

Tarjeta inteligente (TI)

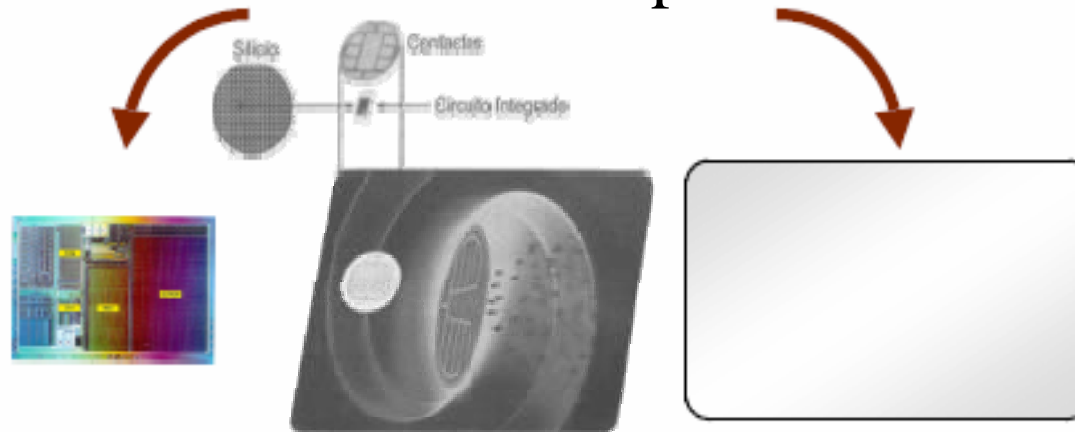


Historia

- 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

¿Qué es?

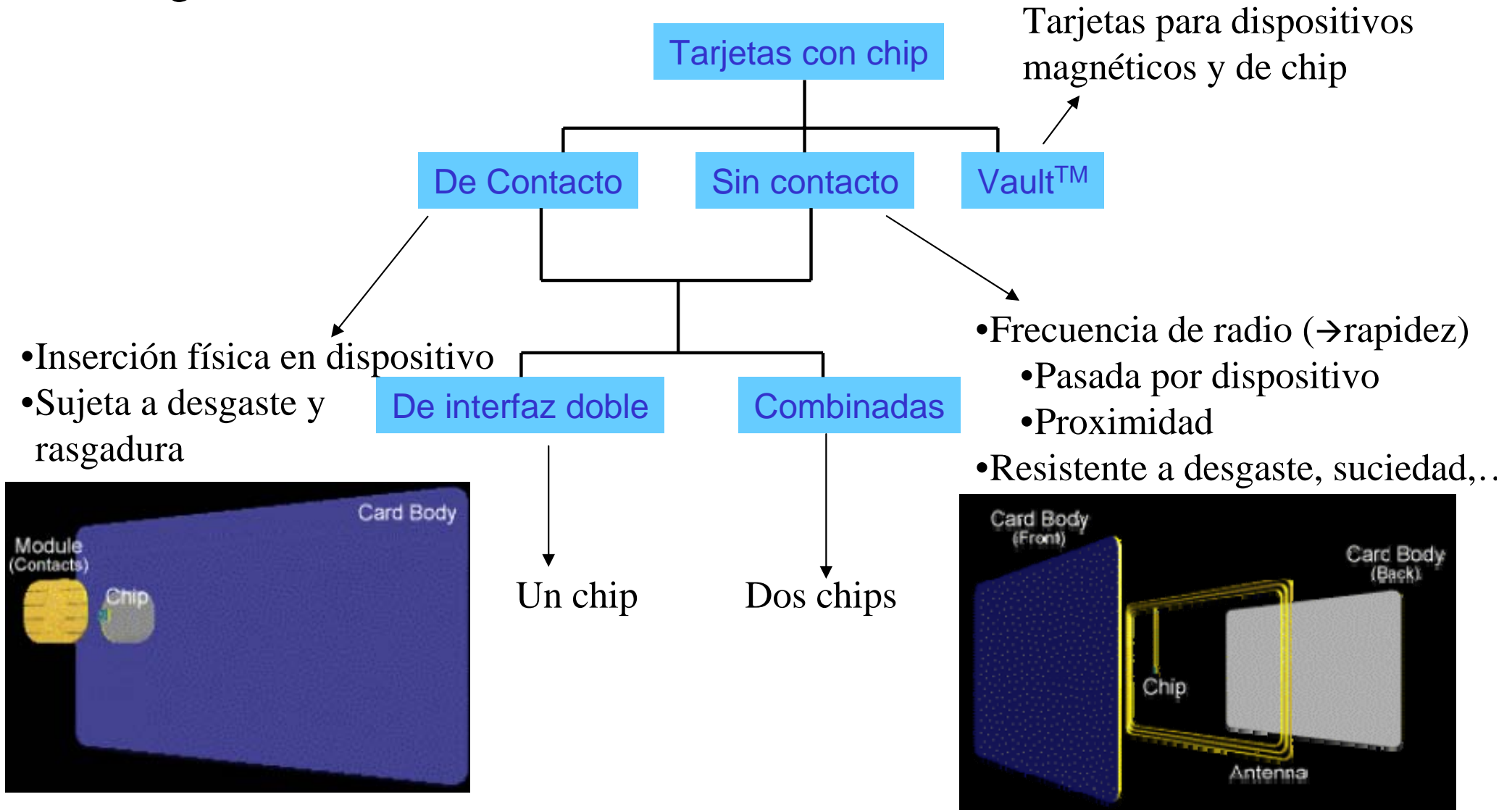
Trozo de silicio sobre un plástico



- De 4000 a miles de millones de transistores
- Capaz de
 - Almacenar información
 - Memorias:
 - RAM, EEPROM, ROM
 - Procesar información
 - Microprocesador:
 - CISC, RISC
 - 6805, 8051, ARM7, MIPS, ...
- Material: PVC, ABS
- Para evitar clonación:
 - Impresión propietaria (sofisticada)
 - Microimpresión, tinta sensible a UV
 - Técnicas de estampado en relieve
- Personalización:
 - Mecánica: foto, firma, fondo ...
 - Eléctrica: datos personales, claves, ...

Tipos

- Según mecanismo de **acceso**:



Tipos (cont.)

- 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

Componentes

SO:

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

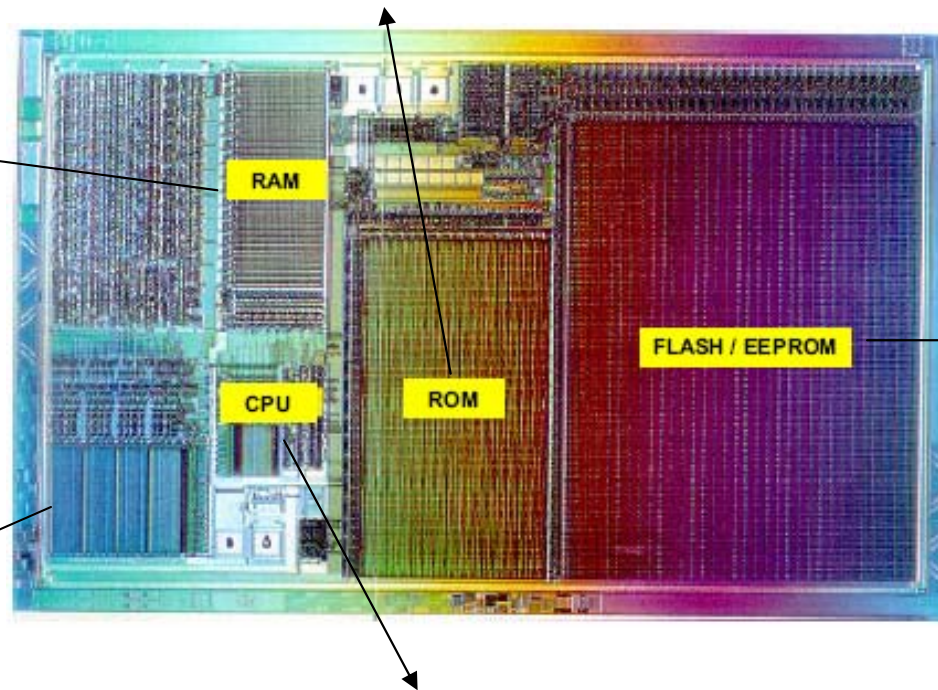
- Estructura de archivos fija
- Sistema de aplicación dinámica

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

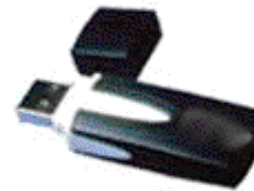
A veces con

procesador matemático
para criptografía

Tipos (cont.)

- Según **tamaño**:

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



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

- Según **forma**:

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



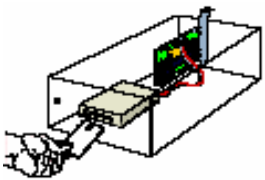
<http://www.useit.com/papers/javaring.html>



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

Comunicación

- **Dispositivos** de lectura y escritura
 - Enlace con máquina / sistema / software de aplicación
 - Sirve de traductor
 - Acepta mensajes de TI y de aplicación
- **Software** de aplicación
 - Diseñado para comunicar con usuario
 - SO en ROM, con varios niveles para seguridad
 - Control de acceso a datos
 - Gestor de archivos
 - Manejador de órdenes
 - Mensajería segura
 - Gestor de transporte
 - Programas y datos de aplicación en EEPROM
 - Funciones (ej., reducir valor en monedero)
 - Lógica de aplicación (ej., transacción no completada hasta que terminal ha realizado secuencia correcta de comprobaciones)



Dispositivos (lectura y escritura)

- **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



Seguridad y TI

- **TI** debe:
 - Asegurarse de que **titular correcto** está presente
 - PIN, biometría
 - Asegurarse de que orden recibida proviene de **origen correcto**
 - Firma, certificado, ...
- **Terminal/Máquina** debe:
 - Establecer **autenticidad de tarjeta**
 - Desafío-respuesta, información almacenada, ...
 - Verificar **identidad de usuario** (directa o indirectamente)
 - PIN, firma digital, biometría, ...
 - Autenticar **origen de datos e integridad**
 - Clave pública, certificado, ...

Para

- **Leer** identidad de usuario, sus privilegios, ...
- **Modificar** datos
- **Comunicar/transferir** datos entre TI y máquina
 - Confidencialidad mediante mecanismos criptográficos

Seguridad y TI. Mecanismos

- **Autenticación de titular** en dos niveles:

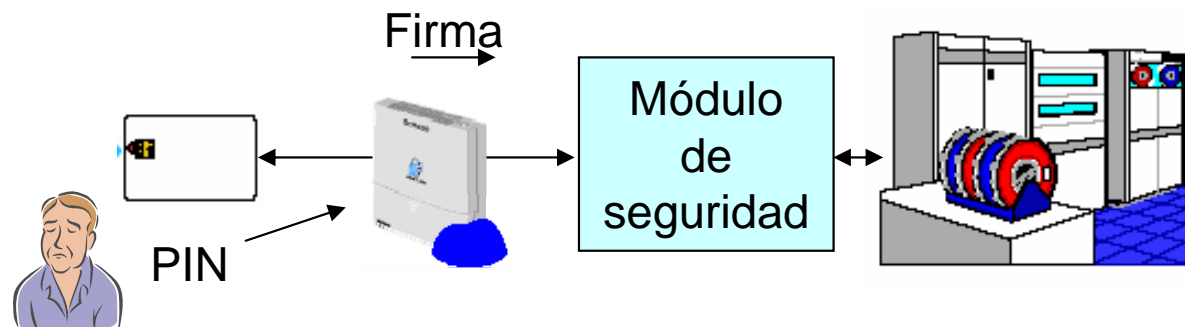
- Titular con TI:

- Algo que se tiene
- Algo que se sabe: PIN
 - nº de intentos limitado
 - Varios posibles (según fin)
- Algo que se es: Biometría
 - Sensores integrados en tarjeta o en dispositivo
 - TI como almacén de características biométricas: huella, retina, iris, ...



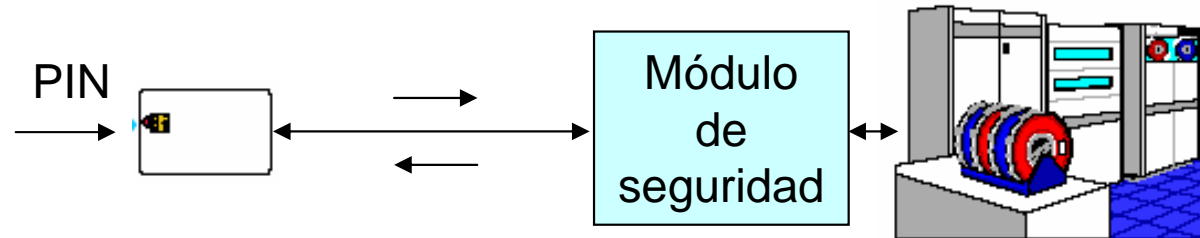
- TI con aplicación:

- Mediante criptografía



Seguridad y TI. Mecanismos (cont.)

- También **autenticación de aplicación**



- **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

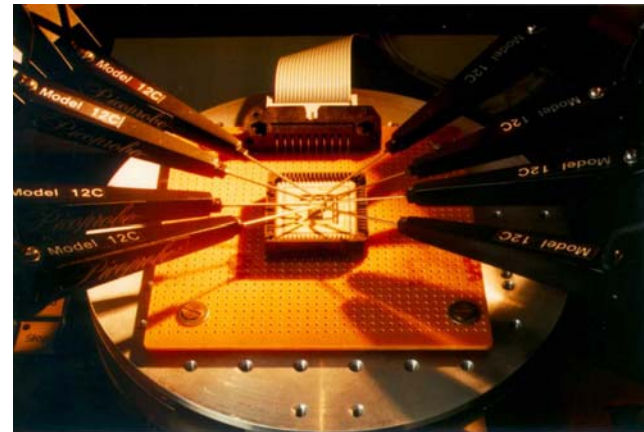
– Almacena credenciales para acceder a recursos (tras autenticación)

– Sensores físicos

– Protección física

Seguridad y TI. Ataques

- **Lógicos**
 - Cptoanalíticos
 - Ej., basados en consumo de energía y tiempo
 - Programas externos
 - Troyanos
- **Físicos**
 - No invasivos
 - Cambios de voltaje, velocidad de reloj, temperatura, ...
 - Impulsos de reloj de distinta duración
 - Análisis de potencia: simple, diferencial
 - Rayos UV sobre EEPROM
 - Invasivos
 - Investigación a fondo
 - Haz de iones
 - Disolventes químicos
- **Ingeniería social**





Aplicaciones



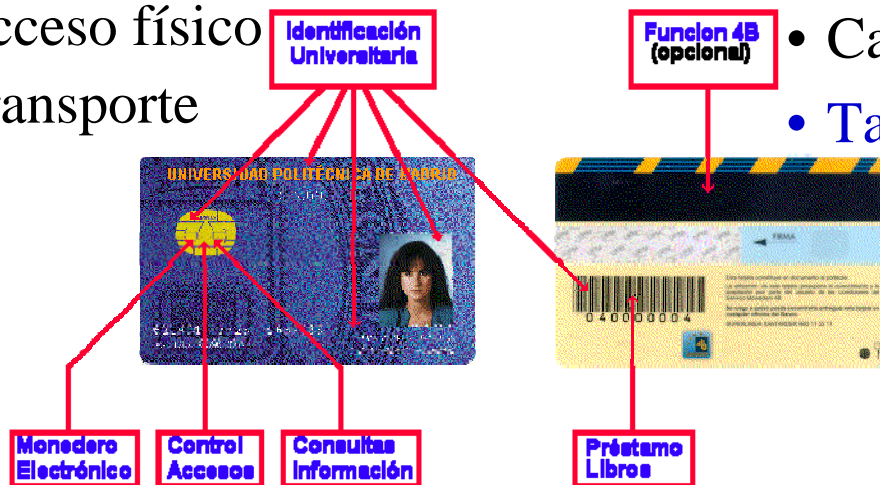
Áreas

- Comercio electrónico
- Finanzas
- Telefonía
- Sanidad
- Entretenimiento
- Comunicación inalámbrica
- Localización y transito de masas
- Seguridad de sistema de información
- Seguridad de redes
- Acceso físico
- Transporte

Ejemplos



- Tarjetas telefónicas prepago
- Tarjetas SIM de móviles
- Tarjeta bancaria
- Monedero electrónico
- Tarjeta sanitaria
- Tarjeta de transporte
- Tarjeta de identidad
- Tarjeta de lealtad
- Tarjeta de TV satélite
- Carné de conducir
- Tarjetas multiaplicación

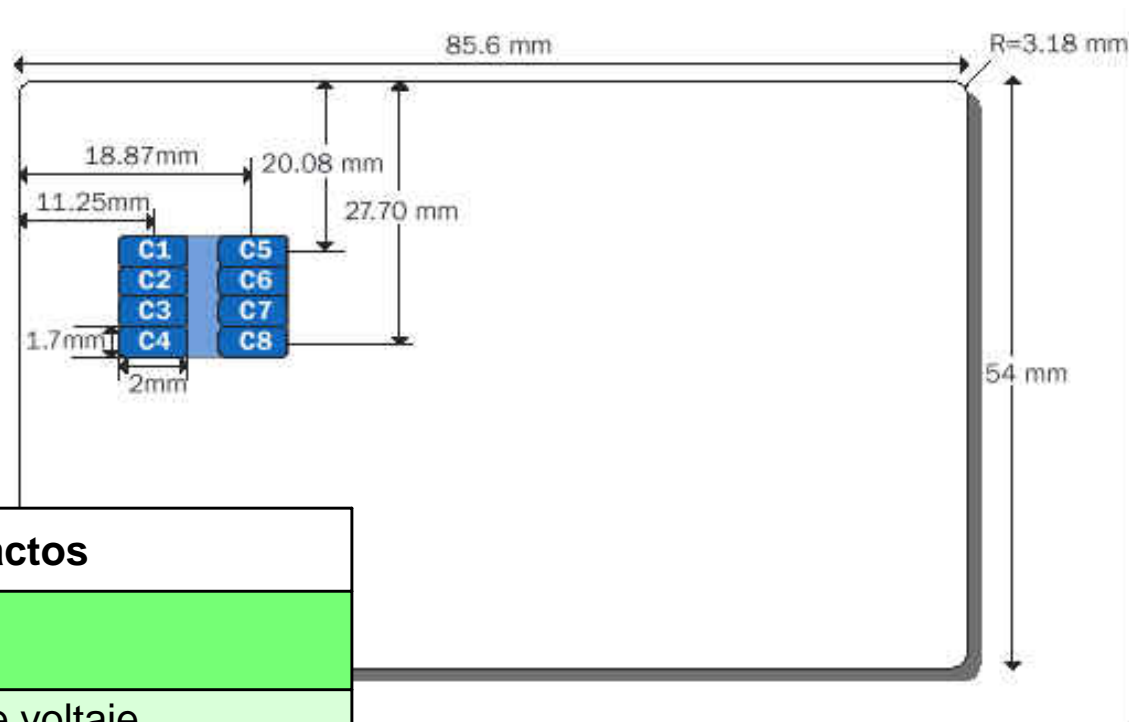


Estándares

- Para
 - Chip, tarjeta, lector, SO, red, emisor
- Algunas relevantes:
 - **ISO 7810**: Características físicas de tarjetas
 - **ISO 7813**: Tarjetas de transacciones financieras
 - **ISO 7816 (1-8)**: Características de tarjetas con chip con contactos
 - **ISO 1443**: Características de tarjetas con chip sin contactos
 - **GSM 11.11/ETSI 300045, EN 726, ISO7816-4**: Conjuntos de instrucciones
 - **PC/SC**: comunicación con Windows
 - **JavaCard**: para ejecutar código Java
 - **OpenCard**: interoperabilidad entre muchas plataformas
 - **FIPS 140 (1-3)**: Diseño e implementación de módulo criptográfico
 - **FIPS 201** tarjetas multifunción para sistemas de gestión de identidad (borrador)
 - Estándares de criptografía

Ejemplo de estándar. ISO 7816

Características físicas de una TI



Descripción de contactos		
Puesto	Función técnica	Descripción
C1	Vcc	Suministro de voltaje
C2	RST	Reinicialización (reset)
C3	CLK	Frecuencia de reloj
C4	RFU	Reservado para uso futuro
C5	GND	Tierra
C6	Vpp	Voltaje de programación externo
C7	I/O	Comunicaciones E/S serie
C8	RFU	Reservado para uso futuro

Ejemplo

Tarjeta criptográfica CERES

<http://www.cert.fnmt.es/pilotos/tarjeta.htm>



- Para infraestructuras de **clave pública**
 - Mantiene material sensible criptográfico siempre interno
 - Protege su uso mediante control de acceso.
- Posibilidad de que **claves RSA** sean generadas por emisor y almacenadas en estado inactivo
 - Operativas cuando usuario las active
- SO para facilitar **interoperabilidad entre aplicaciones**
 - Versión 1.0 de estándar PKCS#15
- Software
 - Para integración con Windows, navegadores
 - Para operaciones criptográficas

Ventajas

- Altos niveles de **seguridad**
 - Clave privada no sale de tarjeta
 - Cifrado de información
 - Posible tener varias contraseñas
 - Certificados y claves portátiles
- Facilidad de **uso**
- **Comodidad** para usuario
 - Liquidez, compras por red, ...
- **Estándares** específicos
- **Evolución** constante
 - Capacidad de memoria
 - Capacidad de procesamiento
 - Previsible caída de precios
- Frente a t. con **banda magnética**:
 - TI es más fiable y segura
 - TI no replicable fácilmente
 - TI no necesita conexión con central para autenticación
 - TI es más difícil de manipular
 - TI puede almacenar más información
 - TI puede ser desechable o reutilizable
 - TI puede realizar varias funciones
 - TI es compatible con dispositivos electrónicos portátiles

Desventajas

- **PIN** es muy vulnerable
- Posibilidad de **virus**
- **Extraviada** fácilmente
- **Recuperación de información** de tarjeta robada o perdida
- Sensible a **fluidos**
- Necesaria **infraestructura**
- **Dispositivos** de lectura/escritura **sin estandarización**
- **Coste** de producción
 - TI con coste por transacción menor que t. con banda magnética