



Tarjetas Inteligentes (*Smart Card*)



Agenda

- Antecedentes.
- ¿Que es una tarjeta inteligente (*smart-card*) ?.
- Tipos de Tarjetas inteligentes
- Componentes de una tarjeta inteligente
- Descripción del CHIP
- ¿Como acceder a la información almacenada en el chip?
- Tarjetas Inteligentes y PKI
- ¿Como funciona ?
- Capaz básicas que la componen.
- Sistemas operativos
- Aplicaciones
- Beneficios
- Estándares

Antecedentes.

- Tarjetas en década de 1950. Primero sólo plástico, luego banda magnética
- J. Dethloff y H. Grotrupp en 1968: Circuito integrado incorporado a tarjeta
- K. Arimura en 1970: Integración de lógica aritmética y almacén en chip
- R. Moreno en 1974: Patente actual, vendida a Bull
- Primer prototipo en 1979
- Primeras tarjetas telefónicas en 1983
- Primeras tarjetas de débito en 1984
- Estándares ISO (ref 7816-X) en 1987
- Primera versión de especificación EMV para aplicaciones financieras en 1994 (última actualización en 2004)
- Primer monedero electrónico en 1997
- Primeras “tarjetas Java” en 1998

¿Que es una Tarjeta Inteligente?



Básicamente una Tarjeta Inteligente es una tarjeta plástica del tamaño de una tarjeta de crédito convencional, que contiene un pequeño microprocesador, que es capaz de hacer diferentes cálculos, guardar información y manejar programas, que están protegidos a través de mecanismos avanzados de seguridad.

Debemos distinguir entre lo que es una Tarjeta Inteligente y lo que es una Tarjeta Chip. No se trata de lo mismo, ya que el chip no es lo que la hace "Inteligente", si no el microprocesador, por esto existen diferentes tipos de tarjetas, de las cuales, unas son "Inteligentes", y otras son de "memoria".



Tipos de tarjetas Inteligentes

- Según **función**:

De **memoria**

- Portadora de **datos**
 - Accesibles mediante protocolo síncrono
 - Su transmisión es vulnerable
 - Pueden estar cifrados
- Tipos:
 - **Directa**
 - No inteligente
 - **Protegida**:
 - Acceso restringido a partes
 - Valor almacenado con contador
 - Desechables o recargables
 - **Óptica**:
 - Mayor capacidad: varios MB
 - Sólo 1 escritura
 - Muy caras
- **Componentes**:
 - EEPROM
 - ROM
 - Lógica de seguridad integrada

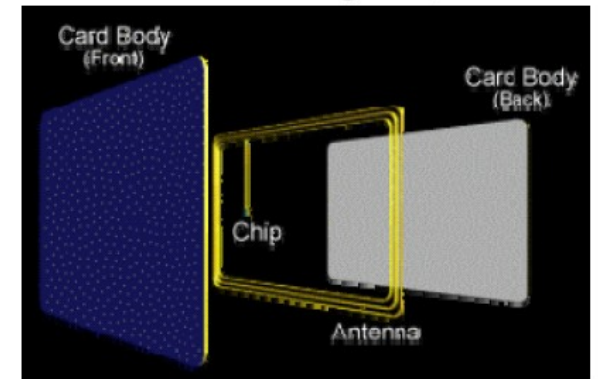
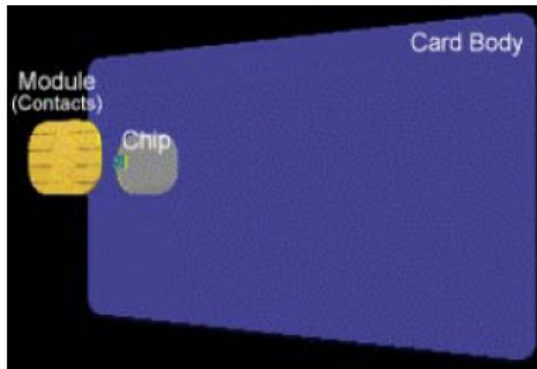
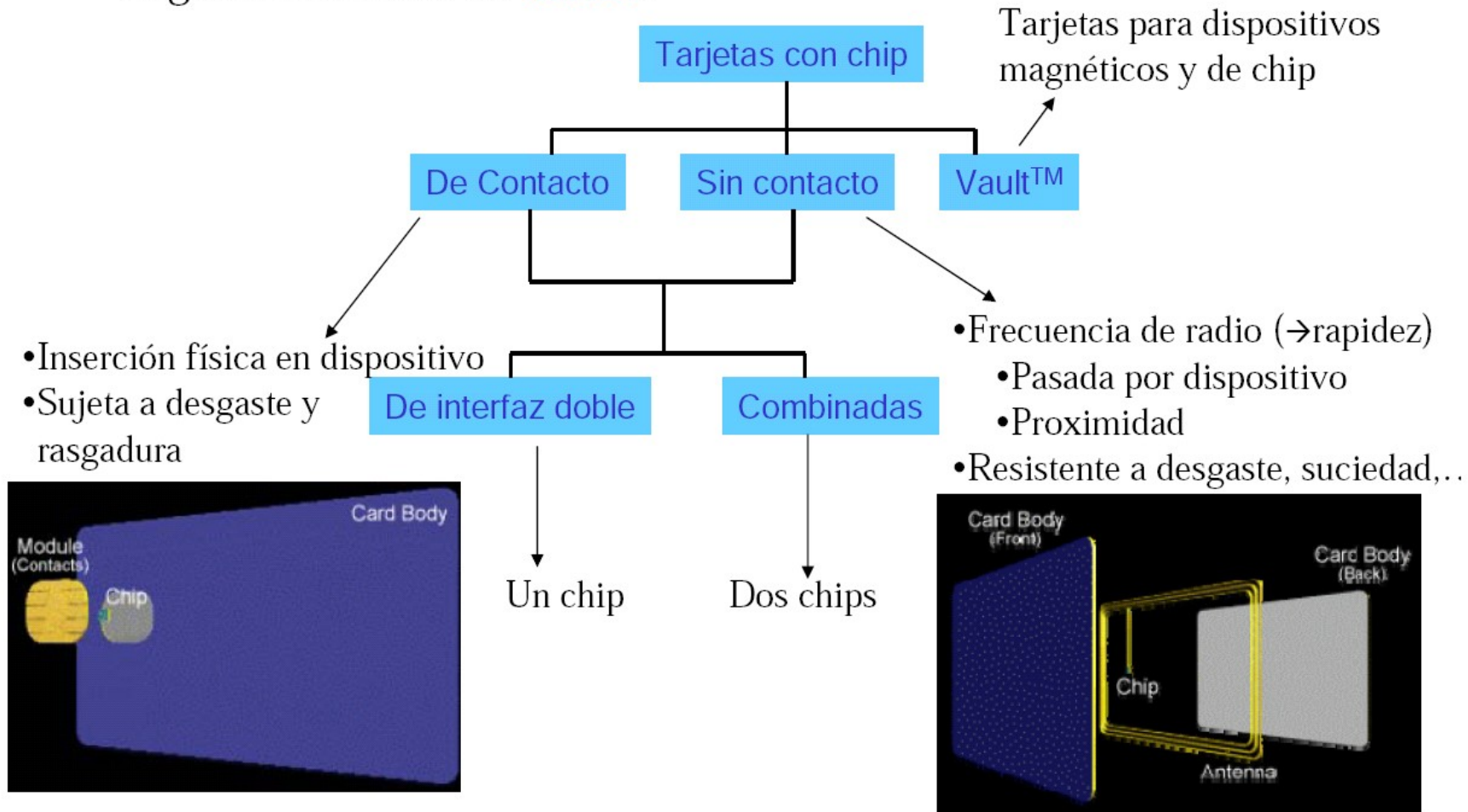
Con **microprocesador**

- Portadora de **datos** y realizadora de **tareas**:
 - Leer
 - Escribir
 - Cifrar
 - ...
- Interacción entre tarjeta y máquina
 - ¿Tarjeta autorizada para sistema?
 - Usuario autenticado
 - Credenciales de tarjeta/máquina para realizar transacción
- **Componentes**:
 - EEPROM
 - ROM
 - RAM
 - CPU
 - Lógica de seguridad integrada

Autenticación. Tarjetas inteligentes

Tipos de tarjetas Inteligentes (cont.)

- Según mecanismo de **acceso**:



Tipos de tarjetas Inteligentes (cont.)



- Según **tamaño**:

- Tarjeta: tarjeta de banda magnética
- Minitarjeta: billete con cinta magnética
- Módulo: tamaño mínimo para albergar chip y sus contactos

- Según **forma**:

- Tarjeta
- Testigo USB
- Anillo
- Llave
- ...



<http://kalysis.com/hardware/>



<http://www.useit.com/papers/javaring.html>



<http://www.maxim-ic.com/products/ibutton/>

Componentes

SO:

- Gestión de memoria y archivos
- Protección de acceso
- Procesamiento de órdenes y comunicaciones
- Gestión de aplicaciones

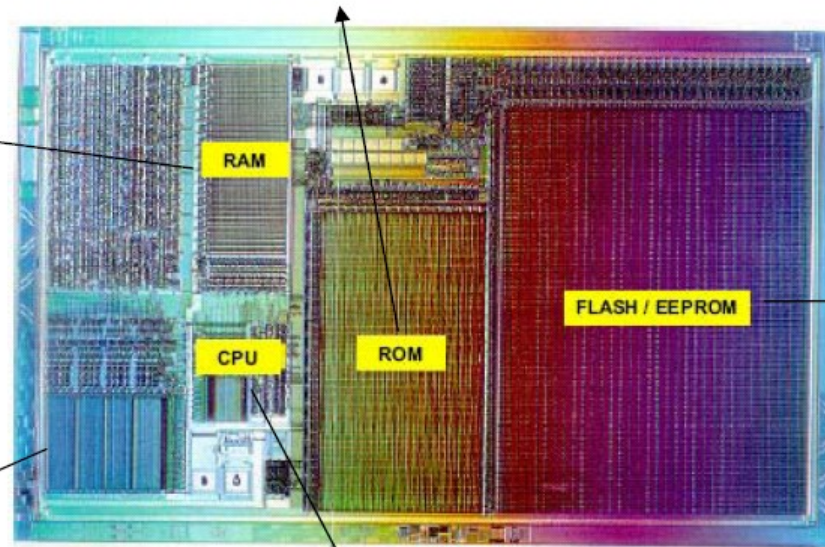
- Estructura de archivos fija
- Sistema de aplicación dinámica

Datos:

- Zona **abierta**: acceso no restringido. Accesible al contactar con lector
- Zona **protegida**: acceso restringido (titular, emisor, ambos). Accesible tras autenticación
- Zona **secreta**: sin acceso (nadie: ni portador, ni emisor)

Programas específicos

Memoria de **trabajo**



Interfaz **E/S**:

Transferencia semiduplex bit a bit

A veces con

procesador matemático
para criptografía

CHIP

VCC		GND
RST		VPP
CLK		I/O
RFU		RFU

El Chip cuenta con 8 diferentes puntos de contacto. La forma y distribución de estos puntos de contacto, varía de acuerdo al fabricante, pero de todas formas conservan las mismas funciones. VCC es la fuente de poder del chip. RST es el Reset. CLK (Clock) es el reloj. Los dos puntos RFU (Reserved for Future Use) son puntos reservados para un uso futuro. GND (ground) es la "tierra" del Chip. VPP es el punto donde se encuentra la memoria EEPROM. Por último, I/O es el Input Output del Chip.

¿Como acceder a la información del chip?



- **Lector** (*reader*): necesita PC

- **Interfaz** entre tarjeta y máquina

- Puerto serie RS232
- Puerto USB
- Ranura PCMCIA
- Ranura de disquete
- Puerto paralelo
- Puerto infrarrojo
- Incorporado a teclado

- Proporciona **energía** eléctrica a tarjeta



- **Terminal** (*terminal*): **autosuficiente**

- Suelen tener SO y herramientas propios

- Otras funciones también:

- Módem
- Lectura de banda magnética
- Impresión de transacciones



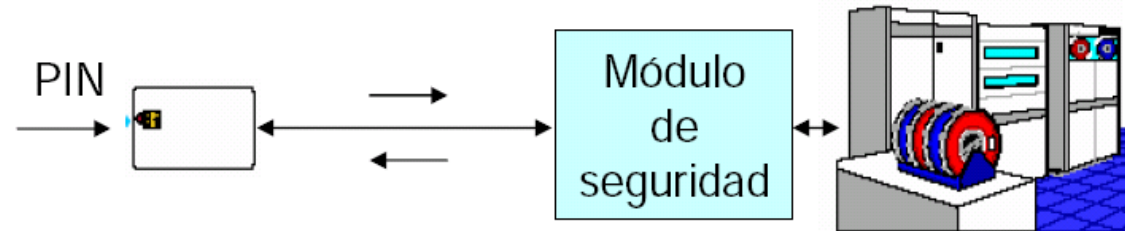
- **Leen y escriben**

- **No estandarización:**

- Protocolo de comunicación distinto para cada fabricante
- Universales o especializados



Tarjetas Inteligentes y PKI



- **Confidencialidad, integridad y disponibilidad**
 - Mediante criptografía:
 - Firma RSA, DSA, DES usado como MAC, funciones hash, ...
 - Titular no tiene acceso a clave (privada)
 - Posible generación de pares clave pública-clave privada
 - Puede almacenar varios certificados y claves
 - Almacena credenciales para acceder a recursos (tras autenticación)
 - Sensores físicos
 - Protección física

Tarjetas Inteligentes y PKI (cont.)



- El **PIN** hace más fuerte la tarjeta
- Es más seguro que software porque:
 - Sólo el usuario de la tarjeta lo conoce
 - La tarjeta nunca deja de estar en posesión de su dueño
 - Los lectores están protegidos para evitar accesos no permitidos
- La tarjeta no puede ser copiada como las de Banda Magnética, e incluso si se pudiera – el PIN no estaría disponible
- Si la tarjeta es robada, no puede ser usada sin el PIN

¿Como Funciona?

Interfaz PKCS#11

Es un interfaz de software definido por RSA Data Security, comúnmente denominado "Cryptoki" que facilita el acceso a la tarjeta inteligente con una gran variedad de aplicaciones criptográficas entre las que se encuentran productos como Netscape, proporcionando servicios de Web segura, correo seguro, cifrado asimétrico y simétrico, operaciones con certificado entre otros.

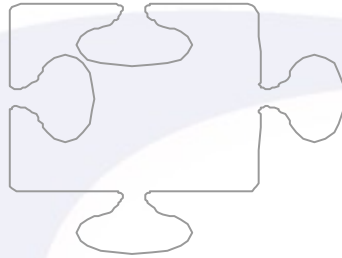
CSP

Es un interfaz de software definido por Microsoft que responde a las siglas "Cryptographic Service Provider" y permite, de forma opcional, el uso de tarjetas inteligentes con una gran variedad de aplicaciones criptográficas con el sistema operativo Windows como: servicios de Web segura, correo seguro, cifrado asimétrico y simétrico, operaciones con certificado entre otros.

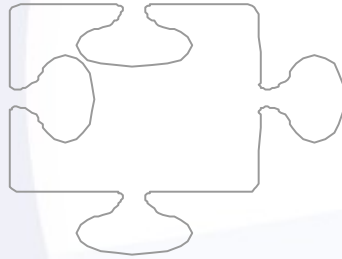
PKCS#15

Es una especificación definida por RSA Data Security que pretende estandarizar el acceso a la información PKI y del método o métodos de autenticación almacenada en una tarjeta inteligente. usada sin el PIN

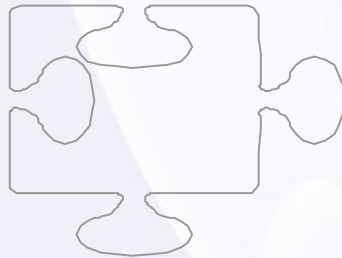
Capas básicas que la componen.



SO



**Protocolo de
Transmisión
ISO 7616-3**



Interfaces



Aplicación



Tipos de tarjetas Inteligentes (cont).



Concepto	Java Card	Multos
Multi Marcas	Hay en el mercado productos que permiten en una misma tarjetas instalar applets EMV con aplicaciones Visa o Mastercard	Sólo hay aplicaciones Mastercard disponible (Visa participa del Java Forum y tiene su producto Java)
Product Line	Hay una infinidad de productos disponibles en el mercado para todos los segmentos y con las más distintas configuraciones de Estándares y características de seguridad	Hay solamente dos versiones, Multos step one y Multos, lo que restringe las opciones de segmentación del Banco.
Costo	Como hay más de un proveedor de chip, los precios son mejores y además, los volúmenes mundiales negociados son altos y consecuentemente el precio final del producto es bajo.	Hay solamente un proveedor de chip mundial. Los volúmenes requeridos por el mercado son bajos, consecuentemente el costo del chip es más alto. Además, KeyCorp cobra una licencia por cada tarjeta emitida.
Logística	Debido al alto volumen de emisión y la grande cantidad de proveedores de chip, hay disponibilidad y buen tiempo de respuesta en la adquisición de los módulos.	Bajo volumen de emisión mundial con una escasez de módulos en el mercado y tiempos de respuestas muy largos, lo que puede comprometer el programa de migración de un banco.



Aplicaciones (cont).

- Identificador físico y control de acceso
- Acceso a redes
- Single Sign-On
- Control de claves
- Firma
- Criptografía
- Pagos
- Voto electrónico
- Inversiones bancarias



Beneficios.

- El usuario es responsable del almacén de claves
- Posee un PIN y PUN
- Costos asumibles ante pérdidas.
- Estándares fuertes y establecidos
- Múltiples niveles de protección de claves

