Interoperability Specification for ICCs and Personal Computer Systems

Part 2. Interface Requirements for Compatible IC Cards and Readers

Bull CP8, a Bull Company

Gemplus SA

Hewlett-Packard Company

IBM Corporation

Microsoft Corporation

Schlumberger SA

Siemens Nixdorf Informationssystemes AG

Sun Microsystems, Inc.

Toshiba Corporation

VeriFone,Inc.

Revision 1.0

December 1997

INTELLECTUAL PROPERTY DISCLAIMER

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER INCLUDING ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION, OR SAMPLE.
NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED OR INTENDED HEREBY.
BULL CP8, GEMPLUS, HEWLETT-PACKARD, IBM, MICROSOFT, SCHLUMBERGER, SIEMENS NIXDORF, SUN MICROSYSTEMS, TOSHIBA AND VERIFONE DISCLAIM ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF PROPRIETARY RIGHTS, RELATING TO IMPLEMENTATION OF INFORMATION IN THIS SPECIFICATION. BULL CP8, GEMPLUS, HEWLETT-PACKARD, IBM, MICROSOFT, SCHLUMBERGER, SIEMENS NIXDORF, SUN MICROSYSTEMS, TOSHIBA AND VERIFONE DO NOT WARRANT OR REPRESENT THAT SUCH IMPLEMENTATION(S) WILL NOT INFRINGE SUCH RIGHTS.

Contents

1 Scope

This Part of the *Interoperability Specification for ICCs and Personal Computer Systems* discusses requirements for physical, electrical, and low-level data communications protocol compatibility between compliant ICC and IFD devices. This material corresponds to that covered in ISO/IEC 7816 Parts 1, 2, and 3. This document is not however, nor is it intended to be, a comprehensive review and discussion of ISO/IEC 7816 requirements. Rather, it identifies specific options and operating parameters that are required to insure interoperability between devices compliant with this specification.

These requirements are intended to create a system that is compatible with a broad range of potential ICC applications suitable for integration with the PC. As such, requirements in industry specific standards such as EMV and GSM were considered in creating this specification.

A future version will contain additional requirements supporting the dynamic retrieval of card specific software (ICC Service Provider) for cards that have not yet been registered locally.

2 Physical Interface Requirements

IFDs and ICCs compliant with this specification must meet ISO/IEC 7816 physical/mechanical interface requirements for such devices. This section describes specific options which compliant devices shall support.

2.1 Dimensions and Location of Contacts

The dimensions and locations of each of the contacts shall comply with Figure 2 of ISO/IEC 7816-2, with the contacts located on the front of the card. The ICC may optionally include a magnetic stripe and/or embossing as depicted in Figure 2-1. Embossing will be compliant with ISO/IEC 7811-1.

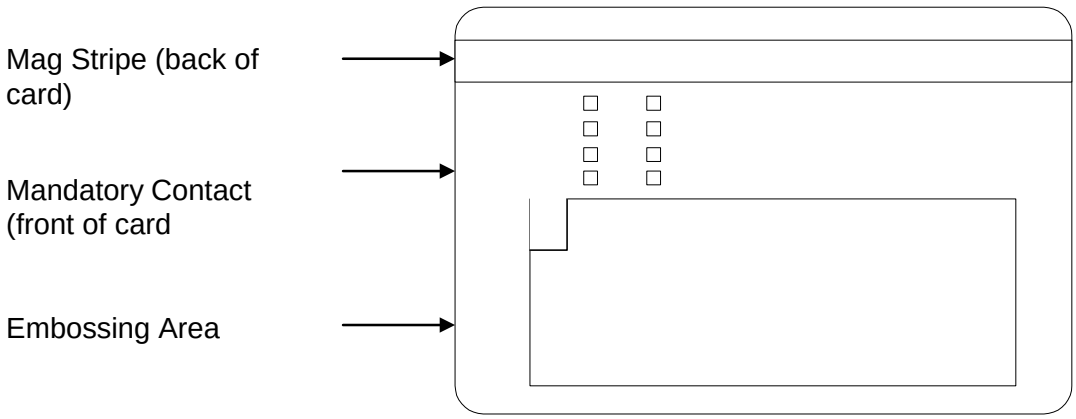


Figure 2-1. Compatible Card Layout

2.2 Contact Assignments

The contacts located on the ICC shall comply with ISO/IEC 7816-2&10. The contact identification and functional assignment is as follows:

Table 2-1. ICC Contacts

Contact ID	Assignment	Contact ID	Assignment
C1	Supply Voltage (V_{CC})	C5	Ground (GND)
C2	Reset (RST)	C6	Reserved (V_{PP})
C3	Clock (CLK)	C7	Input/Output (I/O)
C4	Function code (FCB)	C8	RFU

C6 is identified by ISO/IEC 7816 as Programming Voltage and C4 as Function Code (FCB) for synchronous card type 2, while C8 is Reserved for Future Use (RFU).

ICCs requiring an external programming voltage are not compliant with these standards. Hence, C6 need not be physically present. If present, it shall be electrically isolated from the integrated circuit and other contacts on the ICC. C4 is optional for synchronous cards type 2 and need not be physically present, if the reader does not support synchronous cards. If C4 is present and the reader does not support synchronous cards, it shall be electrically isolated from the integrated circuit and other contacts on the ICC. C8 is Reserved for Future Use (RFU) and need not be physically present. If present, they shall be isolated from the integrated circuit and other contacts on the ICC.

A compatible IFD need only implement contact arms for defined ICC contact pads. Implementation of contact arms for C4, C6, and C8 is optional at this time. If any of the optional contact arms are present and not used in the context of these standards, they will be electrically isolated from the other contact arms and IFD electronics. The force exerted by the contact arms on the ICC contact pad shall not exceed 0.6 N.

2.3 ICC Card Insertion and Removal

These standards are compatible with IFDs with either manual or automated insertion/removal mechanisms. It is recommended that IFDs position the ICC such that it is always accessible to the card owner. If the IFD draws the ICC inside however, there must be a mechanism provided to return the ICC to the card owner in the event of failure, such as power loss.

A goal of these standards is to insure development of cost-effective and highly reliable IFDs. As such, simple manual insertion/removal mechanisms are recommended. For reliability, a “landing card” or “landing contact” IFD socket design is recommended, because “wiping contact” designs are far more likely to damage ICC contacts and/or mar graphics imprinted on the ICC.

IFDs must be designed to insure that any location guides, clamps, rollers, and so on will not damage the ICC, particularly in the areas reserved for optional magnetic stripe and embossing areas.

2.4 Tamper Resistant/Evident Devices

These specifications do not require tamper resistant or tamper evident design. However, many applications for which ICCs are being employed have security and privacy requirements associated with them. As such, it is strongly recommended that ICCs contain state-of-the-art tamper resistant features to prevent unauthorized access to, or modification of data stored therein.

Compliant IFDs are expected to be used primarily in conjunction with PCs. In this environment, tamper resistant designs are not believed to be cost effective. However, for IFDs that implement Authentication and/or Security Assurance enhancements as described in Part 3, Section 3.2.3, it is desirable that the user be able to determine whether the device is operating in accordance with the manufacturers specifications. In these cases, some form of tamper evident seals is recommended.

3 Electrical Interface Requirements

IFDs compliant with this specification must meet ISO/IEC 7816 electrical interface requirements for ICC terminal devices and the specific options discussed in the subsequent sections.

All electrical measurements are made at the point of contact between the ICC contact pad and the IFD contact arm. Measurements are defined with respect to the ground contact (C5) over an ambient temperature range of 0° to 50° C. All currents flowing out of the IFD defined as positive.

3.1 I/O Connection

3.1.1 Half-Duplex Serial I/O

Contact C7 supports a half-duplex, serial data link between the ICC and IFD. Both devices must support the ability to selectively set their I/O line driver to transmission or reception mode. Unless transmitting, the I/O line driver shall be set to reception mode.

During operation, both devices should never be in transmit mode at the same time. Should this occur, the state of the I/O contact will be indeterminate and no damage should occur to either device. When both the IFD and ICC are in reception mode, the contact shall be in the high state. The IFD shall incorporate a pull-up resistor to insure that this is the case. The IFD shall not pull I/O high unless V_{CC} is powered and stable within tolerances given in Section 3.4. The IFD shall limit the current flowing into or out of the I/O contact to ±5mA at all times.

3.1.1.1 IFD Operating Requirements

When in transmission mode, the IFD shall send data to the ICC within the following electrical parameters.

Table 3-1. IFD Transmission Mode Parameters

Symbol	Conditions	Minimum	Maximum
V_{OH}	$-20\mu A < I_{OH} < 20\mu A$, V_{CC} = min	$0.8 \times V_{CC}$	V_{CC}
V_{OL}	$-1mA < I_{OL} < 0mA$, V_{CC} = min	0 V	0.3 V
t_r and t_f[1]	C_{IN} = 30 pF max	--	0.8 µs
Undershoot and Overshoot	--	–0.25 V	V_{CC} + 0.25 V

When in reception mode, the IFD shall correctly interpret signals from the ICC within the following electrical parameters.

Table 3-2. IFD Reception Mode Parameters

Symbol	Minimum	Maximum
V_{IH}	$0.6 \times V_{CC}$	V_{CC}
V_{IL}	0 V	0.5 V
t_r and t_f	--	1.2 µs

[1] t_r = rise time between 10% and 90% of signal amplitude; t_f = fall time between 90% and 10% of signal amplitude.

When in transmission mode, the ICC shall send data to the IFD within the following electrical parameters.

Table 3-3. ICC Transmission Mode Parameters

Symbol	Conditions	Minimum	Maximum
V_{OH}	$-20\mu A < I_{OH} < 20\mu A$, V_{CC} = min	$0.7 \times V_{CC}$	V_{CC}
V_{OL}	$0 < I_{OL} < 1mA$, V_{CC} = min	0 V	0.4 V
t_r and t_f	C_{IN} = 30 pF max	--	1.0 µs

When in reception mode, the ICC shall correctly interpret signals from the IFD within the following electrical parameters.

Table 3-4. ICC Reception Mode Parameters

Symbol	Minimum	Maximum
V_{IH}	$0.7 \times V_{CC}$	V_{CC}
V_{IL}	0 V	0.8 V
t_r and t_f	--	1.0 µs
Overshoot and Undershoot	–0.3 V	V_{CC} + 0.3 V

3.2 Clock

The IFD shall generate a CLK signal (C3) having the following characteristics.

Table 3-5. IFD CLK Parameters

Symbol	Conditions	Minimum	Maximum
V_{OH}	$0 < I_{OH} < 50\mu A$, V_{CC} = min	V_{CC} – 0.5V	V_{CC}
V_{OL}	-50 mA $< I_{OL} < 0$, V_{CC} = min	0 V	0.4 V
t_r and t_f	C_{IN} = 30 pF max	--	8% of clock period
Overshoot and Undershoot	--	–0.25 V	V_{CC} + 0.25 V

Duty cycle shall be between 45% and 55% of the clock period during stable operation. Frequency shall be a minimum of 1 MHz with a default frequency in the range of 1 to 5 MHz. The IFD may support a maximum clock frequency(s) greater than 5 MHz. The maximum clock frequency that may be used with a given ICC shall be encoded in the ATR string as described in Section 4.4. Use of a CLK frequency above the default shall only be initiated by the IFD. The CLK shall return to the default value any time the ICC activation sequence or ICC reset is initiated (see Section 4). During stable operation, the clock frequency shall not vary by more than 1%.

The ICC shall operate correctly with a CLK signal having the following characteristics.

Table 3-6. ICC CLK Parameters

Symbol	Conditions	Minimum	Maximum
V_{IH}	--	V_{CC} – 0.7V	V_{CC}
V_{IL}	--	0 V	0.5 V
t_r and t_f	V_{CC} in valid range	--	9% of clock period
Overshoot and Undershoot	--	–0.3 V	V_{CC} + 0.3 V

3.3 Reset

The IFD shall generate an RST signal (C2) having the following characteristics.

Table 3-7. IFD RST Parameters

Symbol	Conditions	Minimum	Maximum
V_{OH}	$0 < I_{OH} < 50\mu A$, V_{CC} = min	V_{CC} – 0.5V	V_{CC}
V_{OL}	$-50\ \mu A < I_{OL} < 0$, V_{CC} = min	0 V	0.4 V
t_r and t_f	C_{IN} = 30 pF max	--	0.8 µs
Overshoot and Undershoot		–0.25 V	V_{CC} + 0.25 V

The ICC shall correctly interpret an RST signal with the following characteristics.

Table 3-8. ICC RST Parameters

Symbol	Conditions	Minimum	Maximum
V_{IH}		V_{CC} - 0.7V	V_{CC}
V_{IL}		0 V	0.6 V
t_r and t_f		--	1.08 µs
Overshoot and Undershoot		-0.3 V	V_{CC} + 0.3 V

Compliant ICCs shall respond to an RST signal using asynchronous active low reset (see Section 4.2).

3.4 Supply Voltage

The IFD shall generate the supply voltage V_{CC} (C1) and will be capable of delivering a steady state output current of at least 55 mA while maintaining V_{CC} ± 8% VDC within designated limits at any supported CLK frequency. The IFD shall contain protection circuitry to prevent damage occurring to it in the event of short circuits. The power supply must be designed to avoid transients and surges, as measured at the ICC, from occurring due to normal operation of the IFD and associated equipment.

The ICC shall be designed to operate correctly with a supply voltage of V_{CC} ± 10% VDC and have a maximum current requirement of 100 mA when operating at any supported CLK frequency.

3.4.1 Operating Voltage Negotiation

At the present time, most ICCs are designed to operate with a nominal supply voltage of 5 VDC. As 3-V and lower devices are now entering the marketplace, IFDs must have a method of determining the presence of such devices. This is discussed in Part 4, Section 2.5.3 of this specification. When the ISO 7816 committee has finalized these methods, this section will be updated to reflect them.

3.5 Contact Resistance

The contact resistance as measured across a clean IFD contact arm and a clean ICC contact pad shall be less than 500 mΩ throughout the design lifetime of the devices. See ISO/IEC 10373 for the appropriate test method.

3.6 Programming Voltage

Compliant IFDs will not generate a Programming Voltage and compliant ICCs shall not require a Programming Voltage (C6).

3.7 Resilience

Resilience, that is short circuits, current and voltage variations, loading, clocking, and so on, shall be as described in the ISO 7816 specifications.

4 ICC Session Management

This section describes the interactions that are expected to occur between a compliant ICC and IFD from the time the ICC is inserted into the IFD until it is removed from the IFD.

4.1 Card Insertion and Activation

The electrical interface between the IFD and the ICC shall not be activated until the IFD contact arms and ICC contact pads are properly aligned and connected. Deactivated is defined as all IFD contact signals in the L state and $V_{CC} < 0.4V$.

The IFD shall be designed to insure that it can detect the ICC after it is seated within ±0.5 mm of the nominally correct position as defined in ISO/IEC 7816-2. Because ICC damage can occur from “hot contact” insertion, care must be taken in the design of the “card present” detection system.

The contact activation sequence shall be as follows:

- RST set to state L.

- V_{CC} powered.
- I/O set to reception mode. This can be done before or after CLK is applied, but must be done within 200 cycles of the CLK application.
- CLK in stable operation.

4.2 ICC Reset

Following ICC activation, the IFD shall initiate a cold reset and obtain an ATR sequence from the ICC. The ATR sequence is defined in Section 4.4. ICCs compliant with this specification shall answer to reset asynchronously using active low reset. The cold reset sequence is depicted in Figure 4-1.

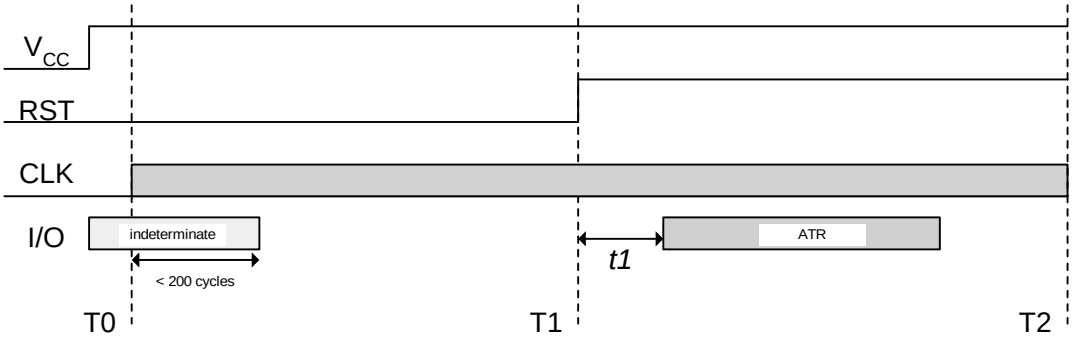


Figure 4-1. Cold Reset Sequence

The time between T0 and T1 must be a minimum of 40,000 clock cycles during which RST must be held in the L state. After RST is set to the H state, the ATR sequence should start with time *t1*, between 400 and 40,000 CLK cycles. If the ATR doesn't start within 40,000 cycles (T2), then the IFD shall assume the ICC is not responding.

The IFD may also initiate a warm reset at anytime during an active ICC session. The warm reset sequence is depicted in Figure 4-2 where the timing requirements are the same as for the cold reset sequence.

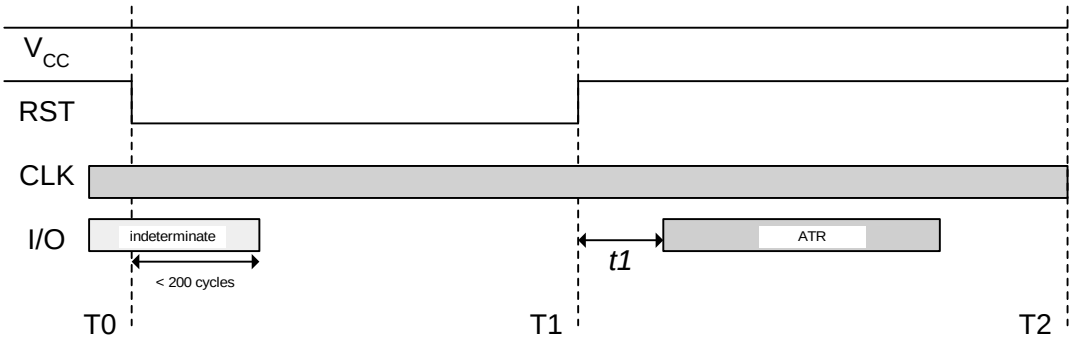


Figure 4-2. Warm Reset Sequence

4.3 Character Transport

Data is exchanged between the IFD and the ICC as a sequence of bits, blocked into characters, over an asynchronous half-duplex I/O channel. The data rate employed is dependent upon the CLK frequency (*f*) and global parameters F (clock rate conversion factor) and D (bit rate adjustment factor). How these are determined is specified in Section 4.4.

The bit duration on the I/O line is defined as an elementary time unit (etu), which has a linear relationship with *f*. It is defined by:

$$\text{Current } \mathbf{etu} = \frac{\mathbf{F}}{\mathbf{D}\,f} \quad \text{seconds}$$

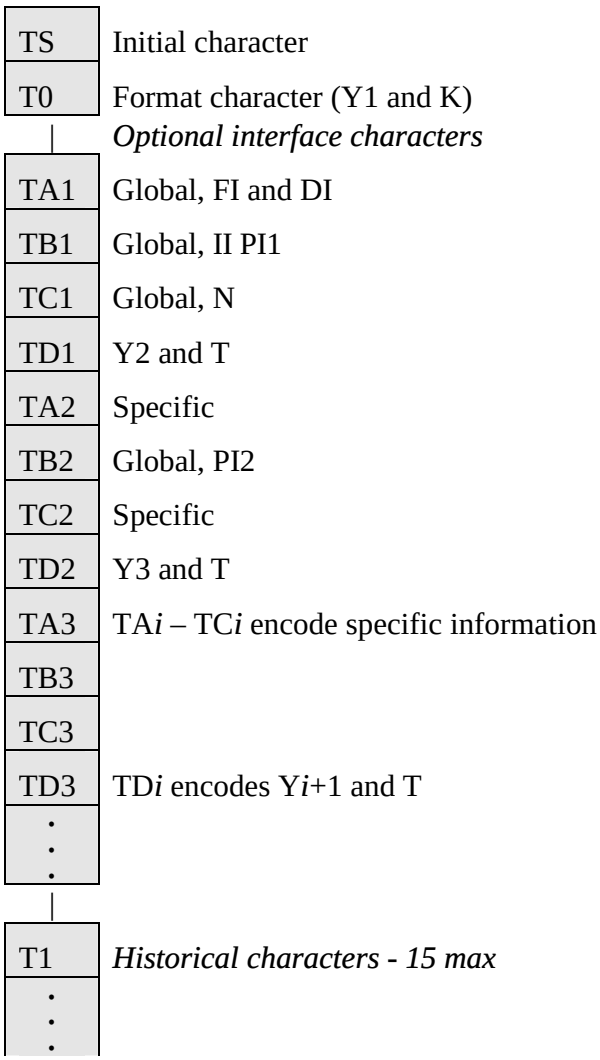
During the ATR sequence, because neither F nor D has been defined, they assume the default values of F=372 and D=1. Hence the etu during ATR processing is always 372/*f*. The value of *f* must be between 1 MHz and 5 MHz during this period.

The bits passed over the I/O line are framed into characters with each character consisting of 10 bits. Prior to transmission of a character, the I/O line is always in the H state. A character consists of the following bits:

- One start bit in state L
- Eight data bits, which comprise a data byte
- One even parity check bit (the number of 1 bits in the data byte and parity bit must be even)

4.4 Answer to Reset Sequence

The ATR byte sequence returned by the ICC depends on the transmission protocol(s), control parameter, and identifying information supported. The ATR sequence must adhere to the following format defined in ISO/IEC 7816-3.



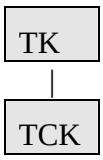


Figure 4-3. ATR Sequence

The total length of the ATR sequence, excluding the initial character TS, is limited to 32 bytes. TS and T0 are the only mandatory bytes in the ATR sequence.

The ATR byte values are defined in the subsequent sections. In each case, the values that ICCs compliant with these specifications may use are indicated. If an ICC returns a non-compliant ATR sequence, the IFD should not reject the ICC. Operation should be continued using the default protocol and parameters. This is necessary to allow an ATR to be initially programmed or reinitialized in the event of an error (see note 1, below). If an ICC does not return an ATR, it means that the ICC is inserted incorrectly (or is nonfunctional), or that the ICC is an unsupported type (a synchronous ICC). A "nonfunctional card" message is sent to the ICC Resource Manager. The ICC Resource Manager can determine how to handle this state: if the system handles only asynchronous ICC's, the card is inserted incorrectly, or is inoperable; if the system handles synchronous ICC's, the user can be given the option of selecting a method to try to read the ICC.

Note 1: Optionally, the IFD may issue a warm reset in an attempt to obtain a valid ATR sequence (assuming the initial ATR was somehow corrupted). The IFD shall not perform more than one automatic warm reset during the initialization sequence in an attempt to retrieve a valid ATR. Note that this operation may take 0.5 to 2.0 seconds, which may be annoying to a user.

4.4.1 TS: Initial Character

TS provides a bit synchronization sequence and defines conventions for encoding data bytes in all subsequent characters. TS defines one of two possible encoding conventions:

> **Direct Convention**. A high state (H) on the I/O line is interpreted as a logic one, and the least significant bit is transmitted first. This is indicated by the value '3B' or (H)LHHLHHHLLH.
>
> **Inverse Convention**. A low state (H) on the I/O line is interpreted as a logic one, and the most significant bit is transmitted first. This is indicated by the value '3F' or (H)LHHLLLLLLH.

IFDs are required to support both Direct and Inverse conventions.

4.4.2 T0: Format Character

T0 is interpreted as two 4-bit nibbles. The upper nibble (bits 5 through 8) is designated Y1. This indicates the presence of optional characters based on a logic one in the following bit positions:

- Bit 5 indicates TA1 is present.
- Bit 6 indicates TB1 is present.
- Bit 7 indicates TC1 is present.
- Bit 8 indicated TD1 is present.

The lower nibble (bits 1 through 4) is designated K and is interpreted as a numeric value in the range zero through 15. It indicates the number of Historical characters present.

4.4.3 TAi, TBi, TCi, TDi: Interface Characters

These characters, if present, are used to determine data communications parameters and protocols. The presence of these characters when i =1 is determined by Y1 (encoded in T0). Their presence when i >1 is determined by the value of Yi, which is encoded in TDi–1. They are interpreted as follows:

TA1. Encodes FI in the upper nibble (bits 5 through 8) and DI in the lower nibble (bits 1 through 4). These are used to determine the clock conversion factor (F) and bit rate adjustment factor (D), and maximum supported clock rate according the tables below.

FI	0000	0001	0010	0011	0100	0101	0110	0111
F	Internal Clock	372	558	744	1116	1488	1860	RFU
f max (MHz)	---	5	6	8	12	16	20	---

FI	1000	1001	1010	1011	1100	1101	1110	1111
F	RFU	512	768	1024	1536	2048	RFU	RFU
f max (MHz)	---	5	7.5	10	15	20	---	---

DI	0000	0001	0010	0011	0100	0101	0110	0111
D	RFU	1	2	4	8	16	32	RFU

DI	1000	1001	1010	1011	1100	1101	1110	1111
D	12	20	1/2	1/4	1/8	1/16	1/32	1/64

TB1, TB2. These are used to encode information concerning the programming voltage and programming current factor. ICCs requiring external programming voltage are not compliant with this specification. It is recommended that compliant ICCs set TB1 = '00' to indicate V_{PP} is not required, and not transmit TB2. If an ICC returns a nonzero value of TB1 or TB2 the IFD should not reject the ICC and should continue as though values of '00' were returned.

TC1. Interpreted as an 8-bit unsigned integer, which represents N, the extra guard time required between characters. The IFD is required to wait 12+N etus between the leading edge of the start bit of a character and the leading edge of the start bit of the subsequent character. If N=255, then the minimum delay time is set to 11 etus.

In the absence of the above characters, the implicitly defined values are:

F = 372; D = 1; I = 50; P = 5; N = 0

TD1. This encodes Y2 in the high nibble as indicated previously. The low nibble encodes the protocol type, T, which is interpreted as an unsigned

integer in the range zero through 15. If TD1 is not present, then T=0 is used implicitly. If TD1 is present, then the protocol indicated is the default protocol. If T=0 is one of the supported protocols, then it must be specified as the protocol type in TD1.

The only protocol types compliant with this specification are:

- T=0. Asynchronous half-duplex character-oriented protocol.
- T=1. Asynchronous half-duplex block-oriented protocol.
- Synchronous.

IFDs may reject ICCs that explicitly specify any other default protocol type.

TA2. If absent indicates that the ICC is in the negotiable mode of operation. It is recommended that ICCs compliant with this specification not return TA2. If TA2 is present, it indicates a specific mode of card operation. Information is encoded as follows:

- Bit 8. If zero, ICC can change mode of operation. If one, ICC is unable to change.
- Bits 6 and 7. RFU.
- Bit 5. If zero, parameters are defined by interface characters. If one, parameters are implicitly defined.
- Bits 1 through 4. Protocol type, T.

TC2. This is specific to T=0 and defines the work waiting time integer (WI), which defines the maximum interval between the leading edge of the start bit of any character sent by the ICC and the leading edge of the start bit of the previous character sent by either the ICC or the IFD. $W = 960 \times D \times WI$. It is recommended that compliant ICCs not return TC2 and use the default WI=10.

TD*i* where *i*>1. Indicates whether subsequent interface characters are present and the protocol type using the encoding defined for TD1.

TA*i* where *i*>2. This is used only for T=1 and encodes the value of the Information Field Size for the Card (IFSC). This is the largest amount of information that the ICC can accept in a single block. The default value is 32, with legal values being in the range 1 through 254.

TB*i* where *i*>2. This is used only for T=1 and encodes the value of the character waiting time integer (CWI) in the low order nibble and the block waiting time integer (BWI) in the high order nibble. The character waiting time (CWT) is the maximum time between the leading edges of two consecutive characters in the same block. The default value of CWI is 13. The block waiting time (BWT) is defined as the maximum time between the leading edges of the last character that gave the right to send to the card and the first character sent by the card. The default value for BWI is 4 and should not be larger than 9.

TC*i* where *i*>2. Bit 0 indicates use of CRC error detection if set to one and LRC error detection if set to zero. All other bits should be set to zero.

4.4.4 T1 to TK: Historical Characters

If K (encoded in T0) is not null, then the ATR sequence will include K “historical characters.” The definition of these characters is provided in ISO/IEC 7816-4: 1995 (E), Section 8, and is required for compliant devices. It is recommended that compliant ICCs

encode an ICC Identification Number in these characters as described in Part 8, Section 6, ATR Requirements.

4.4.5 TCK: Check Character

TCK is a checksum character computed such that performing a bit-wise XOR operation on all bytes in the ATR from T0 through TCK is null. In the event that only the T=0 protocol is indicated by the ATR sequence, TCK shall not be sent.

4.5 Protocol Negotiation

IFDs compliant with this specification are required to support implicit protocol type selection as defined in ISO/IEC 7816-3. To make an implicit protocol selection, they merely continue to use the default protocol and timing parameters.

An IFD may optionally support the ability to explicitly select from among the ICC offered protocols and parameters using the Protocol Type Selection (PTS) procedure defined in ISO/IEC 7816. The PTS request and response consist of a byte sequence as shown below.

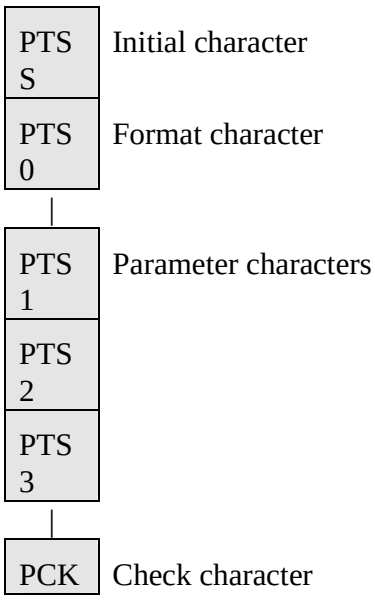


Figure 4-5. PTS Sequence

PTSS. Identifies the PTS request/response and is coded as 0xFF.

PTS0. Bits 5, 6, and 7 indicate the presence of the parameter bytes PTS1 through PTS3, respectively. The low-order nibble encodes the protocol type in the same manner as the TD*i* bytes (see Section 4.4.3).

PTS1. Encodes F1 and D1 in the same manner as TA1 (see Section 4.4.3). These values should lie in the range between the default values and those

indicated in TA1. If PTS1 is not sent, then the default values are assumed. In the response, the ICC echoes PTS1 to acknowledge these values or does not send PTS1 to indicate defaults should be used.

PTS2 and PTS3. RFU.

PCK. Checksum generated such that performing a bit-wise XOR operation on all bytes from PTSS through PCK is null.

Negotiation is successful if the response echoes the request or the response selectively does not echo PTS1, PTS2, or PTS3 and zeros the associated indicator bit in PTS0. All other responses indicate failure. The new protocol and/or parameters shall be used following a successful PTS exchange.

4.6 Power Management

See Part 4, Section 2.5.3.

4.7 Deactivation Sequence

At the end of a session, or upon abnormal session termination (unresponsive ICC or detection of ICC removal), the ICC contacts shall be deactivated in the following sequence:

- RST set to state L
- CLK set to state L
- I/O set to L
- V_{CC} set to inactive (< 0.4 VDC)

4.8 Data Communications Protocol Support

4.8.1 Protocol Support

IFDs compliant with this specification must be compatible with all ISO/IEC 7816-3 data communications protocol specifications: T=0 and T=1. All supported protocols are assumed to use the same physical layer and character framing rules as defined in Section 4.3.

The following section discusses the data link and transport layers in terms of specific requirements for compliant devices. In particular, it describes the level of protocol support and error handling expected of compliant IFDs and the protocol support implemented at the Service Provider layer.

4.8.2 Data Representation

All data exchanged using the T=0 or T=1 protocols is assumed to represent 8-bit, binary quantities.

4.9 Data Link Level

This sections describes specific options related to implementation of T=0 or T=1 protocols.

4.9.1 T=0 Character Protocol

4.9.1.1 Character and Bit Timing

Bit and character timing shall be consistent with ISO/IEC 7816 and shall reflect valid timing options for compliant ICCs and IFDs as specified in Section 4.3 and 4.4.

4.9.1.2 Command-Response Processing

Commands are always initiated from the IFD to the ICC. These commands are generated by an appropriate Service Provider within the PC, generally as the result of a request from an application program running in the PC.

IFDs compliant with this specification are expected to process Command Transport Data Units (C-TPDU), consisting of command information and associated data, as a single entity. The IFD initiates a command by sending a 5 byte command header to the ICC containing the following bytes.

CLA	1-byte command class.
INS	1-byte instruction code.
P1	1-byte parameter #1, which is instruction dependent.
P2	1-byte parameter #2, which is instruction dependent.
P3	1- byte indicating the length of data that will be sent to the ICC, or the length of data expected in response from the ICC. This is instruction dependent.

If the command has associated data, it is transferred subsequently based on the response from the ICC.

Following receipt of the command header, the ICC responds with a procedure byte. This is defined as shown in the following table.

Table 4-1. ICC Response Codes

Definition	Value	IFD Action
ACK	INS	All remaining data bytes are transferred to the ICC, or the IFD shall be ready to receive all remaining data bytes from the ICC.
	___ INS	The next data byte shall be transferred to the ICC, or the IFD shall be ready to receive the next data byte from the ICC.
NULL	0x60	The IFD shall provide additional work waiting time, and wait for another procedure byte from the ICC.
'SW1'	0x6x or 0x9x	The IFD shall wait for receipt of a second status byte 'SW2'

The IFD is not expected to interpret an SW1 byte when received. To insure the broadest possible compatibility, IFDs are not to implement support for SW1 responses as defined in ISO/IEC 7816-4. This is the responsibility of the associated Service Provider.

If a command has associated data, the IFD will send it (or the next byte in the sequence) following receipt of an ACK procedure byte as defined above. After the data has all been transferred to the ICC, the ICC shall respond with an another procedure byte.

Note that if an ACK procedure byte is received when no data is remaining to be sent to the ICC, then implicitly, the IFD assumes the ICC will be sending data to the IFD.

4.9.1.3 Error Handling

T=0 defines procedures for handling byte parity errors during transmission. Support for these procedures is mandatory and shall be implemented by the IFD and ICC.

If a character is received incorrectly, or correctly but with a parity error, the receiver shall indicate an error by setting the I/O line to state L at time 10.5 ± 0.2 etus following the leading edge of the start bit of the character for a minimum of 1 etu and a maximum of 2 etus.

The transmitter shall test the I/O line at 11 ± 0.2 etus after the leading edge of the start bit of a character was sent and assumes that the character was correctly received if the I/O line is in state H. If the I/O line is in state L, the transmitter shall wait at least 2 etus and then repeat the character for a maximum of three retries.

4.9.2 T=1 Block Protocol

4.9.2.1 Block Frames

Bit and character timing shall be consistent with ISO/IEC 7816 and shall reflect valid timing options for compliant ICCs and IFDs as specified in Sections 4.3 and 4.4. Parity will be checked at the character level.

Each block frame is structured as follows, where the Prologue and Epilogue fields are mandatory and the Information field is optional.

Table 4-2. T=1 Frame Structure

Prologue Field			**Information Field**	**Epilogue Field**
Node Address (NAD)	**Protocol Control Byte (PCB)**	**Length (LEN)**	**APDU or Control Information (INF)**	**Error Detection Code (EDC) See Note 1**
1 byte	1 byte	1 byte	0 to 254 bytes	1 or 2 bytes

Note 1 The EDC can be either a 1-byte LRC or a 2-byte CRC. LRC is the default, and is most common.

The NAD field may be used to define a logical channel between the IFD and ICC. It is encoded as follows:

- Bits 1, 2, and 3 are the Source Node Address (SAD).
- Bit 4 is zero.
- Bits 5, 6, and 7 are the Destination Node Address (DAD).
- Bit 8 is zero.

If node addressing is used, the first block from the IFD to the ICC will establish the initial logical channel. If node addressing is not used, then SAD and DAD should always be zero. The IFD will be capable of operating in either mode. If node addressing is used, the SAD and DAD may not be set to the same value.

The PCB defines the type of block being sent and must be one of the following:

- Information block (I-block) used to transmit an APDU:
  - Bits 1 through 5 are RFU.
  - Bit 6 indicates chaining.
  - Bit 7 is sequence number.
  - Bit 8 is zero.
- Receive-ready block (R-block) used to indicated acknowledgment:
  - Bit 8 is one.
  - Bits 6 and 7 are zero.
  - Bit 5 is sequence number.
  - Bits 1 through 4 indicate errors: 0= no errors; 1=EDC and/or parity error; 2=other error.

In the above, the sequence number is a modulo-2 value coded on one bit. The sequence number is maintained independently by the ICC and IFD. The value starts with zero for the first I-block sent after the ATR and is incremented by 1 after each I-block. The sequence number is reset to zero following a resynchronization. For an R-block, the sequence number used is that of the next expected I-block during chaining operations and of the last received block when requesting a block repetition.

- Supervisory block (S-block) used to exchange control information:
  - Bits 7 and 8 are 1.
  - Bit 6 indicates response if 1, else request.
  - Bits 1 through 5 indicate type of information: 0 = resynchronization request; 1= information field size request; 2=abort request; 3=extension of BWT request; 4=V_{PP} error (not used).

When the INF is present, it can be no larger than the negotiated Information Field Size (IFS). When the IFD is sending to the ICC, the IFS Card (or IFSC) is initially established by TA3 in the ATR sequence. The IFSC size can be renegotiated by the ICC sending an S(IFS request) block to the IFD. When the ICC is sending to the IFD, the IFS Device (IFSD) is initially set to 32. The IFSD can be renegotiated by the IFD sending an S(IFS request) block to the IFD. To insure maximum throughput, it is recommended that both ICCs and IFDs compliant with this specification support an IFS of 254 bytes.

It is possible to transmit data that exceeds the IFS. This is done via chaining as described in ISO/IEC 7816-3 and is accomplished by sending a series of I-blocks with bit 6 in the PCB set to one, indicating that a subsequent block follows. This bit is set to zero in the PCB of the last I-block in the chain. The receiver must acknowledge or reject each block in the chain using an R-block. It is the responsibility of the IFD and ICC to implement chaining; It is the IFD's responsibility to format and transmit the data received from the Service Provider based on the current IFS setting.

Finally the Epilogue contains the error detection code associated with the block. This can be either a CRC or LRC as negotiated during the ATR sequence. The IFD shall compute the Epilogue.

4.9.2.2 Rules for Error Free Operation

Devices compatible with this specification should observe the following rules:

1. After ATR is complete, the first block transmitted shall be sent by the IFD and may be either an S-block or an I-block.

2. Whenever transmission of a block is complete, the sender shall switch to the receiving state and await a block from the other devices. After a receiver has read a complete block, per the LEN field, it has the right to send.

3. If node addressing is being used, the node value will be included in the first block sent by the IFD. These values will be used for all subsequent exchanges related to this logical session between the Service Provider and the ICC.

4. If the IFD wishes to change the IFSD from the initial value of 32, it will send an S(IFS request) block. It is recommend this be set to 254 and that this be the first block sent by the IFD to the ICC. The IFD may perform this action independently, but should wait until a Service Provider has initiated a logical session so that the node addressing mode may be properly set.

5. The receiver must acknowledge all I-blocks by sending an appropriate I-block or R-block. R-blocks are used when chaining is in effect.

6. S-blocks are always exchanged in pairs, with an S(request) followed by an S(response).

4.9.2.3 Error Detection

IFDs compliant with this specification shall detect the following errors:

- Transmission error (incorrect parity or an EDC error) or a BWT time-out
- Loss of synchronization (wrong number of characters received)
- Protocol error
- Abort request for a chain of blocks

IFDs are responsible for attempting to recover through retransmission of a block or deactivation of the ICC contacts. In the latter case, the IFD will inform the Service Provider that an unrecoverable error has occurred.

ICCs are responsible for attempting to recover from errors through retransmission of a block or becoming unresponsive.

4.9.2.4 Protocol Error Handling Rules

The following rules shall apply when attempting error recovery based on block retransmission:

1. If the first block received by the ICC after ATR is invalid it shall return an R-block with bit 5 = 0.

2. If there is no response from the ICC to a block sent by the IFD within BWT, the IFD Subsystem shall follow the scenario 33 or 35 defined in the ISO 7816-3 Annex A document, in order to try to recover the communication. If it fails, the IFD Subsystem shall deactivate the ICC and inform the ICC Service Provider that an unrecoverable error has occurred.

3. If an invalid block is received in response to an R-block, the sender shall retransmit the R-block.

4. If an S(response) is not received in response to an S(request), the sender shall retransmit the S(request).

5. If an invalid block is received in response to an S(response) block, the sender shall transmit an R-block with bit 5 = sequence number of the next expected I-block.

6. If the IFD has sent a block a maximum of three times in succession, or the ICC has sent a block a maximum of twice in succession, without obtaining a valid response, the IFD may either attempt recovery through an S(Resynch request) or deactivate the ICC and inform the Service Provider that an unrecoverable error has occurred.

7. If a receiver detects an underrun or overrun condition, it will wait the greater of CWT or BWT before transmitting.

8. An S(Resynch request) may be initiated only by the IFD. If successful, this will resynch the ICC and IFD and reset communication parameters to the initial values. If a valid S(Resynch response) is not received after three attempts, then the IFD will deactivate the ICC.

9. When the ICC sends an S(IFS request) and receives an invalid response, it will retransmit the block only 1 time to elicit an S(IFS response) and then remain in receive mode.

10. The abortion of an I-block chain may be initiated by either the sender or receiver sending an S(Abort request).

4.10 Transport Level

This specification is compatible with ISO/IEC 7186 rules for mapping APDUs onto the T=0 or T=1 data link layer protocols. It is the responsibility of the ICC and associated Service Provider to perform this mapping. They are also responsible for defining the meaning of all 0x6x and 0x9x response codes and insuring that appropriate processing is performed.