Interoperability Specification for ICCs and Personal Computer Systems

Part 2. Interface Requirements for Compatible IC Cards and Readers

Apple Computer, Inc.

Axalto

Gemplus SA

Infineon Technologies AG

Ingenico SA

Microsoft Corporation

Philips Semiconductors

Toshiba Corporation

Revision 2.01.01

September 2005

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.
AXALTO, BULL CP8, GEMPLUS, HEWLETT-PACKARD, IBM, MICROSOFT, 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. AXALTO, BULL CP8, GEMPLUS, HEWLETT-PACKARD, IBM, MICROSOFT, SIEMENS NIXDORF, SUN MICROSYSTEMS, TOSHIBA AND VERIFONE DO NOT WARRANT OR REPRESENT THAT SUCH IMPLEMENTATION(S) WILL NOT INFRINGE SUCH RIGHTS.

Revision History

Revision	Issue Date	Comments
2.00.9	May 10, 2004	Spec 2.0 Final Draft
2.00.10	June 22, 2005	Minor edits to 3.1.1 and 3.2
2.01.00	June 23, 2005	Final Release
2.01.01	September 29, 2005	Changed Schlumberger to Axalto

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.

For ICCs with contacts, this material corresponds to that covered in ISO/IEC 7816 Parts 1, 2. For asynchronous transmission protocol cards, the relevant requirements are given in ISO/IEC 7816, part 3. ISO/IEC 7816 part 10 defines requirements for synchronous transmission protocol cards.

For contactless ICCs, the requirements recognized by this specification are given in the ISO/IEC 14443 or ISO/IEC 15693 documents.

ISO/IEC 14443 compatible cards and IFDs are respectively called PICC (Proximity Integrated Circuit(s) Card) and PCD (Proximity Coupling Device). ISO/IEC 15693 compatible cards and IFDs are called VICC (Vicinity Integrated Circuits(s) Card) and VCD (Vicinity Coupling Device). In the current revision of the spec the terms card and reader or IFD respectively are usedThis document is not however, nor is it intended to be, a comprehensive review and discussion of ISO/IEC 7816, nor ISO/IEC 14443 / 15693, requirements. Rather, it identifies specific options and operating parameters that are required to ensure 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, additional requirements in industry specific standards such as EMV and GSM may need to be considered by vendors.

2 Physical Interface Requirements

2.1 ISO/IEC 7816 Compatible Card and IFD

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.

2.1.1 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. IFDs should be compatible with ICCs embossed according to ISO/IEC 7811-1.Contact Assignments.

The contacts located on the ICC shall comply with ISO/IEC 7816-2. Additional provisions for synchronous cards are also given in ISO/IEC 7816-10. 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 ISO/IEC 7816-10 synchronous card type 2, while C8 is Reserved for Future Use (RFU).

2.1.1.1 ICC Requirements

An ICC must support the physical contacts required by its protocol. If a contact is not used, it shall be electrically isolated from the integrated circuit and other contacts on the ICC

To ensure interoperability with IFDs compatible with this specification, ICCs must not require an external programming voltage, hence contact C6 must not be used.

2.1.1.2 IFD Requirements

A compatible IFD need only implement contact arms for defined ICC contact pads. The following table indicates which contact must be provided, according to the protocols supported.

Table 2-2. IFD Supported Contacts According to Protocol Support

Protocol	Contacts Supported
ISO/IEC 7816-3	C1, C2, C3, C5 and C7
ISO/IEC 7816-3 plus ISO/IEC 7816-10	C1, C2, C3, C4, C5 and C7

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.

2.1.2 ICC Card Insertion and Removal

IFDs may support either a manual or an automated insertion/removal mechanism. 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 the PC/SC specification is to ensure 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 ensure 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.

2.1.3 Tamper Resistant/Evident Devices

The PC/SC specification does 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, the user should 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.

2.2 Contactless Card and IFD Systems

The IFD uses inductive coupling to provide power to the card by the RF field, which is modulated for communication. No mechanical contact is required between them. A reader and a card operate typically within a range of 0 to 10cm.

The physical characteristics of a PICC must comply with ISO/IEC 14443-1, those of a VICC to ISO/IEC 15693-1

2.2.1 Card Insertion and Removal

PCDs Contactless readers do not, by definition, implement a mechanical card insertion and removal detection scheme. However, it is required that readers, at the data link layer, have some functionality for detecting cards entering and leaving the energizing field. This issue is discussed further in section 4.2.1.3.

3 Electrical Interface Requirements

Each IFD and ICC compliant with this specification must meet its respective ISO/IEC standard electrical interface requirements. They must also support the specific options discussed in the subsequent sections.

3.1 ISO/IEC 7816-3 Compatible Card and IFD

3.1.1 Operating Voltage Conditions

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.

ISO/IEC 7816-3 defines two classes of operating conditions that specify mainly the nominal supply voltage:

- 5 V under class A
- 3 V under class B
- 1.8 V under class C

ISO/IEC 7816-3 categorizes devices by their supported operating conditions in the following fashion:

- Class A devices operate only under 5 V nominal supply voltage
- Class B devices operate only under 3 V nominal supply voltage
- Class C devices operate only under 1.8 V nominal supply voltage
- Class AB devices can operate in both class A and class B environments.
- Class ABC devices can operate in class A, class B and class C environments.

For the sake of interoperability, IFDs and ICCs compliant with this specification must belong to one of the following classes:

- IFD: class A or class AB or class ABC
- ICC: class A or class AB or class ABC

ISO/IEC 7816-3, section 4.2.2 specifies how IFDs must negotiate the appropriate operating voltage.

3.1.2 Programming Voltage

Compliant ICCs shall not require a Programming Voltage and, accordingly, compliant IFDs must not generate a Programming Voltage.

3.2 ISO/IEC 7816-10 Compatible Card and IFD

A compliant IFD must support ISO 7816-3 cards, as described in this part. In addition, it can optionally support synchronous cards, as defined in ISO/IEC 7816-10. The latter defines two types of synchronous protocols, type 1 and type 2. An IFD that supports synchronous cards must support type-1 and may optionally support type-2 and use C4 (FCB). In the case C4 and C8 are used within an IFD, their function shall refer to ISO

7816-12 (Part 12: Cards with contacts: USB electrical interface and operating procedures). The relevant electrical interface requirements are defined in ISO/IEC 7816-10.

3.3 Contactless Card and IFD Systems

The IFD provides power to the card via an inductive coupling RF field. Data transfer is performed by modulation of this RF field.

4 ICC Session Management

This section describes specific provisions regarding the interactions that are expected to occur between a compliant ICC and IFD.

In the context of this section, a session is defined as:

- *For contact cards*, the period covering the insertion of the ICC into the IFD to its removal from the IFD.
- *For contactless cards*, the period covering the entry of the PICC/VICC into the PCD/VCD's energizing field to its removal from the energizing field.

4.1 ISO/IEC 7816-3 Compatible Card and IFD

4.1.1 ICC Answer To Reset Requirements

The ATR sequence returned by an ICC may contain "historical characters." Their framing into the ATR is defined in ISO/IEC 7816-3, while the definition of these characters is provided in ISO/IEC 7816-4: 1995 (E), Section 8. It is recommended that ICCs support the initial access data mechanism (ISO/IEC 7816-4, section 8.3.3) to enable application selection, as discussed in Part 5, Section 2.6 of this specification. As an alternative, the recommendations of Part 8, Section 6 can be used.

4.1.2 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.

A compliant IFD must support the ability to explicitly select from among the ICC offered protocols and parameters using the Protocol and Parameters Selection PPS[1] procedure defined in ISO/IEC 7816.

4.1.3 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.

Compliant ICCs have to support either the T=0 or T=1 protocols. They may also support both T=0 and T=1.

4.2 Contactless Card and IFD Systems

Contactless PICC/VICC session management is defined by the following items:

1. Initialization and anticollision (ISO/IEC 14443-3, ISO/IEC 15693).

[1] PPS was referred to as *PTS* in revision 1.0 of this specification. Due to these historical considerations, PTS and PPS are used interchangeably in the current revision.

2. Protocol entry, (Answer To Select with ISO/IEC 14443-4 PICCs, protocol entry with ISO/IEC 14443-3 PICCs / 15693 VICCs).

Specific provisions are further required in order to ensure optimal operation of PICC/VICCs and PCD/VCDs within the PC/SC framework. These are presented in the following sections.

4.2.1 PCD Requirements

4.2.1.1 ISO/IEC 14443 Type A , B PICC and ISO/IEC 15693 VICC Support

The IFD should support

- ISO/IEC 14443 both Type A and Type B PICC types and their associated protocols (ISO/IEC 14443 parts 2, 3 and 4), but not necessarily support simultaneous activation of cards of different types,

- ISO/IEC 15693 VICCs and their associated protocols (ISO/IEC 15693 parts 1 to 4).

Figure 2.1 shows one possibility of card polling as seen from the IFD perspective. In this particular example simultaneous activation of ISO/IEC 14443, ISO/IEC 15693is not supported. The IFD is switched from one mode to the next during insertion polling while no card is yet inserted:

- The type of the first card inserted determines the mode the IFD stays in during subsequent acquisition and operation.

- While cards are inserted the type of cards to operate is limited to the type of the first card detected.

- The IFD system is able to detect cards of other types after all cards have been removed and the necessity to stick to one mode goes away.

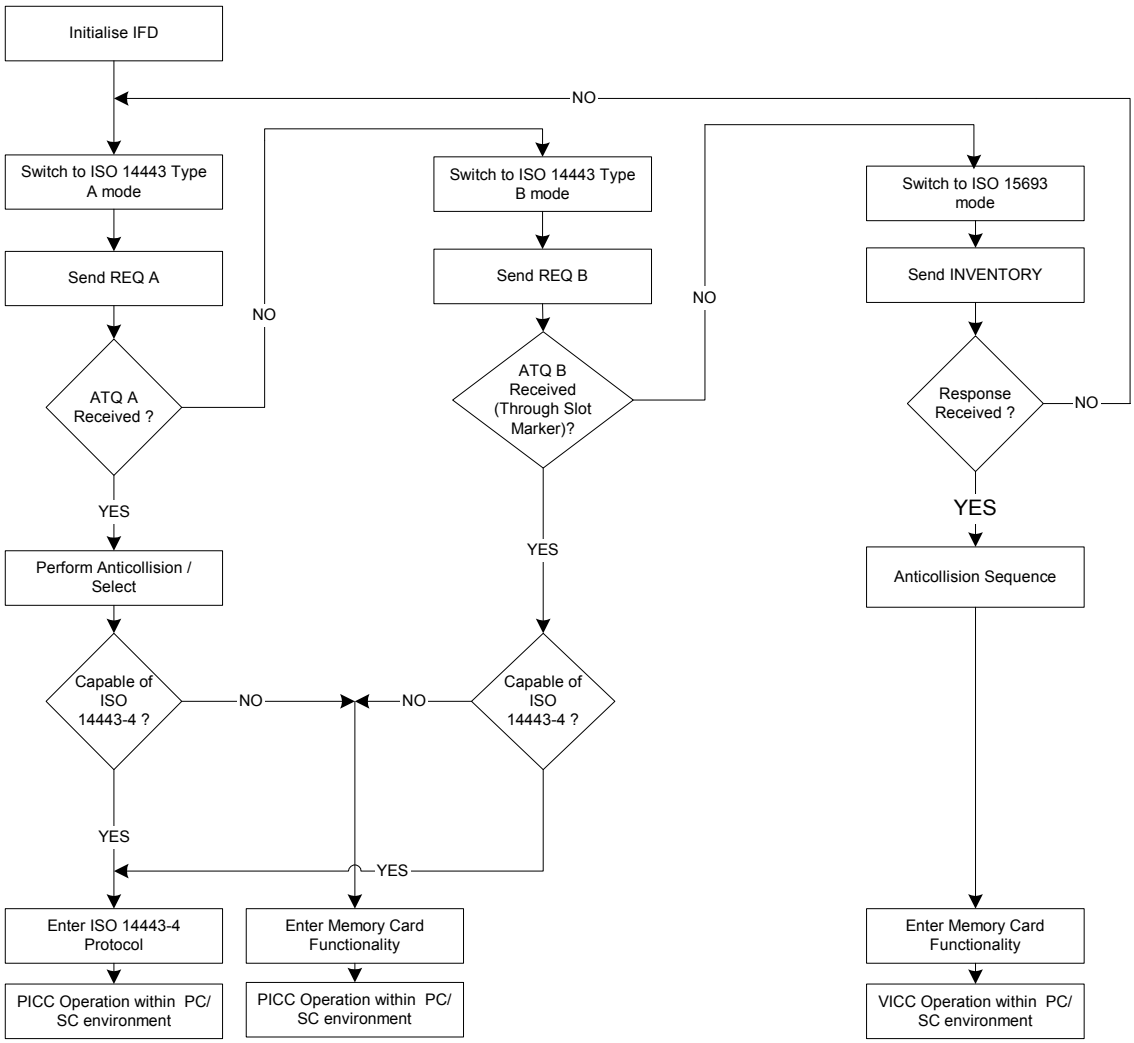

Figure 2-1. Example polling and activation sequence

4.2.1.2 Multi-Activation of Contactless ICCs

In order to implement a multi-slot IFD subsystem the reader must be able to handle several cards simultaneously. This is accomplished by:

- CID Addressing:
  CIDs are temporary card numbers, ranging from 0 to 14, that allow addressing simultaneously several active ISO/IEC 14443-4 PICCs within a single PCD coupling field. ISO/IEC 14443-4 describes CID addressing.

- Direct Addressing:
  VICCs compliant to ISO/IEC 15693 are, once their UID is known, directly addressable or selectable respectively.

- Exclusive Activation:
  By exclusively activating an ISO/IEC 14443-3 PICC for communication and immediately de-activating it after, the system shall handle those PICCs quasi-simultaneously.

This document does not specify the minimum number of cards that can be activated simultaneously by a PCD subsystem. Accordingly, compliant PCDs may exhibit either mono-slot or multi-slot functionality.

This implies that a multi-slot system must follow the rules for operating ISO/IEC 14443-3 and ISO/IEC 14443-4 PICCs simultaneously. It needn't operate ISO/IEC 15693 cards together with ISO/IEC 14443 PICCs since the signals are different.

4.2.1.3 Support for Card Insertion/Removal Detection

Part 3, section 3.1.3 of this specification mandates an ICC mechanism that enables notifications of card insertion and removals events. In a contactless environment, card insertion events correspond to PICC/VICCs being recognised by an IFD during insertion polling, performing periodic activation attempts. Card removal events map to a PICC/VICC being physically removed from the energizing field.

The current revisions of ISO/IEC 14443-3 and –4, ISO/IEC 15693 provide all necessary functionality at the PCD/VCD, PICC/VICC and protocol level to implement a PC/SC card insertion and removal notification mechanism.

Within contactless environments the IFD subsystem shall poll for card events:

- Insertion:
  A PICC/VICC being inserted into the RF field is detected by the IFD system by periodically sending commands to activate a card. When these commands succeed the PICC/VICCs properties are recorded and an insertion event is generated.

- Removal:
  A PICC/VICC being removed from the field shall be detected by the system. There are, depending on the type of PICC, different possibilities:

  - ISO/IEC 14443.3:
    These PICCs can be polled for presence by periodically attempting to reactivate and deactivate them again since they are in deactivated (halted) state in periods of no communication with them.

  - ISO/IEC 14443-4 PICCs : Usually they are in the protocol most of the time since they support CID addressing. A mechanism exists within ISO/IEC 14443-4 to poll for card presence. The PCD sends negative acknowledge frames to the PICC expecting either a positive acknowledge or the last I-block to be repeated (according to ISO/IEC 14443-4 scenario 6 and 8).

  - ISO/IEC 15693 cards can be polled for presence by periodically by selecting and sending them into Quiet state immediately after..

4.2.2 Card Requirements

4.2.2.1 Card Multi-Activation Support

To guarantee interoperability with no interference, the system must take into account the following rules:

1. Piccs supporting CID must be operated using CID addressing. NAD must not be used to distinguish between different PICCs.

2. Cards not capable of CID addressing must be halted immediately after detection in order not to interfere with other PICCs. Communication with such a card is done by exclusive re-activation, protocol operation and de-activation immediately after. This makes sure that field monopolization is avoided.

4.2.2.2 Initial Access Data

In order to leverage the application selection scheme introduced with revision 2.0 of this specification, an ICC should support a mechanism to get access to a Card Info Structure that identifies ICCOS and ADSPL service providers.

In a contact card environment, the ISO/IEC 7816-4 initial access data mechanism is proposed by this specification to fetch the Card Info Structure.

For the ATS, ISO/IEC 14443-4 references the ISO/IEC 7816 Historical Bytes specification.

4.2.2.3 Halt state requirements

Once it has completed its transactions with a card, an application may programmatically terminate a communication session with an ICC. The actual API call performed at the Resource Manager level to terminate such session is `SCARDCOMM::disconnect`, as described in Part 5, section 3.2.5.2. In the PC/SC application usage model, the ICC may then be allocated to a second application willing to perform some other transactions.

When disconnecting from a card, the application may want to reset the ICC security state it has established, so that subsequent (rogue) applications cannot leverage it. The `Disposition` parameter of the `SCARDCOMM::disconnect` method lets the application specify if it wants the ICC to be reset or not. In the contact card environment, a reset (either warm or cold) re-initializes the ICC's security.

In an ISO/IEC 14443-4 environment, a cold/warm reset maps naturally to a DESELECT of an active card, followed by its reactivation through WAKE-UP and an explicit SELECT. However, this sequence of operations must also guarantee that the PICC's security context gets reset for the pattern described above to remain valid. Otherwise, it would introduce a serious security hole.

ISO/IEC 14443-3 compatible cards are not affected by a cold/warm reset since they are in HALT state most of their time, only reactivated for communication.

ISO/IEC 15693 cards see no effect from the cold/warm reset since they are in Quiet mode most of their time, only selected and operated for communication.