55

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DINERO ELECTRÓNICO Y DESARROLLO DE APLICACIONES EN TARJETAS INTELIGENTES

T E S I S

QUE PARA OBTENER EL TÍTULO DE
INGENIERO MECÁNICO ELECTRICISTA
ÁREA ELÉCTRICA ELECTRÓNICA

P R E S E N T A:
RUBÉN MORA MAGAÑA

DIRECTOR DE TESIS:
ING. VÍCTOR MANUEL SÁNCHEZ ESQUIVEL

CIUDAD UNIVERSITARIA 2002.

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Agradecimientos:

Primeramente cito a mis Padres del Cielo, a *Dios* y a la *Virgen*, quienes me han dado el don y el derecho de vivir.

Ahora, de acuerdo a la cronología de mi vida:

Le doy las gracias a mis Padres, *Rubén Mora y Silvia Magaña*, quienes confiaron siempre en mí y me apoyaron siempre, generando en mí, el buen hábito del esfuerzo.

A mis hermanos *Alejandro, Silvia, Héctor, Cristina y Marcos*, quienes han estado conmigo durante mis etapas de infancia y adolescencia, y han cooperando en todo momento para mis triunfos y mis levantamientos.

A mi *dulce Esposa Alicia*, a quién le entrego mi trabajo, mi cariño y la vida sin condiciones y con la esperanza y la sapiencia de que creceremos juntos con cada suspiro.

También agradezco al Ing. *Armando Magaña*, quién me dio valiosos consejos sobre lo que es buscar y conseguir una vida con metas.

Dejo para el final mi lealtad a mis compañeros y amigos de la casa y del trabajo, pues en ellos he encontrado valores que sin duda, son dignos de reconocerse y preservarse. En este parte, me refiero muy gratamente el Ing. Gabriel Jaramillo.

Y, por último menciono la frase que me señala como Salesiano:

Hodie Labor Cras Fructus.

ÍNDICE

Objetivo

Con el fin de difundir un tema con un gran desarrollo (y grandes expectativas) en el campo de la información durante los últimos años, se ha decidido realizar este trabajo de tesis que lleva por nombre **Dinero Electrónico y Desarrollo de Aplicaciones en Tarjetas Inteligentes**.

Se pretende clarificar qué es una Tarjeta Inteligente y el entorno que la rodea. Además, para hacer más interesante el tema, se presenta un ejemplo de una aplicación sencilla, pero que nos permite visualizar un importante campo, el cual apenas comienza su camino, pero que prevé importantes evoluciones.

Para evitar violar la confidencialidad respecto a partes estratégicas de mercado y de tecnología sobre el tema que nos ocupa, se omitirán varios aspectos de la índole mencionada.

Capitulo I: Introducción

"Pagos Electrónicos", ésta es una idea que surgió desde hace algunos años debido a la necesidad de ser más eficiente al momento de efectuar una transacción y que viene a sustituir el uso del efectivo, conduciéndonos a vislumbrar un mundo en el que los billetes y las monedas serán sólo un recuerdo, o bien, articulos de colección.

La idea de realizar pagos por medio de la electrónica se remonta a muchos años atrás y ve sus inicios al momento de introducir en la vida diaria, una tarjeta prepagada, la cual eliminó problemas como el manejo del dinero; entre los primeros beneficiados se advierten las compañias telefónicas, las cuales ahorraron (y siguen ahorrando) dinero en mantenimiento.

En la década de los 70's se desarrollan diferentes tecnologías que contemplan el concepto del prepago, entre las que podemos citar a las tarjetas con banda magnética o a las tarjetas holográficas.

Al principio de los 80's, Japon adopta el concepto de prepago de manera extensiva con el uso de tarjetas con banda magnética, poco después, en Francia, se desarrolla en un laboratorio el prototipo de la tarjeta con chip; es aqui donde nacen las transacciones electrónicas como una solución enfocada al manejo del dinero.

Aunque el manejo de los chips integrados a una tarjeta plàstica era la opción más cara para ese entonces, toma la ventaja sobre otras tecnologías por diversas razones, entre las que podemos mencionar:

a) Permitió un desarrollo de estándares internacionales, dejando de ser una tecnologia propietaria, lo cual permite que se integren proveedores

distintos pudiendo mejorar con esto (entre otros rubros) un factor importante: el precio por unidad de cada tarjeta con chip.

b) Los costos de mantenimiento son mucho menores, además de que los lectores para tarjetas con chip son más baratos.

c) La seguridad en los datos es, por mucho, más alta en comparación con las tarjetas con banda magnética o las holográficas, por citar sólo un par de ejemplos.

Ahora bien, las tarjetas con chip se empezaron a desarrollar en la forma arriba descrita, pero el concepto de Tarjeta Inteligente, al cual nos enfocaremos más ampliamente, es un concepto mucho más avanzado y que se irá describiendo en los capitulos contenidos dentro del trabajo.

A continuación presentamos un extracto cronológico de la historia (anónima) de alguien que se dedico a la búsqueda de información de Tarjetas Inteligentes y que desde el punto de vista del autor de la tesis es importante, puesto que esto nos indica que aunque el desarrollo de la Tarjeta Inteligente puede llegar a abarcar grandes actividades en la vida diaria del ser humano, la difusión de la información aún no es suficiente ni extensiva.

"A finales de los años 70 aparece la idea de colocar un chip en una tarjeta de plastico, pero la tecnologia necesaria no esta disponible. A finales de los 80 se dispone ya de chips suficientemente pequeños, pero con capacidades de memoria muy reducidas. Es a principios de los 90 cuando las tarjetas inteligentes inician su despegue al empezar la telefonia móvil GSM, inicialmente con tarjetas con 1Kbyte de memoria. La Fase 1 de GSM requeria muy poca capacidad de memoria. En España se empiezan a usar de forma masiva al iniciarse la telefonia GSM. Se empezó directamente con GSM Fase 2 en septiembre de 1995 empleando tarjetas con 8Kbytes de memoria. A finales de 1997 aparecieron las tarjetas de 16Kbytes, algunas de las cuales ya

implementaban GSM Fase 2+ con SIM Application Toolkit. A lo largo de 1999 aparecen diferentes tarjetas Java, aunque no son compatibles entre sí, y a finales, las tarjetas de 32Kbytes.
En el campo del monedero electrónico se inicia el despegue en 1997 con la aparición del monedero VisaCash ®, versión propietaria implementada por Visa España ®. A mediados de año comenzó otro tipo de monedero siguiendo el estándar europeo CEN WG10.
Aunque existen prototipos desde algunos años antes, hasta finales de 1999 no salen al mercado de forma masiva tarjetas sin contacto, debido principalmente a los problemas para integrar la antena en la tarjeta. Su uso es, básicamente, para monedero electrónico y control de acceso."

Como podemos ver, la información dista mucho de ser completa, por lo que nos disponemos a dar un panorama mucho más amplio de las tarjetas inteligentes y su uso presente y futuro, mediante varios capítulos, los cuales describimos a continuación

En el capítulo de Antecedentes se hace referencia a como han ido evolucionando los medios de pago, desde siglos atrás, hasta nuestros días, en los que usamos plásticos con chips (que son circuitos integrados) embebidos para poder realizar consumos de todo tipo. También se explica que tipos de tarjetas con chip hay en la actualidad y qué estándares rigen a cada una de ellas.

Monederos Electrónicos es el siguiente capítulo que se trata en el presente trabajo y es aquí donde definimos los conceptos más importantes de dicha aplicación, cómo funciona y los beneficios que aporta a nuestra actual sociedad. También se explica cómo funciona el Monedero Electrónico en nuestro país y cómo nos encontramos en el ámbito internacional. Lo tocante a la telefonía pública es descrito dentro de este capítulo; al tema se le considera

de gran interés ya que aquí se explica cómo funciona una sola terminal (el teléfono público) para poder realizar consumos y recargas de dinero.

Cuando en una sola tarjeta podemos guardar información que está relacionada con diferentes servicios, hablamos de una tarjeta con capacidad multiaplicativa, por esto un capítulo más es el que lleva por nombre Multiaplicaciones. Aquí describimos el concepto anterior y se dan posibles esquemas de las tarjetas, además de desarrollar un ejemplo que nos clarifica dudas sobre cómo funcionan las tarjetas con chip.

¿Hasta dónde podemos llegar con las tarjetas?, es ésta una pregunta muy importante que nos podemos hacer, por esto describimos ambientes que ya existen en la actualidad (por ejemplo, el caso de internet) son usados para ampliar más el campo de uso de las Tarjetas Inteligentes

Con estos tópicos podemos llegar a tener un conocimiento bastante amplio sobre qué son y cómo funcionan las Tarjetas Inteligentes, cumpliendo con el claro objetivo de difundir el conocimiento sobre una nueva tecnología que revolucionará al mundo de las transacciones monetarias.

Capítulo II: Antecedentes

II.1. Conceptos básicos

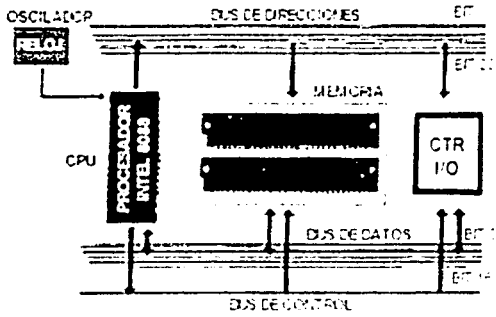
Después de la introducción del transistor, en la década de los años cuarenta, se han presenciado cambios importantes, como la introducción del Circuito Integrado (en los años sesenta), que posibilitó la fabricación de varios transistores en un único sustrato de silicio en el que los cables de interconexión iban soldados. El circuito integrado permitió una posterior reducción del precio, el tamaño y los porcentajes de error. Luego entonces, se desarrollo el microprocesador que se convirtió en una realidad a mediados de la década de 1970, con la introducción del circuito de integración a gran escala (LSI, acrónimo de Large Scale Integrated) y, más tarde, con el circuito de integración a mayor escala (VLSI, acrónimo de Very Large Scale Integrated), con varios miles de transistores interconectados soldados sobre un único sustrato de silicio. Si no se hubieran dado estos desarrollos los circuitos individuales y sus componentes ocuparían demasiado espacio como para poder conseguir un diseño compacto.

El circuito integrado típico, llamado chip, consta de varios elementos como resistores, capacitores y transistores integrados en una única pieza de silicio. En los más pequeños, los elementos del circuito pueden tener un tamaño de apenas unos centenares de átomos, lo que ha permitido crear sofisticadas computadoras del tamaño de un cuaderno.

Ahora bien, con el fin de adentrarnos en este trabajo, hablaremos en este tema, sobre conceptos básicos que se relacionan con las Tarjetas Inteligentes.

II.1.1. Microcontrolador

Un microcontrolador está compuesto de las siguientes partes:



Oscilador o reloj.- Es el encargado de dar un ritmo de funcionamiento al procesador y a toda la circuiteria en genera', por lo tanto, determina la cantidad de instrucciones que puede ejecutar el procesador por segundo.

CPU (Unidad Central de Proceso) - Es el microcircuito al cual se encuentran las instrucciones de código maquina y donde son procesadas las mismas. El CPU es capaz de interpretar las instrucciones y coordinar su ejecución. Esta constituida por los siguientes subsistemas funcionales:
Unidad aritmética Logica (ALU) Es el elemento controlador del sistema, capaz de realizar operaciones logicas (AND, OR, XOR) y aritméticas;
Unidad de Control (UC) Es el elemento controlador del flujo de información (instrucciones y datos) en el sistema Generador de reloj.

Memoria.- Esta formada por una serie de chips donde se almacena toda la información del sistema , lo cual incluye tanto al código (instrucciones) como los datos de cualquier tipo.

Bus de datos.- Es por donde se mueve la información digital que circula por todo el sistema (memoria, puertos...), desplazándose principalmente entre la memoria y el CPU y viceversa. Por ejemplo, este bus es de 16 bits en el 8086, 8 bits en el 8088 y 32 bits en el 80386.

Bus de Direcciones.- Es por donde el CPU indica a los circuitos la posición física dentro de la memoria en la que está la información a la que quiere acceder (ya sea para leerla o para escribir en ella) para después enviar o leer su contenido a través del mencionado bus de datos. Este bus posee 20 bits de ancho de banda.

Bus de control.- Este bus es el encargado de indicar al sistema qué tipo de información circula por el bus de datos en cada momento y sincroniza las señales que controlan el funcionamiento de la circuitería del sistema.

A grandes rasgos, puede decirse que los buses son pequeños "cables" que conducen bits de información de sus respectivos tipos y usos. Estos "cables" están formados cada uno por X hilos (filamentos), por cada uno de estos hilos circula un solo bit y su número indica el ancho de banda del bus. Así, por ejemplo, un computador de 32 bits puro posee los buses de datos y direcciones, ambos con 32 hilos cada uno, con lo cual puede hacer circular 32 bits simultáneamente en un solo ciclo de reloj

Sistemas I/O - El Sistema de entrada y salida permite la comunicación del microcomputador con el mundo exterior. Se denomina interfase al sistema hardware-software que permite la comunicacion con un periférico determinado, es decir el conjunto de circuitos (hardware) y programas (software) que se utilizan para establecer la comunicacion.

Las tareas de entrada y salida pueden consumir excesivo tiempo de máquina, por lo que puede ser precisa la utilización de circuiteria externa. Existen dos tipos de información en la comunicación microprocesador - periférico:

1) Datos: entrada de información para proceso y salida de resultados.

2) Control: salida de señales para el gobierno de periféricos y entrada de información del estado de los mismos.

Ahora bien, existen *Registros* que nos permiten manejar la información que se procesa en el microcontrolador, y a continuación los definimos:

Registros Generales

Acumulador: Este registro es usado sobre todo en operaciones aritméticas como primer operador y también como registro de propósito general a disposición del programador.

Base: Se usa principalmente para indicar posiciones de memoria (offsets).

Contador: Este registro se usa siempre que se necesite un contador en operaciones repetitivas y bucles.

Dato: Se usa como registro auxiliar en operaciones aritméticas y como contenedor de datos a la hora de usar instrucciones de comunicación de puertos.

Estos cuatro registros, como todos los restantes, son de 16 bits, o sea, pueden almacenar valores comprendidos entre 0 y 65535 (2^16), pero para permitir también realizar operaciones tipo byte (8 bits), cada uno de estos cuatro registros está dividido en dos de 8 bits a los que se puede acceder de forma independiente. Se tiene que todas las instrucciones ensamblador pueden

operar con datos de 8 y 16 bits según lo que se precise. En los demás registros que se explicarán, esta subdivisión no es posible.

Registros de Segmentos

Son cuatro registros de 16 bits usados para referenciar direcciones de memoria.

Code Segment: Este, llamado <segmento de código>, es usado por el procesador para saber dónde está dentro de la memoria la instrucción actual que está siendo ejecutada.

Data Segment: Se usa para referenciar dónde están todas las variables del programa en ejecución.

Stack Segment: Aquí se indica al procesador dónde está la zona de memoria que se usa como <segmento de pila>.

Extra segment. Se usa como apuntador de memoria auxiliar en operaciones complejas donde se necesitan dos punteros de datos simultáneos.

Registros Puntero/Indice

Se utilizan como desplazamientos (offsets) complementarios para Data Segment y Extra Segment a la hora de referenciar la posición donde se encuentran datos a los que queremos acceder.

Source index: Se usa como puntero origen en operaciones de desplazamiento de datos entre dos zonas de memoria.

Destination index: Se usa como destino en operaciones como la comentada en el anterior registro.

Registro de Banderas

Este es un registro usado para tener el control de las operaciones del micro. Cada uno de los 16 bits indica una cosa diferente (en caso de que lo use el micro para indicar algo).

Registros de Puntero/Instrucción

Sólo hay uno, es usado por la CPU para tener recordar la posición relativa a la base donde se encuentra la instrucción que se está ejecutando actualmente. Este registro no puede ser modificado por parte del programador. Este puntero cambia su contenido automáticamente cada vez que saltamos a otro punto del programa mediante una instruccion de salto.

Instruction pointer: Su traducción es "Puntero de instrucción".

Registros de PILA

La pila es un area de memoria importante y por ello tiene, en vez de uno, dos registros que se usan como desplazamiento (offset) para apuntar a su contenido. Se usan como complemento al registro <segmento de pila> y son:

Stack Pointer: Se traduce como puntero de pila y es el que se reserva el procesador para uso propio en instrucciones de manipulado de pila. Por lo general , el programador no debe alterar su contenido.

Base pointer: Se usa como registro auxiliar. El programador puede usarlo para su provecho.

II.1.2. Protocolos

Otro concepto importante es el de protocolo, y es aquél que establece una descripción formal de los formatos que deberán presentar los mensajes para poder ser intercambiados por equipos de cómputo (por ejemplo); además definen las reglas que ellos deben seguir para lograrlo.

Los protocolos están presentes en todas las etapas necesarias para establecer una comunicación entre equipos de cómputo, desde aquellas de más bajo nivel (como la transmisión de flujos de bits a un medio físico) hasta aquellas de más alto nivel (como el compartir o transferir información desde una computadora a otra en la red).

Ahora bien, para poder verificar la integridad en la información que estamos transmitiendo, se hace uso del código CRC (Cyclic Redundancy Code) y un método para poder calcularlo es el polinomial, el cuál trata a las cadenas de bits como polinomios con coeficientes de 0 y 1.

II.2. Generales

Desde principios de los tiempos el ser humano ha comprado, vendido, intercambiado, regalado, pagado, todo esto con el fin de obtener algún bien o servicio. Se han usado metales, semillas, papel moneda, últimamente tarjetas con banda magnética y, ahora, Tarjetas Inteligentes, las cuales llevan un chip inmerso en el plástico y que nos permite guardar dinero electrónico dentro de él, pero la Tarjeta Inteligente no restringe su uso al pago de bienes y servicios, mediante la aplicación conocida como Monedero Electrónico (a la cual nos referiremos en el futuro como ME), es también un medio en el cual se almacenan aplicaciones diversas tales como Lealtad, Transporte y Acceso, entre otras.

Este tipo de tarjetas nace de la necesidad de hacer más eficientes los medios de pago, dando seguridad, rapidez y comodidad a todo tipo de gente, y ofreciendo dentro de un sólo chip, la posibilidad de almacenar información que nos ayudará en la realización de diferentes operaciones en terminales (ya sean de consumo o de carga).

La eficiencia de pagos por medio de las tarjetas de débito ha sido probada desde hace algunos años, pero el pago de pequeños montos (es decir, no mayores a los $1000.00 pesos, en la actualidad) está aún limitado debido a los altos costos por transacción. Es por esta razón que el mercado está demandando nuevas formas de pago para las compras pequeñas. En suma, se requiere una calidad probada y mejorada en comparación con el uso de una tarjeta de débito.

La forma de pago, a la cual se recurre, es por medio de la Tarjeta Inteligente con aplicación ME.

Grosso modo, una Tarjeta ME es aquella que contiene un chip (la tarjeta y el chip son la Tarjeta Inteligente), en el cual se almacena *dinero electrónico* dentro de la memoria del mismo.

La Tarjeta Inteligente es uno de los últimos avances que se han dado dentro del mundo de la información. Es similar en tamaño a una tarjeta plástica con banda magnética, pero posee un chip, el cual cuenta con un microprocesador (con sistema operativo propio) embebido en el plástico. El chip almacena datos electrónicamente de una manera segura. Cuando la tarjeta es acoplada a un dispositivo lector, se pueden procesar diferentes aplicaciones, tal como la aplicación ME.

La aplicación del ME está pensada para realizar pagos pequeños que requieran *dinero real* y cheques de baja denominación. Está dirigido a:

- Tiendas
- Máquinas expendedoras
- Parquímetros
- Transporte público
- Teléfonos
- Actividades móviles (como taxis)
- Internet y comercio electrónico
- Etcétera ...

Con respecto a otros medios de pago, un ME cuenta con ventajas tales como rapidez y seguridad, además de que tiene la posibilidad de ser recargado a través de dispositivos especiales desarrollados para tal fin, como puede ser un teléfono público, el cual, por estar muy diseminado en nuestro país, nos ofrece un buen servicio.

A lo largo del desarrollo de la tesis, no sólo nos enfocaremos a expresar qué es y cómo funciona un ME, sino que también hablaremos sobre lo que es la Tarjeta Inteligente, todo bajo el compromiso de no violar estatutos de confidencialidad con empresas involucradas en el manejo y desarrollo de este tipo de tarjetas.

II.3 Tipos de tarjetas

De memoria, de microprocesador (contacto y sin contacto).

De las tarjetas con chip que se pueden encontrar actualmente en el mercado, las que nos interesan para desarrollar aplicaciones son las Tarjetas Inteligentes, pero es importante mencionar las Tarjetas de Memoria, las cuales

fueron y son las antecesoras de esta nueva tecnología, es por ello que damos un acercamiento de lo que es cada una de ellas.

Las Tarjetas de Memoria son incapaces de procesar información; son simplemente dispositivos de almacenamiento y en este aspecto son muy similares a las tarjetas de banda magnética. Poseen una memoria extensa pero están condenadas a tener un bajo nivel de seguridad. Dichas tarjetas están dirigidas a aplicaciones muy sencillas, y como ejemplo las tenemos en los teléfonos, los cuales debitan unidades de la memoria de las tarjetas. Al momento en el que una tarjeta de memoria ha sido consumida totalmente con todas sus unidades, queda inservible y sin posibilidad de ser usada una vez más; van directo al depósito de basura o al sitio de honor de un coleccionista.

Por otro lado, las Tarjetas Inteligentes (las cuales reciben también nombres como Tarjetas de o con Microprocesador y Smart Cards en inglés) poseen grandes cantidades de memoria y un microprocesador, y no sólo almacenan datos, sino que también son capaces de procesarlos y ejecutan cálculos algoritmicos. Una de las aplicaciones más obvias para las Tarjetas con Microprocesador consiste en la encripción de datos para intercambiarlos con dispositivos lectores que prevengan y detecten intentos de fraude. Ver anexo 1.

Es posible considerarlas como una pequeña computadora localizada en un plástico, y con la habilidad suficiente para soportar aplicaciones avanzadas con la garantía de un alto nivel de seguridad.

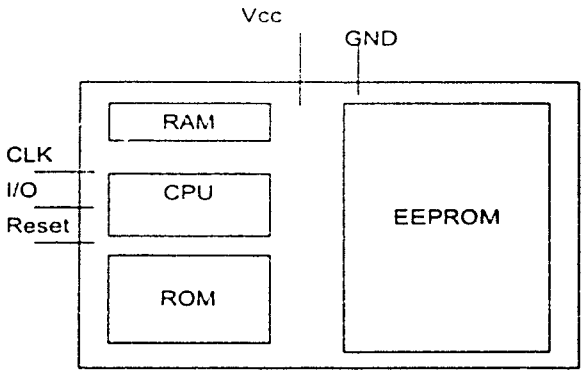
Dentro de las Tarjetas Inteligentes se tiene la división entre tarjetas de contacto y sin contacto.

Las que son por contacto deben de ser insertadas en un lector de tarjetas. Tienen un plato sólido dorado de alrededor de media pulgada de diámetro en el

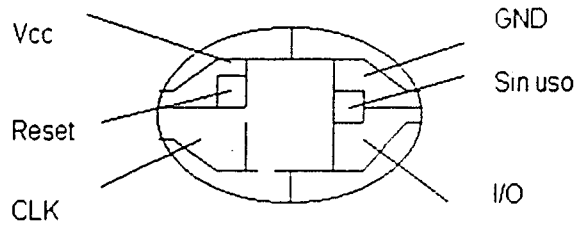
frente, en vez de una banda magnética en la parte trasera como las tarjetas de débito y crédito. Cuando la tarjeta es insertada en el lector se hace el contacto eléctrico necesario con los puntos que permiten transferir datos de y hacia el chip. Este tipo de tarjetas son las que se usan más comúnmente en casi cualquier aplicación, aunque en algunas aplicaciones, tal como es el transporte, son de uso más frecuente y eficaz, las tarjetas sin contacto.

Por otro lado, a las tarjetas sin contacto se les hace pasar frente a una antena para poder ejecutar una transacción. Físicamente se parecen a una tarjeta como cualquier otra, con contacto o sin contacto, excepto que tienen un microchip y una antena embebida dentro del chip. Estos componentes le permiten a la tarjeta comunicarse con una unidad acopladora de antenas sin un contacto físico. Estas tarjetas ofrecen la solución ideal para transacciones que deben de ser procesadas rápidamente; el sector que puede ser beneficiado más ampliamente en este apartado es el Transporte masivo de personal, como lo es el metro, o camiones en la ciudad.

Ahora bien, la arquitectura de un chip, es la siguiente:



Luego entonces, los puntos de conexión, son los siguientes (según la norma ISO -*Organización Internacional de Estándares*-):



Definiendo los términos arriba mencionados, tenemos lo siguiente:

CPU.- Es la unidad central de proceso, donde se llevan a cabo cálculos lógicos y aritméticos, manejando la comunicación con la tarjeta.
Sistema operativo.- Es un programa, el cual es *inicializado* cuando el chip recibe alimentación, permite ejecutar cálculos e intercambios con el exterior (terminales punto de venta)
El sistema operativo está grabado en la memoria ROM y por lo tanto, no puede ser modificado

RAM.- Esta memoria es usada sólo por el sistema operativo para operaciones propias del microprocesador. El desenergizar dicha memoria, provoca el borrado de la misma.

EEPROM.- En esta memoria se almacenan los datos de las aplicaciones. El desenergizar la memoria EEPROM, no causa la pérdida de dichos datos.

II.4. Estándares de tarjetas con contacto y sin contacto

La primera pregunta que se nos puede ocurrir es: ¿qué es un estándar?. De acuerdo con la Organización Internacional de Estándares (ISO de las siglas en inglés de International Standards Organizations), "Los estándares son acuerdos documentados que contienen las especificaciones técnicas u otros criterios muy precisos para ser usados consistentemente como reglas, lineamientos o definiciones de características para asegurarse que los materiales, productos, procesos y servicios cumplan con sus propósitos". Los estándares son documentos que no dependen del número total de páginas.

Los estándares gobiernan nuestra vida diaria, especifican las características de muchos de los productos que usamos frecuentemente, como rollos de cámaras, la industria de automóviles o unidades métricas. Las características físicas y eléctricas de las tarjetas también cumplen con estándares provenientes de las normas ISO y son respetados a lo largo y ancho de todo el mundo.

Es importante mencionar que los estándares pueden evolucionar a medida que los involucrados en un desarrollo lo requieran.

Durante los últimos años, varias organizaciones internacionales como ISO, CEN (European Comitee for Standarization), IEC (International Electrotechnical Commision), entre otras, han estado trabajando conjuntamente para decidir en qué formas se pueden definir las tarjetas para el uso internacional y se han dictado los Estándares Normativos para Tarjetas Inteligentes que se resumen a continuación:

ISO 7810 Características Físicas

ISO 7816 Tarjetas de Circuito Integrado con Contacto
ISO 10373 Métodos de Prueba
ISO 10536 Tarjetas de Circuito Integrado sin Contacto

Nota: *Embosado* proviene de la palabra *Embossing* en inglés; a lo que hace referencia este vocablo, es al hecho de resaltar (en la impresión gráfica de la tarjeta) el nombre o número de cuenta del cliente.

Los últimos desarrolladores de aplicaciones han adoptado los estándares existentes para tarjetas con banda magnética. Estos estándares establecen las caracteristicas físicas de las tarjetas plásticas y fijan la localización de la banda magnética en la parte trasera de la tarjeta, el *embosado* en la parte delantera de la tarjeta, así como de los chips que se pueden colocar sobre la tarjeta sin violar los estándares existentes.

Las Tarjetas Inteligentes, además de poseer su chip, tienen la posibilidad de contar con el embosado y/o la banda magnética, para así poder obtener información del chip, de la banda y de la impresión en papel del *embosado*.

Cada estándar tiene sus propias caracteristicas, el estándar ISO 7810 define la durabilidad física de las tarjetas con banda magnética, también define la flexibilidad y la locación del *embosado* en la tarjeta

En ISO 7816 se establecen los estándares para Tarjetas Inteligentes con Contacto, es aquí donde vamos a concentrarnos más ampliamente.

Este estándar se compone de varias secciones en donde se especifican los requerimientos mínimos para las caracteristicas físicas, técnicas de acceso a los datos y técnicas de almacenamiento de datos. Para ser más claros, veamos la siguiente tabla:

Sección	Nombre de la Sección
1	Características físicas
2	Tamaño y localización de los contactos
3	Señales electrónicas y protocolos (Ver anexo 2)
4	Comandos
5	Identificadores de aplicaciones
6	Elementos de los datos para intercambio
7	Comandos mejorados para intercambio de datos

La idea de tener secciones dentro de ISO 7816, es debido a la posible evolución por partes, y de acuerdo con las demandas que exija el mercado y los avances tecnológicos obligados. A continuación explicamos las secciones de este estándar.

En la sección 1 se describen las características físicas de las Tarjetas Inteligentes (como por ejemplo el ancho del plástico) y diferentes métodos usados para probar su concordancia con los requerimientos.

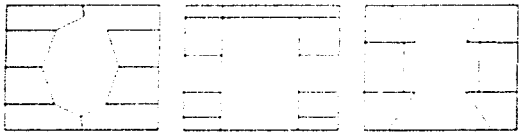
En la sección 2 se sustentan las dimensiones y las posiciones de los contactos eléctricos.

Cada contacto debe tener un área rectangular mínima de 2 (mm) de ancho por 1.7 (mm) de largo y debe de estar aislado de los demás contactos. Se definen 8 contactos, a los cuales nos referimos como C1 a C8.
A continuación se muestra una tabla con los contactos que posee un chip:

Contacto	Función
C1	Voltaje de alimentación (+5 [V] generalmente)

C2	Reset (RST)
C3	Reloj (CLK)
C4	Sin conexión y reservado para uso futuro
C5	Tierra (0 [V])
C6	Vpp (Voltaje de programación)
C7	I/O
C8	Sin conexión y reservado para uso futuro

Los diseños de los chips son variados, pero mantienen los contactos en la posición indicada en el estándar. Algunos diseños de chips, pueden lucir como los siguientes, y el dibujo depende del fabricante:



De acuerdo con las disposiciones de los fabricantes del chip, se omite su diagrama interno.

En la tercera sección se habla sobre las señales electrónicas y protocolos de transmisión. También se describe en qué dirección se entabla la conversación terminal-tarjeta. Es importante mencionar que la función de reset de la tarjeta corresponde al primer contacto eléctrico que se da al introducir la tarjeta en una terminal y esta función se describe más adelante, en este apartado de la norma ISO 7816. Hablemos ahora un poco sobre los contactos de las tarjetas:

Vcc: Este contacto es usado para proveer de energía a la tarjeta con la fuente de alimentación. La corriente máxima está definida por la tarjeta misma. La

interfase debe ser capaz de entregar esta corriente dentro del rango especificado para los valores de voltaje.

I/O: Este contacto es usado como entrada (modo de recepción) o salida (modo de transmisión). La información intercambiada usa los siguientes estados lógicos, definidos en ISO 1177:

- Estado Z.- Si la tarjeta y el dispositivo de interfase están en modo de recepción o si el estado es impuesto por el transmisor.

- Estado A.- Si este estado es impuesto por el transmisor.

Cuando ambos extremos de la línea estén en modo de recepción, la línea deberá estar en estado Z (estado alto). Cuando ambos extremos no estén igualados en modo de transmisión, el estado lógico de la línea puede estar indeterminado. Durante la operación, el dispositivo interfase y la tarjeta no deben de estar en modo de transmisión.

El dispositivo interfase debe de ser capaz de enviar la corriente definida dentro de los rangos establecidos y en los voltajes predeterminados.

CLK: Este contacto es usado para proveer a la tarjeta de una señal de reloj. Los valores de la frecuencia se definen en ciertas tablas especificadas dentro de esta sección del ISO.

RST: Este contacto es muy útil ya que nos sirve para dar una señal de reset (restauración) a la tarjeta. Como ya se mencionó, el *reset*, es la primera respuesta que una tarjeta chip nos entrega al momento de ser energizada y está compuesta por una cantidad definida de bytes los cuales nos sirven para identificar datos como que tipo de tarjeta es, a que proveedor pertenece o que sistema operativo emplea.

Vpp: Este contacto actualmente está reservado para uso futuro, por lo que su definición no es de interés para fines prácticos.

Los intercambios de datos, entre tarjeta y lector, son descritos dentro de la sección número 4 del estándar. Estas instrucciones son la base de los comandos comunes que son empleados para interactuar con la tarjeta, permiten la creación de directorios dentro de la tarjeta, modificación, lectura, escritura y borrado de los datos dentro de los archivos. Veamos la siguiente tabla en la cual se especifican los comandos elementales dentro de ISO: (Ver anexo 2).

Comandos ISO 7816
Seleccionar archivo
Escritura binaria
Lectura binaria
Actualización binaria
Borrado binario
Lectura de registros
Escribir registros
Log de registros
Actualizar registros
Obtener datos
Poner datos
Verificación
Autenticación interna
Autenticación externa
Obtener *challenge*
Manejar canal
Obtener respuesta

En esta sección de la norma ISO, se habla de dos categorías de archivos:

- DF (Archivo Dedicado, de las siglas en inglés *Dedicated File*, ver tema de *Estructuras*).

- EF (Archivo Elemental, de las siglas en inglés Elementary File)

La organización de los archivos dentro de una tarjeta lleva una jerarquía, la cual consiste de un archivo principal o maestro al nivel de raiz, que también es un DF, y los demás archivos DF, que corresponden a las diferentes aplicaciones en la tarjeta. Es importante mencionar que los archivos EF están contenidos dentro de los archivos DF.

Los archivos EF se dividen en:

a) EF's que almacenan datos para manejo y para propósitos de control de la tarjeta; en esta división encontramos a los públicos y a los secretos.

b) EF's que almacenan datos que son interpretados por la tarjeta, a estos archivos se les llaman de "trabajo".

Los Archivos EF pueden ser de diferentes tipos:

- Fijos
- Ciclicos

Los archivos que son del tipo ciclicos, son usados para almacenar datos que continuamente están siendo modificados; como ejemplo tenemos los archivos donde se guardan las últimas transacciones (caso de la aplicación ME) que se han realizado con el chip, ya sean compras o recargas.

Los archivos fijos, permiten almacenar datos que no requieren ser modificados, tales como nombres, edades, números de placas, etcétera.

En la quinta sección, se define la forma de como se deben reservar los identificadores de archivos correspondientes a los emisores de tarjetas. Provee la información necesaria para uniformar la industria.

Los Identificadores de Archivo nos sirven para poder diferenciar entre distintos tipos de archivos de la tarjeta y niveles dentro de la misma y están compuestos por 2 Bytes. Los niveles en la tarjeta son usados para poder diferenciar entre aplicaciones.

La norma ISO 7816, en su parte sexta, describe los elementos de los datos (como el nombre, NIP, fecha de expiración, entre otros) que pueden ser manipulados por el microcontrolador. Estos elementos pueden ser manejados por los comandos mencionados en la sección número 4

La sección 7 se encuentra en desarrollo y describe las funciones adicionales y caracteristicas que estaran disponibles para mejorar comandos.

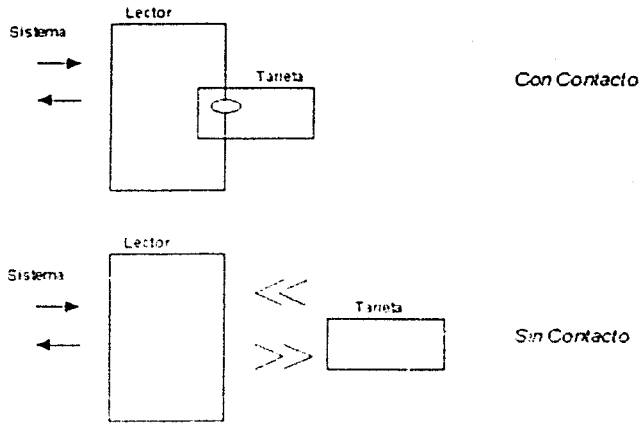
Los estandares para tarjetas Sin Contacto (del ingiés, *contactless*) son muy similares a los descritos anteriormente, razon por la cual nos quedamos con las anteriores definiciones y sólo abordaremos los siguientes puntos.

Un sistema contactless esta compuesto por:

Un chip (microcontrolador + interfase de radiofrecuencia)
Una tarjeta que contenga antena
Un lector

La interfase de radiofrecuencia debe de proveer al microntrolador energía estable, una señal de reloj y los datos recibidos del lector (demodulador), y debe recibir del microcontrolador datos que serán enviados al lector y por último una señal de reset.

El esquema siguiente, nos permite hacer una pequeña comparación entre un sistema con contacto y el contactless:



Entre los múltiples beneficios que se pueden observar al momento de usar una tarjeta sin contacto, podemos encontrar muy claramente la rapidez con la que se realiza una transacción con monedero electrónico, puesto que el tiempo total de proceso es inferior al medio segundo.

Las operaciones que son realizadas con chips *contactless*, se dan de acuerdo con los cambios de corriente que experimentan tanto la antena de la tarjeta como la antena del dispositivo receptor, y son estos cambios los que se interpretan como la información que está siendo intercambiada entre ambos elementos. Pero, ¿qué pasa si dos o más tarjetas intentan realizar una operación al mismo tiempo sobre un solo lector?; pues bien, existe un método conocido como *anticolisión*, que permite que una y sólo una tarjeta sea la que realice su intercambio de datos con el lector en un mismo diferencial de tiempo, con el fin de no mezclar y confundir información; es decir, identifica las tarjetas presentes en el campo y permite *direccionamientos* (instrucciones) sobre una y sólo una tarjeta seleccionada.

El estándar que rige las tarjetas sin contacto es el ISO 14443 y consta de las siguientes secciones:

Parte 1. Características Físicas.

Parte 2. Potencia para Radiofrecuencia y señal para la interfase.

Parte 3. Inicialización y anticolisión.

Parte 4. Protocolos.

Actualmente, el diseño con tarjetas contactless está limitado significativamente por la energía disponible para energizar y operar un chip en un campo de radiofrecuencia. El factor importante en tarjetas contactless es el tamaño de las antenas. El tamaño de la antena determina la cantidad de energía que puede ser inducida a la tarjeta y limita los rangos de lectura/escritura en la tarjeta.

Las aplicaciones contactless son simples (por lo general) y van desde simplemente detectar la tarjeta en el campo de RF a la interpretación de un

mensaje que puede ser actualizado por una tarjeta. Los datos intercambiados están limitados a unos cuantos bytes.

Los diseños para tarjetas sin contacto, indudablemente están evolucionando para poder mantenerse en la aceptación de los usuarios.

Las consideraciones para estos diseños incluyen:

- Distancias y rangos amplios en campos de RF
- Detección de colisiones.
- Velocidades de proceso.
- Seguridad al transmitir datos.

En la actualidad existen tarjetas que son conocidas como *combi cards*, *las cuales* son producidas por varios fabricantes y su importancia radica en la habilidad de integrar ambos tipos de chips para tenerlas en un solo semiconductor.

Capitulo III: Monederos Electrónicos

III.1. Concepto de Monedero Electrónico en Tarjeta Inteligente

Con el fin de entender un poco cómo se realiza una transacción monetaria en especifico, imaginemos a una ama de casa, la cual requiere hacer sus compras normales para mantener su casa limpia, cómoda y con comida. Entonces será necesario que ella salga de compras con el fin de abastecerse de lo necesario para poder cumplir con los requerimientos, arriba citados. En un supermercado ella puede realizar sus compras, después de haber seleccionado y guardado todo aquello que necesita, tomará su bolsa, la abrirá, tomará el dinero que le permita saldar su deuda con el supermercado, en caso de ser necesario recibirá cambio de la encargada de la caja, guardará ese cambio en su bolso y al cerrar éste, podrá tomar sus artículos y salir del supermercado. La transacción la puede realizar con billetes y monedas, así como con una tarjeta de débito y/o crédito que esté afiliada al comercio en cuestión. Ahora bien, en el caso de monedas y billetes, una de las maneras en que ella los pudo haber obtenido fue yendo a un cajero automático o a un banco para hacer un retiro de efectivo, estas acciones actualmente son muy comunes en nuestra sociedad; otra forma común es la de pagar con la tarjeta de debito o de crédito.

Un ME puede realizar una transaccion de este tipo de manera rapida, eficiente y sin tener que visitar alguna institución bancaria o sucursal de la misma, además de que también mejora el uso de una tarjeta de débito o crédito (para compras de montos pequeños) puesto que en el ME se puede cargar una cantidad aproximada de lo que creemos nos pueden costar los articulos que vamos a comprar, ahorrándonos con esto el tener que portar una tarjeta que pueda tener cantidades en miles de pesos dentro de la cuenta de cheques a la cual esté asociada y provocando a los delincuentes a delinquir.

Una forma sencilla de explicar el concepto de ME es realizando algunas preguntas, para las cuales iremos dando su respuesta inmediatamente, y que estarán ligadas unas con otras para comprender mejor la definición y las entidades relacionadas.

¿Qué es un Monedero Electrónico?
El ME es la forma electrónica que se le da al dinero en efectivo y que es almacenado dentro del chip de una Tarjeta Inteligente.

¿Cómo hago uso del dinero almacenado dentro del chip?
Siempre que un tarjetahabiente decida gastar el dinero almacenado en el chip, deberá acudir a terminales especialmente diseñadas para este fin y donde se realizarán los pagos de manera mucho más rápida y eficiente aunado al descuento exacto del precio del producto. Actualmente los supermercados nos ofrecen productos con precios tales como $9.31, pero no existe moneda fraccionaria para pagar el importe de artículos con precios similares, y usualmente el consumidor se ve obligado a pagar una cantidad redondeada (usualmente hacia arriba) que no corresponde al precio real del producto. Con el ME es posible pagar este tipo de cantidades sin que existan complicaciones de tipo alguno

¿A qué se le llama terminal?
Una terminal es un dispositivo electrónico que nos permite leer la tarjeta y realizar cambios sobre ella (lo cual podemos interpretar como las transacciones monetarias en el caso de un ME u operaciones propias de una aplicación especifica). Las terminales son de tres tipos:

a) Terminales de compra

b) Terminales de carga

c) Otras

Las primeras son aquéllas en donde se puede pagar un bien o un servicio; como ejemplos podemos citar a las máquinas expendedoras de refrescos y botanas, o aquellas que se localizan en centros comerciales. Las segundas son aquellas terminales desde las cuales podremos realizar cargas de dinero a nuestro ME y como ejemplos citamos a los cajeros automáticos y los teléfonos públicos. Por último, las que se encuentran en el rubro Otras, son las que dependen de la aplicación en especifico, pudiendo no estar dirigidas al manejo de dinero, sino más bien al manejo de puntos, por ejemplo.

Es importante mencionar que una terminal de carga puede ser a la vez una terminal de compra y esto lo vemos muy claramente ejemplificado con los teléfonos públicos, puesto que a traves de ellos es posible realizar cargas y también se puede realizar el pago de las comunicaciones (llamadas telefónicas).

¿Qué pasa si pierdo mi tarjeta ME?
Como el dinero almacenado dentro del chip es dinero en efectivo, es lo mismo que si perdiera un billete o una moneda al ir caminando por la calle. Por esto, el cuidado de la tarjeta chip es el mismo que debemos de tener con cualquier otro medio de pago.

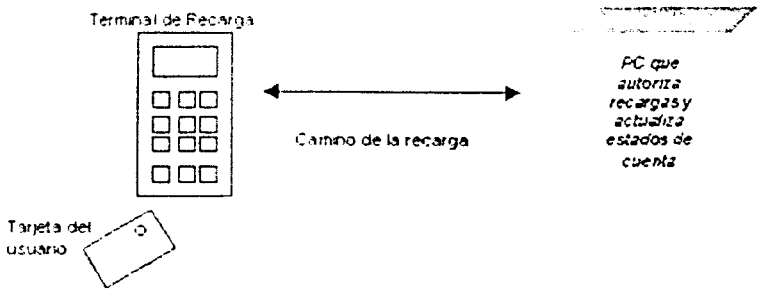
¿Alguien puede disponer del dinero si encuentra la tarjeta?
El dinero que se encuentre almacenado en el chip, podrá ser gastado de manera normal, pero por contar con un Número de Identificación Personal (NIP), no se podrá disponer de más dinero del que se encuentre en ese preciso momento en el chip de la tarjeta, a menos que se divulgue o se conozca el código (NIP) especifico de esa tarjeta.

¿Qué cantidad de dinero puede almacenar mi ME?

Los montos máximos están definidos por el emisor de la aplicación ME y es importante considerar que para evitar que al momento de un robo se pueda disponer de grandes cantidades de efectivo, se establezcan límites que protejan de cierta manera a los tarjetahabientes.

¿Puedo pagar artículos de un valor monetario alto? (podemos entender que alto se refiere a los miles de pesos)
El ME actualmente está encaminado a los pagos de pequeños montos que se refieran a cantidades que no vayan más allá de los cientos de pesos. Aquí es importante mencionar que la mejor alternativa para realizar pagos en miles de pesos, sigue siendo la tarjeta con banda magnética, pudiendo ser de crédito o de débito, aunque de acuerdo con la pregunta anterior, dependerá del emisor de la aplicación el pago de los bienes y servicios.

¿A qué se refiere el concepto de recarga del ME?
Para dejar claro este concepto nos apoyamos en el diagrama siguiente:



Este proceso lo definimos a continuación:

El usuario introduce su tarjeta en una terminal de carga y se le despliega un mensaje para que se introduzca el NIP; validándose este código, se procede a introducir la cantidad a cargar, y para confirmar el monto a cargar, se deberá presionar una tecla aceptando tal monto, con lo cual se establece comunicación con una PC *autorizadora* (la cual está situada en el dibujo anterior, en la parte derecha); como esta PC administra el dinero que tenemos en nuestra cuenta bancaria, se procede a realizar el descuento (sobre la cuenta) del dinero que será ahora cargado al chip. El camino de la recarga es sobre el mismo canal de transmisión y recepción de datos.

Si el proceso es interrumpido en algún momento de la carga, puede que se origine un bloqueo de la tarjeta, dependiendo del momento en el que se retiró la tarjeta o si hubo algún problema.

Cabe mencionar que hay operaciones que son en línea y otras fuera de línea; las primeras se refieren al hecho de que se requiere establecer una comunicación directa (a través de un cable de red, una línea telefónica o microondas, entre otros) entre la terminal y un *Host* (PC que autoriza recargas de dinero o de vales, por ejemplo), para realizar ciertas transacciones. Las segundas, sólo se hacen a nivel local, es decir, dentro de la terminal. Podemos citar como ejemplos de las transacciones en línea a la recarga y a las que son fuera de línea, a la compra o pago de comunicaciones.

¿A qué se refiere el hecho de bloquear una tarjeta?
Esta actividad se presenta al momento de introducir erróneamente el NIP de la tarjeta, en el instante en que se interrumpe un proceso de recarga, o por diversas condiciones de mal estado de cuenta del cliente.

¿Cómo se desbloquea la tarjeta?

Para dejar una vez más funcional la tarjeta deberá ser introducida nuevamente para que se realice el desbloqueo de la misma; este es un proceso inmediato para evitar que el usuario tenga que preocuparse por realizar una operación más. El bloqueo de una tarjeta también puede ser provocado por la introducción incorrecta y sucesiva del NIP (como se mencionó anteriormente), para este caso, la terminal no realiza un desbloqueo, puesto que se supone pudo haber sido robada y por esta razón se bloquea su uso para realizar recargas y compras; la única manera de desbloquear esta tarjeta es contactando al proveedor de la misma, pudiendo ser éste el banco emisor de la aplicación.

Todo tipo de bloqueo de tarjetas se puede identificar muy claramente en un archivo contenido dentro de la tarjeta, y los podemos identificar al analizar los bits que se han encendido en dicho campo.

El campo que contiene los bits que controlan los bloqueos, es identificado y procesado por las terminales desde que los primeros instantes en que la tarjeta es energizada.

¿Si pierdo mi NIP, es posible recuperarlo?
Los atributos de los archivos almacenados en la tarjeta son muy variados, existen algunos sobre los que es posible realizar cambios o leerlos; para los archivos que contengan un NIP, se dan atributos de Nunca Lectura, con el fin de ofrecer seguridad al tarjetahabiente, por lo cual no es posible recuperarlo.

¿Qué beneficios obtengo al hacer uso de una tarjeta ME?
En primera instancia podemos ver que las transacciones son mucho más rápidas y que se pueden realizar con el importe exacto; si esto lo sumamos a la posibilidad de que en una sola tarjeta con chip, se pueden manejar más aplicaciones, obtenemos un valor agregado a nuestra tarjeta.

¿Sólo puedo realizar pagos con el ME si además mi tarjeta cuenta con banda magnética?
Por el lado del tarjetahabiente: si una tarjeta con chip además cuenta con la banda magnética, nos permitirá entonces tener un rango más amplio en cuanto a formas de pago se refiere.

Por el lado del comerciante: bajo la premisa de tener chip y banda magnética, se le ofrece la posibilidad de prestar un mejor servicio a sus clientes puesto que su dinero lo pueden manejar a su entera satisfacción personal.

En este rubro es importante mencionar que el emisor de la aplicación ME es quien decide, a su libre arbitrio, si una tarjeta combinará el chip con la banda magnética o no.

A últimas fechas, se ha venido desarrollando un concepto a escala internacional, en la que se observa la migración paulatina, que tendrá que ser total a mediano plazo (5 a 7 años) de las tarjetas que cuentan con banda magnética y con chip en la misma tarjeta, para erradicar por completo la banda y tener todo los controles, campos y aplicaciones en el chip.

Por último, ¿mi tarjeta ME sólo me sirve para realizar consumos?
Una Tarjeta Inteligente, por su capacidad multiaplicativa, puede contener más de una aplicación dentro de su chip, pudiendo convivir con diferentes aplicaciones que no tengan que ver con dinero electrónico (caso de la aplicación de Lealtad).

Cabe aclarar que una Tarjeta Inteligente no requiere forzosamente contar con la aplicación de ME.

De todas estas preguntas y respuestas podemos resumir lo siguiente:

Una tarjeta con aplicación ME es aquella que posee un chip (el cual cuenta con un microprocesador con sistema operativo y memoria propia), capaz de manejar dinero en efectivo (que puede ser considerado como virtual), y que nos permite realizar compras y cargas por medio del chip y de terminales especiales capaces de manejar dinero electrónico; nos ofrece rapidez en las transacciones, confiabilidad y la oportunidad de tener otra forma alternativa de pago.

A continuación se hace referencia a requerimientos necesarios para que una aplicación ME, sea eficaz.

a) Requerimientos para interfase con el usuario

NIP

- Se pretende que el usuario de la tarjeta tenga un número de intentos de NIP (de las siglas Número de Identificación Personal) determinado, y que para ingresar este número en la terminal, se cuente con un teclado que incluya todos los dígitos (en nuestro sistema numérico) para poder *digitar* su código personal. Al presionar cada tecla, no debe de emitirse un sonido característico a cada número, y en el display de la terminal se debe ver cada número ingresado como un asterisco, por ejemplo, como en la actualidad lo hace un cajero automático.

- Si el usuario ingreso mal su NIP, debe tener la posibilidad de ingresarlo nuevamente y se le debe de informar cuantos intentos le quedan aún.

Interfase de usuario

- El tarjetahabiente siempre debe tener acceso a la consulta de su saldo en el ME (chip).

- Se le puede de dar la opción de abortar una operación de recarga sin tener que retirar su tarjeta del lector de la terminal.
- Y finalmente, el usuario debe de ser informado sobre el éxito o fracaso de su operación de recarga; para el segundo caso, se le debe desplegar mensajería correspondiente al por qué de su fracaso.

Mensajería

- Los mensajes que son desplegados, deben corresponder siempre a la acción que se está llevando a cabo en ese momento, deben ser breve (esto por la limitante de los caracteres que soporta una pantalla en especifico) pero suficiente para que el usuario esté debidamente informado.

- Pueden ser desplegados en otros idiomas, como es el caso de los teléfonos públicos.

Divisa

- El monto de la carga debe estar siempre expresado en la divisa del monedero.

b) Requerimientos para la terminal

Seguridad

- La terminal debe de :

  Manejar correctamente los parámetros del ME

Tratar los problemas que se presenten durante una operación con falla.

Obtener los certificados de autenticación sobre los resultados en operaciones de crédito.

Cumplir con los estándares

Requerimientos de hardware

- El display debe ser lo suficientemente capaz de desplegar una cantidad determinada de caracteres para informar al usuario sobre el estado de su transacción.

- Lector de la terminal. Este lector debe ser capaz de aceptar Tarjetas Inteligentes y soportar los protocolos de comunicación.

- En caso de tener impresora, ésta debe de tener un número mínimo de líneas de impresión, donde se pueden adicionar datos como:
  Logotipo de la empresa.
  Monto de la transacción.

- El *buzzer* es el mecanismo emisor de sonidos que son característicos a cierta operación y que identifican a cada una de las mismas, tal es el caso de inicio o fin de transacción, o la introducción del NIP.

III.2. Panorama internacional

Las tarjetas chip se usan a lo largo y ancho de todo el globo terráqueo y su uso va de lo más simple a lo más complejo y sus aplicaciones sólo se verían limitadas por la imaginación.

En algunos países son usadas para el pago de comunicaciones a través de teléfonos públicos, como es el caso de Francia y México (cabe señalar de manera muy importante, que México –según encuestas revisadas del año de 1999 - es el país donde hay un mayor consumo de tarjetas chip que en el resto del mundo, y es ésta una de las razonas por las cuales se decidió implantar el ME en nuestro país), en otros países son usadas para pagar servicios como la gasolina, en este rubro México también está emplazado; y en otros más - hablando ya de tarjetas que cuentan con un chip con un microprocesador y no uno de memoria como en los casos anteriores – son usadas para pagar bienes, servicios y/o comunicaciones. Este último caso es el que nos ocupa para el desarrollo de esta tesis.

Los países que van a la vanguardia en la tecnología de tarjetas con chip con microprocesador son: Francia, Bélgica y E. E. U. U., principalmente, siendo diseñadores de aplicaciones, chips, terminales y sistemas de supervisión; como usuarios masivos están: México - quién se espera tenga (a corto plazo) el mercado más grande en el ámbito internacional -, Bélgica, Francia, Holanda; y se encuentran los usuarios a menor escala como: Países Bajos, Chile, Canadá, Argentina, Australia, España, que cuentan con programas piloto para comenzar a explotar la tecnología en cuestión.

Es fácil imaginar que integrar cualquier tecnología a la sociedad, a escala masiva, es bastante complicado y requiere de tiempo, debido a factores económicos, sociales, políticos y culturales, principalmente; ahora bien, para el caso que nos ocupa, el cambio que se está dando también conlleva sus

implicaciones, puesto que toca todos los ámbitos de la sociedad, ya que todos manejamos dinero, en mayor o menor escala, pero todos estamos involucrados; por esto, para dar ese cambio hay que implantar lugares (ya sea ciudades o centros comerciales, por ejemplo) piloto para dar a conocer el producto, sus alcances, beneficios y restricciones, conocer fallas y resolverlas, evolucionar y mantener en condiciones óptimas la plataforma tecnológica sobre la cual estemos trabajando.

Como dato interesante podemos remitirnos al proyecto del cambio de moneda que se ha venido manifestando en el viejo continente y que aún no se ha conseguido en su totalidad.

Actualmente no hay un solo país en todo el mundo en el que la difusión de este avance en el campo de la información y la electrónica haya sido extensivo a toda su población, pero se prevee que una década sea suficiente para dar un salto agigantado en el conocimiento, uso y manejo de la tecnología que envuelve el campo de las Tarjetas Inteligentes.

III.3. Monedero Electrónico Mexicano

El ME mexicano, entro en funcionamiento a finales de la década de los 90 con programas piloto en diferentes partes de la República; no se restringió a que una sola empresa lo introdujera bajo la tecnología de un solo proveedor, sino que fue implementada en diferentes lugares y con diferentes proveedores, lo cual nos obliga a tener que pensar en la interoperabilidad que es un tema que será tratado más adelante, en otro capítulo de esta tesis. A pesar de lo anterior, el desarrollo no se ha visto obstaculizado.

La idea del ME nace de la necesidad de ofrecer a los tarjetahabientes otra forma alternativa de pago, y comienza su implantación en algunas plazas

comerciales dentro del país, en donde los negocios que estuvieron dispuestos a formar parte del proyecto recibieron una terminal de compra, la cual está situada a un lado de su caja registradora y de las terminales que soportan el pago de artículos mediante el uso de tarjetas con banda magnética.

Es posible que nos hagamos la pregunta siguiente: ¿quién debe pagar la terminal de compra, el negocio o el emisor de la aplicación del ME?

Pues bien, al igual que las cajas registradoras o los pin pads (terminales para banda magnética) las terminales de compra deben ser adquiridas por el comercio, de acuerdo con contratos previamente establecidos, aunque para un programa piloto, en el cual los comercios aún no están convencidos de los beneficios que esto les puede representar, es posible que el precio de las terminales sea absorbido en un principio por el emisor de la aplicación, para posteriormente negociar con los mercaderes sobre la posición económica final de la terminal.

Con las terminales en los comercios, obviamente surge la necesidad de tener clientes que vayan a hacer uso de las mismas, es por esto, que a un núcleo reducido de personas se les otorga una tarjeta con la cual van a tener la posibilidad de realizar compras en los comercios afiliados.

Con tarjetas, terminales de recarga y puntos de venta instalados y repartidos en el campo, se aterriza el proyecto como un piloto, que permite analizar, modificar y actualizar todos los entes relacionados con el concepto, según las necesidades y las evoluciones.

La forma en como se implementan las tecnologías, sea cual fuere el ramo, dependen de las regiones geográficas, económicas, políticas, culturales, etc. Para el caso del tema que nos ocupa, los aspectos económicos y los culturales nos preocupan en extremo.

La razón del comentario anterior se refiere a lo siguiente: México (el cual está considerado como un país en vías de desarrollo, apelativo que suena más alentador que el de tercermundista) se encuentra en una posición en la que el poder adquisitivo de su moneda se encuentra deteriorado desde hace algunos años y requiere que las formas de pago, entre otros rubros, sean eficientes, que no le causen molestias, sean accesibles al común de la gente, solucione problemas de pérdidas de tiempo, modernicen su infraestructura y sean atractivas para comerciantes y consumidores. Por el lado cultural podemos hacer referencia a que un cambio como el propuesto por las Tarjetas Inteligentes conlleva una educación general a la población que tenga contacto con esta tecnología, dado que la ideología de muchas personas, según hemos podido apreciar en estos últimos tres años, no permite que exista un avance a gran escala.

Una vez que éstos y otros inconvenientes que pudieran surgir de aquí en lo futuro, la explotación será cada vez mayor; el cambio es inminente, pero requiere más que nada el factor tiempo.

III.4. La telefonía en el ambiente del Monedero Electrónico

Para hacer uso de un ME es necesario contar con dispositivos que nos permitan realizar cargas de dinero electrónico al chip y, en consecuencia, también se requieren dispositivos donde podamos gastar ese dinero almacenado en el chip.

Un teléfono es un dispositivo de carga y compra bastante amigable para cumplir con estos dos requisitos, debido a que es posible a través del mismo cargar el dinero suficiente y necesario para realizar el pago de comunicaciones en el mismo teléfono público.

El teléfono público es conocido dentro del entorno del ME como una terminal inteligente, ya que puede procesar información y/o debitar unidades de una tarjeta, ya sea de memoria o de microprocesador.

Si reunimos la ventaja que se describió (terminal inteligente), junto al hecho de que en México hay teléfonos públicos en casi cualquier dirección a donde volteemos la vista (hablando en sentido figurado), entonces podemos contar con una infraestructura bastante poderosa por medio de la cual haremos uso de un ME.

Actualmente otros países están desarrollando su telefonía para poder aceptar tarjetas con microprocesador para así poder ir eliminando con el paso del tiempo las tarjetas de memoria y las monedas por diversas razones, las cuales describimos a continuación. Dentro de los países que se encuentran a la vanguardia tecnológica encontramos a Francia. Este país ha tenido un gran desarrollo en este sentido desde la década de los *80's*, el crecimiento en dicha industria ha podido rebasar sus fronteras y ha llegado a varios países entre los que podemos contar a México como uno de los principales.

Las monedas han ido extinguiendo su uso para pagar el servicio de comunicaciones debido a los altos costos que le representan a las empresas telefónicas: el mantenimiento del aparato, puesto que es necesario limpiar los aceptadores de monedas que se van dañando día con día, es necesario contratar gente que se dedique a la recolección, varias veces al día, de las monedas almacenadas en las alcancías del teléfono. Otra de las causas principales es el vandalismo, que es la acción malintencionada que se ejerce sobre los teléfonos públicos, con el fin de ponerlos fuera de servicio. Esta actividad delictiva representa en un mayor número, el motivo de falla de los dispositivos. El rayado de los *displays* también se emplaza como una actividad importante de delincuencia.

Las tarjetas de memoria son un asunto diferente. Existen muchas más ventajas para usuarios y empresarios en el manejo de estas tarjetas con respecto a las monedas.

Primero hablemos del usuario. Éste recibe el beneficio de contar con un plan de venta de tarjetas bastante extensivo a todo lo largo de un territorio donde haya teléfonos públicos, para que no le sea difícil conseguir una tarjeta telefónica; por otro lado, como las tarjetas tienen diferentes imágenes en la parte delantera de la misma, los coleccionistas se ven beneficiados, claro, es el menor de los beneficios, pero es bueno hacer notar este tópico.

Para el empresario, el beneficio es mucho mayor puesto que va a poder tener un control más específico por lotes de tarjetas, como es un concepto de prepago, podrá tener un flotante del dinero que aún no se haya usado para pagar las comunicaciones de los usuarios, siendo éste tal vez el mayor de sus beneficios; las tarjetas usualmente llevan propaganda de productos ajenos a los emisores de la tarjeta, y este *servicio* permite abatir los costos de las tarjetas y recibir un ingreso extra por la misma propaganda

He querido recurrir a estadísticas internacionales sobre el uso de tarjetas de memoria, y de las cifras encontradas se puede observar que en el año 2000 México se encontró colocado como el primer país (en todo el mundo) consumidor de tarjetas con casi un 20 % del total mundial. Esto es un indicador del nivel de aceptación que se tiene en nuestro país hacia el uso de las tarjetas de memoria.

Debido a la evolución en la forma de realizar el pago de las comunicaciones en los teléfonos públicos y a la aceptación de las tarjetas en nuestro país, se ha desarrollado el concepto de ME dentro de las empresas telefónicas, tanto nacional como internacional.

Este es un tema por demás interesante e innovador, lleno de ingeniería y con tecnología de punta, que se encuentra a la vanguardia en todo momento.

Ya entrados en el tema de la telefonía y el ME, hablemos sobre beneficios para usuarios y empresarios al igual que como lo hicimos con las tarjetas de memoria.

El usuario es beneficiado ampliamente puesto que recibe otra forma alternativa para el pago de sus comunicaciones, ahora puede pagar con tarjetas de memoria y también con tarjetas chip con microprocesador (que es lo que nos ocupa en esta tesis). Es importante mencionar que últimamente se han instalado teléfonos públicos como en antaño, que aceptan las monedas como forma de pago. Debido a que es una tarjeta que puede ser recargable, se le da al usuario la libertad de tener el dinero que él juzgue suficiente o necesario para realizar sus comunicaciones; tiene la misma capacidad de realizar llamadas locales, nacionales y/o internacionales. No tiene que recurrir a un supermercado o una pequeña tienda para comprar una tarjeta cada vez que su crédito se agote o sea insuficiente, ya que podrá recargar la tarjeta cuando el propio usuario lo requiera y con la cantidad que le plazca (hasta ciertos límites, por seguridad del tarjetahabiente, definidos por el emisor de la aplicación). Por ser una tarjeta que puede manejar varias aplicaciones dentro de un mismo chip, no verá limitado el uso de la tarjeta al momento de llamar y/o de recargarla, sino que tendrá un mundo virtual mucho más amplio y amigable, pero esto será más ampliamente explicado en el capítulo de *Multiaplicaciones* del presente trabajo

Ahora, hablando del empresario podemos citar también cuantiosos beneficios, entre los que podemos contabilizar, en un principio, los siguientes: publicidad a través de sus tarjetas, abatimiento de costos por emisión de tarjetas, ya que una sola tarjeta puede tener una vida útil de unos dos años, distribución de las

mismas, mejor control del dinero recargado y gastado por y con el uso de las tarjetas, mejor calidad en el servicio.

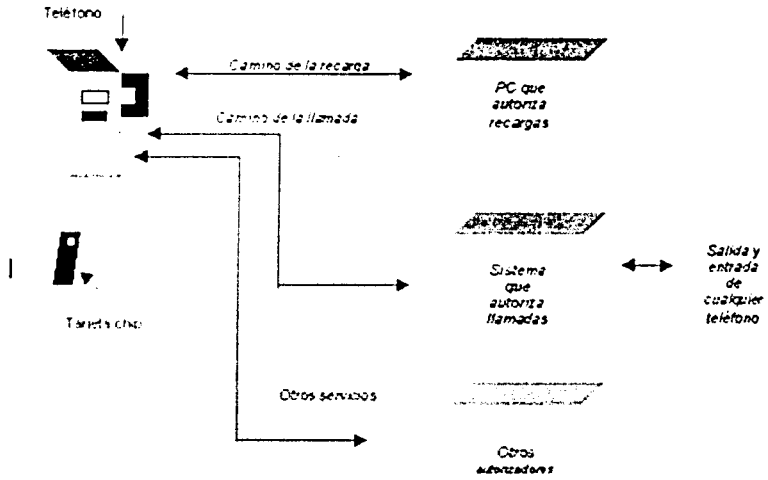
Si pudiéramos echar un pequeño vistazo a los costos que realizan las empresas al momento de vender, comprar, distribuir, almacenar, etcétera, tarjetas de memoria, nos daríamos cuenta de que el costo/beneficio será mucho mayor si nos vamos por el uso de las tarjetas chip con microprocesador.

Hasta el momento sólo hemos hablado de las ventajas de unas tarjetas sobre otras, pero ahora hemos alcanzado el punto preciso para contestar a varias preguntas que nos podemos formular.

El concepto de telefonía manejada con tarjeta chip, siendo la primera tarjeta usada una de memoria y no de microprocesador, nace de la necesidad de disminuir costos y mejorar el servicio, adicionándose la imperiosa urgencia de llevar un control mucho más eficiente (desde el punto de vista del proveedor del servicio de las empresas telefónicas) sobre el pago de las comunicaciones, el tráfico de las mismas así como sus orígenes y destinos. Este desarrollo se ha venido dando en México desde hace más de una década, pero todo tiene evoluciones. La evolución que se le dio fue el uso de las tarjetas inteligentes con aplicación ME dentro del chip y que actualmente se encuentra funcionando de manera real pero limitada a un pequeño núcleo de personas, por el hecho de que todo comienza con poco y sobre la base de las posibles evoluciones.

Primeramente mostramos un posible sistema de telefonía, grosso modo, mediante cajas negras para hacer del conocimiento del lector cómo es que se establecen las comunicaciones para realizar llamadas o recargas con la tarjeta chip.

Por cuestiones de confidencialidad no se tocarán los puntos muy a detalle, pero si trataremos de dar la explicación suficiente y necesaria para que cualquier persona pueda consultar este tema.



Ahora explicamos los caminos y las entidades arriba mostradas.

El teléfono es el medio por el cual podemos realizar llamadas y cargas con ME, además de permitirnos consultas y transacciones referentes a otros servicios; está provisto de un display que nos permite darle una interfase al usuario, un

teclado, auricular, y un lector de tarjetas chip (de memoria o de microprocesador).

Por otro lado está la tarjeta chip, que para nuestro caso es una tarjeta con microprocesador, y es en ésta, donde tenemos personalizada la aplicación ME.

La personalización de la tarjeta se refiere a la acción eléctrica electrónica de escribir sobre la memoria del chip, la información necesaria para llevar a cabo una u otra aplicación, y que contendrá datos genéricos por aplicación y datos propios por tarjetahabiente.

Las cajas negras nos indican los servidores o *PC's* que administran y/o autorizan las diferentes transacciones que efectuemos en el teléfono. El caso de la *PC que autoriza recargas* es una máquina de grandes proporciones físicas, además de almacenamiento y procesamiento de datos (siendo éstas sus cualidades primordiales) y que posee la información que nos indica si una tarjeta puede ser recargada o no, también nos indica si la tarjeta está en algún estado incorrecto (debido a fraude o a mal uso de la misma) y nos proporciona información sobre si la tarjeta debe de ser bloqueada para evitar que siga siendo usada; nos indica además, en caso de ser necesario, la actualización de información en algunos registros contenidos en el chip de la tarjeta.

El *sistema autorizador de llamadas* es en general un sistema muy complejo y requiere de una tesis especializada para poder describir todos sus actores; pero podemos decir que está compuesta por *cajas negras* que conectan los teléfonos públicos, y son estas *cajas* las que guardan dentro de *módulos especiales* (que también cuentan con chips de seguridad) el dinero de las transacciones realizadas en los teléfonos públicos.

Los *otros autorizadores* están definidos por los dueños de una aplicación en particular y están sujetos a cambios y evoluciones como cualquier otro sistema;

en general, contienen bases de datos y pueden realizar cálculos estadísticos que les permiten saber si su propuesta de aplicación es bien aceptada o no por los usuarios.

Las *cajas negras*, a las que acabamos de hacer referencia, son dispositivos electrónicos que permiten operaciones mediante el uso de los teléfonos; guardan dentro de si los registros en los que se contempla información sobre una comunicación o sobre una recarga; esta información es procesada y permite obtener las estadísticas de flujos de comunicación, flujos de recargas, averías en los teléfonos o fallas en las comunicaciones. En este dispositivo se encuentran los chips de seguridad, los cuales almacenan dentro de ciertas localidades de memoria (del mismo chip) el dinero virtual, producto del uso de tarjetas con aplicación ME. Estos chips forman parte importante del entorno ME, ya que se encuentran los dispositivos arriba mencionados, o en cualquier terminal que acepte Tarjetas Inteligentes.

El aspecto físico de tales chips es muy parecido a los de las tarjetas con microprocesador, pero cuentan con un sistema operativo propio, diferentes tamaños de memoria y, obviamente, diferentes archivos, que procesan las transacciones.

Este tema también es bastante extenso y no es tratado en esta tesis.

Capítulo IV: Multiaplicaciones

IV.1. Concepto general

El concepto de multiaplicaciones se refiere al hecho de que en una sola tarjeta se puedan tener incluidas varias aplicaciones, incluyendo o no, el ME.

Ahora bien, una aplicación puede ser definida como el conjunto de datos que se enfocan a un mismo fin, y que serán procesados tanto por terminales como por la misma tarjeta para ejecutar una tarea especifica. Para entender mejor el concepto, hagamos la siguiente analogia con una PC de escritorio:

Una PC de escritorio posee una carcaza (plástico en la tarjeta), un disco duro (el chip), un sistema operativo residente en el CPU de la máquina (sistema operativo propio del microprocesador) y programas que tienen diferentes usos, como diseño por computadora o software de audio y video, entre otras (aplicaciones en el chip como las que nombramos en lo sucesivo de este capítulo).

Por lo anterior, el uso de la Tarjeta Inteligente no debe ser limitado a una forma de pago únicamente, ya que nos permite incluirle diversas aplicaciones, las cuales nos permiten abarcar un mercado más amplio. Como ejemplos de aplicaciones tenemos las siguientes: Lealtad, Control de Acceso, Identificación Personal, Viajes, es importante mencionar que no son las únicas aplicaciones, la creación de nuevas dependerá de aquel mercado que desee cubrir un comerciante. En el siguiente tema (*Esquemas*), describimos estas aplicaciones.

IV.2. Esquemas

Los esquemas (en al ámbito de las Tarjetas Inteligentes), son aquellos que están dirigidos a resolver y/o facilitar una necesidad que tengamos en nuestra vida diaria. Están conformados por la aplicación, la tecnología, la solución y la infraestructura general de la necesidad a resolver.

Como acabamos de ver, un esquema puede llegar a ser tan grande como se requiera, por esto, sólo nos enfocaremos a la parte que nos interesa de ellos: las aplicaciones en la tarjeta, las cuales explicamos a continuación.

La aplicación Lealtad se emplea en aquellos comercios que obsequian artículos a los clientes que hayan llegado a completar *puntos* por una cantidad de compras considerable y de acuerdo con ciertas reglas determinadas por el mismo comercio. Este tipo de aplicación se puede extender a supermercados, plazas donde exista comida rápida (o del inglés *fastfood*), tiendas de discos, donde es posible realizar compras frecuentemente.

Desde hace mucho tiempo, el Control de Acceso se ha venido dando como una necesidad de las empresas para controlar los horarios de entrada y de salida de los empleados, para permitir el acceso a personas autorizadas a un área determinada del edificio (como un *site* de computadoras), y la Tarjeta Inteligente permite hacer más eficientes estos controles, puesto que se puede proveer de un NIP a cada empleado, restringiendo su paso a diferentes estancias. Como estará interactuando la tarjeta con terminales y un sistema de base datos, se pueden tener estadísticas muy precisas de cada empleado, sobre su estadía en cierto edificio de la corporación.

Como Identificación Personal, esta aplicación nos permite almacenar dentro de la tarjeta diversos datos del portador de la tarjeta; puede haber datos oficiales como el RFC (Registro Federal de Causantes), el CURP (Clave Única de

Registro Poblacional) o la Clave del IMSS, y datos personales como Tipo de Sangre o Fecha de Nacimiento, entre otros muchos más.

Un campo seguro para explotar el uso de la Tarjeta Inteligente es el del Viajero Constante; si hablamos del caso de los viajes a través de aerolíneas, es muy benéfico proporcionar una Tarjeta Inteligente a los pasajeros que utilizan este medio para desplazarse de un lugar a otro con fines de negocio o particulares, y obsequiarles kilómetros o millas (según sea el caso) para amortizarles costos en futuros viajes. Tal vez suene un poco parecida esta aplicación a la de Lealtad, pero en la primera se suman puntos únicamente y no existen descuentos y en ésta se suman los kilometros y/o millas (equivalentes a los puntos) y se ofrecen, además, descuentos al pagar boletos con el uso del ME.

Como nos podemos dar cuenta, las aplicaciones pueden tomarse en forma independiente y su alcance es bastante amplio, pero si combinamos una aplicación cualquiera con el ME, podremos tener una tarjeta realmente poderosa y eficaz.

Una aplicación de particular interes es la relacionada con el transporte masivo de pasajeros a través del servicio del metro y camiones; cabe hacer un paréntesis para explicar y resaltar este concepto.

El concepto de Tarjetas Sin Contacto es de gran importancia al hablar de aplicaciones que requieren una gran rapidez al momento de realizar una transacción. Si compramos una revista o un mueble en una tienda de autoservicio, la relevancia del tiempo al efectuar el pago del articulo no es realmente importante, a juicio del autor, es posible que sea soportable hacer un pago en un minuto con cualquier medio de pago, ya sean tarjetas con banda, dinero en efectivo y/o tarjetas con chip. Sin embargo, si nos encontramos en una estación del metro o esperamos abordar un camión para trasladarnos hacia nuestro destino, un minuto es demasiado tiempo para realizar el pago

correspondiente a nuestro viaje, y esto es un factor que deteriora el servicio de transporte. Ésta es una razón lo bastante fuerte y convincente para evolucionar la forma en como se realiza el cobro en los transportes públicos y cambiar hacia una Tarjeta Sin Contacto, la cual puede realizar transacciones en milésimas de segundo y que requiere una terminal en la cual no se debe de introducir la tarjeta para que se realice la operación.

IV.3. Estructuras

Para este tema, nos enfocaremos a describir breve y únicamente, la estructura de las Tarjetas Inteligentes con Contacto.

Dentro de las Tarjetas Inteligentes existen los niveles y las estructuras.

Los niveles hacen referencia de donde han sido grabados los archivos; es decir, si están a nivel Raíz de la tarjeta o a niveles de Aplicación o Subaplicación.

Las estructuras de los archivos son las siguientes:

Archivo dedicado: Estos archivos son aquellos que nos sirven para delimitar aplicaciones. Hay tantos archivos dedicados como aplicaciones tenga la tarjeta.

Archivo de trabajo: Dentro de estos archivos se almacenan los datos propios de cada aplicación. De acuerdo con el ejemplo que observaremos en el tema siguiente, los campos que hemos considerado están dentro de este tipo de archivo.

Archivo público: Estos archivos sirven para identificar y almacenar información referente al número de serie de la tarjeta.

Archivo secreto: Aquí podemos encontrar los archivos que contemplan las "claves" (ver tema: *Ejemplo*) para poder acceder a otros archivos. Son importantes ya que se les requiere para poder realizar autenticaciones (que significa verificación de autenticidad) de las aplicaciones, tomando en cuenta las tarjetas y las terminales.

Ahora bien, todas las estructuras de archivo, en cualquier nivel, constan de un encabezado y de un cuerpo.

El encabezado es aquel que permite identificar al tipo de archivo (en su nivel y en su estructura). Por poseer un campo para definir su identificador, nos permite realizar diferentes operaciones con el archivo en cuestión, tal como lectura, escritura y/o borrado.

El cuerpo del archivo es aquel que almacena el contenido del archivo, para el ejemplo que desarrollaremos, los campos Id_Cliente, Puntaje y Fecha_expiración corresponden al cuerpo de un archivo de trabajo.

IV.4. Ejemplo

Hemos alcanzado un tema importante y muy explicativo, donde desarrollamos cuál puede ser el procedimiento para implantar una aplicación dentro de la tarjeta de microprocesador. Nos enfocamos ampliamente al desarrollo interno de la tarjeta pero no nos desviamos mucho con lo que son terminales ni con PC's administradoras de aplicaciones.

Es importante considerar que en la vida real una aplicación puede llegar a contemplar evoluciones que permitan un mejor rendimiento o una extensión

para lo que en un principio fue concebida; para nuestro caso planteamos una necesidad y sobre ésta nos enfocamos durante todo el desarrollo.

Primeramente planteamos la siguiente necesidad qué queremos resolver mediante el uso de una tarjeta inteligente:

"Usualmente, las grandes tiendas, con el fin de captar más clientela o conservar a la que tienen, ofrecen *ganar puntos* que serán acumulables para obtener productos gratuitos después de haber realizado una compra (o varias), para la cual se ha establecido un monto mínimo, conduciendo de una manera muy sutil, a la compra de artículos que ofrece la tienda".

La explicación anterior hace referencia a la "lealtad" que se le tiene a la tienda y que tomamos como nuestra aplicación

Pero, ¿cómo podríamos implantar una aplicación de Lealtad en una tarjeta? es muy sencillo y ahora empezamos a dictar las reglas para nuestro producto:

"Pensemos en que somos los dueños de una gran cadena de supermercados y que sabemos que el poner de oferta productos nos hará vender más rápido de lo que siempre lo hemos hecho. La gente entonces acudirá a nuestras diferentes sucursales en busca de sus artículos además de ir con el fin de aprovechar los descuentos que ofrendamos. Si a todo esto le añadimos que como un valor agregado (o "plus" como también es conocido) al consumidor, después de haber realizado sus compras y el total de éstas alcancen (en ese día) un mínimo definido por nosotros mismos, les regalamos puntos que al momento de sumarlos les permitan obtener descuentos en su siguiente compra, entonces el cliente volverá con nosotros y nosotros podremos tener mejores ventas."

Ahora la pregunta es: ¿cómo tener un esquema de Lealtad dentro de una tarjeta con microprocesador? ; es este el momento de aplicar la ingeniería:

a) Todo desarrollo de una aplicación se basa en contemplar el tipo de tecnología que se quiere implantar y hemos decidido que usaremos una Tarjeta Con Contacto, puesto que no requerimos tiempos muy pequeños para ejecutar nuestra aplicación de Lealtad; por usar la tarjeta con contacto nos vemos beneficiados en el dinero que debemos invertir para la emisión de las tarjetas, puesto que una tarjeta sin contacto es más cara, comparada con la que hemos seleccionado.

b) Ahora debemos pensar que tipo de información requerimos para la tarjeta, con lo cual podemos definir el tamaño de los campos que contengan esta información.

Supongamos que lo que queremos incluir es lo siguiente:

Nombre del Campo	**Tamaño en bytes**	**Definición del campo**
Id_Cliente	4 bytes	Número que identifica al cliente, de manera única, con la tienda.
Puntaje	2 bytes	Total de puntos acumulados por las compras del cliente en la tienda.
Fecha_expiración	3 bytes	Fecha en la que expira el total de puntos acumulado sobre los clientes de la tienda.
	9 bytes	

Id_cliente: Este campo es incluido para poder darle números (que pueden ser consecutivos, ya sea en formato decimal o hexadecimal) a nuestros clientes, con el fin de tener un control perfecto sobre la

información que nos sea de utilidad, tal como domicilio o número de teléfono (información que no la tendremos en el chip, por razones obvias de espacio, pero si en una base de datos, a la cual sólo nosotros, como comercio, tendremos acceso).

Puntaje: Este campo se irá incrementando a medida que se vayan realizando compras y se obtenga lo necesario para sumarse un punto o varios, a nuestra tarjeta. La forma en cómo se irá modificando este campo es bit a bit; la terminal será la encargada de traducir el total de puntos (bits en la tarjeta) a una forma fácil de interpretar (decimal) para el comerciante y el cliente.

Fecha_expiración: En este campo incluiremos la fecha en la que la aplicación dejará de ser válida, por cuestiones de control y prevención de fraudes.

Es importante que para el campo "Fecha_expiración", se decida el orden que se tomará para los días, los años y los meses, para evitar errores al momento de interpretar fechas. Para nuestro caso el formato de este campo es *ddmmaa*.

Ahora bien, si la tienda tuviera más de una sucursal, se podría pensar en especificar un nuevo campo para identificar el lugar donde se han realizado las compras, con fines de poder obtener datos estadísticos.

De acuerdo con el comentario anterior se puede deducir fácilmente que la aplicación puede llegar a contemplar evoluciones en su diseño y en su funcionamiento, es por esta razón que la definición de los campos debe considerar estos cambios; el espacio reservado para la aplicación también es un factor fundamental para las mejoras a posteriori, ya que la memoria dentro del chip, es limitada.

La disposición de bytes dentro de la memoria del chip, está dada en un mapa de memoria que se puede apreciar como el siguiente:

1 byte	1 byte	1 byte	1 byte
1 byte	1 byte	1 byte	1 byte

Sabemos que:

	Valores	Equivalencia
Bit	0 ó1	
Byte	00 → FF	8 bits = 1 Byte
Word	00 00 → FF FF	1 *word* = 4 Bytes

Es decir que si tenemos 9 bytes, esto nos da un total de 2 *words* y 1 byte, los cuales los podemos tener en un arreglo como el siguiente.

Byte 1	Byte 2	Byte3	Byte 4
Id_Cliente			
Fecha_expiracion			Puntaje
Puntaje	*Futura evolución*	*Futura evolución*	*Futura evolución*

Los 3 bytes con el nombre "Futura evolución" los podemos reservar por si se requiere adición de un campo totalmente nuevo.

Es importante saber la posición exacta de cada uno de los campos y el identificador del archivo que contiene dichos campos en cuestión para cualquier aplicación, puesto que la selección de cada campo puede corresponder a archivos diferentes.

c) Con los campos especificados y la disposición de cada uno de ellos dentro del mapa de memoria de la tarjeta, debemos ahora especificar las condiciones de acceso al archivo.

Para enfrentar este punto, hablaremos ahora de las "claves en las tarjetas".

Estas "claves" son aquellas que nos permiten tener cierto tipo de acceso a los archivos en las tarjetas. Estos accesos pueden (y en ocasiones deben) estar limitados con el fin de evitar manipulaciones malintencionadas en la tarjeta.

Los tipos de accesos a que nos referimos: son lectura, borrado y escritura.

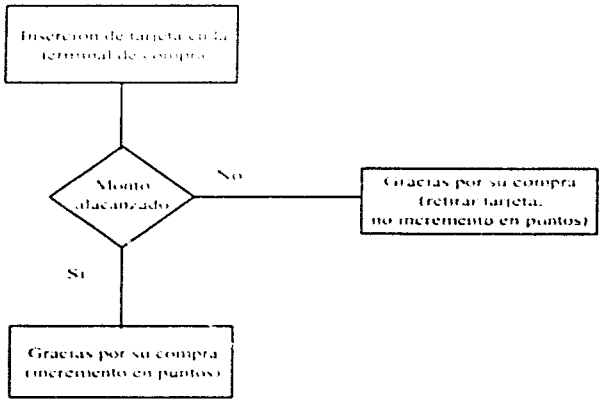
En el de lectura se observa la cualidad de poder leer libremente sobre un archivo de la tarjeta. Con el borrado se consigue eliminar la información que se encuentra en un momento dado en un archivo de la tarjeta. Mientras que con la escritura podemos añadir información a los archivos en la tarjeta.

Para nuestro caso, daremos las condiciones de lectura, borrado y modificación "Prohibidas para el usuario y permitidas para el comercio", aunque es posible que si los campos los tuviéramos por separado en diferentes archivos de trabajo, se pueden tomar las siguientes condiciones:

Nombre del Campo	Condiciones de lectura		Condiciones de borrado		Condiciones de escritura	
	Comercio	Cliente	Comercio	Cliente	Comercio	Cliente
Id_Cliente	Prohibido	Libre	Libre	Prohibido	Libre	Prohibido
Puntaje	Libre	Libre	Prohibido	Prohibido	Libre	Prohibido
Fecha_expiración	Libre	Libre	Libre	Prohibido	Libre	Prohibido

Las condiciones son fijadas de acuerdo con los criterios del comercio y con la suficiente ética para no incurrir en delitos.

d) La forma en la que se opera es la siguiente, pensando en que el cliente ya ha realizado sus compras y se dispone a pagar:



Nota: El Monto alcanzado es el que nos indica si el total de dinero a pagar nos permite añadir o no, puntos a la aplicación de Lealtad.

Con esto, el cliente termina el proceso de su compra y se le añaden los puntos (en la aplicación Lealtad de su tarjeta) correspondientes al equivalente de su compra; mientras tanto, el comerciante realiza (o al final del día) una actualización de información proveniente de su terminal de compra hacia su PC, la cual controla la base de datos de los clientes y aquí puede cotejar la cantidad de puntos que dicho cliente ha acumulado. Como es de suponerse, la base de datos con la que contamos, debe ser lo suficientemente capaz de darnos información exacta.

A la siguiente visita del cliente, éste puede realizar sus compras normalmente y sumar aún más puntos.

Cuando la cantidad de puntos requerida por el comercio ha sido alcanzada o rebasada, éste tiene la obligación de informar al cliente de este suceso y proceder a realizar el descuento o la promoción a la que se haya hecho acreedor.

Como el cliente puede cotejar la información de sus puntos en cualquier momento (en la terminal del comercio), éste puede llevar su propio control y calcular sus futuras compras.

Es importante mencionar que como evolución es posible considerar que la terminal sea quien despliegue, en el momento preciso, que se han alcanzado los requerimientos de acumulación de puntos por el cliente y realizar de manera automática el descuento prometido.

Nota: Por cuestiones de confidencialidad, no se definen los encabezados del archivo de trabajo al cual nos hemos referido, ni se incluyen otras estructuras de archivos (ver tema *Estructuras*).

Como hemos visto, es posible automatizar más los procesos que se llevan a cabo con las Tarjetas Inteligentes, en conjunto con sistemas y terminales; se puede evolucionar un proyecto y puede concebir mejoras. Pero el fin de este tema es ejemplificar cómo se puede idear una aplicación y cómo se debe prever el futuro.

Capítulo V: Alcances

V.1. Comercio Electrónico

Se piensa que existirán nuevos tipos de tecnologías disponibles en un futuro no muy lejano, en los escenarios para el acceso de información en los cuales el comerciante no tendrá la necesidad de estar físicamente en su comercio. Esto significa que nosotros compraremos dondequiera que sea, lo que queramos, sin el requerimiento de estar presente físicamente en una tienda, o un restaurante. El consumidor, asumirá electrónicamente el control en muchas de las futuras transacciones. Algunos escenarios predicen que más del 85 por ciento de las nuevas terminales y sitios de aceptación de tarjetas bajo desarrollo, serán manejadas por el usuario.

Nuestras televisiones (que podemos contar en muy grandes cantidades), tendrán la habilidad de aceptar tarjetas inteligentes para fomentar el comercio electrónico. Hoy en día hay teléfonos celulares que ya aceptan este tipo de tecnología con tarjetas.

En la actualidad existen algunos dispositivos que nos permiten consultar las últimas transacciones que hemos hecho con nuestra tarjeta ME, para tener un registro de cómo gastamos y cuándo gastamos. El número de transacciones mostradas en tales dispositivos, depende de cómo la tarjeta fue personalizada y de cómo el dispositivo lector ha sido programado.

En el futuro próximo, tendremos más que un dispositivo de entretenimiento (como es el caso de las televisiones), puntos de comunicación (teléfonos) o lugares de trabajo (computadoras personales) los cuales nos permitirán realizar transacciones monetarias al momento de comprar diferentes productos.

Estos dispositivos inteligentes llagarán a ser puntos de interacción y transacciones electrónicas en la economía del mañana. Un dispositivo seguro, como una Tarjeta Inteligente con microprocesador, será de suma importancia habilitando esta visión para llegar a convertirse en una realidad.

Por ahora, el caso más común que tenemos de comercio electrónico en la actualidad es el de la internet.

Esta red WAN, se ha ido desarrollando en los últimos años y ha alcanzado gran popularidad por la diversidad de servicios que se ofrecen mediante ella. Pero esta red no sólo nos permite obtener información o tener entretenimiento, ya que también nos ofrece la posibilidad para realizar el pago de bienes y servicios a través de portales que se dediquen a comerciar; en estas páginas uno puede comprar un artículo con el simple hecho de llenar una pequeña forma en la que se incluyen datos de una tarjeta de crédito/débito, como número de cuenta del cliente y nombre.

A juicio propio del autor, no es recomendable realizar este tipo de transacciones, ya que siempre existe la gente que está dedicada a la delincuencia y que además es capaz de obtener información de estas transacciones, "colgandose" de las líneas que transportan nuestros datos.

Un medio, por mucho, más seguro al momento de realizar transacciones en línea es un ME, ya que la información que se envía va codificada mediante algoritmos sobre los cuales se ha probado y comprobado su efectividad para mantener secretos. Los datos que viajan a través de las líneas de transmisión, van cifrados y están libres de la posibilidad de fraude.

El uso de NIP, nos da una vez más, un grado de seguridad mayor, aunque no es 100 % efectivo, desde el punto de vista de que si un delincuente nos amenaza, no podríamos negar la divulgación del código.

V.2. Interoperabilidad

Simple y llanamente, el término de interoperabilidad se refiere al hecho de poder integrar bajo un mismo esquema tecnológico la posibilidad de trabajar con diferentes proveedores.

En el mundo actual donde vivimos, la creciente necesidad de alcanzar la compatibilidad entre sistemas electrónicos se ve reflejada también en el manejo de la tecnología de las Tarjetas Inteligentes; es por eso que existe un desarrollo de estándares para la industria manufacturera de chips y plásticos, que nos permitirá contar con distintos proveedores sabiendo que todos y cada uno de ellos nos ofrecerán las mismas funcionalidades y será un punto menos sobre el cual debemos de preocuparnos

Pero la interoperabilidad también está muy enfocada al manejo de una misma aplicación, como por ejemplo el ME, el cual pudo ser desarrollada por diferentes organizaciones

En México, al igual que en otras partes del mundo, es importante tener diferentes proveedores que nos ofrezcan productos que cumplan con las mismas características aplicativas a las cuales nos enfocamos.

Un desarrollo muy importante por venir, es poder realizar pagos con el ME en diferentes partes del mundo y con el empleo de una sola tarjeta, aunque la divisa en que esté expresado el valor virtual del dinero dentro del chip, pertenezca a diferentes monedas

V.3. Crecimiento

El crecimiento de cualquier producto está determinado (y hasta cierto punto podemos decir que también está limitado) por varios factores, entre los que

podemos destacar el grado de aceptación que le da la misma gente, de acuerdo con los problemas que les soluciona y también de acuerdo con su facilidad de uso, la rentabilidad del producto, la infraestructura que se tiene para mantenerlo con un periodo de vida determinado por quien o quienes comercializan el producto, la posibilidad de evolución y la obsolescencia de la tecnología.

Para el caso específico de las tarjetas inteligentes, según estudios de mercado, se puede ver que los factores arriba mencionados cumplen satisfactoriamente estas expectativas; es posible observar que desde la introducción de las tarjetas chip (ya sean de memoria, o nuestro caso especial con microprocesador) ha ido en aumento su uso y ha sido un buen mercado para empresas telefónicas, principalmente, y más recientemente, para la banca, como es el caso de varios países europeos como Bélgica, o de unos pocos del continente Americano, como lo es México, que se coloca como líder hasta estas fechas

Se espera que la popularidad de las Tarjetas Inteligentes crezca ya que se le ofrece a los consumidores la posibilidad de realizar cargas desde diferentes dispositivos como computadoras de escritorio o portátiles (donde podemos mencionar el caso muy particular de internet), teléfonos públicos, cajeros automáticos, teniendo con esto una sucursal bancaria hacia donde *dirijamos la vista*, pudiendo disponer, es decir, gastar el dinero electrónico almacenado en el chip en terminales punto de venta como teléfonos públicos, a través de compras en portales virtuales, tiendas de autoservicio o el transporte público. Pero el campo no está limitado sólo al pago con aplicaciones de monederos electrónicos, y como se ha visto, es posible que nos sirva para almacenamiento de datos personales

Por el momento en México, se tiene una infraestructura suficientemente fuerte en el campo de la telefonía pública, lo cual permite tener puntos de recarga y

de compra en bastantes sitios. Los teléfonos públicos, no importando el modelo o marca, cumplen con las mismas características, a nivel usuario, para realizar los consumos (llamadas) y para depositar electrónicamente dinero dentro del chip en su aplicación ME. Se le puede considerar a este medio como el más grande que hay en la actualidad en el ámbito nacional e incluso en el internacional.

Pero la expansión de terminales no se limita únicamente a los teléfonos públicos, y como parte del crecimiento podemos señalar que las recargas o consumos a través de internet son fundamentales para poder ampliar el mercado, debido a que el uso de esta red WAN, es a escala mundial, y se sabe que México es uno de los países con más accesos a internet en el continente americano y que sólo se encuentra por debajo de países como E.E.U.U. o Argentina. Esto nos da una muy buena razon para expandir las fronteras en donde un ME puede ser de uso cotidiano

De acuerdo con lo anterior, los teléfonos públicos y el uso de internet adoptan para estos momentos los puntos clave para iniciar un buen mercado en el que la buena impresión que estos dejen, nos conducirá a tener un alto grado de aceptación entre usuarios y empresas proveedoras del producto.

Afortunadamente lo anterior no nos limita a sólo estos entes, pues como ya lo hemos mencionado, existen *vending machines* (maquinas expendedoras de refrescos y botanas) que cada vez son de uso más frecuente en escuelas, gasolineras y edificios corporativos

El caso del transporte público es un nicho de mercado bastante interesante, puesto que aquí podemos contar con el transporte masivo de personas (como lo es el metro o los camiones), aplicando tecnología sin contacto; aunque también es posible introducir el concepto a trenes (notando que en nuestro país no hay un uso muy generalizado), camiones foráneos, que no requieren

forzosamente una tecnología contactless, sino una con contacto, lo cual abarata costos, transporte aéreo y marítimo.

El anterior rubro es muy amplio y prácticamente aquí se abarca casi el 100 % de los individuos que conformamos la sociedad, razón por la cual se debe trabajar rápidamente, sin perder con esto calidad en el servicio.

Debido a que es posible manejar aplicaciones sin tener que hacer uso de dinero, las aplicaciones de Lealtad, también abren las puertas al mundo de la captación de clientela.

Con todo esto podemos ver que el crecimiento puede y debe ser a gran escala y afectivo a la sociedad en general, y a medida que el tiempo avance y nos mezclemos más y más con las tarjetas las haremos imprescindibles en nuestra vida, pero no con el fin de depender de ellas, sino con el claro objetivo de que nos sirvan para facilitar nuestras transacciones comerciales, nuestro resguardo de datos, el acceso a ciertos lugares y todo aquello que podamos imaginar en lo sucesivo.

Anexo 1: Algunos Algoritmos de encripción de datos

DES y Triple DES.

El algoritmo DES (Data Encryption Standard), establecido en las normas ISO 8731-1 y 8732 es el utilizado como algoritmo criptográfico, para la identificación del usuario y el manejo de mensajes seguros.

El DES es un mecanismo de encripción que fue originalmente pensado para su implementación en hardware. Cuando se usa, como en el caso de las tarjetas, en un sistema de comunicación, tanto quien genera los mensajes como el receptor deben conocer la clave secreta. Esta clave es la que se usará para encriptar o desencriptar un mensaje, o para generar un código de autenticación MAC. Como en estos sistemas de varios usuarios la distribución de las claves secretas puede ser problemática, suele complementarse con un algoritmo de clave pública (por ejemplo RSA)

Por lo tanto, en este caso particular, el DES simple y el Triple DES (DES3) se usan en la derivación de claves, MAC (Message authentication code) y los mecanismos de encripción que describiremos más adelante.

El algoritmo DES toma una entrada de texto plano de 8 bytes (X), y una clave secreta de 8 bytes (K), con lo que produce una texto cifrado (Y). En general, de la clave secreta sólo se toman los primeros 56 bits, eliminando los 8 bits de paridad.

$$Y=DES(K)[X]$$

La desencripción será:

$$X=DES\text{-}1(K)\ [Y]$$

Si se utiliza el mecanismo de Triple DES, el texto plano de 8 bytes se transformará en un texto cifrado de 8 bytes, pero utilizando una clave de 16 bytes. Esta clave K resultará de la concatenación de dos claves de 8 bytes cada una, KR y KL.

$$Y=DES3(K)[X]=DES(KL)[DES\ -1(KR)[DES(KL)[X]]]$$
$$X=DES3\ -1(K)[Y]=DES\ -1(KL)[DES(KR)[DES\ -1(KL)[Y]]]$$

Cifrado de bloques

En muchas ocasiones es necesario encriptar información que ha sido separada en bloques. De este modo, es posible implantar varios formas de combinar los bloques de información cifrada y de información "plana", obteniendo diferentes resultados.

Los modos de cifrado de bloques definidos normalmente para DES son cuatro: ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher Feedback) y OFB (Output Feedback). El método CBC se emplea para el cifrado del PIN de la tarjeta.

En el modo CBC, se efectua una suma exclusiva (OR Ex) entre cada bloque de texto plano y el bloque cifrado previo. Debe usarse un vector inicial, también llamado "semilla" para poder cifrar el primer bloque.

Una de las ventajas de este método que los patrones existentes en el texto plano desaparecen en el texto cifrado ya que son "eliminados" al aplicar la suma exclusiva con el bloque cifrado anterior.

MAC (Message Authentication Code).

El MAC es un campo a veces llamado "cheksum"), que se obtiene al aplicar un mecanismo de autenticación con una clave secreta, sobre el mensaje. A diferencia de los mecanismos de firma, el MAC se calcula y se verifica con la misma clave, de forma que pueda ser verificado sólo por el destinatario del mensaje.

RSA / RABIN.
El RSA es un mecanismo criptográfico de clave pública que puede ser usado tanto en el cifrado como en la firma de mensajes.

El algoritmo RSA, y su variante Rabin con exponente 2, son los algoritmos asimétricos reversibles usados en el esquema de firma digital para la verificación estática y dinámica de los datos.

Este algoritmo produce una firma con una longitud igual al tamaño del módulo utilizado. La longitud en bits de todos los módulos debe ser múltiplo de 8, con los dígitos extremos (LSB y MSB) en '1'.

Anexo 2: Protocolo T = 0

Primeramente, podemos mencionar que un protocolo de comunicación es aquel que fija ciertas reglas para establecer una comunicación.

Para este tipo de protocolo comando inicia la secuencia. La interacción entre la tarjeta y la terminal consta de sucesivos comandos y respuestas. La dirección de los datos que formarán parte de la respuesta está implícita en el comando.

El mensaje de comando consiste en un encabezamiento de 5 caracteres, que la interfase envía hacia la tarjeta, y que es contestado con un byte de procedimiento.

El encabezamiento consta de cinco bytes:

CLA – Clase de instrucción;
INS – Código de instrucción;
P1 – Calificador de instrucción;
P2 – Calificador de instrucción adicional;
P3 – Longitud del bloque de datos.

Luego de que la tarjeta envía el byte de procedimiento y se realiza el traspaso de datos (desde o hacia la tarjeta), la interfase recibe dos bytes de status SW1 y SW2. Estos sirven para que la interfase sepa el estado en que quedó la tarjeta luego del comando. La respuesta normal es:

SW1, SW2 = 90h, 00h.

Capitulo VI: Conclusiones

Las innovaciones tecnológicas que adquieren popularidad y que continúan entre nosotros son aquellas que permiten evoluciones, son eficientes, solucionan problemas y nos facilitan la vida, por citar algunas razones. Si meditamos acerca de las tarjetas con chip, podemos ver cubiertas estas razones.

Desde un principio las tarjetas con chip, refiriéndonos a las tarjetas de memoria, le ganaron terreno a otras tecnologías que empleaban un elemento de soporte plástico y algún dispositivo sensor como el óptico, para realizar transacciones monetarias, debido a que las primeras permitían una evolución mucho más rápida y de mejor calidad, abatiendo costos. Esa evolución son las Tarjetas Inteligentes y que han sido el punto central de este trabajo.

El chip ha sido un elemento electrónico que ha venido a revolucionar la forma en como se aplica la electrónica, este desarrollo tecnológico vio sus inicios hace algunas décadas, pero en los últimos años ha sido realmente exitoso y abarca casi todos los sectores del desarrollo en ingeniería, tocando a nuestra puerta en muchos de los artículos que intervienen en nuestra vida diaria. El campo de las Tarjetas Inteligentes ha sido uno de los más beneficiados y espera aún más desarrollos en cuanto a capacidades de memoria, rapidez y seguridad en la transmisión y recepción de datos, hablando del sistema con contacto, y además de las anteriores, para el caso de tarjetas sin contacto, se visiumbran avances en lo referente a métodos de anticolisión y a la distancia entre tarjeta y terminal lectora

Hoy en día contamos con chips, embebidos en un plástico, que son capaces de almacenar dinero en su interior, además de que a través de ellos se pueden desarrollar aplicaciones que nos facilitan diversos procesos en la vida diaria. Hay chips que para ejecutar sus funciones, forzosamente deben ser

introducidos en el lector de una terminal, pero también existen los que no requieren de contacto alguno, sino que emplean tecnologías de radiofrecuencia que permiten su interacción con terminales diseñadas especialmente para no tener una ranura en la cual se inserte la tarjeta (Tecnología Sin Contacto).

En general, las tarjetas (sean de banda o con chip) han sido muy prósperas dentro de nuestra sociedad, las vemos con mucha frecuencia en tarjetas de débito y que están encaminadas a ser nuestra alcancía en el banco, es aquí donde muchas empresas depositan el dinero correspondiente a la nómina de sus empleados para que ellos puedan disponer de su dinero en casi cualquier cajero automático; esto ayuda a que los empleados no estén cargando con el dinero por el cual han trabajado durante un periodo, y por un descuido o una acción mal intencionada se pierda esa recompensa a la labor diaria. Si una tarjeta de débito, además cuenta con uno de los logotipos clásicos que son aceptados en el ámbito internacional, también se nos abre la oportunidad de pagar en una gran cantidad de comercios, no con el dinero en efectivo (monedas y/o billetes), sino haciendo uso de la banda magnética que se localiza en el reverso del plástico.

Las tarjetas plásticas también tienen su uso en las tarjetas de crédito, con las cuales podemos realizar pagos, con la salvedad de que el dinero del cual estamos haciendo uso, en ese momento es un préstamo del banco emisor de la tarjeta.

Con esto podemos ver que las tarjetas nos permiten manejar más eficazmente el dinero, bajo el concepto de crédito o de débito. Pero las tarjetas también trabajan con el concepto de prepago. Este concepto ha sido muy funcional en nuestro país desde que se introdujeron los teléfonos públicos que trabajan basándose en esta idea, mas sin embargo, hablando claramente, el principal beneficiado es el empresario, puesto que el flotante que tiene por el pago anticipado de las comunicaciones es bastante grande.

Debido a lo anterior el concepto de ME, alcanza un gran interés, ya que el dinero ahora es dinero en efectivo que lo tiene el usuario en su chip (cuando éste ha sido cargado previamente y de acuerdo con el monto definido por el mismo) y del cual puede disponer en cualquier momento.

En México, se tiene una gran visión que abarca muchos campos de la vida cotidiana, ya que se pretende que la tarjeta no sirva única y exclusivamente como un medio de almacenamiento y pago con el dinero electrónico en efectivo, sino que también ofrezca a usuarios siempre un valor agregado que es un atractivo realmente importante para poder tener éxito en cualquier programa. Este valor agregado es el de las multiaplicaciones.

Como ya hemos visto, una aplicación está encaminada hacia diferentes objetivos planteados por los comerciantes y con ellas pretenden atraer clientela a su negocio (caso de la aplicación Lealtad), aunque también una aplicación puede tener la habilidad de manejar diversos datos en conjunto con PC's administradoras y terminales especiales para facilitar nuestra vida, ya que en el chip podemos guardar suficiente información relevante de nosotros mismos, como puede ser el registro del IFE o tipo de sangre.

Es esta capacidad multiaplicativa de una Tarjeta Inteligente, la que hace que el mercado se vea interesado en esta novedosa plataforma tecnológica para poder llegar a tocar más núcleos sociales y económicos, abatiendo muchos de los costos que existen en la actualidad.

A juicio del autor de este trabajo, las Tarjetas Inteligentes (con microprocesador) dejarán de ser un caso de ciencia-ficción y pasarán a formar parte importante de nuestra vida cotidiana, en un lapso no muy grande. Nos ayudarán a manejar mejor nuestras finanzas, nos auxiliarán al momento de

almacenar datos que nos identifiquen como ciudadanos o conductores, nos identificarán como clientes frecuentes de tal o cual negocio, etcétera.

Si pensamos en las complicaciones que puede tener esta tecnología, creemos que las más importantes son:

- Renuencia al cambio y evolución hacia mejores tecnologías.

- Tiempo de implantación.

La segunda implica cambios muy fuertes a nivel software sobre terminales, masificación de tarjetas emitidas, nuevo hardware capaz de manejar tarjetas con microprocesador y mejoras y crecimiento en sistemas de cómputo (este rubro es muy importante, aunque en el desarrollo de este trabajo no se incluyó por salir del tema central de la tesis)

Pero la de mayor complicación es la primera, debido a que usualmente le tememos al cambio, y en muchas de las ocasiones sólo estamos de acuerdo en usar nuevas tecnologías cuando sabemos que en un país desarrollado las propuestas ya funcionan normalmente y a un porcentaje de confiabilidad demasiado alto. Tal vez esta sea la mayor problemática, pero debido a esto, la explotación del proyecto no se lleva de manera total en toda la población, ya que se pone en marcha una ciudad piloto o con un núcleo controlado de gente, para conocer el nivel de aceptación del producto, además de que esto nos permite valorar las futuras evoluciones y mejoras sobre nuestro sistema en general.

A pesar de estos dos puntos anteriores, que pueden superarse a medida que avance el tiempo y con la confianza que se genere en los usuarios y los emisores de tarjetas, se estima que las Tarjetas Inteligentes vayan poco a poco entrando a nuestras actividades diarias, mediante la implementación de las

tecnologías con contacto y las que no lo requieren, y sin ensombrecer procesos que ya en la actualidad gozan de la mala reputación de ser ineficientes y obsoletos en un mundo donde el que no cambia, no avanza.

ESTA TESIS NO SALE
DE LA BIBLIOTECA

Bibliografía

66.69 Criptografía y seguridad informática, Trabajo práctico final, Tarjetas Inteligentes. Pablo A. Batch. Universidad de Buenos Aires. Pp: 4 a 17 y 23 a 38.

Smart cards: A guide to building and managing smart cards applications. Dreifus Henry y J. Thomas Monk. Editorial John Wiley & sons, Inc. Pp: 15 a 28, 29 a 44 y 112 a 119.