

Anexo C – Especificación PC/SC

Introducción

PC/SC es una especificación desarrollada por un grupo de trabajo el cual se conforma de varias empresas, entre ellas fabricantes de tarjetas inteligentes como Bull, Schlumberger, Gemplus y de otras empresas como Microsoft, Toshiba, Sun Microsystems, HP e IBM. Este grupo se inició para desarrollar una especificación que facilite la interoperabilidad necesaria para el uso efectivo de la tecnología de las tarjetas con circuito integrado (ICCs, por sus siglas en inglés de “*Integrated Circuit Card*”) en computadoras personales (PC). Además del desarrollo de esta especificación, el grupo se encarga de la implementación de hardware y componentes de software necesarios para la validación del diseño.

Actualmente, el uso de tarjetas con chip en ambientes de PCs se encuentra obstaculizado por la falta de interoperabilidad en varios niveles. Primero, la industria carece de estándares para interfaces entre PCs y lectores de tarjetas (IFDs, por sus siglas en inglés de “*Interface Device*”). Esto ha hecho difícil el desarrollo de aplicaciones que puedan trabajar con lectores de distintos fabricantes. Segundo, no existe una interfaz de programación de alto nivel para funciones comunes de las tarjetas con chip que sea aceptada ampliamente. Por último, no se han definido mecanismos para permitir que múltiples aplicaciones compartan de manera efectiva los recursos de las tarjetas con chip. Esto es crítico debido a la tendencia que existe de contar con varias aplicaciones en una sola tarjeta con chip. Sin el uso de estándares para compartir dispositivos, será imposible que los desarrolladores de aplicaciones aseguren la ejecución correcta de los servicios de las tarjetas con chip.

Objetivos

La especificación PC/SC se encuentra actualmente en su versión 2.01.3 [PC/SC, 2006]. Esta describe la funcionalidad mínima requerida para las ICCs, IFDs, y PCs para permitir

la interoperabilidad entre elementos de los distintos fabricantes. La especificación busca cumplir los siguientes objetivos:

- Mantener consistencia con los estándares existentes para ICCs y para PCs.
- Permitir la interoperabilidad entre componentes que se ejecuten en distintas plataformas (neutralidad entre plataformas).
- Permitir a las aplicaciones aprovechar las ventajas de los productos y componentes de los distintos proveedores (neutralidad entre proveedores).
- Permitir el uso de los avances tecnológicos sin necesidad de volver a escribir software a nivel de aplicación (neutralidad entre aplicaciones).
- Facilitar el desarrollo de estándares de interfaces a nivel de aplicación para servicios de las ICCs para incrementar la disponibilidad de aplicaciones basadas en tarjetas en ambientes de PCs.
- El soporte de ambientes que promuevan lo más posible el uso de tarjetas con chip como un elemento adicional de los ambientes de PCs.

Organización de la especificación

La especificación PC/SC se compone de nueve partes. Estas partes describen los requerimientos específicos para la interoperabilidad entre dispositivos compatibles, información de referencia para diseño, interfaces de programación y requerimientos de compatibilidad funcional. Las nueve partes se mencionan a continuación:

- **Parte 1.** Introducción y vista general de la arquitectura.
- **Parte 2.** Requerimientos de interfaz para tarjetas con chip (ICC) y lectores (IFD) compatibles.
- **Parte 3.** Requerimientos para dispositivos de interfaz de conexión a PC.
- **Parte 4.** Consideraciones de diseño de IFDs e información de referencia. Provee recomendaciones para la implementación de IFDs en teclados con interfaz PS/2.

- **Parte 5.** Describe las interfaces y funcionalidad que provee el administrador de recursos de las ICCs.
- **Parte 6.** Describe el modelo del proveedor de servicios del ICC, identifica las interfaces requeridas e indica como estas se pueden extender para cumplir con los requerimientos de aplicaciones de dominio específico.
- **Parte 7.** Describe las consideraciones para el diseño de aplicaciones y como hacer uso de los demás componentes.
- **Parte 8.** Recomendaciones para la implementación de ICCs de seguridad y privacidad.
- **Parte 9.** Describe el manejo de IFDs con algunas capacidades extendidas.
- **Parte 10.** Describe el manejo de IFDs con capacidades de entrada segura de PIN.

Arquitectura de PC/SC

La arquitectura que define la especificación PC/SC se compone básicamente de los siguientes elementos:

- **Tarjeta con circuito integrado (ICC)** – Se refiere a la tarjeta inteligente. Esta especificación es compatible con ICCs que cumplen con estándares ISO 7816-1,2,3 y 10 para tarjetas de contacto síncronas y asíncronas. También es compatible con tarjetas sin contacto que cumplen con estándares ISO/IEC 14443 (de proximidad), ISO/IEC 15693 (de vecinidad) y similares.
- **Dispositivo lector (IFD)** – Se refiere al lector de tarjetas, el cual es la interfaz física por medio del cual el ICC se comunica con la PC. Un IFD puede tener una o más ranuras para tarjetas y pueden también permitir ciertas funciones adicionales como pantallas de despliegue, lector de huella digital y teclado. Además los lectores pueden tener diferentes puertos de conexión con la PC, como por ejemplo USB, serial, puerto de teclado, PCMCIA, etc.

- **Controlador del lector** - Es un software de bajo nivel que se encuentra en la PC y controla los canales de entrada y salida utilizados para conectar el IFD a la PC. Este provee acceso a funciones específicas del IFD y esconde las diferencias entre IFDs que tienen varias funciones y los que son sencillos.

- **Administrador de recursos del ICC** – Este es un componente clave de la arquitectura PC/SC. Se encuentra a nivel del sistema y es el responsable de administrar los otros recursos relevantes al ICC dentro del sistema, además de controlar el acceso a los IFDs y, a través de ellos, el acceso a ICCs en particular. Lo provee el vendedor del sistema operativo y debe existir solamente un controlador de recursos por sistema. Administración el acceso entre múltiples IFDs e ICCs de la siguiente manera:
 1. Es el responsable de la identificación y rastreo de los recursos, lo cual incluye:
 - Rastrear los IFDs instalados y presentar información respecto a ellos a las demás aplicaciones.
 - Rastrear los tipos de ICC conocidos, junto con sus proveedores de servicios asociados e interfaces que soporta, haciendo disponible esta información a las demás aplicaciones.
 - Rastrear los eventos de inserción y retiro de ICCs para mantener información exacta sobre los ICCs que están insertados en los IFDs disponibles.

 2. Es el responsable de controlar la localidad de los IFDs y sus recursos a través de múltiples aplicaciones.

 3. Soporta transacciones para el acceso a servicios disponibles dentro de un ICC, permitiendo ejecutar varios comandos dentro de una misma función.

- **Proveedores de servicios del ICC** – Son componentes que encapsulan funcionalidad expuesta por cierto ICC para hacerla accesible a través de interfaces de programación de alto nivel. Estas funcionalidades se dividen en servicios del sistema operativo del ICC y en servicios específicos del dominio de la aplicación.
- **Proveedor de servicios criptográficos** – Encapsula acceso a funciones criptográficas del ICC a través de interfaces de programación de alto nivel. Entre las funciones se encuentran la generación de llaves, administración de llaves, firmas digitales, algoritmos Hash, servicios de cifrado, importación y exportación de llaves.

En la figura C1 se muestra el diagrama de la arquitectura que define la especificación PC/SC, en términos de elementos de hardware y software.

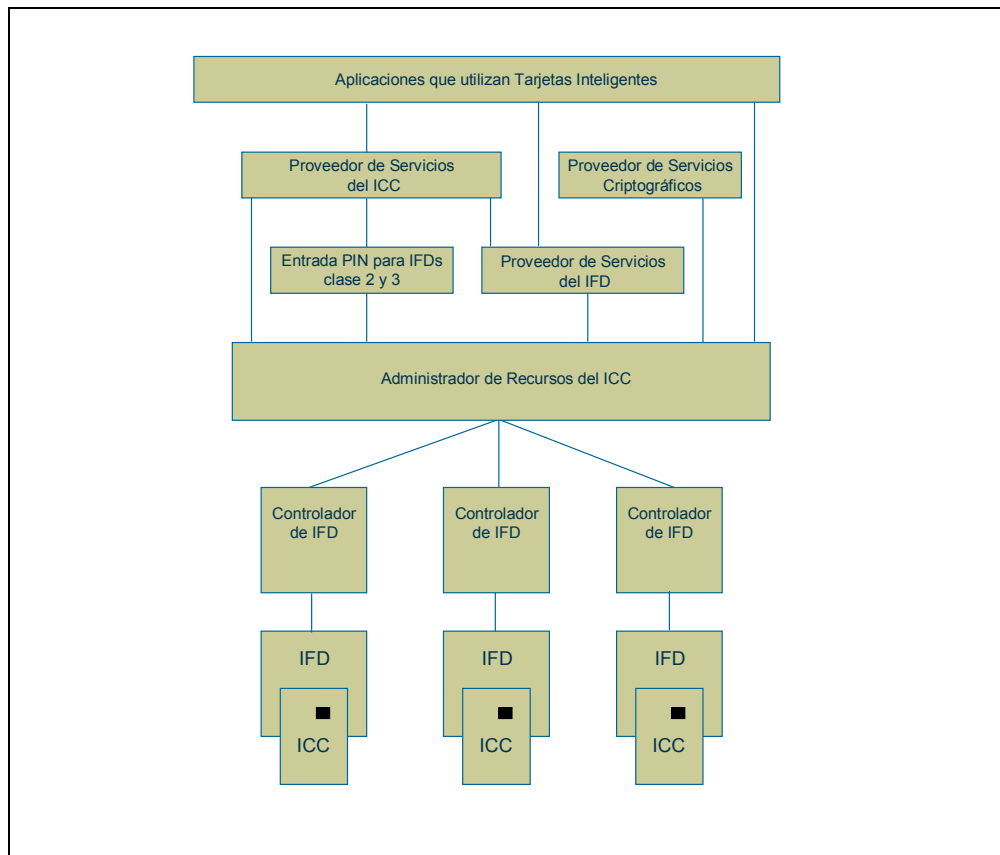


Figura C1 - Arquitectura de la especificación PC/SC