PC/SC Specification
Information Paper

(Interoperability Specification for ICCs and Personal Computer Systems)

V-ONE Corporation
May 26, 1998

Contents

1. Introduction

1.1 What Is The PC/SC Specification?

The PC/SC (Personal Computer/Smart Card) specification was developed to facilitate the interoperability necessary to allow Integrated Circuit Card (ICC) technology, also known as smart cards, to be effectively utilized in the PC environment. This specification was designed to allow PC-based applications to utilize functionality provided by one or more specific smart cards and to accomplish this in a flexible manner, which would support both existing and future ICC-based applications. The PC/SC specification is based on the ISO 7816 standards and is compatible with both the Europay-Mastercard-Visa (EMV) and Global System for Mobile communications (GSM) industry-specific specifications. Its formal name is "Interoperability Specification for ICCs and Personal Computer Systems."

1.2 Who Created The PC/SC Specifications?

The PC/SC specification was created by the PC/SC Workgroup, a joint effort of Bull CP8, Gemplus, Hewlett-Packard, IBM Corporation, Microsoft, Schlumberger, Siemens Nixdorf, Sun Microsystems, Toshiba and VeriFone. In addition to development of the specifications, the PC/SC Workgroup members are committed to implementation of both hardware devices and PC system components necessary to validate the design efforts. This is deemed a critical step in the process of moving toward accepted standards.

The PC/SC Workgroup will retain ownership of this specification until such time as it can be submitted and accepted by a formal standards body. The Workgroup will work with other interested parties to make this happen as quickly as possible. Until that time, the PC/SC Workgroup will support the general review by the PC and ICC communities at large and evolution of the specification as necessary to respond to this general review process.

1.3 Why Even Use Smart Cards?

Smart cards are an intrinsically secure computing platform ideally suited to providing enhanced security and privacy functionality for applications running within general purpose computing environments such as personal computers. ICCs are capable of providing secure storage facilities for sensitive information such as:

- Private keys
- Account numbers
- Passwords
- Medical information

At the same time, the ICC provides an isolated processing facility capable of using this information without exposing it within the PC environment where it is at potential risk from hostile code (viruses, Trojan horses, and so on). This becomes critically important for certain operations such as:

- Generation of digital signatures, using private keys, for personal identification
- Network authentication based on stored secrets
- Maintenance of electronic representations of value (that is, prepaid purchase credits)

1.4 Why Is The PC/SC Specification Needed?

Currently, the use of smart cards in the PC environment is hampered by the lack of interoperability at several levels. First, the industry lacks standards for interfacing PCs to Interface Devices (IFDs). This

has made it difficult to create applications that can work with IFDs from a variety of vendors. Attempts to solve this problem in the application domain invariably increase costs for both development and maintenance. It also creates a significant problem for the PC user in that an IFD used with one application may not work with future applications.

Second, there is no widely accepted high-level programming interface for common ICC functionality. Encapsulation of ICC interfaces can dramatically simplify application development and reduce costs by allowing low-level interface software to be shared across multiple applications. In addition, a standardized high-level interface allows applications to reduce their dependency on a specific ICC implementation, making it far more likely that an application will be able to use future, enhanced ICCs.

Third, mechanisms to allow multiple applications to effectively share the resources of a single ICC are not defined. These are critically important for the deployment of multiple-application ICCs and generic cryptographic ICCs that will be used as part of a multiprocessing PC environment. Without agreed upon standards for device sharing, it becomes effectively impossible for application developers to ensure that they can complete an operation using ICC services without interruption.

ICC technology offers a vital addition to the security infrastructure of the PC and network environments. It is an enabling technology for network commerce in general. To achieve this potential, however, it is essential that a consistent framework exist into which the diverse efforts of application developers, network technology vendors, and ICC technology vendors can be coherently channeled.

1.5 What Are The Objectives Of The PC/SC Specification?

The specification as a whole seeks to achieve the following objectives:

- Maintain consistency with existing ICC-related and PC-related standards while expanding upon them where necessary and practical
- Enable interoperability among components running on various platforms (platform neutral)
- Enable applications to take advantage of products and components from multiple manufacturers (vendor neutral)
- Enable the use of advances in technology without rewriting application-level software (application neutral)
- Facilitate the development of standards for application-level interfaces to ICC services in order to enhance the fielding of a broad range of ICC-based applications in the PC environment
- Support an environment that encourages the widest possible use of ICCs as an adjunct to the PC environment

1.6 Who Benefits From PC/SC Standardization?

By using the smart card APIs and device management infrastructure, application developers can easily and rapidly develop and maintain applications that will work with any compliant smart card reader via attachment to PCs.

For smart card manufacturers, PC/SC standards simplify development and maintenance of interface libraries. Smart card reader manufacturers benefit because any PC/SC-compliant smart card application will work with a PC/SC-compliant reader.

The end-user marketplace will be the ultimate beneficiary of PC/SC standardization due to investment protection and lower costs. End-users will have a large number of smart card-enabled applications that will use the same interface device, and the cost of the devices will be market-driven based upon a standardization/volume effect.

2. System Architecture And Components Overview

2.1 Specification Organization

The “Interoperability Specification for ICCs and Personal Computer Systems” is composed of eight parts. These are intended to apply only to devices and software intended to operate as a part of an overall system that includes a personal computer. Their potential application in other environments is outside the scope of this specification.

The parts of this specification detail specific interoperability requirements for compliant devices, reference design information, programming interfaces, and functional compatibility requirements. The are eight parts to this specification:

- Part 1. Introduction and Architecture Overview
- Part 2. Interface Requirements for Compatible IC Cards and Interface Devices
- Part 3. Requirements for PC-Connected Interface Devices
- Part 4. IFD Design Considerations and Reference Design Information
- Part 5. ICC Resource Manager Definition
- Part 6. ICC Service Provider Interface Definition
- Part 7. Application Domain/Developer Design Considerations
- Part 8. Recommendation for Implementation of Security and Privacy ICC Devices

2.2 Architecture Overview

The architecture defined by this specification, in terms of software and hardware components, is depicted in the Figure 2-1.

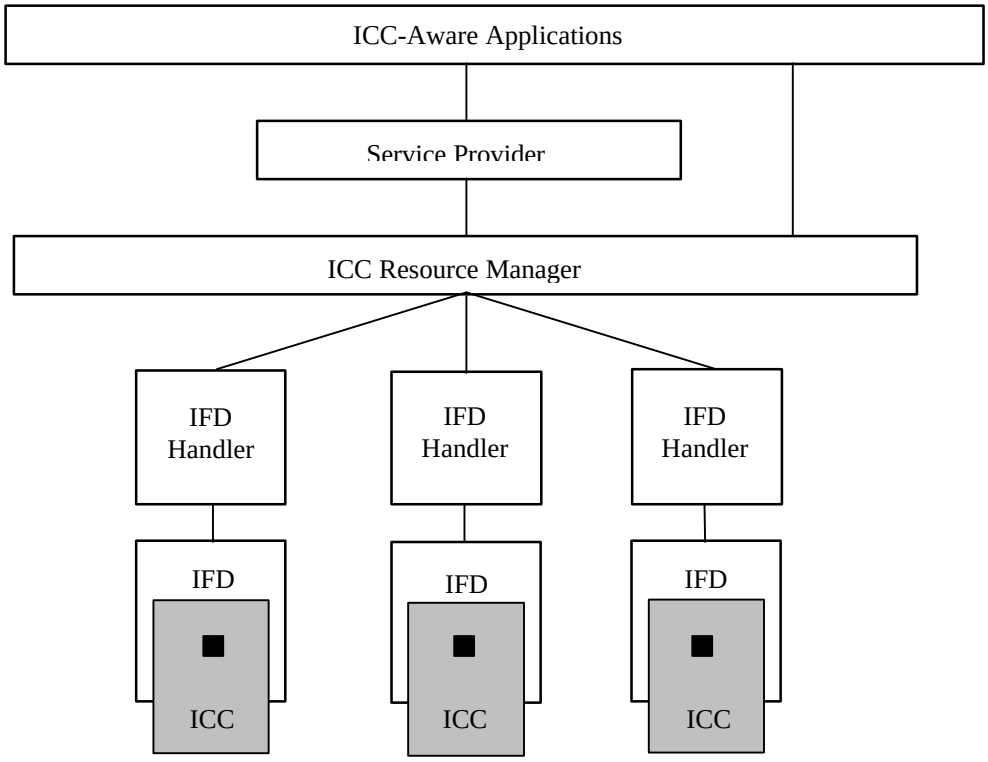

Figure 2-1. General architecture

2.2.1 Integrated Circuit Card (ICC)

The ICC (commonly called a “smart card”) is a credit card–sized plastic case with an embedded microprocessor chip. This specification specifically deals with contact-type ICCs as defined by ISO/IEC 7816. Electrical contacts connected to various pins on the microprocessor chip are embedded in the surface of the plastic case such that an electrical connection can be made between an ICC Interface Device (IFD), commonly called a “smart card reader,” and the card itself. Through these electrical connections, power is supplied (by the IFD) to the microprocessor on the card. An I/O channel is also established by these electrical connections allowing the movement of binary information between the IFD and the ICC.

An ICC compliant with this interoperability specification will conform physically and electrically to the ISO 7816-1, 7816-2, and 7816-3 standards. In addition, an ICC that is compliant with the ISO 7816-10 draft specification for synchronous cards can be supported by this specification. These standards provide a detailed definition of the physical form factor and the electrical characteristics of a compliant ICC.

An ICC is an intrinsically secure computer platform that offers a variety of services, varying from simple secure data storage, to sophisticated cryptographic services, to an ICC-aware application.

2.2.2 Interface Device (IFD)

The IFD (commonly called a “smart card reader”) is the physical interface device through which an ICC communicates with a PC. The IFD establishes a set of electrical connections with the embedded microprocessor of an ICC through the electrical contacts on the surface of the ICC. Through these electrical connections, the IFD provides DC power to the microprocessor chip. Also through these electrical connections, the IFD provides a clock signal, which is used to step the program counter of the microprocessor, as well as an I/O line through which digital information may be passed between the IFD and the ICC.

An IFD may use a variety of physical access ports to the PC. Typically, these will be the keyboard port, a serial line port, or a PC Card (PCMCIA) port. In the future, Universal Serial Bus (USB) devices will likely become common.

A compliant IFD will conform to the ISO 7816-1, 7816-2, and 7816-3 standards. In addition, an IFD may support the ISO 7816-10-draft specification for synchronous cards. IFDs may vary widely in their implementations, allowing vendors to make tradeoffs between intelligence embedded within the device itself and within the IFD Handler software within the PC. For the simplest devices, an IFD need provide little more than electrical connectivity and I/O signal passing between the ICC and the PC. In more complex configurations, an IFD may actually support the data link layer protocols defined in the ISO 7816-3 standards.

2.2.3 Interface Device Handler (IFD Handler)

The IFD Handler encompasses the PC software necessary to map the native capabilities of the IFD to the IFD Handler interface defined in Part 3 of this specification. This is typically low-level software within the PC that supports the specific I/O channel used to connect the IFD to the PC and provides access to specific functionality of the IFD. The differences between “smart” IFDs and “dumb” IFDs are hidden at the IFD Handler API. This is the layer of the interoperability specification primarily responsible for facilitating the interoperability between different IFDs.

The IFD Handler is the terminus (on the PC side) of the ISO 7816-3 defined ICC communication protocols (T=0, T=1), and the synchronous protocol specified by the ISO 7816-10 draft specification. At

the IFD Handler API, all distinctions between ICCs based on ISO protocol handling, whether synchronous or asynchronous, are hidden.

2.2.4 ICC Resource Manager

The ICC Resource Manager is a key component of the PC/SC Workgroup's architecture. It is responsible for managing the other ICC-relevant resources within the system and for supporting controlled access to IFDs and, through them, individual ICCs. The ICC Resource Manager is assumed to be a system-level component of the architecture. It must be present and will most likely be provided by the operating system vendor. There should be only a single ICC Resource Manager within a given system.

The ICC Resource Manager solves three basic problems in managing access to multiple IFDs and ICCs.

First, it is responsible for identification and tracking of resources. This includes:

- Tracking installed IFDs and making this information accessible to other applications.
- Tracking known ICC types, along with their associated Service Providers and supported Interfaces, and making this information accessible to other applications.
- Tracking ICC insertion and removal events to maintain accurate information on available ICCs within the IFDs.

Second, it is responsible for controlling the allocation of IFDs and resources (and hence access to ICCs) across multiple applications. It does this by providing mechanisms for attaching to specific IFDs in shared or exclusive modes of operations.

Finally, it supports transaction primitives on access to services available within a given ICC. This is extremely important, as current ICCs are single-threaded devices, which often require execution of multiple commands to complete a single function. Transactions allow multiple commands to be executed without interruption, ensuring that intermediate state information is not corrupted.

2.2.5 Service Provider

The Service Provider is responsible for encapsulating functionality exposed by a specific ICC and making it accessible through high-level programming interfaces. This specification defines programming interfaces for commonly exposed functionality such as file access, authentication, and cryptographic services. These interfaces may be enhanced and extended to meet the needs of specific application domains.

This specification divides the Service Provider into two independent components: the ICC Service Provider and the Cryptographic Service Provider. While they may be logically thought of as a single component, they are distinct in recognition of the realities of dealing with existing international export and/or import laws for cryptographic devices. Only those ICCs exposing cryptographic functionality, accessible to programs running within the PC, will need to develop a Cryptographic Service Provider.

An important point to note is that this specification does not require a Service Provider to be a monolithic component running on a single PC. In particular, one can envision building a Service Provider as a client/server component. This would allow a server-side application developer to take advantage of the high-level interfaces and interoperability supported by this architecture. In addition, we recognize that some ICC applications require secure messaging, for confidentiality and integrity of data moving between an application and the ICC. This type of implementation can ensure that secure messaging is done within a protected server security perimeter.

In operation, an application may know *a priori* which Service Provider it wants to work through. In this case, it can connect to the Service Provider and wait until the proper ICC is inserted. However, an

application may also determine which Service Provider to use at run time by using the ICC Resource Manager to enumerate the available providers and their supported interfaces. This is intended to provide flexibility to the developer and meet the needs of a variety of applications.

2.2.5.1 ICC Service Provider

The ICC Service Provider encapsulates access to a specific ICC through high-level programming interfaces. It should not expose cryptographic functions to PC applications. (Note: it may expose interfaces that use cryptography internal to the ICC, such as secure messaging or cryptogram-based authentication.)

Interfaces for commonly implemented file access and authentication services are defined by this specification. If an ICC implements these services, it shall make use of the defined interfaces. However, additional interfaces may be defined and implemented to meet domain-specific requirements.

Before an ICC Service Provider can be used within this architecture, it must be "introduced" to the ICC Resource Manager. Typically, this is done through an ICC setup utility provided by the ICC vendor. This utility must provide four pieces of information about the card:

1. Its ATR string and a mask to use as an aid in identifying the ICC

2. An identifier for the Service Provider(s) that support the ICC

3. A list of ICC Interfaces supported by the ICC

4. A "friendly name" for the ICC; to be used in identifying the ICC to the user (in most cases, the user will supply this to the setup utility)

2.2.5.2 Cryptographic Service Provider

The Cryptographic Service Provider encapsulates access to a specific ICC cryptographic functionality through high-level programming interfaces. It should expose only cryptographic functions to PC applications. Other functionality should be implemented in an ICC Service Provider.

Interfaces are defined in this specification for general-purpose cryptographic services including:

- Key generation.
- Key management.
- Digital signatures.
- Hashing (or message digests).
- Bulk encryption services.
- Key import/export.

2.2.6 ICC-Aware Application

The ICC-Aware Application ("Application") is an arbitrary software program within the PC operating environment, which wants to make use of the functionality provided by one or more ICCs. It is assumed the Application is running as a process within a multi-user, multiprocess, multiple-threaded, and multiple device environment. The architecture components defined within this specification provide mechanisms to map PC application requests to the ICC, which is typically a single user, single-threaded, but multiple application environment.

This overall architecture can alternatively be presented as a peer-to-peer communication protocol, as illustrated in Figure 2-2.

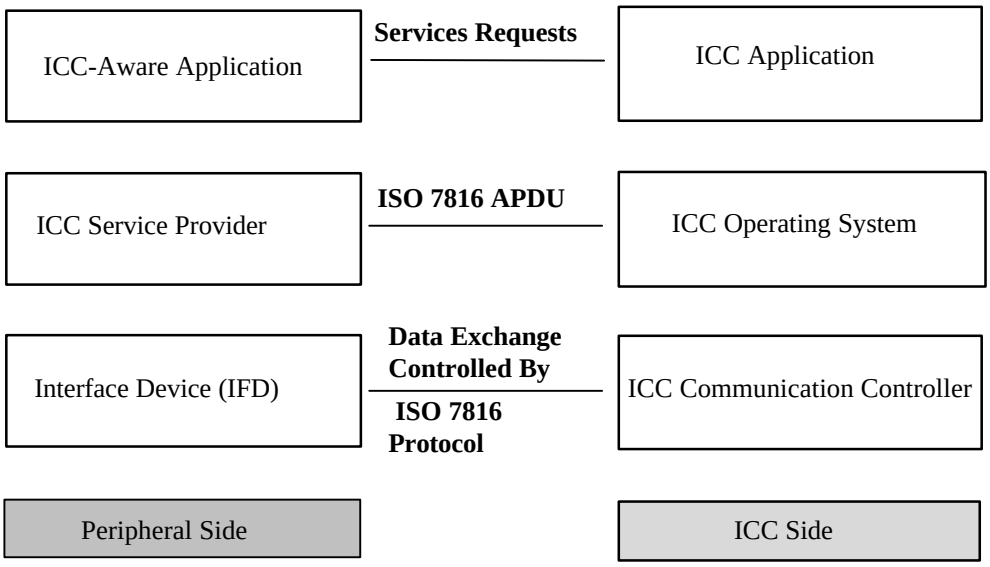

Figure 2-2. ICC/PC communication layers

2.3 Specification Breakdown

Figure 2-3 shows how the different Parts that make up this specification can be related to the overall system architecture:

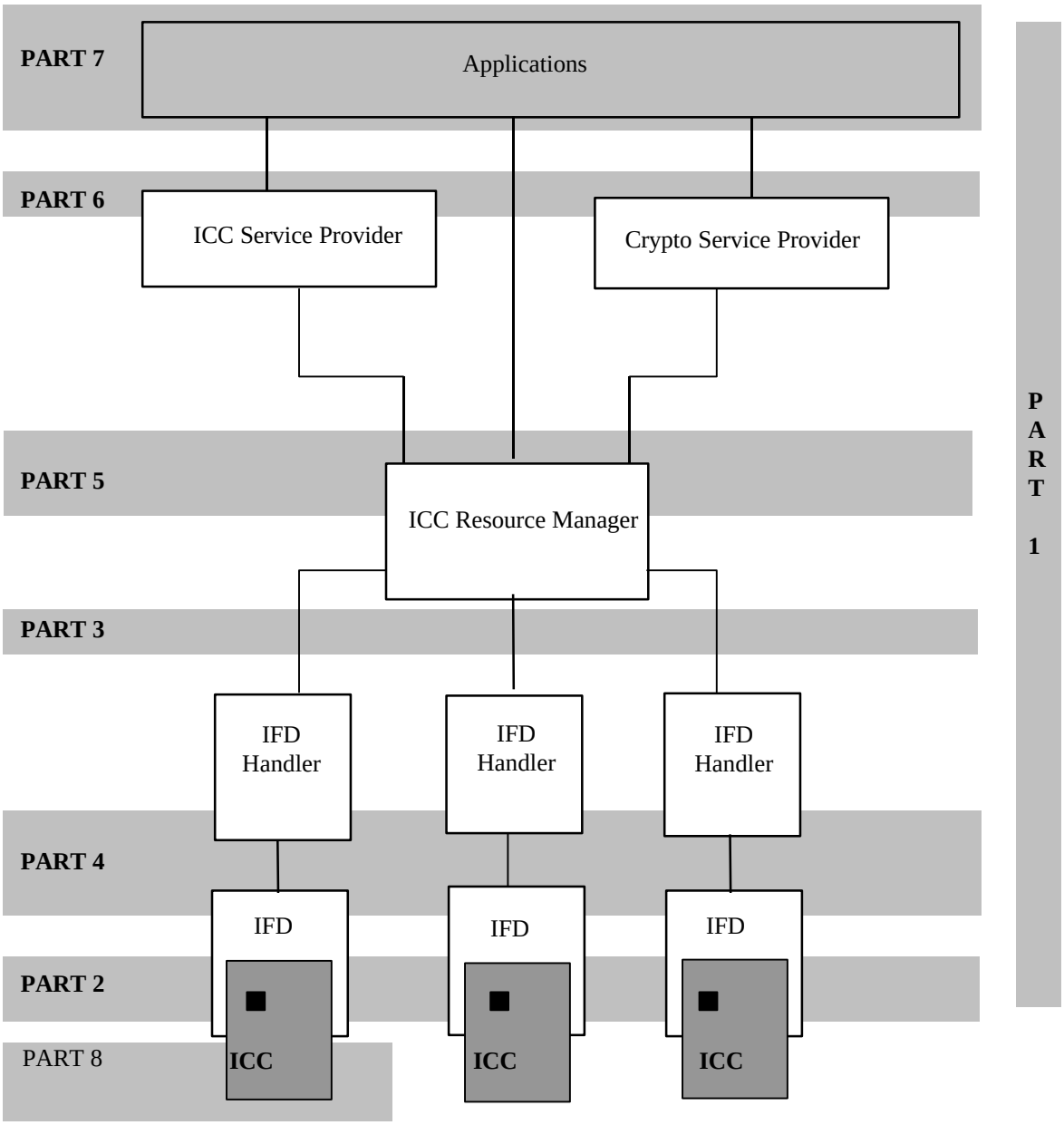

Figure 2-3. Specification breakdown

References

This paper was prepared primarily by editing and combining the following documents:

Interoperability Specification for ICCs and Personal Computer Systesm, Part 1. Introduction and Architecture Overview; Bull CP8, Gemplus SA, Hewlett-Packard Company, IBM Corporation, Microsoft Corporation, Schlumberger SA, Siemens Nixdorf Informationssysteme AG, Sun Microsystems, Inc., Toshiba Corporation, and Verifone, Inc.; Revision 1.0 December 1997

PC/SC Workgroup releases first specifications for integration of smart cards with personal computers; PC/SC Workgroup; Press Release Dec. 10,1997

Smart Cards; Microsoft Corporation; White Paper 1997