

Tarjeta inteligente

Una **tarjeta inteligente** (*smart card*), o tarjeta con circuito integrado (TCI), es cualquier tarjeta del tamaño del bolsillo con circuitos integrados, que permite la ejecución de cierta lógica programada. Aunque existe un diverso rango de aplicaciones, hay dos categorías principales de TCI. Las tarjetas de memoria contienen solo componentes de memoria no volátil y posiblemente alguna lógica de seguridad. Las tarjetas microprocesadoras contienen memoria y microprocesadores.

La percepción estándar de una tarjeta inteligente se corresponde con la de una tarjeta microprocesadora, de las dimensiones de una tarjeta de crédito (o más pequeña, como por ejemplo, del tamaño de tarjetas SIM o GSM), con varias propiedades especiales (ej. un procesador criptográfico seguro, sistema de archivos seguro, y características legibles por humanos), la que, entre otras cosas, es capaz de proveer servicios de seguridad (ej. confidencialidad de la información en la memoria).

Este tipo de tarjetas no contienen ni necesitan baterías; la energía es suministrada por los lectores de las propias tarjetas.

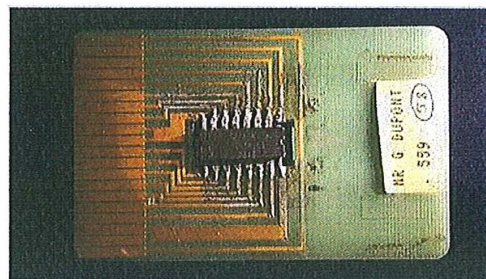
Historia

Las *Tarjetas inteligente* fueron desarrolladas y patentadas en los años setenta. Existen algunas discusiones de quién es el "inventor" original; entre los que se encuentran Juergen Dethloff y Helmut Gröttrup de Alemania, Kunitaka Arimura de Japón y Roland Moreno de Francia.

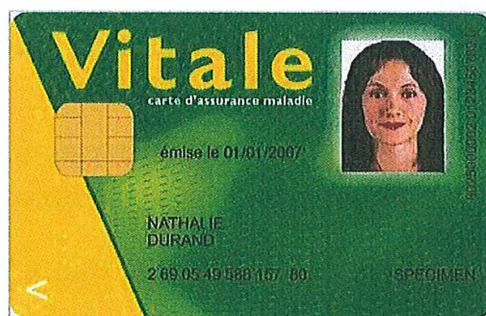
El primer uso masivo de las tarjetas fue para el pago telefónico público en Francia, en el año 1983. Desde los años 1970, la historia de las tarjetas inteligentes ha reflejado los constantes avances en capacidades técnicas y ámbitos de aplicabilidad.

El mayor auge de las tarjetas inteligentes fue en los años noventa, con la introducción de las tarjetas SIM utilizadas en la telefonía móvil GSM en Europa.

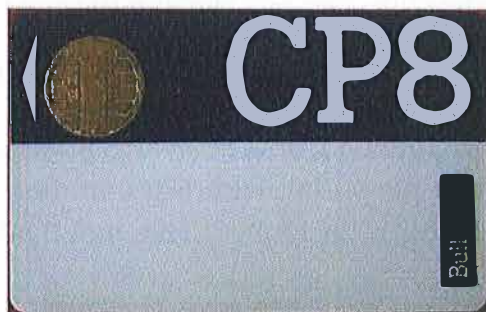
Las firmas internacionales MasterCard, Visa, y Europay, publicaron un estándar de interoperabilidad para el pago con tarjetas inteligentes en 1996, que fue revisado en el año 2000. Este estándar llamado EMV, se ha introducido mundialmente de manera gradual, con la esperanza de reemplazar las tarjetas basadas en cintas magnéticas. Actualmente, las especificaciones EMV



Uno de los primeros prototipos de tarjeta inteligente, realizado por su inventor Roland Moreno en 1975. Demuestra como, en una tarjeta inteligente, cada "pata" del microcircuito (al centro) está conectada con un contacto (elementos dorados) que la relaciona con el mundo exterior.



Carte Vitale con fotografía del asegurado (tarjeta inteligente de salud en Francia).



Tarjeta inteligente Bull con microcircuito monochip (1983).

son costosas de implementar, con el único beneficio de la reducción del fraude. Algunos críticos aseguran que los ahorros son mucho menores que los costos de implementar EMV, y muchos creen que la industria optará por esperar que termine el actual ciclo de vida del EMV, para implementar una nueva tecnología sin contacto.

Las tarjetas inteligentes con interfaces sin contacto, están transformándose en un medio popular para aplicaciones de pago como el transporte masivo. Estándares de este tipo de interoperabilidad han sido publicados y aplicados en el Reino Unido y en Europa IOPTA.

Las tarjetas inteligentes también se han utilizado para identificar al personal de las empresas. Las tarjetas de identificación y el permiso de conducir, están prevaleciendo más y más, por ejemplo, en Malasia con la tarjeta inteligente multipropósito Mykad, la que es usada a escala nacional (18 millones de tarjetas) para manejar todo en una sola tarjeta: identificación personal, licencia de conducir, tarjeta de seguro, y pago (*ePurse*) para transporte público e información de viajero.

Los circuitos integrados RFID, parecidos en concepto a las tarjetas inteligentes, se están implantando en los denominados pasaportes biométricos, y contienen información personal para su lectura automática.

Cronología

En 1970 el Dr Kunitaka Arimura presentó en Japón la primera y única patente en el concepto de tarjeta inteligente.

En 1974 Roland Moreno presentó en Francia la patente original de la tarjeta chip (con un circuito integrado), más tarde bautizado como *tarjeta inteligente*.

En 1977 tres fabricantes, Bull CP8, SGS Thomson, y Schlumberger, comenzaron a desarrollar tarjetas chip.

En 1979 Motorola desarrolló el primer chip seguro para su uso en la banca francesa.

En 1982 se realizaron en Francia ensayos con tarjetas de memoria para usar en teléfonos (France Télécom; ésta fue la primera gran prueba de las tarjetas chip).

En 1984 se realizaron con éxito, pruebas en cajeros automáticos con tarjetas chip bancarias.

En 1986, 14 000 tarjetas equipadas con el Bull CP8 se distribuyeron a los clientes del Banco de Virginia y Maryland National Bank. Además, 50 000 tarjetas Casio se distribuyeron a los clientes del Palm Beach First National Bank y el Mall Bank.

En 1987 se implantó el primer proyecto a gran escala de tarjetas inteligentes en los Estados Unidos, con la *Peanut Marketing Card* del Departamento de Agricultura del país.

En 1988 se creó la primera tarjeta bancaria con el algoritmo criptográfico DES para *Carte Bancaire*.

En 1992 se lanzó un proyecto de monedero electrónico prepago (DANMONT), el que se inició en Dinamarca.

En 1993 se implementaron proyectos piloto de múltiples aplicaciones de tarjetas inteligentes en Rennes, Francia, donde la función *Telecarte* (para teléfonos públicos) fue habilitado en una tarjeta bancaria.

En 1994, Europay, MasterCard y Visa (EMV) publicaron la primera versión de las especificaciones de interoperabilidad de las aplicaciones bancarias de las tarjetas inteligentes. Al mismo tiempo, Alemania comenzó la emisión de 80 millones de tarjetas con chip de memoria para las tarjetas sanitarias de sus ciudadanos.

En 1995, ya había más de 3 millones de abonados de teléfonos móviles en todo el mundo (con tarjetas chip SIM GSM).

En 1996, más de 1,5 millones de tarjetas monedero VISACash se emitieron en los Juegos Olímpicos de Atlanta. MasterCard y Visa entonces desarrollaron por separado sus tecnologías y participan en EMV para intentar forzar la interoperabilidad: la Java Card respaldada por Visa, y la aplicación de múltiples sistemas operativos (MULTOS) respaldada por MasterCard.

En 1998, la Administración de Servicios Generales y de la Marina de los Estados Unidos unieron sus fuerzas y pusieron en marcha un sistema administrativo de gestión basado en una tarjeta inteligente, para así demostrar y evaluar la integración de múltiples aplicaciones de tarjetas inteligentes con otros tipos de tecnología y su aplicabilidad en la administración electrónica en el Gobierno Federal. Además y por su parte, Francia inició la aplicación experimental de una tarjeta inteligente de salud para sus 50 millones de ciudadanos.

En 2001, el Departamento Nacional de Identificación de Malasia desplegó a nivel masivo su sistema multipropósito de identificación por tarjetas inteligentes Mykad, incorporando en una sola tarjeta: banca, micropagos, identificación nacional, pago de transporte público, información de salud, licencia de conducir, e información de viajero.

Clasificaciones

Tipos de tarjetas según sus capacidades

Según las capacidades de su chip, las tarjetas más habituales son:

- **Memoria:** tarjetas que únicamente son un contenedor de ficheros pero que no albergan aplicaciones ejecutables. Por ejemplo, MIFARE. Éstas se usan generalmente en aplicaciones de identificación y control de acceso sin altos requisitos de seguridad.
- **Microprocesadas:** tarjetas con una estructura análoga a la de un ordenador (procesador, memoria volátil, memoria persistente). Estas tarjetas albergan ficheros y aplicaciones, y suelen usarse para identificación y pago con monederos electrónicos.
- **Criptográficas:** tarjetas microprocesadas avanzadas en las que hay módulos hardware para la ejecución de algoritmos usados en cifrados y firmas digitales. En estas tarjetas, es posible almacenar de forma segura un certificado digital (y su clave privada), a efectos de firmar documentos o autenticarse con la tarjeta, sin que el certificado salga de la tarjeta (o sea y por ejemplo, sin que se instale en el almacén de certificados de un navegador web) ya que es el

procesador de la propia tarjeta el que realiza la firma. Un ejemplo de estas tarjetas son las emitidas por la Fábrica Nacional de Moneda y Timbre (FNMT) española para la firma digital.

Tipos de tarjetas según la estructura de su sistema operativo

- *Tarjetas de memoria.* Tarjetas que únicamente son un contenedor de ficheros pero que no albergan aplicaciones ejecutables. Disponen de un sistema operativo limitado con una serie de comandos básicos de lectura y escritura de las distintas secciones de memoria, y pueden tener capacidades de seguridad para proteger el acceso a determinadas zonas de memoria.
- *Basadas en sistemas de ficheros, aplicaciones y comandos.* Estas tarjetas disponen del equivalente a un sistema de ficheros compatible con el estándar ISO/IEC 7816 parte 4 y un sistema operativo en el que se incrustan una o más aplicaciones (durante el proceso de fabricación) que exponen una serie de comandos que se pueden invocar a través de APIs de programación.
- *Java Cards:* Una Java Card es una tarjeta capaz de ejecutar mini-aplicaciones Java. En este tipo de tarjetas, el sistema operativo es una pequeña máquina virtual Java (JVM) y en ellas se pueden cargar dinámicamente aplicaciones desarrolladas específicamente para este entorno.

Tipos de tarjetas según el formato (tamaño)

En el estándar *ISO/IEC 7816* parte 1, se definen los siguientes tamaños para tarjetas inteligentes:

- *ID 000* : el de las tarjetas SIM usadas para los teléfonos móviles GSM. También acostumbran a tener este formato las tarjetas SAM (*Security Access Module*) utilizadas para la autenticación criptográfica mutua de tarjeta y terminal.
- *ID 00* : un tamaño intermedio poco utilizado comercialmente.
- *ID 1* : el tamaño más habitual, que se corresponde con el de las tarjeta de crédito.

Tipos de tarjetas según la interfaz

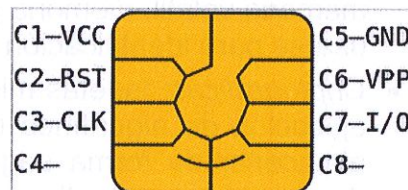
Tarjeta inteligente de contacto

Véase también: Documento de identidad electrónico

Estas tarjetas disponen de unos contactos metálicos visibles y debidamente estandarizados (parte 2 de la *ISO/IEC 7816*). Estas tarjetas, por tanto, deben ser *insertadas* en una ranura de un lector, a efectos de poder operar con ellas. A través de estos contactos, el lector alimenta eléctricamente a la tarjeta y transmite los datos oportunos para operar con ella conforme al estándar.

La serie de estándares *ISO/IEC 7816* e *ISO/IEC 7810* definen:

- La forma física (parte 1)
- La posición de las formas de los conectores eléctricos (parte 2)
- Las características eléctricas (parte 3)
- Los protocolos de comunicación (parte 3)
- El formato de los comandos (ADPU's) enviados a la tarjeta y las respuestas retornadas por la misma
- La dureza de la tarjeta
- La funcionalidad



Contactos del *chip* de una «tarjeta con contactos»

Los lectores de tarjetas inteligentes de contacto son utilizados como un medio de comunicación entre la tarjeta inteligente y un anfitrión, como por ejemplo una computadora.

Tarjetas inteligentes sin contacto

El segundo tipo es la tarjeta inteligente sin contacto mediante etiquetas RFID en el cual el chip se comunica con el lector de tarjetas mediante inducción a una tasa de transferencia de 106 a 848 Kb/s).

El estándar de comunicación de tarjetas inteligentes sin contacto es el ISO/IEC 14443 del año 2001, que define dos tipos de tarjetas sin contacto (A y B), permitidos para distancias de comunicación de hasta 10 cm. Ha habido propuestas para la ISO 14443 tipos C, D, E y F que todavía tienen que completar el proceso de estandarización. Un estándar alternativo de tarjetas inteligentes sin contacto es el ISO 15693, el cual permite la comunicación a distancias de hasta 50 cm. Las más abundantes son las tarjetas de la familia MIFARE de Philips, las cuales representan a la ISO/IEC 14443-A.

Un ejemplo del amplio uso de tarjetas inteligentes sin contacto es la tarjeta Octopus en Hong Kong, la cual usa el estándar anterior al ISO/IEC 14443.

Las tarjetas inteligentes sin contacto son una evolución de la tecnología usada desde hace años por los RFID (identificación por radio frecuencia - radio frequency identificación), añadiéndoles dispositivos que los chip RFID no suelen incluir, como memoria de escritura o micro controladores.

Tarjetas híbridas y duales

Una *tarjeta híbrida* es una tarjeta sin contactos (*contactless*) a la cual se le agrega un segundo *chip* de contacto. Ambos *chips* pueden ser microprocesadores o simples *chips* de memoria. El *chip* sin contacto es generalmente usado en aplicaciones que requieren transacciones rápidas. Por ejemplo el transporte, mientras que el *chip* de contacto es generalmente utilizado en aplicaciones que requieren de alta seguridad como las operaciones bancarias. Un ejemplo es la tarjeta de identificación llamada MyKad en Malasia, que usa un *chip* Proton de contacto y un chip sin contacto MIFARE (ISO 14443A).

Una tarjeta de *interfaz dual* es similar a la tarjeta híbrida en que la tarjeta presenta ambas interfaces con y sin contacto. La diferencia más importante es el hecho de que la tarjeta de interfaz dual tiene un solo circuito integrado. Un ejemplo es la Oberthur Cosmo Card Dual-Interface.

Aplicaciones comerciales

Las tres aplicaciones fundamentales de las tarjetas inteligentes son:

- *Identificación* del titular de la misma.
- *Pago* electrónico de bienes o servicios mediante dinero «virtual».
- *Almacenamiento seguro* de información asociada al titular.

Las aplicaciones de las tarjetas inteligentes incluyen su uso como tarjeta de crédito, SIM para telefonía móvil, tarjetas de autorización para televisión por pago, identificación de alta seguridad, tarjetas de control de acceso, y como tarjetas de pago del transporte público.

Las tarjetas inteligentes también son muy utilizadas como un monedero electrónico. Estas aplicaciones disponen normalmente de un fichero protegido que almacena un contador de saldo y comandos para decrementar e incrementar el saldo (esto último solo con unas claves de seguridad especiales, obviamente). Con esta aplicación, el circuito integrado de la tarjeta inteligente puede ser «cargado» con dinero, que puede ser utilizado en parquímetros, máquinas expendedoras, etc. El intercambio de dinero entre la tarjeta inteligente y la máquina receptora es protegido por protocolos criptográficos.

Cuando las tarjetas son criptográficas, las posibilidades de identificación y autenticación se multiplican, ya que se pueden almacenar de forma segura certificados digitales o características biométricas en ficheros protegidos dentro de la propia tarjeta, de modo que estos elementos privados nunca salgan de la tarjeta, pues las operaciones de autenticación a través del propio chip criptográfico de la tarjeta.

De un modo más particular, las aplicaciones más habituales son:

- *Identificación digital*: este tipo de aplicaciones se utilizan para validar la identidad del portador de la tarjeta en un sistema centralizado de gestión.
- *Control de acceso*: este tipo de aplicaciones se utilizan para restringir o permitir el acceso a una determinada área, en función de distintos parámetros que pueden estar grabados en la tarjeta, o pueden ser recuperados de un sistema central de gestión a partir de la identidad grabada en la tarjeta. Este tipo de aplicaciones suelen estar ligadas a puertas o tornos automatizados, que permiten/impiden el paso físico de una persona a una determinada área, si bien también tiene sentido este servicio en el ámbito de la autenticación en sistemas informáticos (webs, sistemas operativos, etcétera). En este último caso, la frontera entre las aplicaciones de identificación y de control de acceso es difusa.
- *Monedero electrónico (electronic purse o electronic wallet, ePurse y eWallet)*: esta aplicación se utiliza como dinero electrónico. Se puede cargar una cierta cantidad de dinero (en terminales autorizados que dispongan de las claves de seguridad oportunas), y luego, sobre esta cantidad de dinero se pueden realizar operaciones de débito o consulta de modo que puede ser utilizado para el pago o cobro de servicios o bienes.
- *Firma digital*: este tipo de aplicaciones permiten almacenar un certificado digital de forma segura dentro de la tarjeta, y firmar con él documentos electrónicos sin que en ningún momento el certificado (y más concretamente su clave privada) salgan del almacenamiento seguro en el que están confinados. Con estas aplicaciones se abre todo un abanico de posibilidades en el campo de la Administración electrónica.
- *Fidelización de clientes*: Este tipo de aplicación sirve a las empresas que ofrecen servicios o descuentos especiales para clientes que hacen uso de la tarjeta, para así poder validar la identidad del cliente, y para descentralizar la información. Suponiendo que se tiene un sistema de puntos acumulables canjeables por bienes o servicios, en el cual participan varias empresas, esto simplifica mucho el tratamiento de los datos, evitando tener que compartir una gran base de datos, o tener que realizar réplicas de las distintas bases (los puntos se podrían guardar en la propia tarjeta).
- *Sistemas de prepago*: En estos sistemas, un cliente *carga* su tarjeta con una cierta *cantidad de servicio*, la cual va siendo debitada a medida que el cliente hace uso del servicio. El servicio puede variar desde telefonía móvil hasta TV por cable, pasando por acceso a sitios web o de transporte público.
- *Tarjetas sanitarias*: En algunos hospitales y sistemas nacionales de salud, ya se está implementando un sistema de identificación de pacientes y almacenamiento de los principales datos de la historia clínica de los mismos en tarjetas inteligentes, a efectos de agilizar la atención. Actualmente, la capacidad de almacenamiento es muy limitada, pero en un futuro

quizás se podría almacenar toda la historia dentro de la tarjeta. Es el caso de la tarjeta ONA de Osakidetza, en el País Vasco.

Nótese, en cualquier caso, que todos estos servicios pueden ser derivados de los tres puntos planteados inicialmente (identificación, pago y almacenamiento seguro).

Estructura de una tarjeta inteligente microprocesada

Internamente, el chip de una tarjeta inteligente microprocesada se compone de:

- Unidad central de procesamiento (*CPU, central processing unit*): el procesador de la tarjeta, suele ser de 8 bits, a 5 MHz y 5 voltios. Pueden tener opcionalmente módulos hardware para operaciones criptográficas.
- Memoria de solo lectura (*ROM, read-only memory*): memoria interna (normalmente entre 12 y 30 KB) en la que se incrusta el sistema operativo de la tarjeta, las rutinas del protocolo de comunicaciones, y los algoritmos de seguridad de alto nivel por software. Esta memoria, como su nombre indica, no se puede reescribir, y se inicializa durante el proceso de fabricación.
- EEPROM: memoria de almacenamiento (equivalente al disco duro en una computadora personal) en el que está grabado el sistema de ficheros, los datos usados por las aplicaciones, las claves de seguridad, y las propias aplicaciones que se ejecutan en la tarjeta. El acceso a esta memoria está protegido a distintos niveles por el sistema operativo de la tarjeta.
- Memoria de acceso aleatorio (*RAM, random access memory*): memoria volátil de trabajo del procesador.

Proceso de fabricación

La fabricación de tarjetas inteligentes abarca normalmente los siguientes pasos:

1. Fabricación de los *chips* en una oblea. Varios miles de circuitos integrados se fabrican a la vez en la forma de obleas de silicio con aproximadamente 3000 a 4000 unidades.
2. Empaquetado de los *chips* individuales para su inserción en una tarjeta. Una vez que se termina una oblea, cada chip se prueba individualmente, se divide la oblea y se realizan las conexiones eléctricas del chip.
3. Fabricación de la tarjeta: la tarjeta está compuesta de cloruro de polivinilo o de un material similar. Las características químicas y las dimensiones de la tarjeta y sus tolerancias son reguladas por estándares internacionales. El material de la tarjeta se produce en una hoja grande, plana del grosor prescrito. Para muchos tipos de tarjetas producidas en serie, estas hojas entonces se imprimen con los elementos gráficos comunes a todas las tarjetas. Las tarjetas individuales entonces se cortan de esta hoja plana y los bordes de cada tarjeta se lijan.
4. Inserción del *chip* en la tarjeta: una vez que el *chip* y la tarjeta estén preparados, los dos se unen: se hace un agujero en la tarjeta, y el chip se pega en él con pegamento.
5. Prepersonalización: una vez la tarjeta está completa, la mayoría de los usos inteligentes de la misma requieren que ciertos ficheros de los programas o de datos estén instalados en cada *chip* (tarjeta) antes de que la tarjeta se pueda personalizar para un titular específico. Esta preparación general del software o de los archivos en la tarjeta se hace con una operación llamada «prepersonalización», que se hace a través de los contactos del chip y por lo tanto puede proceder solamente a la velocidad proporcionada por esa interfaz.
6. Personalización: El procedimiento de la personalización implica el poner de la información tal como nombres, perfiles o números de cuenta en la tarjeta; a partir de la realización de este proceso la tarjeta está asignada a una persona en particular. Normalmente esta personalización será gráfica (estampando o troquelando datos personales del titular sobre la

superficie plástica de la tarjeta) o eléctrica (grabando información personal del titular en algún archivo de la tarjeta).

Seguridad

La seguridad es una de las propiedades más importantes de las tarjetas inteligentes y se aplica a múltiples niveles y con distintos mecanismos. Cada fichero lleva asociadas unas condiciones de acceso y deben ser satisfechas antes de ejecutar un comando sobre ese fichero.

En el momento de personalización de la tarjeta (durante su fabricación) se puede indicar qué mecanismos de seguridad se aplican a los ficheros. Normalmente se definirán:

- Ficheros de acceso libre.
- Ficheros protegidos por claves: pueden definirse varias claves con distintos propósitos. Normalmente se definen claves para proteger la escritura de algunos ficheros y claves específicas para los comandos de consumo y carga de las aplicaciones de monedero electrónico. De ese modo la aplicación que intente ejecutar comandos sobre ficheros protegidos tendrá que negociar previamente con la tarjeta la clave oportuna.
- Ficheros protegidos por *PIN*: el *PIN* es un número secreto que va almacenado en un fichero protegido y que es solicitado al usuario para acceder a este tipo de ficheros protegidos. Cuando el usuario lo introduce y el programa se lo pasa a la operación que va a abrir el fichero en cuestión el sistema valida que el *PIN* sea correcto para dar acceso al fichero.

Finalmente, indicar que la negociación de claves se realiza habitualmente apoyándose en un módulo *SAM*, que no deja de ser otra tarjeta inteligente en formato ID-000 alojada en un lector interno propio dentro de la carcasa del lector principal o del TPV y que contiene aplicaciones criptográficas que permiten negociar las claves oportunas con la tarjeta inteligente del usuario. Operando de este modo se está autenticando el lector, la tarjeta y el módulo *SAM* involucrados en cada operación.

Modelos de programación

Al aproximarse a la programación de tarjetas inteligentes hay que distinguir dos ámbitos claramente diferenciados:

- Programación de aplicaciones para el circuito integrado de la tarjeta, es decir, de aplicaciones que se almacenan y ejecutan dentro del chip de la tarjeta cuando ésta recibe alimentación eléctrica de un lector.
- Programación de aplicaciones para los sistemas en los que se utiliza la tarjeta, esto es, aplicaciones que se ejecutan en ordenadores (en un sentido genérico, ya que pueden ser TPV empotrados, cajeros automáticos, computadoras personales, etc.) a los que se conecta un lector de tarjetas en el que se inserta (o aproxima si es un lector sin contactos) una tarjeta inteligente. Estas aplicaciones se comunican con el lector, el cual se comunica con la tarjeta y sus aplicaciones.

Programación de aplicaciones para el chip de la tarjeta

Este tipo de programación es de muy bajo nivel y depende normalmente del tipo y proceso de fabricación de las propias tarjetas. En la mayoría de las tarjetas inteligentes el sistema operativo de la tarjeta y las aplicaciones que van dentro del chip se cargan en el propio proceso de fabricación y no pueden ser luego modificadas una vez que la tarjeta ha sido fabricada.

Una excepción clara a este caso pueden ser las Java Cards, que son tarjetas que en el proceso de fabricación incorporan un sistema operativo y una máquina virtual Java específica para este entorno. Una vez fabricada la tarjeta, los desarrolladores pueden implementar miniaplicaciones (applets) Java para ser cargadas en la tarjeta (mediante un procedimiento que garantice la seguridad del sistema).

Programación de aplicaciones para los sistemas en los que se utiliza la tarjeta

Existen varias APIs de programación estandarizadas para comunicarse con los lectores de tarjetas inteligentes desde un ordenador. Las principales son:

- PC/SC (*Personal Computer/Smart Card*), especificado por el PC/SC Workgroup. Existe una implementación para Microsoft Windows y también el proyecto MUSCLE proporciona una implementación casi completa de esta especificación para los sistemas operativos GNU Linux-UNIX.
- OCF (*OpenCard Framework*), especificado por el grupo de empresas OpenCard. Este entorno intenta proporcionar un diseño orientado a objetos fácilmente extensible y modular. El consorcio OpenCard publica el API y proporciona una implementación de referencia en Java. Existe un adaptador para que OCF trabaje sobre PC/SC.

En ambos casos, el modelo de programación que utilizan las tarjetas inteligentes está basado en protocolos de petición-respuesta. La tarjeta (su software) expone una serie de comandos que pueden ser invocados. Estos comandos interactúan con los ficheros que subyacen a cada aplicación de la tarjeta y proporcionan un resultado. Desde el terminal se invocan estos comandos a través de cualquiera de las APIs antes descritas componiendo APDUs (*Application Protocol Data Unit* - comandos con parámetros) que son enviados a la tarjeta para que ésta responda.

Véase también

-
- | | |
|--------------------|---|
| ▪ <u>EMV</u> | ▪ <u>Near field communication (NFC)</u> |
| ▪ <u>ISO 7816</u> | ▪ <u>Tarjeta SIM</u> |
| ▪ <u>ISO 14443</u> | ▪ <u>Tarjeta monedero</u> |
| ▪ <u>Java Card</u> | ▪ <u>UICC</u> |
| ▪ <u>Mifare</u> | |

Enlaces externos

-
-  Wikimedia Commons alberga una categoría multimedia sobre **Tarjeta inteligente**.
 - Open Card Framework (OCF) (<https://www.openscdp.org/ocf/>) (en inglés)
 - PC/SC Workgroup (<http://www.pcscworkgroup.com>) (en inglés)
 - Tutorial de las tarjetas inteligentes (<http://www.smartcardbasics.com>) (en inglés)
 - Introducción a las tarjetas inteligentes (<http://sumitdhar.blogspot.com/2004/11/introduction-to-smart-cards.html>) (en inglés)
 - Smart Card Alliance (<http://www.smartcardalliance.org>) (en inglés)
-

Obtenido de «https://es.wikipedia.org/w/index.php?title=Tarjeta_inteligente&oldid=158057656»

▪

