VNIVERSIDAD NACIONAL AVFNOMA DE MEXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

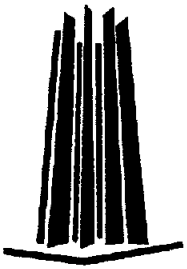
FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

"CARACTERIZACIÓN DEL CIRCUITO INTEGRADO SLE4432/SLE4442 Y ALGUNAS APLICACIONES EN TARJETAS INTELIGENTES"

T E S I S PROFESIONAL
QUE PARA OBTENER EL TITULO DE:
M ECANICO ELECTRICISTA INGENIERO
(AREA ELECTRONICA)

P R E S E N T A:

FERNANDO DOMINGUEZ PEREZ



ASESOR:ING.ELEAZAR MARGARITO PINEDA DIAZ

MÉXICO ,D.F. 2005

A DIOS

POR DARME LA VIDA

A MI MADRE

POR TODOS SUS SACRIFICIOS, EL APOYO Y LOS CONSEJOS QUE ME HA BRINDADO PARA LOGRAR UNO DE MIS MAS GRANDES ANHELOS.

A MIS PADRINOS

POR QUE EN ELLOS SIEMPRE HE VISTO UN EJEMPLO A SEGUIR

A MI FAMILIA

QUIENES DE DIFERENTE MANERA SIEMPRE ME HAN DADO SU APOYO INCONDICIONAL PARA SEGUIR ADELANTE.

A MIS AMIGOS

QUE SIEMPRE ME HAN DEMOSTRADO SU AMISTAD AUN EN MOMENTOS DIFICILES.

INDICE

CAPITULO 4 ALGUNAS APLICACIONES DE LAS TARJETAS

INTRODUCCIÓN

El ser humano es el único ser cognoscitivo que ha tenido curiosidad con los fenómenos que suceden a su alrededor. Podemos mencionar que en su mayoría, los descubrimientos han surgido en forma casual, pero recordando que a partir de la observación y experimentación se ha podido llegar a entender sus principios. Desde los primeros científicos y alquimistas que pretendían estudiar y entender las ciencias, hasta nuestros doctores y/o científicos, reúnen algo en común, ese espíritu inquebrantable de curiosidad y tenacidad.

El descubrimiento de la electricidad y la electrónica, marcan una nueva era y traen consigo los beneficios y consecuencias de utilizar tal fuente de energía. Recordemos que primero entendimos la electricidad y después empezamos a realizar aplicaciones mas detalladas con ella. El desarrollo de la ciencia en las últimas décadas ha generado avances en todos los campos: medicina, ciencia, comunicaciones. En la actualidad, sería imposible imaginar al hombre sin alguna herramienta o algún medio en donde no ocupara la electrónica. Aunque para muchos pasa a ser una rutina utilizar una computadora personal, el realizar una llamada telefónica, o encender la radio, realmente no apreciamos el desarrollo logrado al controlar uno de los elementos que es fundamentales y que es la base de la electrónica: los electrones.

En una breve reseña, mencionaremos las etapas y avances logrados en lo que a dispositivos electrónicos se tiene, empezando por los tubos de vacío. Consisten en una cápsula de vidrio de la que se ha extraído el aire, y que lleva en su interior varios electrodos metálicos. Un tubo sencillo de dos elementos (diodo) está formado por un cátodo y un ánodo, este último conectado al terminal positivo de una fuente de alimentación. El cátodo es un pequeño tubo metálico que se calienta mediante un filamento y libera electrones que migran hacia él (un cilindro metálico en torno al cátodo, también llamado placa). Si se aplica una tensión alterna al ánodo, los electrones sólo fluirán hacia el ánodo durante el semiciclo positivo; durante el ciclo negativo de la tensión alterna, el ánodo repele los electrones, impidiendo que cualquier corriente pase a través del tubo. Los diodos conectados de tal manera que sólo permiten los semiciclos positivos de una corriente alterna (c.a.) se denominan tubos rectificadores y se emplean en la conversión de corriente alterna a corriente continua.

El transistor bipolar fue inventado en 1948 para sustituir al tubo de vacío triodo. Está formado por tres capas de material dopado, que forman dos uniones pn (bipolares) con configuraciones pnp o npn. Una unión debe estar conectada a una batería para permitir el flujo de corriente (polarización directa), y la otra está conectada a una batería en sentido contrario llamada polarización inversa. Si se varía la corriente en la unión de polarización directa mediante la adición de una señal, la corriente de la unión de polarización inversa del transistor variará en

consecuencia. El principio se puede utilizar para construir amplificadores en los que una pequeña señal aplicada a la unión de polarización directa provocará un gran cambio en la corriente de la unión de polarización inversa.

Los circuitos integrados son pequeños trozos, o chips, de silicio, de entre 2 y 4 mm^2, sobre los que se fabrican los transistores. La fotolitografía permite al diseñador crear centenares de miles de transistores en un solo chip situando de forma adecuada las numerosas regiones tipo n y p. Durante la fabricación, estas regiones son interconectadas mediante conductores minúsculos, a fin de producir circuitos especializados complejos. Estos circuitos integrados son llamados monolíticos por estar fabricados sobre un único cristal de silicio. Los chips requieren mucho menos espacio y potencia, y su fabricación es más barata que la de un circuito equivalente compuesto por transistores individuales.

Día a día surgen avances en el mundo de la electrónica y para muestra basta recordar el desarrollo que se ha tenido en el área informática. Recordamos que a finales de la década de los 70, una computadora era del tamaño de un cuarto grande, generaba un excesivo calor y solo podía realizar unos cuantos cálculos, en sus componentes, estaban los famosos tubos de vacío, ya descritos anteriormente. Además, consumían una basta cantidad de energía. Hoy se tienen maquinas tan potentes que caben en la palma de la mano, que están constituidos básicamente por circuitos de alta escala de integración. Podemos apreciar, que al aumentar el nivel de componentes, y optimizarlos, podemos manejar entonces una gran cantidad de datos, los cuales, representan para ciertas, personas información muy valiosa. Debido a que cada día, estos circuitos se hacen cada vez mas pequeños, se pueden utilizar en una diversidad de aplicaciones, y una de áreas que se ha invertido una cantidad generosa de recursos tanto económicos como intelectuales es la seguridad. Nos vamos a referir a ésta como los medios confiables que se tienen para proteger ciertos datos confidenciales.

Ante la necesidad de contar con información sobre el funcionamiento interno de las tarjetas inteligentes, las especificaciones que las rigen como la organización internacional de estándares (ISO), la comisión de electrotecnia internacional (IEC), sus posibles aplicaciones y la escasa información en español que existe en nuestro país es lo que impulsa al desarrollo de este tema.

El objetivo de esta tesis es dar una idea clara y concisa de lo que son las denominadas tarjetas inteligentes, sus características internas, así como algunas aplicaciones que actualmente están en uso en diversos países y no por ello sean las únicas. Se pretende que esta tesis muestre los principales rubros en lo que a tarjetas inteligentes se refiere, en un lenguaje amigable, a fin de que sea fácilmente entendible para todos..

Dado que hay una gran cantidad de modelos en el mercado de tarjetas así como de fabricantes, elegimos el modelo del chip SLE4432/SLE4442 del fabricante Siemens por ser uno de los mas utilizados en las tarjetas telefónicas prepagadas. Además me parece un buen ejemplo en el cual basarse para futuras aplicaciones debido a su naturaleza.

También se mostrará una idea general de la operación de ellas y por que no, en un futuro desarrollar aplicaciones tomando como referencia este documento. Se incluyen las principales especificaciones ISO y IEC para tarjetas inteligentes, Las cuales abarcan tanto características físicas como eléctricas y se mencionan las aplicaciones que a la fecha se han desarrollado. Además es de las primeras tesis en este campo.

A manera de metodología y para alcanzar los objetivos, el contenido del la tesis se desarrolla de la siguiente forma:

Uno de los componentes principales que se utilizan en las tarjetas inteligentes son los microprocesadores, en el primer capitulo se tendrán generalidades de ellos. También mencionaremos las normas ISO/IEC que nos dan una idea acerca de las dimensiones físicas de las tarjetas.

Puesto que toda tesis tiene un elemento de estudio, la cual es base al tema, en el capitulo segundo se hará una caracterización del circuito integrado con chip inteligente 256 byte EEPROM SLE4432/SLE4442 para el uso en tarjetas inteligentes, se mencionaran las características mas importantes de éste como son los valores de corrientes y voltajes, modos de operación frecuencia de funcionamiento distribución y capacidad de memoria; protocolos utilizados y además se mencionarán comandos de programación.

En el tercer capitulo haremos una caracterización de las tarjetas inteligentes, mostrando primeramente las normas que rigen el embozado para anotar datos del cliente, la localización de caracteres, y tarjetas financieras; además una clasificación de tarjetas inteligentes.

Una vez que se ha dado una idea tanto eléctrica como física, el capítulo cuarto, se mencionan algunas aplicaciones de las tarjetas inteligentes, como son el monedero electrónico, tarjetas de prepago telefónicas, tarjetas universitarias, y tarjetas para cuidados médicos. No sin antes recalcar que no son las únicas aplicaciones.

En la parte final de esta tesis, expondré mis comentarios a las que llegue al haber concluido esta investigación. Mencionando las experiencias adquiridas, así como las dificultades que se presentaron.

CAPÍTULO 1.- GENERALIDADES DE LOS MICROPROSESADORES Y NORMAS.

1.1 El microprocesador.

Es un componente electrónico en cuyo interior existen miles o millones de elementos llamados transistores empaquetados en una cápsula cuyo tamaño varia según las necesidades de las aplicaciones a las que van dirigidas, y que actualmente van desde el tamaño de una lenteja hasta el de una galleta. Es utilizado como unidad central de proceso (cpu) en un sistema microordenador y en otros dispositivos electrónicos complejos como cámaras fotográficas, impresoras, y como añadido en pequeños aparatos extraibles de otro aparato más complejo como por ejemplo: equipos musicales de automóviles, etc. Los microprocesadores, suelen tener forma de cuadrado o rectángulo negro, y van sobre un elemento llamado zócalo, soldados en la placa o, metidos dentro de una especie de cartucho que se conecta a la placa base, aunque el chip en sí está soldado en el interior de dicho cartucho. A veces al microprocesador se le denomina CPU, este término tiene cierta ambigüedad, pues también puede referirse a toda la caja que contiene la placa base, el micro, las tarjetas y el resto de la circuitería principal.

Las partes lógicas que componen un microprocesador son: unidad aritmético-lógica, registros de almacenamiento , unidad de control , unidad de ejecución, memoria caché y buses de datos, control y dirección .

Unidad aritmético-lógica (ALU) unidad incluida en la CPU encargada de realizar operaciones aritméticas y lógicas sobre operandos que provienen de la memoria principal y que pueden estar almacenados de forma temporal en algunos registros de la propia unidad. Físicamente, la ALU es parte de la altamente integrada lógica-electrónica del microprocesador principal de cualquier computadora.

Memoria principal: Son circuitos integrados capaces de almacenar información digital, a los que tiene acceso el microprocesador. En las tarjetas electrónicas son utilizados los siguientes tipos de dispositivos:

Memoria de solo Lectura ROM (Read Only Memory), almacena códigos de programa grabados en fábrica. No se puede escribir sobre ella, y conserva intacta la información almacenada, incluso en el caso de interrupción de corriente. Una razón de que todavía se utilice la memoria ROM para almacenar datos es la Aún más importante, no se puede leer un programa que es necesario para ejecutar un disco desde el propio disco. Por lo tanto, el BIOS o un sistema de arranque del ordenador normalmente se encuentran en la memoria ROM.

Memoria de acceso aleatorio RAM (Random Access Memory), almacena datos que pueden ser escritos y borrados atendiendo a los procesos de computación. Se trata de una memoria volátil, es decir, pierde su contenido al desconectar la energía eléctrica. Se utilizan normalmente como memorias temporales para almacenar resultados intermedios y datos similares no permanentes. Aleatorio indica que sus localidades pueden ser accedidas directamente, dando rapidez a los procesos; a diferencia de las memorias seriales en que, para llegar a una localidad, hay que pasar antes por las localidades previas. Se dividen en estáticas y dinámicas. Una memoria RAM estática mantiene su contenido inalterado mientras esté alimentada. La información contenida en una memoria RAM dinámica se degrada con el tiempo, llegando ésta a desaparecer, a pesar de estar alimentada. Para evitarlo hay que restaurar la información contenida en sus celdas a intervalos regulares, operación denominada refresco.

Memoria flash o EEPROM (Electrically Erasable Read-Only Memory) la memoria de solo lectura programable y eléctricamente borrable, puede ser borrada eléctricamente y luego escrita sin sacarla del ordenador. Esta forma de escritura es más lenta que copiar en la memoria RAM o leer desde cualquier memoria ROM.

La memoria caché: Una memoria ultrarrápida que sirve al micro para tener a mano ciertos datos que previsiblemente serán utilizados en las siguientes operaciones sin tener que acudir a la memoria RAM, reduciendo el tiempo de espera. es lo que se conoce como caché de primer nivel; es decir, la que está más cerca del micro, tanto que está encapsulada junto a él.

Unidad de Control: Es la unidad incluida en la CPU encargada de leer las instrucciones máquina almacenadas en la memoria principal y de generar las señales de control necesarias para controlar y coordinar el resto de las unidades funcionales de un ordenador con el fin de ejecutar las instrucciones leídas. Consta de los siguientes componentes: Contador de programa, registro de instrucción, decodificador y reloj interno.

Bus de datos: Son las conexiones internas de datos que se dan en un sistema en funcionamiento. En el bus todos los nodos reciben los datos aunque no se dirijan a todos los nodos, los nodos a los que no van dirigidos simplemente lo ignorarán. El bus es el conjunto de conductores eléctricos en forma de pistas metálicas impresas sobre la tarjeta por donde circulan las señales que corresponden a los datos binarios del lenguaje máquina con que opera el Microprocesador. Hay tres clases de buses: Bus de datos, bus de direcciones y bus de control. El primero mueve los datos entre los dispositivos del hardware: de entrada como el teclado, el escáner, el ratón, etc.; de salida como la impresora, el monitor o la tarjeta de sonido; y de almacenamiento como el disco duro, el disco flexible o la memoria-Flash.

El bus de direcciones, por otra parte, está vinculado al bloque de control de la CPU para tomar y colocar datos en el sub-sistema de memoria durante la ejecución de los procesos de cómputo,

El bus de control transporta señales de estado de las operaciones efectuadas por el CPU con las demás unidades.

1.2 Diferencia entre microcontroladores y microprocesadores.

Es importante distinguir las diferencias entre ambos circuitos integrados para poder identificar cuándo es conveniente emplearlos. Los microcontroladores generalmente tienen una arquitectura con un bus dual es decir, un bus dedicado para la memoria del programa y otro para la memoria de datos, mientras que los microprocesadores es común encontrar la arquitectura Von Neummann, un solo bus para la memoria de datos y programas.

Los pines de un microprocesador sacan al exterior las líneas de sus buses de direcciones, datos y control, para permitir conectarle con la memoria y los módulos de entrada y salida (E/S) y configurar un computador implementado por varios circuitos integrados. Se dice que un microprocesador es un sistema abierto por que su configuración es variable de acuerdo con la aplicación que se destine.

En la Figura 1.1 se muestra un sistema abierto basado en un microprocesador. La disponibilidad de los buses en el exterior permite que se configure a la medida de la aplicación.

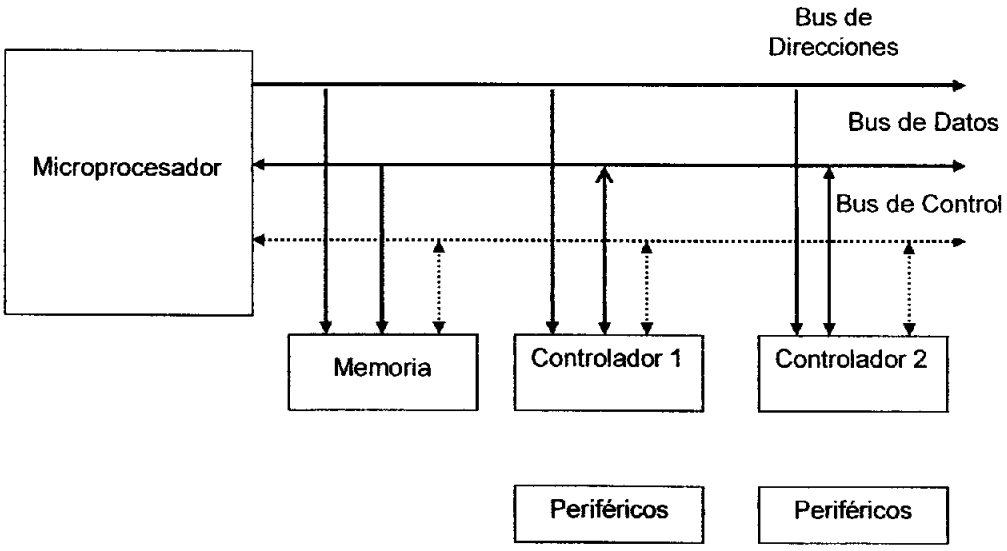


Figura 1.1 Sistema abierto basado en un microprocesador.

Si solo se dispusiese de un modelo de microcontrolador, éste debería tener muy potenciados todos sus recursos para poderse adaptar a las exigencias de las diferentes aplicaciones.

Esta potencialización supondría en muchos casos un despilfarro. En la práctica cada fabricante de microcontroladores oferta un elevado número de modelos diferentes, desde los mas sencillos hasta los mas poderosos. Es posible seleccionar la capacidad de las memorias, el número de líneas de E/S, la cantidad y potencia de los elementos auxiliares, la velocidad de funcionamiento, etc. Un aspecto muy destacado del diseño, es la selección del microcontrolador a utilizar. En la figura 1.2 se muestra como el µc es un sistema cerrado. Todas las partes del computador están contenidas en su interior y solo salen al exterior las líneas que gobiernan los periféricos.

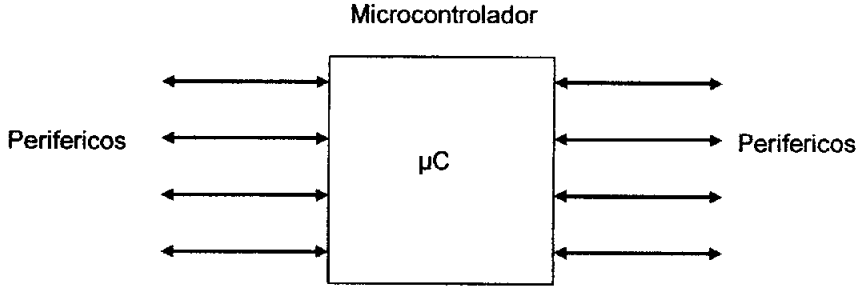


Figura 1.2 Sistema cerrado basado en un microcontrolador.

La siguiente es una lista cronológica de los eventos tecnológicos más recientes que han tenido impacto sobre la aparición y el desarrollo del campo de los microprocesadores en la electrónica digital.

- 1971. Intel fabrica el primer microprocesador (el 4004) de tecnología PMOS. Este era un microprocesador de 4 bits y fue fabricado por Intel a petición de Datapoint Corporation con el objeto de sustituir la CPU de terminales inteligentes fabricadas en esa fecha por Datapoint mediante circuitería discreta. El dispositivo fabricado por Intel resultó 10 veces más lento de lo requerido y Datapoint no lo compró, de esta manera Intel comenzó a comercializarlo. El 4004 podía direccionar sólo 4096 (4k) localidades de memoria de 4 bits, reconocía 45 instrucciones y podía ejecutar una instrucción en 20 µseg en promedio.

- 1972. Las aplicaciones del 4004 estaban muy limitadas por su reducida capacidad y rápidamente Intel desarrolló una versión más poderosa (el 8008), el cual podía manipular bytes completos, por lo cual fue un microprocesador de 8 bits. La memoria que este podía manejar se incrementó a 16 kbytes, sin embargo, la velocidad de operación continuó igual.

- 1973. Intel lanza al mercado el 8080 el primer microprocesador de tecnología NMOS, lo cual permite superar la velocidad de su predecesor (el 8008) por un factor de diez, es decir, el 8080 puede realizar 500,000 operaciones por segundo, además se incrementó la capacidad de direccionamiento de memoria a 64 kbytes. A partir del 8080 de Intel se produjo una revolución en el diseño de microcomputadoras y varias compañías fabricantes de circuitos integrados comenzaron a producir microprocesadores. Algunos ejemplos de los primeros microprocesadores son: el IMP-4 y el SC/MP de National Semiconductors, elPPS-4 y PPS-8 de Rockwell International, el MC6800 de Motorola, el F-8 de Fairchild.

- 1975. Zilog lanza al mercado el Z80, uno de los microprocesadores de 8 bits más poderosos. En ese mismo año, Motorola abate dramáticamente los costos con sus microprocesadores 6501 y 6502 (este último adoptado por APPLE para su primera microcomputadora personal). estos microprocesadores se comercializan en $20 y $25 (dls. USA) respectivamente. Esto provoca un auge en el mercado de microcomputadoras de uso doméstico y un caos en la proliferación de lenguajes, sistemas operativos y programas (ningún producto era compatible con el de otro fabricante).

- 1976. Surgen las primeras microcomputadoras de un solo chip, que más tarde se denominarán microcontroladores. Dos de los primeros microcontroladores, son el 8048 de Intel y el 6805R2 de Motorola.

En la década de los 80's comienza la ruptura entre la evolución tecnológica de los microprocesadores y la de los microcontroladores, Ya que los primeros han ido incorporando cada vez más y mejores capacidades para las aplicaciones en donde se requiere el manejo de grandes volúmenes de información y por otro lado, los segundos han incorporado más capacidades que les permiten la interacción con el mundo físico en tiempo real, además de mejores desempeños en ambientes de tipo industrial. Esta ruptura se representa esquemáticamente en la figura 1.3.

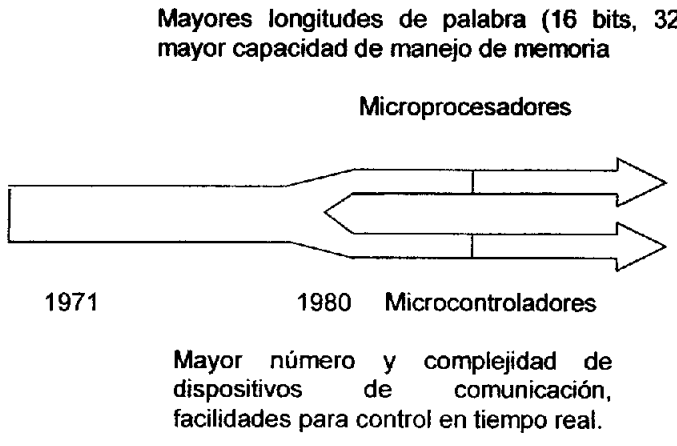


Figura 1.3 Separación de aplicaciones.

Para clarificar un poco más el campo de aplicaciones de un microprocesador y un microcontrolador, podemos recurrir a la figura 1.4, en donde se pretende representar el tipo de aplicaciones como un tiempo continuo desde el extremo de los sistemas que manejan grandes volúmenes de información, hasta los que requieren una gran interacción con el mundo físico en tiempo real.

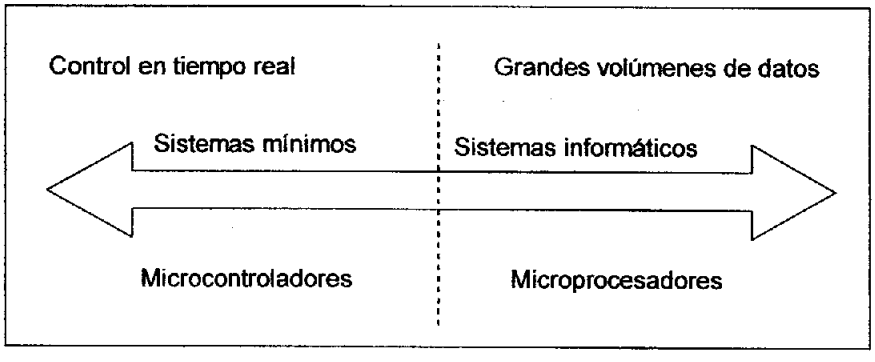


Figura 1.4 Diferencias entre ambos componentes.

Las aplicaciones específicas de los microcontroladores son tan enormemente variadas que no se exagera cuando se dice que éstas están limitadas solamente por la imaginación del diseñador.

1.3 Arquitectura general de las tarjetas inteligentes.

Básicamente, contiene los módulos que posee una Computadora persona (PC), por ejemplo, una unidad central de proceso (CPU), un sistema operativo, diferentes tipos de memoria (RAM, ROM), así como un canal de comunicación, en este caso de entrada/salida. Podríamos decir que es una pequeña PC y solo podrá manejar un arreglo de 8 bits de información. Comparada con los sistemas modernos que manejan hasta 32 bits. Todas estas características se encuentran en un chip de muy alta escala de integración.

En la siguiente figura, podemos apreciar un diagrama a bloques para darnos una idea de como interactúan todos los módulos dentro de una tarjeta inteligente.

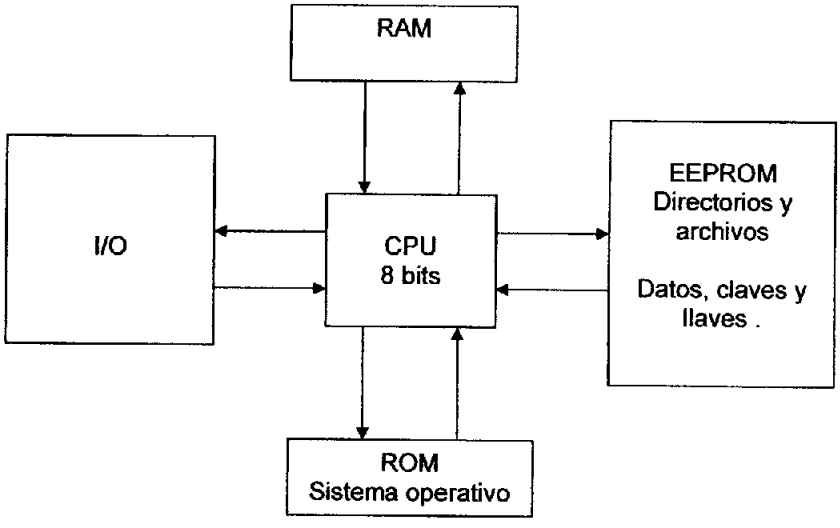


Figura 1.5 Arquitectura general de las tarjetas inteligentes.

1.4 Sistema operativo en las tarjetas inteligentes.

Parece ser presuntuoso referirse como sistema operativo a los pocos miles de bytes de código de programa que posee el microprocesador de una tarjeta. Se entiende por sistema operativo al interfaz existente entre el hardware y el software que se está ejecutando en ella. Es importante no asociar este concepto con el programa que poseen los ordenadores basados en DOS, Windows o UNIX, Desgraciadamente, las características y el funcionamiento de las tarjetas aun dependen de la filosofía del fabricante, esto hace que posean propiedades muy diferentes entre ellas.

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 almacenar es bastante pequeña, estando entre 2 y 60Kbytes. Los módulos de programa se graban en la ROM, esto 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 ningún cambio. Por esto el programa grabado en la ROM debe ser 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 ejecución de los programas.
- Administración de los datos.
- Manejo y administración de algoritmos criptográficos.

1.5 Estructura de la memoria.

Existen tres tipos de memoria dentro de una tarjeta de circuito integrado y cada una tiene propiedades totalmente diferentes. La ROM sólo se puede programar durante el proceso de fabricación y no se puede alterar una vez terminada dicha fase. Por otro lado, la RAM mantiene su contenido solamente cuando se aplica tensión sobre la tarjeta. Cualquier fallo en la alimentación provoca la perdida total de los datos almacenados en dicha memoria. La memoria EEPROM puede retener los datos almacenados en ella incluso una vez desconectada la alimentación. El tiempo de escritura y lectura sobre ella es bastante grande (1 ms/byte). En la siguiente tabla, se muestra un ejemplo de cómo está dividida la memoria RAM en varias secciones. Si por ejemplo es necesario un bufer de entrada/salida de 256 bytes, que es la capacidad total de la memoria, el sistema operativo puede usar memoria EEPROM como si fuera RAM, con la desventaja de que la escritura sobre la EEPROM es mas lenta.

Registro	10 bytes
Pila	26 bytes
Variables generales	50 bytes
Espacio de trabajo para algoritmos criptográficos	70 bytes
Buffer de entrada/salida	100 bytes

Tabla 1.1 Ejemplo de la estructura de una memoria RAM de 256 bytes

La estructura de la EEPROM es bastante mas complicada que las otras memorias, en los sistemas operativos modernos, la división es la siguiente: primero están almacenados algunos datos de producción que pueden ser números fijos, y por lo tanto no varían, y además son usados para funciones especificas. Esta zona suele estar protegida frente a accesos no autorizados por algún mecanismo hardware. Después de esta zona, que habitualmente es de 32 bytes, están las tablas y los punteros de sistema. Estos se graban durante la fase de fabricación y en conjunto con el programa ROM forman el sistema operativo. Para asegurar que el sistema funcione perfectamente, estas sección de la EEPROM está protegida con una suma de comprobación que es calculada antes de cada acceso a esta zona. Si se encuentra algún error en este cálculo, el sistema operativo dejará de usar esta zona de memoria.

A la sección de memoria anterior le sigue otra que contiene códigos adicionales de los programas de aplicación. En algunos casos esta zona está protegida frente a posibles alteraciones mediante el uso de una suma de comprobación. Los datos contenidos también pueden ser algoritmos que no están almacenados en la ROM por falta de espacio. La zona adyacente contiene todas las estructuras de ficheros.

Esta zona no está protegida por ningún mecanismo pero generalmente existen módulos de hardware o software orientados a proteger los ficheros.

Al final de la memoria EEPROM existe una zona libre que está administrada por el portador de la tarjeta, esto quiere decir que en ella se pueden almacenar los datos del usuario, la tabla 1.2 nos da una idea del orden de los niveles que se emplean:.

Datos de producción
Sistema operativo
Programas de aplicación
Área de ficheros
Zona de datos del usuario

Tabla 1.2 Ejemplo de la división de la EEPROM

1.6 La norma ISO.

La organización internacional para la standarización (ISO) y la comisión de Electrotecnica internacional (IEC) forman el sistema especializado para la regularización mundial.de normas a seguir.

Miembros de ISO y de IEC participan en el desarrollo de normas internacionales a través de los comités técnicos establecidos por la organización respectiva para tratar con campos particulares de investigación técnica. Los comités técnicos de ISO y IEC colaboran en campos de interés mutuo con otras organizaciones internacionales, gubernamentales y no-gubernamental, en enlace con ISO y IEC, también toman parte en el trabajo.

En el campo de información tecnología ISO y IEC ha establecido una junta en el comité técnico ISO/IEC JTC 1. El Proyecto Standars internacional adoptó el siguiente esquema: un comité técnico designa las normas y para que la publicación sea considerada como una norma internacional requiere aprobación por lo menos del 75% de los miembros nacionales. Las normas que vamos a manejar son las referentes a las tarjetas inteligentes y son las siguientes:

Las normas para la ISO 7816 están separadas en 3 partes que contienen:

- ISO7816-1 Características físicas de la tarjeta.
- ÍSO7816-2 Dimensiones y posiciones de los contactos en la tarjeta.
- ISO7816-3 Protocolos de transmisión de señales eléctricas.

1.6.1 ISO / IEC 7816-1 CARACTERÍSTICAS FÍSICAS DE LAS TARJETAS:

Esta norma especifica las características físicas de las tarjetas de circuito integrado con contactos y solo se describirán las más importantes. Aplica a las tarjetas de identificación del tipo ID-1 que puede incluir chip y/o la banda magnética como se especifica en la norma ISO/IEC 7811-1 a ISO/IEC 7811-6. Esta contemplada para las tarjetas que tienen interfase física con contactos eléctricos.

Esta norma esta dividida en los siguientes puntos:

1.- Características físicas.

Las características físicas para todos los tipos de identificación mencionadas en la norma ISO/IEC 7810 debe aplicarse también en este tipo de tarjetas. dichas características se describen en el Capítulo 3.

2.- Características adicionales.

A.-Luz ultra-violeta (UV)

Cualquier indicio que pueda alterar la luz UV ambienta a la operación de la tarjeta será responsabilidad del fabricante de la tarjeta.

B.-Rayos X

La exposición de cualquier lado de la tarjeta a una dosis relativa a la radiación de energía media de 70 a 140 Kv (dosis acumulada por año) no causará funcionamiento defectuoso de la tarjeta.

C.-Perfil de la superficie de los contactos

La diferencia en nivel entre todos los contactos y la superficie de la tarjeta adyacente estará a menos de 0.1 mm.

D.-La fuerza mecánica de la tarjeta y contacto

La tarjeta resistirá cualquier daño a su superficie y cualquier componente contenido en él y permanecerá intacto durante el uso normal, almacenamiento y manejando.

Superficie (con pins) no debe ser dañada por una presión causada por una pelota de acero de 1.5 diámetro del mm en que se aplica un fuerza de 1.5 N.

E.-Resistencia eléctrica de los contactos.

Todo las resistencias medidas entre dos puntos de los pines no deben ser más de 0.5 Ohm, con cualquier valor de 50 uA a 300 mA.

F.-Interferencia magnética entre la banda magnética y el circuito integrado

El circuito integrado no deberá de sufrir daños, fallas, o algún daño después de leer, escribir o borrar en la banda magnética. Recíprocamente, la lectura o escritura en el circuito integrado no debe causar daños en la banda magnética.

G.-Electricidad estática.

El circuito integrado no deberá sufrir daños por una descarga de una persona cargada electrostáticamente. La tarjeta no debe ser dañada por una descarga eléctrica entre cualquier contacto y tierra cuando está alimentada a través de una resistencia de 1500 ohms y un capacitor de 100pF.

H.-Temperatura de operación:

Las tarjetas deberán operar en un rango de temperaturas que comprendidas entre 0°C a 50°C

I.-Propiedades de Torcimiento de la tarjeta.

- Lado grande de la tarjeta
  deformación: 2 cm
  periodicidad: 30 torcimientos en un minuto
- Lado corto de la tarjeta
  deformación: 1 cm
  periodicidad: 30 torcimientos en un minuto

1.6.2 ISO/IEC 7816-2 DIMENSIÓN Y POSICIÓN DE LOS CONTACTOS.

Esta norma describe los parámetros para el circuito integrado de las tarjetas con los contactos y el uso de tales tarjetas para el intercambio internacional. Especifica las dimensiones, situaciones y asignación para cada uno de los contactos en circuitos integrados las tarjetas tipo ID-1.

Se establece lo siguiente:

1.-Las dimensiones de los contactos *

Cada contacto debe tener una área mínima rectangular no menor que las especificadas en la figura 1.6

Nota: Esta parte de ISO/IEC 7816 no define las dimensiones máximas o formas de los contactos.

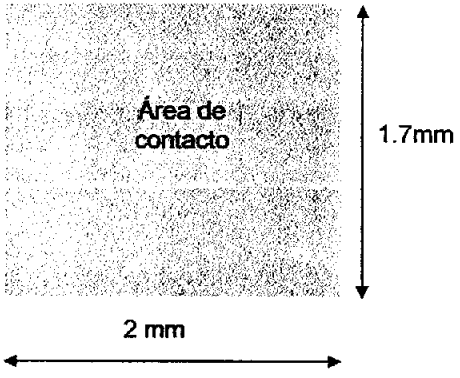


Figura 1.6 Área de contacto

*No se definen la superficie y forma de contacto

2.-Número y localización de los contactos.

En esta parte la ISO/IEC 7816-2 designa 8 contactos nombrados de C1 a C8, el diseño se muestra en la figura 1.7

Estos contactos deben ser localizados en un lado de la tarjeta. Se toma como referencia el borde izquierdo de la tarjeta y el borde superior para ubicar en la posición, que se recomienda.

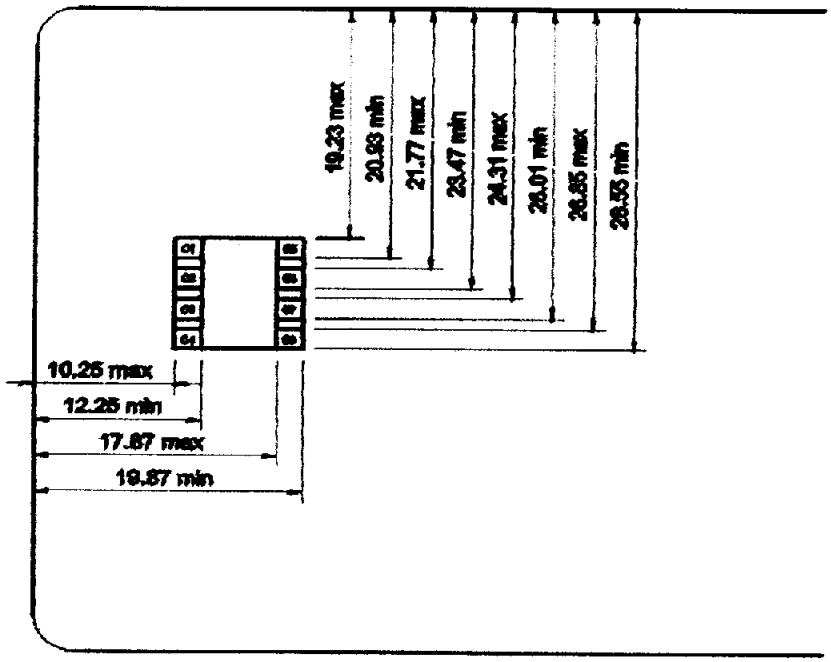


Figura 1.7 Posición de los contactos en la tarjeta.

3.-Asignación de los contactos.

Cada pin de contacto debe ser asignado según las especificaciones de la tabla 1.3.

Asignación de Pins: ISO7816-2	
C1 VCC (5V)	**C5** Tierra
C2 RST	**C6** VPP
C3 Reloj	**C7** I/O
C4 RFU	**C8** RFU

Tabla 1.3 Asignación de pins

4.-Localización de contactos respecto a otras tecnologías.

El embosado que se muestra a continuación es localizado en el mismo lado que los contactos, la banda magnética que se muestra, esta ubicada en el lado posterior, para mayor referencia se muestra la figura 1.8, como se puede observar, las líneas marcadas muestran el lado principal de la tarjeta, mientras que la banda magnética se representa con rayas punteadas.

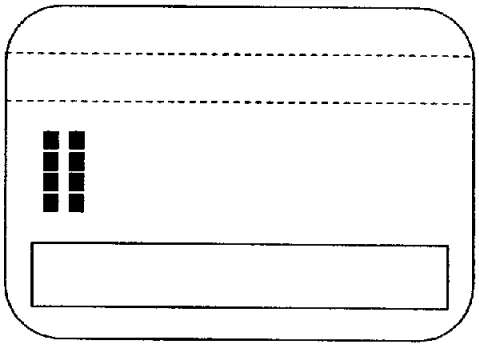


Figura 1.8 Localización respecto a otras tecnologías

Comunicación entre la tarjeta y los dispositivos externos .

Debido a la existencia de un único canal de comunicaciones entre la tarjeta y los dispositivos externos, ambos deben de turnarse para llevar a cabo la transmisión de datos. A este procedimiento intermitente de enviar y recibir información se le denomina half duplex.

El procedimiento full duplex, donde cada parte puede enviar y recibir al mismo tiempo, aún no está disponible en ninguna de las tarjetas inteligentes, sin embargo, la mayoría de los microprocesadores incorporan un canal de entrada y otro de salida, y como dos contactos de los ocho disponibles que posee una tarjeta están sin uso, se podría utilizar uno de ellos para añadir una segunda vía de comunicación.

Toda comunicación que se realice con una tarjeta es iniciada siempre por el dispositivo externo, esto quiere decir que la tarjeta nunca transmite información sin que se haya producido antes una petición externa. Esto equivale a una relación maestro-esclavo, siendo el terminal maestro y la tarjeta el esclavo.

Cada vez que se inserta una tarjeta en la terminal lector, sus contactos se conectan a los del terminal y éste procede a activarlos eléctricamente, a continuación, la tarjeta inicia un reset de encendido y envía una respuesta llamada ATR (answer to reset) hacia el terminal. Esta respuesta contiene información referente ha como ha de ser la comunicación tarjeta-lector, estructura de los datos intercambiados, protocolo de transmisión, etc. Una vez que el dispositivo lector interpreta el ATR procede a enviar la primera instrucción. La tarjeta procesa la orden y genera una respuesta que es enviada al terminal. El intercambio de instrucciones y respuestas acaba una vez que la tarjeta es desactivada.

Entre la respuesta ATR y la primera orden enviada, el terminal puede transmitir una instrucción de selección del tipo de protocolo o PTS . esto sucede cuando la tarjeta especifica mas de un protocolo en la respuesta al reset y el terminal no sabe cual usar. Todos los datos enviados por la línea de comunicación son digitales y usan valores de 0 y 1 . Los valores de tensión usados son 0 y 5 volts parte de la información contenida en la ATR tiene la misión de informar sobre que valor de tensión se va a aplicar en cada digito binario. El método de comunicación usado en las tarjetas inteligentes es el de transmisión serie.

1.6.3.- ISO/IEC 7816-3 PROTOCOLOS DE TRANSMISIÓN Y SEÑALES ELECTRICAS.

En esta norma, se especifica la alimentación, formato de señales y la información de intercambio entre el circuito integrado de la tarjeta y la interfase.

Descripción de los símbolos eléctricos que se utilizan:

I/O: Entrada y/o salida para los datos de serie al circuito integrado dentro de la tarjeta.
VPP: Voltaje de programación, uso optativo por la tarjeta.
GND: Tierra .
CLK: Señal de reloj, uso optativo por la tarjeta.
RST: Reestablecimiento(restablezca signo proporcionado del dispositivo de la interface) o en combinación con un reset interno el circuito del mando reestablecimiento(uso optativo por la tarjeta). Si el reset interno se lleva a cabo, el suministro de voltaje en Vcc es obligatorio.
VCC: Suministro energía, uso optativo por la tarjeta.
RFU: Reservado para el uso futuro

Símbolos de los voltajes y corrientes:

Vih: Voltaje de la entrada nivel alto.
Vil: Voltaje de la entrada nivel bajo.
Vcc: Energía suministra voltaje a VCC.
Vpp: Voltaje programación.
Voh: Voltaje del rendimiento nivel alto.
Vol: Voltaje del rendimiento nivel bajo.
tr: Tiempo del levantamiento entre 10% y 90% de amplitud señalada.
tf: Cada tiempo entre 90% y 10% de amplitud señalada.
Iih: Corriente de la entrada nivel alta.
Iil: Corriente de la entrada nivel baja.
Icc: Suministro actual a VCC.
Ipp: Programando actual a VPP.
Ioh: Corriente del rendimiento nivel alta.
Iol: Corriente del rendimiento nivel baja.
Cin: Capacitancia de la entrada.
Cout: Capacitancia de la salida.

Las características eléctricas de I/O bajo condiciones de funcionamiento normales.

Este contacto se usa como entrada (modo de recepción) o salida (modo de transmisión) para el intercambio de datos. Dos posibles estados existen para I/O:

- Marca o estado alto (estado Z), si la tarjeta y el dispositivo de la interfase están en modo de recepción o si el estado es impuesto por el transmisor.
- Espacio o estado bajo (estado A), si este estado se impone por el transmisor.

Cuando los dos extremos de la línea están en modo de recepción, la línea será mantenida en estado Z. Cuando los dos extremos están en modo de transmisión, el estado lógico de la línea puede ser indeterminado. Durante el funcionamiento, el dispositivo de la interfase y la tarjeta no deben estar ambos en modo de transmisión.

Simbolo	Condiciones	Mínimo	Máximo	Unidad
V_{ih} I_{ih}	Vih	0.70 x Vcc -300	Vcc +20	V uA
Vi_L Ii_L	Vil	0 -1000	0.15 x Vcc +20	V uA
V_{oh} I_{oh}		0.70 v Vcc	Vcc +20	V uA
V_{oL}	$I_{oL} = 1\,mA$ [a]	0	0.15 x V_{cc}	V
Tr tf	$C_{in} = 30\ pF$; $C_{out} = 30\ pF$		1	uS
El voltaje I/O permanecerá entre -0.3v y +0.3 V.				
[a] las aplicaciones de dispositivo de interfase no deben exigir a la tarjeta más de 500 uA				

Tabla 1.4 Características eléctricas de I/O de las tarjetas

A continuación se hace una descripción de los símbolos mas importantes:

VPP

Este contacto puede proporcionar el voltaje exigido para programar o para borrar la memoria no-volátil interior. Dos posibles estados existen para VPP: Estado pasivo y el estado activo, el estado pasivo será mantenido por el dispositivo de la interfase a menos que el estado activo sea requerido.

Simbolo	Condiciones	Mínimo	Máximo	Unidad
V_{pp} I_{pp}	Estado pausa	0.95x Vcc	1.05 x Vcc 20	V mA
V_{pp} I_{pp}	Estado programación	0 -1000	0.15 x Vcc +20	V mA
tr tf		a	1200	uS
La potencia no debe exceder 1.5 W por un periodo de 1s				

Tabla 1.5 Características eléctricas Vpp.

CLK

La frecuencia real, entregada por el dispositivo de la interfase en el pin CLK, es o designado por fi la frecuencia inicial durante la respuesta a restablezca, o por fs la frecuencia subsecuente durante la transmisión subsecuente.

Para los funcionamientos asíncronos estará entre 45% y 55% de el periodo durante el funcionamiento estable. El cuidado se tendrá al cambiar frecuencias (del fi al fs) para asegurar que ningún pulso es más corto que 45% del periodo más corto.

Protocolo tipo T

Una vez que la tarjeta ha enviado toda la respuesta al reset o ATR, espera que el terminal externo le proporcione la primera instrucción. Existen varias maneras de estructurar la comunicación entre ambos dispositivos. Los protocolos de transmisión especifican con precisión cómo han de ser las instrucciones, las respuestas a las mismas y el procedimiento a seguir en caso de que se produzcan errores durante la transmisión. Existen 15 protocolos distintos.

Protocolo de transmisión	Significado
T=0	Transmisión byte a byte de manera asíncrona y half duplex
T=1	Transmisión por bloques de manera asíncrona y half duplex
T=3	Transmisión por bloques de manera asíncrona y full duplex
T=4	Expansión del protocolo T=0
T=5 hasta T=13	Aún sin especificar
T=14	Para funciones nacionales, no está especificado por ISO
T=15	Aún sin especificar

Tabla 1.6 Descripción de los distintos tipos de protocolos

Dos de estos protocolos son los más usados en la actualidad. El primero es T=0 que fue diseñado en 1989 (ISO/IEC7816/3). El segundo es T=1 que fue introducido en 1992. El T=2 está siendo estudiado en la actualidad y estará disponible en pocos años.

El protocolo T=14 es usado en Alemania en las tarjetas de pago telefónico y fue diseñado por la compañía DBP Telekom.

A cada unidad de datos que transporta un protocolo se le denomina TPDU (Transmisión Protocol Data Unit). Estas unidades son las encargadas de llevar la información entre la tarjeta y el terminal y viceversa.

Aparte de los protocolos citados en la Tabla anterior existen otros aplicados únicamente en las tarjetas de memoria y que son síncronos. La aplicación mas corriente es la del pago de cabinas en tarjetas de teléfono, tarjetas de seguros médicos y similares. Estos protocolos no poseen técnicas para corrección de errores.

El protocolo de transmisión T=0

Fue usado en Francia durante la fase inicial del desarrollo de tarjetas inteligentes y fue el primero en incluirse dentro de un estándar internacional. Es un protocolo orientado al uso del byte, esto quiere decir que la unidad mínima de información procesada es un byte.

-La unidad de datos o TPDU consiste en una cabecera que incluye un byte para especificar la clase de instrucción (CLA), otro para el código de la misma (INS) y tres bytes adicionales que actúan como referencias (P1,P2 y P3) A la cabecera le sigue opcionalmente una sección de datos.

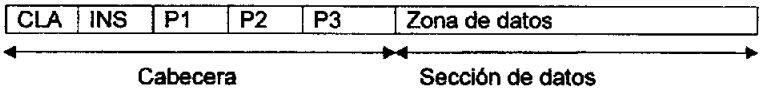


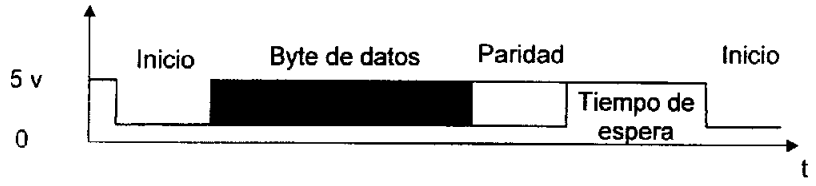
Figura 1.9 Formato de la instrucción del protocolo

El byte CLA es la clase de instrucción. El valor FFH está reservado para la selección del tipo de protocolo o PTS. El byte INS especifica el código de la instrucción. Este campo sólo es valido si el bit menos significativo es igual a cero, y el byte más significativo tiene cualquier valor distinto a 6 y 9.

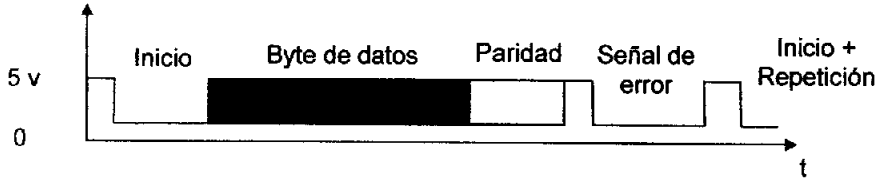
P1 y P2 son referencias, por ejemplo una dirección que completa el código de la instrucción El byte P3 especifica el número de bytes que serán transmitidos en la sección de datos (instrucción de escritura) o los bytes que serán leidos (instrucción

de lectura). Cuando P3 es igual a cero y la orden es de lectura, la tarjeta enviara una cadena de 256 bytes.

En caso de que se detecte un error en la transmisión de algún byte, se debe proceder al reenvío del byte dañado. El único mecanismo de detección de errores es el bit de paridad. Cuando el receptor detecta un error después de recibir el bit de paridad, debe poner la línea de comunicaciones a nivel bajo(0 voltios) al menos durante un ETU y como máximo dos.
Esto sirve para que el dispositivo transmisor compruebe si los datos se recibieron correctamente. Si la línea, después de transmitir los datos, está a nivel alto, quiere decir que la recepción fue correcta, en caso contrario se procede al reenvío del byte erróneo después de finalizar la señal de error.



Recepción sin errores



Recepción con errores

Figura 1.10 Esquema de recepción con errores y sin errores.

El protocolo T=0 proporciona un mecanismo para activar o desactivar la tensión de programación de la EEPROM. Esta tensión es suministrada a través del contacto VPP. El mecanismo consiste en el envío por parte de la tarjeta de un byte de procedimiento cada vez que recibe una instrucción con ese byte indica al terminal lector que es lo que debe hacer a continuación. Existen tres tipos de bytes de procedimiento cada vez que recibe una instrucción, con este byte indica al lector qué es lo que debe hacer a continuación. Existen tres tipos de bytes de procedimiento:

ACK

Indica al terminal lector cómo controlar la tensión sobre VPP y cómo transferir el resto de los datos. El valor ACK está relacionado con el código de instrucción,

NULL

Tiene el valor 60h e indica que no se debe de cambiar la tensión sobre VPP. En este caso el terminal lector espera por un nuevo byte de procedimiento

SW1

Tiene el valor 6Xh ó 9Xh excepto 60h. Cuando el terminal recibe este byte de procedimiento debe desconectar la tensión sobre VPP y espera por el byte de procedimiento SW2

SW2

Con este byte termina la ejecución de la instrucción en curso y la tarjeta está lista para recibir una nueva orden.

Byte de procedimiento	Valor	Descripción de la acción requerida por la tarjeta
ACK	INS	Desactivar VPP y a continuación se transfieren todos los bytes de datos restantes.
	INS +1	Activar VPP y transferir todos los datos restantes
	INS	Desactivar VPP y transferir el siguiente byte de datos
	INS +1	Activar VPP y transferir el siguiente byte de datos.
NULL	60h	No existe acción sobre VPP. El terminal espera por el siguiente byte de procedimiento.
SW1	6Xh o 9Xh menos 60h	Desactivar VPP, el terminal espera por SW2
SW2	Depende del valor de SW1	La ejecución de la instrucción en curso ha finalizado, el terminal puede enviar una nueva orden.

Tabla 1.7 Resumen de la interpretación de los bytes de procedimiento.

En las tarjetas inteligentes modernas no es necesario aplicar un voltaje sobre VPP y por esto pueden obviarse las instrucciones referentes al estado de dicho contacto.

La secuencia de procesamiento de una orden es la siguiente: el terminal envía a la tarjeta la cabecera de 5 bytes de la instrucción. Si no hubo errores, la tarjeta envía un byte de procedimiento, si es NULL el terminal espera por otro byte. Si el byte recibido es ACK, el terminal debe interpretarlo y realizar la acción requerida por la tarjeta. Este mecanismo termina cuando todo el paquete de datos se ha enviado o recibido. Entonces la tarjeta envía la pareja de bytes SW1 y SW2 que indican al terminal si la orden se proceso con éxito o no. En el caso de fallo, los bytes SW1 y SW2 indican la razón del mismo. Cuando una orden se ha procesado con éxito la secuencia final ha de ser 90h-00h. La interpretación de los bytes SW1 y SW2 depende de la instrucción transmitida.

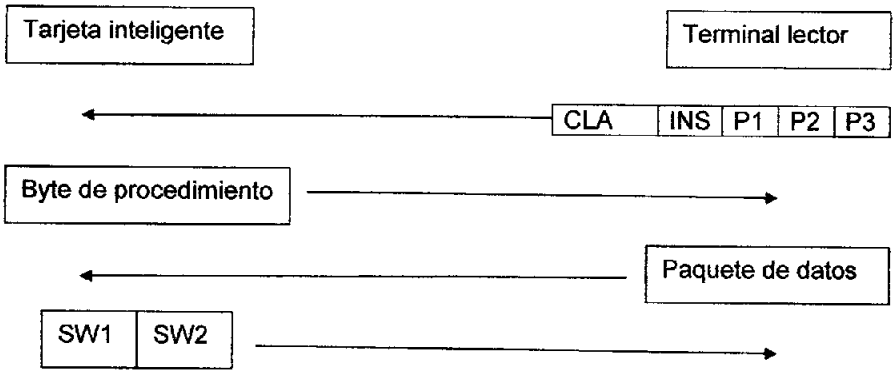


Figura 1.11 Secuencia de intercambio de comandos durante una orden de escritura.

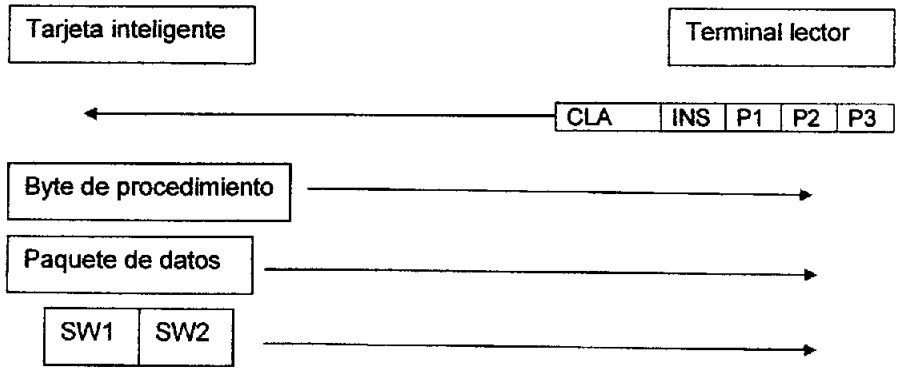


Figura 1.12 Secuencia de intercambio de comandos durante una orden de lectura.

El protocolo de transmisión T=1

Está orientado a la transmisión de bloques de manera asíncrona half duplex. Tomando como referencia el modelo de interconexión de sistemas abiertos (OSI), este protocolo opera en el nivel dos o capa de enlace. La característica principal de este protocolo es que permite formar con los vides de datos. Con esto se consigue:

- Control de flujo.
- Corrección de errores.
- Encadenamiento de paquetes.

Otra ventaja importante de este protocolo es la posibilidad de administrar en ambos sentidos el flujo de datos. El T=0 no permite que la tarjeta tome el control de las comunicaciones y solo puede enviar información por la línea de datos cuando en terminal los haya solicitado. El T=1 elimina esta barrera originada de la relación maestro esclavo, y permite que la tarjeta envíe comandos de igual manera que el terminal lector.

Las desventajas que presenta este tipo de protocolo son :

- Mayor complejidad del sistema operativo.
- Incremento en le uso de la memoria de la tarjeta.

Protocolo de PTS

Sólo el dispositivo de la interfase permite empezar un procedimiento de PTS:
El dispositivo de la interfase envía una demanda de PTS a la tarjeta.
Si la tarjeta recibe que un PTS correcto, contesta enviando un PTS confirmación, si llevó a cabo o el tiempo de espera inicial se excederá.
Después del intercambio sucesivo de demanda de PTS y PTS confirme, se transmitirán datos del dispositivo de la interfase que usa el tipo protocolar seleccionado y/o parámetros de la transmisión.
Si la tarjeta recibe un PTS erróneo, piden, no enviará un PTS confirmación. - Si el tiempo de espera inicial se excede, el dispositivo de la interfase debe rechazar la tarjeta.
Si el dispositivo de la interfase recibe un PTS erróneo confirma, debe restablecer o debe rechazar la tarjeta.
Los parámetros para la transmisión de la demanda de PTS y PTS confirman corresponderá a aquéllos usados dentro de la Respuesta para Restablecer con respecto a la proporción del bit y la convención descubierta por TS y posiblemente modifica por TC1.

CAPITULO 2. CARACTERIZACIÓN DEL CIRCUITO INTEGRADO PARA EL USO DE TARJETAS CON CHIP INTELIGENTE 256-BYTE EEPROM SLE 4432/SLE 4442.

2.1. Corrientes y voltajes.

a) Alimentación. Los valores del voltaje de alimentación se encuentran en la tabla 2.1

Parámetro	Símbolo	Valores limites		Unidad
		Min.	Max.	
Alimentación	V_{CC}	-0.3	6.0	V
Voltaje de la entrada	V_I	-0.3	6.0	V
Temperatura de almacenamiento	Tstg	-40	125	°C
Potencia consumida	P_{tot}		70	mW

Tabla 2.1 Voltaje de alimentación.

Si se sobrepasan los valores máximos. pueden causar daño permanente al dispositivo. Los valores considerados dentro del rango se consideran propicios para una buena operación del dispositivo. Exponer el dispositivo a los rangos máximos y o mínimos por periodos prolongados puede afectar la fiabilidad del producto, incluyendo la retención de datos de la memoria así como reducir los ciclos de borrado y escritura en la memoria. .

b) Rangos de operación: Los rangos del voltaje y corriente de alimentación se muestran en la tabla 2.2

Parámetro	Símbolo	Valores			Unidades	Condiciones de prueba
		Min.	Tipico	Max.		
Voltaje alimentación	V_{CC}	4.75	5.0	5.25	V	
Corriente alimentación	I_{CC}		3	10	mA	V_{CC}= 5 V
Temperatura ambiente	T_A	0		70	°C	

Tabla 2.2 Rangos de operación.

c) Características en DC: Los rangos de voltajes y corrientes cuando la tarjeta está en operación se muestran en la tabla 2.3.

Parámetro	Símbolo	Valores			Unidades	Condiciones de prueba
		Min.	Típico	Máx.		
Voltaje entrada nivel alto (I/O,CLK,RST)	V_{IH}	3.5		Vcc	V	
Voltaje entrada nivel bajo (I/O,CLK, RST)	V_{IL}	0		0.8	V	
Corriente entrada nivel alto (I/O,CLK,RST)	I_{IH}			50	µA	V_{IH} =5 V
Corriente de salida nivel bajo (I/O)	I_{OL}	1			mA	V_{OL} = 0.4 V drenado abierto
Corriente salida nivel alto (I/O)	I_{OH}			50	µA	V_{OH} = 5V drenado abierto
Capacitancia de entrada	CI			10	pF	

Tabla 2.3 Valores de voltaje y corrientes cuando la tarjeta esta en funcionamiento

d) Características en AC: Se refieren a los valores en los diagramas de tiempos típicos de la tarjetas

Parámetro	Símbolo	Valores			Unidades	Condiciones de prueba
		Min.	Típico	Max.		
RST alto a CLK tiempo de espera	t_{10}	4			µs	
CLK bajo y RST tiempo espera	t_{11}	4			µs	
RST alto tiempo (reset a dirección)	t_{12}	20	50		µs	
RST bajo a validación tiempo I/O	t13			2.5	µs	
RST bajo a CLK tiempo set up	t_{14}	4			µs	
Frecuencia de reloj	f_{CLK}	7		50	khz	
Tiempo levantamiento reloj	t_R			1	µs	
Tiempo caida reloj	t_F			1	µs	
Tiempo alto reloj	t_{15}	9			µs	
Tiempo bajo reloj	t_{16}	9			µs	
Tiempo bajo de i/o	t_{17}			2.5	µs	
Tiempo reseteo rompimiento	t_{18}	5			µs	
RST alto ara I/O tiempo limpio (descanso)	t_{19}	2.5			µs	
I/O Tiempo alto condición salida	t_1	10			µs	

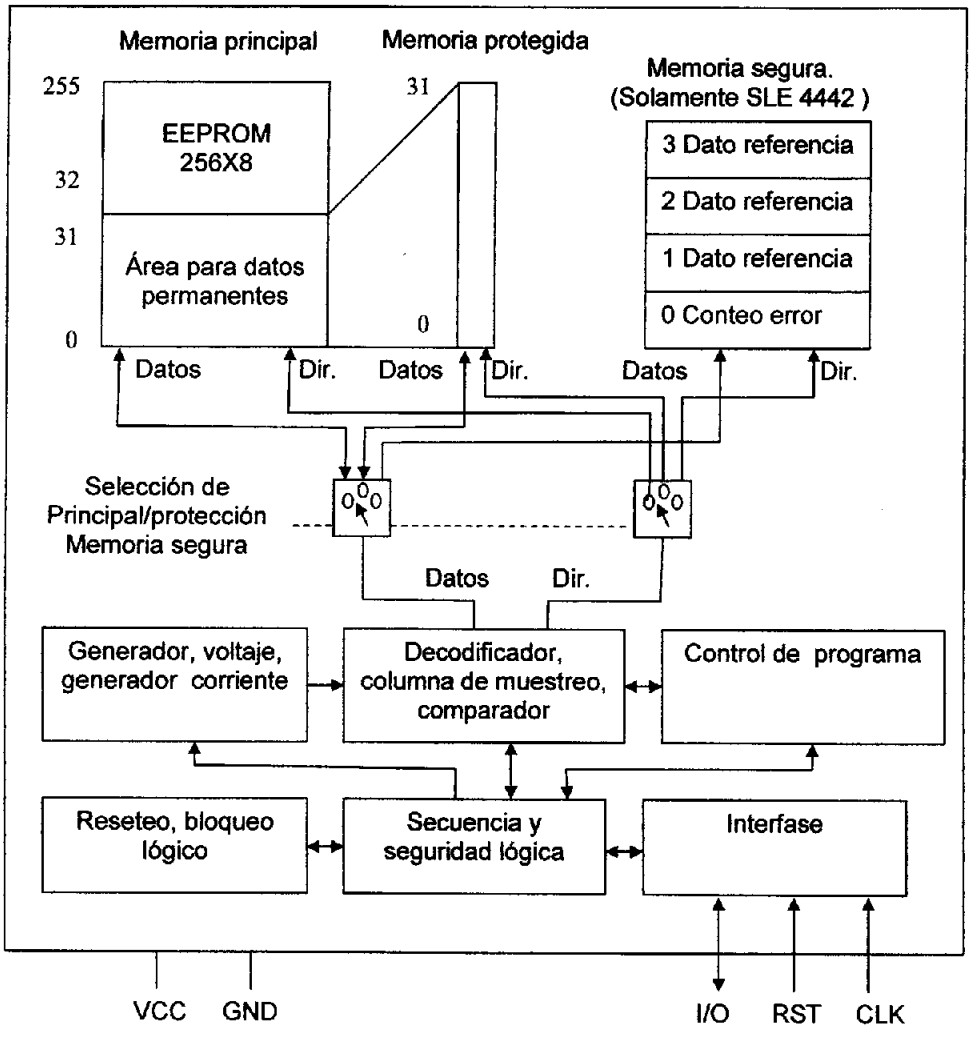
Continuación....

Parámetro	Símbolo	Valores			Unidades	Condiciones de prueba
		Min.	Tipico	Max.		
Reloj alto a I/O tiempo espera	t_2	4			µs	
I/O bajo y reloj en espera (condición salida)	t_3	4			µs	
I/O setup a clk tiempo alto	t_4	1			µs	
Reloj bajo a I/O tiempo descanso	t_5	1			µs	
Reloj alto a I/O tiempo limpio (condición de alto)	t_6	4			µs	
Reloj bajo y tiempo de validación I/O	t_7			2.5	µs	
Reloj bajo y tiempo de validación I/O	t_8			2.5	µs	
Reloj bajo y tiempo de limpieza	t_9			2.5	µs	
Tiempo de borrado	t_{ER}	2.5			ms	f_{CLK}=50 kHZ
Tiempo de escritura	t_{WR}	2.5			Ms	f_{CLK}=50 kHz
Tiempo restablecimiento encendido	t_{POR}			100	µs	

Tabla 2.4 Valores de respuesta en AC

NOTA: Los resultados mostrados se realizan por encima del rango de operación del circuito integrado. Las características se evalúan a una temperatura ambiente de T_A = 25 °C y el voltaje del alimentación dado.

2.2 Arquitectura.



Funcionamiento global de la memoria.

SLE 4432 Contiene 256 X 8 bit en la memoria EEPROM principal y 32 bit de protección de memoria con funcionalidad PROM. La memoria principal es borrada y escrita byte por byte. Cuando se borra, todos los 8 bits de datos son puestos a un uno lógico. Cuando se escribe, la información en cada célula de la EEPROM es, de acuerdo con los datos de entrada, modificada bit por bit a ceros lógicos. (lógica AND entre los datos viejos y los nuevos en la EEPROM). Normalmente, el cambio de datos consiste en un proceso de borrado y escritura. Esto depende de los contenidos de los bits de datos en la memoria principal y el nuevo dato para determinar si la EEPROM es realmente borrada o escrita. Si ninguno de los 8 bits en la dirección requiere un cambio cero-uno, el borrado es suprimido. Y viceversa, el acceso de escritura puede ser suprimido si no es necesario el cambio uno-a-cero. La operación de escritura y borrado toma alrededor de 2.5 mseg. cada uno.

Cada uno de los primeros 32 bytes puede protegerse irreversiblemente contra los cambios de datos escribiendo la dirección correspondiente en la memoria de la protección. Cada byte de datos en este rango de dirección se asigna a un bit de la memoria de la protección y tiene la misma dirección como el byte de los datos en la memoria principal a la que se asigna. Una vez escrito el bit de protección no puede borrarse (Prom)

Adicionalmente a las funciones anteriores el SLE 4442 provee un código de seguridad lógica que controla el acceso de escritura/borrado en la memoria. Para este propósito, el SLE 4442 contiene una seguridad de 4 bit en la memoria con un contador de error EC (bit 0 a bit 2) y 3 bits como referencia de datos. Estos 3 bytes se llaman código de seguridad programable. (Programmable Security Code). Después de encender la memoria, a excepción de los datos de referencia, solamente pueden ser leídos. Solamente después de una comparación exitosa de verificación, entre los datos y la referencia interna de los datos, la memoria tiene el mismo funcionamiento que el SLE 4432 hasta que la energía no sea desconectada. Después de tres comparaciones sucesivas no exitosas, el contador de error bloquea cualquier posibilidad de escritura y borrado.

2.3. Modos de operación.

Después de la respuesta al reset, el chip espera un comando. Cada comando empieza con una condición de salida, incluye una longitud de 3 bites seguida de un pulso de reloj y termina con una condición de alto.

-condición de la salida: flanco de bajada en el i/o del pulso de reloj en nivel alto.
-condición de alto: flanco de subida en I/O durante el pulso de reloj en nivel alto

después de realizado un comando se tiene dos posibles modos:

-Salida de datos para lectura:

En este modo el circuito integrado le envía datos al IFD. El primer bit se vuelve válido en I/O después del primer flanco de caída en el reloj. Después de que los últimos datos es necesario un pulso del reloj para pone I/O en estado de impedancia alta Z y se prepara el IC para un nuevo comando Durante este modo, cualquier condición de salida y la parada se desecha.

Modo de proceso:

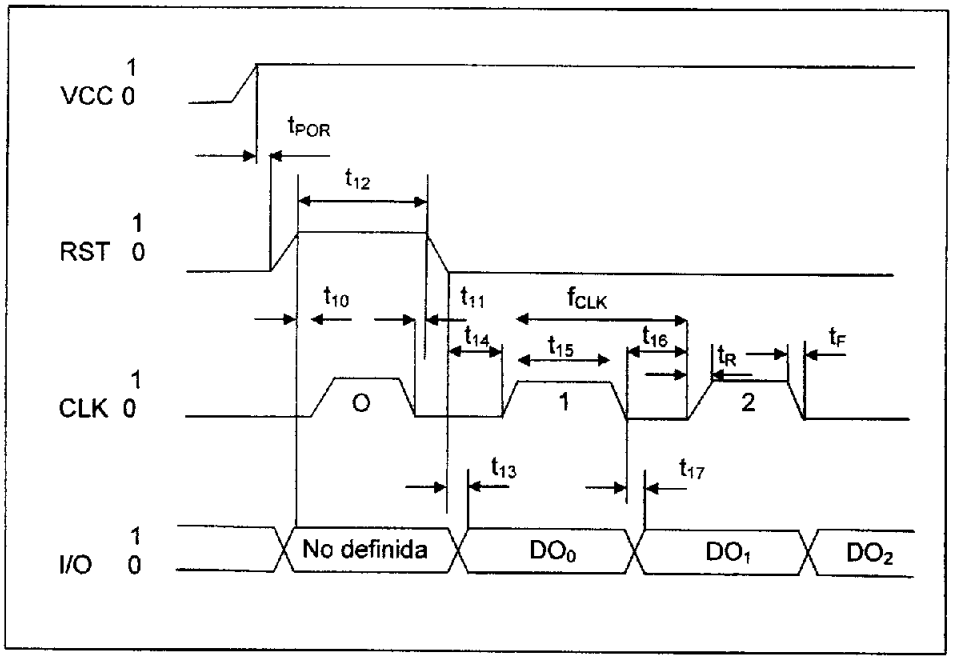
El circuito integrado procesa internamente y el que ser continuamente pulsado hasta i/o que se cambió ti L nivelado después del primer flanco de caída del reloj se pone a la impedancia alta z nivelado cualquier condición de salida y parada se desecha durante este modo.

Nota: La señal de RST es baja durante los modos de operación. Si el RST está en alto durante un nivel bajo de reloj (CLK), cualquier operación es abortada y la I/o es puesta a alta impedancia.

2.4. Diagramas de Tiempos.

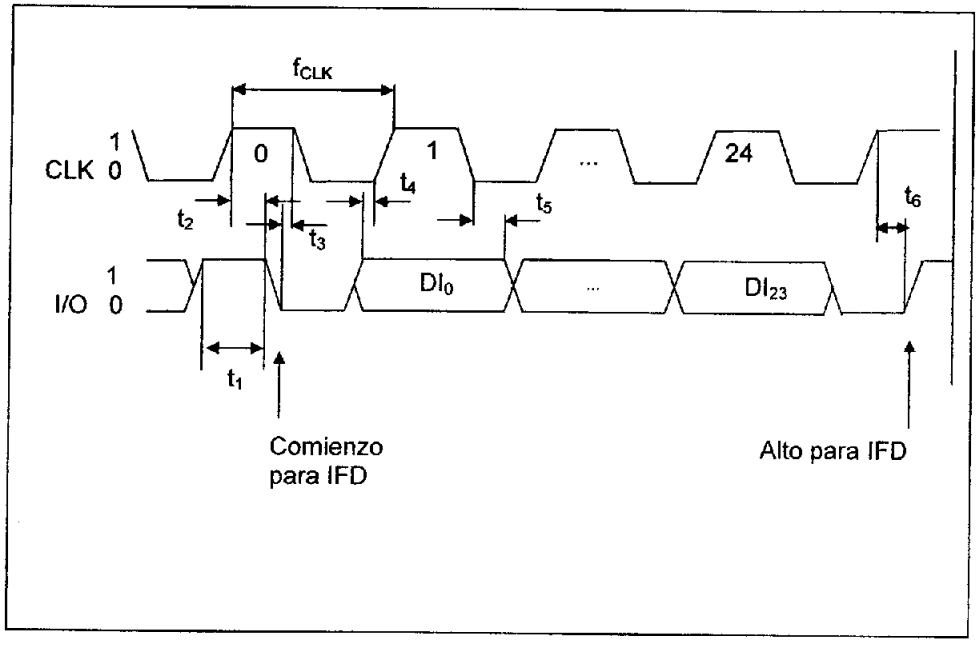
Al considerar los diagramas de tiempo podemos entender mas el funcionamiento interno de la tarjetas. En la mayoría de los equipos electrónicos es necesario contar con un reloj, el cual va a servir para que el sistema pueda sincronizar los procesos. Ya sea en un periodo positivo o negativo, el sistema realizara diversos operaciones, como el envío o recepción de información, la consulta a memoria, o simplemente el estar en estado de espera. Aquí mostraremos los diagramas de tiempo para las tarjetas SLE4432 y SLE 4442.

Tiempo en modo Reset y respuesta al reset



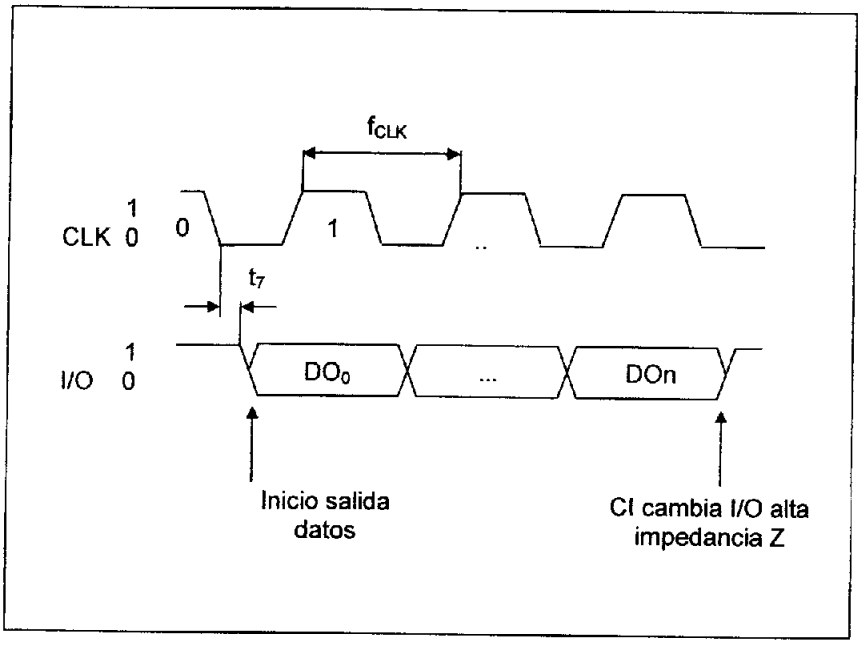
En este diagrama se tienen los principales estados en los que puede estar una tarjeta, en el primer renglón el VCC esta puesto en uno, es decir, se encuentra energizada nuestra tarjeta. El segundo renglón, tiene un reestablecimiento por parte de la tarjeta, se puede observar que existe un tiempo entre la energización, y la respuesta de la tarjeta, esta representado por t_{POR} en el tercer renglón veremos los pulsos del reloj, y en el ultimo esquema, se podrá apreciar la entrada/salida de datos. Como se puede apreciar, cada símbolo que aparece, tiene su descripción en las tablas mostradas anteriormente llamadas características en corriente alterna.

Tiempos en modo de comando



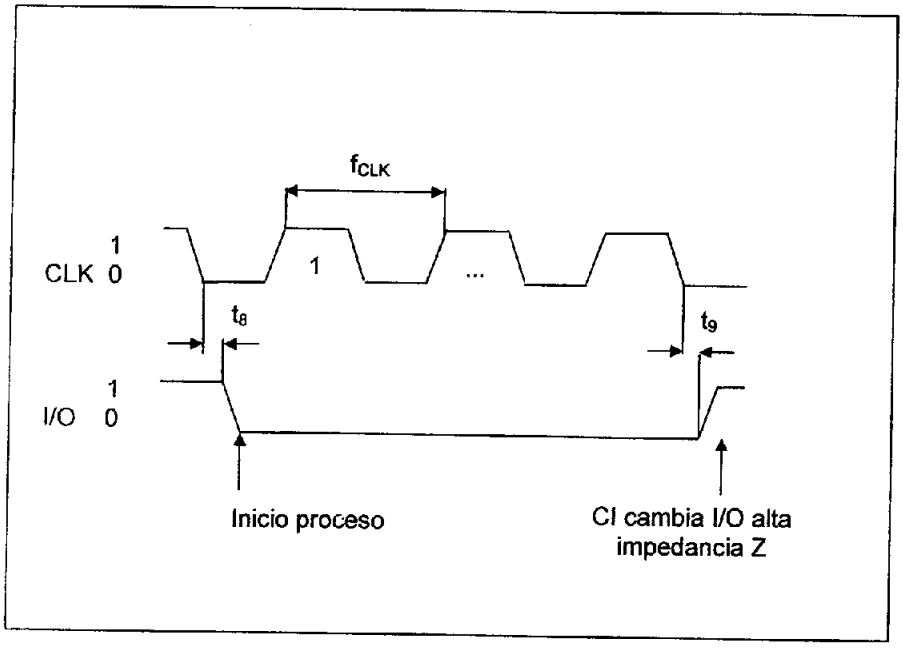
En este diagrama nos muestra solamente el reloj y la entrada salida, durante los modos de comandos, es decir cuando recibe una instrucción la tarjeta, podemos ver el comportamiento de la E/S de esta.

Tiempo en modo salida de datos:



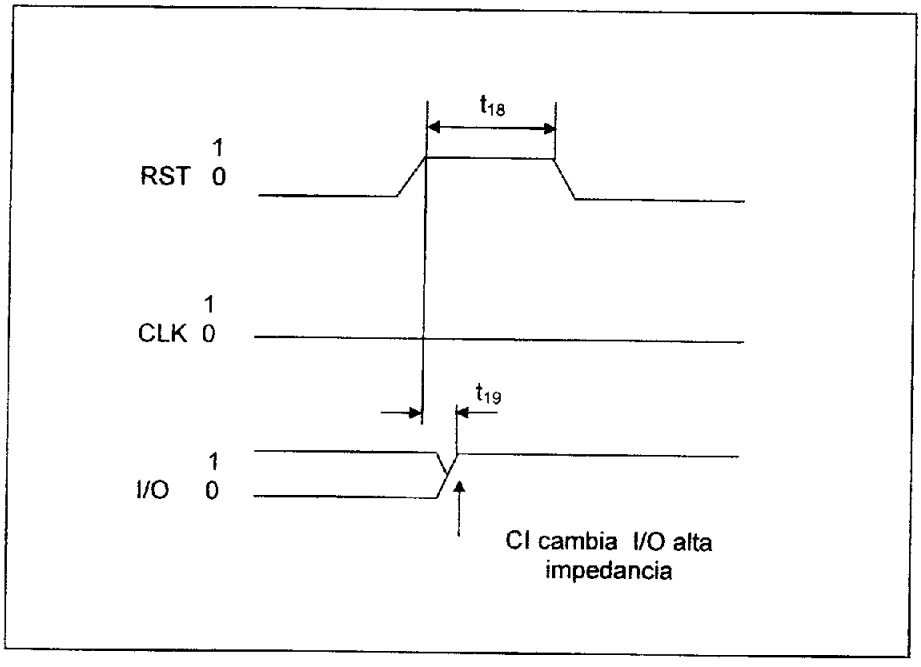
En el diagrama podemos ver que en cada ciclo positivo o puesta en uno del reloj, se estará enviando información, generalmente la frecuencia de operación es de 50 khz,

Tiempos en modo de procesamiento de datos



Cuando se encuentra procesando datos internamente la tarjeta, se tiene que no hay ni envío ni recepción de datos como se muestra en este diagrama.

Tiempo en rompimiento



En el caso de un rompimiento, esto es, se corte de alguna forma la frecuencia, automáticamente la tarjeta va a entrar a un estado de reseteo.

2.5 Mapa de memoria.

Esta es una referencia de como se encuentra organizada la memoria de nuestra tarjeta de estudio.

Dirección (decimal)	Memoria Principal	Memoria Protegida	Memoria de Seguridad (solamente SLE 4442
255	Dato 255 (D7...D0)		
:	:		
32	Dato 32 (D7... D0)		
31	Dato 31 (D7 ...D0)	Bit protegido 31 (D31)	
:	:	:	
3	Dato 3 (D/ ...D0)	Bit protegido 3 (D3)	Byte dato referencia 3 (D7...D0)
2	Dato 2 (D7...D0)	Bit protegido 2 (D2)	Byte dato referencia 2 (D7...D0)
1	Dato 1 (D7...D0)	Bit protegido 1 (D1)	Byte dato referencia 1 (D7...D0)
0	Dato 0 (D7...D0)	Bit protegido 0 (D0)	Contador error (0,0,0,0,0,D2,D1,D0)

Tabla 2.5 Mapa de memoria de la tarjeta SLE4432.

Los bits de datos del 0 al 31 pueden protegerse contra los cambios mas allá de los programados al momento de la fabricación. El SLE 4442 permite modificar datos que sólo cambian después de la comprobación correcta de los bytes de datos de referencia.

2.6 Protocolos.

El protocolo de la transmisión entre la interfase del dispositivo IFD y el circuito integrado IC. Es idéntico al tipo protocolo S = A. Todos los datos se intercambian en el pin I/O cuando es inicializado por el flanco de bajada del reloj

El protocolo de la transmisión controla los 4 modos de operación siguientes:

-Restablecimiento espera para restablecer.
-Modo comando.
-Modo de los datos saliente.
-Modo procesamiento de datos.

2.7 Comandos de programación.

a) Lectura en memoria principal (SLE 4432 y SLE 4442)

El comando lee fuera los volúmenes de la memoria principal comienza en el primer bit de la dirección (N=0,,,255) de principio a fin de la memoria. Después de la entrada en orden con flanco de bajada (IFD) tiene que proporcionar pulsos del reloj suficientes. El número de pulsos del reloj m = (256-N)X8+1. el acceso de lectura a la memoria principal siempre es posible.

Dirección (decimal)	Memoria principal
255	Dato 255 (D7...D0)
:	:
32	Dato 32 (D7... D0)
31	Dato 31 (D7 ...D0)
:	:
3	Dato 3 (D/ ...D0)
2	Dato 2 (D7...D0)
1	Dato 1 (D7...D0)
0	Dato 0 (D7...D0)

Tabla 2.6 Relación entre las direcciones decimales y los datos en memoria principal

Commando para leer la memoria principal: READ MAIN MEMORY.

	Control								Dirección	Dato
	B7	B6	B5	B4	B3	B2	B1	B0	A7....A0	D7...D0
Binario	0	0	1	1	0	0	0	0	Dirección	
Hexadecimal	30_H								00_H....FF_H	

b) Lectura de Memoria protegida (SLE 4432 y SLE 4442)

El comando transfiere la protección de bits bajo una continua salida de 32 pulsos de reloj hacia la salida. I/O es activado en alta impedancia Z por un pulso adicional. La protección de la memoria puede ser leida, y los indicadores de los datos de bites de la memoria principal pueden cambiar,

Dirección (decimal)	Memoria protegida
255	
:	
32	
31	Bit protegido 31 (D31)
:	:
3	Bit protegido 3 (D3)
2	Bit protegido 2 (D2)
1	Bit protegido 1 (D1)
0	Bit protegido 0 (D0)

Tabla 2.7 Relación entre las direcciones decimales y los datos al realizar una lectura en memoria protegida

Comando para lectura de memoria protegida: READ PROTECTION MEMORY

	Control								Dirección	Dato
	B7	B6	B5	B4	B3	B2	B1	B0	A7....A0	D7...D0
Binario	0	0	1	1	0	1	0	0	Sin efecto	Sin efecto
Hexadecimal	34_H								Sin efecto	Sin efecto

c) Actualización memoria la principal (SLE 4432 y SLE 4442)

El comando programa la dirección de al EEPROM con el dato transmitido. Dependiendo si es nuevo o viejo dato, una de las siguientes secuencias se lleva a cabo durante este modo.

-Borrado y escritura (5 ms) corresponden a m = 255 pulsos de reloj.
-Escritura sin borrado (2.5ms) corresponde a m= 124 pulsos de reloj.
-borrado sin escritura (2.5ms) corresponde a m= 124 pulsos de reloj.
(todos los valores corresponden a un reloj a 50KHZ)

Dirección (decimal)	Memoria Principal
255	Dato 255 (D7...D0)
:	:
32	Dato 32 (D7... D0)
31	Dato 31 (D7 ...D0)
:	:
3	Dato 3 (D/ ...D0)
2	Dato 2 (D7...D0)
1	Dato 1 (D7...D0)
0	Dato 0 (D7...D0)

Tabla 2.8 Relación entre las direcciones decimales y los datos en memoria principal en una secuencia de actualización

Comando para actualizar la memoria principal: UPDATE MAIN MEMORY.

	Control								Dirección	Dato
	B7	B6	B5	B4	B3	B2	B1	B0	A7....A0	D7...D0
Binario	0	0	1	1	1	0	0	0	Dirección	Dato entrada
Hexadecimal	38_H								$00_H...FF_H$	Dato entrada

d) Escritura en la memoria protegida (SLE 4432 y SLE 4442)

La ejecución de este comando contiene una comparación entre el dato nuevo entrante y el asignado en la EEPROM. En caso de identidad, la protección de bit se escribe haciendo los datos incambiables. Si en la comparación de datos hay cambios, la protección de datos puede ser suprimida.

Dirección (decimal)	Memoria Protegida
255	
:	
32	
31	Bit protegido 31 (D31)
:	:
3	Bit protegido 3 (D3)
2	Bit protegido 2 (D2)
1	Bit protegido 1 (D1)
0	Bit protegido 0 (D0)

Tabla 2.9 Relación entre las direcciones decimales y la memoria protegida en un ciclo de escritura.

Comando para escribir en la memoria protegida: WRITE PROTECTION MEMORY.

	Control								Dirección	Dato
	B7	B6	B5	B4	B3	B2	B1	B0	A7....A0	D7...D0
Binario	0	0	1	1	1	1	0	0	Dirección	Dato entrada
Hexadecimal	$3C_H$								$00_H...1F_H$	Dato entrada

e) Lectura en la memoria de seguridad. (solamente SLE 4442)

Similar a el comando de lectura en la memoria protegida, este comando lee únicamente 4 bits memoria de seguridad. El numero de pulsos de reloj durante la salida de datos en este modo es de 32. La I/O es activada en alta impedancia Z por un pulso adicional. Sin un procedimiento exitoso del PSC la salida de la referencia de datos es suprimida. Eso significa rendimientos de I/O para el estado L como referencia datos.

Dirección (decimal)	Memoria de Seguridad (solamente SLE 4442
255	
:	
32	
31	
:	
3	Byte dato referencia 3 (D/...D0)
2	Byte dato referencia 2 (D7...D0)
1	Byte dato referencia 1 (D7...D0)
0	Contador error (0,0,0,0,0,D2,D1,D0)

Tabla 2.10 Relación entre la dirección decimal y la lectura en la memoria de seguridad del SLE4442

Comando para leer la memoria de seguridad: READ SECURITY MEMORY.

	Control								Dirección	Dato
	B7	B6	B5	B4	B3	B2	B1	B0	A7....A0	D7...D0
Binario	0	0	1	1	0	0	0	1	Sin efecto	Sin efecto
Hexadecimal	31_H								Sin efecto	Sin efecto

f) Actualización de la memoria de seguridad (SLE 4442)

Con respecto a los bytes de datos de referencia este comando se ejecutará sólo si un PSC se ha verificado exitosamente. Por otra lado, solamente cada bit del contador de error (dirección 0) puede escribirse del 1 al 10 . El tiempo de ejecución y la cantidad de pulsos de reloj son descritos en la sección actualizando la memoria principal.

Comando para actualizar la memoria de seguridad: UPDATE SECURITY MEMORY.

	Control								Dirección	Dato
	B7	B6	B5	B4	B3	B2	B1	B0	A7....A0	D7...D0
Binario	0	0	1	1	1	0	0	1	Dirección	Dato entrada
Hexadecimal	39_H								$00_H...003_H$	Dato entrada

Comparación de datos verificados

Este comando solamente puede ser ejecutado en combinación con un procedimiento de actualización de el contador de error. (ver verificación de PSC) el comando compara un byte de la verificación de datos con el dato de referencia correspondiente. Para este procedimiento los pulsos de reloj son necesarios durante el modo de proceso.

Comando para comparar los datos verificados: COMPARE VERIFICATION DATA

	Control								Dirección	Dato
	B7	B6	B5	B4	B3	B2	B1	B0	A7....A0	D7...D0
Binario	0	0	1	1	0	0	1	1	Dirección	Dato entrada.
Hexadecimal	33_H								$00_H...03_H$	Dato entrada-

g) Verificación PSC (solamente SLE 4442)

El SLE 4442 requiere una comprobación correcta del código de seguridad programable (PSC) guardada en la memoria de seguridad por si desea alterar datos.
El procedimiento siguiente tiene que ser llevado exactamente como es descrito, cualquier variación provocará un fracaso, para que un acceso de escritura/borrado no se logre, y el procedimiento no se haya concluido con éxito el contador de error sólo pueden cambiarse de 1 a 0 pero no pueden borrarse.

La tabla 2.11 muestra una apreciación global de los comandos necesarios para la verificación del PSC. La secuencia en la zona obscura es prioridad.

Comando	Control	Dirección	Dato	comentario
	B7...B0	A7...A0	D7...D0	
Read security memory	31H	Sin efecto	Sin efecto	Checar contador de error
Update security memory	39H	00H	Dato entrada	Escritura libre en contador de error dato entrada: 0000 0ddd binario
Compare verification data	33H	01H	Dato entrada	Byte referencia 1
Compare verification data	33H	02H	Dato entrada	Byte referencia 2
Compare verification data	33H	03H	Dato entrada	Byte referencia 3
Update security memory	39H	00H	FFH	Borrado contador error
Read security memory	31H	Sin efecto	Sin efecto	Checa contador error

Tabla 2.11 Comandos de verificación para PSC

CAPITULO 3. CARACTERIZACIÓN DE LAS TARJETAS INTELIGENTES

3.1 Normas

3.1.1 ISO/IEC 7811-1 TËCNICAS DE GRABADO EN TARJETAS DE IDENTIFICACIÓN (EMBOSADO)

Este estándar especifica los requerimientos para el embozado de tarjetas de identificación.

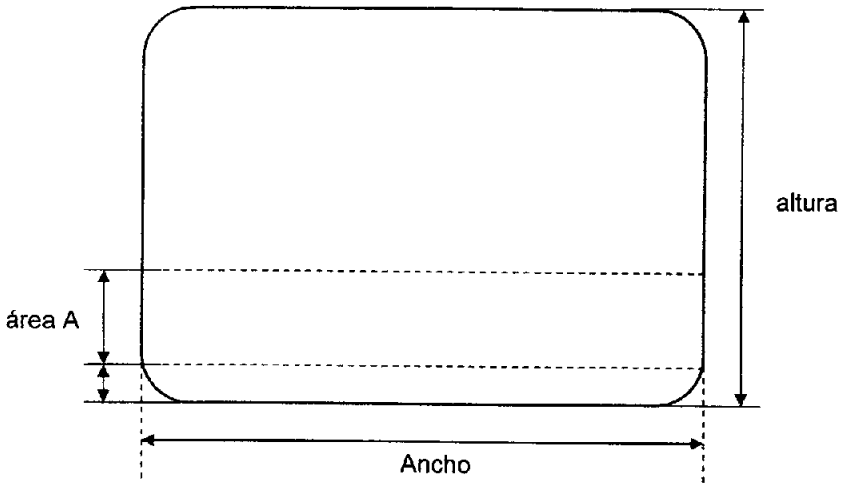


Figura 3.1 Dimensiones de la tarjeta de identificación

Dimensiones de la tarjeta:

Ancho: 85.90mm (3.382 in) máxima, 85.47mm (3.365in) min.
Altura : 54.18mm (2.133 in) máxima, 53.92(2.123in) min.
Área A : 2.54mm (0.100 in)

a. Espacio entre caracteres:

2.54mm +- 0.15mm (0.146 in +- 0.006 in)

b. Altura de los caracteres :

La altura máxima de los caracteres impresos abarca el línea central y un alineación del carácter es 4.32 mm (0.170 in)

c. Juego de caracteres,

El tipo de letra que se utilizara deberá ser la Farrington 7B la cual incluya los números 0-9

OCR-A

OCR-B

Farrington 7B

Figura 3.2 Tipo de letras utilizadas en el estándar 7811-1

d. Espacio y alineación de los caracteres

1.-El espacio nominal de los caracteres es 7 por pulgada

2.- El la separación horizontal mínima entre los caracteres adyacentes es 0.80 mm (0.015 in)

3.- La alineación vertical entre los caracteres adyacentes 2.03mm (0.080 in) máximo

4.- La inclinación de los caracteres es 3° máximo

Áreas de embozado:
Lo referente a las especificaciones de la ubicación de los embosados se tratan en la siguiente norma ISO 7811-3

3.1.2 ISO/IEC 7811-3 LOCALIZACIÓN DEL EMBOSADO DE CARACTERES EN LAS TARJETAS

Este estándar especifica la ubicación de los caracteres embosados que se piensa para el traslado de datos para el uso de impresoras o por visual o lectura de la máquina.

A. Hay dos áreas para el embozado de caracteres como se muestra en la figura 3.3

1 Área1 esta área es reservada para el número de identificación, de acuerdo con el ISO/IEC 7812. los caracteres en esta área son para identificación visual y lectura de maquinas.

2 Área 2 esta área esta creada para la identificación de la tarjeta, como es nombre, dirección y demás datos que sean requeridos. Los datos en esta área son expuestos normalmente para una lectura visual.

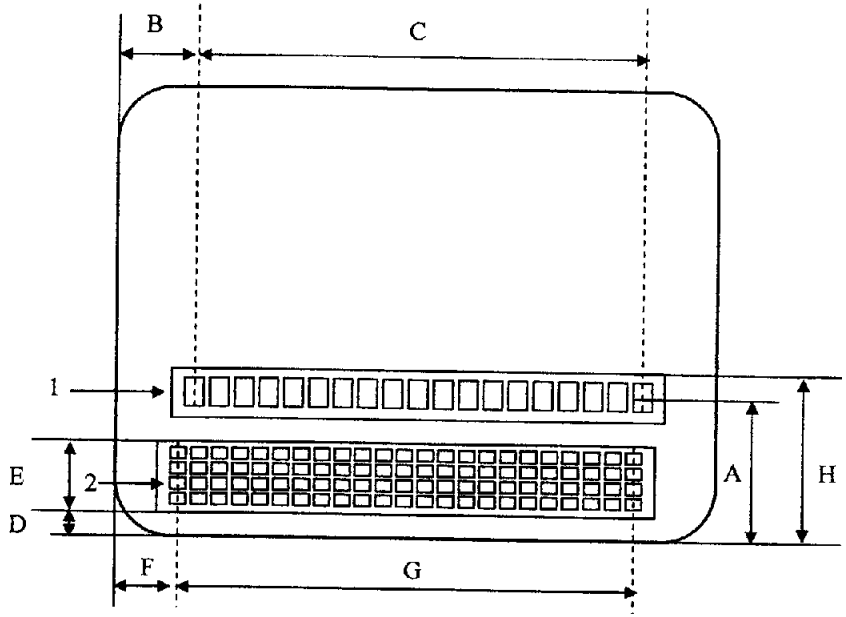


figura 3.3 Ubicación de embosado.

B. Área de Identificación de números (Vea Figura 3.3)

Esta línea es de un solo renglón y comprende un máximo de 19 carácteres a un espacio nominal de 7 carácteres por pulgada.

Las medidas son las siguientes:

a. distancia A, entre la parte media horizontal del numero de identificación al borde de la tarjeta:

21.42 mm + 0.12 mm (0.843 in + 0.005 in.)

b. distancia B, entre el centro de la posición del primer carácter y el borde izquierdo de la tarjeta:

10.18 mm + 0.25 mm (0.401 in. + 0.010 in.)

c. distancia C, entre el centro del primer carácter y el carácter 19 no debe exceder:

65.31 mm + 0.76 mm (2.571 in. + 0.030 in.)

d. distancia máxima, H, del borde inferior de la tarjeta al borde superior del área 1 debe ser:

24.03mm (0.946 in.)

C. Área de Nombre y dirección (Vea Figura 3.3)

Este área tiene espacio para cuatro renglones de 27 carácteres cada uno a un espacio nominal de 10 carácteres por pulgada. Cualquier información embosada en este área siempre debe estar cerca hasta donde sea posible del número de identificación

Las especificaciones para esta área son las siguientes:

a. la altura máxima D, debe ser:

14.53 mm (0.572 in.)

b. el margen E, en esta área y el borde inferior de la tarjeta debe ser

2.41 mm min. (0.095 in min.)
3.30 mm max. (0.130 in max.)

Nota: Cuando es utilizada junto con una banda magnética, el margen mínimo debe ser 2.54mm (0.010 in.)

c. la distancia, F, entre el centro de la posición del primer carácter y el borde izquierdo de la tarjeta:

7.65 mm + 0.25 mm (0.301 en. + 0.100 en.)

Nota: El primer carácter en el área del nombre y la dirección no se justifica a la izquierda. Sin embargo, el uso de 27 posiciones del carácter es basado en 7.65 mm (.0301 in.) la distancia al borde de la tarjeta es como se declaró anteriormente.

d. distancia de G, entre el centro del primer carácter y la posición 27 no debe exceder:

66.04 mm + .076 mm (2.600 in. + 0.030 in.)

3.2 Clasificación

Es bastante frecuente denominar a todas las tarjetas que posean contactos dorados o plateados sobre su superficie, como tarjetas inteligentes. Sin embargo, este término es bastante ambiguo y conviene hacer una clasificación mas correcta. ISO(Internacional Estándar Organization) prefiere usar el termino de 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 procesado 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 contacto por medio de campos electromagnéticos.

Estas tarjetas presentan ventajas en comparación con las de banda magnética:

- Son capaces de almacenar mas información, hasta 60 Kbytes.
- Pueden proteger la información que almacenan en sus memorias de posibles accesos no autorizados.
- Poseen una mayor resistencia la 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 lectura, escritura y borrado de la memoria pueden ser controladas tanto por hardware como por software, o por ambos ala vez. Esto permite una gran variedad de mecanismos de seguridad.

Siendo el chip integrado el componente más importante, las tarjetas están clasificadas según el tipo de circuito, así existen:

- Tarjetas de memoria.
- Tarjetas de memoria con circuitos de seguridad.
- Tarjetas con CPU o tarjetas inteligentes.

3.2.1 TARJETAS DE MEMORIA.

Los datos que se requieren para las aplicaciones con tarjetas de memoria son almacenados en una EEPROM (Electrica Erasable Programable Read Only Memory). Los accesos a esta no están controlados y por lo tanto coexiste protección contra escritura o borrado de la memoria o de alguna de sus áreas.

Las funciones que desempeñan las tarjetas de memoria están optimizadas para aplicaciones particulares en las que no se requieren complejos mecanismos de seguridad. Una aplicación típica son las tarjetas de pago en cabinas de teléfono.

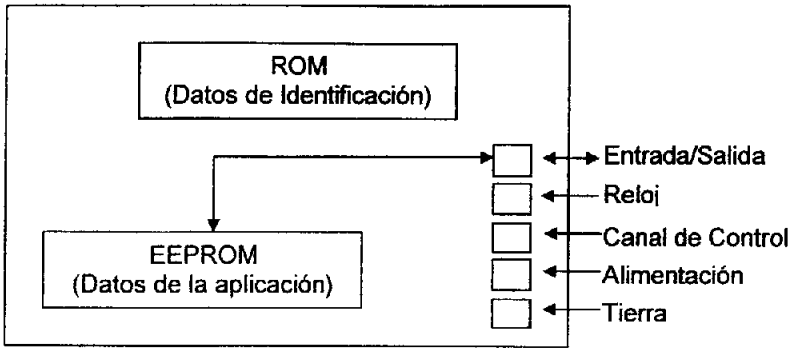


Figura 3.4 Esquema de bloques de la arquitectura de una tarjeta de memoria.

Tarjetas de memoria con circuitos de seguridad

El circuito de seguridad 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.

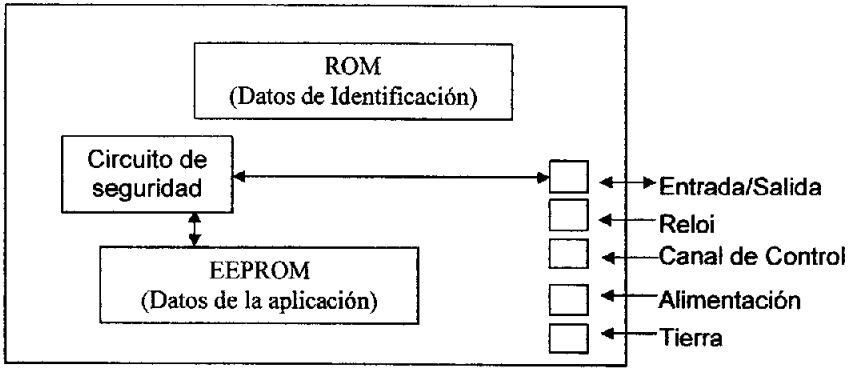


Figura 3.5 Esquema de bloques de la arquitectura de una tarjeta de memoria con circuito de seguridad.

3.2.2 TARJETAS INTELIGENTES

Estas tarjetas poseen en su chip un microprocesador, que además cuenta con algunos elementos adicionales como son:

- ROM enmascarada.
- EEPROM
- RAM.
- Un puerto de entrada/salida.

La ROM (Memoria de Lectura únicamente) enmascarada contiene el sistema operativo de la tarjeta y se graba durante el proceso de fabricación.

La EEPROM es la memoria no volátil del microprocesador y en ella se encuentran los datos del usuario o de la aplicación, así como el código de las instrucciones bajo el control de l sistema operativo. También puede contener información como el nombre del usuario, numero de identificación personal o PIN (Número de Identificación Personal), etc.

La Ram (Memoria de Acceso Aleatorio) es la memoria del trabajo del microprocesador. Al ser volátil, toda la información se perderá al desconectar la alimentación. El puerto de entrada y salida normalmente consiste en un simple registro, través del cual la información es transferida bit a bit.

Las tarjetas con microprocesador son bastante flexibles puesto que pueden realizar bastantes funciones. El caso mas simple, solo contienen datos referentes a una aplicación especifica, esto hace que dicha tarjeta solo se pueda emplear para esa aplicación sin embargo, los sistemas operativos de las tarjetas mas modernas hace n posible que se puedan integrar programas para distintas aplicaciones en una sola tarjeta. En este caso, la ROM contiene sólo el sistema operativo con las instrucciones básicas, mientras que el programa especifico de cada aplicación se graba en la EEPROM después de la fabricación de la tarjeta.

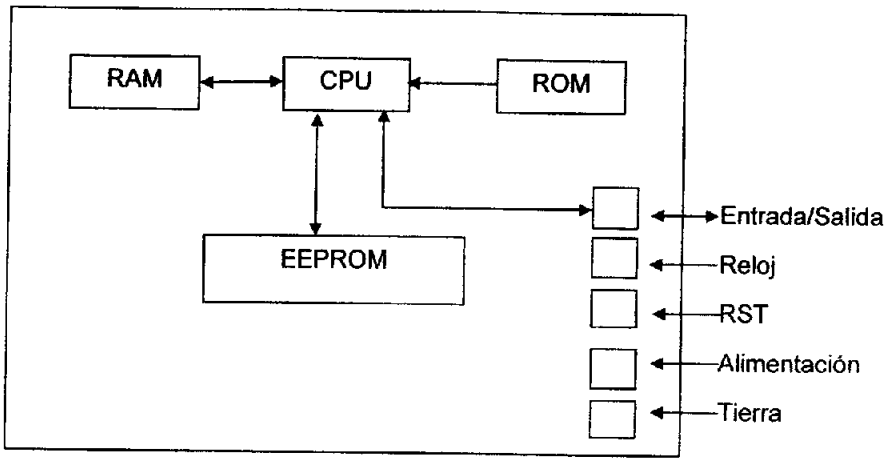


Figura 3.6 Arquitectura típica de una tarjeta con microprocesador.

Contactos en las tarjetas

Las tarjetas inteligentes pueden tener en su superficie unos contactos dedicados a posibilitar la comunicación de la propia tarjeta con los dispositivos exteriores. El tamaño y la posición de estos contactos se especifica en el estándar ISO7816 mencionada en el capítulo 1

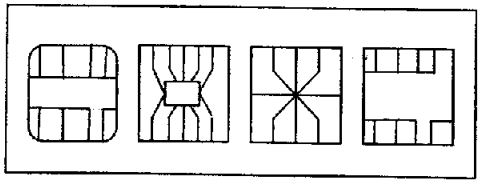


Figura3.7 Diferentes tipos de contactos.-

Como resultado de la experiencia conseguida en los últimos años por los fabricantes de tarjetas, la fiabilidad de éstas se ha visto considerablemente aumentada, por ejemplo, la tasa de fallo en tarjetas de pago en cabinas telefónicas es inferior al 0.001%, sin embargo, los contactos son casi siempre los culpables de los fallos de funcionamiento. En algunos casos debido al deterioro en la superficie de contacto o debido a la suciedad adherida a los mismos.

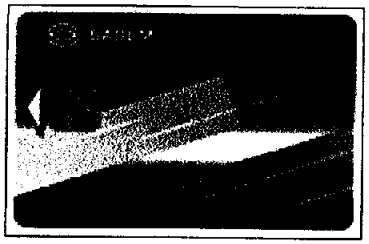


Figura 3.8 Tarjeta con contactos.

Características de los contactos eléctricos.

La mayoría de las tarjetas poseen en su superficie 8 contactos, Los cuales representan el único interfaz eléctrico existente entre la tarjeta y el terminal lector. Todas las señales eléctricas circulan a través de estos contactos, sin embargo el estándar ISO/IEC7916/2 reserva para uso futuro a C4 y C8. Está previsto que uno de esos dos contactos sea usado para un segundo canal de entrada y salida de tal manera que las tarjetas soporten comunicaciones full duplex. Estas características están descritas en el capítulo 1 sección 1.6 referente a las normas que rigen estas tarjetas

Hasta hace poco era necesario proporcionar a las memorias EEPROM un voltaje externo para poder grabar y borrar en ellas. El contacto C6 (VPP) era el encargado de proporcionar dicha tensión. Sin embargo, con los nuevos avances tecnológicos es posible generar dicho voltaje a partir de la alimentación del chip (contacto VCC), con lo que no es necesario el uso de VPP. Quiere decir esto, que todas las tarjetas actuales llevan un contacto que no sirve para nada, peor no puede ser eliminado por motivos de compatibilidad con el estándar ISO 7816

Tarjetas sin contactos.

Las tarjetas sin contactos ofrecen otras mejoras, una de ellas 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 radio frecuencias. Según la proximidad necesaria entre tarjeta y lector existen dos tipos:

- Tarjeta cercana: debe estar a unos pocos milímetros de lector para que sea posible la comunicación.
- Tarjeta lejana: La distancia varia entre centímetros y unos pocos metros.

Fueron desarrolladas por primera vez en el Instituto Arimura en 1978. el grosor de las tarjetas puede variar entre 0.76mm(estándar de una tarjeta de crédito) y 3mm. Los principios técnicos en los que se basan no son nuevos, y han sido ampliamente usados en otras aplicaciones. Debido a que no existe contacto entre la tarjeta y el lector, se presentan cuatro problemas principales:

- Alimentación del circuito integrado de la tarjeta.
- Transmisión de la señal de reloj.
- Transmisión de datos desde la tarjeta hacia el lector.
- Transmisión de datos desde el lector hacia la tarjeta.

Para solucionar estos problemas, se han desarrollado varias técnicas, como por ejemplo, transmisión por medio de microondas, transmisión óptica y acoplamiento capacitivo e inductivo. La técnica de acoplamiento es la mas apropiada para aplicaciones con tarjetas sin contactos.

En el acoplamiento capacitivo existen unas pistas conductoras en la tarjeta que actúan como un condensador de unas cuantas décimas de picofaradio. Por norma general, este sistema es insuficiente para alimentar los circuitos de una tarjeta, pero sí es bastante útil para transmisión de datos.

La técnica de acoplamiento inductivo, sí permite transmisiones de datos y también alimentar a la tarjeta, esto hace que sea la técnica más usada en la actualidad. En la figura 3.9 se muestra la disposición de la antena y el chip dentro de la tarjeta..

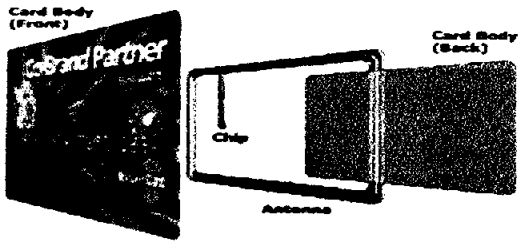


Figura 3.9 Tarjetas sin contactos.

3.3 CORRIENTES Y VOLTAJES

Tensión de alimentación

El voltaje estándar para todas las tarjetas existentes en el mercado es de 5 voltios con una tolerancia del +- 10% que es utilizado en circuitos de lógica TTL (Lógica Transistor- Transistor.) En telefonía existe una tendencia a disminuir el voltaje de trabajo. Hoy en día los componentes integrados en un teléfono móvil requieren solo 3 voltios, siendo la tarjeta la única que necesita 5 voltios. Por eso los teléfonos requieren de un conversor de tensión que es bastante caro. Está previsto que las próxima generación de tarjetas inteligentes puedan operar en un rango de 3 a 5 voltios.

Consumo de corriente.

De acuerdo con el estándar GSM 11.11, el consumo de corriente no debe ser mayor a 10 mA. Aunque en las recomendaciones de ISO todavía se especifica un valor de corriente de 200 mA, este valor está en desuso y será modificado en las próximas normas.

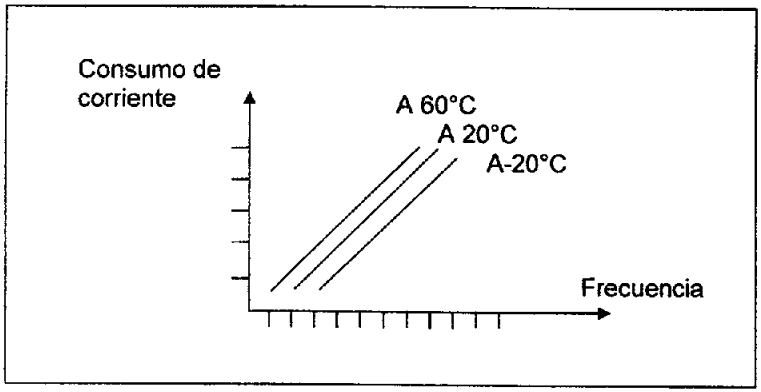


Figura 3.10 Consumo de corriente en función de la frecuencia de reloj aplicado y la temperatura.

Considerando una tensión de 5 voltios y un consumo de corriente de 100mA, se obtiene un apotencia de 50mW que resulta ser lo suficiente mente baja para no calentar el chip de la tarjeta.

Se prevé que en el futuro, el estándar GSM reduzca el valor permitido de corriente a 1mA para lograr una mayor duración en las baterías de los teléfonos, esto se conseguirá en pocos años gracias a los rápidos avances hechos de la tecnología de los semiconductores. El único obstáculo lo representa la corriente necesaria para la EEPROM de la tarjeta.

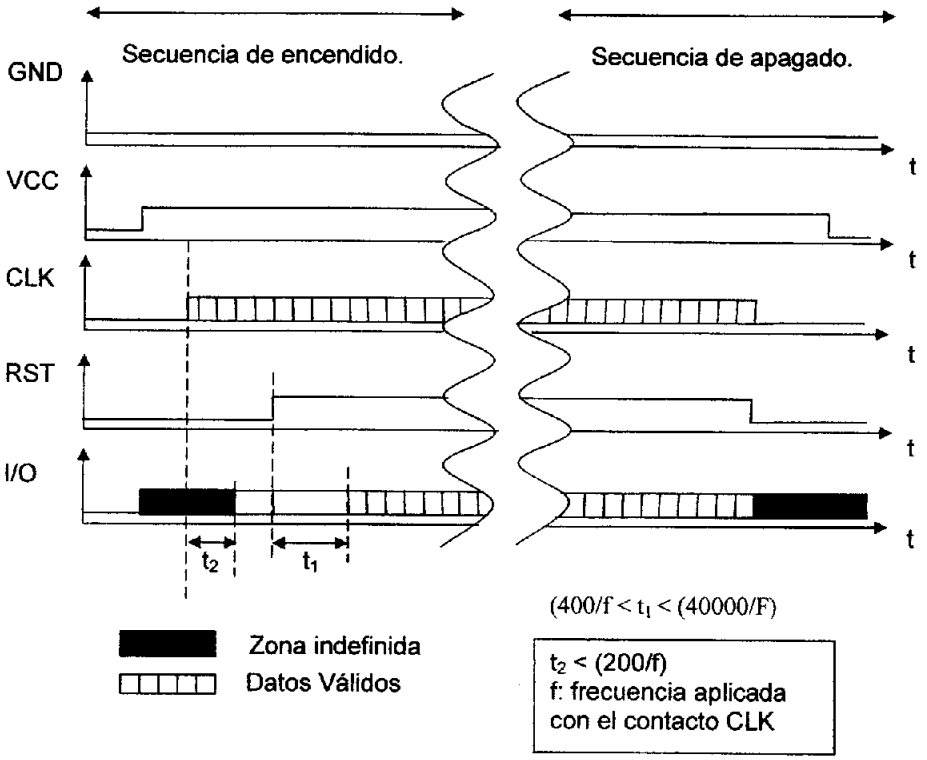


Figura 3.11 Secuencia de encendido y apagado de una tarjeta según el estándar ISO/IEC 7816/3

Los microprocesadores de las tarjetas inteligentes están protegidos frente a posibles descargas de tensión sobre sus contactos. El estándar ISO/IEC 7813/3 se define con precisión como ha de ser la secuencia de encendido y apagado. Como se muestra en la figura 3.11, la tierra debe estar conectada antes que la fuente de alimentación. Una vez conectada la tensión se aplica la señal de reloj, si se conecta el reloj antes que la alimentación, el microprocesador intentará alimentar a sus circuitos a través de la señal que le llega por la línea CLK, pudiéndose producir el deterioro en el chip de manera irreversible.
Cuando el microprocesador está perfectamente alimentado, puede ser iniciado a través del contacto RST, lo que se consigue colocando esta línea en nivel alto, figura 3.11. Una vez que se aplica el reset sobre el contacto RST, los datos de la línea I/O no son fiables hasta pasado un tiempo t1

En la secuencia de apagado de la tarjeta primero se desconecta los contactos clk y RST, y por último el de alimentación. Después de este proceso es posible extraer la tarjeta del terminal lector, si no se sigue este procedimiento se pueden producir daños en el circuito interno de la tarjeta.

3.4 FORMATOS DE LAS TARJETAS

El mas conocido es el de 85.6mm por 54mm., este tamaño ha sido el mas usado durante bastante tiempo y está recomendado por el estándar internacional ISO 7810. a este formato se le denomina ID-1 Este estándar creado en 1985, no tiene nada que ver con las tarjetas que se fabrican en la actualidad, en el no aparece ninguna recomendación frente al chip incrustado en la tarjeta. Fue unos cuantos años mas tarde cuando se definieron nuevas recomendaciones que tomaron en cuenta la presencia del chip y su posición.

Con la gran variedad de tarjetas que existen en la actualidad, que son usadas para múltiples aplicaciones, es a menudo bastante complicado determinar si una tarjeta posee el formato ID-1. Otra característica importante es el grosor, éste ha de ser igual a 0.76mm. El tipo ID-1 proporciona al usuario bastante comodidad en su manejo, de tal manera que la tarjeta no sea demasiado larga para llevarla en la cartera ni demasiado pequeña para que se pueda perder con facilidad. Sin embargo, este tamaño es a veces incompatible con la tecnología en miniatura que poseen ciertas aplicaciones, como por ejemplo los teléfonos móviles, que en algunos casos no pesan mas de 200 gramos y que no son mas grandes que un paquete de cigarrillos. Por tanto, es necesario definir un nuevo formato mas pequeño para cubrir estos nuevos requisitos. Para ello fue creado el ID-000, el cual actualmente sólo es empleado en teléfonos con tecnología GSM (Sistema para Comunicación Global)

Este nuevo formato ha dado paso, debido a su dificultad para el manejo y fabricación, a uno nuevo denominado ID-00 o mini-tarjeta, cuyas dimensiones están a medio camino entre el formato ID-1 y el ID-000. El ID-00 proporciona la portador de la tarjeta una mayor facilidad en su manejo y el coste de producción es menor. A pesar de todo el ID-00 es bastante reciente y su uso aun no se ha extendido lo suficiente.

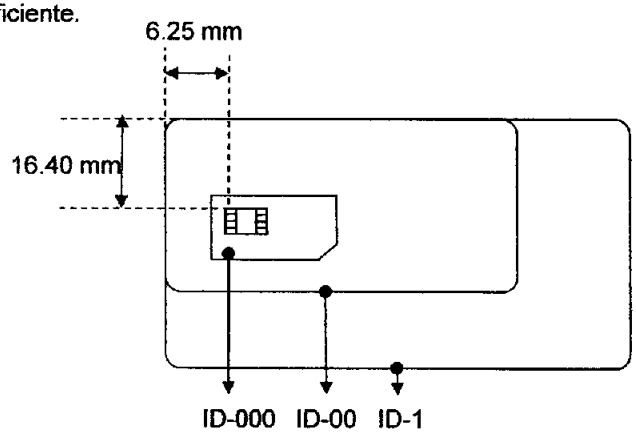


Figura 3.12 Relación entre los distintos tipos de tarjetas.

El alto y el ancho del formato ID-1 debe ser tal que sin tener en cuenta las esquinas redondeadas de la tarjeta, esta encaje perfectamente dentro de dos rectángulos concéntricos con las siguientes dimensiones:

- Rectángulo externo: ancho 85.72mm y alto 54.03mm
- Rectángulo interno: ancho 85.46mm y alto 53.92mm

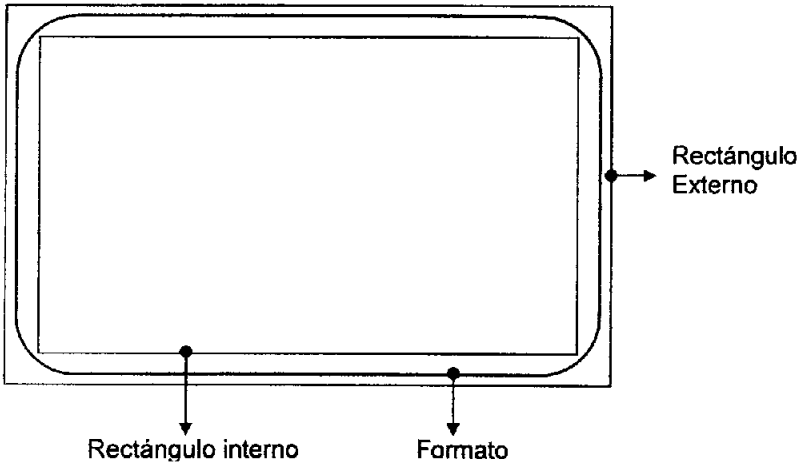


Figura 3.13 Representación gráfica del formato ID-1

El grosor ha de ser 0.76mm con una tolerancia de I +- 0.08mm En la figura 3.14 se representan las dimensiones de una tarjeta tipo ID-1.

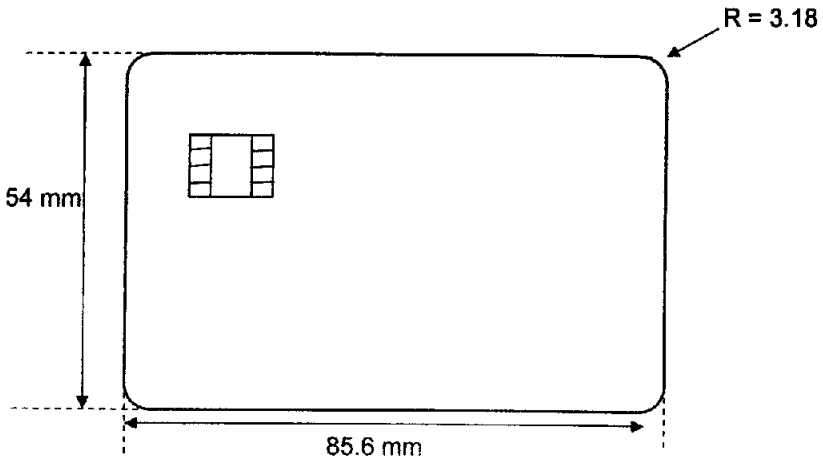


Figura 3.14 Dimensiones del formato ID-1

El formato ID-000 también se defina usando dos rectángulos concéntricos. Las medidas de dichos rectángulos son las siguientes:

- Rectángulo externo: ancho 25.10mm y alto 15.10mm
- Rectángulo interno: ancho 24.90mm y alto 14.90mm

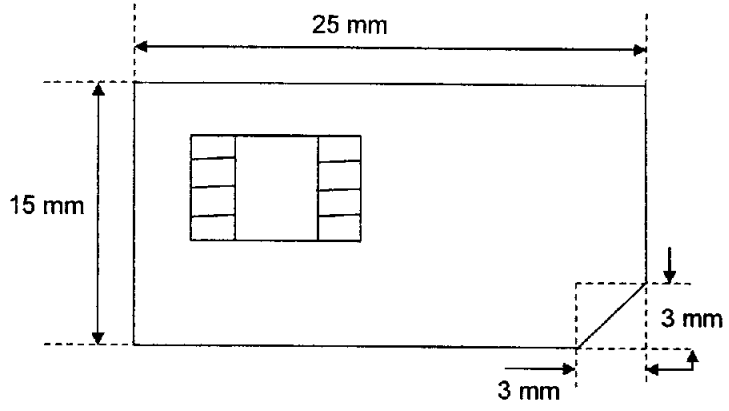


Figura 3.15 Dimensiones del formato ID-000

Las medidas del formato ID-00 también están basadas en un sistemas de rectángulos concéntricos siguientes:

- Rectángulo externo: ancho 66.10mm y alto 33.10mm
- Rectángulo interno: 65.90mm y alto 32.90mm

Tanto el formato ID-00 como el ID-000 son originarios de Europa y se usan mayoritariamente en teléfonos de tecnología GSM el corte rectangular de la base, lado derecho, que representa el formato ID-000 proporciona una mayor facilidad a la hora de insertar la tarjeta en la ranura del dispositivo lector.

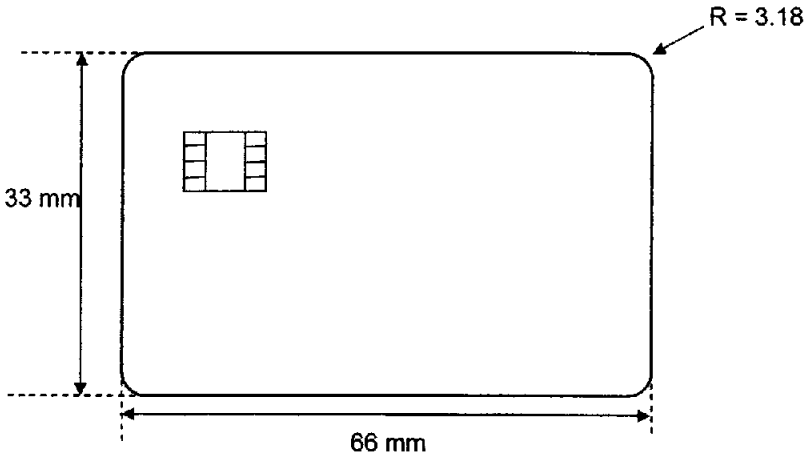


Figura 3.16 Dimensiones del formato ID-00

Dimensiones de la superficie de contacto

La diferencia fundamental entre las tarjetas de circuito integrado y el resto de las tarjetas de chip que lleva incrustado. Dado que el microprocesador requiere de unas vías por donde tomar la alimentación de sus circuitos o para llevar a cabo la transmisión de datos, es necesario una superficie física de contacto que haga en lace entre el lector y la tarjeta. Esta superficie consiste en 6 u 8 contactos que se encuentran en una cara de la tarjeta. Para el formato ID-1, la posición de los contactos y sus dimensiones se mencionan en el capitulo 1. en la norma ISO 7816-2.

Características eléctricas

Las propiedades eléctricas dependen únicamente del microprocesador que incorpora la tarjeta, dado que es el único componente electrónico. En los primeros años de existencia, el único factor crucial era la funcionalidad de las tarjetas, y se prestaba menos atención a las propiedades eléctricas. Esta situación esta cambiando en la actualidad, dado que existen una gran cantidad de aplicaciones con tarjetas y terminales lectores, y es importante que todas las tarjetas posean idénticas propiedades eléctricas. Las características se definen en la norma ISO 7816-3 mostradas en el capítulo 1.

La aplicación mas representativa que determino estas propiedades fue el sistema de telefonía móvil GSM. En este tipo de telefonía existe una amplia variedad de teléfonos que deben adaptarse a cualquier tarjeta. Las tarjetas usadas en telefonía móvil cumplen el estándar GSM 11.11. Otro estándar que esta bastante reconocido es el ISO/IEC7816/3.

3.5 ESTRUCTURA DE LOS DATOS CONTENIDOS EN UNA TARJETA INTELIGENTE.

Una de las principales características que las tarjetas de circuito integrado es que pueden almacenar datos e incluso proteger el acceso a dichos datos frente a lecturas no autorizadas. Las primeras tarjetas existentes incluían memorias direccionables de manera directa, pero hoy en día se puede restringir el acceso de varias maneras.

Las tarjetas actuales incluyen auténticos sistemas de administración de ficheros que siguen una estructura jerárquica. Los programas que gobiernan estos sistemas están bastante minimizados para reducir el uso de memoria. Naturalmente estos programas dependen mucho del tipo de memoria que contenga la tarjeta.

Los sistemas operativos mas recientes están orientados a trabajar con objetos, esto quiere decir que todos los datos referentes a un fichero están contenidos en él mismo (véase la figura 3.17). Otra consecuencia es que para efectuar cambios en el contenido de un fichero, éste debe ser antes seleccionado con la correspondiente instrucción. Los ficheros están divididos en dos secciones distintas: La primera se conoce como cabecera y contiene datos referentes a la estructura del fichero y a las condiciones de acceso. La otra sección es el cuerpo del fichero que contiene los datos del usuario.

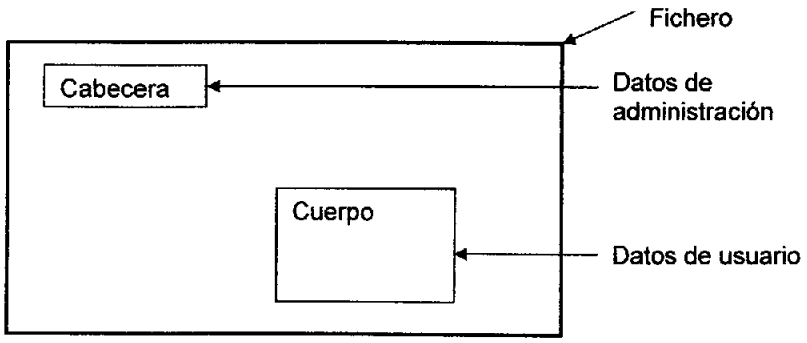


Figura 3.17 Estructura interna del sistema de fichero de una tarjeta inteligente.

Tipos de ficheros

La estructura de los ficheros contenidos en una tarjeta está especificada en el ISO/IEC 7816/4 y es similar a los sistemas DOS y UNIX. Existen varios directorios que hacen las funciones de carpetas que contienen ficheros. Los tipos de ficheros son:

Fichero maestro o MF

Es el directorio raíz y es seleccionado de manera automática después de iniciar la tarjeta. En él están contenidos todos los directorios y ficheros. El fichero maestro representa a toda la memoria disponible de la tarjeta para almacenar datos.

Fichero dedicado o DF

En caso necesario pueden existir ficheros dedicados en el siguiente nivel. El DF es un directorio que puede contener ficheros o incluir a otros DF. El nivel de anidamiento es infinito pero ha restringirse debido a lo escasez de memoria.

Fichero elemental o EF

Los datos de usuario necesarios para la aplicación están almacenados en estos ficheros. Los EF pueden existir a continuación del fichero maestro

Fichero interno del sistema

Aparte de los ficheros elementales pueden existir en las tarjetas unos ficheros propios del sistema operativo que se usan para ejecutar determinadas aplicaciones o almacenar códigos secretos. El acceso a estos ficheros esta protegido por el sistema operativo. Existén dos maneras distintas de integrar estos ficheros dentro de la memoria, el método de ISO consiste en ocultarlos dentro del fichero dedicado correspondiente a la aplicación y por tanto no pueden ser seleccionados. Otro método, propuesto por el Instituto Europeo para la estandarización de las Telecomunicaciones (ETSI), consiste en asignar a estos ficheros un nombre (FID) con el cual pueden ser seleccionados.

Es bastante habitual relacionar todos los datos referentes a una determinada aplicación con un mismo fichero dedicado. Con esto se consigue una estructura clara y organizada, si el usuario desea aumentar el número de aplicaciones de su tarjeta se basará con crear un nuevo DF que contenga los nuevos datos. SI la tarjeta se usa para una sola aplicación, los datos del usuario pueden estar contenidos simplemente en el fichero maestro.

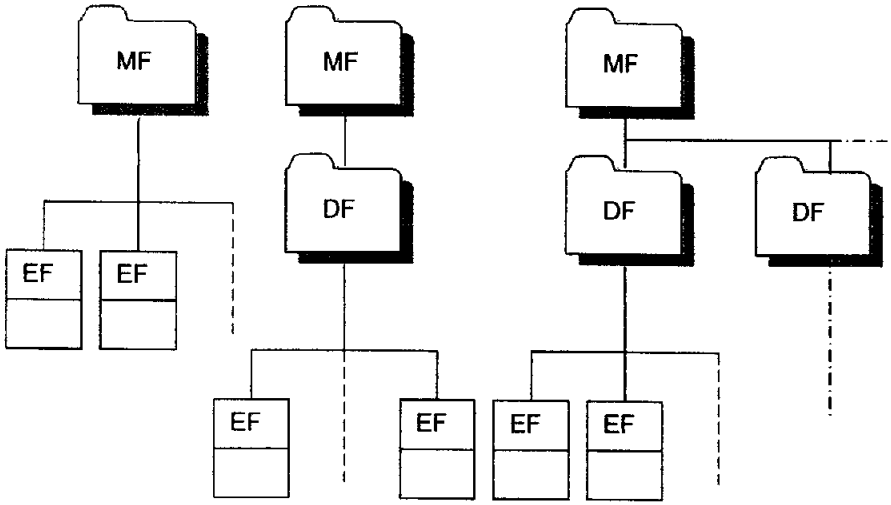


Figura 3.18 Diferencias en la organización de los datos, el ejemplo de la izquierda y el centro corresponden a tarjetas de una sola aplicación y el de la derecha a tarjetas de varias aplicaciones.

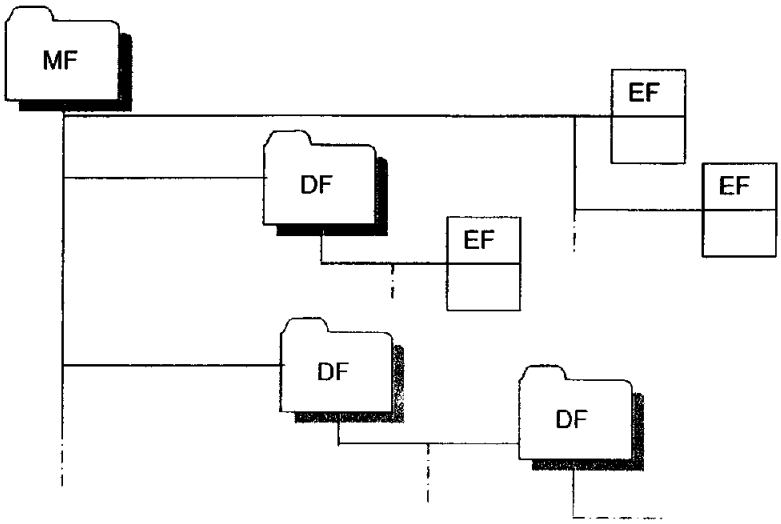


Figura 3.19 Tipos de ficheros contenidos en las tarjetas inteligentes

Identificación de los ficheros

Todos los ficheros e incluso los directorios poseen un identificador o FID de 2 bytes de longitud que se usan para poder seleccionarlos. Por razones históricas el fichero maestro tiene el valor FID 3F00h. El valor FFFFh está reservado para aplicaciones futuras.
Los valores del FID de cada fichero deben escogerse de tal manera que no se repitan, de forma que dos EF que estén dentro del mismo DF no deben tener el mismo FID y tampoco está permitido que un DF posea un FID igual al de un EF que esta directamente relacionado con él.

La telefonía GSM representa un buen ejemplo del uso del identificador FID. En el estándar GSM 11.11 el byte mas significativo del FID representa la posición dentro de la estructura de los ficheros. Si el fichero es un DF este byte tiene siempre el valor 7Fh.Los EF que pertenezcan directamente al fichero maestro tiene el valor de 2Fh como primer byte del FID, y todos los EF que pertenezcan a un mismo DF tienen el valor 6Fh en esa posición. El byte menos representativo se numera de manera consecutiva según se vayan creando los ficheros.

Los fichero dedicados o DF se usan para organizar los ficheros que pertenecen a una misma aplicación y por lo tanto actúan como si fueran carpetas. Poseen aparte del FID, un identificador de aplicación o AID que tiene una longitud de 5 a16 bytes. Este identificador está dividido en dos secciones bien diferenciadas: el primer elemento es el identificador de registro o RID que tiene una longitud fija de 5 bytes. En el se almacena información como el código del país, la categoría de la aplicación y un número que sirve para identificar al proveedor de una aplicación. El segundo elemento consiste en un identificador del propietario de la aplicación o PIX. Este último elemento es opcional y es grabado por el proveedor de la aplicación. Su longitud es de 11bytes.

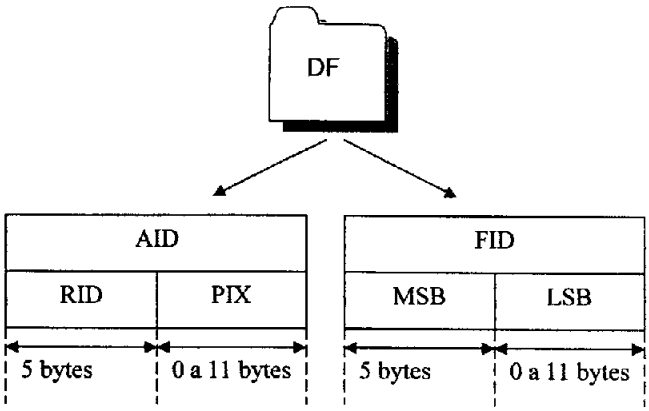


Figura 3.20 Componentes de la identificación de un fichero dedicado o DF.

Direccionamiento de los ficheros

Debido a la estructuración en objetos del sistema operativo de las tarjetas inteligentes, es necesario seleccionar los ficheros antes de acceder a ellos. Esto sirve para indicarle al sistema con qué fichero trabajar. Esto presenta el inconveniente de que no es posible seleccionar dos objetos a la vez.

Acceso al fichero maestro y a los ficheros dedicados

El fichero maestro se puede seleccionar desde cualquier parte de la estructura de la memoria usando el identificador 3F00h. Los ficheros dedicados se pueden direccional a través del correspondiente FID o también usando el identificador de aplicación o AID

Selección de ficheros elementales o EF

Existen dos métodos para seleccionar este tipo de estructuras. La selección explicita consiste en enviar a la tarjeta una instrucción especial que contenga 2 bytes del FID como parámetro para identificar al fichero.

En algunos casos, sólo es necesario especificar en la instrucción de selección del fichero, los 5 primeros bits de menos peso del FID, en tal caso la selección se le denomina implícita. Este método permite seleccionar un fichero y al mismo timepo posibilita que el acceso a dicho fichero se realice con la misma instrucción de selección.

Opciones de selección de ficheros.

Dado que es imposible controlar que no se repitan los identificadores del FID dentro de la memoria de la tarjeta, el acceso a dichos ficheros posee algunas restricciones de cara a evitar ambigüedades en la selección.
El fichero maestro se puede seleccionar desde cualquier parte de la estructura de ficheros dado que su FID es único. La selección de los DF que cuelgan del fichero maestro solo es posible desde el MF o desde otros DF que estén situados en el mismo nivel de la estructura jerárquica.

Tipos de estructura de los ficheros

Los ficheros da las tarjetas inteligentes poseen una estructura interna, existiendo varios tipos que se pueden aplicar libremente a cualquier EF dependiendo del propósito del mismo

Fichero transparente

A este tipo de estructura se le conoce normalmente como fichero binario. Estos ficheros no poseen ningún tipo de escritura y los datos se pueden leer o escribir byte a byte por medio de un puntero que se desplaza través del mismo. Las instrucciones usadas para trabajar con estas estructuras son: READ BINARY, WRITE BINARY y UPDATE BINARY.

El tamaño mínimo que pueden tener es de 1 byte mientras que el máximo no está especificado

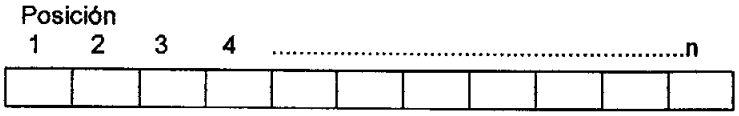


Figura 3.21 Estructura de un fichero transparente o binario.

Fichero lineal fijo.

Esta estructura esta basada en una serie de celdas de igual longitud que están unidas en forma de matriz. La unidad mas pequeña a la que se tiene acceso e s una celda, y no se puede acceder a fracciones de la misma. Las instrucciones que se usan para acceder a las celdas son: READ RECORD, WRITE RECORD, UPDATE RECORD.

A la primera celda se le identifica con el número 01h mientras que el número mas alto permitido es FEh, estando FFh reservado para usos futuros. El tamaño de cada celda puede variar entre 1 y 254 bytes, siendo las celdas de una misma matriz del mismo tamaño.

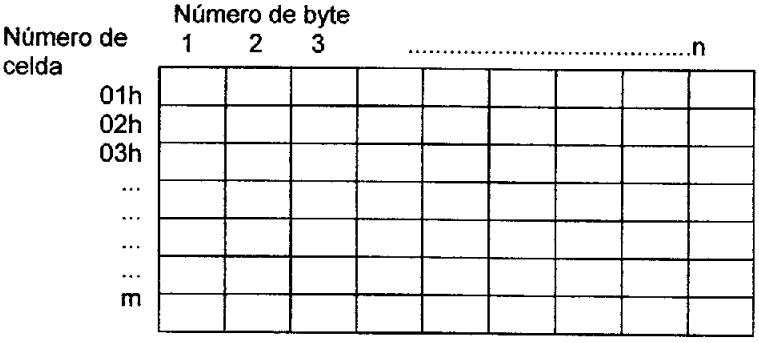


Figura 3.22 Estructura de un fichero lineal fijo.

Fichero lineal variable

Debido a las restricciones de espacio de memoria y como los datos almacenados en las celdas pueden tener una longitud variable, fue creado este nuevo tipo de fichero que es útil para optimizar el uso de la memoria. Cada celda puede tener un tamaño variable en función de los datos que s e almacenan en ella. El tipo de numeración y el tamaño de cada celda son exactamente iguales que en el caso anterior. Las instrucciones usadas también son las mismas.

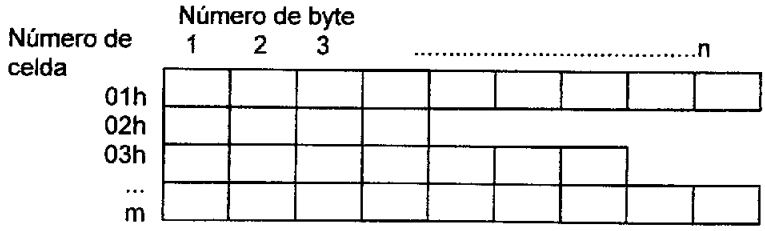


Figura 3.23 Estructura de un fichero lineal variable

Fichero cíclico

Esta estructura de datos está basada en un fichero lineal fijo. En este caso existe un puntero que indica cuál fue el último conjunto de datos al que se accedió. Una vez que el puntero llega a la última celda, éste es puesto por el sistema operativo de la tarjeta, en la primera posición de la matriz.

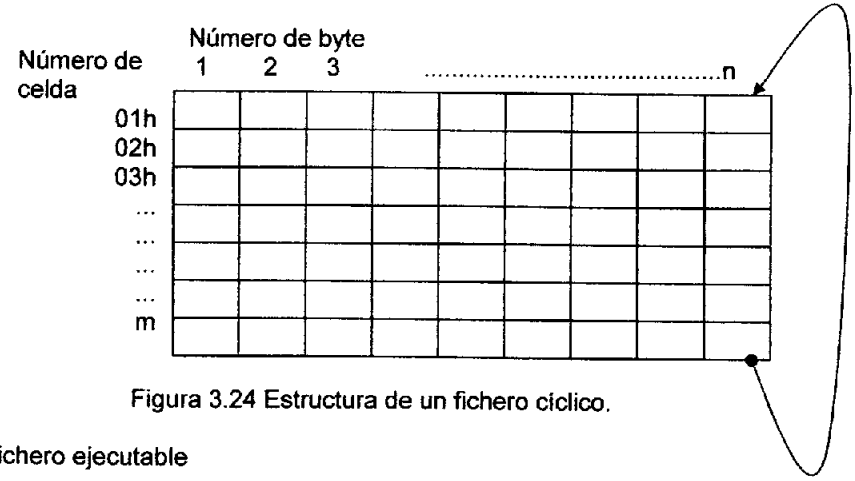


Figura 3.24 Estructura de un fichero cíclico.

Fichero ejecutable

Este tipo de estructura está descrito en el estándar europeo EN 726-3 y ofrece posibilidades de ampliación del sistema operativo de las tarjetas inteligentes. Este fichero no se creó para almacenar datos si no para contener ficheros que puedan ser ejecutados directamente por la propia tarjeta.

Tipos de acceso a los ficheros

Todas las estructuras contienen datos que sirven para regular el acceso a las mismas. Estos datos están contenidos en la cabecera. El peso de la seguridad de los datos almacenados en una tarjeta recae sobre la administración de ficheros, dado que sirve para controlar el acceso a sus datos.

La autorización de acceso es determinada cuando se crea el fichero y como norma general no se puede modificar mas tarde. Los distintos tipos de acceso varían en función del sistema operativo de la tarjeta y de las instrucciones que soporte. Cada vez que se crea un EF, es necesario, por la seguridad de los datos, definir con precisión los derechos de acceso sobre dicho fichero.

Las instrucciones para manipular ficheros varían de un sistema operativo a otro, las mas comunes puede apreciarse en la tabla 3.1

Instrucción	Descripción
APPEND	Ampliar el tamaño de un fichero.
DELETE FILE	Borrar fichero.
INVALIDATE	Bloquear el acceso al fichero.
LOCK	Bloquea indefinidamente el fichero.
READ/SEEK	Lee o busca en el contenido de un fichero.
REHABILITATE	Desbloquear fichero.
WRITE/UPDATE	Escribe en un fichero.
CREATE	Generar un fichero nuevo.
REGISTER	Registrar un fichero nuevo.

Tabla 3.1 Instrucciones para la administración de un fichero.

Atributos de los ficheros

Aparte de los derechos de accesos que se pueden aplicar a los ficheros, existen unos atributos especiales que establecen nuevas propiedades. Estos atributos se definen a la misma vez que se crea el fichero y generalmente no pueden ser modificados con posterioridad. Los atributos posible son:

El atributo W.O.R.M.

Este símbolo provienen de la frase "write once, read many" o escribe una vez, lee muchas veces, cuando un fichero posee este atributo, los datos contenidos en él sólo se pueden escribir una sola vez, pero pueden ser leídos cuantas veces se desee. Esta característica debe ser soportada por el hardware de la EEPROM o también se puede incorporar usando una función software. El propósito de este atributo es proteger los datos importantes contenidos en la tarjeta frente a posibles escrituras.

Atributo de escritura múltiple

Este tipo de atributo es bastante usado en la telefonía GSM para ficheros con gran actividad en uso. Permite que el contenido del fichero pueda ser alterado muchas veces, el número máximo depende de los ciclos de lectura y escritura de la EEPROM.

Atributo de corrección de errores

Este atributo se usa para datos que son particularmente importantes y que requieren algún tipo de código de detección de errores o EDC (Detección de código de errores). La protección EDC combinada con la posibilidad de múltiples escrituras, permite incluso la corrección de errores producidos en la memoria EEPROM.

3.6 INSTRUCCIONES DE PROGRAMACIÓN

Cada microcontrolador tiene un set de instrucciones. El usuario puede organizar las instrucciones en un orden lógico para crear un programa. El microcontrolador ejecuta el programa para realizar una tarea especifica. Para comprender completamente el set de instrucciones debemos entender los siguientes conceptos:

Opcode.- (Código de operación) es un código numérico de la instrucción que representa la operación a ser realizada por el CPU, es decir, el Opcode es un grupo de bits los cuales le indican al microcontrolador qué operación en particular hay que realizar. Por ejemplo un 64 podría significar limpiar el acumulador.

Mnemónicos.- Los mnemónicos son nombres asignados a una operación en particular. Cada mnemónico es asociado a un opcode. El usuario puede hacer referencia a una operación por medio de un mnemónico ADD en lugar del opcode 84. Con el uso de los mnemónicos se hace mas fácil escribir un programa. Por ejemplo, el mnemónico LD representa la operación Cargar.

Podríamos agrupar todo el set de instrucciones en los siguientes grupos que son:

- Aritméticas/lógicas/recorrimientos.
- Transferencias de control
- Movimientos en memoria
- Manipulación de bits.
- Control de la pila.
- Condicionales/prueba.

Las instrucciones de escritura y lectura permiten escribir y leer datos en ficheros elementales o EF. Debido a que los ficheros poseen unas condiciones de acceso, el acceso a los mismos solo esta permitido a usuarios autorizados, por esto deberán satisfacerse previamente unas condiciones de seguridad, que serán más o menos rígidas dependiendo del tipo de dato al que se quiera acceder.

Existen varias instrucciones diferentes para la lectura y escritura de ficheros, esto se debe a la existencia de distintos tipos de ficheros. En las tarjetas de memoria puede simplificarse uso de la memoria tomando a esta última como un solo fichero, para acceder a la información deseada solamente es necesario especificar la dirección de inicio de los datos y el número de bytes que se desea leer o grabar.

Las instrucciones de lectura y escritura están clasificadas en función del tipo de fichero, para un fichero transparente, el cual no posee ningún tipo de estructura interna, se usan las siguientes instrucciones:

- READ BINARY: operación de lectura.
- WRITE BINARY y UPDATE BINARY: operación de escritura

La diferencia fundamental entre las instrucciones WRITE y UPDATE tiene mucho que ver con el estado de tierra de las celdas de la memoria EEPROM de la tarjeta. El estado de tierra ese l valor lógico que posee una celda de la EEPROM cuando alcanza su valor mínimo de energía. Normalmente, este estado representa el valor lógico "0". La instrucción WRITE BINARY solo puede usarse para pasar de un valor lógico "1" al estado de tierra o valor lógico "0". Por otro lado, UPDATE BINARY es propiamente una instrucción de escritura puesto que no depende del valor previo existente en las celdas de memoria.

La orden de lectura READ BINARY sólo requiere de dos campos: uno donde se le indique la dirección de datos y otro que representa el número de bytes que se desean leer. La operación de escritura es idéntica pero incluye los datos que se desean almacenar.

Existen otros tipos de ficheros que poseen estructuras en forma de matrices o registros. La unidad mínima de información en este caso es una celda de la matriz. Las instrucciones para el manejo de estas estructuras son:

- READ RECORD: operación de lectura
- WRITE RECORD y UPDATE RECORD: operación de escritura.
- SEEK: operación de búsqueda dentro de la matriz.
- APPEND RECORD: añade celdas al fichero.

Todas estas instrucciones deben especificar el tipo de acceso sobre la matriz, esto se realiza a través de un byte de parámetro. El método mas común es el directo, donde basta con especificar la dirección absoluta de la celda de la matriz. Otro acceso posible se realizase realiza usando el byte de procedimiento "first" (primero), con esto se consigue colocar el puntero sobre la primera celda existente en el fichero. Otros parámetros similares son: "last"(ultimo), "next"(próximo) y "previus" (previo).

El estándar ISO/IEC 7816/4 posibilita la opción de leer todas las celdas del fichero, desde la primera hasta otra que se especifica en la instrucción, o desde una celda determinada hasta el final del fichero.

La instrucción APPEND RECORD sirve para añadir celdas a un fichero existente, y además puede incluir los datos que se desean almacenar en las mismas.

Instrucciones de identificación

Una aplicación muy común de las tarjetas inteligentes es la identificación del portador de la misma. Para evitar posibles suplantaciones de personalidad y el uso no autorizado, las tarjetas incluyen un mecanismo para identificar al usuario verdadero. Este mecanismo está basado en la existencia de una clave o PIN, que solo es conocida por el dueño y por la propia tarjeta. Cuando el usuario quiere acceder a aplicaciones que están protegidas debe introducir la clave, si está es errónea la tarjeta puede pedirla de nuevo o auto bloquearse.

La instrucción para comprobar la clave es VERIFY PIN, que suele incluir normalmente 4 caracteres que representa al PIN. Una vez recibida esta instrucción, la tarjeta comprueba la clave con la que tiene almacenada en la EEPROM, si son idénticas la tarjeta confirma la operación y envía la respuesta al terminal. En caso contrario la tarjeta rechaza el PIN y se lo indica al terminal.

Muchos sistemas operativos usan varias claves, entonces es necesario especificar en la instrucción VERIFY PIN, qué clave se desea utilizar. En el estándar EN 726-3 las siglas PIN se cambian por CVH (Chip Holder Verification). La instrucción VERIFY CHV tiene las misma características que la anterior.

Instrucciones para la administración de ficheros.

Los sistemas operativos de las tarjetas modernas permiten realizar numerosas operaciones sobre los ficheros. En el caso de tarjetas de una sola aplicación, muchas de esas operaciones no están incluidas debido a problemas de espacio de memoria y coste de fabricación.

Las operaciones con ficheros no pueden llevarse a cabo sin antes complementar un os requisitos de seguridad, con los que se asegura que solo la persona actualizada tiene acceso a los ficheros que están protegidos.

En las tarjetas multi-aplicación debe segmentarse el espacio de memoria disponible, de tal manera que una sola aplicación no pueda ocupar toda la memoria. Para crear una nueva aplicación se utiliza la instrucción REGISTER. Uno de los campos de esta orden es el identificador de aplicación o AID, otro es el tamaño máximo de la memoria reservada, y por último debe especificarse una clave para acceder a dicha aplicación.

La instrucción reservada para crear un fichero EF o un DF es CREATE FILE. Cada vez que se crea un fichero deben especificarse las condiciones de acceso, los atributos, el tipo, la longitud, el identificador de fichero, etc. Una vez que el fichero ha sido creado, para poder operar con él es necesario seleccionarlo con la instrucción SELECT FILE. En caso de que se deseen cambiar las propiedades de un fichero se utiliza la instrucción CHANGE ATTRBUTES. En muchos casos esta operación requiere previamente la presentación de una clave de acceso al fichero.

La instrucción INVALITE permite bloquear de manera reversible el fichero que esta seleccionado, en este caso no se permitirán las operaciones de escritura y lectura, estando solo permitido la selección de fichero. La instrucción inversa a ésta es REHABILITE la cual desbloquea el fichero previamente seleccionado. Estas dos instrucciones solamente se permiten si antes se han cumplido unos requisitos de seguridad.

Otra orden importante para la administración de ficheros es LOCK, que bloquea de manera irreversible el fichero seleccionado previamente. Esta instrucción presenta el inconveniente de que la zona de memoria que hay a sido bloqueada no podrá usarse para otros propósitos, con la consiguiente disminución de la memoria disponible. La manera mas elegante de acabar con un fichero para siempre se consigue con las instrucción DELETE FILE.

Instrucciones de autentificación.

Como se puede ver hasta ahora, existe instrucciones que sirven para identificar al portador de la tarjeta frente a esta. Además de esto, existen otras ordenes destinadas a la identificación del terminal frente a la tarjeta y viceversa. Este procedimiento es más complejo que la verificación de una llave y por tanto resulta más seguro.

Dependiendo del sistema operativo de la tarjeta, existen varias instrucciones para realizar dicha verificación. La instrucción GET CHIP NUMBER sirve para obtener un número "único" de cada tarjeta que será usado para generar las claves necesarias para el proceso de autentificación. Otra instrucción importante es ASK RANDOM que sirve para pedirle a la tarjeta un número aleatorio, en el estándar ISO IEC 7816/4 esta instrucción se denomina GET REQUEST, y tiene la misma función. La instrucción que sirve para verificar la autenticidad de la tarjeta frente al terminal lector es INTERNAL AUTENTÍCATE, el mecanismo es el siguiente: la tarjeta recibe un número aleatorio, lo cifra usando una clave que solo conocen la tarjeta y el terminal. El resultado de esta operación es enviado al terminal que realiza la misma operación con el número aleatorio, compara el resultado con le obtenido por la tarjeta y si ambos son iguales la tarjeta queda validada.

La instrucción EXTERNAL AUTHENTÍCATE es usada para demostrar la autenticidad del terminal frente a la tarjeta. El mecanismo es el siguiente: el terminal solicita a la tarjeta un número aleatorio (usando ASK RANDOM), lo cifra con una clave secreta que sólo conocen ambos , y el resultado es enviado hacia la tarjeta mediante la orden EXTERNAL AUTENTÍCATE. La tarjeta realiza la misma operación y compara ambos resultados, si son iguales, el terminal queda validado frente a la tarjeta.

Existe una instrucción destinada a disminuir el tiempo necesario para llevar a cabo las dos autentificaciones, MUTUAL AUTENTÍCATE. Esta orden aún no está incluida en ningún estándar de tarjetas inteligentes, pero la norma ISO/IEC 9798/2 sugiere una futura inclusión de dicha orden.

Instrucciones usadas para algoritmos criptográficos.

Debido a los problemas de escasez de memoria que padecen las tarjetas inteligentes, no es frecuente que una tarjeta incluya varios algoritmos criptográficos. En caso de usar un algoritmo de cifrado de bloques, se puede optar por el uso del modo ECB (libro de código electrónico) o le modo CBC (cipher block Chiang). La instrucción para que la tarjeta cifre los datos enviados por el terminal es ENCRYPT dicha orden debe especificar la dirección de una clave almacenada en la tarjeta que será usada para cifrar los datos.

La orden inversa a ENCRYPT es DECRYPT. El funcionamiento de esta instrucción se similar a la anterior. Con la introducción de los algoritmos de clave pública en la industria de las tarjetas inteligentes, ha sido necesario incluir, en los sistemas operativos d el as mismas, nuevas instrucciones. La instrucción SIGN DATA es usada para la firma digital de datos, la cadena de dato que se desea firmar es enviada a la tarjeta, indicándole a ésta qué clave privada se desea usar. Esta clave está almacenada en la memoria de la tarjeta y solo se puede acceder a ella tras haber cumplido satisfactoriamente unas condiciones de acceso. Una vez seleccionada la clave, la tarjeta ejecuta el algoritmo correspondiente y los datos firmados son devueltos hacia el dispositivo controlador del terminal.

La tarjeta también puede realizar el proceso contrario, que consiste en verificar la firma digital de un mensaje. Esto lo realiza usando la orden VERIFY SIGNATURE. Los campos de entrada de esta instrucción son las siguientes: los datos sin firmar que se desean verificar, los datos firmados digitalmente, y la dirección donde se encuentra almacenada la clave publica. La respuesta a esta instrucción consiste en la pareja de bytes SW1 y SW2, cuyo contenido indica si la firma es válida.

CAPITULO 4. ALGUNAS APLICACIONES DE LAS TARJETAS.

4.1. Para el manejo de dinero.

Actualmente, es muy común el uso de tarjetas como forma de pago en detrimento del dinero en efectivo, estas tarjetas son en su mayoría de banda magnética. Auque es un método muy extendido tiene sus limitaciones, las cuales han sido solucionadas con la aparición del monedero electrónico.

Las tarjetas magnéticas que todo el mundo conoce , tales como VISA, MASTER CARD, AMERICAN EXPRESS, etc, utilizan la misma técnica para hacer los pagos. Estas tarjetas siempre tienen una cuenta bancaria asociada, en la cual se encuentran los fondos reales o de crédito que se pueden gastar. Cuando se realiza un pago o se saca efectivo de un cajero automático, lo que se hace es descontar dinero de esa cuenta. El flujo de información que se sigue cuando se paga un producto en un establecimiento comercial es el siguiente:

- En primer lugar, se pasa la tarjeta por un lector que tomará los datos necesarios de la banda magnética para conectarse con la entidad bancaria donde esté la cuenta asociada.
- Dichos datos junto con algunos propios del establecimiento son enviados al banco.
- El banco certifica los datos que le llegan y decide si se hace el pago o no, esto depende de los fondos que haya en la cuenta o del crédito que se le concede al propietario de la tarjeta.
- Si el banco decide hacer el pago transferirá los fondos correspondientes a la cuenta en donde se realiza la compra.
- Si el pago se ha llevado a cabo con éxito se le comunica al establecimiento el resultado de la operación y ésta queda consolidada.

Cuando se saca dinero de un cajero automático la operación es similar, en lugar de certificar una compra se le entrega efectivo al poseedor de la tarjeta.

4.1.1 DINERO ELECTRÓNICO.

El dinero electrónico o dinero digital no es más que una serie de unos y ceros lógicos que en un futuro no muy lejano sustituirán al dinero acuñado en papel y en moneda. Este tipo de dinero tiene que cumplir una serie de propiedades para que sea eficaz en el uso diario:

- Independencia: ha de poder usarse independientemente del lugar.
- Privacidad: el dinero electrónico ha de proteger la privacidad del usuario, su uso no debe aportar información que lo identifique.

- Pagos fuera de línea (off-line), el pago de cualquier producto o servicio no debe depender de una red de comunicaciones que valide la transacción.
- Transferibilidad: el dinero debe poder ser transferido entre usuarios sin límite.
- Divisibilidad: una pieza de dinero digital ha de poder dividirse en unidades menores y también se han de poder recombinar pequeñas unidades en otras mayores.

Estas propiedades son exigentes de tal forma que el papel moneda no las cumple, como por ejemplo la divisibilidad, propiedad que sí se le puede atribuir a algunos tipos de dinero electrónico existentes. A continuación se definen algunos conceptos necesarios para la posterior comprensión del dinero electrónico.

Dinero en línea (on-line) y dinero fuera de línea (off-line).

Una traducción mas o menos literal sería: dinero con la línea de comunicación conectada y dinero con la línea desconectada. El primer concepto, necesita que el punto de venta esté conectado, por medio de algún tipo de red, a un banco u oficina central que certifique la transacción. Por ejemplo, la compra con tarjeta de crédito necesita la conexión con una entidad que confirma tanto la autenticidad de la tarjeta y su tomador, como la disponibilidad de crédito para la operación. El segundo concepto no tiene esos inconvenientes, funciona de la misma manera que el dinero tradicional; se entrega directamente y no es necesaria una tercera entidad que controle la operación.

Otra diferencia entre ambos es el de la privacidad. En el primero el banco sabe donde, cómo, cuando y quien realiza la compra, mientras que en el segundo esta información no está disponible.

4.1.2 MONEDERO ELECTRÓNICO.

Las bases del monedero electrónico lo forman la tarjeta inteligente y el dinero electrónico. De las tarjetas inteligentes ya se ha hablado den detalle anteriormente, las principales características del monedero electrónico son:

- El control de accesos.
- La posibilidad de la firma de la tarjeta.
- Su capacidad para almacenar datos.

Con los puntos anteriores se ha visto de forma rápida cuál es la teoría del dinero electrónico. Como se pudo comprobar, éste se puede generar por medio de un ordenador y una conexión de red con el banco donde se tengan fondos. Es normal llevar algo de dinero en efectivo (papel moneda y monedas) para los gastos diarios. El dinero electrónico, que al fin y al cabo sólo son bits almacenados en una memoria, también ha de poderse sacar del ordenador para realizar estos

pequeños gastos y es ahí donde entra en juego la participación de la tarjeta inteligente, ésta permite almacenar las monedas electrónicas en su memoria y controlar el acceso a ese efectivo. A este conjunto de tarjeta inteligente, mas el dinero almacenado en su memoria , se le llama monedero electrónico.

Pero no es esta la única función del monedero, la capacidad de la tarjeta para realizar operaciones con los datos almacenados en ella, para cifrarlos, para realizar firma digital, hace posible que no sea necesario un ordenador para la adquisición de monedas electrónicas. el monedero está preparado para conectarse directamente con el banco y realizar la transacción de fondos desde la cuenta del usuario hasta la tarjeta en forma de dinero digital. También esta capacitado para recibir dinero de otros monederos. Es en sí un sistema que sustituye perfectamente al papel moneda.

Tipos de monedero.

Se pueden diferencia varios tipos de monedero dependiendo de la forma de interactuar honestos. En primer lugar se encuentran los que son solo una tarjeta inteligente como VISA CASH.

Por otro lado están los monederos que incorporan un teclado y un display para poder interactuar con la tarjeta o para adaptar ésta a otro tipo de comunicación distinta a la realizada a través de los contactos de la tarjeta, por ejemplo, la comunicación por infrarrojos, por ultrasonido etc.

Y por último existen otros monederos que no necesitan una tarjeta inteligente, sino que disponen de un microprocesador interno que se encarga de la gestión de las monedas electrónicas. Se suele usar para el intercambio de efectivo entre tarjetas o para cobro de servicios. La mayoría de los bancos ya han puesto en funcionamiento sus monederos electrónicos, pero aún no son muchos los establecimientos que permiten trabajar con este tipo de efectivo, aunque se prevee un crecimiento exponencial de esta forma de pago conforme los pequeños establecimientos como panaderías, quioscos, restaurantes, y demás servicios como taxi, estacionamientos, transporte eléctrico, y cine, adopten el sistema.

La seguridad en los monederos electrónicos y las tarjetas magnéticas

Las garantías de seguridad que ofrecen las tarjetas magnéticas dependen en gran medida del PIN del usuario. Este PIN se encuentra cifrado en una de las pistas magnéticas. El procedimiento de uso es el siguiente: cuando se introduce la tarjeta en algún terminal, éste lee el PIN cifrado de una de las pistas y luego le pide al usuario que teclee dicho PIN, el número teclado por el usuario se cifra con un o o varios números que tiene almacenado el terminal en forma secreta. Si el resultado del cifrado es idéntico al PIN cifrado que se guarda en la pista magnética, se

puede decir que el PIN tecleado es correcto, y por lo tanto el usuario queda reconocido como el verdadero dueño de la tarjeta.

El punto mas débil del sistema aparece cuando el usuario usa una terminal distinto al de su compañía. Si sucede esto, el terminal ha de realizar el proceso de comprobación preguntando al servidor de la entidad emisora de la tarjeta. En este intercambio de información a través de un área de datos puede quebrarse la seguridad del sistema.

Otro problema es el llamado caballo de troya en donde la utilización de una terminal no segura implicaría revelar el contenido tanto de la banda magnética como el del PIN. Con dicha información puede realizarse una copia exacta (a nivel de banda magnética que es lo único que leen los cajeros) de la tarjeta, y usarla en cualquier terminal válido suplantando la personalidad del verdadero dueño.

El monedero posee la seguridad que proporcionan las tarjetas inteligentes, siendo muy difícil el acceso al dinero electrónico almacenado en ellas si no se tienen las claves correctas. Además, si el usuario tiene una copia, por ejemplo en el disco duro de ordenador, del dinero que lleva en la tarjeta, podrá ir al banco y solicitar que le validen la copia con otros números de serie, invalidando los que están en el monedero. Por otro lado, y como se ha visto en los puntos anteriores, el dinero electrónico lleva intrínseco unos sistemas de seguridad que superan en gran medida a las tarjetas magnéticas e incluso el papel moneda.

4.2 Para telefonía.

Hoy en dia es raro encontrarse a una persona que se dirija hacia una cabina telefónica con las manos llenas de monedas pequeño valor (0.50, 1.0, 2.0 y 5.0 pesos) y para prevenir que la cabina se quede con el dinero no usado durante la llamada, es cada vez mas frecuente el uso de las tarjetas de pago para teléfonos públicos. Éstas proveen comodidad al usuario, evitan la incomodidad que presenta el llevar monedas, eliminan el problema de la devolución del dinero que se ha introducido en el teléfono y que no se ha gastado, evita a las compañías telefónicas el tener que recoger las monedas de todas las cabinas que tengan instaladas, etc.

Mostraremos como es una tarjeta de pago por dentro, que significan los datos que lleva almacenados y su funcionamiento.

Este tipo de tarjetas se encuentran dentro del grupo de tarjetas de memoria, pero no tienen ningún tipo de inteligencia. Su funcionamiento se basa en una memoria en la que se van guardando datos como el dinero que queda en ella, nombre del fabricante, etc.

Datos que almacena

Estas tarjetas se basan en una memoria no volátil (PROM)de 128 o 256 bits. Las tarjetas de 128 bits tiene un a estructura similar a las de 256 bits, pero se diferencian en la forma de almacenar las unidades monetarias. Al ser este tipo de tarjetas poco frecuentes, se cerrará el estudio en tarjetas de 256 bits.

Desde el bit 1 al 96 se encuentra almacenada cierta información referente a la tarjeta, esta información contiene la suma de identificación (checksum), identificación de la tarjeta, número de serie, fabricante, etc. Desde el 97 al 255 se almacena información referente al dinero restante en la tarjeta. Los bits 1 al 96, poseen un fusible interno fundido en la fábrica, por lo que no se pueden reescribir. Desde el bit 97 al bit 256 sólo se podrán escribir un os binarios. Estos unos representan la cantidad de dinero gastada durante las llamadas telefónicas realizadas con dicha tarjeta. Teóricamente este tipo de memorias se pueden borrar con rayos ultravioletas, dejando la tarjeta tal como fue comprada, pero el chip de la tarjeta está cubierta con una resina que evita el borrado.

Mapa de bits para la tarjeta de 256 bits

Desde el bit 13 al 32 se encuentra la información de unidades gastadas y no gastadas. Cuando la tarjeta es nueva, y aún no se ha usado, todos los bits de éstos últimos bytes tienen el valor cero, a medida que la tarjeta es usada, se van poniendo estos ceros a uno, con lo que quedan marcados como gastados. En esta última zona de datos, se pueden diferenciar dos partes, la zona lenta, que en las tarjetas pertenecientes a la compañía española Telefónica se dividen de la siguiente manera:

- Del bit 107 al bit 206 para las tarjetas de 1.000 pesetas.
- Del bit 127 al bit 166 par alas tarjetas de 2.000 pesetas.
- Del bit 107 al bit 166 para las tarjetas de 2.100 pesetas.

En esta zona cada bit tiene un valor de cinco pesetas, el resto de bits pertenecen a la zona rápida que en las tarjetas españolas se dividen de la siguiente manera:

- Del bit 207 al bit 256 para las tarjetas de 1.000 pesetas.
- Del bit 167 al bit 256 par alas tarjetas de 2.000 pesetas.
- Del bit 167 al bit 256 par alas tarjetas de 2.100 pesetas.

En esta zona los valores de cada bit son de 10 pesetas para las tarjetas de 1000 pesetas y de 20 pesetas para las tarjetas de 2.000 y 2.100 pesetas. A partir del bit 97 existen unos bits puestos a uno, esto se realiza durante el proceso de comprobación de calidad de tarjeta, y sirve para comprobar que la tarjeta funcione correctamente.

Byte	Bits	Binario	hexadecimal	significado
1	1...8			checksum
2	9...16	1000 0011	83	Código que indica tarjeta para teléfonos
3	17...24	1111 1111	FF	
4	25...32	1111 1111	FF	
5	33...40	1001 0000 1001 1110 0011 0000 0101 1010	90 9F 30 5A	Oberthur Oberthur(argentina) G+D Gemplus
6	41...48			
7	49...56			Numero de serie
8	57...64			
9.1	65...72	0001 0100	14	1000 pesetas España
9.2	65...72	0010 0101	25	2000 pesetas España
9.3	65...72	0010 0101	25	2100 pesetas España
9.4	65...72	0001 0100	14	N$ 25.00 México
9.5	65...72	0000 0000	00	N$ 25 Argentina
9.6	65...72	0000 0000	00	100u Croacia
9.7	65...72	0010 1010	2A	1000u Croacia
10	72...80	1000 1010	8A	Byte 10 correspondiente al byte 9.1
10	72...80	0000 0100	04	Byte 10 correspondiente al byte 9.2
10	72...80	0000 0110	06	Byte 10 correspondiente al byte 9.3
10	72...80	1100 1010	CA	Byte 10 correspondiente al byte 9.4
10	72...80	0000 0011	03	Byte 10 correspondiente al byte 9.5
10	72...80	0000 1010	0A	Byte 10 correspondiente al byte 9.6
10	72...80	0010 0101	85	Byte 10 correspondiente al byte 9.7
11	81...88	0001 1110	1E	
12	89...96	0010 0010	22	España
		0010 0100	24	México
		0010 0110	26	Croacia
		0010 1000	28	Argentina
		0001 1110	1E	Suecia

Continúa

		0011 0000	30	Noruega
		0011 0011	33	Andorra
		0011 1100	3C	Irlanda
		0100 0111	47	Portugal
		0101 0101	55	República Checa
		0101 1111	5F	Gabón
		0110 0101	65	Finlandia
13	97..104	1111 1111	FF	Las primeras diez posiciones están a uno
		11xx xxxx	xx	Zona lenta
		xxxx xxxx	xx	
		xxxx xxxx	xx	
		xxxx xxxx	xx	Zona rápida
		xxxx xxxx	xx	
		xxxx xxxx	xx	
32	148..256	Xxxx xxxx	Xx	

Tabla 4.1 Estructura de la memoria de una tarjeta para teléfonos públicos.

Funcionamiento interno de la tarjeta.

Es bastante sencillo, en la figura 4.1 puede observarse un esquema simple de la arquitectura interna de una tarjeta.

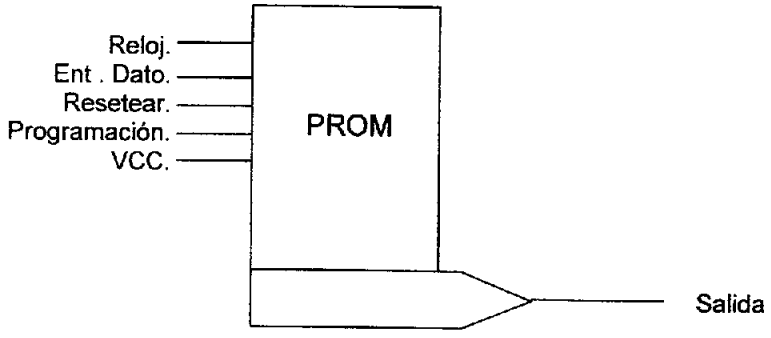


Figura 4.1 Arquitectura interna de una tarjeta de memoria

Como se puede apreciar, una tarjeta telefónica solo consta de seis patillas de entrada, una de salida y una memoria PROM. El uso de dichas patillas es el siguiente:

- Programación: la tensión de programación es de 21 voltios. Cuando no se están grabando datos en la tarjeta, dicha patilla ha de estar siempre a 5 voltios. Lo que se consigue al aplicar la tensión de 21 voltios es fundir la posición de memoria que esté en este momento seleccionada y que se quede fija a uno.
- Salida: es la patilla destinada a la salida de datos. Posee el valor de la posición de memoria seleccionada.
- Resetear: activando esta patilla se obliga al contador interno de posiciones de memoria a ponerse en la primera posición.
- Reloj: cada vez que se aplica un pulso de reloj sobre esta patilla, el contador de posiciones de memoria avanza una posición. Cuando este contador llega a 256 se pone automáticamente en la posición 1.
- Entrada de datos: es importante únicamente cuando la patilla de programación está a 21 voltios, en este caso, el valor presente en la patilla de entrada de datos es almacenado en la posición de memoria actual.
- Vcc: a través de esta entrada se le proporciona a la tarjeta la tensión necesaria para alimentar sus circuitos.

La tarjeta funciona de la siguiente manera: el circuito integrado posee un contador donde se almacena la posición de memoria seleccionada en ese momento. Existe una entrada a la que se aplica una señal de reloj que aumenta el contador en una unidad por cada pulso. Cuando el contador ha llegado a la ultima posición (bit 256), éste vuelve a la posición inicial de la memoria (bit 1) por otro lado, si el pin de entrada resetear se activa pone el contador a su valor inicial.

En el pin de salida se encuentra el valor de l bit al que apunta el contador, si éste tiene el valor 125, en la salida estará el valor del bit que esté en la memoria 125. ciando se quiere grabar un dato en una posición de memoria hay que poner el contador apuntando a esa dirección, después se coloca en la entrada de datos el valor que se desea almacenar, que ha de ser un uno ya que lo único que se permite grabar son unos, y por último poner la tensión de programación a 21 voltios.

4.3 Tarjetas de cuidados de salud

El cuidado de salud es una de las áreas de mayor aplicación de tarjetas. La intensa demanda en tarjetas para los pacientes, con varios archivos de salud computarizadas han sido motivos de diversas conferencias anuales, congresos científicos, y simposios alrededor del mundo. Hojeando los procedimientos de estas reuniones, uno puede encontrar contribuciones de muchos países donde se sugieren aplicaciones para las tarjetas enfocadas a los servicios de salud. La mayoría de las aplicaciones está en la fase de proyecto piloto. Los servicios de salud de muchos países están usando o están probando tarjetas diferentes tipos de tarjetas con sus pacientes. Es por consiguiente razonable esperar un aumento rápido de aplicaciones en un futuro cercano.

El mercado de tarjetas en cuidados de salud .-

Los fabricantes de tarjetas están conscientes del gran número de tarjetas involucrado en cualquier aplicación de cuidado de salud, y están intentando demostrar las ventajas de usar su tecnología de tarjetas en particular (plástico, microfilm, código de barras , banda magnética, óptica, inteligente)y por ello están buscando nicho en el mercado de cuidado de salud. Considerado las aplicaciones, es importante comprender cuantos tipos de tarjeta pueden usarse. dependiendo del tipo y alcance de la información requerida, por ejemplo, las tarjetas para el área administrativa tiene requisitos que son diferentes de aquéllas en donde se almacena información como datos clínicos. Los pacientes de alto-riesgo, o pacientes que exigen atención especial, puede proporcionarse tarjetas con mayor capacidad y por ende más caro en comparación de las tarjetas promedio de los usuarios. Los grupos específicos de la población como por ejemplo los niños, requieren de tarjetas que contengan información específica por ejemplo, el crecimiento, peso, calendario de la vacunación, alergias, etc. Finalmente, las personas impedidas y los pacientes crónicos como diabéticos deben poseer tarjetas teóricamente especializadas y adaptadas a sus enfermedades.

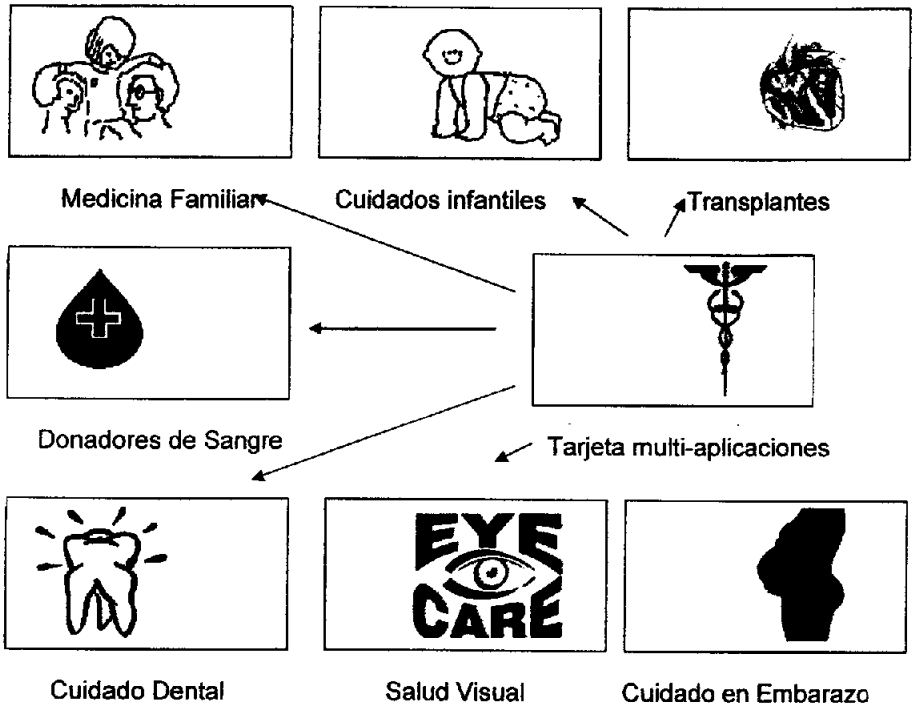


Figura 4.2 Principales aplicaciones en cuidados de salud

La salud es un área en donde se tiene una concentración grande de personas, por lo cual es importante la protección de datos del paciente, que ha de ser garantizado, y su acceso restringido para destinar a los profesionales cuidados adecuados como médicos, enfermeras, farmacéuticos sin que haya contratiempos.

4.3.1 CARACTERISTICAS PARA LAS TARJETAS DE CUIDADO DE SALUD..

Aunque la última solución en tarjetas de cuidado de salud tendría que ser basada en multi-usos o tarjetas híbridas, en varios países se han adoptado soluciones diversas por resolver, por lo menos parcialmente, según las necesidades de sus ciudadanos. Pueden emplearse tarjetas de la banda magnética simples para propósitos de identificación y pueden ser incluidas algunos datos de cuidado de salud críticos quizás como el tipo de sangre, alergias, vacunas, y alergias a medicamentos.

Las tarjetas inteligentes ofrecen un completo juego de servicios potenciales y pueden tener las reglas de la administración, emergencias, citas, además, son mayormente ventajosas en lo que se refiere a la seguridad.

El uso de tarjetas inteligentes, es desafiado por los fabricantes de tarjetas ópticas que normalmente sostienen que las historias médicas contienen demasiados datos para la capacidad del almacenamiento limitado de las tarjetas, y no es apropiado por lo que se han codificado esquemas internacionalmente aceptadas para los diagnósticos, procedimientos, y medicinas, que están disponible permitiendo ahorrar considerable espacio del almacenamiento en comparación al idioma natural.

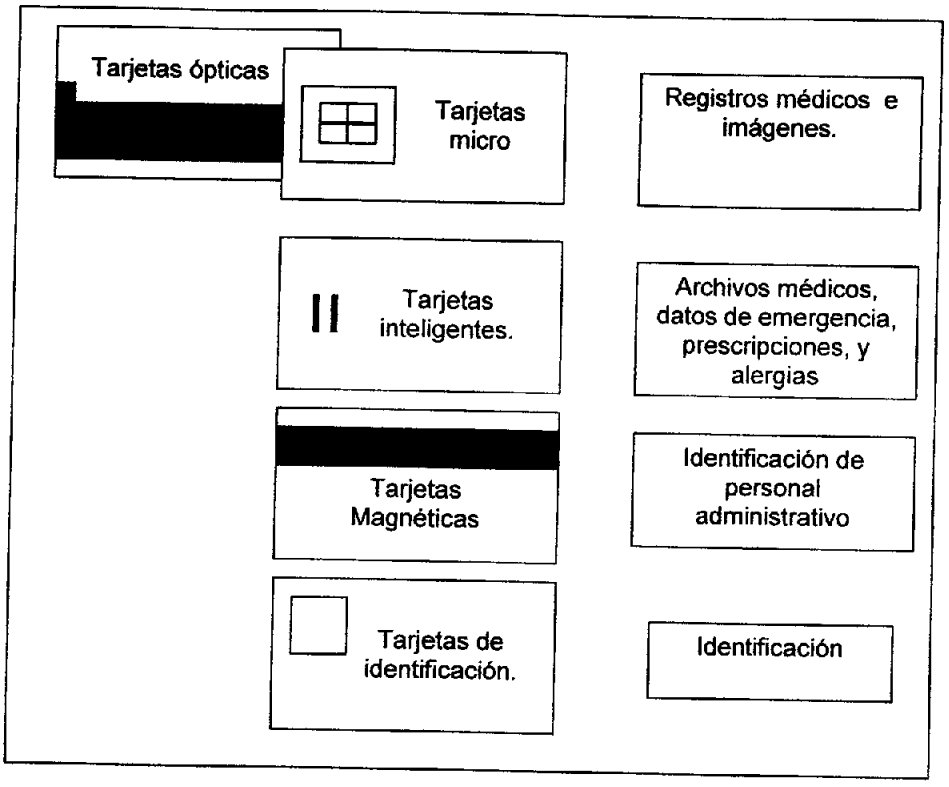


Figura 4.3 Tipos de tarjetas para cuidados médicos utilizados

La pregunta de escoger una tecnología de la tarjeta se relaciona finalmente a varios factores extranjeros, a saber, la movilidad de los usuarios y el nivel de información que comparten los centros de salud.

Por ejemplo, cuando los usuarios buscan servicio fuera de su centro asignado, y este no este conectando a una red de computadoras no se podrá transferir la información de salud solicitada. La mejor solución es una tarjeta óptica capaz de tener tantos datos pertinentes como sea posible. En donde solo un centro de salud se usa, sería aconsejable tener el registro médico entero en el centro asignado, y darle una tarjeta inteligente que contiene simplemente los datos más críticos para las emergencias y las versiones de codificado de la historia clínica del usuario y datos de la enfermedad qué pueden traducirse al idioma natural por software externo al leer la tarjeta, adicionalmente podrían ser incluidas citas automáticas, administración, y reglas.

4.3.2 PROYECTOS ALREDEDOR DE L MUNDO

En Canadá en los últimos años, se han dirigido varios proyectos piloto que involucran tarjetas cuidado salud. algunos simplemente han terminado, mientras otros todavía están continuando. los proyectos terminaron, tras ocho meses de pruebas de campo en el mes de febrero de 2003. Estos involucraron a 3000 pacientes del noroeste de Ontario. Y están evaluándose seis áreas presentemente para determinar la efectividad del sistema: interacción entre los pacientes y profesionales de salud, información dada a los usuarios, mejora de salud individual, comunicación entre servicios de salud, accesibilidad de información en emergencias, y de alergias. La atención también está dirigida a la aceptación del sistema por profesionales de salud y pacientes, así como la seguridad y confidencialidad de datos sensibles. por ejemplo, el ministerio del Ontario patrocinador del proyecto, recibió copias de todos los archivos de la consulta, y la información de identidad de pacientes fue modificada para proteger su retiro de datos en computadoras ajenas. si esta experiencia piloto tiene éxito, el uso de tarjetas inteligentes para el cuidado de salud se extenderá a la provincia entera.

Francia.

Francia es hoy el país principal en aplicaciones de tarjetas en cuidados de salud además de muchas otras áreas. el sistema nacional de Santé–Pharma basado en banda magnética, se extiende por el país entero e involucra la mayoría de sus farmacias; las estimaciones del número actual de tarjetas emitidas son cercanas al millón.

Un nuevo procedimiento del pago dentro del sistema está manejando más de 25000 pagos actualmente por mes. En cuanto a tarjetas inteligentes, las primeras experiencias y pruebas de campo en Francia han comenzado ya desde 1984,

mientras que la primera tarjeta de cuidados médicos para la población fueron dadas en 1985 llamadas proyecto de cartera de salud (Carté sante Project).

El servicio de seguro social francés a participado en diferentes proyectos por diversos años y prácticamente el 100% de la población francesa esta asegurada. su trabajo en pagar-por servicio funciona así: los pacientes pagan los servicios directamente al profesional de salud y entonces pide reembolsos. Esto genera un volumen de documentos administrativos cercanos a 800 millones los se evitaran con las tarjetas es más, el departamento del seguro social no cubre gastos del medico por completo, sólo aproximadamente 75% en cuidados primarios. Por esta razón, cerca del 80% de personas francesas tiene seguro de salud complementario, privado o de compañías de seguros mutuos. Hay más de 30 proyectos de tarjetas de cuidado de salud corriendo actualmente en Francia, la mayoría de ellos basó en tarjetas inteligentes. Algunas aplicaciones se han usado durante varios años, mientras otras, sobre todo aquéllos de las compañías privadas o diseños para el cuidado especial, está empezando simplemente su aplicación.

Reino Unido

La tarjeta de salud de Exeter es un proyecto notable, y ha estado corriendo desde 1989 en Exmouth (Devon), la preocupación principal es el maniobrabilidad de datos médicos, y los datos administrativos. Para ahorrar espacio en la tarjeta tipo 2K bull CP8 tarjeta inteligente, cinco-caracteres alfanuméricos son usados y permiten codificar patologías según el stándar internacional enfermedades. Técnicas de compresión de datos también son utilizados. El periodo del ensayo de un año se llevó a cabo entre 1989 y 1990 e involucra a médicos de cuidados primarios, dentistas, farmacéuticos, dos hospitales y 8,500 tarjetas inteligentes. Se dieron tarjetas para propósitos de identificación, acceso a los archivos de pacientes, y sus prescripciones médicas. Se usaron computadoras portátiles para las visitas de la casa. la compatibilidad entre las computadoras personales externas fue concedida para permitir el uso de los sistemas instalados. Después de la evaluación de periodo de ensayo llevada a cabo, se presentó a las autoridades de salud los resultados para decidir el futuro del proyecto. La experiencia ha sido considerada muy exitosa, actualmente unos 27,000 de 34,000 habitantes de Exmouth tienen una tarjeta inteligente que se usa en las oficinas de los médicos, farmacias, y hospitales. Estas tarjetas son accesibles por lo menos en cuatro sistemas de la computadora. Otros proyectos involucrados con tarjetas de cuidado son llebados en Londres. La Rhydyfelin-pharmacy emitió 2500 tarjetas, principalmente usado como medios de comunicación de regla electrónicos, Southport experimento en una comunidad que de servicio de alimentos, basados en tarjetas de memoria SRAM, y el hospital de Londres Oriental ha estado probando una tarjeta de memoria óptica para su servicio de maternidad.

Italia.

Se están dirigiendo varios proyectos de cuidado de salud. tres de ellos se localizan al Lombardy, Sardinia, y Umbria, y son apoyados por el ministerio de salud utilizandose tarjetas inteligentes y ópticas en estos proyectos. el más grande es Salus, en Lombardy, con 60,000 tarjetas inteligentes tipo bull cp8. Se lanzó en enero de 1989, para un periodo de pruebas de 18 meses enfocado en los servicies de emergencia de hospital y médicos.
Estas tarjetas contienen datos de patologías de riesgo: hipertensión, alergias, riesgos cardiacos, embarazo de alto riesgo, así como los datos de salud generales: el grupo de sangre, prescripciones de medicina actual, hospitalizaciones; este proyecto es bastante similar al Santal en Francia. El proyecto del Sardinia usó 20,000 tarjetas ópticas se desarrolló interesado los archivos médicos, familia y historias personales, problemas clínicos, y datos de la emergencia. el proyecto de Umbria es basado en tarjetas inteligentes principalmente para nefrologia, cardiología e hipertensión.

Tarjetas de cuidado de salud en países de Europa.

El INSALUD español, los servicios nacionales de cuidado de salud, está distribuyendo tarjetas de banda magnética para administrativo y propósitos de identificación.

Algunos estudios limitados en tarjetas inteligentes para pacientes han sido llevados a cabo, pero ninguno se ha aceptado todavía para el uso general. algunas propuestas basados en tarjetas inteligentes para grupos de pacientes seleccionados, como niños y el riesgo alto y crónicamente los pacientes enfermos, está actualmente bajo estudio. También , dos proyectos piloto de la balanza pequeño proyecta, las tarjetas del donador de sangres y la presión de sangre siguen a para los pacientes hipertensos, está corriendo actualmente.

En Portugal estudiaron la posibilidad de adoptar una tarjeta de banda magnética para usos generales, pero finalmente una tarjeta del papel simple fue seleccionada, mientras la aplicación eventual de tarjetas inteligentes es analizada. Entretanto, un proyecto geográficamente limitado para pacientes diabéticos basados en tarjetas inteligentes se ha preparado.

Suecia ha estado usando tarjetas de cuidado de salud embosadas durante 25 años, en 1989 un proyecto piloto en reglas de medicinas basadas en tarjetas inteligentes se comenzó en Tjorn, una isla cerca del Gothernburg. varios estudios en áreas de cuidado de salud específicas, como la oftalmología, maternidad, o administración se ha anunciado. También planean adjuntarse a la tarjeta profesional para cuidados de salud.

Los Alemanes empezaron una prueba de campo de piloto que involucra 2200 médicos y dentistas y 1.2 millones de pacientes, usando tarjetas de banda magnética para propósitos de identificación. la prueba debe de haber sido completada a través de 1992 ya que algunas dificultades legales del uso de tarjetas inteligentes para el momento no fue completada. los proyectos de estas son limitados para las vacunaciones y diabetes están llevándose a cabo actualmente.

4.4 Tarjetas universitarias.

Los grupos de la investigación universitarios han estado tradicionalmente envueltos en aplicaciones de la tarjeta inteligentes. no se sorprenda por consiguiente, de las aplicaciones de tarjetas inteligente en servicios universitarios son bastante comúnes. Por lo tanto las universidades comenzaron aplicaciones en los principios del desarrollo de tarjetas inteligentes. Algunas de estas eran el acceso al campus, estacionamiento, servicio de fotocopias, cafetera, y accesos a diversas áreas como se muestra en la figura

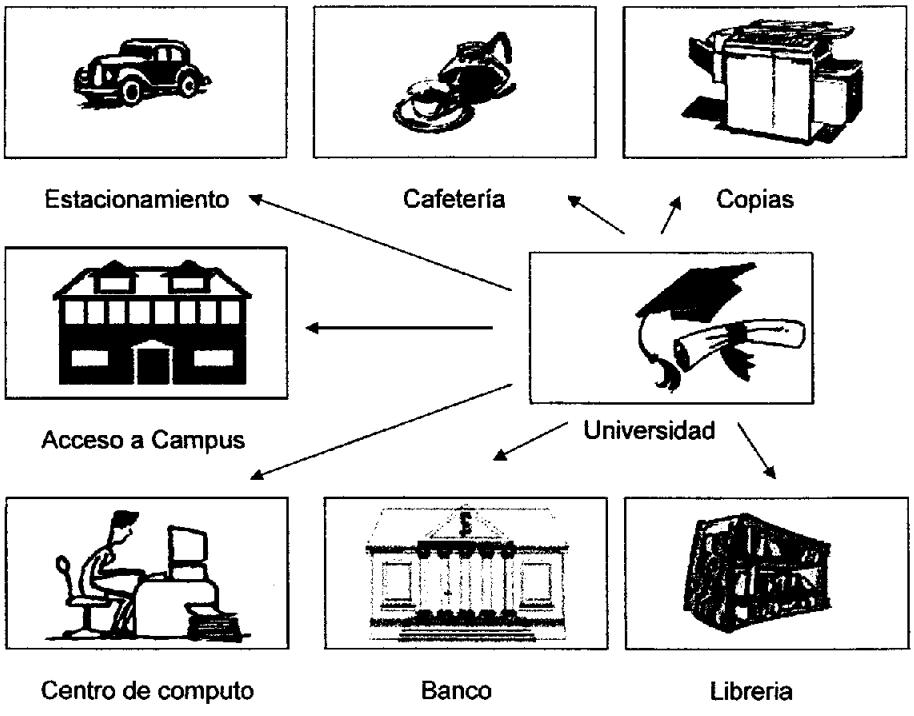


Figura 4.4 Aplicaciones en Universidades

Universidades francesas.

La primera aparición de una tarjeta con registros universitarios fue en 1983 en la universidad de Paris VII. La tarjeta almacenaba información académica de los estudiantes, datos de el progreso, año cursado, y calificaciones. En otras palabras la tarjeta almacenaba el currículo académico del poseedor, mientras ofrecía un numero de funciones extras relacionadas a las servicios del campus.

Pero el mayor proyecto comenzó en hacia 1985 en la Universidad de Ciencia y Tecnología de Lille. La tarjeta siguió la idea de la universidad de Paris, pero nuevas características fueron incluidas. Para 1989 el periodo de prueba había concluido y mas de 5000 estudiantes poseían una tarjeta electrónica. La tarjeta incluía datos académicos y administrativos, y como siempre, era utilizada con propósitos de identificación y acceso a la librería universitaria, mejorando el manejo de libros y periódicos. La tarjeta también puede usarse para obtener servicios de salud, por medio de la compañia de seguro, se puede hacer uso de esta.

El producto final fue una tarjeta multi-aplicaciones, que contenía las siguientes: control de acceso, archivo de registros y compras electrónicas. Los datos incluyen registros académicos, registro de cursos, y datos médicos. El acceso fue para las habitaciones individuales , librerías, laboratorios, y algunas áreas controladas por la tarjeta.

Universidades italianas

El mayor numero de aplicaciones para universidades esta situado en la universidad de Roma, La Sapienza, comenzó con 5000 tarjetas inteligentes otorgadas a los estudiantes de la Facultad de Economía. El llamado libreto electrónico (Libretto electrónico) trata de resolver problemas administrativos y de dirección para los estudiantes y el personal, puesto que es una de las universidades mas grandes de Europa y del mundo con 180,000 estudiantes, mas de 40 carreras, 7000 miembros de académicos y 6000 miembros de administrativo. En resumen cada estudiante generaba 30 documentos por año, por lo que se tienen mas de 5 millones de documentos. La tarjeta estudiantil , puede operar en 50 terminales alrededor del campus, donde los estudiantes consultan su historial, pregunta por documentos, u obtiene información de su facultad. Las terminales son interactivas, si los estudiantes requieren cambios en los cursos, es aplicable a documentos; si los documento s no necesitan ser certificados se pueden obtener en línea por la terminal .cuando son certificados, son transmitidos a un a red que general los documentos automáticamente, y después el estudiante puede recogerlos en la dirección de su facultad.

Los académicos tienen una tarjeta diferente, que pueden usar, a través de un PIN de identificación, para poner las calificaciones de sus alumnos. Así como cualquier tipo de información académica. Son mas de 1000 terminales las que son dispuestas para esta aplicación. Los miembros del staff tienen otra versión de la tarjeta, la cual sirve para dar de alta bases de datos, nuevas tarjetas y reposición de ellas. Más de 250,000 tarjetas están en circulación, , nuevas características son planeadas para implementarlas incluyendo privilegios de accesos a áreas restringidas, o funciones de comercio electrónico.

4.5 Telecomunicaciones y tarjetas de computo.

Las aplicaciones de telefonía publica son de las mas utilizadas, mas de 200 millones de tarjetas para teléfono prepagadas se están usando en este año alrededor del mundo. No son consideradas estrictamente tarjetas inteligentes, puesto que les falta el microprocesador. En Japón se utilizan la rededor de 400 millones de tarjetas de banda magnética para teléfonos públicos. Pero se esta considerando utilizar tarjetas inteligentes para teléfonos semipúblicos, en restaurantes, hoteles, etc. Estos teléfonos no pueden operar con tarjeta de banda magnética. Actualmente las tarjetas inteligentes son utilizadas mayormente en telecomunicaciones, computadoras y aparatos electrónicos. Como se describirá mas adelante. Algunos servicios de telefonía, usan tarjetas inteligentes como lo es el GSM en donde se integran servicios que últimamente se han empezado a comercializar. Las tarjetas pueden proteger la comunicación de datos, y almacenar datos personales con un nivel de seguridad muy alto. Las tarjetas inteligentes, son utilizadas también en otros servicios de telecomunicaciones, a saber por ejemplo el pago por recibir la señal de televisión privada es uno de los mas importantes.

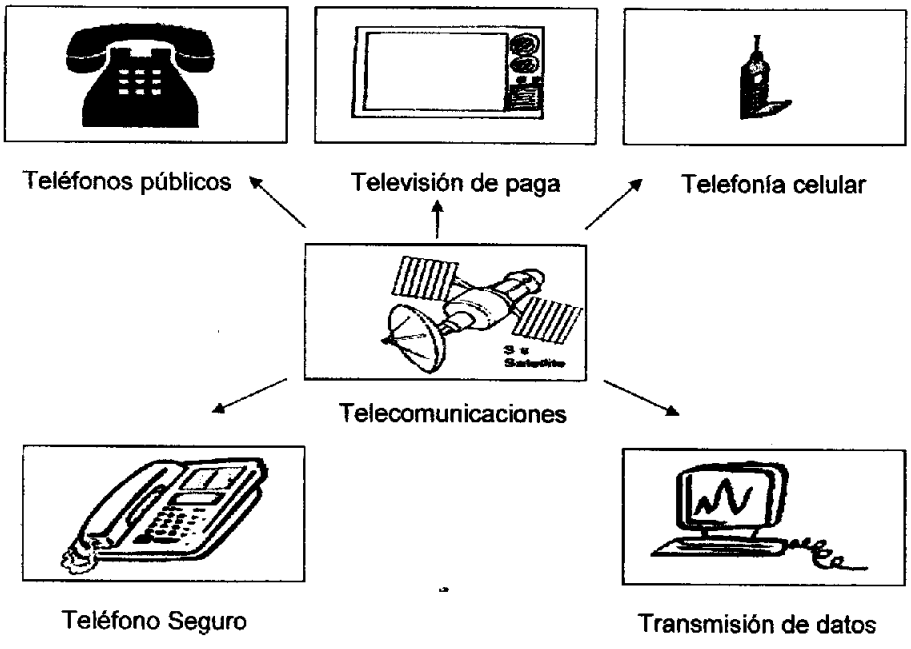


Figura 4.5 Aplicaciones en telecomunicaciones

Romin automático (follow me phones) Telefonía.

Siemens ofrece un teléfono de intercambio en donde las extensiones no están asociadas a un teléfono físico, pero si a tarjetas inteligentes. Con este sistema, el teléfono de la compañía puede ser personalizado, cada persona inscrita, posee una tarjeta inteligente, que contiene el numero de extensión asignado. Cuando el usuario llega a su oficina, el/ella inserta la tarjeta en el teléfono e introduce un PIN. Si el usuario cambia de oficina, simplemente tiene que insertar la tarjeta en el teléfono mas cercano y las llamadas automáticamente son transferidas a la nueva locación. Si la tarjeta no es insertada en un teléfono las llamadas son transferidas a una central. Como protección extra, se pide el pin a determinado intervalo de tiempo que es predefinido por el usuario. Esta protección se utiliza también para evitar malos usos en caso de que la tarjeta sea olvidada en la oficina.

La tarjeta también posee otra función, encriptación/desencriptación de voz. La voz es distorsionada cuando es enviada a través de la línea telefónica y es reconstruida al otro lado. Al utilizar esta característica ambos teléfonos se mantienen en el sistema, los datos también pueden enviarse a través de la línea. Y siempre es posible swichear entre la voz y los datos en la misma conexión. Para la salida de llamadas, la tarjeta contiene restricciones de tiempo y/o larga distancia dependiendo de los permisos otorgados al usuario. Además, la facturación puede ser distribuida individualmente desde cada registro en cada tarjeta.

GSM comunications

Los teléfonos móviles, han tenido un desarrollo importante en los últimos años, en un principio el sistema celular tenia que permanecer en un área determinada para poder tener servicio, pero debido a la problemática que presentaban al desplazarse los usuarios a diferentes áreas, fue lo que impulso el desarrollo de esta tecnología. Además del creciente numero de subscriptores que día con día se iban sumando. Un sistema basado en las tarjetas inteligentes, fue lanzado en diversos países, siendo la compañía Gemplus la pionera en este rubro. El sistema global para comunicaciones telefónicas, GSM basada en transmisiones digitales para la infraestructura celular, ofrece poderosas características. Las señales digitales en la frecuencia de 900MHZ brindan alta calidad en la transmisión de voz, transmisión de datos, fax y servicios de mensajería, codificación / decodificación de mensajes y servicios extra. La tarjeta inteligente es utilizada primeramente como autentificación. Cuando la tarjeta es insertada en el teléfono móvil, el sistema utiliza los datos de la tarjeta y un número PIN generado para identificar el modulo de subscriptor. Este número es utilizado para saber quien es su proveedor. La tarjeta puede ser movida por el usuario a otro teléfono del mismo sistema recibiendo el mismo servicio de comunicación.

Seguridad de datos en computadoras.

Las tarjetas inteligentes puedes usurase como llave electrónica en las terminales y/o computadoras. La ausencia de la tarjeta o el número correcto de PIN puede bloquear el teclado del sistema. Los discos duros también pueden ser protegidos por la tarjeta, codificados los contenidos utilizando las características de la tarjeta, o almacenando información crucial en la estructura de los datos. En cualquier caso, accesos no autorizados para leer los archivos del disco, solamente producen basura.

Las tarjetas inteligentes son tradicionalmente asociadas a aplicaciones de seguridad; la mayoría de los compañías productoras de tarjetas inteligentes como son Bull Phillips and Gemplus han desarrollado aplicaciones en donde las tarjetas están asociadas a computadoras, terminales y periféricos. En computadores personales, la tarjeta es conectada externamente a la computadora, también por medio de unidades internas mas pequeñas que una drive de 3.5. La comunicación entre diferentes computadores también puede ser protegida, antes que comience a enviar información a través de la red o del MODEM, los datos son codificados por la tarjeta inteligente. Se requiere de otra tarjeta al final de la línea para decodificar el mensaje.

Las oficinas centrales una corporación de banco Suizo ha instalado cerca de 1500 lectores de tarjetas inteligentes para sus sistemas de acceso /consulta/transacciones. Cada usuario autorizado tiene privilegios de acceso específicos. Cada tarjeta posee un PIN con los que se tienen acceso a diferentes niveles de servicios que el sistema registra. Adicionalmente si la tarjeta esta fuera de servicio por un tiempo determinado, se bloquea las funciones de esta.

Pago de TV privada.

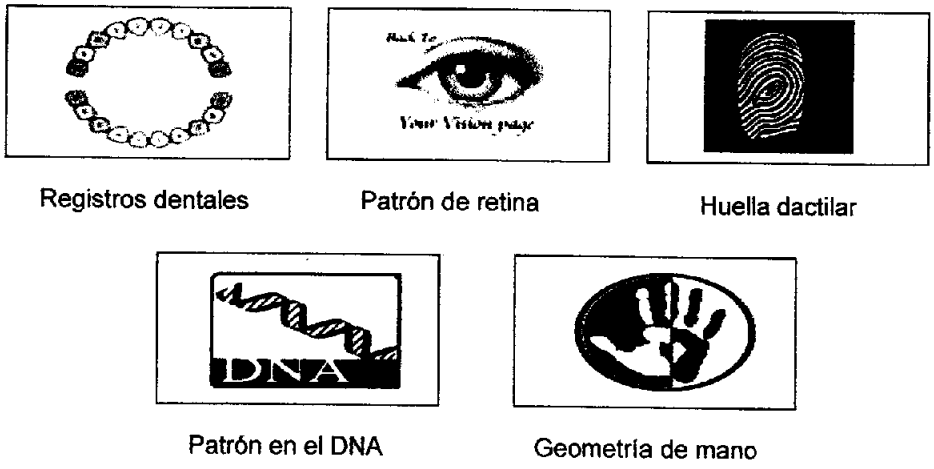
El pago por canales transmitidos de tv privada, ya sea por satélite vía microondas o cable, se a transformado hoy por hoy en una de las modalidades aplicaciones mas empleadas. Las compañías de tv privadas, obtienen ciertas ventajas al utilizar este sistema. El servicio solo es disponible para ciertos consumidores. Un ejemplo de esto lo encontramos en sistemas satelitales en donde para ver una serie de canales, hay que pagar para habilitar el servicio. En México, la tv privada vía satélite es una realidad hoy en día. Los subscriptores necesitan una antena satelital así como una caja decodificadora que se encarga de reconstruir la señal enviada digitalmente a través del satélite. Es en este componente, en donde la presencia de tarjetas inteligentes tiene su aplicación. La tarjeta guarda información del subscriptor, así como los servicios que tiene habilitados que puede ofrecer el sistema satelital.

Las tarjetas inteligentes pueden encontrar un lugar en diversas actividades, las aplicaciones pueden utilizarse en diversas áreas, por ejemplo tarjetas prepagadas para transporte urbano, como camiones, ferrocarriles, y metros. También en aplicaciones deportivas como practica del golf, membresías de clubes, etc. También pueden ser utilizadas para emplearse en hoteles, estaciones de gas, centros de compras, cinemas, y teatros.

4.6 Biomedicina.

En las siguientes líneas, diversas áreas tienen un alto nivel de actividad Una vez mas la lista no es exclusiva, en las pruebas biométricas, se puede mostrar que tan importante son las tarjetas en esta área ya que representan una inversión muy baja a largo plazo.

Las huellas digitales son un ejemplo típico aplicado en los humanos, algunas otras características pueden ser analizadas y propuestas para objetivos de identificación. Las tarjetas inteligentes de control de acceso pueden incluir además datos biomédicos. Estos datos son almacenados en la tarjeta y comparados en tiempo real con las mediciones obtenidas por los dispositivos de la persona a identificar. Se tiene un valor predefinido de tolerancia, que es utilizado para determinar el nivel de seguridad. Por ejemplo se compara el DNA que es una medida extrema de seguridad en aplicaciones tanto civiles como militares. Algunas aplicaciones se mencionaron en la sección de tarjetas de cuidados de salud. Podemos citar también el llamado reconocimiento por medio de la retina, por registros dentales, y por sistema de reconocimiento de voz.



Registros dentales | Patrón de retina | Huella dactilar

Patrón en el DNA | Geometría de mano

Figura 4.6 Ejemplos de aplicaciones de tarjetas inteligentes en bio-medicina

CONCLUSIONES

Al terminar la presente tesis, he tratado de alcanzar los objetivos planteados en la introducción. Durante la investigación, una de las dificultades que se presentaron fue la falta de información referente a las tarjetas inteligentes, ya que en diferentes bibliotecas no había algún libro dedicado a este tema, por una parte por que este tema es, por decirlo de alguna forma un tema nuevo en México, en segundo lugar, la información con la que contaba se encontraba en diversos idiomas. En cuanto al las normas ISO /IEC que nos referimos, fueron tomadas de las publicaciones oficiales de ISO. Se tomaron las normas que mas se enfocaban a este tema, pues también están involucradas a su vez las tarjetas de banda magnética. A continuación daré las conclusiones a las que he llegado al desarrollar esta tesis.

Como se he dicho en los primeros capítulos, las semejanza que hay entre una micro computadora y una tarjeta inteligentes es mínima, pues ambas poseen componentes que de una u otra formas son semejantes. Sin embargo la capacidad de procesamiento es diferente, pues están enfocadas para diferentes aplicaciones.

Uno de los errores que comúnmente tenemos es la de nombrar a todas las tarjetas que poseen terminales como tarjetas inteligentes. A simple vista parecen ser iguales pero es en su interior en donde está marcada esta diferencia. Recordemos que hay tarjetas de solo memoria como es el caso de la descrita en el capitulo 2 pero también hay tarjetas que poseen un microprocesador integrado. Para poder decidir cual vamos a utilizar, primero debemos tomar en cuenta que tipo de aplicación requerimos, y la seguridad que deseamos. En gran parte de los casos solo bastará con una tarjeta de memoria, pues en la mayoría de los casos son utilizadas como tarjetas de identificación. En donde requerimos mayor seguridad como en aplicaciones bancarias conviene enfocarse en tarjetas de microprocesador pues poseen un mayor nivel de seguridad, ya que podemos encriptar datos utilizando para este fin el microprocesador.

A nivel mundial, estamos regidos por una serie de estándares internacionales (ISO/IEC), en este caso las referentes a las tarjetas inteligentes, se mencionaron aquí. En su mayoría se refieren a cuestiones físicas, esto es, a tamaños y medidas de las tarjetas según el formato. Algunas a lo referente a las cuestiones eléctricas, como son los valores de alimentación, etc. Lo que realmente interesaría es que los fabricantes utilizaran una estandarización en cuanto al sistema operativo de las tarjetas se refiere, puesto que cada diseñador de tarjetas inteligentes tiene su propio sistema operativo. Por una parte es interesante el contar con diversas opciones, pero hay mas problemas por que en muchos casos no hay compatibilidad de plataformas. Esto se traduce en perdidas a futuro de los usuarios. Ya que muchas veces el fabricante quiere ser el único proveedor de tarjetas. La implementación de normas para los sistemas operativos para tarjetas solucionaría en gran parte estos problemas de diseño e implementación.

Uno de los puntos que es importante destacar es el de los lectores de las tarjetas, instrumento sin el cual, no podríamos tener acceso a la información contenida en estas. Existe un amplio mercado de lectores para tarjetas inteligentes, y que pueden ser de diversos tamaños y formas. También nos referimos aquí a los lectores que se utilizan en las tarjetas sin contactos. Y aunque puede haber lectores híbridos, mucho depende de la aplicación que se les destina. En esta tesis no se mencionaron ningún lector en especial, ya que la mayoría son universales, esto es en su forma física. Como se menciono antes, cada fabricante tiene su propio sistema operativo o plataforma, así mismo cada quien diseña su propio lector. Además, el punto de atención son las tarjetas no los lectores.

Las tarjetas inteligentes al tener la opción de ser una tarjeta multi-aplicaciones nos da la pauta para poder desarrollar en un futuro cercano una sola tarjeta en la cual podamos tener diversas aplicaciones como son identificación, programas de lealtad, registros médicos, accesos a clubs, incluso monedero electrónico.

Las instrucciones que se mencionan para tener acceso a la información en el capítulo 4 son genéricas, pero como sabemos, cada fabricante maneja sus propias instrucciones. Lo que se pretende es dar una idea general de como están relacionadas con esta tecnología.

La clave de un buen sistema se logra estudiando las necesidades individuales de cada cliente pues no se puede generalizar y realizar un aplicación general. Suponiendo que se diera el caso para una tarjeta en donde pudiera haber diversas aplicaciones, se tendría que examinar y en forma global, llevar a cabo dicha implementación.

Dentro del diseño de un sistema para la implementación de tarjetas inteligentes, se deben de tomar diversos aspectos que se deben de cumplir como son los siguientes:

- La aplicación a la que esta destinada. Puede ser una tarjeta de solo identificación, o de aplicaciones múltiples.

- La selección del tipo de tarjeta, y la cantidad de memoria disponible. Con esto me refiero si va a ser de contacto o sin contacto dependiendo de las necesidades del usuario.

- El proveedor de tarjetas así como la plataforma utilizada, esto es con el fin de poder tener opciones futuras de abastecimiento.

- El nivel de seguridad deseado. En los ámbitos bancarios, por ejemplo es de fundamental importancia.

- Los dispositivos a implementar. Conocidos como lectores así como su infraestructura de comunicación o configuración .

Al haber realizado la caracterización de el chip intelligent 256 byte EEPROM SLE 4432/SLE 4442 de Simens es por que es una de las tarjetas que se utilizan para aplicaciones de prepago para cabinas telefónicas. Como podemos observar, también se dieron mayores detalles en cuanto a la información que contiene esta. Seleccioné este ejemplo ya que nos muestra de manera clara y concisa la estructura interna de la tarjeta y nos da una idea de cómo podemos organizar diferentes aplicaciones.

Como recomendación se debiera de considerar importante el espacio de las memorias para optimizarlas al máximo, esto se logra implementando claves de acuerdo al criterio del diseñador con el fin de utilizar un espacio menor con la mayor cantidad de datos, teniendo en cuenta que los costos tienden a subir al requerir mayor espacio de memoria, y la mayoría de los casos esta no es justificable.

Como se mencionó en el capítulo 4 las aplicaciones a las que podemos tener acceso no son únicas y me pareció importante mencionarlas, pues en México apenas estamos implementando el uso de esta tecnología en forma masiva. Las tarjetas de prepago para cabinas telefónicas han sido pioneras en México, además de ser utilizadas cotidianamente. Tal ves se haya desarrollado a la par alguna aplicación en donde esta tecnología ya haya sido implementada, pero solo ha sido para el sector privado. Una de las áreas en donde hay mayor auge es la bancaria, pues disponen de tecnología y recursos por obvias razones. Hoy en día empezamos a observar que hay diversas aplicaciones sencillas de esta tecnología como por ejemplo en los peajes, en el cobro de tarifas de los estacionamientos, en algunas universidades privadas, en programas de lealtad de tiendas departamentales. Pero estas aplicaciones aun están floreciendo y no se les explota adecuadamente ya que por desgracia aún resulta costoso implementarla en sectores donde pudiera haber un mayor mercado como es el caso de instituciones de seguridad social.

En lo que respecta a los fabricantes de tarjetas, deberán de contar con un centro de personalización en las urbes mas importantes, ya que en la mayoría de los casos, ésta se hace en las fabricas, teniendo como consecuencia un retrasos en los tiempos de entregas. Además debe de existir la sincronización entre las partes técnico-cliente. Los detalles de los diseños de las tarjetas, colores, publicidad resultan otro factor de cuidado pues no deberá de relegarse la posición del chip en las tarjetas. Aún mas importante los materiales empleados no deberán de causar en ningún caso y bajo ninguna circunstancia, interferencia en cualquier tipo de tarjeta inteligente. Resulta paradójico que la parte mas cara de esta tecnología es su diseño/selección, implementación y licencias, pues los costos de las tarjetas

tienden a disminuir. Como podemos apreciar, se tiene un gran futuro en el desarrollo e implementación de las tarjetas inteligentes.

La oportunidad que tuve al haber ingresado y concluido mis estudios en la UNAM me dio la pauta para comprender el funcionamiento no solo de las tarjetas inteligentes, sino de una gran variedad de sistemas electrónicos.

BIBLIOGRAFIA .

1.- Smart cards Security and Applications
Mike Hendry
Second edition.
Artech house

2.- Smart Cards
Jose Luis Zoreda, José Manuel Otón
Artech house

3.- Tarjetas inteligentes
Juan Domingo Sandoval , Ricardo Brito, Juan Carlos Mayor
Paraninfo España

4.- Smart Cards "A guide to building and managing smart cards applications"
Hendry Dreifus, J. Thomas Monk
John Wiley & sons Inc.

5.- Smart card and memory card ic data briefing databook
7th Edition
STMicroelectronics.

6.-ICs for chips cards, Intelligent 256-Byte EEPROM SLE 44.2/4442 Data Sheet 07.95 Siemens AG.

7.- ISO/IEC 7816-1 Características físicas de las tarjetas

8.- ISO/IEC 7816-2 Dimensión y posición de los contactos.

9.- ISO/IEC 7816-3 Protocolos de transmisión de señales eléctricas

10.- ISO/IEC 7811-1 Técnicas de grabado en tarjetas de identificación.

11.- ISO/IEC 7811-3 Localización del embozado de caracteres en las tarjetas.

12.- Direcciones de internet con artículos relacionados:

- Open Card Framework http://www.opencard.org/
- ISO http://www.iso.ch/
- GEMPLUS http://www.gemplus.com
- AXALTO (SCHLUMBERGER) http://www.axalto.com/
- OBERTHUR http://www.oberthurcs.com
- BASICCARD http://www.basiccard.com/

- Javacard http://www.javasoft.com/products/javacard/index.html