historical Bytes
Lc field	Empty
Data field	Empty
Le field	'00'

Tab. C.1: RESET-Command

1.3 Antwort-Struktur

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

Tab. C.2: RESET-Response

1.4 Status-Kodierungen

a) Functional Unit (Device) = CT

'9000' = Reset successful
'6400' = Reset not successful

b) Functional Unit (Device) = ICC

'9000' = Synchronous ICC, reset successful
'9001' = Asynchronous ICC, reset successful
'6400' = Reset not successful
'64A1' = No ICC
'64A2' = ICC not activated
'64A3' = Non-supported protocol
'64A8' = Protocol error

2 DEACTIVATE ICC

2.1 Funktion

Das DEACTIVATE ICC-Kommando bewirkt die Deaktivierung des elektrischen Interfaces und wirft die Chipkarte aus, falls ein Ejector vorhanden. Das DEACTIVATE ICC-Kommando ist eine Untermenge des EJECT ICC-Kommandos.

2.2 Kommando-Struktur

CLA	'20'
INS	'14' (= DEACTIVATE ICC)
P1	Functional unit (Device): '01' = ICC1 '02' = ICC2
P2	'00'
Lc field	Empty
Data field	Empty
Le field	'00'

Tab. C.3: DEACTIVATE ICC-Command

2.3 Antwort-Struktur

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

Tab. C.4: DEACTIVATE ICC-Response

2.4 Status-Kodierungen

'9000' = Command successful
'64A1' = No ICC

3 Sonstige B1-Kommandos

Die Unterstützung weiterer B1-Kommandos
wie z.B. die File-Kommandos ist optional.

Anhang D (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.

