Part 2

CT-ICC-Interface

MCT interface
for contact orientated ICCs
with
asynchronous and synchronous transmission

Version 0.9

Date: 28.07.95

GMD- Forschungszentrum Informationtechnik GmbH

Contents

1. Scope

In this specification, the interface of Multifunctional CardTerminals (MCT) for

- IC cards with asynchronous transmission (processor cards with T=0 and T=1 protocol) and

- IC cards with synchronous transmission (memory cards with SDA-, 2WB- and 3WB-protocol)

is specified. The MCTs described in this specification are made for communication with contact orientated IC cards.

2. Normative references

DIN NI-17: 1995
IC cards with synchronous transmission,
Part 1: ATR and data sections

DIN NI-17: 1995
IC cards with synchronous transmission,
Part 2: Transmission protocols

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

(The WD 1137 dated october 1994 is applied, in which AM 1 and AM 2 are integrated.)

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. Definitions und abbreviations

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
EDC	= Error Detection Code
etu	= elementary time unit
ICC	= Integrated Circuit(s) Card
H	= High state
HB	= Historical Bytes
HTSI	= Host Transport Service Interface
IFSC	= Information Field Size Card
IFSD	= Information Field Size Device
IM	= Interface Module
INS	= Instruction code
ietu	= initial etu
L	= Low state
LRC	= Longitudinal Redundancy Check
MCT	= Multifunctional CardTerminal
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
XOR	= Exclusive Or
2WB	= 2 Wire Bus
3WB	= 3 Wire Bus

4. Basic concept

A Multifunctional CardTerminal shall be able to communicate with those contact orientated IC cards which use one of the transmission protocols supported by the MCT (see fig. 1).

Fig. 1: Transmission protocols supported by the MCT

Basically the communication relevant ISO/IEC-standards 7816-1/-2 und -3 shall be followed as long as they are not restricted by the definitions in this specification.

The interaction with the IC card starts after the MCT has received the CT command REQUEST ICC (see CT-BCS specification) and the IC card has been inserted. By default the insertion of an asynchronous IC card is assumed. If so, the IC card will answer to the reset with an Answer-to-Reset, from which the MCT can read which transmission protocol is set. Communication can be continued, if either T=0 or T=1 (see ISO/IEC 7816-3) is indicated as transmission protocol. If not, communication with the IC card is aborted and the contacts are deactivated. The host system from which the REQUEST ICC command came receives a return code with the information about success or failure of the reset procedure.

If there is no answer to the reset, the insertion of a synchronous IC card is assumed, i.e. after deactivation an activation is started according to the conventions for synchronous IC cards. After reset the IC card with synchronous transmission sends during the first 32 clock cycles the 4-byte-ATR (structure see ´ICCs with synchronous transmission, Part 1: ATR and data sections´). Communication is possible with IC cards, whose chips support either

- the Serial Data Access Protocol (e.g. I^2C-bus chips with reset) or
- the 3 Wire Bus Protocol (e.g. SLE 4418/28) or
- the 2 Wire Bus Protocol (e.g. PCB 2032/42 and SLE 4432/42)

If there is no answer to this reset, the MCT shall assume the insertion of an IC card with SDA protocol but without reset function. The host system is informed as described above of success or failure of the reset procedure.

5. Interface for ICCs with asynchronous transmission

5.1 Physical communication

5.1.1 Physical Characteristics

The ICC's with asynchronous transmission which the MCT shall support are contact orientated IC cards with 5V technology as described in ISO/IEC 7816-3 (WD 1137) (Vcc = 5V ± 0.25V DC). The physical characteristics shall comply with ISO/IEC 7816-1.

It can be postulated that the maximum power consumption of the IC cards is not 200 mA as stated in the ISO-standard but only 50 mA. The power supply for the IC card shall, however, be able for a period of not more than 400 ns to supply a charge of up to 40 nAs from a maximum power input of 100 mA.

In the MCTs only contact units shall be used which do not cause undue wear to the contacts.

5.1.2 Location and usage of contacts

The location and usage of the contacts comply with fig 2 in ISO/IEC 7816-2. Contacts C4 and C8 are not used.

Contact C6 (programming voltage Vpp) shall also remain unused, i.e. the MCT shall not produce Vpp.

5.1.3 Frequency

If an ICC is inserted, at a card with asynchronous transmission is assumed. The initial frequency shall be acc. to ISO/IEC 7816-3 (WD 1137) within the range from 1 to 5 MHz. The use of 3.5712 MHz or 4.9152 MHz is recommended as (initial) clock frequency. The support of frequencies higher than 5 MHz is optional. If an IC card indicates in the interface character TA1 (see section 5.2.3), that it can handle higher frequencies, the CardTerminal shall proceed in accordance with the specification given in tab. 1 (see 5.1.4).

5.1.4 Bit duration

The bit duration for IC cards with asynchronous transmission is defined as the elementary time unit (etu). During the execution of the Answer-to-Reset the initial etu (ietu) is used which is defined as follows:

initial etu = 372/f sec

where f is the frequency between 1 and 5 MHz.

The use of the frequency 3,5712 MHz results in a baud rate of 9,6 Kbps for the communication between IC card and CardTerminal.

For the communication after the Answer-to-Reset the work etu (wetu) is used. This is defined as

work etu = F/Df sec

where F is the clock rate conversion factor und D is the bit rate adjustment factor. When using the default values (F = 372, D = 1) then wetu = ietu.

The value of the work etu is dependent on the capabilities of the CardTerminal, the existence and coding of

- interface character TA1 (see 5.2.3),

- interface character TA2 (see 5.2.7)

and on the support of the protocol type selection procedure (see 5.3).

Tab. 1 shows the combinations conforming to ISO/IEC 7816-3 and those to be supported.

	TA1 absent	**TA1 present**
TA2 absent (negotiable mode)	wetu = ietu (to be supported)	wetu = ietu, if no PTS procedure is performed (to be supported) ---------- wetu = F/Df after succesful PTS (not applicable, because PTS is not supported)
TA2 present (specific mode)	wetu = ietu (to be supported)	wetu = F/Df immediately after ATR (support for F = 372 und D=1; if other values are given, new reset (warm reset); if identical ATR, abort)

Tab. 1: TA1/TA2 combinations

5.1.5 Character frame

A character consists of 10 bits:

- 1 start bit
- 8 data bits (= data byte)
- 1 parity bit with even parity.

The bits of the data byte are designated b1 to b8, where b1 is the least significant bit 'lsb' and b8 the most significant bit 'msb'. Whether lsb or msb is transmitted first is indicated in the initial character TS (first byte of the ATR).

Fig. 2 shows the transmission conventions with the level H (=High) and L (=Low). They apply not only for the Answer-to-Reset, but also for the total communication. Prior to transmission of a character, I/O shall be set to H. The start bit is recognized by polling at intervals of max. 0.2 etu.

Fig. 2: Character frame

5.1.6 Contact activation and reset

When an IC card is inserted all contacts shall be on level L (Vcc ≤ 0.4V, V_{OL} 0 - 0.3V). When the MCT has recognized the insertion of an IC card and all contacts are physically connected, the contacts shall be activated as follows:

- first Vcc is powered
- RST remains in state L during activation
- the I/O driver of the MCT ist set to reception mode after Vcc is stable (after max 400 ns), at the latest, however, after 200 clock cycles after the start of the clock.

Fig. 3 shows the activation of the contacts.

Fig. 3: Activation of the contacts

40.000 cycles after start of the clock the RST contact is put to level H. The IC card starts the ATR not before 400, at the latest, however, after 40.000 clock cycles starting at T1 (see Fig. 4).

Fig. 4: Reset

5.2 Answer-to-Reset

5.2.1 ATR Concept

The ATR is used to transmit information specifying certain properties of the communication between IC card and CardTerminal. It is assumed that in an IC card with asynchronous transmission normally only one transmission protocol is present (either T=0 or T=1).

5.2.1 TS - Initial character

The ATR coming from IC cards with asynchronous transmission starts with the initial character TS. It has either the value '3F', when inverse convention is applied, or '3B', when direct convention is applied.

When direct convention is used, state H (see 5.1.5) represents the bit value 1 and the lsb is transmitted first (usual convention). When inverse convention is used, state represents the bit value 1 and the msb is transmitted first (the inverse convention applies only to the data bits and the parity bit, not to start and stop bits).

Thus TS allows bit synchronisation between the CardTerminal and the ICC *and* indicates the logical convention for the interpretation of the following characters.

Support of the direct convention (´3B´) is mandatory, support of the inverse convention (´3F´) is optional.

5.2.2 T0 - Format character

The most significant nibble (bits b8-b5)´ of T0 indicates, whether the following characters TA1 to TD1 are present (see fig. 5).

Fig. 5: Indication of presence of interface characters in T0 (i=0) and TDi-character (i=1, 2, ...)

The 'least significant nibble (bits b4-b1)´ of T0 indicates the number of the historical characters (0 - 15).

5.2.3 TA1 - Interface character for frequency and bit duration

The interface character TA1, if present, contains the codings for FI and DI (integer values for frequency F and bit rate adjustment factor D, see ISO/IEC 7816-3).

In the transmission phase after the answer to reset the following formula applies

work etu = F/Df sec

where F is the ´clock rate conversion factor´ and D is the ´bit rate adjustment factor´. The values of D and F, coded in DI and FI, are indicated acc. to ISO/IEC 7816-3 in the interface character TA1 of the ATR.

The default values F=372 and D=1 shall be supported. f other values are indicated, they shall, however, be handled acc. to the guidelines in Tab.1.
When the default values are used, TA1 shall not be transmitted.

5.2.4 TB1 - Interface character for programming voltage and current

TB1 indicates the values of P (programming voltage) in the least significant 5 bits (bits b5-b1) and the maximum value of the programming current I in the bits b7 and b6 (default values acc. to ISO/IEC 7816-3: P=5, I=50; bit b8 is not used and shall be set to 0). As no programming voltage is supported, the IC cards should return the value for TB1 '00' (= I max = 25 mA, Vpp not connected).
If the value for TB1 is different from '00', it is not evaluated.

5.2.5 TC1 - Interface character for extra guard time

TC1 codes the extra guard time N (unit: etu), which shall be added to the minimum duration between the edges of the start bits of two consecutive characters. The default value of N is 0 and should be supported by the IC cards. TC1 should therefore not be transmitted in the ATR.

5.2.6 TD1 - Interface character for subsequent characters indication and protocol type

The most significant nibble (bits b8-b5) of TD1 indicates whether the following charcters TA2 to TD2 are present (layout see Fig. 5)

The least significant nibble (bits b4-b1) indicates the protocol type, which shall be used for the communication between MCT and ICC.

ICCs with transmission protocol T=0 shall not return TD1 (in the absence of TD1 acc. to ISO/IEC 7816-3 the transmission protocol T=0 shall be used; as TA2 to TD2 are not used for T=0, the transmission of TD1 for T=0 is redundant and therefore not significant).

For ICCs with transmission protocol T=1 TD1 shall be present with b1 set to 1. If more information for T=1 is needed (this is usually the case) then the presence of TD2 shall be indicated. A usual coding of TD1 for T=1 is therefore '81'.

5.2.7 TA2 - Interface character for specific mode of operation

When TA2 is *not* transmitted in the ATR, the ICC indicates, that it is in the negotiable mode. When TA2 is transmitted, the ICC indicates herewith the specific mode of operation.

5.2.8 TC2 - Interface character for T=0 work waiting time

TC2 indicates the maximum interval between the beginning of a character, sent by the ICC, and the previous character, which was sent either from the CardTerminal or the IC card. The work waiting time results from 960 x D x WI, where TC2 contains the value for WI. The default values of D and WI are used, i.e. the maximum interval is 9600 etus. TC2 should, therefore, not be transmitted in the ATR.

5.2.9 TD2 - Interface character for subsequent protocol parameters of T=1

The most significant nibble (bits b8-b5) of TD2 indicates whether the following characters TA3 to TD3 are present (layout see fig. 5)
As TA2 and TB3 normally are transmitted, the usual value of this nibble is 3.

The least significant nibble (bits b4-b1) indicates again the protocol type. TD2 therefore has the value '31'.

5.2.10 TA3 - Interface character for T=1 information field size card

TA3 contains the maximum length of the information field of a T=1 block, that can be received by the IC card (IFSC, see ISO/IEC 7816-3, 9.5.1.1) and shall always be returned by the IC card, as there are hardly any IC cards restricted to an IFSC of 32 byte, the default value. The value of TA3 shall be within the range from 32 to 254 ('20' - 'FE').

5.2.11 TB3 - Interface character for T=1 character and block waiting time

The character waiting time 'CWT´ defines the maximum time between the edges of the start bits of two consecutive characters (see ISO/IEC 7816-3, 9.5.2.1). The least significant nibble (bits b4-b1) of TB3 indicates the value CWI, which is used for the calculation of CWT. The value of CWI may range from 0 to 15 acc. to ISO/IEC 7816-3.

The block waiting time 'BWT´ defines the maximum time between the edges of the start bits of the last character of a received block and the first character of a block to be sent (see ISO/IEC 7816-3, 9.5.2.2). The most significant nibble (bits b8-b5) of TB3 contains the value BWI, which is used for the calculation of BWT. The value of BWI may range from 0 to 9 acc. to ISO/IEC 7816-3.

The default value is '4D'. To get the quickest possible transmission, the values for TB3 should be lower than the default value.

5.2.12 TC3 - Interface character for T=1 error detection code

TC3 is used for the indication of the type of the error detection code in the epilog field of a T=1 block. When b1 is set to 1, CRC is used. If bir 11 is 0 (default value), LRC is used. Only LRC, i.e. exclusive OR,shall be supported. If the IC card indicates CRC, communication shall be aborted.

5.2.13 T1 to TK - Historical bytes

The historical bytes (HB) for ICCs with asynchronous transmission contain no information relevant for the MCT. The number of historical bytes is indicated in T0.
The ISO conform use of the historical bytes is described in ISO/IEC 7816-4. The following figure shows the recommended coding of the historical bytes.

Fig. 6: Recommended coding of the historical bytes

Notes:
1. The card profile data object is a mandatory DO and denotes, which application selection method(s) are supported by the IC card and which command shall be used to read a DIR file and/or an ATR file, if available. If only direct application selection method is supported, the coding '80' shall be used, i.e. the right nibble is not evaluated and shall therefore be set to '0'.
2. Dependent on the features of the card, the DO 'card capabilities' may also be necessary.

5.2.14 TCK - Check Character

The check character TCK allows checking of the ATR for transmission errors. The value is calculated by exclusive OR-ing from T0 to TCK inclusive to ensure the result is zero.
ICCs with transmission protocol T=0 shall not send TCK. When T=1 is used, TCK shall be sent.

5.2.15 Recommended ATR coding for T=0 und T=1

Fig. 7 shows the recommended ATR coding for ICCs with T=0 or T=1 transmission protocol.

Fig. 7: Recommended ATR coding for ICCs with asynchronous transmission

5.3 Protocol type selection PTS

The function PTS is not supported.

6. Transmission protocols

6.1 Character transmission protocol T=0

6.1.1 Send and receive

The command message, which is transmitted from the MCT to the ICC, contains the command header incl. length byte (CLA, INS, P1, P2, L). L indicates either the length of the data which follow in the command data field or the length of the data which are expected in the response data field. After sending the 5 header bytes the MCT waits for a procedure byte.

Also after receiving a command message with data, the IC card sends a procedure byte to the CardTerminal to inform it about how the communication will continue.
The procedure bytes and their meaning are described in tab. 2.

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 and their meaning

6.1.2 Error handling

If a character has been received incorrectly or with the wrong parity, the receiver shall set I/O to Low after 10.5 ± 0.2 etus from the beginning of the start bit for a time of minimum 1 and maximum 2 etus. Therefore the sender shall check I/O after 11 ± 0.2 etus. When I/O is set to High, transmission can be continued, otherwise an error situation has occurred and the character concerned has to be sent again.

6.2 Block transmission protocol T=1

A transmission block of T=1 consists of

- the prolog field (mandatory)
- the information field (conditional)
- the epilog field (mandatory).

Fig. 8 shows the general structure.

Fig. 8: T=1 Block

6.2.1 NAD - Node address byte

The node address byte shall be set to '00' by the CardTerminal.

Note: The use of the NAD byte is reserved for a later version.

6.2.2 PCB - Protocol control byte

The PCB byte identifies the type of T=1-block:

- Information block (I-block)
- Receive ready block (R-block)
- Supervisory block (S-block).

The following 3 tables show the codings of the T=1 blocks.

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: Coding of the I-block

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: Coding of the R-block

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: Coding of the S-block

6.2.3 LEN - Length byte

The coding of the length byte contains the length of the information field of a block. LEN may principally have values from 0 to 254 (255 is RFU), the real upper limit in a communication between MCT and ICC results however from the ATR byte TA3, which contains the value for IFSC. IFSD has the value 254 and is therefore always greater than or equal to IFSC.

6.2.4 INF - Information field

The information data field of the I blocks contains application data and that of the S-blocks - if INF present - control information. There is no information field in R-blocks.

6.2.5 EDC - Error detection code

Only the LRC (longitudinal redundancy check) shall be used for error detection code (LRC is the EDC default value). The value of the LRC results from using the 'exclusive OR' of the NAD byte up to and inclusive of the last byte of the INF field if present.

6.2.6 Block numbering

MCT and ICC have their own block numbering on the basis of modulo-2 counters.

The value of the sequence numbers after the start of the communication or after a resynchronisation is zero.

6.2.7 Setting of IFSC

An IC card shall indicate the IFSC value in the ATR (see interface character TA3). An S-block for setting the IFSC shall therefore not be sent. If a CardTerminal nevertheless receives such an S-block, this block shall not be answered.

6.2.8 Setting of IFSD

The default value for IFSD (buffer size in the CardTerminal for blocks sent by the IC card) is 32 bytes. An MCT, however, has to be equipped with a buffer of 258 byte (IFSD = 254 bytes, 3 byte T=1 prolog field and 1 byte T=1 EDC field).

To inform the IC card about the buffer size in the CardTerminal, the CardTerminal shall send the S-block 'IFS request' with the value 'FE' to the IC card. This must be done before sending the first ICC command, thus directly after the Answer-to-Reset. The IC card shall answer the 'IFS request' with an 'IFS response'.

6.2.9 Errorfree communication

In errorfree communication without chaining only I-blocks are transmitted. The M bit is set to 0, the send sequence counter alternatively to 0 or 1.

The MCT has the right to send the first I-block after the Answer-to-Reset.

Fig. 9: Exchange of I-blocks

If chaining is used, flow control is necessary, i.e. a block with M bit =1 shall be acknowledged with an R-block, to indicate to the partner that the block was received correctly and that further blocks can be received. The send sequence number of the R-block therefore is the number of the next expected I-block.

Fig.10: Exchange of I-blocks with chaining

6.2.10 Error handling

a) Communication errors

A communication error occurs, when the parity of one or more bytes is incorrect and/or the EDC is wrong. In this case an R-block is sent with b4-b1='1' and the send sequence number of that block that will be retransmitted.

Fig. 11: Repetition of blocks after a communication error

b) Synchronisation error

When the MCT recognizes a BWT- or CWT-time out, the MCT shall send an R-block with b4-b1='2'. To avoid collisions the MCT shall check in advance whether the I/O is inactive. When it is active, the IC card shall be deactivated and SW1,SW2 = ´6F00´ shall be returned to the application.

c) Protocol error

When the IC card receives a block with non-permissible coding, it shall return an R-block with b4-b1 = '2' and abort the communication.

When the CardTerminal receives a block not conforming to the protocol, the IC card shall be deactivated and SW1,SW2 = ´6F00´ shall be returned to the application.

d) Abort request

When the CardTerminal receives an abort request, this shall be indicated to the application by SW1, SW2 = ´6F00´ and the IC card shall be deactivated. The CardTerminal itself shall not send an abort request to the IC card.

7. IC card interface for ICCs with synchronous transmission

7.1 Physical communication

7.1.1 Physical characteristics

The ICC's with synchronous transmission which the MCT shall support are contact orientated IC cards with 5V-technology as described in ISO/IEC 7816-3 (WD 1137). The physical characteristics shall comply with ISO 7816-1.

7.1.2 Position and usage of the contacts

For the position and usage of the contacts the same conventions apply as for the IC cards with asynchronous transmission.

7.1.3 Frequency

The frequency for ICCs with synchronous transmission lies between 7 and 50 KHz. It is recommended to work with the highest possible frequency to achieve a high baud rate and thus a reduction of the transmission time.

7.1.4 Bit transmission

The logical 0 of a bit corresponds with the state Low and the logical 1 with the state High (see ISO/IEC 7816-3, section 6.22) The least significant bit lsb of a byte is transmitted first (direct convention), if not otherwise specified by the chip manufacturer.

7.1.5 Reset

After insertion of an IC card, the MCT assumes a card with asynchronous transmission and applies a clock frequency between 1 and 5 MHz. If no response is given, an IC card with synchronous transmission shall be assumed. The contacts are then deactivated and afterwards activated again with the clock frequency between 7 and 50 KHz. The ATR is then read after the reset with the first 32 cycles. When IC cards do not react to this reset, an I^2C-bus chip without reset shall be assumed. In this case the ATR must be read via a read command.

7.2 ATR

Acc. to ISO/IEC 7816-3 the ATR for IC cards with synchronous transmission consists of

- Byte H1: Protocol type
- Byte H2: Protocol parameter
- Bytes H3, H4: Historical bytes.

The exact structure of the ATR is described in ´IC cards with synchronous transmission, Part 1: ATR and data sections.´

7.3 Transmission protocols

IC cards with the following protocols shall be supported:

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

Details of the transmission protocol 2WBP are be specified in: 'IC Cards with synchronous transmission, Part 2: Transmission protocols' and in the manufacturer's documentation. The specifications of SDAP and 3WBP can be required from manufacturers producing chips with these protocols.