

PC/SC Workgroup

White Paper

Presentation of the Interoperability specification for ICCs and Personal Computer Systems, Revision 2.0

Abstract

This document presents the upcoming revision 2.0 of the Interoperability specification for ICCs and Personal Computer Systems (PC/SC) as defined at the time of publication. The PC/SC specification is an evolutionary document. Changes to it, made periodically to it by the PC/SC Workgroup, may not always be reflected in this document.

The objective of revision 2.0 is to extend the specification to cover a broader range of smart card based products. It focuses on the support of four main technologies:

- **Dynamic Assignment of ICC Service Providers and enhanced Card Recognition** Defined to help list on-card applications and retrieve a reference to the appropriate ICC service provider implementation related to a chosen on-card application. This mechanism is ensured by the Application Domain Service Provider Locator (ADSPL), which gathers information from the card in order to redirect the ICC aware application to the appropriate service provider. Should the card not contain this information, the existing mechanism of revision 1.0 is still available.
- **IFDs with extended capabilities** Covered by an IFD Service Provider (IFDSP), which provides interfaces to manage new functionality, allowing IFD capabilities such as pin pad, display and multi-slot. The concept of application context is introduced to represent a list of IFD functions with security features required for ICC aware applications and ICC Service Provider (ICCSP).
- **Support of synchronous protocols for ICCs** Embedded in the actual scheme of PCSC. The impact on the specification is minimal and the functionality must be ensured by the IFD Subsystem.
- **Support of contactless ICCs** Also embedded in the actual scheme of PCSC. The impact on the specification is that new tags must be defined (in part 3), and functionality must be ensured by the IFD Subsystem.

© 1996, 1997, 1998, 1999, Bull CP8, Gemplus, Hewlett-Packard, IBM, Intel, Microsoft, Schlumberger, Siemens, Sun Microsystems, and Toshiba. All rights reserved.

INTELLECTUAL PROPERTY DISCLAIMER

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY AND 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, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED OR INTENDED HEREBY.

BULL CP8, GEMPLUS, HEWLETT-PACKARD, IBM, INTEL, MICROSOFT, SCHLUMBERGER, SIEMENS, SUN MICROSYSTEMS, AND TOSHIBA DISCLAIM ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF PROPRIETARY RIGHTS, RELATING TO IMPLEMENTATION OF INFORMATION IN THIS SPECIFICATION. BULL CP8, GEMPLUS, HEWLETT-PACKARD, IBM, INTEL, MICROSOFT, SCHLUMBERGER, SIEMENS, SUN MICROSYSTEMS AND TOSHIBA DO NOT WARRANT OR REPRESENT THAT SUCH IMPLEMENTATION(S) WILL NOT INFRINGE SUCH RIGHTS.

Product or company names mentioned herein may be the trademarks of their respective owners.

CONTENTS

INTRODUCTION.....	1
DYNAMIC ASSIGNMENT OF ICC SERVICE PROVIDERS AND ENHANCED CARD RECOGNITION.....	2
Motivation	2
Application Domain Service Provider (ADSP) – A new concept	2
ADSP Locator (ADSPL) – Application Plug & Play	2
Enhanced Card Recognition	3
How things work together	4
IFDs WITH EXTENDED CAPABILITIES.....	6
Motivation	6
Application context	6
The IFD service provider	7
SUPPORT OF SYNCHRONOUS PROTOCOLS FOR ICCS.....	11
Motivation	11
Handling synchronous protocols	11
SUPPORT OF CONTACTLESS ICCs.....	12
Motivation	12
Supported protocols	12
Characteristics of a contactless environment	12
Implementation directives	13
Card selection	13
Card event	13
Card Identification	13
Other impacts on the PC/SC specification	13
ADDITIONAL REFERENCES.....	14
Documents	14
PC/SC Workgroup Members	14
For More Information	15

INTRODUCTION

The objective of this document is to present the main changes proposed by the PC/SC Workgroup's revision 2.0 of the Interoperability specification for ICCs and Personal Computer Systems (PC/SC), namely:

- Dynamic card service provider support and enhanced Card Recognition.
- IFDs with extended capabilities.
- Support of synchronous protocols for ICCs.
- Support for contactless ICCs and readers.

Revision 2.0 also proposes several new service providers along with extended capabilities for the Resource Manager, as explained in this document.

The following new terms are introduced in this document:

- **Application Domain Service Provider (ADSP)** A service provider for a specific on-card application.
- **ADSP Locator (ADSPL)** A service provider that allows enumeration of on-card applications and assignment of an appropriate ADSP.
- **Card Info Structure** A data structure stored on the ICC. It contains the information required for the enhanced card recognition mechanism.
- **Card OS ID** An identifier associated with the card OS. It is a part of the Card Info Structure.
- **ICC-OS** The operating system of a card.
- **ICC-Type** The card type.
- **IFD Service Provider (IFDSP)** A service provider that manages IFD's extended capabilities.
- **Application Context** An identifier for a list of requirements associated with a set of functions and security features present in an IFD.
- **Functional Logical Device** A physical part, or a group of physical parts, of an IFD exposed as a logical device.

DYNAMIC ASSIGNMENT
OF ICC SERVICE
PROVIDERS AND
ENHANCED CARD
RECOGNITION

Motivation

In revision 1.0 of the PC/SC specification, ICCs were introduced to the system as an ICC type. An ICC type was defined by a specific combination of the ICC-OS and a set of applications.

This approach made it necessary to introduce any other combination of ICC-OS and on-card applications as a new ICC-Type to the system. It also prevented ICC-Issuers from maintaining on-card applications with the related off-card components independently from ICC vendors introducing the card type to the system.

Revision 2.0 of the architecture reflects the different roles of ICC vendors and ICC issuers. It supports this by linking the ICC type to an ICC-OS implementation only. The ICC issuer then maintains the linking of the on card applications and their specific off-card components (ICCSPs).

Benefits achieved by these enhancements are:

- Dynamic assignment of an appropriate service provider can be based on information given by the card (plug-and-play).
- Increased flexibility and independence of the off-card component when dealing with multi-application cards.

Application Domain Service Provider (ADSP) – A new concept

This revision of the PC/SC specification introduces a new type of ICC Service Provider, the Application Domain Service Provider (ADSP).

The difference from the previous ICCSP as defined in revision 1.0 is that the ADSP is a service provider that is intended to interface with an on-card application rather than an ICC-type or ICC-OS.

ADSPs support on-card applications in a more flexible way. Currently, ICCSPs can only be mapped to the ICC using the ATR through the Resource Manager. This is not viable in a multi-application card world.

The new mechanism of ADSP Locator, described in the following sections, makes it possible to have dynamic assignment of an ADSP. This will allow multiple ADSPs to be available to off-card applications for the same ICC.

There will be a one-to-one relationship between ICCs and their ICC-OS related service provider. This relationship is mapped when the system is prepared to interact with an ICC.

From then on, a modification to an on-card application only needs to be accompanied with an updated implementation of the corresponding ADSP.

ADSP Locator (ADSPL) – Application Plug & Play

In revision 1.0 of the PC/SC specification, the Resource Manager (RM) is responsible for the mapping between ICC-Type and ICCSP. This is statically defined in the RM's database.

In a multi-application card environment it is not possible to have static linking between card types and available on-card applications. For this reason, revision 2.0 introduces a new component, the Application Domain Service Provider Locator (ADSPL), an on-card application plug for off-card application play.

The ADSPL is a service provider (typically written by the ICC issuer) that is loaded by the Resource Manager.

The ADSPL allows the RM to provide off-card applications with:

- A way of listing on-card applications.
- A way of retrieving a reference to the appropriate ADSP implementation related to a chosen on-card application.

The provider of the ADSPL is responsible for specifying the way in which ADSPs should be introduced to the ADSPL. The design of the ADSPL could even be such that it can retrieve an appropriate ADSP automatically when it is needed.

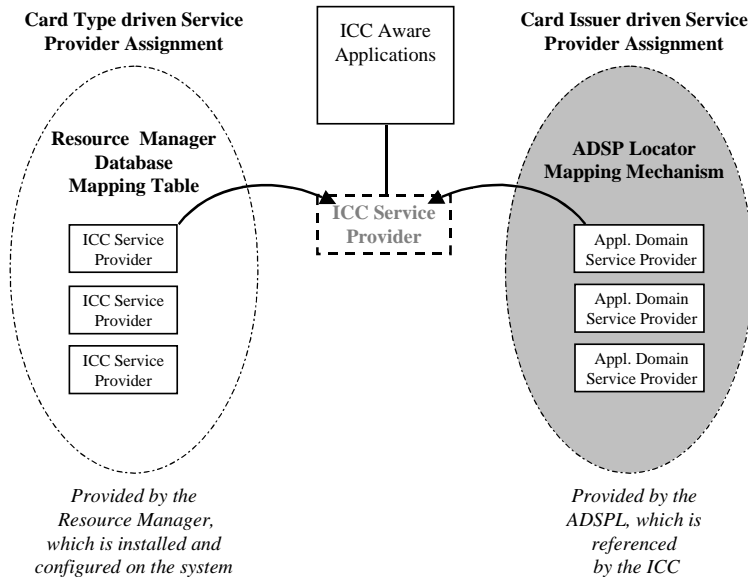


Figure 1 – Retrieving a card service provider

Enhanced Card Recognition

Today's ICCs are identified by the ATR String they present to the off-card system. Due to the restricted length and complexity of an ATR, the flexibility of this common card recognition method is limited. Card issuers, manufacturers and card application developers need to share the available ATR. This obstacle leads to severe restrictions when dealing with complex multi-application cards.

The revision 2.0 of PC/SC introduces an enhanced card recognition mechanism to retrieve the basic information for identifying an ICC (see Figure 1 – Retrieving a card service provider on page 3) .

All information regarding the identification of an ICC with this new mechanism must be available on the ICC itself. The identity information is stored in a Card Info structure (or “extended” ATR). The information can be placed, for example, in a file or applet – depending on the used ICC technology. The ICC has to include a command in the ATR’s historical bytes, which can be used by the off–card system (Resource Manager) to retrieve the Card Info Structure. Specifying a command within the historical bytes of an ICC is described in more detail in the ISO 7816–4 document (part 8.3.3).

When dealing with this type of enhanced ICC, the Resource Manager interprets the historical bytes of the ATR, sends the included command back to the ICC, and retrieves the Card Info Structure. The information from this structure is used by the Resource Manager to identify the ICC.

Revision 2.0 specifies a number of fields that can be used in the Card Info structure, including a reference to the ICC operating system and a reference to an ADSPL.

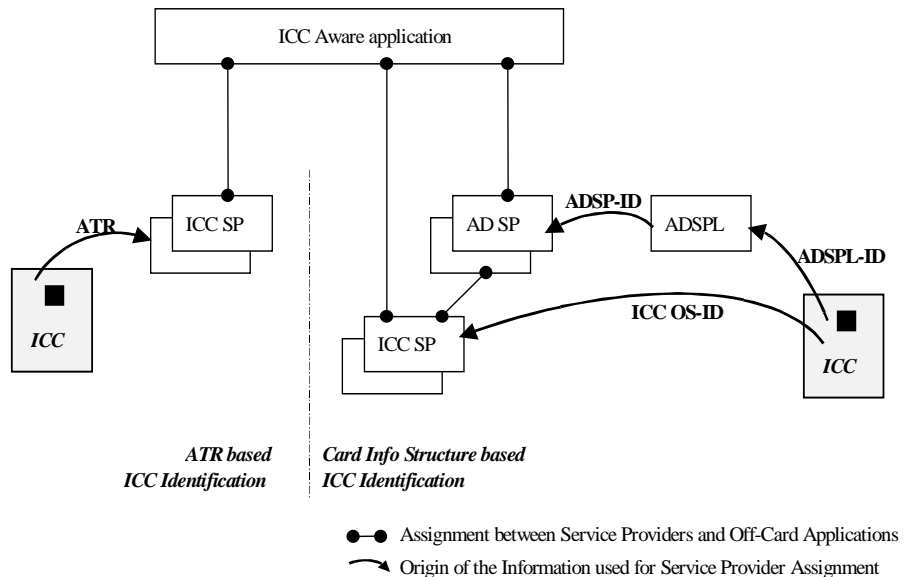


Figure 2 – Card recognition mechanism

How things work together

Cards supporting this new mechanism for dynamic assignment of ADSPs will have to support the enhanced Card Recognition mechanism (see Figure 2 – Card recognition mechanism).

When the ICC is inserted, the Resource Manager will retrieve the Card Info, get the ADSPL reference from the Card Info structure and load the ADSPL. When appropriate, the Resource Manager will retrieve the list of on-card applications from the ADSPL. It is now possible to choose which on-card application to interact with. The ADSPL returns the reference to the appropriate ADSP to the Resource Manager that returns it in turn to the off-card application.

It is important to note that ICCs supporting the enhanced Card Recognition mechanism do not need to be introduced to the Resource Manager as ICC-Types anymore. For these cards, only ICC-OS related service providers are introduced to the Resource Manager.

IFDs WITH EXTENDED CAPABILITIES

Motivation

In many cases, IFDs can have capabilities other than just APDU communication. Such capabilities may be related to security (e.g. secure PIN entry, biometric components, cryptography, etc.) or ergonomics (e.g. use of the display/keypad features of a device). To support these extended IFD capabilities, part 9 has been added to the PC/SC specification. Part 9 is principally an extension of the PC/SC architecture that allows some additional components to encapsulate these new IFD capabilities. It also pre-defines a set of services. This extension has been designed to provide interoperability between ICCSPs, or ICC aware applications that require a set of extended capabilities, and the IFDs that support them.

Application context

The “application context” is a new concept. It represents a list of IFD functions with related security features that an ICC aware application or ICCSP requires when using the device. An application context can be defined for a particular card application or for a set of card applications. It may be defined by the card or application issuer. For example, an application context could be defined by a payment or health care system.

For a health care system, an application context could contain the following requirements:

- Support of secure PIN functionality as defined in the pre-defined services.
- Interface for IFD authentication.
- Non-support of generic user entry for security reasons when the application context is selected.

The method of implementing an application context and verifying that a given IFD is compliant with it is outside the scope of these specifications. The issuer of an application context might define certain implementation rules or specifications in order to achieve security certification, for instance.

The IFD service provider

Extended IFD capabilities are presented to the application or ICC Service Provider through interfaces implemented in an IFD Service Provider. An IFDSP interfaces with an IFD’s functionality in the same way an ICC Service Provider interfaces with an ICC’s functionality (see Figure 3 – General Architecture Overview).

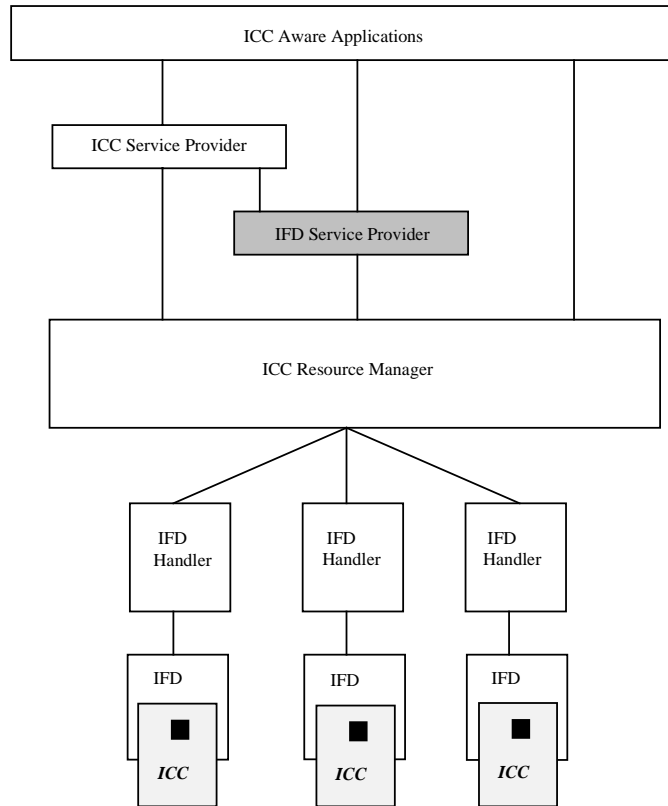


Figure 3 – General Architecture Overview

For each application context (which defines some type of functionality), the IFD Service Provider (IFDSP) may provide different interfaces. The IFDSP implementation structure is up to the IFDSP designer. With different application contexts supported, a configuration similar to the following may appear:

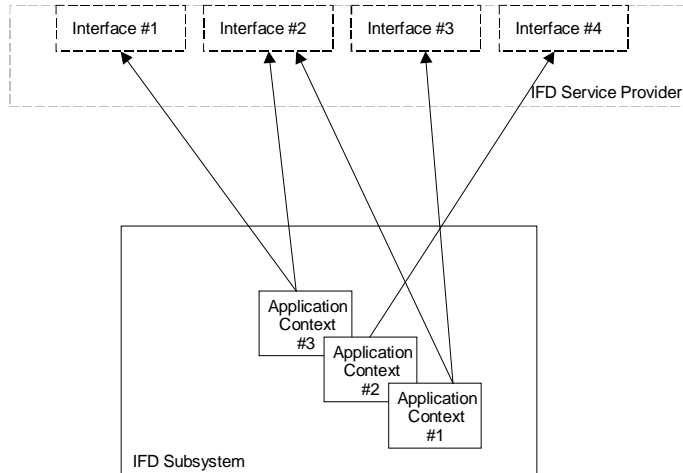


Figure 4 – Example of Multiple Application Contexts with Multiple Interfaces

Part 9 of the Specification describes the following four pre-defined services, the support of which depends on IFD capabilities and security requirements:

- **Secure PIN** With this service, the user enters his PIN directly on the IFD. The PIN is submitted directly to the ICC without being transported back to the PC environment. In order to achieve interoperability, a method for describing PIN formats is specified.
- **Display** This service displays basic character-based messages on the screen of an IFD.
- **User confirmation** This service requests a YES/NO (or VALID/CANCEL) type of response from the user, usually through the IFD keypad.
- **Generic user entry** This service requests the user to enter a character string, usually via the IFD keypad.

Functional Logical Device

In order to manage these new types of functionality at the IFD Subsystem level, another type of device has been introduced in addition to the slot device. This new device is called the Functional Logical Device. An example of logical device configuration is depicted below:

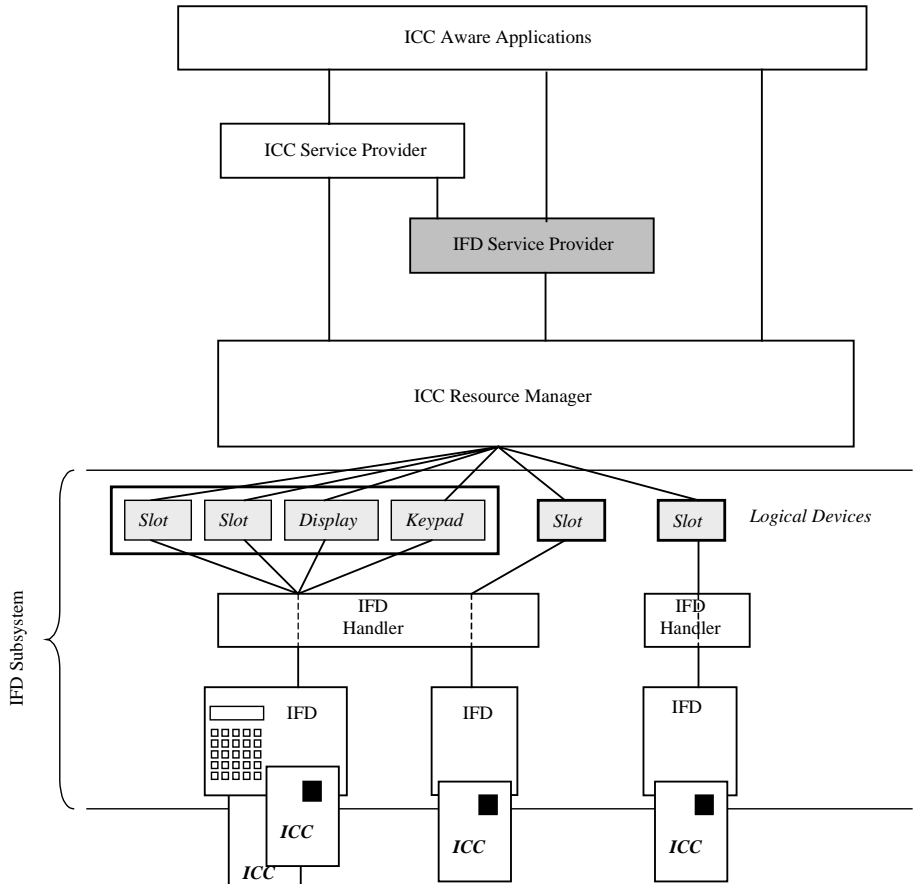


Figure 5 – Example of Logical Device Configuration

Depending on flexibility and security, one or several Functional Logical Devices can be present. For example, they can be mapped directly to a physical sub-device such as a display or keyboard, or regrouped as a PINpad Functional Logical Device. The main role of these Functional Logical Devices is to enable the IFDSP to lock independent types of functionality via the Resource Manager (see Figure 6 – Interaction with Functional Logical Devices). However, the Resource Manager is completely transparent to the communication between the IFDSP and the functional logical devices. Indeed, unlike the slot device, the Functional Logical Device supports only a generic communication channel.

Moreover, as these Functional Logical Devices are only used by the IFDSP, the ICC aware application or ICC Service Provider is completely independent of the Functional Logical Device layout. This preserves the interoperability for IFDs with different Functional Logical Device layout.

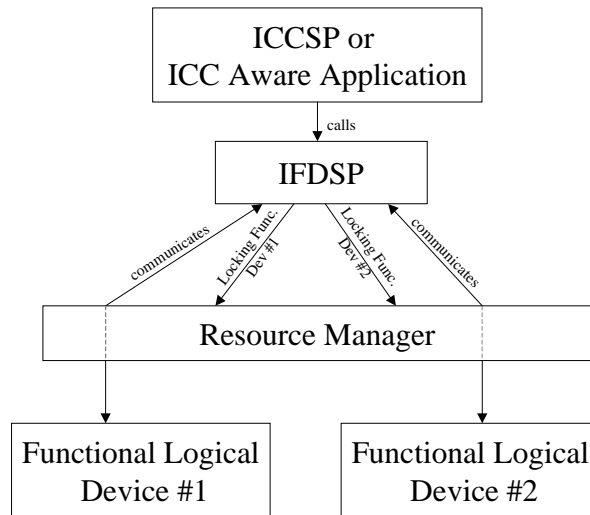


Figure 6 – Interaction with Functional Logical Devices

Finally, modifications to Parts 3 and 5 of the Specification are also required to extend the Resource Manager to handle the new interfaces, the application contexts and logical devices.

SUPPORT OF
SYNCHRONOUS
PROTOCOLS FOR ICCs

Motivation

Many applications work with ICCs using a synchronous communication protocol. There is a wide range of synchronous cards on the market, starting from simple storage cards up to cards supporting cryptographic schemes. Revision 1.0 of the PC/SC specification did not allow support of synchronous ICCs. Support of synchronous communication is now optional with revision 2.0. This allows IFDs to support synchronous ICCs as well as asynchronous ICCs as defined in revision 1.0. It is assumed that synchronous ICCs will mainly be used within closed systems.

Handling synchronous protocols

The goal of the revision 2.0 extensions is to give applications the same look and feel when using synchronous or asynchronous cards as defined in ISO 7816-4 and in part 2 of the revision 1.0 specification. For IFDs supporting synchronous ICCs, it will be mandatory to comply with ISO 7816-10 by supporting “Synchronous card type 1” and “Synchronous card type 2.”

It's the responsibility of the IFD Subsystem to handle the protocols necessary for synchronous ICCs and to map APDUs given by the application to the corresponding ICC commands.

SUPPORT OF CONTACTLESS ICCs

Motivation

Use of contactless ICCs has begun to spread recently. They have proven to be useful for applications such as mass transportation, hands-free access control and logistics. Revision 2.0 of the PC/SC specification allows support of the main standards for interoperable contactless ICCs. The aim of the proposed modification is to provide the same interfaces and look-and-feel at the application level for contactless and asynchronous ICCs. This is achieved by the addition of new tags for interface device capabilities. Implementation of the IFD subsystem (IFD and IFD Handler) must emulate basic functional requirements such as card insertion and removal events and ATR (Part 3). IFD subsystems must also take care of the initialization, selection and communication processes with ICCs.

Supported protocols

Presently, ISO/IEC 14443 for proximity ICC (PICC) has the potential to conform closely to the requirements of the PC/SC architecture. Contactless ICCs specifications are still evolving and, as a result, other protocols such as ISO/IEC 15693 for vicinity ICC (VICC), may also fit these requirements in the future.

Characteristics of a contactless environment

A contactless ICC usually communicates with a reader via radio frequencies using a specific protocol. In a contactless environment, several ICCs can be present at the same time in an activation field. To communicate with a specific ICC, the IFD subsystem uses an anticollision procedure. Each ICC is identified and addressed using a specific ID. Depending on the protocol, the ID can vary partly or totally from session to session.

The contactless environment raises several issues. For instance, card tracking is not as straightforward as in a contact environment since there is no mechanical interaction between the card and the reader. In a contactless environment, the presence of a new card is detected by the reader using a polling mechanism. Card removal, however, is only detected when a card no longer answers a request.

Other issues that need to be considered include:

- Communication with an ICC is done using its address. Switching from one ICC to another or sending a command can alter the state of the ICC.
- A cold reset can be done for all cards within the field by switching the radio frequency (RF) on and off. Unfortunately only a subset of the supported contactless ICCs has the functionality to be reset individually.
- Contactless ICCs do not provide an ATR, although this is subject to change at the standardization level in the near future.

Implementation directives

The contactless environment allows the presence and use of several ICCs in the activation field. We will therefore use a multi-slot scheme to represent this system's behavior.

Card selection

The IFD subsystem must establish and keep a link between an ICC and a slot logical device. An IFD must select an ICC to communicate with it. The IFD subsystem must ensure that addressing an ICC does not affect the current states of other ICCs present in the field.

Card event

The IFD subsystem must generate card insertion and removal events. ICC insertion can easily be recognized by the IFD. Since there is no mechanical interaction, a polling mechanism must be used by the IFD subsystem to detect ICC removal. The IFD subsystem must ensure that states of the ICCs present in the field are not affected by this mechanism.

Card Identification

The IFD subsystem is in charge of providing an ATR compliant with ISO/IEC 7816-4. This ATR will allow ICC service providers to be used. If the ICC does not provide such an ATR, it must be generated by the IFD subsystem. Revision 2.0 will provide guidelines for the construction of the ATR to ensure interoperability between IFDs.

Other impacts on the PC/SC specification

Modifications will be provided in Parts 2 and 3 of the specification in order to accommodate the use of contactless ICCs with the IFD. Part 2 defines the standards supported by PC/SC. Part 3 presents the implementation directives and adds the necessary tags for the new protocols.

ADDITIONAL
REFERENCES

Documents

ISO/IEC 14443 – Identification Cards – Contactless Circuit(s) Cards – Proximity Cards

ISO/IEC 15693 – FCD Identification Cards – Contactless Circuit(s) Cards – Vicinity Cards

ISO/IEC 7816 – Identification Cards – Integrated Circuit(s) cards with contacts

<http://www.iso.ch/>

Interoperability Specification for ICCs and Personal Computer Systems Revision 1.0

<http://www.pscsworkgroup.com>

PC/SC Workgroup Members

Bull CP8:

<http://www.bull.com/>

Gemplus:

<http://www.gemplus.com/>

Hewlett–Packard:

<http://www.hp.com/>

IBM:

<http://www.ibm.com/>

Intel:

<http://www.intel.com/>

Microsoft:

<http://www.microsoft.com/>

Schlumberger:

<http://www.slb.com/>

Siemens:

<http://www.sni.de/>

Sun Microsystems:

<http://www.sun.com/>

Toshiba:

<http://www.toshiba.com/>

For More Information

For the latest information on PC/SC, visit the PC/SC Workgroup Web site at <http://www.pscsworkgroup.com>.