Teil 8

Host-CT-Schnittstelle
für
MKTs mit V.24/V.28-Anschluß

Version 0.9

28.07.95

GMD - Forschungszentrum Informationstechnik

Inhalt

1. Zweck

Ziel dieser Spezifikation ist, die Schnittstelle für multifunktionale Kartenterminals festzulegen, die als externes Gerät ausgeprägt sind und über eine V.24-Schnittstelle an einen Host-Rechner angeschlossen werden sollen. Die Schnittstellen-beschreibung beschränkt sich auf die physikalische Schicht und die Übertragungsschicht. Auf der Anwendungsebene treten Kartenterminal-Kommandos (siehe CT-BCS) und Chipkarten-Kommandos auf.
Als Übertragungsprotokoll wird das Block Transmission Protocol T=1 verwendet.
Die multifunktionalen Kartenterminals (MKTs) sind funktionell aufwärtskompatibel zu den Versichertenkartenterminals (VKTs).

2. Referenzen

Deutsche Telekom, GMD, RWTÜV, TeleTrusT Deutschland: 1995
CT-API 1.1 - Anwendungsunabhängiges Card-Terminal Application Programming Interface für Chipkartenanwendungen

TeleTrusT Deutschland: 1995
CT-BCS - Anwendungsunabhängiger CardTerminal Basic Command Set für Chipkartenanwendungen

ISO/IEC 7816-3: 1989
Identification cards - Integrated circuit(s) cards with contacts
Part 3 - Electronic Signals and transmission protocols
AM 1: Clause 9: Protocol T=1, asynchronous half duplex block transmission protocol
AM 2: Protocol type selection
(Verwendung findet der WD vom Oktober 1994, in dem AM 1 und AM 2 integriert sind)

ITU-T Recommendation V.24 (03/93)
List of Definitions for Interchange Circuits between Data Terminal Equipment (DTE) and DATA Circuit Terminating Equipment (DCE)

ITU-T Recommendation V.28 (03/93)
Electrical Characteristics for Unbalanced Double-Current Interchange Circuits

3. Abkürzungen

ATR = Answer-to-Reset
BWT = Block Waiting Time
CT = CardTerminal
CT-API=CT Application Programming Interface
CT-BCS = CT Basic Command Set
CTS = Clear to Send
CWT = Character Waiting Time
DAD = Destination Address
EDC = Error Detection Code
HB = Historical Bytes
HTSI = Host Transport Service Interface
ICC = Integrated Circuit(s) Card
IFS = Information Field Size
MKT = Mulrtifunktionales Kartenterminal
NAD = Node Address byte
PCB = Protocol Control Byte
R-Host = Remote Host
RTS = Request to Send
SAD = Source Address
Vpp = Programming Voltage
XOR = Exclusive Or

4. Übertragungsparameter

Für die Kommunikation zwischen Host (PC oder Workstation) und Karten-Terminal werden folgende Übertragungsparameter festgelegt:

- Geschwindigkeit (Baud Rate): 9600 Baud und optional zusätzlich höhere Geschwindigkeiten
- Zeichenrahmen (Character-Frame): 1 Startbit, 8 Datenbits, 1 Parity bit (Even Parity), 1 Stopbit; Bit b1 ist das ´least significant bit (lsb)´, Bit b8 das ´most significant bit (msb)´; das lsb-Bit wird stets zuerst übertragen
- Zu unterstützende Größe des Informationsfeldes in einem Übertragungsblock (Information Field Size CardTerminal IFST): 254 Byte (d.h. der Ein-/Ausgabe-Puffer im Karten-Terminal muß mindestens 258 Byte (254 Byte Informationsfeld + 4 Byte T=1-Rahmen) aufnehmen können)
- Maximale Wartezeit auf einen Übertragungsblock mit der Rückantwort zu einen vorher gesandten Kommando (Block Waiting Time BWT): 1000 ms

- Maximaler Zeitabstand zwischen zwei Zeichen eines Übertragungsblocks (Character Waiting Time CWT): 100 ms
- Minimale Wartezeit zwischen Empfang des letzten Zeichen eines Blocks und Aussenden des ersten Zeichen des Antwort-Blocks (Block Guard Time BGT): 2 ms
- Prüfsumme (Error Detection Code EDC): XOR (Exclusiv-Oder-Verknüpfung)
- RTS- und CTS-Leitungen: RTS- und CTS-Leitungen werden von der Host-Software nicht bedient. Es ist daher ein gebrücktes Kabel zu verwenden (siehe Anhang).

5. Das Übertragungsprotokoll

Als Übertragungsprotokoll ist das Block Transmission Protokoll T = 1 (s. ISO/IEC 7816-3) zu verwenden. Abb. 1 zeigt den Aufbau eines T=1-Blockes.

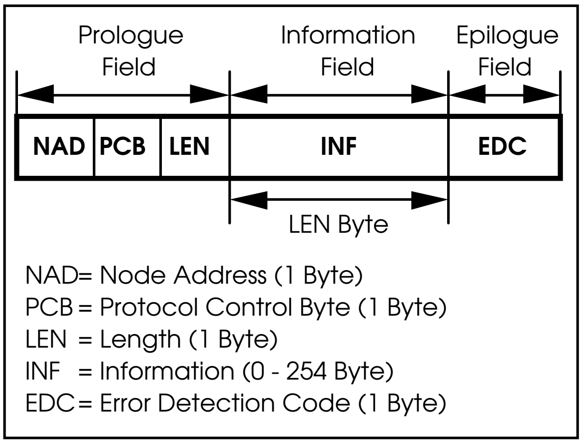

Abb. 1: T=1 Block

Folgende Festlegungen sind zu beachten:

a) Das NAD-Byte

Das NAD-Byte dient zur Kennzeichnung von Sender und Empfänger eines Übertragungsblocks. Im linken Halbbyte steht die Empfänger-Adresse (Destination Address DAD), im rechten Halbbyte die Absender-Adresse (Source Address SAD). Beim Senden eines Kommandos vom Host sind folgenden Adressen zu verwenden:

NAD (DAD/SAD)	Bedeutung
02 05	ICC Command von Host an ICC1 ICC Command v. R-Host an ICC1
12 15	CT Coomand von Host an CT CT Command von R-Host an CT
22 25	ICC Command von Host an ICC2 ICC Command v. R-Host an ICC2
...	...
E2 E5	ICC Command von Host an ICC14 ICC Command v. R-Host an ICC14

Tab. 1: Adressen beim Senden eines Kommandos von Host oder R-Host an das CT bzw. an eine ICC

Die Unterstützung der DAD-Adressen ´0´ und ´1´ ist obligatorisch, die Unterstützung höherer Adressen ist abhängig von der Anzahl der zusätzlich vorhanden ICC-Interfaces in einem Kartenterminal.
Das NAD-Byte wird von dem HTSI-Modul (s. CT-API-Beschreibung) gesetzt, wobei das rechte Nibble des in der CT_data-Funktion übergebenen DAD-Bytes auf das linke Nibble des NAD-Bytes und das rechte Nibble des in der CT_data-Funktion übergebenen SAD-Bytes auf das rechte Nibble des NAD-Bytes abgebildet wird.

Beim Senden einer Antwort werden vom Kartenterminal folgende NAD-Codierungen verwendet, wobei SAD-Werte > ´1´ nur bei Kartenterminals mit mehreren ICC-Schnittstellen auftreten:

NAD (DAD/SAD)	Bedeutung
20 50	ICC Response von ICC1 an Host ICC Response v. ICC1 an R-Host
21 51	CT Response von CT an Host CT Response von CT an R-Host
22 52	ICC Response von ICC2 an Host ICC Response v. ICC2 an R-Host
...	...
2E 5E	ICC Response von ICC14 an Host ICC Response v. ICC14 an R-Host

Tab. 2: Adressen beim Senden einer Antwort vom CT bzw. einer ICC an Host oder R-Host

b) Das PCB-Byte

Das Protocol Control Byte (PCB-Byte) enthält Informationen, die zur Kontrolle der Übertragung benötigt werden. Die Codierungen für

- I-Block
- R- Block
- S-Block

sind ISO/IEC 7816-3-konform vorzunehmen (siehe Tab. 3-5).

Die nachfolgenden 3 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. 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 (not used) 2 = ABORT (not used) 3 = WTX (BWT extension) 4 = Vpp error (not used) Other values RFU

Tab. 5: Codierung des S-Blocks

1. Fehlerfreie Übertragung

CT-Kommandos und ICC-Kommandos sowie deren zugehörige Antworten werden im sog. I-Block (Information-Block) übertragen. Der Sende-Sequenz-Zähler ist ein Sicherheitsmerkmal zur Erkennung des Verlustes eines Übertragungsblocks und ist daher zu unterstützen. Er nimmt alternierend die Werte 0 und 1 an, d.h. der erste vom Host gesendete Block hat im PCB-Byte die Codierung ´00´, der 2. die Codierung ´40´, der 3. wieder ´00´ usw.
Der Daten-Kettungs-Mechanismus (More data bit) ist ebenfalls zu unterstützen, sodaß Anwendungseinheiten (z.B. die Antwort auf ein READ BINARY-Kommando) über die Länge eines einzelnen Blocks hinausgehen können. Die Information wird hierbei auf n Blöcke aufgeteilt, wobei (n-1) Blöcke eine Länge entsprechend der Information Field Size (254 Byte) haben und der n-te Block die restlichen Bytes (max. 254) enthält. Da beim Senden aufeinander folgender Informationsblöcke Flußkontrolle benötigt wird, ist ein I-Block mit M-Bit=1 mit einem Receive Ready-Block (R-Block) zu quittieren.

2. Übertragung mit Fehlerbehandlung

Wird ein fehlerhafter I-Block empfangen, ist dies dem Kommunikationspartner mit einem R-Block anzuzeigen (siehe Abb. 6). Hierbei hat Bit b5 des R-Blocks den Wert der Send Sequence Number des Blocks, der wiederholt werden soll.
Tritt ein Fehler zum zweiten Mal hintereinander auf, ist vom Host her eine Resynchronisation durchzuführen (siehe Abschnitt 4). Auch in anderen Fehlersituationen (z.B. falscher R-Block oder Timeout) ist eine Resynchronisation anzustoßen. Blöcke, deren Adressen im NAD-Byte fehlerhaft sind, werden vom CardTerminal ignoriert, d.h. es wird keine Antwort gesendet.

3. Antwortzeit-Verlängerung

Empfängt das Karten-Terminal ein Kommando, dessen Ausführung länger als die Block Waiting Time von 1000 ms dauert (das kommt z.B. beim Anfordern der Chipkarte vor), dann sendet das

Karten-Terminal einen WTX request (WTX = Waiting Time Extension), der vom Host her mit einem WTX response zu beantworten ist. WTX request/response werden mit einem S-Block (Supervisory Block) übertragen, wobei im INF-Feld der 1-byte-lange Multiplikator des BWT-Wertes angegeben wird. Die Waiting Time Extension beginnt, nachdem das letzte Byte der WTX response empfangen wurde. Sie bezieht sich grundsätzlich nur auf den nächsten zu übertragenden Antwort-Block.
Ein WTX request kann auch vom Host abgelehnt werden. In diesem Fall wird als Antwort auf ein WTX request ein RESYNCH request gesendet, das vom Karten-Terminal mit RESYNCH response zu beantworten ist. Einzelheiten hierzu sind in Abschnitt 4 beschrieben.

4. Resynchronisation

Zur Resynchronisation kann vom PC bzw. der Workstation ein RESYNCH request gesendet werden, der vom Karten-Terminal mit dem RESYNCH response zu beantworten ist. Der RESYNCH request ist *immer* nach dem Start einer Anwendung vom HTSI-Modul im Host zum Karten-Terminal als Bestandteil der Ausführung der CT_init-Funktion (s. CT-API-Beschreibung) zu senden. Auch in bestimmten Fehlersituationen (siehe Abschnitt 2) sowie zum Abbruch eines Kommandos, falls dies notwendig ist (siehe Abschnitt 3), ist der RESYNCH-Mechanismus einzusetzen. Mit dem RESYNCH request/response-Paar werden die Übertragungsprotokollautomaten in Host und Karten-Terminal sychronisiert bzw. nach fehlerhafter oder unterbrochener Kommunikation resynchronisiert. Die Sende-Sequenz-Zähler werden durch diesen Befehl ebenfalls auf Null zurückgesetzt. Ein ggf. in Bearbeitung befindliches Anwendungs-Kommando wird abgebrochen.

c) Das LEN-Byte

Im LEN-Byte wird die Länge des Informationsfeldes als Binärzahl angegeben.

d) Das INF-Feld

Im Informationsfeld wird das Kommando bzw. die Antwort auf das Kommando übertragen.

e) Das EDC-Feld

Im EDC-Feld wird die XOR-Prüfsumme (1 Byte) übertragen.

Anhang (normativ)

Anschlußbelegung für serielle Kommunikation

Zur Verbindung des MKT mit einem Hostrechner wird am MKT eine 9-polige Sub-D-Buchse (female) verwendet.

Für die serielle Kommunikation mit dem Hostrechner werden folgende Signale benutzt:

RxD = Received Data
TxD = Transmitted Data
GND = Signal Ground

Tab. 1 zeigt die Stift-Belegungen auf der Host- und der MKT-Seite, wobei die Host-Seite hier beispielhaft als ein Rechner der PC-AT-Klasse angenommen wird.

Tab. 1: Stift-Belegungen

Sift-Nr. Bsp. PC-AT, 9-polig, Stecker	Host	MKT	Stift-Nr. MKT, 9-polig, Buchse
2	RxD	TxD	2
3	TxD	RxD	3
5	GND	GND	5

Die Belegung wurde so gewählt, daß das MKT mit einem Hostrechner über ein Kabel verbunden werden kann, welches auf der einen Seite eine Buchse und auf der anderen Seite einen Stecker hat und bei dem die Stifte (Pins) gleicher Nummer ohne Kreuzungen miteinander verbunden werden.