Teil 2

CT-ICC-Interface

MKT-Schnittstelle
fŸr kontaktorientierte Chipkarten
mit synchroner und asynchroner †bertragung

Version 0.9

28.07.95

GMD - Forschungszentrum Informationstechnik

€nderungen und ErgŠnzungen sind dem AK MKT vorbehalten.
GewŠhrleistung und Haftung sind ausgeschlossen.

Inhalt

1. Zweck

Zweck dieser Spezifikation ist es, fŸr Multifunktionale Kartenterminals (MKTs) die Schnittstelle fŸr

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

festzulegen. Die MKTs sind in ihrer derzeitigen AusprŠgung auf die Kommunikation mit kontaktorientierten Chipkarten ausgerichtet.

2. Referenzen

DIN NI-17: 1995
Chipkarten mit synchroner †bertragung
Teil 1: ATR und Datenbereiche

DIN NI-17.4: 1995
Chipkarten mit synchroner †bertragung
Teil 2: †bertragungsprotokolle

DIN NI-17.4: 1995
Chipkarten mit synchroner †bertragung
Teil 3: Anwendung von Inter-industry Commands

ISO 7816-1: 1987
Identification cards - Integrated circuit(s) cards with contacts
Part 1 - Physical characteristics

ISO 7816-2: 1988
Identification cards - Integrated circuit(s) cards with contacts
Part 2 - Dimensions and location of contacts

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 1137 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 10373 : 1993
Identification cards - Test methods

3. Definitionen und AbkŸrzungen

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
ICC = Integrated Circuit Card
H = High state
HB = Historical Bytes
HTSI = Host Terminal Software Interface
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
PTS = Protocol Type 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. Basis-Konzept

Ein Multifunktionales Kartenterminal soll in der Lage sein, mit kontaktorientierten Chipkarten kommunizieren zu kšnnen, die eines der vom MKT unterstŸtzten †bertragungsprotokolle (s. Abb. 1) verwenden.

Abb. 1: Vom MKT unterstŸtzte †bertragungsprotokolle

GrundsŠtzlich sind die fŸr die Kommunikation wichtigen ISO/IEC-Standards 7816-1/-2 und -3 zu beachten soweit sie nicht durch Festlegungen in dieser Spezifikation eingeschrŠnkt werden.
Die Interaktion mit der Chipkarte beginnt, nachdem das MKT das CT-Kommando REQUEST ICC (siehe CT-BCS-Spezifikation) erhalten hat und die Chipkarte eingefŸhrt wurde. DefaultmŠ§ig wird zunŠchst immer von einer asynchronen Chipkarte ausgegangen. Handelt es sich um eine solche, wird die Chipkarte auf den Reset mit einem Answer-to-Reset antworten, dem das MKT das eingestellte †bertragungsprotokoll entnehmen kann. Die Kommunikation kann fortgesetzt werden, falls 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, erhŠlt einen Return Code, der es Ÿber Erfolg oder Mi§erfolg der Reset-Prozedur unterrichtet.

Kommt keine Antwort auf das Reset, wird von einer synchronen Karte ausgegangen, d.h. nach Deaktivierung wird dann eine Aktivierung nach den Konventionen fŸr synchrone Karten durchgefŸhrt. Nach Reset sendet die Chipkarte mit synchroner †bertragung mit den 32 ersten Taktzyklen den 4-Byte-ATR (Aufbau s. DIN NI-17.4-Dokument). Eine Kommunikation ist mit Chipkarten mšglich, 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)

unterstŸtzen. Erfolgt keine RŸckantwort auf das Reset, soll das MKT versuchsweise von einer Chipkarte mit SDA-Protocol, aber ohne Reset-Funktion ausgehen. †ber Erfolg oder Mi§erfolg der Reset-Prozedur wird das Endsystem wie oben dargelegt informiert.

5. Chipkarten-Schnittstelle fŸr ICCs mit asynchroner †bertragung

5.1 Physikalische Ansteuerung

5.1.1 Physical Characteristics

Die vom MKT zu unterstŸtzenden ICCs mit asynchroner †bertragung sind kontaktorientierte Chipkarten mit 5V-Technologie wie in ISO/IEC 7816-3 (WD 1137) beschrieben (Vcc = 5V ± 0.25V DC). Die «Physical characteristics« sind entsprechend ISO/IEC 7816-1 auszugestalten.

In Abweichung vom ISO-Standard ist jedoch nicht von einer maximalen Stromaufnahme einer Chipkarte von 200 mA, sondern nur von 50 mA auszugehen. Die Stromversorgung fŸr die Chipkarte soll jedoch in der Lage sein, in einem †bergangszustand fŸr die Dauer von weniger als 400 ns eine Ladung von bis zu 40 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 Abb. 2 in ISO/IEC 7816-2. Die Kontakte C4 und C8 werden nicht benutzt.
Auch der Kontakt C6 (Programming Voltage Vpp) soll unbenutzt bleiben, d.h. das MKT soll keine Vpp erzeugen.

5.1.3 Frequenz

Nach EinfŸhrung einer Chipkarte ist zunŠchst immer von einer Mikroprozessor-Chipkarte mit asynchroner †bertragung auszugehen. Die Anfangsfrequenz kann nach ISO/IEC 7816-3 (WD 1137) im Bereich von 1 bis 5 MHz liegen. Es wird empfohlen, 3,5712 MHz oder 4,9152 MHz als (Anfangs-)Taktfrequenz zu benutzen. Die UnterstŸtzung von Frequenzen oberhalb von 5 MHz ist optional. Zeigt eine Chipkarte im Interface Character TA1 (siehe Abschnitt 5.2.3) an, da§ sie hšhere Frequenzen verkraften kann, so kann das Kartenterminal, falls es dazu in der

Lage ist, nach dem ATR sofort die hšhere Frequenz benutzen.

5.1.4 Bit-Dauer

Die Bit-Dauer fŸr Chipkarten mit asynchroner †bertragung wird als elementary time unit (etu) bezeichnet. FŸr die AusfŸhrung des Answer-to-Reset wird die initial etu (ietu) benutzt, die wie folgt definiert ist:

initial etu = 372/f sec

mit f = Frequenz zwischen 1 und 5 MHz. Wird die Frequenz 3,5712 MHz benutzt, ergibt sich eine Baudrate von 9,6 Kbps fŸr die Kommunikation zwischen Chipkarte und Kartenterminal.

FŸr die Kommunikation nach dem Answer-to-Reset wird die work etu (wetu) benutzt. Sie ist definiert durch

work etu = F/Df 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, hŠngt einerseits von den FŠhigkeiten 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 UnterstŸtzung der Protocol Type Selection Prozedur (siehe 5.3) ab.

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

	TA1 abwesend	**TA1 anwesend**
TA2 abwesend (negotiable mode)	wetu = ietu (zu unterstŸtzen)	wetu = ietu, wenn keine PTS-Prozedur durchgefŸhrt wird (zu unterstŸtzen) ---------- wetu = F/Df nach erfolgreichem PTS (entfŠllt, da PTS nicht unterstŸtzt)
TA2 anwesend (specific mode)	wetu = ietu (zu unterstŸtzen)	wetu = F/Df sofort nach ATR (UnterstŸtzung fŸr F = 372 und D=1; falls andere Werte angegeben, erneuter Reset (warm Reset); falls gleicher ATR, Abbruch)

Tab. 1: TA1/TA2-Kombinationen

5.1.5 Character Frame

Ein Character besteht aus 10 Bits:

- 1 Start Bit
- 8 Data Bits (= Data Byte)
- 1 Parity Bit mit gerader ParitŠt.

Die Bits des Data Bytes werden mit b1 bis b8 bezeichnet, wobei b1 das least significant bit lsb und b8 das most significant bit msb ist. Ob lsb oder msb zuerst Ÿbertragen wird, zeigt der Initial Character TS (erstes Byte des ATR) an.
Abb. 2 zeigt die †bertragungskonventionen mit den Pegeln H (=High) and L (=Low). Sie gelten nicht nur fŸr den Answer-to-Reset, sondern auch fŸr die gesamte Kommunikation. Bevor ein Character Ÿbertragen wird, mu§ die I/O-Leitung auf H gesetzt werden. Das Start Bit wird erkannt durch periodisches PrŸfen der I/O-Leitung in einem Zeitabstand von max. 0.2 etu.

Abb. 2: Character Frame

5.1.6 Kontakt-Aktivierung und Reset

Bei EinfŸhrung der Chipkarte sollen alle Signal-Kontakte den Pegel L haben (Vcc ² 0.4V, VOL 0 - 0.3V). Wenn das MKT die EinfŸhrung der Chipkarte erkannt hat und alle Kontakte physisch hergestellt sind, dann sollen die Kontakte wie folgt aktiviert werden:

- zuerst wird Vcc angelegt
- RST bleibt wŠhrend der Aktivierungsphase auf Low
- nachdem sich Vcc (nach max. 400 ns) stabilisiert hat, wird der I/O-Treiber des MKT auf Empfangs-Mode gesetzt, spŠtestens jedoch nach 200 Takt-Zyklen nach Einschaltung des Takts.

Abb. 3 zeigt die Kontakt-Aktivierung.

Abb. 3: Aktivierung der Kontakte

40.000 Zyklen nach Einschaltung des Takts wird der RST-Kontakt auf den Pegel H gesetzt. Die Chipkarte beginnt mit dem ATR frŸhestens nach 400, spŠtestens jedoch nach 40.000 Taktzyklen, gerechnet vom Zeitpunkt T1 an (= Zeitpunkt, des Setzens des RST-Kontakts auf H, siehe Abb. 4).

Abb. 4: Reset

5.2 Answer-to-Reset

5.2.1 ATR-Konzept

Der ATR dient zur †bertragung von Informationen, die bestimmte Eigenschaften der Kommunikation zwischen Chipkarte und Kartenterminal spezifizieren. Es wird davon ausgegangen, da§ *in der Regel* in einer Chipkarte mit asynchroner †bertragung nur *ein* Transmission Protocol vorhanden ist (entweder T = 0 oder T = 1).

5.2.1 TS - Initial Character

Der ATR bei ICCs mit asynchroner †bertragung beginnt mit dem Initial Character TS. Er hat entweder den Wert «3F« bei Verwendung der «inverse convention« oder «3B« bei Verwendung der «direct convention«.
Wird die direkte Konvention benutzt, dann bedeutet der Zustand H (siehe 5.1.5) eine logische 1 und das lsb wird zuerst gesendet (Ÿbliche Konvention). Wird die inverse Konvention benutzt, dann bedeutet der Zustand L eine logische 1 und das msb wird zuerst gesendet (die inverse Konvention bezieht sich nur auf die Datenbits und das Parity-Bit, nicht auf Start- und Stop-Bits).
TS erlaubt daher die Bit-Synchronisation zwischen Kartenterminal und ICC *und* zeigt die logische Konvention fŸr die Interpretation der nachfolgenden Characters an.
Die UnterstŸtzung der «direct convention« («3B«) ist mandatory, die UnterstŸtzung der «inverse convention« («3F«) ist optional.

5.2.2 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. 5).

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

5.2.3 TA1 - Interface Character fŸr Frequenz und Bit-Dauer

Der Interface Character TA1 enthŠlt, falls vorhanden, die Codierungen fŸr FI und DI (Integerwerte fŸr Frequenz F und Bit Rate Adjutment Factor D, siehe Tabellen 6 und 7 in ISO/IEC 7816-3).
FŸr die †bertragungsphase nach dem answer to reset gilt die Gleichung

work etu = F/Df 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 unterstŸtzen. Andere Werte kšnnen angezeigt werden, sind jedoch entsprechend den Vorgaben in Tab. 1 zu behandeln.
Werden die Defaultwerte benutzt, soll die †bertragung des TA1 Characters entfallen.

5.2.4 TB1 - Interface Character fŸr «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). Da keine Programmierspannung unterstŸtzt wird, sollte als Wert fŸr TB1 von den ICCs «00« zurŸckgeliefert werden (= I max = 25 mA, Vpp not connected).
Sollte fŸr TB1 ein Wert «00« codiert sein, wird dieser nicht weiter ausgewertet.

5.2.5 TC1 - Interface Character fŸr «Extra Guard Time«

TC1 ŸbertrŠgt die «extra guard time« N (Einheit: etu), die der minimalen Dauer zwischen den

Abb. 5: Anzeige des Vorhandenseins von Interface-Characters in T0 (i=0) und TDi-Character (i=1, 2, ...)

Flanken der Start-Bits zweier aufeinanderfolgenden Characters hinzugefŸgt werden soll. Der Defaultwert von N ist Null und sollte von den Chipkarten unterstŸtzt werden. TC1 sollte daher im ATR nicht Ÿbertragen werden.

5.2.6 TD1 - Interface Character fŸr «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 fŸr die Kommunikation zwischen MKT und ICC benutzt werden soll.

FŸr ICCs mit †bertragungsprotokoll T=0 soll TD1 nicht zurŸckgeliefert werden (bei Abwesenheit von TD1 ist nach ISO/IEC 7816-3 das †bertragungsprotokoll T=0 zu benutzen; da TA2 bis TD2 fŸr T=0 nicht benutzt werden, ist die †bertragung von TD1 fŸr T=0 redundant und daher nicht sinnvoll).

FŸr ICCs mit †bertragungsprotokoll T=1 mu§ TD1 anwesend sein, wobei b1 auf 1 gesetzt ist. Werden weitere Angaben zu T=1 benštigt (was in der Regel der Fall ist), dann ist die Anwesenheit von TD2 anzuzeigen. Eine Ÿbliche Codierung von TD1 ist fŸr T=1 daher «81«.

5.2.7 TA2 - Interface Character fŸr «Specific Mode of Operation«

Wird TA2 im ATR *nicht* Ÿbertragen, dann zeigt die Chipkarte damit an, da§ sie sich im «negotiable mode« befindet. Wird TA2 Ÿbertragen, dann zeigt die Chipkarte damit den «specific mode of operation« an.

5.2.8 TC2 - Interface Character fŸr 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 x D x WI, wobei TC2 den Wert fŸr WI enthŠlt. Es wird von den Default-Werten fŸr D und WI Gebrauch gemacht, d.h. das maximale Intervall betrŠgt 9600 etus. TC2 soll daher nicht im ATR Ÿbertragen werden.

5.2.9 TD2 - Interface Character fŸr 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 Ÿbertragen werden, ist der Ÿbliche Wert dieses Nibbles 3.

Das «least significant nibble (bits b4-b1)« enthŠlt wieder die Angabe des Protokoll-Typs. TD2 hat daher den Wert «31«.

5.2.10 TA3 - Interface Character fŸr T=1 Information Field Size Card

TA3 gibt die maximale LŠnge 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 zurŸckgeliefert werden, da kaum eine Chipkarte nur ein IFSC von 32 Byte hat, was der (veraltete) Default-Wert ist). Der Wert von TA3 mu§ im Bereich 32 bis 254 liegen («20«- «FE«).

5.2.11 TB3 - Interface Character fŸr 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 mšglichst schnelle †bertragung zu haben, sollten die Werte fŸr TB3 unter dem Defaultwert liegen.

5.2.12 TC3 - Interface Character fŸr 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 unterstŸtzen. Sollte die Chipkarte die Verwendung von CRC anzeigen, ist die Kommunikation abzubrechen.

5.2.13 T1 bis TK - Historical Bytes

Die Historical Bytes (HB) fŸr ICCs mit asynchroner †bertragung 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.

Abb. 6: 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 unterstŸtzt werden und mit welchem Kommando ein DIR- und/oder ATR-File auszulesen ist, falls vorhanden. Wird nur die «direct application selection«-Methode« unterstŸtzt, ist als Codierung «80« zu verwenden, d.h. das rechte Nibble wird nicht ausgewertet und ist daher auf 0 zu setzen.
2. Je nach AusprŠgung der Karte kann z.B. auch das DO «Card Capabilities« erforderlich sein.

5.2.14 TCK - Check Character

Der «check character TCK« erlaubt die †berprŸfung des ATR auf †bertragungsfehler. Der Wert wird durch exclusive ORing von T0 bis einschlie§lich TCK so berechnet, da§ Null herauskommt.
FŸr ICCs mit †bertragungsprotokoll T=0 darf TCK nicht gesendet werden. Wird T=1 benutzt, mu§ TCK gesendet werden.

5.2.15 Empfohlene ATR-Codierung fŸr T=0 und T=1

Abb. 7 zeigt die empfohlene ATR-Codierung fŸr ICCs mit T=0 oder T=1 †bertragungsprotokoll.

Abb. 7: Empfohlene ATR-Codierung fŸr ICCs mit asynchroner †bertragung

5.3 Protocol Type Selection PTS

Die Funktion PTS wird nicht unterstŸtzt.

6. †bertragungsprotokolle

6.1 Character Transmission Protocol T=0

6.1.1 Senden und Empfangen

Die Command Message, die vom MKT zur Chipkarte Ÿbertragen wird, enthŠlt den Command Header inclusive LŠngen-Byte (CLA, INS, P1, P2, L). L zeigt entweder die LŠnge der Daten, die im «command data field« folgen oder die LŠnge 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 Ÿber den Fortgang der Kommunikation zu informieren.
Die Procedure Bytes und ihre Bedeutung sind in Tabelle 2 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. 2: Procedure Bytes und ihre Bedeutung

6.1.2 Fehlerbehandlung

Wurde ein Zeichen nicht korrekt oder mit falscher Parity empfangen, dann soll der EmpfŠnger die I/O-Leitung auf Low setzen nach 10.5 ± 0.2 etus nach Beginn des Start Bits fŸr eine Zeitspanne von mindestens 1 und maximal 2 etus. Der Sender mu§ daher die I/O-Leitung nach 11 ± 0.2 etus prŸfen. 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.

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. 8 zeigt den generellen Aufbau.

Abb. 8: T=1 Block

6.2.1 NAD - Node Address Byte

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

Hinweis: Die Nutzung des NAD-Bytes ist jedoch fŸr eine spŠtere Version vorgesehen.

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 3 Tabellen zeigen die Codierungen der T=1-Blšcke.

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. 3: 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. 4: 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. 5: Codierung des S-Blocks

6.2.3 LEN - Length Byte

Das LŠngen-Byte enthŠlt die LŠnge des Informationsfeldes eines Blocks. LEN kann im Prinzip die Werte von 0 bis 254 annehmen (255 ist RFU), die tatsŠchliche obere Grenze bei einer Kommunikation zwischen MKT und ICC ergibt sich jedoch aus dem ATR-Byte TA3, das den Wert fŸr IFSC enthŠlt. IFSD hat den Wert 254 und ist damit immer grš§er oder gleich IFSC.

6.2.4 INF - Information Field

Das Informationsfeld enthŠlt 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 einschlie§lich letztes Byte des INF-Feldes.

6.2.6 Block-Numerierung

MKT und ICC haben ihr eigenes Numerierungssystem auf der Basis von modulo-2-ZŠhler.
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 erhŠlt, soll es diesen nicht beantworten.

6.2.8 Einstellung von IFSD

IFSD (Puffergrš§e im Kartenterminal fŸr Blšcke, die die Chipkarte sendet) hat als Defaultwert die Grš§e 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 Puffergrš§e im Kartenterminal mitzuteilen, mu§ 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, durchzufŸhren. Die Chipkarte mu§ den «IFS-request« mit «IFS-response« beantworten.

6.2.9 Fehlerfreie Kommunikation

Bei fehlerfreier Kommunikation und ohne Chaining werden nur I-Blocks Ÿbertragen. Das M-Bit hat den Wert 0, die Sende-Sequenz-ZŠhler alternierend den Wert 0 bzw. 1. Das Senderecht fŸr den ersten I-Block nach dem «answer to reset« liegt beim MKT.

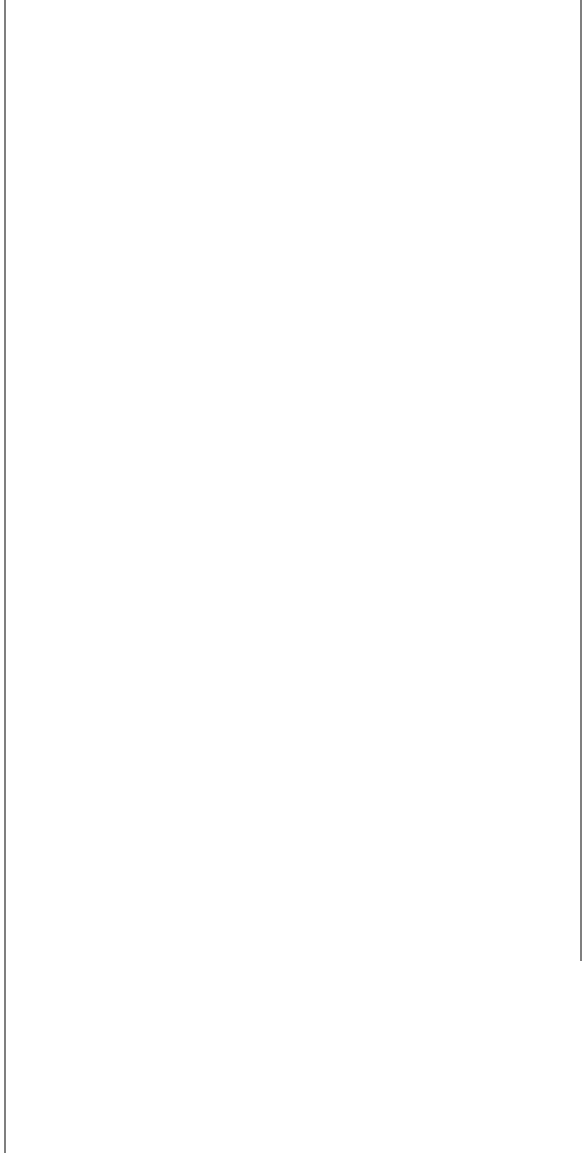

Abb. 9: Austausch von I-Blocks

Bei Verwendung von Chaining ist Flu§kontrolle erforderlich, d.h. ein Block mit M-Bit = 1 mu§ mit einem R-Block quittiert werden, um dem Partner den korrekten Empfang und die weitere Empfangsbereitschaft anzuzeigen. Der R-Block trŠgt daher die Send Sequence Number des nŠchsten erwarteten I-Blocks.

Abb.10: Austausch von I-Blocks mit Chaining

6.2.10 Fehlerbehandlungen

a) †bertragungsfehler

Ein Transmission Error liegt vor, wenn die ParitŠt bei einem oder mehreren Bytes inkorrekt und/oder EDC falsch ist. In diesem Fall wird ein R-Block mit b4-b1 = «1« und der Sequenz-Nr. des Blocks, der wiederholt werden soll, gesandt.

Abb. 11: Blockwiederholung nach †bertragungs-fehler

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, mu§ 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« zurŸckgeliefert werden.

c) Protokoll Fehler

ErhŠlt die Chipkarte einen Block mit unzulŠssiger Codierung, soll sie einen R-Block mit b4-b1 = «2« zurŸcksenden und die Kommunikation beenden.
EmpfŠngt das Terminal einen nicht protokollkonformen Block, soll die Karte deaktiviert und der Anwendung SW1,SW2 = «6F00« zurŸckgeliefert werden.

d) Abort Request

ErhŠlt 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 fŸr ICCs mit synchroner †bertragung

7.1 Physikalische Ansteuerung

7.1.1 Physical Characteristics

Die vom MKT zu unterstŸtzenden ICCs mit synchroner †bertragung sind kontaktorientierte Chipkarten mit 5V-Technologie wie in ISO/IEC 7816-3 (WD 1137) beschrieben. Die «Physical characteristics« sind entsprechend ISO/IEC 7816-1 auszugestalten.

7.1.2 Lage und Bedeutung der Kontakte

Es gelten dieselben Konventionen wie fŸr ICCs mit asynchroner †bertragung.

7.1.3 Frequenz

Die Frequenz fŸr ICCs mit synchroner †bertragung liegt zwischen 7 und 50 KHz. Es wird empfohlen, mit einer mšglichst hohen Frequenz zu arbeiten, um eine hohe †bertragungsrate und damit eine VerkŸrzung der †bertragungszeit zu erzielen.

7.1.4 Bit-†bertragung

Die logische 0 eines Bits korrepondiert 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 Ÿbertragen (direct convention), falls vom Chiphersteller nicht anders angegeben.

7.1.5 Reset

Erfolgt nach EinfŸhren einer Chipkarte beim Reset und einer Taktfrequenz zwischen 1 und 5 MHz keine Antwort, ist von einer Chipkarte mit synchroner †bertragung auszugehen. Die Kontakte werden dann deaktiviert und anschlie§end 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 I^2C-Bus-Chip ohne ATR-UnterstŸtzung auszugehen. In diesem Fall mu§ der ATR mit einem Read-Befehl ausgelesen werden.

7.2 ATR

Entsprechend ISO/IEC 7816-3 besteht der ATR fŸr Chipkarten mit synchroner †bertragung aus

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

Der genaue Aufbau des ATR ist in dem DIN-Papier «Chipkarten mit synchroner †bertragung: Teil 1: ATR und Datenbereiche« beschrieben.

7.3 †bertragungsprotokolle

Es sind Chipkarten mit folgenden Transmission-Protokollen zu unterstŸtzen:

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

Die Einzelheiten der †bertragungsprotokolle sind dem DIN-Papier «Chipkarten mit synchroner †bertragung, Teil 2: †bertragungsprotokolle« und herstellerspezifischen Unterlagen zu entnehmen.