Tarjetas Inteligentes

Desarrolladas en Europa en la década del '70, las tarjetas inteligentes fueron incorporando tecnología y sumando prestaciones. Hoy es frecuente su uso en telefonía, control de accesos y personal, mercado en el que tiene cada vez mayor participación. Su aplicación como monedero electrónico está cada vez más difundida entre los medios de pago y transacciones.

Las tarjetas inteligentes son, básicamente, tarjetas de plástico de similares estándares físicos a las tarjetas de crédito pero, a diferencia de éstas, llevan estampadas un circuito integrado, que puede ser únicamente de memoria o contener un microprocesador con un sistema operativo que le permita una serie de tareas. Entre ellas, almacenar y encriptar información o leer y escribir datos.

Como mecanismo de control de accesos, las tarjetas inteligentes hacen que los datos personales y de negocios solo sean accesibles a los usuarios apropiados, ofreciendo, además, portabilidad, seguridad y confiabilidad.

La incorporación de un circuito integrado, asimismo, ofrece elementos que pueden favorecer su utilización generalizada. Principalmente:

- **Miniaturización:** Las densidades de integración de controladores y memorias que se alcanzan en la actualidad permiten ofrecer un nuevo abanico de posibilidades y de funciones, lo que origina su expansión en el mercado y un nuevo medio de intercambio de información.

- **Lógica programable:** La tarjeta inteligente incorpora la potencia de los ordenadores, incluyendo las funciones lógicas y de control que se aplican a los negocios junto con funciones avanzadas de seguridad y nuevas aplicaciones.

- **Interfaz directa de comunicaciones electrónicas:** Las comunicaciones están en crecimiento constante. Cada nuevo avance ofrece un nuevo campo en el que puede aplicarse las tarjetas inteligentes.

Orígenes

La tarjeta magnética convencional se desarrolló a fines de los '60 para satisfacer varias necesidades. Entre ellas, permitir a los clientes de los bancos y entidades de ahorro activar y operar de forma rápida y efectiva con los cajeros automáticos, además de proporcionar un medio con el que operar en puntos de venta específicos.

El objetivo de esta tarjeta es identificar a un cliente para acceder a una base de datos remota con la que se establece una conexión y la información que posee esa base de datos permite aceptar o rechazar esa transacción.

Si bien este tipo de tarjetas dieron buen resultado en el mercado financiero, no ofrecen soluciones para los nuevos mercados y servicios que aparecen, como la telefonía digital.

El problema se debe a que las tarjetas magnéticas actuales se han utilizado para dar solución a problemas que aparecieron hace 25 años y están ligados a esas tecnologías: dependencias de ordenadores centrales y grandes redes dedicadas, a diferencia de los sistemas distribuidos actuales y de las nuevas soluciones. Además, la tarjeta magnética ofrece muy baja densidad de datos, baja fiabilidad y poca o ninguna seguridad en la información que lleva.

La tarjeta inteligente nació, precisamente ante las nuevas necesidades del mercado, en la década del '70 cuando inventores de Alemania, Japón y Francia inscribieron las patentes originales. Debido a varios factores que se presentaron, entre los cuales la inmadura tecnología de semiconductores tuvo un mayor peso, muchos trabajos sobre tarjetas inteligentes *(smart cards)* estuvieron en investigación y desarrollo hasta la primera mitad de los años ochenta.

Es a principios de los noventa las tarjetas inteligentes inician su despegue, coincidentemente con el boom de la telefonía móvil GSM, inicialmente con tarjetas de 1K de memoria.

En el campo del monedero electrónico, su uso comenzó en 1997 con la aparición de la *VisaCash*, versión propietaria implementada por Visa España, paralelamente otro tipo de monedero electrónico siguiendo el estándar europeo, certificado bajo *norma ISO/IEC TR 15504* (relacionada con los modelos y estándares de evaluación y mejora de los procesos de software).

Aunque existen prototipos desde algunos años antes, hasta fines de 1999 no salen al mercado de forma masiva tarjetas sin contacto, debido principalmente a los problemas para integrar la antena en la tarjeta.

Continúa en página 150

Viene de página 146

Magnética vs. inteligente

La tecnología más extendida en la actualidad es la basada en banda magnética: prácticamente todo el mundo dispone de alguna tarjeta, normalmente de uso financiero, que en su parte posterior tiene una banda de color marrón oscuro. Esta banda magnética es similar a un pedazo de cinta de un cassette de audio y su misión es almacenar cierta información, como el nombre del titular, el número de su cuenta, el tipo de tarjeta y el PIN. Básicamente se puede decir que identifica al usuario con el dispositivo con el que se pone en contacto y este dispositivo, gestiona una serie de operaciones y guarda cierta información de cada transacción. Hasta el punto mencionado la tecnología chip aporta prácticamente lo mismo que la banda magnética.

Sin embargo hay al menos tres campos en los que la potencialidad implícita en el chip da a esta última tecnología una clara ventaja de cara al futuro.

• **Seguridad:** El contenido de la banda magnética, por la tecnología que utiliza, puede ser leído y, aunque no es sencillo, puede ser manipulado por personas con conocimiento y medios adecuados. El chip, sin embargo, contiene una tecnología interna mucho más sofisticada que hace que las posibilidades de manipulación física se reduzcan de forma muy sensible. Además, por su capacidad interna, puede soportar procesos criptográficos muy complejos (DES[1] simple, triple DES, RSA[2])

• **Capacidad de almacenamiento:** La cantidad de información incorporable a una banda magnética es pequeña y parcialmente modificable, por lo que la relación entre el usuario de la tarjeta y el emisor es unidimensional: únicamente se actualiza cuando se interactúa a través de hardware sofisticado *(ATMs)*. El chip, sin embargo, une a su mayor capacidad de almacenamiento la posibilidad de gestionar información. Estas características diferenciales motivan que la difusión de la tecnología chip aplicada en tarjetas de plástico sea cada vez mayor, gracias a la estandarización del producto.

• **Flexibilidad:** La tecnología de tarjetas inteligentes es compatible con los principales tipos de sistemas operativos. También un entorno de programación que permite crear, almacenar o suprimir aplicaciones en las tarjetas, seleccionando las que se adapten a las circunstancias y necesidades de cada persona.

Qué es una tarjeta inteligente

Es bastante frecuente denominar a todas las tarjetas que poseen contactos dorados o plateados sobre su superficie como "*tarjetas inteligentes*". Sin embargo, este término es bastante ambiguo y conviene hacer una clasificación más correcta.

La International Standard Organization (ISO) prefiere usar el término "*tarjeta de circuito integrado*" (Integrated Circuit Card o ICC), para referirse a todas aquellas tarjetas que posean algún dispositivo electrónico. Este circuito contiene elementos para realizar transmisión, almacenamiento y procesamiento de datos. La transferencia de datos puede llevarse a cabo a través de los contactos, que se encuentran en la superficie de la tarjeta, o sin contactos por medio de campos electromagnéticos.

Estas tarjetas presentan bastantes ventajas en comparación con las de bandas magnéticas: son capaces de almacenar más información; pueden proteger la información almacenada de posibles accesos no autorizados y poseen una mayor resistencia al deterioro de la información almacenada.

Dado que el acceso a la información se realiza a través de un puerto serie y supervisado por el propio sistema operativo de la tarjeta, es posible escribir datos confidenciales que no puedan ser leídos por personas no autorizadas. En principio, las funciones de escritura, lectura y borrado de la memoria pueden ser controladas tanto por el hardware como por el software, o por ambos a la vez. Esto permite una gran variedad de mecanismos de seguridad.

Al ser el chip integrado su componente más importante, las tarjetas están clasificadas según el tipo de circuito.

Clasificación

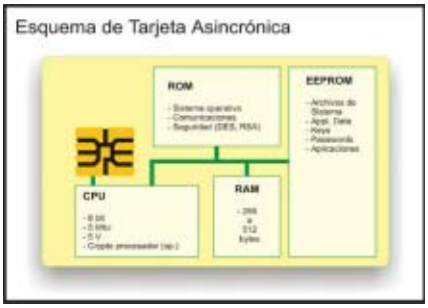
• **Tarjeta Inteligente de Contacto:** Estas tarjetas necesitan ser insertadas en una terminal con lector inteligente para que, por medio de contactos, pueda ser leída. Existen dos tipos de tarjeta inteligente de contacto: sincrónicas y asincrónicas.

- Sincrónicas o Tarjetas de Memoria: Los datos que se requieren para las aplicaciones con tarjetas de memoria son almacenados en una EEPROM *(electrically erasable programmable read-only memory)*. Estas tarjetas son cargadas previamente con un monto o valor que va decreciendo a medida que se utiliza y una vez que éste se acaba se vuelve desechable.

Las hay de memoria libre, carecen de mecanismos de protección para acceder a la información y se utilizan para el pago de peajes, teléfonos públicos, máquinas dispensadoras y espectáculos, y de memoria protegida. Estas poseen un circuito de seguridad que proporciona un sistema para controlar los accesos a la memoria frente a usuarios no autorizados. Este sistema funciona mediante el empleo de un código de acceso que puede ser de 64 bits o más.

- Asincrónicas: Estas tarjetas poseen en su chip un microprocesador que además cuenta con algunos elementos adicionales: ROM enmascarada; EEPROM, RAM y un puerto de Entrada/Salida.

La tarjeta inteligente es, generalmente, de plástico, de forma similar a una tarjeta de crédito pero que posee un procesador (microchip) insertado en el cual se almacena información, lo que permite mayor eficiencia que en el sistema de tarjetas de crédito convencional.



La ROM *(Read Only Memory)* enmascarada contiene el sistema operativo de la tarjeta y se graba durante el proceso de fabricación mientras que la EEPROM es la memoria no volátil del microprocesador y en ella se encuentran datos del usuario o de la aplicación, así como el código de las instrucciones que están bajo el control del sistema operativo. También puede contener información como el nombre del usuario o su número de identificación personal *(PIN, Personal Identification Number)*.

Continúa en página 154

Viene de página 150

La RAM *(Random Access Memory)*, en tanto, es la memoria de trabajo del microprocesador que, al ser volátil, perderá toda la información contenida en ella una vez desconectada la alimentación.

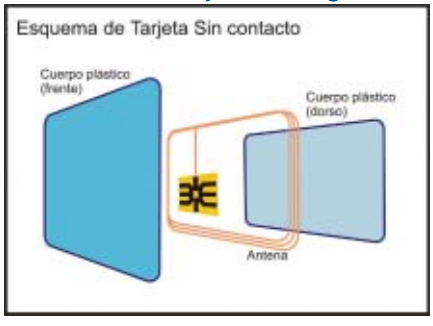
Finalmente, el puerto de entrada y salida normalmente consiste en un simple registro a través del cual la información es transferida bit a bit.

• **Tarjetas Inteligentes sin Contacto:** Son similares a las de contacto en usos y funciones pero utilizan diferentes protocolos de transmisión en capa lógica y física, no utilizan contacto galvánico sino de interfase inductiva. Poseen además del chip, una antena de la cual se valen para realizar transacciones. Son ideales para las transacciones que tienen que ser realizadas muy rápidamente.

Cuando en una tarjeta de contacto se producen fallos de funcionamiento casi siempre se deben al deterioro en la superficie de contacto o a la suciedad adherida a los mismos. Las tarjetas sin contacto eliminan esos problemas técnicos, debido, claro está, a que carecen de contactos. Otra de las ventajas es la de no tener que introducir la tarjeta en un lector. Esto es una gran ventaja en sistemas de control de accesos donde se necesita abrir una puerta u otro mecanismo, puesto que la autorización de acceso puede ser revisada sin que se tenga que sacar la tarjeta del bolsillo e introducirla en un terminal.

Este tipo de tarjetas se comunican por medio de radiofrecuencias y la distancia necesaria entre tarjeta y lector varía según su aplicación, modelo y fabricante.

Lectores de tarjetas inteligentes



Como el propio nombre lo indica, un lector de tarjetas es una interfaz que permite la comunicación entre una tarjeta y otro dispositivo. Los terminales se diferencian unos de otros en la conexión con el ordenador, la comunicación con la tarjeta y el software que poseen.

Existen distintos tipos de lectores:

• **Conectados a un PC:** Son lectores fabricados para ser usados conectándolo a un computador a través de un puerto serie, usb u otro

• **Conectados a un equipo específico:** Se pueden instalar, previo fabricación y diseño, en un dispositivo determinado para cumplir una función; cajeros automáticos, máquinas expendedoras, parquímetros, control de accesos, etc.

• **Portátiles:** No necesitan de otro aparato para cumplir su función y generalmente poseen todos los recursos integrados como baterías, memoria, pin pad, etc.

Sistema operativo

En contraste con los sistemas operativos conocidos, los sistemas basados en tarjetas inteligentes no permiten al usuario el almacenamiento externo de información, siendo las prioridades más importantes la ejecución segura de los programas y el control de acceso a los datos.

Debido a la restricción de memoria, la cantidad de información que se puede grabar es bastante pequeña. Los módulos de programa se graban en la ROM, lo cual posee la desventaja de no permitir al usuario programar el funcionamiento de la tarjeta según sus propios criterios, ya que una vez grabado el sistema operativo es imposible realizar cambios. Por esto el programa grabado en la ROM debe ser bastante fiable y robusto.

Otra característica importante del sistema operativo es que no permite el uso de "*puertas traseras*", que son bastante frecuentes en sistemas grandes. Esto quiere decir que es imposible hacer una lectura desautorizada de los datos contenidos usando el código propio de la tarjeta.

Existen otras funciones que desempeña el código almacenado en la ROM: transmisión de datos desde y hacia la tarjeta, control de la ejecución de los programas, administración de los datos y manejo y administración de algoritmos criptográficos.

Unas de las principales características de las tarjetas de circuito integrado es que permiten almacenar datos e incluso proteger el acceso a dichos datos frente a lecturas no autorizadas. Las tarjetas incluyen auténticos sistemas de administración de ficheros (o carpetas) que siguen una estructura jerárquica. Los programas que gobiernan estos sistemas están bastante minimizados para reducir el uso de memoria.

Los sistemas operativos más recientes están orientados a trabajar con objetos, lo que significa que todos los datos referentes a una carpeta están contenidos en ella mismo. Otra consecuencia es que para efectuar cambios en el contenido de una carpeta, ésta debe ser seleccionada con la correspondiente instrucción. Las carpetas están divididas en dos secciones distintas: la primera se conoce como cabecera y contiene datos referentes a la estructura de la carpeta y sus condiciones de acceso. La otra sección es el cuerpo, que contiene los datos del usuario.

La tarjeta inteligente es un mecanismo que permite almacenar de manera fiable información financiera o transaccional, claves privadas, números de cuenta, password o información personal. Esta capacidad se la otorga la encriptación de datos.

Seguridad

Existen en la actualidad empresas que han tomado la decisión de basar la seguridad de sus sistemas en las tarjetas inteligentes: sin el PIN, por ejemplo, estas tarjetas no se activan impidiendo su uso por usuarios no autorizados.

Un problema de seguridad que hasta ahora ha quedado sin resolver es el de la comunicación entre la tarjeta y el lector. Algunas tarjetas se utilizan sobre redes de comunicaciones como Internet, en las que se pueden producir escuchas de información confidencial. Otro aspecto es el de la autenticación, consistente en asegurar de forma fiable la identidad del interlocutor. La tarjeta tiene que estar segura de que el lector con el que trata o el expendedor de dinero electrónico del que extrae dinero son confiables y a su vez los lectores y sistemas centrales de las aplicaciones financieras tienen que asegurarse que

Continúa en página 158

Viene de página 154

están tratando con una tarjeta válida.

Esos problemas están resueltos por la criptografía: la confidencialidad, integridad *(que la información no sea modificada sin autorización)* y autenticación.

Para entender algunas de las aplicaciones de dinero electrónico en tarjetas inteligentes hay que entender también las técnicas criptográficas de demostración de identidad de conocimiento cero (Zero-knowledge proof identity, ZKPI[3]).

Encriptación de datos

La técnica de encriptado se basa en un algoritmo de cifrado y una clave, de tal forma que se requieren ambos para generar, a partir del texto claro, el texto cifrado. Para descifrar se requieren un algoritmo de descifrado y una clave de descifrado.

Un protocolo criptográfico es aquel que utiliza técnicas criptográficas junto con las reglas de comunicación.

• **Cifrado simétrico:** Se caracteriza por poseer un único algoritmo de cifrado/descifrado, aunque en la ejecución de ambas operaciones pueden existir pequeñas variaciones, y por una única clave para cifrar y descifrar. Esto implica que la clave tiene que permanecer oculta y ser compartida por el emisor y el receptor, por lo que se debe distribuir en secreto y se necesita una clave para cada par de interlocutores.

• **Cifrado asimétrico (Clave pública):** Se caracteriza por la existencia de dos claves independientes para cifrar y para descifrar. Esta independencia permite al receptor hacer pública la clave de cifrado, de tal forma que cualquier entidad que desee enviarle un mensaje pueda cifrarlo y enviarlo. La clave de descifrado permanece secreta, por lo que sólo el receptor legitimo puede descifrar el mensaje. Ni siquiera el emisor es capaz de descifrar el mensaje una vez cifrado.

Dentro de los sistemas criptográficos hay que distinguir entre el algoritmo criptográfico y el protocolo criptográfico. Un algoritmo criptográfico es un mecanismo que permite convertir un texto claro *(legible)* en otro cifrado *(ilegible)*. Un protocolo criptográfico es un protocolo en el que se utilizan algoritmos criptográficos.

La seguridad de un sistema con protección criptográfica puede venir de la debilidad de sus algoritmos, protocolos o a través de sus claves. Un algoritmo es inseguro cuando existe un método eficaz para obtener la clave o cuando es posible debilitar alguna de sus propiedades criptográficas *(autenticación, integridad y confidencialidad).*

Usos más frecuentes

Cada vez más programas de fidelización en sectores como líneas aéreas, hoteles, restaurantes de comida rápida y grandes almacenes, utilizan las tarjetas inteligentes, que registran los puntos y premios, y que ofrecen datos detallados sobre los hábitos y experiencias de los clientes a los operadores de dichos programas, a fin de elaborar sus campañas de marketing con mayor precisión.

Las tarjetas inteligentes también están muy extendidas entre los grupos cerrados de usuarios (residentes de una ciudad, personal de una universidad, personal de una compañía, aficionados de un equipo deportivo, clientes de un parque de atracciones, etc.), los cuales pueden utilizar tarjetas con múltiples aplicaciones para pagar sus cuotas o acceder a servicios (por ejemplo, descuento en compras, entrada para partidos, máquinas expendedoras, credenciales de biblioteca, parques de atracciones, estacionamientos, etc.), de forma ilimitada de acuerdo con la autorización y circunstancias personales

Asimismo, las tarjetas inteligentes pueden almacenar expedientes médicos, información para casos de emergencia y situación en materia de seguros de enfermedad.

Aplicaciones de control

Además de los usos frecuentes, la tarjeta inteligente permite su aplicación en distintos sistemas de control de accesos. Entre ellos:

- **Recursos Humanos:** Permite reunir y administrar datos de los empleados de una empresa, dando acceso inmediato e intuitivo a una segura y detallada información de cada uno de sus empleados o lugares por divisiones, por secciones o por cargo.

- **Control de presencia:** La consolidación en el ámbito de los recursos humanos y de la cultura empresarial de conceptos como el del capital humano están cambiando la visión del departamento de personal. Las tarjetas inteligentes son una ayuda para la adaptación a estos cambios.

- **Seguridad:** La autenticación del personal ayuda a combatir el fraude en la entrada o salida de personal. Su función de backup, además, asegura la custodia de los datos.

- **Controles de acceso físico:** Apertura de puertas y horario, registro por fotografía y acceso por huella digital.

- **Control de PC:** Protección de acceso a la computadora y bloqueo en caso de retirar la tarjeta con protección por huella digital.

- **Control informático de aplicaciones:** Permite proteger la información y el uso del software de la empresa: una vez dentro de la aplicación cada tarjeta permite el acceso a determinados datos. Cumple casi al 100% de los requerimientos más rigurosos de seguridad.

- **Internet:** Control de navegación en internet *(sistema prepago)* y control de acceso al ordenador. Este es un programa desarrollado para la gestión de cybercafés o bibliotecas, donde la navegación virtual o uso de software estén sujetos a cobro o tiempo. ☒

La tarjeta inteligente permite su aplicación en distintos sistemas de control de accesos, la autenticación del personal por medio de la misma ayuda a combatir el fraude en la entrada o salida de personal. Su función de backup, además, asegura la custodia de los datos.

*(1) **DES** (Data Encryption Standard): Es uno de los sistemas criptográficos más utilizados en todo el mundo. Su verdadera importancia reside en la aceptación que ha tenido en el mercado criptográfico, ya que fue uno de los primeros intentos por parte del gobierno de los Estados Unidos por implantar un estándar para transmitir datos digitales de una forma segura.*

*(2) **RSA** es un algoritmo de clave pública. Sirve tanto para cifrar como para realizar firmas digitales. Es uno de los pocos algoritmos que se pueden implementar y comprender de una manera sencilla. Su nombre se debe a las iniciales de sus tres inventores, Rivest, Shamir y Adleman, los cuales crearon el algoritmo en 1978. La verdadera fortaleza del sistema radica en la dificultad de obtener la clave privada a partir de los datos públicos del sistema.*

*(3) **ZKPI** (Zero knowledge proof identity): Es un protocolo criptográfico que permite demostrar la identidad de un interlocutor sin que un espía obtenga información que le permita suplantarlo en el futuro. El problema de la identificación por nombre de usuario y clave es que un espía que escuche una vez las comunicaciones obtiene la información suficiente para suplantar al legitimo usuario. El protocolo ZPKI obvia este problema impidiendo un ataque tan simple como escuchar las comunicaciones cuando se está ejecutando el protocolo de demostración de identidad.*