

Teil 2

CT-ICC-Interface

**MKT-Schnittstelle
für kontaktorientierte Chipkarten
mit synchroner und asynchroner Übertragung**

MKT-Version 1.0

15.04.1999

Inhalt

1	Zweck	1
2	Referenzen	1
3	Abkürzungen	1
4	Basiskonzept	2
5	Chipkarten-Schnittstelle für ICCs mit asynchroner Übertragung	2
5.1	Physikalische Ansteuerung	2
5.1.1	Physical Characteristics	2
5.1.2	Lage und Bedeutung der Kontakte	3
5.1.3	Frequenz	3
5.1.4	Bit-Dauer	3
5.1.5	Character Frame	4
5.1.6	Kontakt-Aktivierung und Cold Reset	4
5.2	Answer-to-Reset	4
5.2.1	ATR-Konzept	4
5.2.2	TS - Initial Character	4
5.2.3	T0 - Format Character	5
5.2.4	TA1 - Interface Character für Frequenz und Bit-Dauer	5
5.2.5	TB1 - Interface Character für 'Programming Voltage and Current'	5
5.2.6	TC1 - Interface Character für 'Extra Guard Time'	5
5.2.7	TD1 - Interface Character für 'Subsequent Characters Indication and Protocol Type'	5
5.2.8	TA2 - Interface Character für 'Specific Mode of Operation'	6
5.2.9	TC2 - Interface Character für T=0 Work Waiting Time	6
5.2.10	TD2 - Interface Character für Subsequent Protocol Parameters of T=1	6
5.2.11	TA3 - Interface Character für T=1 Information Field Size Card	6
5.2.12	TB3 - Interface Character für T=1 Character and Block Waiting Time	6
5.2.13	TC3 - Interface Character für T=1 Error Detection Code	6
5.2.14	T=15-Anzeige mit Voltage Class und Clock Stop Mode	6
5.2.15	T1 bis TK - Historical Bytes	6
5.2.16	TCK - Check Character	7
5.2.17	Empfohlene ATR-Codierung für T=0 und T=1	7
5.3	Protocol Parameter Selection PPS	8
6	Übertragungsprotokolle	8
6.1	Character Transmission Protocol T=0	8
6.1.1	Senden und Empfangen	8
6.1.2	Fehlerbehandlung	8
6.2	Block Transmission Protocol T=1	9
6.2.1	NAD - Node Address Byte	9
6.2.2	PCB - Protocol Control Byte	9
6.2.3	LEN - Length Byte	9
6.2.4	INF - Information Field	9
6.2.5	EDC - Error Detection Code	10
6.2.6	Block-Numerierung	10
6.2.7	Einstellung von IFSC	10
6.2.8	Einstellung von IFSD	10
6.2.9	Fehlerfreie Kommunikation	10
6.2.10	Fehlerbehandlungen	10
7	Chipkarten-Schnittstelle für ICCs mit synchroner Übertragung	11
7.1	Physikalische Ansteuerung	11
7.1.1	Physical Characteristics	11
7.1.2	Lage und Bedeutung der Kontakte	11
7.1.3	Frequenz	11
7.1.4	Bit-Übertragung	11
7.1.5	Reset	11
7.2	ATR	12
7.3	Übertragungsprotokolle	12

1 Zweck

Zweck dieses Teils der Spezifikation ist es, für Multifunktionale Kartenterminals (MKTs) die Schnittstelle für

- Chipkarten mit asynchroner Übertragung (Mikroprozessor-Chipkarten mit T=0- und T=1-Protokoll) und
- Chipkarten mit synchroner Übertragung (Speicher-Chipkarten mit SDA-, 2WB- und 3WB-Protokoll)

festzulegen. Die MKTs sind in ihrer derzeitigen Ausprägung auf die Kommunikation mit kontaktorientierten Chipkarten ausgerichtet, sind jedoch offen für die Unterstützung von kontaktlosen Karten (z.B. mit Close Coupling) und Kombikarten.

2 Referenzen

MKT-Teil 4: CT-BCS – Anwendungsunabhängiger CardTerminal Basic Command Set für Chipkartenanwendungen

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

MKT-Teil 6: Chipkarten mit synchroner Übertragung - Übertragungsprotokolle

ISO/IEC 7816-1: FDIS 1998 (2nd edition)
Identification cards - Integrated circuit(s) cards with contacts
Part 1 - Physical characteristics

ISO/IEC 7816-2: 1997 (2nd edition)
Identification cards - Integrated circuit(s) cards with contacts
Part 2 - Dimensions and location of contacts

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
AM1 (FDIS 1998): IC manufacturer registration

ISO/IEC 7816-10: FDIS 1998
Identification cards - Integrated circuit(s) cards with contacts
Part 10 - Electronic signals and answer to reset for synchronous cards

ISO/IEC 10373 : 1993
Identification cards - Test methods

3 Abkürzungen

API = Application Programming Interface
ATR = Answer-to-Reset
BWI = Block Waiting Time Integer
BWT = Block Waiting Time
CH = Command Header (= CLA, INS, P1, P2)
CIE = Card Interface Environment
CLA = Class Byte
CT = Card Terminal
CWI = Character Waiting Time Integer
DC = Direct Current
DO = Data Object
EDC = Error Detection Code
etu = elementary time unit
FCB = Function Code Bus
ICC = Integrated Circuit Card
H = High state
HB = Historical Bytes
HTSI = Host Terminal Software Interface
ICC = Integrated Circuit(s) Card
ICM = IC Manufacturer
IFSC = Information Field Size Card
IFSD = Information Field Size Device
IM = Interface Modul
INS = Instruction Code
ietu = initial etu
L = Low state
MKT = Multifunktionales Kartenterminal
NAD = Node Address Byte
PCB = Protocol Control Byte
PIN = Personal Identification Number
PPS = Protocol Parameter Select
P1, P2 = Parameter 1 bzw. 2
RFU = Reserved for Future Use
SDA = Serial Data Access
Vcc = Supply Voltage
Vpp = Programming Voltage
wetu = work etu
WTX = Block Waiting Time Extension
2WB = 2 Wire Bus
3WB = 3 Wire Bus

4 Basiskonzept

Ein Multifunktionales Kartenterminal soll in der Lage sein, mit kontaktorientierten Chipkarten kommunizieren zu können, die eines der vom MKT unterstützten Übertragungsprotokolle (s. Abb. 1) verwenden.

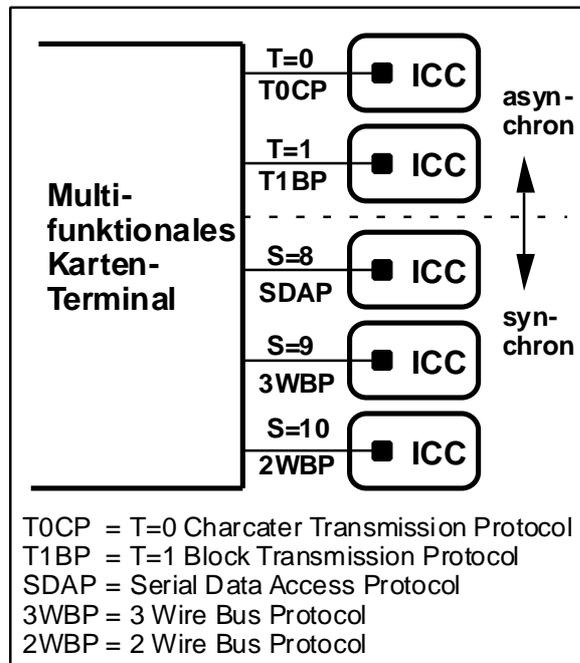


Abb. 1: Vom MKT unterstützte Übertragungsprotokolle

Grundsätzlich sind die für die Kommunikation wichtigen ISO/IEC-Standards 7816-1/-2 und -3 sowie der neue Standard ISO/IEC 7816-10 für synchrone Karten zu beachten soweit sie nicht durch Festlegungen in dieser Spezifikation eingeschränkt werden. In ISO/IEC 7816-10 ist ein weiteres Übertragungsprotokoll für synchrone Chipkarten spezifiziert (Function Code Bus Protocol FCBP), dessen Unterstützung aber für MKTs optional ist.

Die Interaktion mit der Chipkarte beginnt, nachdem das MKT das CT-Kommando REQUEST ICC (siehe CT-BCS-Spezifikation) erhalten hat und die Chipkarte eingeführt wurde. Defaultmäßig wird zunächst immer von einer asynchronen Chipkarte ausgegangen. Handelt es sich um eine solche, wird die Chipkarte auf den Reset mit einem Answer-to-Reset antworten. Die Kommunikation kann fortgesetzt werden, falls im ATR als Transmission-Protocol entweder T= 0 oder T = 1 (siehe ISO/IEC 7816-3) angezeigt wird. Ist dies nicht der Fall, wird die Kommunikation mit der Karte beendet

und die Kontakte werden deaktiviert. Das Endsystem, das das REQUEST ICC-Kommando initiiert hat, erhält einen Return Code, der es über Erfolg oder Mißerfolg der Reset-Prozedur unterrichtet.

Kommt keine Antwort auf das ggf. 2x durchgeführte Reset (siehe Abb. 1 in ISO/IEC 7816-3), wird von einer synchronen Karte ausgegangen, d.h. nach Deaktivierung wird dann eine Aktivierung nach den Konventionen für synchrone Karten durchgeführt. Nach Reset sendet die Chipkarte mit synchroner Übertragung mit den 32 ersten Taktzyklen den 4-Byte-ATR (Aufbau siehe Teil 5). Eine Kommunikation ist mit Chipkarten möglich, deren Chips entweder

- das Serial Data Access Protocol (z.B. i^2C -Bus Chips mit Reset)
- das 3 Wire Bus Protocol (z.B. SLE 4418/28) oder
- das 2 Wire Bus Protocol (z.B. PCB 2032/42 und SLE 4432/42)

unterstützen. Erfolgt keine Rückantwort auf das Reset, soll das MKT versuchsweise von einer Chipkarte mit SDA-Protocol, aber ohne Reset-Funktion ausgehen. Über Erfolg oder Mißerfolg der Reset-Prozedur wird das Endsystem wie oben dargelegt informiert.

Für die Kommunikation mit Chipkarten, die mit FCB-Protocol arbeiten und von MKTs unterstützt werden können, gelten die für die Karten in ISO/IEC 7816-10 beschriebenen Konventionen.

5 Chipkarten-Schnittstelle für ICCs mit asynchroner Übertragung

5.1 Physikalische Ansteuerung

5.1.1 Physical Characteristics

Die vom MKT zu unterstützenden ICCs mit asynchroner Übertragung sind kontaktorientierte Chipkarten mit 5V-Technologie oder 5V/3V-Technologie wie in ISO/IEC 7816-3 (2nd edition) beschrieben ($V_{cc} = 5V \pm 0.25V$ DC). Die Unterstützung von Chipkarten der Class B (3 Volt only) ist optional. Die 'Physical characteristics' sind entsprechend ISO/IEC 7816-1 auszugestalten.

Die maximale Stromaufnahme einer Chipkarte mit 5V-Technologie beträgt 60 mA. Die Stromversorgung für die Chipkarte soll jedoch in der Lage sein, in einem Übergangszustand für die Dauer von weniger als 400 ns eine Ladung von bis zu 20 nAs bei einem max. Strom von 100 mA abzugeben.

In den Kartenterminals sollten nur kontaktschonende Kontaktiereinheiten zum Einsatz kommen.

5.1.2 Lage und Bedeutung der Kontakte

Die Lage und Bedeutung der Kontakte ergibt sich aus ISO/IEC 7816-2. Die Kontakte C4 und C8 werden nicht benutzt und sollen elektrisch nicht angeschlossen sein (Ausnahme: MKTs, die das FCB-Protocol für synchrone Karten unterstützen, müssen auch den Kontakt C4 bedienen).

Auch der Kontakt C6 (Programming Voltage Vpp) soll unbenutzt bleiben, d.h. das MKT soll keine Vpp erzeugen (Ausnahme: MKTs, die zusätzlich das FCB-Protokoll beherrschen, müssen beim Lese/Schreibvorgang Vpp unterstützen).

5.1.3 Frequenz

Nach Einführung einer Chipkarte ist zunächst immer von einer Mikroprozessor-Chipkarte mit asynchroner Übertragung auszugehen. Die Anfangsfrequenz kann nach ISO/IEC 7816-3 im Bereich von 1 bis 5 MHz liegen. Es wird empfohlen, 3,5712 MHz oder 4,9152 MHz als (Anfangs-) Taktfrequenz zu benutzen. Die Unterstützung von Frequenzen oberhalb von 5 MHz ist optional, jedoch zur Steigerung der Chipkarten-Reaktionszeiten und zur schnelleren Datenübertragung wünschenswert. Zeigt eine Chipkarte im Interface Character TA1 (siehe Abschnitt 5.2.3) an, daß sie höhere Frequenzen verkraften kann, so kann das Kartenterminal, falls es dazu in der Lage ist, nach dem ATR sofort die höhere Frequenz benutzen.

MKTs, die z.B. in tragbaren Endgeräten eingebaut sind, sollten den Clock-Stop-Mode unterstützen (siehe ISO/IEC 7816-3).

5.1.4 Bit-Dauer

Die Bit-Dauer für Chipkarten mit asynchroner Übertragung wird als elementary time unit (etu) bezeichnet. Für die Ausführung des Answer-to-Reset wird die initial etu (ietu) benutzt, die wie folgt definiert ist:

$$\text{initial etu} = 372/f \text{ sec}$$

mit f = Frequenz zwischen 1 und 5 MHz. Wird die Frequenz 3,5712 MHz benutzt, ergibt sich eine Baudrate von 9,6 Kbps für die Kommunikation zwischen Chipkarte und Kartenterminal. Für die Kommunikation nach dem Answer-to-Reset wird die work etu (wetu) benutzt. Sie ist definiert durch

$$\text{work etu} = F/Df \text{ sec}$$

mit F = clock rate conversion factor und D = bit rate adjustment factor. Setzt man die Defaultwerte ein ($F = 372$, $D = 1$), dann ist die wetu = ietu.

Welchen Wert die work etu bekommt, hängt einerseits von den Fähigkeiten des Kartenterminals und andererseits von Vorhandensein und Codierung von

- Interface Character TA1 (siehe 5.2.3),
- Interface Character TA2 (siehe 5.2.7)

sowie der Unterstützung der Protocol Parameter Selection Prozedur (siehe 5.3) ab.

Tab. 1 zeigt die ISO/IEC 7816-3-konformen Varianten und welche davon zu unterstützen sind.

	TA1 abwesend	TA1 anwesend
TA2 abwesend (negotiable mode)	wetu = ietu (zu unterstützen)	wetu = ietu, wenn keine PPS-Prozedur durchgeführt wird (zu unterstützen) ----- wetu = F/Df nach erfolgreichem PPS
TA2 anwesend (specific mode)	wetu = ietu (zu unterstützen)	wetu = F/Df sofort nach ATR (Unterstützung für F = 372 und D=1; falls andere Werte angegeben, erneu- ter Reset (warm Reset); falls glei- cher ATR, Abbruch)

Tab. 1: TA1/TA2-Kombinationen

5.2.3 T0 - Format Character

Das 'most significant nibble (bits b8-b5)' von T0 zeigt an, ob die nachfolgenden Characters TA1 bis TD1 vorhanden sind (siehe Abb. 4).

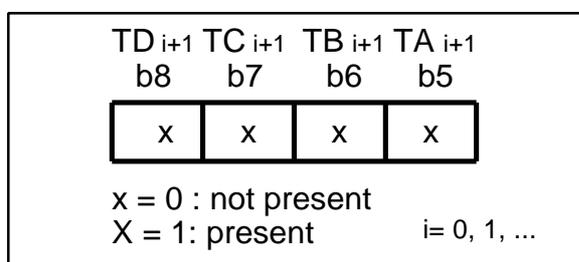


Abb. 4: Anzeige des Vorhandenseins von Interface-Characters in T0 (i=0) und TDi-Character (i=1, 2, ...)

Das 'least significant nibble (bits b4-b1)' von T0 gibt die Anzahl der Historical Characters an (0 bis 15).

5.2.4 TA1 - Interface Character für Frequenz und Bit-Dauer

Der Interface Character TA1 enthält, falls vorhanden, die Codierungen für FI und DI (Integerwerte für Frequenz F und Bit Rate Adjustment Factor D, siehe Tabellen 7 und 8 in ISO/IEC 7816-3).

Für die Übertragungsphase nach dem answer to reset gilt die Gleichung

$$\text{work etu} = F/Df \text{ sec}$$

wobei F der 'clock rate conversion factor' und D der 'bit rate adjustment factor' ist. Die Werte von D und F, codiert durch DI und FI, werden nach ISO/IEC 7816-3 im Interface Character TA1 des ATR angezeigt.

Die Defaultwerte F=372 und D=1 sind zu unterstützen. Andere Werte können angezeigt werden, sind jedoch entsprechend den Vorgaben in Tab. 1 zu behandeln.

Werden nur die Defaultwerte benutzt, soll die Übertragung des TA1 Characters entfallen.

Es wird empfohlen, daß MKTs die Fi-Werte 372 und 512 (d.h. FI = 1 und 9) und die Di-Werte 1, 2, 4, 8 und 12 (d.h. DI = 1, 2, 3, 4 und 8) unterstützen.

5.2.5 TB1 - Interface Character für 'Programming Voltage and Current'

TB1 zeigt die Werte von P (programming voltage) in den least significant 5 bits (bits b5-b1) an und den maximalen Wert des Programmierstroms I in den bits b7 und b6 an (Default-Werte nach ISO/IEC 7816-3: P=5, I=50; Bit b8 wird nicht benutzt und ist auf 0 zu setzen). Die Default-Werte haben jedoch keine Bedeutung, wenn T=15 mit Voltage class und clock stop mode im ATR übertragen wird. In diesem Fall entfällt die Übertragung von TB1, andernfalls sollte - da keine Programmierspannung von modernen Chips benötigt wird - als Wert für TB1 von den ICCs '00' zurückgeliefert werden (= I_{max} = 25 mA, V_{pp} not connected).

Sollte für TB1 ein Wert ? '00' codiert sein, wird dieser nicht weiter ausgewertet.

5.2.6 TC1 - Interface Character für 'Extra Guard Time'

TC1 überträgt die 'extra guard time' N (Einheit: etu), die der minimalen Dauer zwischen den Flanken der Start-Bits zweier aufeinanderfolgenden Characters hinzugefügt werden soll. Der Defaultwert von N ist Null und sollte von den Chipkarten unterstützt werden. TC1 sollte daher im ATR nicht übertragen werden.

5.2.7 TD1 - Interface Character für 'Subsequent Characters Indication and Protocol Type'

Das 'most significant nibble (bits b8-b5)' von TD1 zeigt an, ob die nachfolgenden Characters TA2 bis TD2 vorhanden sind (Zuordnungsschema siehe Abb. 5).

Das 'least significant nibble (bits b4-b1)' gibt den Protocol Type an, der für die Kommunikation zwischen MKT und ICC benutzt werden soll.

Für ICCs mit Übertragungsprotokoll T=0 soll TD1 nicht zurückgeliefert werden (bei Abwesenheit von TD1 ist nach ISO/IEC 7816-3 das Übertragungsprotokoll T=0 zu benutzen; da TA2 bis TD2 für T=0 nicht benutzt werden, ist die Übertragung von TD1 für T=0 redundant und daher nicht sinnvoll).

Für ICCs mit Übertragungsprotokoll T=1 muß TD1 anwesend sein, wobei b1 auf 1 gesetzt ist. Werden weitere Angaben zu T=1 benötigt (was in der Regel der Fall ist), dann ist die Anwesenheit von TD2 anzuzeigen. Eine übliche Codierung von TD1 ist für T=1 daher '81'.

5.2.8 TA2 - Interface Character für ‘Specific Mode of Operation’

Wird TA2 im ATR *nicht* übertragen, dann zeigt die Chipkarte damit an, daß sie sich im ‘negotiable mode’ befindet. Wird TA2 übertragen, dann zeigt die Chipkarte damit den ‘specific mode of operation’ an.

5.2.9 TC2 - Interface Character für T=0 Work Waiting Time

TC2 zeigt das maximale Intervall zwischen dem Beginn eines von der ICC gesandten Characters und dem vorhergehenden Character, der entweder vom Kartenterminal oder der Chipkarte gesandt wurde. Die ‘work waiting time’ ergibt sich aus $960 \times D \times WI$, wobei TC2 den Wert für WI enthält. Es wird von den Default-Werten für D und WI Gebrauch gemacht, d.h. das maximale Intervall beträgt 9600 etus. TC2 soll daher nicht im ATR übertragen werden.

5.2.10 TD2 - Interface Character für Subsequent Protocol Parameters of T=1

Das ‘most significant nibble (bits b8-b5)’ von TD2 zeigt an, ob die nachfolgenden Characters TA3 bis TD3 vorhanden sind (Zuordnungsschema siehe Abb. 5).

Da TA3 und TB3 in der Regel übertragen werden, ist der übliche Wert dieses Nibbles 3.

Das ‘least significant nibble (bits b4-b1)’ enthält wieder die Angabe des Protokoll-Typs. Da empfohlen wird, entsprechend ISO/IEC 7816-3: 1997 auch T=15 mit voltage class und clock stop mode anzuzeigen, hat TD2 den Wert ‘B1’.

5.2.11 TA3 - Interface Character für T=1 Information Field Size Card

TA3 gibt die maximale Länge des Informationsfeldes eines T=1-Blockes an, der von der Chipkarte empfangen werden kann (IFSC, siehe ISO/IEC 7816-3, 9.5.1.1) und sollte immer von der Chipkarte zurückgeliefert werden, da kaum eine Chipkarte nur ein IFSC von 32 Byte hat, was der (veraltete) Default-Wert ist). Der Wert von TA3 muß im Bereich 32 bis 254 liegen (‘20’ - ‘FE’).

5.2.12 TB3 - Interface Character für T=1 Character and Block Waiting Time

Die ‘character waiting time CWT’ gibt die maximale Zeit zwischen den Flanken der Start-Bits zweier aufeinanderfolgender Character an (siehe ISO/IEC 7816-3, 9.5.2.1). Das ‘least significant nibble (bits b4-b1)’ von TB3 zeigt den Wert CWI an, der in die Berechnung von CWT eingeht. CWI kann nach ISO/IEC 7816-3 die Werte 0 bis 15 haben.

Die ‘block waiting time BWT’ gibt die maximale Zeit zwischen den Flanken der Start-Bits des letzten Characters eines empfangenen Blocks und des ersten Characters eines zu sendenden Blocks an (siehe ISO/IEC 7816-3, 9.5.2.2). Das ‘most significant nibble (bits b8-b5)’ von TB3 zeigt den Wert BWI an, der in die Berechnung von BWT eingeht. BWI kann nach ISO/IEC 7816-3 die Werte 0 bis 9 haben. Der Defaultwert ist ‘4D’. Um eine möglichst schnelle Übertragung zu haben, sollten die Werte für TB3 unter dem Defaultwert liegen.

5.2.13 TC3 - Interface Character für T=1 Error Detection Code

TC3 dient der Kennzeichnung der Form des Error Detection Codes im Epilog-Feld eines T=1-Blockes. Ist Bit B1 auf 1 gesetzt, kennzeichnet dies die Benutzung von CRC. Ist das Bit b1 = 0 (Defaultwert), dann wird LRC verwendet. Es ist nur LRC und damit exclusive OR zu unterstützen. Sollte die Chipkarte die Verwendung von CRC anzeigen, ist die Kommunikation abubrechen.

5.2.14 T=15-Anzeige mit Voltage Class und Clock Stop Mode

Es wird empfohlen, T=15 anzuzeigen und im darauffolgenden TA1 die voltage class und den clock stop mode anzugeben (siehe ISO/IEC 7816-3, Kapitel 6.5.6 und 6.5.5).

5.2.15 T1 bis TK - Historical Bytes

Die Historical Bytes (HB) für ICCs mit asynchroner Übertragung enthalten keine Information, die vom MKT auszuwerten ist. Die Anzahl der Historical Bytes wird in T0 angezeigt.

Die ISO-konforme Nutzung ist in ISO/IEC 7816-4 beschrieben. Die folgende Abb. zeigt die empfohlene Codierung der Historical Bytes.

Historical Bytes				
CI	PIDO	CPDO	CLS	SW1-SW2
CI	= Category indicator ('00')			
PIDO	= Pre-issuing data object			
CPDO	= Card profile data object			
CLS	= Card life status (1 byte)			
SW1-SW2	= Status bytes			
Pre-issuing Data Object				
TPI	ICM	ICT	OSV	DD
TPI	= Tag pre-issuing DO ('6x')			
ICM	= IC manufacturer Id (1 byte)			
ICT	= IC type (1 byte, if b8 = 0; 2 bytes, if b8 = 1 of first byte)			
OSV	= Operating system version (2 bytes)			
DD	= Discretionary data (x bytes)			
Card Profile Data Object				
TCP	CP			
TCP	= Tag card profile DO ('3x')			
CP	= Card profile according ISO/IEC 7816-4, 8.3.2 (1 byte)			

Abb. 5: Historical Bytes (empfohlene Codierung)

Hinweise:

1. Das 'Card Profile Data Object' ist ein mandatory DO und gibt an, welche Anwendungs-Selektionsmethode(n) von der Chipkarte unterstützt werden und mit welchem Kommando ein DIR- und/oder ATR-File auszulesen ist, falls vorhanden. Wird nur die 'direct application selection'-Methode unterstützt, ist als Codierung '80' zu verwenden, d.h. das rechte Nibble wird nicht ausgewertet und ist daher auf 0 zu setzen.
2. Je nach Ausprägung der Karte kann z.B. auch das DO 'Card Capabilities' erforderlich sein.

Die Codierung für das Datenelement 'IC Manufacturer' ist der nachfolgenden Tabelle zu entnehmen (siehe auch ISO/IEC 7816-6/AM1).

ICM	IC Manufacturer according to ISO/IEC 7816-6/AM1
'01'	Motorola
'02'	STMicroelectronics
'03'	Hitachi
'04'	Philips Semiconductor
'05'	Siemens
'06'	Cylinec
'07'	Texas Instruments
'08'	Fujitsu
'09'	Matsushita
'0A'	NEC
'0B'	Oki
'0C'	Toshiba
'0D'	Mitsubishi
'0E'	Samsung
'0F'	Hyundai
'10'	LG

Tab. 2: ICM Codierung

5.2.16 TCK - Check Character

Der 'check character TCK' erlaubt die Überprüfung des ATR auf Übertragungsfehler. Der Wert wird durch exclusive ORing von T0 bis einschließlich TCK so berechnet, daß Null herauskommt.

Für ICCs mit Übertragungsprotokoll T=0 darf TCK nicht gesendet werden. Wird T=1 benutzt, muß TCK gesendet werden.

5.2.17 Empfohlene ATR-Codierung für T=0 und T=1

Abb. 6 zeigt die empfohlene ATR-Codierung für ICCs mit T=0 oder T=1 Übertragungsprotokoll entsprechend der 2. Ausgabe von ISO/IEC 7816-3:1997. Chipkarten, die beide Protokolle unterstützen und diese im ATR anzeigen, können ebenfalls von MKTs unterstützt werden.

T=0 ATR						
TS	T0	TD1	TD2	TA3	T1-TK	TCK
'3B'	'8x'	'80'	'1F'	'xx'	HB	XOR

TS = Initial Character (direct convention)
 T0 = Format Character (TD1 indic., x HB)
 TD1 = Interface Character (T=0, TD2 indication)
 TD2 = Interface Character (T=15, TA3 indic.)
 TA3 = Interface Character (XI- and UI-indication for clock stop mode and voltage class)
 T1-TK= Historical Characters (Hist. Bytes, max. 15)

T=1 ATR									
TS	T0	TD1	TD2	TA3	TB3	TD3	TA4	T1-TK	TCK
'3B'	'8x'	'81'	'B1'	'20' to 'FE'	'42'	'1F'	'xx'	HB	XOR

TS = Initial Character (direct convention)
 T0 = Format Character (TD1 indic., x = no. of HB)
 TD1 = Interface Character (T=1, TD2 indication)
 TD2 = Interface Character (T=1, TA3, TB3 indic.)
 TA3 = Interface Character (IFSC)
 TB3 = Interface Character (BWI, CWI)
 TD3 = Interface Character (T=15, TA4 indic.)
 TA4 = Interface Character (XI- and UI-indication for dock stop mode and voltage class)
 T1-TK= Historical Characters (Hist. Bytes, max. 15)
 TCK = Check Character (exclusive OR)

NOTES
 1. Other parameters may be present
 2. TB1 may be set to '00' or absent. Default values for Vpp support are not valid.

Abb. 6: Empfohlene ATR-Codierung für ICCs mit T= 0 oder T=1

5.3 Protocol Parameter Selection PPS

Die Unterstützung der PPS-Funktion wird für MKTs V1.0 dringend empfohlen. Zeigt die Chipkarte im TA1 an, daß sie mit anderen als den Default-Werten für Fi/Di zur Erzielung einer höheren Übertragungsrate arbeiten kann und unterstützt das MKT die PTS-Funktion, dann ist sie automatisch entsprechend ISO/IEC 7816-3 abzuwickeln. Ein MKT sollte in der Lage sein, neben der Basis-Baudrate von 9,6 kbaud eine Baudrate von mindestens 38,4 Kbaud bezogen auf eine Taktfrequenz von 3,5712 MHz zu unterstützen (siehe empfohlene TA1-Werte, Kap. 5.2.4).

6 Übertragungsprotokolle

6.1 Character Transmission Protocol T=0

6.1.1 Senden und Empfangen

Die Command Message, die vom MKT zur Chipkarte übertragen wird, enthält den Command Header inclusive Längen-Byte (CLA, INS, P1, P2, L). L zeigt entweder die Länge der Daten, die im 'command data field' folgen oder die Länge der Daten, die im 'response data field' erwartet werden. Nach Aussenden der 5 Header Bytes wartet das MKT auf ein Procedure Byte.

Auch nach Empfang einer Command Message mit Daten sendet die Chipkarte ein Procedure Byte zum Terminal, um es über den Fortgang der Kommunikation zu informieren.

Die Procedure Bytes und ihre Bedeutung sind in Tabelle 3 dargestellt.

Procedure Byte Value	Action
Equal to INS byte	All remaining data bytes should be transferred by the terminal, or the terminal should be ready to receive all remaining data bytes from the ICC
Equal to complement of INS byte	The next data byte should be transferred by the terminal, or the terminal should be ready to receive the next data byte from the ICC
'60'	The terminal should take into account additional work waiting time (max. 9600 etus). The ICC will sent a new procedure byte
'6x' or '9x' except '60'	The ICC returns as next byte SW2

Tab. 3: Procedure Bytes und ihre Bedeutung

6.1.2 Fehlerbehandlung

Wurde ein Zeichen nicht korrekt oder mit falscher Parity empfangen, dann soll der Empfänger die I/O-Leitung auf Low setzen nach 10.5 ± 0.2 etus nach Beginn des Start Bits für eine Zeitspanne von mindestens 1 und maximal 2 etus. Der Sender muß daher die I/O-

Leitung nach 11 ± 0.2 etus prüfen. Ist die I/O-Leitung im Zustand High, dann kann weitergesendet werden, andernfalls liegt die Fehlersituation vor und das betreffende Zeichen ist erneut zu senden.

Wird ein von der Chipkarte gesendetes Zeichen zweimal hintereinander mit falscher Parität empfangen, oder signalisiert die Chipkarte zweimal hintereinander den Empfang eines Paritätsfehlers, dann soll die Chipkarte deaktiviert werden und der Anwendung SW1-SW2 = '6F00' zurückgeliefert werden.

6.2 Block Transmission Protocol T=1

Ein T=1 Block besteht aus

- dem Prolog-Feld ('mandatory')
- dem Informations-Feld ('conditional')
- dem Epilog-Feld ('mandatory').

Abb. 7 zeigt den generellen Aufbau.

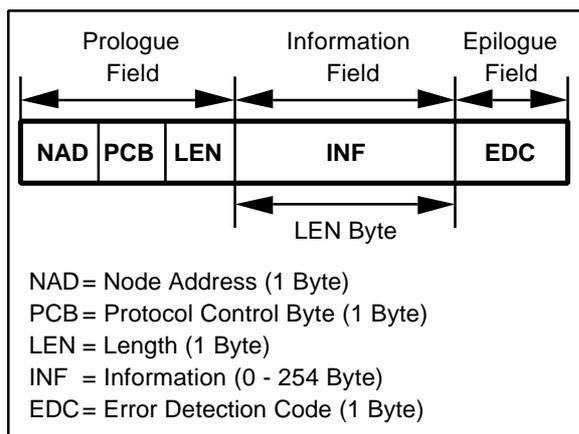


Abb. 7: T=1 Block

6.2.1 NAD - Node Address Byte

Das Node Address Byte ist vom Kartenterminal auf den Wert '00' zu setzen.

6.2.2 PCB - Protocol Control Byte

Das PCB-Byte kennzeichnet den Typ des T=1-Blocks:

- Information Block (I-Block)
- Receive Ready Block (R-Block)
- Supervisory Block (S-Block).

Die nachfolgenden drei Tabellen zeigen die Codierungen der T=1-Blöcke.

b8	0 (= Indication I-block)
b7	Send sequence number N(S)
b6	Chaining (more data bit M) M = 1 Chained data follow in subsequent block(s) M = 0 Last block of chain
b5-b1	0 (RFU)

Tab. 4: Codierung des I-Blocks

b8	1
b7	0 (b8,b7 = Indication of R-block)
b6	0 (RFU)
b5	Receive sequence number N(R)
b4-b1	0 = Error free 1 = EDC and/or parity error 2 = Other error(s) Other values RFU

Tab. 5: Codierung des R-Blocks

b8	1
b7	1 (b8,b7 = Indication of S-block)
b6	0 = Request 1 = Response
b5-b1	0 = RESYNCH (Resynchronisation) 1 = IFS (Information field size) 2 = ABORT (not used) 3 = WTX (BWT extension) 4 = Vpp error (not used) Other values RFU

Tab. 6: Codierung des S-Blocks

6.2.3 LEN - Length Byte

Das Längen-Byte enthält die Länge des Informationsfeldes eines Blocks. LEN kann im Prinzip die Werte von 0 bis 254 annehmen (255 ist RFU), die tatsächliche obere Grenze bei einer Kommunikation zwischen MKT und ICC ergibt sich jedoch aus dem ATR-Byte TA3, das den Wert für IFSC enthält. IFSD hat den Wert 254 und ist damit immer größer oder gleich IFSC.

6.2.4 INF - Information Field

Das Informationsfeld enthält bei I-Blocks 'application data' und bei S-Blocks - falls INF vorhanden - Kontroll-Information. Bei R-Blocks ist das Informationsfeld leer.

6.2.5 EDC - Error Detection Code

Als Error Detection Code darf nur der LRC ('longitudinal redundancy check') Verwendung finden (EDC-Default Wert). Der Wert des LRC ergibt sich durch 'exclusive OR' des NAD-Bytes bis einschließlich letztes Byte des INF-Feldes.

6.2.6 Block-Numerierung

MKT und ICC haben ihr eigenes Nummerierungssystem auf der Basis von modulo-2-Zähler.

Der Wert der Sequenz-Nummern nach dem Start der Kommunikation oder nach einer Resynchronisation ist null.

6.2.7 Einstellung von IFSC

Eine Chipkarte soll den IFSC-Wert im ATR anzeigen (siehe Interface Character TA3). Ein S-Block zur Einstellung der IFSC soll daher nicht gesendet werden. Falls das Kartenterminal doch einen entsprechenden S-Block erhält, soll es diesen nicht beantworten.

6.2.8 Einstellung von IFSD

IFSD (Puffergröße im Kartenterminal für Blöcke, die die Chipkarte sendet) hat als Defaultwert die Größe von 32 Bytes. Ein MKT ist jedoch mit einem Puffer von 258 Bytes auszustatten (IFSD = 254 Bytes, 3 Byte T=1-Prolog-Feld und 1 Byte T=1-EDC-Feld). Um der Chipkarte die Puffergröße im Kartenterminal mitzuteilen, muß das Kartenterminal daher den S-Block 'IFS-Request' mit dem Wert 'FE' an die Chipkarte senden. Dies ist vor Senden des ersten ICC-Kommandos, also unmittelbar nach dem Answer-to-Reset, durchzuführen. Die Chipkarte muß den 'IFS-request' mit 'IFS-response' beantworten.

6.2.9 Fehlerfreie Kommunikation

Bei fehlerfreier Kommunikation und ohne Chaining werden nur I-Blocks übertragen. Das M-Bit hat den Wert 0, die Sendesequenz-Zähler alternierend den Wert 0 bzw. 1. Das Senderecht für den ersten I-Block nach dem 'answer to reset' liegt beim MKT.

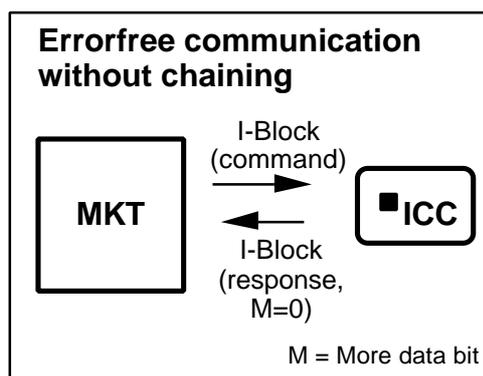


Abb. 8: Austausch von I-Blocks

Bei Verwendung von Chaining ist Flußkontrolle erforderlich, d.h. ein Block mit M-Bit = 1 muß mit einem R-Block quittiert werden, um dem Partner den korrekten Empfang und die weitere Empfangsbereitschaft anzuzeigen. Der R-Block trägt daher die Sendesequenznummer des nächsten erwarteten I-Blocks.

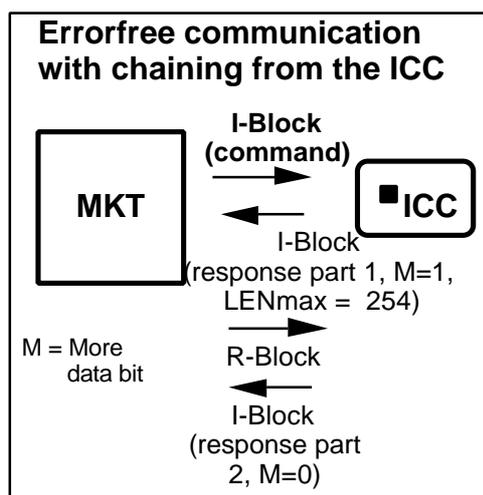


Abb.9: Austausch von I-Blocks mit Chaining

6.2.10 Fehlerbehandlungen

a) Übertragungsfehler

Ein Transmission Error liegt vor, wenn die Parität bei einem oder mehreren Bytes inkorrekt und/oder EDC falsch ist. In diesem Fall wird ein R-Block mit $b_4-b_1 = '1'$ und der Sequenz-Nr. des Blocks, der wiederholt werden soll, gesandt.

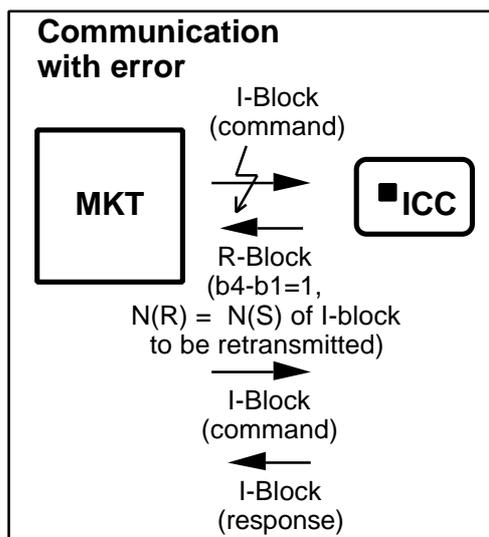


Abb. 10: Blockwiederholung nach Übertragungsfehler

b) Synchronisations-Fehler

Wird vom MKT ein BWT- oder CWT-Time-out erkannt, dann soll das MKT einen R-Block senden mit $b4-b1 = '2'$. Um Kollisionen zu vermeiden, muß das MKT jedoch zuvor feststellen ob die I/O-Leitung inaktiv ist. Ist sie jedoch aktiv, soll die Chipkarte deaktiviert und der Anwendung $SW1, SW2 = '6F00'$ zurückgeliefert werden.

c) Protokoll Fehler

Erhält die Chipkarte einen Block mit unzulässiger Codierung, soll sie einen R-Block mit $b4-b1 = '2'$ zurücksenden und die Kommunikation beenden.

Empfängt das Terminal einen nicht protokollkonformen Block, soll die Karte deaktiviert und der Anwendung $SW1, SW2 = '6F00'$ zurückgeliefert werden.

d) Abort Request

Erhält das Kartenterminal einen Abort Request, soll der Vorfall der Anwendung mit $SW1, SW2 = '6F00'$ mitgeteilt und die Karte deaktiviert werden. Das Kartenterminal selbst soll keinen 'abort request' an die Chipkarte senden.

7 Chipkarten-Schnittstelle für ICCs mit synchroner Übertragung

7.1 Physikalische Ansteuerung

7.1.1 Physical Characteristics

Die vom MKT zu unterstützenden ICCs mit synchroner Übertragung sind kontaktorientierte Chipkarten mit 5V-Technologie wie in ISO/IEC 7816-3 bzw. ISO/IEC 7816-10 beschrieben. Die 'Physical characteristics' sind entsprechend ISO/IEC 7816-1 auszugestalten.

7.1.2 Lage und Bedeutung der Kontakte

Es gelten dieselben Konventionen wie für ICCs mit asynchroner Übertragung.

7.1.3 Frequenz

Die Frequenz für ICCs mit synchroner Übertragung liegt zwischen 7 und 50 KHz. Es wird empfohlen, mit einer möglichst hohen Frequenz zu arbeiten, um eine hohe Übertragungsrate und damit eine Verkürzung der Übertragungszeit zu erzielen.

7.1.4 Bit-Übertragung

Die logische 0 eines Bits korrespondiert mit dem Zustand Low und die logische 1 mit dem Zustand High (siehe ISO/IEC 7816-3, Abschnitt 6.2.2). Das least significant bit lsb eines Bytes wird zuerst übertragen (direct convention), falls vom Chiphersteller nicht anders angegeben.

7.1.5 Reset

Erfolgt nach Einführen einer Chipkarte beim Reset und einer Taktfrequenz zwischen 1 und 5 MHz keine Antwort, ist von einer Chipkarte mit synchroner Übertragung auszugehen. Die Kontakte werden dann deaktiviert und anschließend erneut aktiviert. Der ATR wird dann nach dem Reset mit den ersten 32 Takten mit einer Frequenz entsprechend 7.1.3 ausgelesen. Bei ICCs, die auf das Reset nicht reagieren, ist von einem I²C-Bus-Chip ohne ATR-Unterstützung auszugehen. In diesem Fall muß der ATR mit einem Read-Befehl ausgelesen werden.

7.2 ATR

Entsprechend ISO/IEC 7816-3 besteht der ATR für Chipkarten mit synchroner Übertragung aus

- Byte H1: Protokoll-Typ
- Byte H2: Protokoll-Parameter
- Bytes H3, H4: Historical Bytes.

Der genaue Aufbau des ATR ist in MKT-Teil 5 'Chipkarten mit synchroner Übertragung - ATR und Datenbereiche' beschrieben. Nach Erhalt und Auswertung des ATR durch das MKT ist das im ATR angezeigte Übertragungsprotokoll zu verwenden.

7.3 Übertragungsprotokolle

MKTs, an denen synchrone Chipkarten und insbesondere Versichertenkarten gelesen werden sollen, müssen folgende Transmission-Protokolle für synchrone Chipkarten unterstützen:

- Serial Data Access Protocol (SDAP)
- 3 Wire Bus Protocol (3WBP)
- 2 Wire Bus Protocol (2WBP)

Die Einzelheiten der Übertragungsprotokolle sind im MKT-Teil 6 'Chipkarten mit synchroner Übertragung - Übertragungsprotokolle' und herstellerspezifischen Unterlagen zu entnehmen.