Universidad de las Ciencias Informáticas

“Facultad 6”

Título: “Propuesta de informatización del proceso de identificación de personas en Cuba”

Trabajo de Diploma para optar por el título de Ingeniero en Ciencias Informáticas

Autor: Alain Díaz Fernández

Tutor: Ing. Elvis Vázquez Aragón

Co-tutor: Lic. Ulises Llorente Pérez

Consultante: Ing. Adonis Cesar Legón Campos

Junio de 2009

“Año del 50 aniversario del triunfo de la Revolución”

"UN EXPERTO ES UNA PERSONA QUE HA COMETIDO TODOS LOS ERRORES QUE SE PUEDEN COMETER EN UN DETERMINADO CAMPO."

NIELS BOHR

DECLARACIÓN DE AUTORÍA

Declaro que soy el único autor de este trabajo y autorizo al Centro de Identidad y Seguridad Digital de la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.

Para que así conste firmo la presente a los ____ días del mes de _____ del año _2009___.

Alain Díaz Fernández

_____

Elvis Vázquez Aragón

_____

DATOS DE CONTACTO

Tutor: Ing. Elvis Vázquez Aragón.
Especialista de Informatización graduado de Ingeniero en Ciencias Informáticas, egresado de la Universidad de las Ciencias Informáticas en adiestramiento.

Co-Tutor: Lic. Ulises Llorente Pérez

Asesor: Ing. Adonis C. Legón Campos
Jefe del Dpto. de Tarjetas Inteligentes

AGRADECIMIENTOS

Le agradezco a mi esposa Saychi por ser parte de mi en cada examen y por apoyarme siempre, a Yadelis y Yuriem por haberme dado fuerzas para terminar la carrera, a mi tutor Elvis por ser un amigo en todo momento y a mi cotutor Ulises por brindarme su experiencia.

DEDICATORIA

A mis padres Félix y Clara a quienes les debo lo que soy.

RESUMEN

El proceso de identificación personal es parte de la vida cotidiana, familiares y amigos están satisfechos con el hecho de reconocer nuestro rostro o voz, en estos casos son las características físicas las que nos identifican. En la interacción con la sociedad se necesita estar identificados por un documento legal que garantice que somos realmente la persona que afirmamos ser, principalmente en los procesos legales. Existe una fuerte tendencia a informatizar el proceso de identificación en el mundo utilizando sistemas o tecnologías: RFID, tarjeta inteligente (TI), match-on-card, lector biométrico, entre otros. En algunos países subdesarrollados se realiza el proceso de identificación de forma mecánica o manual, lo cual no garantiza la autenticidad del documento de identificación. La oficina del carné de identidad (OCI) del municipio La Lisa realiza el proceso de identificación de forma manual al igual que en todas las oficinas del carné de identidad en Cuba, esto provoca un gasto significativo en materiales fungibles de oficinas, que la gestión de la información sea lenta y que con el deterioro de los documentos archivados existan pérdidas de datos, después de analizar la problemática existente se plantea la siguiente pregunta: ¿Cómo contribuir a la mejora de la gestión de información en el proceso de identificación de personas en Cuba, en el municipio La Lisa? Este trabajo tiene como principal objetivo proponer una solución informática empleando tarjetas inteligentes que de ser desarrollada y aplicada por la entidad autorizada (MININT) resolvería la problemática existente en el proceso de identificación.

SUMMARY

The personal identification process is part of our diary life, parents and friends are satisfied recognizing our face or voice, in these cases the physics characteristics identifies us. When persons interact in society is necessary to be identified by a legal document that's guaranties we really are the person we claim to be, mainly in legal processes. There is a strong tendency of computerize the identification process in the world using systems and technologies: RFID, smart card, match-on-card, biometric reader, among others. There are some underdeveloped countries that make the identification process manually or mechanic, this fact doesn't guaranty the authenticity of the identification document. The office of the identification national document (OCI) in La Lisa town makes this process manually as all this offices around Cuba, this cause stationery significant spending, slow information management and information data looses by the store document damage, after analyze the existing problem it is suggest the following question: How to get better the management of the identification process information of Cubans citizens, La Lisa town? The main objective of this work is to propose informatics solution using smart cards in case of being developed by an authorized entity (MININT) would solve the identification process problem.

PALABRAS CLAVES

Tarjeta Inteligente.

Identificación.

Proceso de identificación.

Sistema de identificación.

Documento Nacional de Identificación

TABLA DE CONTENIDOS

INTRODUCCIÓN

Una de las acepciones de la palabra "Identificar" es reconocer si una persona es la que se busca, es decir, se trata de establecer su individualidad determinando aquellos rasgos o conjunto de cualidades que la distinguen de todos los demás y hacen que sea ella misma. Muy poco después del origen del hombre, éste trató de encontrar alguna particularidad que sirviera para diferenciarlo de los demás, las particularidades se resumían, en sus características físicas, comportamiento, destrezas, carácter, habitad, etc. Al pasar el tiempo, surgió la necesidad de cuantificar y mensurar las características de cada ser humano surgiendo los sistemas de identificación biométricos.

Como expresa el artículo 6 Declaración Universal de Derechos Humanos, “Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica” (1). Por tanto la identidad personal es un derecho de todo ciudadano y los Gobiernos tienen la obligación de establecer los mecanismos adecuados para facilitársela.

Los seres humanos al interactuar en la sociedad necesitan estar identificados por un documento legal emitido por una entidad autorizada que garantice que la persona es realmente quien dice ser, surgiendo entonces el Documento Nacional de Identidad (DNI) el cual a lo largo de su vida ha ido evolucionado e incorporando las innovaciones tecnológicas disponibles en cada momento, con el fin de aumentar tanto la seguridad del documento como su ámbito de aplicación. Con la llegada de la Sociedad de la Información y la generalización del uso de Internet se hace necesario adecuar los mecanismos de acreditación de la personalidad a la nueva realidad y disponer de un instrumento eficaz que traslade al mundo digital las mismas certezas con las que se operan cada día en el mundo físico y que, esencialmente, son:

- Acreditar electrónicamente y de forma indubitada la identidad de la persona.
- Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita.

En Cuba existen diferentes documentos que contienen información personal, por lo que cada persona deberá portar cada documento para ser identificado en cada caso. El documento nacional de identificación es generado manualmente en la Oficina del Carné de Identidad (OCI) y luego plastificado con una foto para la identificación visual del individuo, la autenticidad es un problema, pues cualquier individuo podría generarse su propia identidad, otro problema que presentan estos documentos es con

su actualización, pues, como es manual, cada dato que cambie generará un nuevo documento, lo cual genera un gran gasto de recursos. En entrevistas realizadas a la directora de la OCI del Municipio La Lisa se corroboró la falsificación de DNI.

En la UCI, existe el Centro de Identificación y Seguridad Digital donde se desarrollan proyectos con múltiples aplicaciones entre los que se encuentra la cédula de identidad electrónica de la República Bolivariana de Venezuela, utilizando tarjetas inteligentes.

El proceso de informatización de la sociedad cubana, justifica la necesidad de elaborar propuestas basadas en el estudio de las principales tecnologías y estándares para informatizar el proceso de identificación en Cuba y otros países de Latinoamérica y para el caso se analizaron la OCI del Municipio La Lisa.
Como posible solución a estos problemas es que se elabora una propuesta de un sistema para informatizar el proceso de identificación en Cuba, municipio La Lisa haciendo uso de la tecnología Tarjetas Inteligentes (TI) como documento nacional de identificación electrónico (DNIe).

Se identifica el siguiente *problema científico* a resolver en la investigación:
¿Cómo contribuir a la mejora de la gestión de información en el proceso de identificación de personas en Cuba, en el municipio La Lisa?

Objeto de estudio:
El proceso de identificación de personas.

Campo de Acción:
El proceso de gestión de información de identificación de personas en la OCI del municipio La Lisa.

Objetivo de la investigación:
Proponer una solución informática que haga uso de las TI como DNIe, que contribuya a mejorar la gestión de información en el proceso de identificación en Cuba, en el municipio La Lisa.

Idea a defender:
La informatización del proceso de identificación de personas haciendo uso de las TI como DNIe en Cuba, en el municipio La Lisa contribuirá a la mejora de la gestión de información en el proceso de identificación de personas.

Tareas de la investigación:

1. Referir las características de los tipos de sistemas que se emplean para la identificación.
2. Puntualizar las tecnologías aplicadas a la identificación personal.
3. Analizar los resultados de la implantación de sistemas de identificación personal existentes en el mundo.
4. Describir el proceso actual de identificación en la Oficina del Carné de Identidad del municipio La Lisa.
5. Realizar el análisis del sistema a proponer.
6. Elaborar la propuesta.
7. Validar la propuesta a partir de criterios de especialistas.

Sistema de métodos.

Partiendo de la concepción dialéctico - materialista como método más general, se emplearon como:

Métodos Teóricos.

Histórico-lógico: Profundización del estudio de los antecedentes del proceso de identificación de personas para poder establecer su desarrollo histórico, las tendencias fundamentales y la determinación de la trayectoria completa de los modelos del proceso de identificación que antecedieron al propuesto, su condicionamiento histórico y sus hitos más relevantes y significativos para el nuevo modelo a partir de la negación dialéctica, es decir, tomando de ellos los elementos positivos y adecuándolos de manera crítica y creadora a nuestro contexto.

Análisis-síntesis: Realización de un estudio exhaustivo y profundo análisis de las diferentes partes del diseño y su articulación, mediante el establecimiento de relaciones entre estos elementos para hacer una síntesis de las características actuales del proceso de identificación en Cuba, municipio La Lisa, explicando los factores que condicionan la necesidad de un modelo teórico de un sistema de identificación personal.

Inductivo-deductivo: Análisis de lo particular del proceso de identificación para llegar a las generalizaciones desde las teorías y particularidades de este proceso en cada país analizado.

Métodos empíricos.

Observación directa: Realización de una observación sistemática, consciente y objetiva que permita obtener información sobre el estado del proceso de identificación personal en cuanto al proceder de los oficiales encargados de emitir el documento de identificación y de los oficiales encargados de verificar la identidad de los ciudadanos.

Entrevistas: A especialista con el objetivo de obtener información detallada sobre el proceso actual de identificación de personas en Cuba, La Lisa.

Aportes prácticos esperados del trabajo.

Un documento que explica de forma detallada el funcionamiento de un sistema de identificación, soportado en la TI como DNIe en la OCI del municipio La Lisa.

Estructuración del contenido con una breve explicación de sus partes.

Capítulo 1: Fundamentación teórica.

En este capítulo se describen las características de los tipos de sistemas que se emplean para la identificación personal, se proporciona una panorámica general acerca de las Tarjetas Inteligentes; de manera que se describe la historia de su desarrollo, los tipos de tarjetas que existen actualmente y sus aplicaciones. Se incluye una breve explicación de sus características físicas y funcionales.

Capítulo 2: Análisis crítico de los sistemas.

En este capítulo se hace un estudio de algunos sistemas de identificación electrónica, se mencionan sus principales características, ventajas y desventajas, así como sus semejanzas y diferencias más significativas, se hace un análisis crítico de algunos de los sistemas implantados en el mundo que utilizan la tecnología TI.

Capítulo 3: Análisis de la propuesta.

En este capítulo se describe el proceso actual del negocio de identificación, se identifican los requerimientos funcionales y no funcionales del sistema y se presenta la propuesta de solución.

CAPÍTULO 1: FUNDAMENTACIÓN TEÓRICA

1.1 Introducción.

En este capítulo se hace un estudio de algunos sistemas informáticos de identificación personal, se mencionan sus principales características, ventajas y desventajas, así como sus semejanzas y diferencias más significativas. A partir de toda esta información e incorporando otras funcionalidades definidas según las necesidades de las diferentes instituciones interesadas, se espera confeccionar un diseño general del sistema. Además se proporciona una panorámica general acerca de las Tarjetas Inteligentes, describiendo la historia de su desarrollo, los tipos de tarjetas que existen actualmente y sus aplicaciones. También se incluye una explicación breve de sus características físicas y de las funciones que realiza su sistema operativo.

1.2 ¿Qué es identificación?

Etimológicamente, identificación deriva del verbo latino ***identificare*****,** vocablo integrado por los también latinos ***identitas y facere*** (***identitatem facere***), comprobar, hacer patente la identidad de alguien o algo. Según el diccionario de la Real Academia de la Lengua Española, identificación es la acción y efecto de identificar o identificarse, entendiendo por identificar: reconocer que una persona o cosa es la misma que se supone o se busca. De un modo más específico, aplicable al ámbito de la identificación personal se considera que identificar a una persona consiste en: El estudio técnico-científico de unas características físicas del individuo, para su posterior comparación o cotejo con un patrón de referencia (Ej.: registro anterior de esas características del individuo) para comprobar su similitud y establecer de este modo su relación de identidad, asociando a esta persona, si fuera posible, unos datos de filiación (1).

(Filiación: conjunto de datos de la persona constituido por: Nombre, apellidos, fecha y lugar de nacimiento, nombre progenitores, domicilio y número de algún documento de identidad) (1).

Se cotejaran datos de tipo físico, que el individuo porta en todo momento, exigiendo a esos datos dos propiedades:

a) que sean consustanciales al individuo, es decir, que lo hagan único respecto al resto de la población, (1)

b) que a poder ser, sean invariables a lo largo del tiempo, por si necesitásemos identificar a esa persona más de una vez a lo largo de su vida. (1)

Para un sinfín de actividades cotidianas es necesario estar identificado, cualidad que normalmente se suelen demostrar mediante un documento que acredita dicha identidad, pero que para la expedición de ese documento acreditativo anteriormente se han registrado junto a los datos de la persona, alguna característica consustancial de la persona portadora (Ej.: impresión dactilar, fotografía, etc.)

1.2.1 Tipos de sistemas de identificación.

Los sistemas de identificación más utilizados en la actualidad son los siguientes:

1) Sistema Antropométrico, basado en características físicas generalistas del individuo, fácilmente observables e incluso algunas de ellas mesurables. Su precursor fue Alphonse BERTILLON, quien estableció un método de observación y registro (Bertillonaje) de ciertas características físicas agrupándolas del siguiente modo:

a) Señalamiento antropométrico general, consistente en la medición de determinadas partes el cuerpo: estatura, longitud máxima de brazos extendidos en cruz, contorno craneal, extremidades, etc. (1)

b) Señalamiento descriptivo, basado en singularidades principalmente fisonómicas de la persona, conformando lo que Bertillon llamaba “el retrato hablado” (portrait parlé). (1)

c) Señalamiento de marcas particulares, como lunares, cicatrices, tatuajes, amputaciones, anquilosis, etc. Este sistema de identificación presenta como principales inconvenientes, su gran laboriosidad, lentitud, subjetividad por parte del especialista que estudia estas características y problemas de variabilidad natural (cambio de estatura con el crecimiento, cambio de color de pelo, de color de tez, etc.) de algunas de los rasgos observados. (1)

2) Sistemas Lofoscópicos: estudian la morfología de determinadas rugosidades presentes en ciertas zonas de la anatomía humana. Las rugosidades más estudiadas son las crestas papilares, finos relieves epidérmicos presentes en manos y pies, dependiendo que zona sea objeto de estudio, tendríamos:

a) Dactiloscopia, sistema de identificación basado en el estudio de los dibujos formados por las crestas papilares en las yemas de los dedos de las manos. (1)

b) Quiroscopia, sistema de identificación basado en el estudio de los dibujos formados por las crestas papilares en la palma de las manos. (1)

c) Pelmatoscopia, sistema de identificación basado en el estudio de los dibujos formados por las crestas papilares en la planta de los pies. No existen dos dibujos iguales formados por crestas papilares, siendo por lo tanto un elemento único para cada individuo. Además de las crestas papilares se estudian otras rugosidades como:

d) Palatoscopia, sistema de identificación basado en el estudio de las rugosidades presentes en el paladar superior de la boca (rugosidades palatinas) cuyo dibujo es esencialmente el mismo a lo largo de la vida del sujeto. (1)

e) Queiloscopia, sistema de identificación basado en el estudio de los pliegues de los labios de la boca. (1)

3) Sistema Odontológico, basado en el estudio de la morfología de las piezas dentales y de las diferentes particularidades que pudieran presentar, como por ejemplo ausencia de alguna pieza, caries, desgastes o como intervenciones hechas por un estomatólogo (empastes, fundas, puentes, prótesis totales o parciales). Este sistema plantea el problema de encontrar elementos de cotejo o comparación, para lo cual se suele utilizar fotografías o radiografías anteriores de las piezas dentales. Sin embargo, en determinadas situaciones extremas (cadáveres carbonizados, cadáveres en avanzado estado de descomposición, cadáveres esqueletizados, grandes catástrofes, etc.) resulta ser un sistema muy útil debido a la gran resistencia de las piezas dentales a altas temperaturas o fuertes impactos. (1)

4) Sistemas biológicos, basados en el análisis en el laboratorio de alguna sustancia del organismo del individuo cuya composición es única para cada persona, constituyendo de este modo un indudable elemento identificativo. Hoy en día dentro de estos estudios analíticos, los más empleados son las técnicas genéticas basadas en el estudio de la composición del ADN (ácido desoxirribonucleico), compuesto presente en todas las células nucleadas del individuo, y cuya composición es única para cada persona. Una ventaja de este sistema de identificación es que para el cotejo se podrá emplear un registro anterior (una muestra con la composición de esta sustancia) o bien una muestra de la composición del ADN de un familiar directo (padres o hijos del interesado), ya que dicha composición es hereditaria y transmisible. (1)

Todos estos sistemas de identificación se basan en “lo que la persona es”, es decir, en características intrínsecas a la persona. Existen otros sistemas de identificación basados en determinadas acciones llevadas a cabo por los individuos (“lo que la persona hace”) a través de las cuales pueden ser identificados y cuya aplicación es más frecuente en el ámbito de la Criminalística. Entre ellos podemos señalar:

5) Sistemas fonológicos o acústicos, basados en la identificación a través de la voz, en la cual existen determinados rasgos inherentes a cada persona, persistentes incluso aunque se modifique el tono, el volumen u otras características de la misma. (1)

6) Sistemas grafoscópicos, basados en la identificación de la persona a través de su escritura, de determinados trazos generados de una manera inconsciente y que pueden caracterizar el modo de escribir de la persona. (1)

1.2.2 Sistema de identificación más adecuado.

En la medida en que los resultados de un sistema satisfagan las necesidades y exigencias que se presentan para la identificación, el sistema será más apropiado.

El modelo del proceso de identificación personal postula la existencia de tres indicadores de identidad que definen el proceso de identificación de un individuo, estos indicadores son:

Posesión, lo que el individuo tiene (DNI).

Conocimiento, se refiere a lo que el individuo sabe (contraseña).

Característica o bien “lo que el individuo es”, es decir, la persona tiene una característica, ya sea física o conductual, por medio de la cual puede ser identificada, sin embargo para que esta pueda ser considerada un indicador de identidad debe cumplir con 4 requerimientos básicos, los cuales se describen a detalle a continuación.

1.2.2.1 Características de un indicador de Identidad

Las características físicas y conductuales de un individuo pueden ser utilizadas como Indicadores de identidad deben cumplir con los siguientes requerimientos básicos:

• *Universalidad*: Define lo que comprende o es común a todos en su especie, en este caso, los seres humanos, por lo que el indicador de identidad seleccionado deberá estar presente en todos los individuos (1).

• *Singularidad*: Hace referencia a lo que es único en su especie, por lo que este requerimiento especifica que la existencia de dos personas con una característica idéntica tiene una probabilidad casi nula (1).

• *Estabilidad*: Algo que es estable se mantiene o permanece invariable e indefinidamente en el mismo estado, situación o lugar, por lo que el indicador de identificación elegido deberá estar presente a lo largo del tiempo y en condiciones ambientales diversas (1).

• *Cuantificación*: Cuantificar significa expresar de manera numérica una magnitud, por lo que este requerimiento nos dice que debe de ser posible medir o conocer la cantidad exacta que posee el indicador de identificación seleccionado (1).

1.3 Situación de los sistemas de identificación en el mundo.

La identificación personal en el mundo se encuentra diversificada debido a que cada país tiene su propio sistema de identificación, en su mayoría diferentes unos de otros, hoy en día existen desde los sistemas más avanzados y automatizados hasta los más atrasados y manuales. En los países desarrollados los sistemas de identificación nacional están convergiendo en la utilización de las tarjetas inteligentes como documento de identificación electrónico nacional, aunque vale reconocer que las personas hacen resistencia al cambio así como también hacen resistencia a la tecnología es por esto que la implantación y utilización regular por parte de los ciudadanos de esta tecnología está siendo un proceso lento. Hay algunos países como Reino Unido y EUA donde no existe un DNI (Documento Nacional de Identificación), sin embargo esto no quiere decir que no exista sistema de identificación, por el contrario existen varios documentos que hacen la función del DNI como son: la licencia de conducir que en estos países es una tarjeta inteligente y el pasaporte que identifica al portador internacionalmente. La identificación empleando tarjetas inteligentes varía su forma de empleo dependiendo en gran medida de las leyes que para ello hayan sido trazadas por los diferentes gobiernos. Presentan diseños diferentes pero en su mayoría cuentan con un número de identificación y un grupo de elementos de diferentes niveles de seguridad, estos serán analizados más adelante en el capítulo.

1.4 Sistemas informáticos de identificación personal.

1.4.1 Sistema de identificación por radio frecuencia (RFID).

La tecnología de auto-identificación por radiofrecuencia (RFID) está empujando con fuerza y ha empezado ya a desplazar al código de barras. El sistema emergente permite identificar objetos a distancia mediante etiquetas electrónicas. Ofrece múltiples ventajas y supone una solución a muchos problemas hasta ahora no resueltos.

La tecnología de auto identificación por radiofrecuencia o, lo que es lo mismo, Radio Frequency Identification Devices (RFID) se basa en unas etiquetas electrónicas o tags que se componen de un chip y una pequeña antena. Estas etiquetas se pueden incorporar a todos los productos y hacen posible identificarlos a distancia y controlarlos a lo largo de toda la cadena de distribución, desde el fabricante hasta el comprador. Además, permiten almacenar múltiples informaciones referentes al artículo portador de las mismas (2).

¿Cómo funciona la RFID?

Para que la tecnología RFID funcione, son necesarios tres elementos básicos: una etiqueta electrónica o tag, un lector de tags y una base de datos. Las etiquetas electrónicas llevan un microchip incorporado que almacena el código único identificativo del producto al que están adheridas. El lector envía una serie de ondas de radiofrecuencia al tag, que éste capta a través de una pequeña antena. Estas ondas activan el microchip, que, mediante la micro-antena y la radiofrecuencia, transmite al lector cual es el código único del artículo. En definitiva, un equipo lector envía una señal de interrogación a un conjunto de productos y estos responden enviando cada uno su número único de identificación. Por este motivo, se dice que la tecnología RFID es una tecnología de auto-identificación. (2)

Una vez el lector ha recibido el código único del producto, lo transmite a una base de datos, donde se han almacenado previamente las características del artículo en cuestión: fecha de caducidad, material, peso, dimensiones, entre otros. De este modo se hace posible consultar la identidad de una mercancía en cualquier momento y fácilmente durante toda la cadena de suministro.

1. El lector manda una señal de interrogación al RFID.

2. El RFID usa la energía de esta señal para funcionar, y su frecuencia como reloj.
3. El RFID lee los datos que manda el lector, en caso de que existan.
4. El RFID contesta con su propia información.
5. Un protocolo anticolisión permite gestionar la respuesta simultánea de múltiples RFID.
6. La información recibida se integra con el resto de Sistemas de Información. (3)

Características

Se rige por el estándar **ISO 14443**.

Este estándar establece la frecuencia de 13.56 Mhz para las tarjetas sin contactos que se comunican a corta distancia del lector, este consta de 4 partes. (4)

Parte 1: Características Físicas

Parte 2: Alimentación de la Radio Frecuencia

Parte 3: Inicialización y anticolisión

Parte 4: Protocolos de Transmisión

Ventaja.

Lecturas más rápidas y precisas: Un lector de RFID detecta automáticamente todas las etiquetas que pasan a través de su campo de radiofrecuencia. Como resultado, puede leer los datos de cada chip RFID adherido a cada objeto etiquetado en una sola operación.

Ahorro en costes de manipulación: Los minoristas y sus proveedores pueden utilizar RFID para ahorrar costos de manipulación e incrementar la eficiencia de los procesos de la cadena de suministros y en los sistemas de gestión de stock. La tecnología RFID permite automatizar ciertos procesos logísticos, así como recoger los datos eficientemente, disminuyendo los costes de adquisición de datos y facilitando la sincronización de la cadena de suministros

Mejor utilización de los activos: La tecnología RFID puede permitir a las empresas realizar un seguimiento no solo de los productos individuales, sino un seguimiento de sus activos reutilizables, embalaje, equipos, etc., de una forma más precisa.

Desventaja.

Costo: Son más costosas que otras tecnologías de ese mismo propósito.

No existe estándar global: No se encuentra estandarizada la frecuencia

Rastreo: El rastreo ilícito de las etiquetas RFID plantea un riesgo a la privacidad personal en términos de localización y de seguridad.

Riesgo de Cáncer: Estudios de toxicología indican que los chips RFID pueden inducir a tumores malignos.

Fácil de falsificar: En la página cuyo vínculo aparece a continuación se muestra con la facilidad que una persona puede copiar la identidad de otra que usa esta tecnología en los nuevos pasaportes de EUA, u otro tipo de documento de identificación que lo utilice.

http://www.engadget.com/2009/02/02/video-hacker-war-drives-san-francisco-cloning-rfid-passports/

1.4.2 Sistema biométrico.

Este sistema clasifica en la punta de la tecnología y consiste en la identificación mediante un lector de datos biométricos, de esta manera las personas podrían prescindir de portar algún documento de identificación, esta es una idea futurista que está siendo analizada por países desarrollados para su utilización en el campo de la identificación y ya está siendo utilizada en centros científicos e instituciones con un alto nivel de seguridad, donde cada persona tiene un nivel de acceso asociado. Este sistema consiste brevemente en el almacenamiento digital de la huella dactilar u otro indicador biométrico que estará asociado a los datos y nivel de acceso de una sola persona y para su futura comparación donde la coincidencia de la huella del identificado y la de la base de datos identificará a dicha persona como personal autorizado o no.

Arquitectura de un sistema biométrico para identificación personal.

Los dispositivos biométricos poseen tres componentes básicos. El primero se encarga de la adquisición análoga o digital de algún indicador biométrico de una persona, como por ejemplo, la

adquisición de la imagen de una huella dactilar mediante un escáner. El segundo maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos con los datos almacenados. El tercer componente establece una interfaz con aplicaciones ubicadas en el mismo u otro sistema. La arquitectura típica de un sistema biométrico puede entenderse conceptualmente como dos módulos (5):

1. *Módulo de inscripción* (enrollment module). Adquiere y almacena la información proveniente del indicador biométrico.

2. *Módulo de identificación* (identification module). Responsable del reconocimiento de individuos.

Fase operacional de un sistema de identificación personal biométrico.

Un sistema biométrico en su fase operacional puede operar en dos modos:

1. Modo de verificación. Verifica la identidad de algún individuo comparando la característica con solo las características de la ficha del individuo. Esto conduce a una comparación uno-a-uno para determinar si la identidad reclamada por el individuo es verdadera o no, responde a la pregunta: ¿eres tú quién dices ser? (5)

2. *Modo de identificación*. Descubre a un individuo mediante una búsqueda exhaustiva en la base de datos con múltiples ficha. Esto conduce a una comparación del tipo uno-a-muchos para establecer la identidad del individuo, responde la pregunta: ¿quién eres tú? (5)

Generalmente es más difícil diseñar un sistema de identificación que uno de verificación. En ambos casos es importante la exactitud de la respuesta. Sin embargo, para un sistema de identificación la rapidez también es un factor crítico. Un sistema de identificación necesita explorar toda la base de datos donde se almacenan las fichas, a diferencia de un sistema verificador. De la discusión anterior resulta obvio notar que la exigencia sobre el extractor y el comparador de características es mucho mayor en el primer caso (5)

Exactitud en la identificación: medidas de desempeño.

Una decisión tomada por un sistema biométrico distingue "personal autorizado" o "impostor". Para cada tipo de decisión, existen dos posibles salidas, verdadero o falso. Por lo tanto existe un total de cuatro posibles respuestas del sistema (3):

1. Una persona autorizada es aceptada.

2. Una persona autorizada es rechazada.

3. Un impostor es rechazado.

4. Un impostor es aceptado.

Las salidas números 1 y 3 son correctas, mientras que las números 2 y 4 no lo son. El grado de confidencia asociado a las diferentes decisiones puede ser caracterizado por la distribución estadística del número de personas autorizadas e impostores. En efecto, las estadísticas anteriores se utilizan para establecer dos tasas.

1. Tasa de falsa aceptación (FAR: False Acceptance Rate), que se define como la frecuencia relativa con que un impostor es aceptado como un individuo autorizado. (3)

2. Tasa de falso rechazo (FRR: False Rejection Rate), definida como la frecuencia relativa con que un individuo autorizado es rechazado como un impostor. (3)

La FAR y la FRR son funciones del grado de seguridad deseado. En efecto, usualmente el resultado del proceso de identificación o verificación será un número real normalizado en el intervalo [0, 1], que indicará el "grado de parentesco" o correlación entre la característica biométrica proporcionada por el usuario y la(s) almacenada(s) en la base de datos. Si, por ejemplo, para el ingreso a un recinto se exige un valor alto para el grado de parentesco (un valor cercano a 1), entonces pocos impostores serán aceptados como personal autorizado y muchas personas autorizadas serán rechazadas. Por otro lado, si el grado de parentesco requerido para permitir el acceso al recinto es pequeño, una fracción pequeña del personal autorizado será rechazada, mientras que un número mayor de impostores será aceptado. El ejemplo anterior muestra que la FAR y la FRR están íntimamente relacionadas, de hecho son duales una de la otra: una FRR pequeña usualmente entrega una FAR alta, y viceversa. El grado de seguridad deseado se define mediante el umbral de aceptación, un número real perteneciente al intervalo [0,1] que indica el mínimo grado de parentesco permitido para autorizar el acceso del individuo (3).

Desventaja.

Es una tecnología muy costosa, ya que siempre debe existir un lector biométrico cada vez que se vaya a verificar una identidad, aun no se ha logrado abaratar los costos de estos lectores biométricos lo suficiente, La información de la huella digital en un dispositivo red-conectado, un servidor externo, o un banco de datos podría ser considerado eslabones débiles en una cadena de seguridad.

1.4.3 Sistema Match-on-Card.

En este sistema se combinan la tarjeta inteligente y el lector biométrico. En este sistema se compara la huella dactilar escaneada por el lector biométrico con una almacenada en la tarjeta y de esta manera se identifica al portador del documento. Aquí la huella dactilar no solo hace función de PIN o contraseña sino que también utiliza la seguridad del chip.

1.5 Tarjeta Inteligente.

1.5.1 Definición.

Se define a la tarjeta inteligente como un dispositivo que posee una apariencia similar a la tradicional tarjeta de crédito, que contiene un pequeño chip[1] incrustado que controla el acceso a la información y brinda protección física a los datos almacenados. (Ver Figura 1.1)

"…el chip puede tener dos funciones, ser un poderoso microprocesador o actuar como un chip de memoria. El chip de silicio tiene tres funciones principales:

1. *Almacenamiento de datos.*
2. *Seguridad en la información.*
3. *Procesamiento de datos.* (6)

La transferencia de datos puede llevarse a cabo a través de los contactos que se encuentran en la superficie de la tarjeta, o sin contactos por medio de campos electromagnéticos. (Ver Figura 1.4).

[1] Un Chip es una pieza de Silicio fusionada con circuitos electrónicos. También se conoce como Circuito Integrado

Figura 1.1: Ejemplo de Tarjeta Inteligente con contactos, una Tarjeta Inteligente está compuesta por un cuerpo de plástico y un circuito integrado (chip).

1.5.2 Surgimiento.

Las tarjetas inteligentes surgen ante nuevas necesidades del mercado, las cuales no pueden ser satisfechas por la tarjeta de banda magnética. Esta tecnología surge en los 70 cuando inventores de Alemania Juergen Dethloff, Japón Arimura y Francia Moreno inscribieron las patentes originales en 1968, 1970, 1974 respectivamente. Muchos de los trabajos relacionados con las TI, estuvieron en investigación hasta la década de los 80, debido a que la tecnología de los semiconductores no estaba lo suficientemente desarrollada.

Las antecesoras de las Smart Cards fueron las Tarjetas Magnéticas (*Magnetic Stripe Cards*), utilizadas en cajeros automáticos y como tarjetas de crédito. Estas almacenan su información en una banda magnética la cual esta adherida a su superficie.

1.5.3 Tipos de tarjetas según la estructura de su sistema operativo

- *Tarjetas de memoria*. Tarjetas que únicamente son un contenedor de ficheros pero que no albergan aplicaciones ejecutables. Disponen de un sistema operativo limitado con una serie de comandos básicos de lectura y escritura de las distintas secciones de memoria y pueden tener capacidades de seguridad para proteger el acceso a determinadas zonas de memoria. (6)

- *Basadas en sistemas de ficheros, aplicaciones y comandos*. Estas tarjetas disponen del equivalente a un sistema de ficheros compatible con el estándar ISO/IEC 7816 parte 4 y un sistema operativo en el que se incrustan una o más aplicaciones (durante el proceso de fabricación) que exponen una serie de comandos que se pueden invocar a través de APIs de programación. (6)

- *Java Cards*. Una Java Card es una tarjeta capaz de ejecutar mini-aplicaciones Java. En este tipo de tarjetas el sistema operativo es una pequeña máquina virtual Java (JVM) y en ellas se pueden cargar dinámicamente aplicaciones desarrolladas específicamente para este entorno. (6)

1.5.4 Tipos de tarjetas según el formato (tamaño).

En el estándar **ISO 7810** se definen los siguientes tamaños para tarjetas inteligentes (4):

- **ID 000**: el de las tarjetas SIM usadas para teléfonos móviles GSM. También acostumbran a tener este formato las tarjetas SAM (*Security Access Module*) utilizadas para la autenticación criptográfica mutua de tarjeta y terminal.

- **ID 1:** *Especifica una medida de 85.60mm × 53.98 mm, tamaño tarjeta de crédito.*

- **ID 2:** *Especifica una medida de 105mm × 74 mm, esta es ligeramente más grande y permite imprimir en ella una foto para una identificación facial.*

- ***ID 3:*** *Especifica una medida de 125mm × 88 mm, es utilizada para pasaportes y visas.*

1.5.5 Tipos de tarjetas según sus capacidades.

"Las tarjetas se pueden clasificar según las capacidades de su chip, las tarjetas más habituales son:

- ***Memoria:*** *tarjetas que únicamente son un contenedor de ficheros pero que no albergan aplicaciones ejecutables. Éstas se usan generalmente en aplicaciones de identificación y control de acceso sin altos requisitos de seguridad.*

- ***Micro procesadas****: tarjetas con una estructura análoga a la de un ordenador (procesador, memoria volátil, memoria persistente). Éstas albergan ficheros y aplicaciones y suelen usarse para identificación y pago con monederos electrónicos.*

- ***Criptográficas****: tarjetas micro procesadas avanzadas en las que hay módulos hardware para la ejecución de algoritmos usados en cifrados y firmas digitales. En estas tarjetas se puede almacenar de forma segura un certificado digital (y su clave privada) y firmar documentos o autenticarse con la tarjeta sin que el certificado salga de la tarjeta (sin que se instale en el almacén de certificados de un navegador Web, por ejemplo) ya que es el procesador de la*

propia tarjeta el que realiza la firma. Un ejemplo de estas tarjetas son las emitidas por la Fábrica Nacional de Moneda y Timbre (FNMT) española para la firma digital (7).

1.5.6 Ventaja.

- Son capaces de almacenar información y procesarla.
- Brindan una mayor versatilidad al poder ser programada.
- Pueden ser multiplicación.
- Reducen el riesgo de fraude.
- En cualquier lugar que las tarjetas Inteligentes reemplacen papel, habrá una reducción de costos.
- Gran capacidad de memoria, con respecto a las anteriores tarjetas (tarjetas de banda magnética).
- Confiabilidad.
- Privacidad.
- Portabilidad.
- Facilidad de usos sin necesidad de conexiones en línea.
- Comodidad para el usuario.
- Cumple con estándares específicos de la ISO 7816.

1.5.7 Desventaja.

- *"Es necesario un lector para las tarjetas inteligentes.*
- *Por su tamaño las tarjetas pueden extraviarse.*
- *Depende de la energía eléctrica para su utilización.*
- *Puede ser dañada si se derrama un líquido sobre ella".* (8)

1.5.8 Seguridad en las Tarjetas Inteligentes.

- *"Seguridad de los componentes*
    - *El chip es a prueba de falsificación y no puede ser duplicado.*
    - *Capacidad de detección de*
        - *Ataques por Rayos X y luz Ultravioleta.*
        - *Voltajes inusuales.*
        - *Cambios de frecuencia de reloj.*
- *Seguridad del sistema operativo*
    - *Control de los accesos a memoria*
    - *Protección de datos y ficheros*
- *Seguridad del sistema operativo y de las transacciones.*
    - *Autentificación del portador. (mediante PIN)*
    - *Autentificación de la tarjeta a través de un sistema de claves diversificadas.*
        - *Encriptación/ Desencriptación DES[2].*
        - *Encriptación/ Des encriptación RSA[3].*
        - *Firma digital: MD5[4] ".* (8)

[2] **DES** (Data Encryption Standard o Estándar de Encriptación de Datos). Es el algoritmo de cifrado simétrico más estudiado, mejor conocido y más empleado del mundo.
[3] **RSA** (Rivest, Shamir, Adleman)**.** Es el algoritmo de mayor uso en encriptación asimétrica.
[4] **MD5** (Message Digest 5). Es una función hash irreversible, es decir, codifica la contraseña tecleada por el usuario y es imposible que partiendo de la cadena codificada obtenga la contraseña origen.

1.6 Tipos de Tarjetas Inteligentes.

1.6.1 Tarjetas de Contactos.

Las tarjetas de contacto son las que necesitan ser insertadas en un lector de tarjetas inteligente para que por medio de contactos pueda ser leída. Existen dos tipos de tarjeta inteligente de contacto: Las sincrónicas y las asincrónicas.

Tarjetas de Contactos Sincrónicas o de Memoria.

Estas tarjetas son cargadas previamente con un valor que va decreciendo a medida que se utiliza y una vez que se acaba el monto se vuelve desechable. (8)

Memoria Libre: La información almacena dentro de estas tarjetas no está protegida por ningún mecanismo de seguridad, lo que las hace utilizable solo en aquellos lugares donde no se necesite una alta seguridad, como: para el pago de peajes, teléfonos públicos, entre otros. (8)

Memoria Protegida: Poseen un circuito de seguridad que proporciona un sistema para controlar los accesos a la memoria frente a usuarios no autorizados. Este sistema funciona mediante el empleo de un código de acceso. (8)

1.6.2 Tarjetas Asincrónicas.

Estas tarjetas poseen en su chip un microprocesador, que además cuenta con algunos elementos adicionales como son: (Ver Figura 1.2) (6):

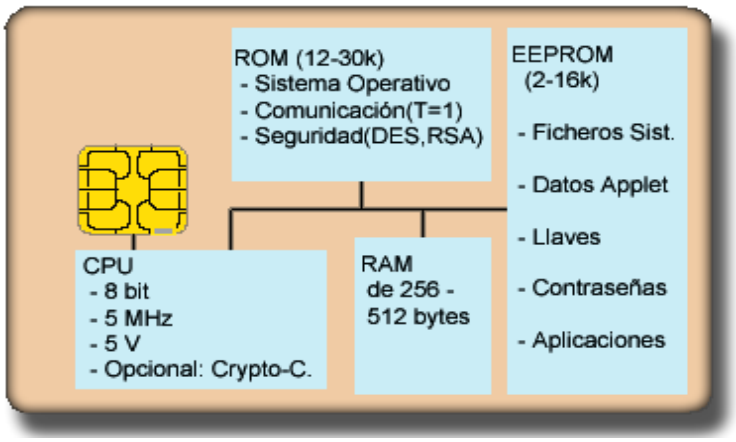


Figura 1.2. (Componentes de una tarjeta inteligente).

- ✓ **ROM**: Read Only Memory**.**

- ✓ **EEPROM**: Electrical Erasable Programmable Read Only Memory.
- ✓ **RAM**: Random Access Memory.
- ✓ **I/O:** Puerto de Entrada/Salida.

El microprocesador y la memoria están fabricados sobre el mismo chip, lo cual hace difícil y caro interceptar las señales que se intercambian entre el procesador y la memoria, proporcionando así una alta seguridad física de los datos almacenados en la memoria.

Memoria ROM.

La memoria ROM es grabada durante la fabricación de la tarjeta y es utilizada para almacenar el Sistema Operativo, datos y aplicaciones de usuarios fijas. Una vez emitida la tarjeta no se puede volver a grabar información en la ROM.

"*Una memoria ROM es aquella que se puede escribir una sola vez y sus datos no se pueden borrar".* (8)

Memoria EEPROM.

Esta memoria es utilizada para gravar información persistente dentro de la tarjeta, ya que preserva el contenido aunque la alimentación se apague. La EEPROM puede ser modifica durante el uso de la tarjeta y los usuarios pueden gravar ahí sus aplicaciones (applets).

"Una EEPROM se borra sometiéndola a radiación ultravioleta. Las tarjetas telefónicas antiguas poseen este tipo de memoria, pero para garantizar la inviolabilidad de la tarjeta, el chip está recubierto de resina opaca que impide el acceso de dicha luz, con lo cual, "en principio", es imposible borrar los datos de la EEPROM. Pero si por algún motivo conseguimos que la luz ultravioleta llegase al chip, lo que haríamos sería borrar por completo los 256 bits de la memoria". (8)

Una gran limitación de la EEPROM es que sufre de desgaste y con la tecnología disponible un bit después de 100,000 escrituras o más deja de ser confiable.

Memoria RAM.

Esta memoria es utilizada para almacenar valores u objetos temporales que los applets necesitan mientras son ejecutados. La RAM es una memoria que no almacena los datos una vez que se quita la alimentación o sea no es persistente.

Puerto de Entrada/Salida.

El puerto de entrada y salida normalmente consiste en un simple registro, a través del cual la información es transferida bit a bit**.**

Contactos de la tarjeta.

Las tarjetas inteligentes poseen ocho contactos en su chip (Figura 1.3), los cuales proporcionan la alimentación y señal de reloj y le permiten recibir y transmitir datos. (8)

*Vcc***:** se utiliza para suministrar la alimentación al chip. El voltaje que se aplica es 3 o 5 voltios, con una desviación máxima del 10 por ciento.

RST: se utiliza para enviar la señal de "reset" al microprocesador.

El microprocesador de la tarjeta inteligente no posee reloj interno. A través del contacto *CLK* se proporciona una señal de reloj externa a partir de la cual se deriva la señal de reloj interno.

CLK: el "reloj" determina la velocidad de funcionamiento de la tarjeta.

*GND***:** es la conexión de masa.

*Vpp***:** se utiliza en tarjetas antiguas para proporcionar el voltaje necesario para programar la EEPROM. En las tarjetas actuales este contacto no se utiliza porque el voltaje se genera internamente.

I/O: se utiliza para transferir datos entre la tarjeta y el dispositivo lector en modo semi-duplex.

RFU: Reservado para su uso en el futuro.

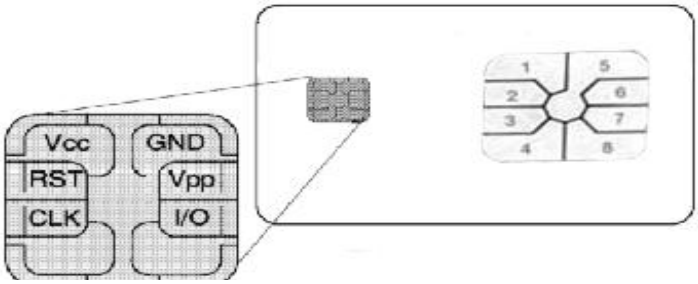


Figura 1.3. (Contactos de una tarjeta inteligente).

1.6.3 Tarjetas Inteligentes sin Contacto.

Estas tarjetas son similares a las de contacto con respecto a lo que pueden hacer y a sus funciones pero utilizan diferentes protocolos de transmisión, el chip se comunica con un lector de tarjetas, puesto en cada estación, mediante inducción[5] transfiriendo información, a una tasa de transferencia que fluctúa entre 106 y 848 Kb/s, no utilizan contacto galvánico sino de interface inductiva. Poseen además del chip, una antena de la cual se valen para realizar transacciones. Son muy utilizadas en las transacciones que tienen que ser realizadas muy rápidamente. (6)

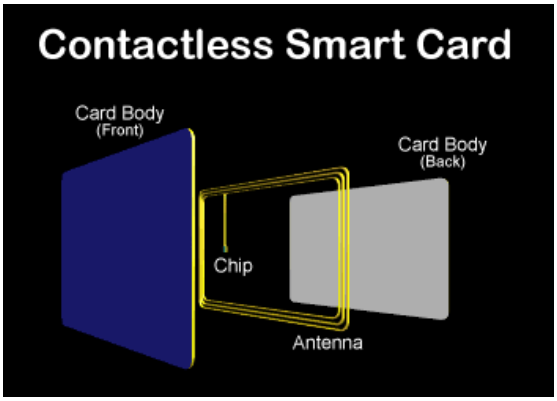


Figura 1.4. (Composición de una tarjeta inteligente sin contacto).

Esta tecnología ofrece ventajas con respecto a la de las tarjetas de contacto. Una de las principales desventajas de las TI con contactos es el deterioro de la superficie de sus contactos. Este problema se resuelve con las TI sin contactos, debido, a que carecen de contactos. Otra de las ventajas es la de no tener que introducir la tarjeta en un lector.

5 Inducción: Fenómeno que origina la producción de una diferencia de potencial eléctrico (o voltaje) en un medio o cuerpo expuesto a un campo magnético variable.

"Este tipo de tarjetas se comunican por medio de radiofrecuencias. Según la proximidad necesaria entre tarjeta y lector, existen dos tipos:

***Tarjeta cercana:** Debe estar a unos pocos milímetros del lector para que sea posible la comunicación.*

***Tarjeta lejana:** la distancia varía entre centímetros y unos pocos metros".* (9)

Alimentación.

"Desde el punto de vista de cómo se alimentan, existen dos tipos:

- *Uno en el cual la tarjeta incorpora junto al chip una batería que alimenta a los circuitos.*
- *Otro tipo que incorpora un hilo metálico incrustado. Este hilo se somete a un campo electromagnético variable que a su vez induce una corriente eléctrica capaz de alimentar los circuitos de la tarjeta"* (9).

1.6.4 Tarjetas híbridas y duales.

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

Una tarjeta de interfaz dual es similar a la tarjeta híbrida en que la tarjeta presenta ambas interfaces con y sin contacto. La diferencia más importante es el hecho de que la tarjeta de interfaz dual tiene un solo circuito integrado. Un ejemplo es la Oberthur Cosmo Card Dual-Interface. (10)

1.7 Lectores de Tarjetas Inteligentes de Contactos.

Un lector de tarjetas es un dispositivo con una interfaz que permite la comunicación entre una tarjeta y otro dispositivo. Los terminales se diferencian unos de otros en la conexión con el ordenador, la comunicación con la tarjeta y el software que poseen, (Ver Figura 1.5). (10)

1.7.1 Tipos de lectores de Tarjetas Inteligentes:

- **Lectores conectados a un PC:** son lectores fabricados para ser usados conectándolo a un computador, esta conexión puede ser a través de un puerto serie, USB, PCMCIA, etc.
- **Lectores conectados a un equipo específico:** Son lectores que se pueden instalar (previo fabricación y diseño) en un aparato determinado para cumplir con una función. Estos lectores se pueden instalar en:
    - Cajeros automáticos.
    - Máquinas expendedoras.
    - Parquímetros.
    - Puertas (control de acceso).
- **Lectores Portátiles:** Son dispositivos que no necesitan de otro aparato para cumplir su función. Generalmente poseen todos los recursos integrados como baterías, memoria, etc.

1.7.2 Lector escogido.

SmartLp3, (Ver Figura 1.5).

¿Por qué este lector?

- Lee y escribe todas las tarjetas inteligentes con microprocesador de la ISO 7816-1, 2, 3, 4, T=0 y T=1.
- Soporta múltiples plataformas de PC.
- Soporta múltiples lenguajes de programación.

Figura 1.5. (Lector de Tarjetas Inteligentes SmartLp3).

1.8 Protocolos de Comunicación.

1.8.1 APDU

El envío y recepción de datos en una tarjeta inteligente se realiza a través de un formato de paquetes llamados **APDU** (Application Protocol Data Units).

Existen dos tipos de APDU, de comando o de respuesta, con distintos formatos:

- **APDU de Comandos.**

  CLA: identifica que el request responde al estándar ISO-7816

  INS: código de la instrucción

  P1: primer parámetro

  P2: segundo parámetro

  L_c: número de bytes en el campo de datos

  Data: datos

  L_e: número máximo de bytes esperados en el campo de datos del APDU de respuesta

- **APDU de Respuesta.**

  Data: cuerpo de datos

SW_1: primer byte de la palabra de estado

SW_2: primer byte de la palabra de estado

La idea de la palabra de estado, es reportar códigos de retorno en el caso de que se produzcan errores o excepciones.

1.8.2 Comunicación con la Tarjeta.

La comunicación desde y hacia la tarjeta inteligente se lleva cabo por el contacto C7 (figura 1.3), de modo half-duplex. Lo que significa que sólo puede existir comunicación en un sentido, o sea desde la tarjeta o hacia la tarjeta.

"La comunicación siempre es iniciada por la terminal, lo que significa que la interacción entre la tarjeta y la terminal es del tipo cliente-servidor. (Ver Figura 1.6)

Una vez que la tarjeta es insertada en el lector, ésta le proporciona la corriente y el voltaje para funcionar. La tarjeta entonces se reinicia (power-on-reset), y envía un ATR (Answer To Reset) a la terminal. La terminal realiza un análisis sintáctico del ATR, donde obtiene varios parámetros y envía a la tarjeta una instrucción inicial. La tarjeta genera entonces una respuesta y la envía a la terminal. La interacción cliente-servidor continúa de la misma manera hasta que los procesos terminan y la tarjeta es removida de la terminal.

La capa física para el proceso de transmisión está especificado en el estándar ISO / IEC 7916-3. En ese estándar se encuentran definidos los niveles de voltaje para los cuales la señal es interpretada como un 1 o como un 0 lógicos.

Existen varios protocolos diferentes para el intercambio de información entre la tarjeta y la terminal. Estos protocolos están identificados mediante los caracteres "T=" más un número, como se muestra en la tabla siguiente:" (6)

1.8.3 Protocolos.

Protocolo	Descripción
T0	Comunicación asíncrona, half-duplex, orientada a bytes
T1	Comunicación asíncrona, half-duplex, orientada a bloques
T2	Comunicación asíncrona, full-duplex, orientada a bloques

T3	Full-duplex
T4	Comunicación asíncrona, half-duplex, orientada a bytes (expansión del protocolo T = 0)
T5 - T13	Reservados para su uso en el futuro
T14	No es un estándar ISO.
T15	Reservado para su uso en el futuro

Tabla 1.1: Protocolos de comunicación entre tarjetas y terminales.

Los dos protocolos más comunes actualmente son T=0 y T=1, de los cuales el más utilizado es T=0.

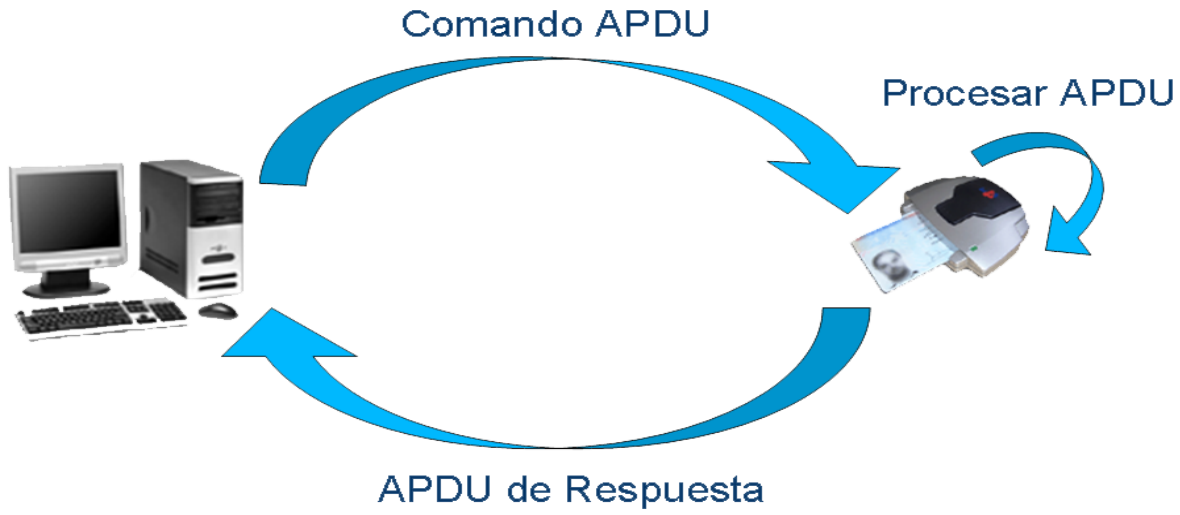


Figura 1.6: Comunicación con la tarjeta.

1.9 Características generales del Sistema Operativo.

"El sistema operativo de una tarjeta inteligente soporta un pequeño conjunto de instrucciones a través del cual se interactúa con la tarjeta. ISO 7816-4 estandariza un amplio rango de instrucciones en forma de APDUs. El sistema operativo de una tarjeta puede soportar todas o algunas de estas APDUs, así como nuevas instrucciones que añada el fabricante". (6)

1.9.1 ¿Por qué Tarjetas inteligentes multi aplicación?

El objetivo principal de las TI multiaplicación es almacenar en una sola tarjeta todas las aplicaciones posibles para así reducir el número de tarjetas en manos del usuario y así eliminar el problema que

trae consigo el uso de tarjetas de banda magnéticas. Las tarjetas telefónicas públicas, tarjetas médicas que almacenan las historias clínicas son ejemplos de tarjetas inteligentes de memoria, pero que traen consigo el mismo problema que el uso de las tarjetas magnéticas, el hecho de que el usuario cuente con una tarjeta para cada aplicación.

"…las tarjetas inteligentes tienen la capacidad de integrar todas esas aplicaciones juntas para formar una tarjeta multiaplicación utilizando el procesador y los espacios de almacenamiento de memoria. Sin embargo este tipo de integración siempre está limitado más por algunos elementos logísticos que por las capacidades técnicas." (11)

Sistemas Operativos Multiaplicación para tarjeta inteligente (MACOS)

- **JavaCard:** Para programación desarrollada en Java.
- **MultOS:** Es el primer COS (Chips Operating System) para tarjeta inteligente que incluye las siguientes características: es abierto, proporciona una alta seguridad y es multiaplicación.
- **Windows para Smart cards:** Sistema operativo de Microsoft para tarjeta inteligente.

1.9.2 Tareas del Sistema Operativo.

"El Sistema Operativo contenido en la tarjeta inteligente se encarga de las siguientes tareas:

- *Transmisión de información a través de la interfaz de comunicación serial.*
- *Carga, operación y administración de aplicaciones.*
- *Procesamiento y control de ejecución de instrucciones.*
- *Administración de la memoria (acceso a la información y manipulación de archivos).*
- *Administración y ejecución de algoritmos criptográficos.*

El tamaño típico de un sistema operativo se encuentra entre los 3 y los 24 Kbytes. Esta variación en el tamaño es debida a que algunas tarjetas son fabricadas para aplicaciones específicas, mientras que otras tienen la capacidad de almacenar diferentes aplicaciones.

Ya que la memoria en este tipo de dispositivos es un recurso muy limitado, no todas las instrucciones y las estructuras de datos se encuentran implementadas en todos los sistemas operativos. Por esta razón, en los estándares ISO 7816-4 y END 726-3 se crearon los llamados "perfiles", que especifican los requerimientos mínimos de estructuras de datos e instrucciones que un sistema operativo para una tarjeta inteligente debe implementar". (11)

1.10 Estándares de la ISO-7816.

En 1987 se publicó el primer estándar para la industria de tarjetas inteligentes, ISO-7816, con el que se intentaba solucionar el problema de interoperabilidad de las tarjetas inteligentes. Por medio de este estándar se establece la forma y dimensiones de las tarjetas, el significado y localización de los contactos del circuito integrado y el protocolo de comunicación de la tarjeta.

La tarjeta inteligente más básica cumple los estándares de la serie ISO 7816, partes 1 a 10. Este estándar detalla la parte física, eléctrica, mecánica y la interfaz de programación para comunicarse con el microchip.

1.10.1 Descripción de cada una de las partes de la ISO 7816:

- *"7816-1: Características Físicas.*
- *7816-2: Dimensiones y ubicaciones de los contactos*
- *7816-3: Señales Electrónicas y Protocolo de Transmisión*
- *7816-4: Comandos de intercambio inter-industriales*
- *7816-5: Sistema de Numeración y procedimiento de registración*
- *7816-6: Elementos de datos inter-industriales*
- *7816-7: Comandos inter-industriales y Consultas Estructuradas para una Tarjeta*
- *7816-8: Comandos inter-industriales Relacionados con Seguridad.*
- *7816-9: Comandos adicionales inter-industriales y atributos de seguridad.*
- *7816-10: Señales electrónicas y Respuesta al Reset para una Smart Card Síncrona.*

- *Una descripción para las smart cards sin contacto está descrito en el estándar ISO 14443".* (4)

1.11 Utilización de las Tarjetas Inteligentes.

Las tarjetas inteligentes fueron desarrolladas con el objetivo de almacenar información e interactuar con la información contenida en ellas. Estas tarjetas estas dejando atrás a las conocidas tarjetas de banda magnética, debido a su capacidad de poder modificar el contenido y de realizar múltiples grabaciones, sin temor a perder la información contenida en ellas.

Debido a las ventajas que estas ofrecen, se ha ido observando a nivel mundial un incremento de la utilización de las TI desde su aparición. Hoy en día suelen utilizarse para implementar módulos de seguridad y entre sus principales aplicaciones se encuentran los sectores bancarios, de telefonía móvil y de comercio electrónico, aunque son muy utilizadas en aplicaciones de la salud.

El uso de la TI ya está probado, algunos países como Francia, Bélgica y los Estados Unidos, están utilizando esta tecnologías, para el almacenamiento de la información de salud y como identificación personal.

"En Bélgica más de un millón personas disponen de carné de identidad electrónicos basados en la tecnología JavaCard, actualmente se están emitiendo unos 150.000 carné al mes y se espera que para finales de 2009, 8,2 millones de ciudadanos mayores de 12 años tengan su carné de identidad". (12)

1.12 Aplicaciones.

La realización de software asociado a este nuevo entorno permite diversidad de aplicaciones comerciales. El primer gran mercado que utilizó las tarjetas con chip fueron las tarjetas telefónicas y las tarjetas bancarias.

Algunos tipos de aplicaciones con tarjetas inteligentes son:

- Monederos Electrónicos.
- Control de Seguridad de Acceso.
- Tarjetas Telefónicas.

- Tarjetas de Salud.
- Tarjetas de Seguro Social.
- Pagos seguros por Internet.
- Tarjetas de Crédito/Debito.
- Transporte.

1.13 JavaCard.

Dentro de la categoría de tarjeta inteligente con microprocesador se encuentran las llamadas JavaCard o Java Smart Card. Una JavaCard es una tarjeta inteligente capaz de ejecutar programas desarrollados en Java. *"La primera JavaCard en salir al mercado fue producida por Schlumberger*[6]*, aún antes de que Sun fijara el estándar".* (13)

Esta tecnología combina parte del lenguaje de programación Java con un entorno de ejecución optimizado para Tarjeta Inteligente y similares. El objetivo de la tecnología JavaCard es llevar los beneficios del desarrollo de software en Java al mundo de las Tarjeta Inteligente y permitir el desarrollo de aplicaciones en estas. Las principales complicaciones tienen que ver con lo limitado de los recursos de hardware.

"Los componentes principales dentro de una JavaCard son el microprocesador y las memorias. La arquitectura básica de una JavaCard consiste de Applets, JavaCard API, JavaCard Virtual Machine (JCVM) JavaCard Runtime Environment (JCRE) y el sistema operativo nativo de la tarjeta". (8) (Ver Figura 1.6)

[6] Grupo industrial internacional que ofrece productos y servicios. Desarrolla y fabrica las tarjetas (con y sin chips) y los terminales asociados que permiten optimizar la seguridad en las transacciones electrónicas.

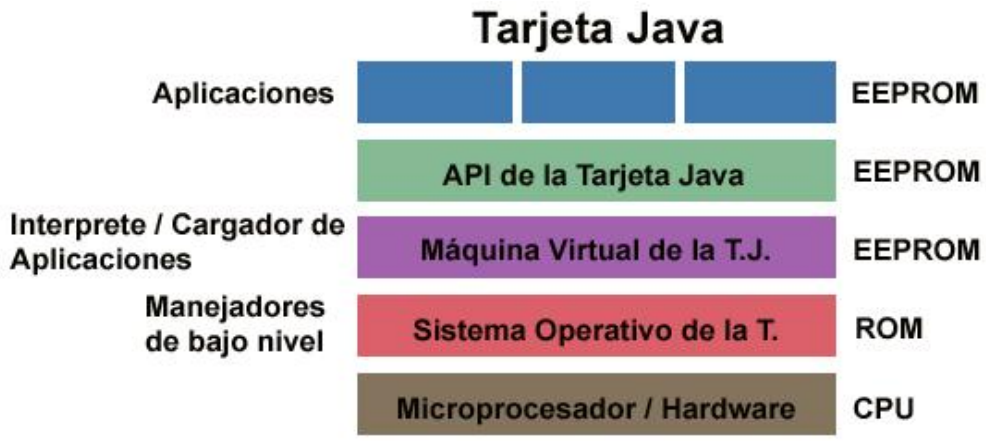


Figura 1.7: Estructura de una Java Card.

1.13.1 Componentes de una JavaCard.

- ***"JavaCard Virtual Machine (JCVM).***

Define la máquina virtual y el lenguaje de programación Java adecuado a las tarjetas inteligentes.

- ***JavaCard Runtime Environment (JCRE).***

Describe el comportamiento en ejecución de JavaCard, incluyendo la gestión de memoria y de las aplicaciones (applets).

- ***Java Card Application Programming Interface (API).***

Describe los paquetes y clases Java para programar aplicaciones en tarjetas inteligentes." (14)

1.13.2 Lenguaje JavaCard.

"Debido a la restricción de memoria y de capacidad de procesamiento de las tarjetas inteligentes, la plataforma JavaCard soporta sólo un limitado subconjunto de los elementos del lenguaje de programación Java". (6)

"Sin embargo, se puede utilizar un compilador de Java para compilar ficheros fuente JavaCard, cambiando las clases estándar de JDK por las del entorno JavaCard". (8)(Tabla 1.3).

Paquetes	**Descripción**

Java.lang	Subconjuto de java.lang de java.
Java.frameword	Funcionalidad basica para applets.
javacard.security	Funciones criptográficas.
javacardx.crypto	Extensión de clases criptográficas.

Tabla 1.3: Paquetes JavaCard.

1.13.3 Máquina Virtual de JavaCard.

"La Máquina Virtual de JavaCard (JCVM) es una versión de la Máquina Virtual de Java adaptada para tarjetas inteligentes. Debido a que los recursos disponibles en las tarjetas son escasos, JCVM se ha dividido en dos partes: una que se ejecuta en la tarjeta, el intérprete, y otra que se ejecuta fuera de ella, (por ejemplo en un PC), el conversor." (6)

La JCVM esta activa en la tarjeta mientras la tarjeta este conectada al lector, una vez quitada la alimentación, la JCMV deja de funcionar temporalmente hasta que no es conectada nuevamente, donde recupera toda la información almacenada en la tarjeta.

La conversión elimina una cantidad significativa de datos relacionada con la descarga dinámica de clases en tiempo de ejecución. La plataforma JavaCard no necesita soportar esta descarga dinámica ya que el propósito principal de una tarjeta inteligente es evitar la necesidad de conexiones on-line.

En lugar de la descarga dinámica de clases, todas las clases de un paquete JavaCard (librerías y aplicaciones) se descargan en la tarjeta al mismo tiempo.

Para ello, las clases de un paquete son convertidas y encapsuladas en un fichero CAP. El fichero CAP contiene una representación binaria ejecutable de las clases de un paquete, es decir, es la forma en la que el software se descargaría a la tarjeta y que el sistema de la tarjeta interpretaría y ejecutaría. Este formato está optimizado para obtener un mejor rendimiento del sistema JavaCard y minimizar el tamaño de los ficheros descargados a la tarjeta. Para ello, el conversor realiza los siguientes procedimientos de optimización:

- *Debido a que, por defecto, JavaCard soporta sólo aritmética de tipo short, se utilizan instrucciones que operan con shorts en vez del conjunto de instrucciones que operan con enteros propia de Java. De esta forma se salva espacio y se consigue un mejor rendimiento del sistema JavaCard.*

- *Para limitar el tiempo de descarga de aplicaciones a la tarjeta, se requiere minimizar el tamaño de los ficheros que se descargarían a través del enlace de comunicaciones con la tarjeta, y el número de escrituras a la memoria EEPROM durante la descarga e instalación de applets. Para ello se convierten las referencias simbólicas de clases, métodos y variables a identificadores tipo short que pueden ser manejados de forma más eficiente por la tarjeta. Cada identificador solamente es válido de forma relativa a su paquete.*

La parte de la Máquina Virtual de JavaCard que reside en la tarjeta, el intérprete, se encarga de proporcionar el soporte para el lenguaje Java en la tarjeta, de forma que los applets escritos en JavaCard pueden ejecutarse independientemente del hardware de la tarjeta. El intérprete realiza tres tareas fundamentales:

- *Ejecuta las instrucciones indicadas por el código de bytes (fichero CAP).*
- *Controla la asignación de memoria y la creación de objetos.*
- *Toma parte en las tareas de seguridad.*

El intérprete ejecuta el código que encuentra en los ficheros CAP, pero no es el encargado de descargar los ficheros en la tarjeta para ejecutarlos. Para descargar e instalar los ficheros CAP en la tarjeta, la plataforma JavaCard utiliza una unidad especial llamada instalador. El instalador reside en la tarjeta y coopera con un programa de instalación fuera de la tarjeta que, a través del dispositivo lector, le transmite el código binario ejecutable de un fichero CAP. El instalador escribe el código en la memoria EEPROM, realiza el linkeado con otras clases que residan ya en la tarjeta, y crea e inicializa las estructuras de datos que el Entorno de Ejecución de JavaCard (JCRE) utiliza internamente". (7).

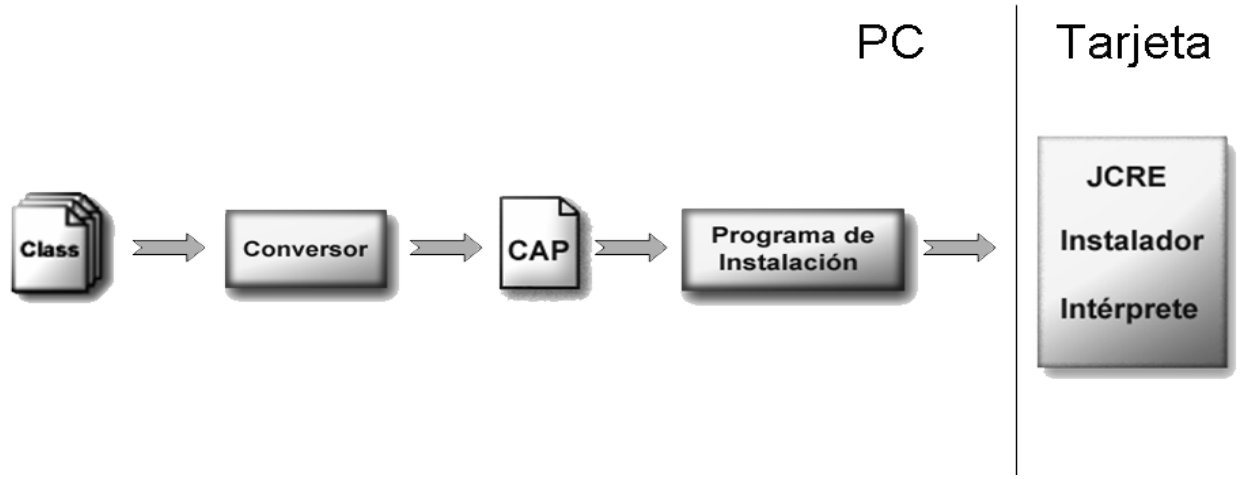


Figura 1.8: Instalación de un applet.

1.13.4 JavaCard Runtime Environment (JCRE).

La clase javacard.framework.Applet define cuatro métodos públicos que son utilizados por el JCRE para hacer funcionar las aplicaciones.

- **Método install(byte[], short, byte)**

Cuando el método Install () es llamado, el applet no ha sido instanciado todavía. Este método llama al constructor de la subclase Applet para registrar una instancia del applet, crear los objetos que el applet necesita para su ejecución, y por ultimo instalar el applet con el método install (). Típicamente, un applet crea varios objetos, los inicializa con valores predefinidos, cambia el estado de algunas variables internas y llama al método Applet.register () o al Applet.register (byte[], short, byte) para especificar el AID (applet IDentifier como se definió en la ISO 7816-5) para ser usados para su selección. Esta instalación es considerada exitosa cuando la llamada al Applet.register() se completa sin ninguna excepción. La instalación es considerada no exitosa si el método install () no llama al método Applet.register (), o si se lanza una excepción en el método install ().Si la instalación no es exitosa, la JCRE realizar una limpieza cuando recobra el control. Esto significa que todas las actualizaciones condicionales del almacenamiento persistente deben ser retornadas al estado que tenían previo a la llamada del método install (). Si la instalación fue exitosa, la JCRE marca al applet como disponible para seleccionar. (6)

- **Método select()**

En un tarjeta pueden coexistir varios applets estos se encuentran en un estado suspendido hasta que son seleccionados. La selección ocurre cuando la JCRE recibe un comando SELECT FILE APDU en el cual se especifica el AID del applet que se desea seleccionar. Si al seleccionar un applet se encuentra otro applet seleccionado, el JCRE es el encargado de deseleccionar dicho applet con el método deselect (), y luego invoca al método select () del applet cuyo AID fue especificado. Un applet puede rechazar la selección en cuyo caso el JCRE es el responsable de responder adecuadamente al CAD (Card Acceptance Device). En caso de fallar la selección, el estado del JCRE es cambiado para indicar que ningún applet fue seleccionado. Si el método select () retorna true entonces se llama al método process (), del applet seleccionado para que lo procese y devuelva al CAD la información que sea pertinente. (6)

- **Método process(APDU)**

Todas las APDUs son recibidas por JCRE y pre-procesadas, este invoca al método process (APDU) del applet seleccionado pasándole como parámetro el COMMAND APDU recibido.

En caso de que la ejecución finalice correctamente, el applet sólo debe encargarse de cargar en el RESPONSE APDU la información que va a devolver, si la hay. El JCRE es responsable de setear los SW del RESPONSE APDU al valor especificado para ejecución exitosa (0x9000, de acuerdo a lo especificado en el ISO 7816). Durante el proceso de un APDU, el applet puede levantar una ISOException con los SW apropiados. (6)

- **Método deselect()**

Cuando el JCRE recibe un comando SELECT FILE APDU donde se le especifica el AID de un applet, (aún cuando el AID del applet a seleccionar coincida con el del applet seleccionado), el JCRE llama al método deselect () del applet que se encuentra seleccionado. El método deselect () permite al applet llevar a cabo las operaciones de limpieza que puedan ser requeridas para permitirle a otros applet su ejecución. (6)

- **Método uninstall()**

Este método es definido en la interfaz javacard.framework.AppletEvent. Cuando el JCRE se está preparando para borrar un instancia de un applet, el JCRE llama al método uninstall (), si es implementado por el applet, para informarle a este de la petición de borrado. En el retorno de este

método, el JCRE chequea por referencias de dependencias antes de borrar la instancia del applet. Este método es llamado múltiples veces para cada intento de borrado de un applet. (6)

1.13.5 Entorno de Ejecución JavaCard

El JCRE es el equivalente al Sistema Operativo de la tarjeta, ya que se ejecuta en la tarjeta y es el responsable de la gestión de recursos de esta, la ejecución de applets y la seguridad entre los applets.

El Entorno de Ejecución de JavaCard (JCRE) se sostiene sobre los siguientes componentes (Figura 1.6):

- La Máquina Virtual de JavaCard (el intérprete)
- Las clases API de JavaCard
- Extensiones específicas del fabricante
- Las clases de sistema

Los métodos nativos dan soporte a la JCVM y a las clases del sistema, y son los responsables de manejar, los protocolos de comunicación y la asignación de memoria, la criptografía, etc. Estas clases son las encargadas de gestionar las transacciones, la comunicación entre los applet y las aplicaciones fuera de la tarjeta, así como controlar la creación y selección de los applets. (14)

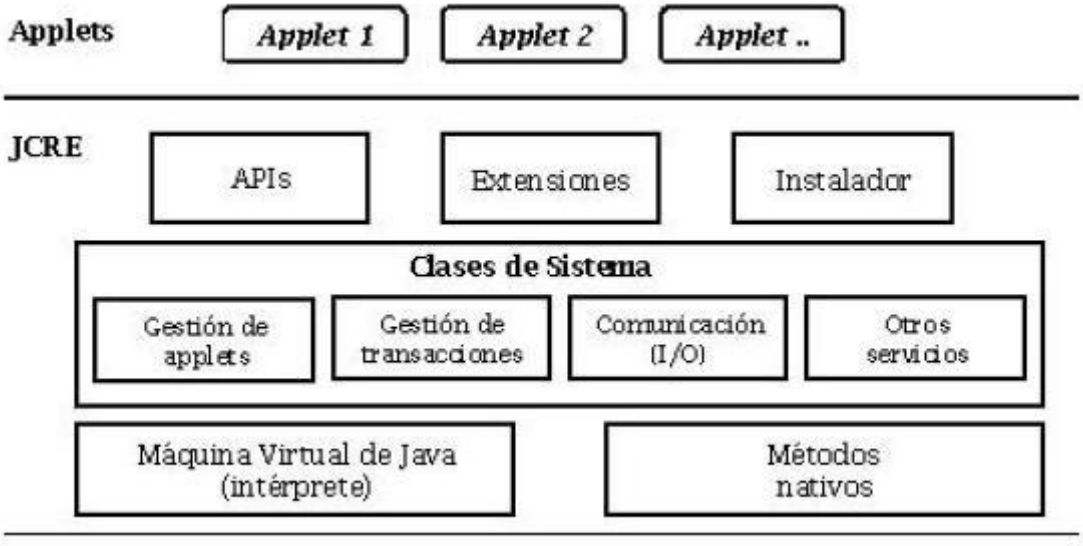


Figura 1.9: (Hardware y Sistema Nativo de una Tarjeta Inteligente).

"El instalador permite descargar los applets a la tarjeta de forma segura después de la fabricación de la tarjeta. El instalador es un elemento opcional, si no se implementa, el software de la tarjeta, incluidos los applets, debe ser escrito en memoria ROM durante el proceso de fabricación de la tarjeta.

Después de que la tarjeta ha sido insertada en el dispositivo lector, que le proporciona las señales de alimentación al, reloj y al reset, el JCRE entra en un bucle a la espera de recibir comandos APDU a través de su interfaz de comunicación serie. Cuando recibe un comando, el JCRE selecciona un applet, si así se lo indica el comando, o envía el comando a un applet previamente seleccionado para que lo procese convenientemente. El applet, entonces, envía la respuesta a través de otra APDU y cede el control al JCRE a la espera de nuevos comandos". (14)

Entre las características destacadas del JCRE hay que mencionar las siguientes:

- **Objetos persistentes y transitorios.** Los applet pueden crear objetos en la RAM y la EEPROM, los objetos creados en la RAM se usan para la seguridad o para tener un mejor rendimiento, estos son destruidos una vez quitada la alimentación. El propósito de este requisito es permitir que los objetos transitorios sean utilizados para almacenar llaves de la sesión.
- **Operaciones y transacciones atómicas.** Definen como la tarjeta maneja la información persistente después de una parada. Una transacción es un sistema lógico de las actualizaciones de datos persistentes, es importante que las transacciones sean atómico: lo que significa que todas las zonas de información son actualizadas, o ningunas lo son. Si la transacción no termina correctamente el JCRE proporciona ayuda para restaurar los datos de la tarjeta a su estado original de la pre-transacción.

  Firewall. Una tarjeta java puede contener varios applets, cada applet tiene su propio espacio de memoria, o sea, están protegidos por un Firewall lo que significa que un applet no puede tener acceso a los campos o a los objetos de un applet en otro contexto.

  Un applet puede obtener información de otro applet, pero el applet de petición debe satisfacer ciertas reglas antes de poder acceder a la información, estas reglas son proporcionadas por el JCRE a través del API de JavaCard, el cual contiene mecanismos bien definidos para accedes de forma segura a los métodos de otros applets.

  El Firewall también proporciona seguridad ante el código incorrecto, para que los applet no puedan ser alcanzados por dicho código. (Ver Figura 1.7). (14)

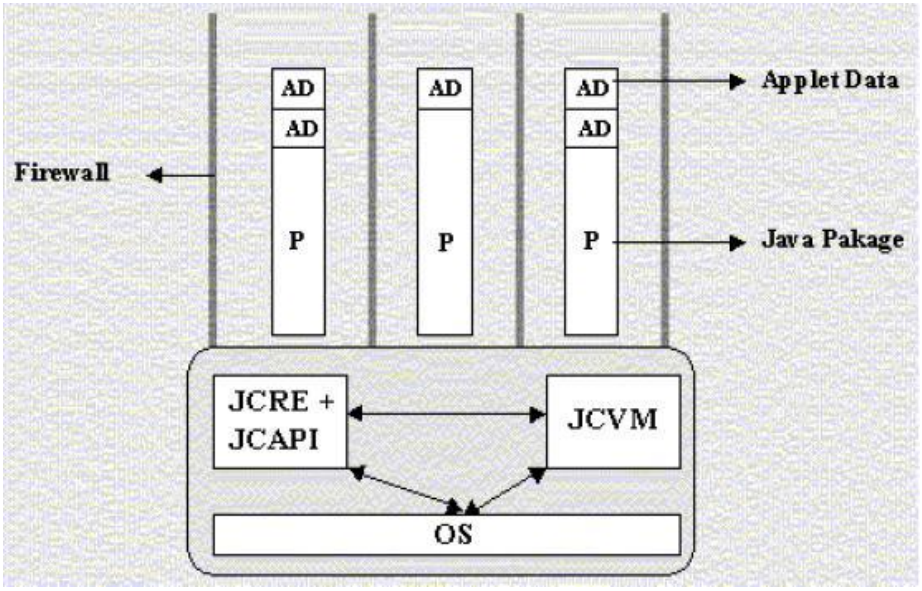


Figura 1.10: Firewall de una Tarjeta Inteligente.

1.13.6 Seguridad.

Seguridad física.

Actualmente muchas personas prefieren a las Tarjetas Inteligentes, ya que estas son muy seguras y difíciles de atacar, física o lógicamente, ya que estas disponen de mecanismos de protección ante diferentes ataques como son: detección de ciclos de reloj anormales en frecuencia, retiro de la cubierta de resina epoxi o exposición del microprocesador a luz ultra violeta. (15)

Sin embargo, en ocasiones se ha logrado obtener información a través de diversos medios, estos ataque sucedieron hace mucho tiempo y los fabricantes asegura que sus componente son cada vez son más seguros lo que deja sin posibilidades de obtener información a los atacantes.

Seguridad lógica.

Actualmente los usuarios finales poseen gran cantidad de tarjetas (una para cada aplicación), estos desean reducir este número, y las Tarjetas Inteligentes Multiaplicación le proporcionan esta ventaja.

Las Tarjetas Inteligentes brindan la posibilidad de cooperación entre diferentes empresas o ministerios, para albergar en una misma tarjeta diferentes servicios al usuario final. (15)

1.14 Principales Fabricantes.

Gemalto (www.gemalto.com)

Schlumberger (www.slb.com)

Bull (www.bull.com)

Oberthur (www.oberthur.com)
Orga (www.orga.com)
Solaic (www.winforms.phil.tu-bs.de/winforms/company/solaic/solaic.html)
De la Rue (www.delarue.com)

1.15 Conclusiones.

En el transcurso de este capítulo se definió lo que es un sistema de identificación, los tipos de sistemas que existen, se describió la tecnología de las tarjetas inteligentes, especialmente de las JavaCard, se ha dado a conocer las diferentes tarjetas que existen, también se ha descrito el funcionamiento de las mismas y los protocolos que usan para su comunicación, para así lograr un mejor entendimiento de las mismas.

CAPÍTULO 2: ANÁLISIS CRÍTICO DE LOS SISTEMAS

Introducción.

En este capítulo se pretende analizar los resultados de la implantación de sistemas de identificación personal existentes en el mundo, identificar semejanzas y diferencias, evaluar las características de dichos sistemas que pueden ser aprovechadas en la informatización del proceso de identificación en Cuba.

2.1 Sistemas implantados en el mundo.

La implantación de sistemas de identificación nacional basados en la utilización de tarjetas inteligentes ha permitido que se reúnan una serie de experiencias, las cuales constituyen un buen punto de partida para aquellos países que pretendan aplicar esta tecnología. En este epígrafe analizaremos algunos de los ejemplos más significativos.

2.1.1 DNI electrónico en España.

Actualmente casi 10 millones de españoles poseen el DNIe que según el Real Decreto 1553/2005, de 23 de diciembre, regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica. La PKI que da soporte al DNIe tiene una AC raíz y tres ACs subordinadas a cargo de la Dirección General de la Policía (Ministerio del Interior). La DGP actúa también como Autoridad de Aprobación de Políticas responsable de aprobar la Declaración de Prácticas de Certificación, así como sus modificaciones.

La AC raíz sólo emite certificados de clave pública para sí misma y sus subordinadas. Éstas a su vez emiten certificados de clave pública a los ciudadanos, que se guardan en la tarjeta criptográfica que constituye el DNIe junto con sus claves privadas asociadas. El acceso a la tarjeta está protegido por una clave personal (PIN) que sólo el ciudadano debe conocer. Las claves privadas permanecen en la tarjeta y no pueden ser exportadas en ningún formato (12).

En Asturias, Aragón, La Rioja y Navarra. La validez para los certificados de los ciudadanos es de 2,5 años o hasta la renovación física de la tarjeta criptográfica. El plazo normal de validez de las tarjetas es 5 años, 10 años o permanente según la edad del solicitante. Cada operación archivada incluye fecha y hora. Todos los servidores del sistema del DNIe se sincronizan en fecha y hora utilizando como referencia la del Real Instituto y Observatorio de la Armada en San Fernando. El DNIe español

contiene además información biométrica del titular, en concreto la huella dactilar, la fotografía de la imagen facial (grabada con láser) y la firma digitalizada. La verificación del titular se realiza utilizando únicamente la huella dactilar, y esta operación sólo se realiza para desbloquear el DNIe producido por el uso incorrecto del mismo. Tipos de certificados y usos del DNIe. (12)

Por cada DNIe se emiten dos certificados con usos diferentes: certificado de autenticación y certificado de firma. El certificado de autenticación se usa para garantizar la identidad del ciudadano al realizar una transacción telemática. Las firmas hechas con la clave privada correspondiente a este certificado no implican compromiso del titular del DNIe con el contenido firmado. Este certificado puede ser utilizado, por ejemplo, como medio de identificación para la realización de un registro que permita la expedición de certificados reconocidos por parte de entidades privadas. (12)

El certificado de firma sirve para firmar trámites o documentos electrónicos. Al tratarse de un certificado reconocido y utilizarse la tarjeta criptográfica del DNIe como dispositivo seguro de creación de firma, permite la generación de firmas electrónicas reconocidas, equiparadas legalmente a la firma manuscrita. Las funcionalidades de autenticación y firma electrónicas del DNI están disponibles sólo para los titulares mayores de edad. En todo caso su activación tiene carácter voluntario, por lo que el ciudadano puede solicitar la revocación de los certificados emitidos como parte del proceso de expedición. (12)

Los certificados incluidos en las tarjetas de identidad electrónicas belgas (http://eid.belgium.be/) son emitidos por la autoridad de certificación denominada “Citizen CA” (CCA), operada por la sociedad anónima Certipost como proveedor de servicios de certificación1. Las funciones de identificación de los ciudadanos, tramitación de solicitudes de certificados o revocaciones, personalización y entrega de las tarjetas a los ciudadanos están delegadas en los ayuntamientos, que actúan como “Autoridades de Registro Locales”, junto con la empresa Zetes, fabricante de las tarjetas bajo contrato con la Administración. Entre marzo de 2003, fecha oficial de comienzo, y marzo de 2004 se desarrolló un proyecto piloto en el que se emitieron unas 70.000 tarjetas en 11 localidades. La emisión de tarjetas a gran escala comenzó en septiembre de 2004. Dos años después, en septiembre de 2006 se habían emitido ya 3,5 millones de tarjetas (aproximadamente la tercera parte de la población del país). El plazo para que el sistema esté completamente implantado en todas las localidades concluye en 2009. (12)

La información personal contenida en el DNIe belga es: fotografía de la imagen facial del titular, nombre, apellidos, género, fecha y lugar de nacimiento, nacionalidad, número de identificación

nacional, firma y fechas de expedición y caducidad. Toda esta información, así como la dirección del titular, está contenida en el chip del DNIe, excepto la fotografía. No contiene ninguna información biométrica. Como en el DNIe español, cada tarjeta de identidad belga contiene dos certificados separados con sus correspondientes parejas de claves, uno para autenticación y otro para firma electrónica, cuya activación es opcional para el ciudadano. Sin embargo, en Bélgica sólo el certificado de firma se emite como certificado cualificado. Aunque la tarjeta puede expedirse a menores de edad, el certificado de firma no puede activarse hasta que el titular ha cumplido 18 años. El certificado de autenticación se puede activar y utilizar a partir de los 6 años de edad. Otras diferencias son un mayor plazo de validez (5 años y 3 meses, frente a 2 años y medio en el caso español). La implantación de las tarjetas de identidad electrónica en Bélgica ha sido objeto de críticas que señalan problemas de privacidad. La ADAPID (ADvanced APplications for electronic IDentity cards in Flanders), consorcio de investigadores y representantes de la industria creado en 2003, publicó un informe en febrero de 2004 describiendo estos problemas y proponiendo un proyecto conjunto entre investigadores e industria para solucionar los problemas de privacidad. El proyecto comenzó en julio de 2005 con una duración de cuatro años y el objetivo de proponer un nuevo diseño para la 3ª generación de tarjetas de identidad que se espera se empezarán a distribuir a partir de 2008. Además el proyecto propondrá aplicaciones avanzadas de la tarjeta en sanidad y administración pública. Los requisitos de privacidad para el nuevo diseño incluyen: minimizar la cantidad de información que el titular de una tarjeta debe dar para comunicarse con una organización, poder identificarse ante cada organización con un pseudónimo diferente, que estos pseudónimos no se puedan relacionar entre sí y evitar que diferentes organizaciones puedan combinar sus datos sobre los ciudadanos. (12)

Por último, aunque aún en proyecto, Bélgica cuenta también con un nuevo pasaporte biométrico que cumplirá las especificaciones dictadas por la Organización Internacional de Aviación Civil (ICAO) y las regulaciones europeas relativas a este tipo de documentos. Este nuevo pasaporte, consta de un chip sin contactos que, además de la información del usuario, alberga también la firma digitalizada y la fotografía. La huella dactilar se contempla incorporarla más adelante. Este nuevo documento tiene una validez de 5 años. (12)

2.1.2 Tarjeta de identidad electrónica en Estonia

En enero de 2002 comenzó la emisión de tarjetas de identidad electrónica (http://www.id.ee/), coincidiendo con la fecha en que empezaban a caducar los primeros pasaportes estonios emitidos en 1992 y con validez por 10 años. Durante el primer año se emitieron 132.000 tarjetas y en octubre de 2006 se alcanzó 1 millón de tarjetas (la población total del país es de 1,35 millones) con un crecimiento

prácticamente lineal. Las tarjetas de identificación son obligatorias. El Estonian Citizenship and Migration Board (CMB) se encarga de tramitar las solicitudes, que pueden hacerse personalmente o por correo postal. La autoridad que emite los certificados, llamada AS Sertifitseerimiskeskus (SK), está formada por empresas privadas: dos bancos y dos operadores de telecomunicación. Las tarjetas, con los certificados emitidos por SK y personalizadas con los datos de los ciudadanos por otra empresa, TRÜB Baltic AS, se entregan a los titulares en las sucursales de los bancos mencionados. (12)

En caso de suspensión de un certificado, puede activarse de nuevo en una de estas sucursales. SK emite también certificados para tarjetas de uso interno en empresas. (En este caso la propia empresa actúa como autoridad de registro). Cada tarjeta contiene dos certificados cualificados con códigos PIN diferentes. Uno se usa para autenticación y cifrado. El otro, para firmas digitales con validez legal equivalente a la firma manuscrita. El algoritmo de firma es RSA con longitud de clave 1024 bits. La AC que emite los certificados se llama ESTEID-SK y su clave pública está certificada por la AC raíz denominada Juur-SK. Ambas autoridades tienen claves de 2048 bits. Los certificados son válidos durante 1100 días (aproximadamente tres años) y se incluyen en todas las tarjetas, pero los ciudadanos que no deseen utilizar sus funciones electrónicas pueden revocarlos. La única información personal que consta en los certificados es el nombre del titular y su número de identificación nacional único, ambos considerados de acceso público en Estonia. No obstante la tarjeta lleva impresa datos adicionales, como la fecha de nacimiento. Todos los datos impresos, salvo la foto y la firma manuscrita, pueden leerse en formato electrónico de un fichero guardado dentro de la tarjeta. El certificado de autenticación contiene, además del nombre y número de identificación del titular, una dirección de correo electrónico asignada por la Administración con el formato "nombre.apellido_NNNN@eesti.ee". Esta dirección está pensada para comunicaciones entre ciudadano y Administración, aunque puede usarse también entre particulares. El titular puede cifrar sus correos electrónicos y/o firmarlos digitalmente con la clave correspondiente a su certificado de autenticación, aunque sin el compromiso legal que implica el certificado de firma. A través de una página web, el usuario puede fácilmente configurar el reenvío de los mensajes que reciba en la dirección anterior a la cuenta de correo electrónico que desee. (12)

2.1.3 Tarjeta de identidad electrónica en Finlandia

Finlandia fue el primer país europeo en emitir tarjetas de identidad electrónica (http://www.fineid.fi/) a finales de 1999. La tarjeta FINEID lleva impresos datos del titular como el nombre, fecha de nacimiento, número de seguridad social y su foto. Sin embargo, salvo el nombre, los otros datos personales no se almacenan electrónicamente en la tarjeta. Cada tarjeta tiene dos certificados, uno

para autenticación y cifrado y el otro para firma electrónica. Cada uno se utiliza con un PIN diferente. Si el solicitante lo desea, puede incluir información médica en la tarjeta FINEID, con lo cual no necesita tener una tarjeta sanitaria separada (denominada KELA). Los certificados FINEID son emitidos por VRK, la autoridad de certificación del Population Register Centre (PRC) de Finlandia, supervisada por la Finnish Communications Regulatory Authority (FICORA). Las comisarías de policía actúan como autoridades de registro locales. Los ciudadanos deben identificarse al solicitar la tarjeta y, posteriormente, al recogerla. En caso de bloqueo de la tarjeta, se debe acudir de nuevo a la comisaría para desbloquearla con un código PUK. La tarjeta cuesta 40 € y su plazo normal de validez es de 5 años. Además de los certificados incluidos en las tarjetas de identidad [CPS-FI04], el PRC emite certificados a los ciudadanos para utilizar en tarjetas Visa Electron (estas tarjetas, que dan los mismos servicios que la de identidad y además servicios bancarios, se solicitan en una sucursal bancaria) y certificados para utilizar con la tarjeta SIM de un teléfono móvil (el ciudadano debe comprar la tarjeta SIM al operador móvil, TeliaSonera o Elisa, y registrarla en el departamento de policía). Los diferentes certificados que pueden emitirse al mismo ciudadano comparten un número de identificación único (FINUID) generado a partir de su número de seguridad social. El PRC emite también tarjetas de identidad para empleados de empresas u otras entidades, con las capacidades básicas de autenticación, cifrado y firma electrónica, más otras específicas como verificar el puesto que ocupa la persona, variar los datos visibles en la tarjeta o personalizar su aspecto según la imagen de la empresa. El PRC mantiene un directorio público con los certificados emitidos de cada tipo, así como las correspondientes listas de certificados revocados. La revocación puede solicitarse por teléfono llamando a un número gratuito. Las consultas de estado mediante OCSP no están disponibles hasta el momento. Hasta el 31 de marzo de 2003, el PRC mantenía una AC independiente para cada tipo de certificado, cada una con su correspondiente certificado raíz. Desde el 1 de abril de 2003, estas ACs pasaron a depender de una autoridad raíz común denominada “VRK Gov. Root CA” que firma los certificados del resto de autoridades [FINEID05]. Además en esa fecha comenzaron a expedir certificados cualificados, condición que no cumplían antes. (Hasta ahora VRK es la única autorizada para emitir certificados cualificados en Finlandia). Todas las ACs tienen claves de 2048 bits. Las claves de los ciudadanos son de 1024 bits. El algoritmo de firma utilizado es RSA con resumen SHA-1. En mayo de 2003, el PRC firmó un acuerdo de colaboración y armonización de prácticas de firma electrónica con la autoridad de certificación de Estonia, denominada SK (AS Sertifitseerimiskeskus). Ver sección 1.3.

A pesar de que la tarjeta FINEID lleva en funcionamiento desde 2000 y de la variedad de servicios a que pueden acceder con ella los ciudadanos (el PRC ha establecido la marca para identificarlos

fácilmente) y las empresas (ver http://www.fineid.fi), su crecimiento está siendo muy lento. Por ejemplo, desde 2000 hasta mediados de 2003 solo se habían emitido 16.000 tarjetas. (Como referencia, la población total del país en 2003 era de 5,2 millones de personas). A finales de septiembre de 2006 se habían emitido 120.500 tarjetas, de las cuales casi el 20% llevan integrada información médica. El ritmo de crecimiento durante el último año ha sido mayor: más de 30.000 tarjetas emitidas entre septiembre de 2005 y septiembre de 2006. Finlandia es el origen del grupo Porvoo, que toma su nombre de la ciudad de este país donde se creó el grupo en 2002. El grupo Porvoo es una iniciativa de cooperación internacional para promover sistemas de identidad electrónica ínter operables entre distintos países, basados en PKI y tarjetas electrónicas, que faciliten las transacciones electrónicas seguras, tanto en aplicaciones del sector público como de tipo privado. Actualmente, cuenta con unos 30 países representados de Europa, Asia y EE.UU. El grupo celebra dos reuniones al año. Las dos más recientes tuvieron lugar en Eslovenia en mayo de 2006 (ver http://porvoo9.gov.si/) y en Finlandia en noviembre de 2006 (ver http://www.porvoo10.net/). En la última reunión se presentó un informe resumen de la situación actual de los sistemas de identidad electrónica en Europa, Asia y EE.UU. (12)

2.1.4 Alemania

El 1 de noviembre de 2005 la República Federal de Alemania introdujo el nuevo pasaporte electrónico con datos biométricos, siendo uno de los primeros Estados miembros de la UE en poner en práctica el reglamento de la CE sobre la materia, que entró en vigor el 18 de enero de 2005. El chip sin contactos del pasaporte (accesible mediante radiofrecuencia) contiene de momento los datos convencionales y la fotografía del titular. A partir de marzo de 2007 también almacenará adicionalmente dos imágenes de la huella dactilar (http://www.ePass.de). Incorpora, además de autenticación pasiva y activa, Basic Access Control. Sigue por tanto las especificaciones ICAO y las normativas europeas. La modificación más importante para los ciudadanos que soliciten un pasaporte a partir del 1 de noviembre de 2005 afecta a la confección de las fotos de pasaporte: según las normas de la ICAO, competente en materia de estandarización, y la Unión Europea, se precisa en todo el mundo un nuevo tipo de foto de pasaporte para controles biométricos. Las fotografías no se toman, como venía siendo habitual para los pasaportes, de medio perfil sino de frente. El despliegue técnico al servicio de la seguridad y la protección de datos exige incrementar la correspondiente tasa de expedición del pasaporte. En Alemania un pasaporte electrónico con una validez de diez años cuesta 59 euros. En términos comparativos, Alemania se sitúa por tanto en el tramo inferior de la escala de precios. Para los pasaportes con una validez de cinco años, expedidos para personas menores de 26 años, la tasa se eleva a 37,50 euros. Por otra parte, el “Bundesamt für Sicherheit in der Informationstechnik” (BSI) ha

llevado a cabo numerosos estudios para evaluar las tecnologías biométricas utilizadas en documentos de identidad, en particular BioFace 1 & 2 y BioP I, basadas en cara, y BioFinger I basadas en huella dactilar. También se llevó a cabo un estudio (BioP II) en el que intervinieron 2000 personas durante 4 meses, analizando varias tecnologías biométricas, cara, huella e iris, en sistemas independientes, como así lo recomiendan las especificaciones ICAO. Los resultados pueden encontrarse en http://www.bsi.bund.de/literat/studien/biop/biop_2.htm. En resumen, se podría decir que el resultado que se obtiene de este trabajo es que el buen funcionamiento de un sistema biométrico de verificación depende de la frecuencia de uso que el ciudadano haga de él (en particular en iris se obtuvieron tasas de falso rechazo del 20% para usuarios que no utilizaron frecuentemente ese sistema). Estos resultados fueron cuestionados por J. Daugman, creador de la técnica biométrica mediante iris. (12)

2.1.5 Austria

A pesar de su nombre, la tarjeta de ciudadano ("Bürgerkarte") utilizada en Austria no es una tarjeta nacional de identidad electrónica, ni siquiera una tarjeta única. La "Bürgerkarte" es en realidad una definición de requisitos para procedimientos de identificación y firma electrónica que pueden implementarse en diferentes tarjetas inteligentes (tarjetas de seguridad social, tarjetas bancarias, tarjetas de identificación de funcionarios,...) y en otros dispositivos como teléfonos móviles, PDAs, dispositivos USB, etc. Por ejemplo, la "Bürgerkarte" establece como requisito para sus implementaciones la capacidad de generar y verificar firmas digitales, pero no impone el algoritmo a usar, que puede ser RSA, DSA o ECDSA. Las especificaciones "Bürgerkarte" se publicaron en agosto de 2002 (v1.1) y se revisaron en mayo de 2004 (v1.2). Las interfaces actuales de la "Bürgerkarte" con el usuario y con las aplicaciones están especificadas en [ACC04] y [ACC05] respectivamente. (12)

En http://www.buergerkarte.at/ se ofrece información sobre los servicios que se han ido implantando en los últimos años y las entidades que los prestan, tanto públicas (por ejemplo la tarjeta sanitaria "e-card") como privadas (por ejemplo la tarjeta "a.sign premium" emitida por el proveedor de servicios de certificación A.trust, el servicio "A1 signature" para generar firmas desde teléfonos móviles con SMS, tarjetas bancarias,...). Además de la multiplicidad de tarjetas y servicios citada, otro aspecto distintivo de la experiencia austriaca es el énfasis en la privacidad. En sus comunicaciones con la Administración el ciudadano utiliza Identificadores Personales específicos de sector (ssPI) que se calculan a partir de los datos guardados en su "Bürgerkarte". Esto se hace para evitar que se puedan relacionar entre sí las comunicaciones de una misma persona con distintos sectores de la Administración. Las entidades de la Administración están agrupadas en 9 sectores (por ejemplo: sanidad, hacienda,...), cada uno de los cuales tiene un identificador de sector diferente. Por su parte, cada "Bürgerkarte" almacena un

número personal secreto del ciudadano (sPIN) que se guarda en la tarjeta y no consta en ningún otro archivo. (No obstante, si es necesario el sPIN de un ciudadano se puede recalcular bajo supervisión de la Comisión de Protección de Datos de Austria). Cuando un ciudadano inicia un trámite con una entidad de la administración, se identifica son un ssPI calculado mediante una función hash de su sPIN y el identificador del sector. Este ssPI no puede relacionarse con otros ssPi de la misma persona para otros sectores ni con su sPIN. En caso de comunicarse con una empresa, el número de registro de ésta sustituye al identificador de sector público en el cálculo del ssPI. A pesar del mecanismo descrito, la privacidad no es completa ya que, además del ssPI, el ciudadano debe identificarse con su nombre y fecha de nacimiento, lo que permite interrelacionar sus actividades. Cuando el ciudadano tiene que hacer firmas digitales, el uso del certificado de firma incluido en su "Bürgerkarte" introduce otro factor de relación entre actividades. (12)

2.1.6 Francia

En Francia existe un amplio debate ante la entrada en circulación de la nueva Tarjeta de Identidad llamada CNIE, dentro del Programa INES, que contendrá un chip sin contactos en el que se almacenará la información en cinco bloques distintivos. El bloque de identificación, que almacena la información biométrica (la fotografía y dos huellas dactilares), así como el resto de información personal del titular, tiene protección criptográfica. El acceso a la información biométrica, por parte de personal autorizado, se realizará sin contactos, mientras que otras funcionalidades se realizarán sin contactos. Este nuevo documento tendría una validez de 5 años. No obstante, antes de su introducción el Gobierno francés encargó a Internet Rights Forum la organización de un amplio debate online, así como debates públicos en diferentes regiones, sobre esta nueva tarjeta de identidad, en particular, y del proyecto INES en general. En este debate participaron 70 organizaciones públicas y privadas (algunas no relacionadas con el sector). El resumen y conclusiones fueron publicados en un informe el 16 de junio de 2005 (http://www.foruminternet.org/). Básicamente, el informe, que recoge más de 3000 contribuciones recibidas online, así como las aportaciones de alrededor de 600 participantes en reuniones físicas, dice que el esquema de tarjeta de identidad propuesto "debe revisarse". Las principales recomendaciones que en este informe se recogen son:

La nueva tarjeta de identidad debería introducirse al mismo tiempo que el nuevo pasaporte biométrico. Se debería realizar un estudio riguroso con el fin de evaluar la extensión real del fraude de identidad en Francia.

Es conveniente establecer una coherencia entre la identificación única y centralizada que se utiliza en el proyecto INES y los identificadores utilizados actualmente en la administración electrónica.

La CNIL (Commission Nationale de l'Informatique et des Libertés) debería ejercer un control global y permanente sobre el sistema.

El uso de chip sin contactos debería admitirse una vez los estudios demuestren que es imposible acceder a los datos. (12)

Después de estas recomendaciones, el Gobierno francés ha pospuesto la introducción de la nueva CNIE a 2008, con el fin de concentrar sus esfuerzos en desarrollar los nuevos pasaportes biométricos. El nuevo pasaporte biométrico francés, disponible en otoño de 2006, sigue las especificaciones de la ICAO y las regulaciones europeas y contendrá, además de la información habitual contenida en los actuales pasaportes, una fotografía digital al principio y después imágenes de la huella dactilar. El pasaporte biométrico francés consiguió el aval de la CNIL en noviembre de 2005. (12)

2.1.7 Reino Unido

A principios de 2005, el Reino Unido adoptó la denominada "Identity Cards Bill" cuyo principal objetivo es la introducción de una tarjeta de identidad nacional. Toda la información puede encontrarse en http://www.identitycards.gov.uk/index.asp. La tarjeta de identidad, cuya utilización quiere hacerse obligatoria para los ciudadanos mayores de 16 años en el año 2010, alberga un chip que, además de la información personal habitual, almacenará una fotografía de la cara (y hombros), imágenes de huella, iris y la firma digitalizada. Todo ello se almacenará en el Registro Nacional de Identidad (NIR). La tarjeta consta también de un Número de Registro Personal (IRN) y un Número de Identificación Personal (PIN). Las características de esta tarjeta de identidad en ha sido muy cuestionada en un reciente informe de la LSE (London School of Economics & Political Science) [LOND05]. Por otra parte, en Marzo de 2006 se lanzó el nuevo pasaporte biométrico británico y en julio de 2006 el IPS (Identity and Passport Service) había ya emitido un millón de pasaportes, ver http://www.passport.gov.uk/general_biometrics.asp. Este pasaporte contiene la imagen facial del titular (almacenada en un chip interno) que servirá para confirmar la identidad del titular del mismo. (12)

2.1.8 Suecia

La tarjeta nacional de identidad electrónica sueca ("nationellt identitetskort") comenzó a emitirse en octubre de 2005, gestionada por la Policía y por la empresa privada Setec. Anteriormente, ya se

utilizaban en Suecia tarjetas de identificación electrónica emitidas por Correos desde 2002 según estándares del Instituto de Normalización Sueco (SIS).

La nueva tarjeta, que no es obligatoria, sirve como documento de identificación del ciudadano, con posibilidad de utilizar funciones de comunicación telemática segura con la Administración, y también como documento de viaje. La tarjeta incluye un chip accesible por radiofrecuencia (RFID) para almacenar datos biométricos del titular, huella digital y fotografía para reconocimiento facial, y cumple normas de la ICAO para documentos de viaje con y sin RFID. En todo caso, Suecia emite desde la misma fecha, octubre de 2005, pasaportes con datos biométricos. Los pasaportes y las tarjetas se expiden en las mismas oficinas y son fabricados por la misma empresa. Suecia ha sido el segundo país europeo en introducir pasaportes con datos biométricos, precedido por Bélgica (en noviembre de 2004) y seguido por Noruega (en octubre de 2005) y Alemania (en noviembre de 2005). (12)

2.1.9 DNI Electrónico en Tailandia.

La circulación de las TI como documento de identificación en Tailandia comenzó en el año 2005, y ya hoy en día 10 millones de personas poseen este documento, en el momento que se complete la distribución, 64 millones de tarjetas habrán sido entregadas a los ciudadanos tailandeses quienes portaran una tarjeta de identificación con sus huellas dactilares. 24 mil lectores biométricos se encuentran en uso en la actualidad para la lectura de las tarjetas y de la huella dactilar. La operación de comparación de la huella se lleva a cabo dentro de la tarjeta y no en el lector, esto reduce considerablemente la posibilidad de fraude. (12)

2.1.10 Características en común que presentan los sistemas de identificación nacional:

El principal objetivo de estos sistemas es que la persona quede identificada mediante un documento electrónico nacional. Hay ciertos datos en común que estarán impresos en todos los documentos electrónicos estos son el nombre y apellidos del titular, el número de identificación nacional y la foto de la persona, los demás datos de filiación dependerán de las leyes de cada entidad que emita este documento. La tecnología es otro punto en común donde todos utilizan la informática de un modo u otro como también utilizan las tarjetas inteligentes como documento electrónico de identificación nacional.

Todos los sistemas analizados son propietarios por lo que no se cuenta con la información detallada de sus estructuras y funcionamiento. Debido a que esta investigación se desarrolla en un país bloqueado económicamente por medio siglo la premisa es la siguiente: ¿Por qué pagar por un producto que

podemos producir? , somos capaces de desarrollar soluciones que impliquen el menor gasto posible, en la UCI se cuenta con el capital humano y la infraestructura necesaria para desarrollar el sistema que se propone.

2.2 ¿Por qué no importar un sistema de identificación?

La compra de un sistema de identificación que utilice la tecnología TI elaborado por Empresas privadas que no liberan el código del programa, implicaría que habría que pagar por cada sistema que se aplique y por su soporte técnico, debido al desconocimiento del código, podrían existir brechas de seguridad lo cual sería un riesgo inaceptable debido a la importancia del proceso de identificación. El MININT no está de acuerdo en implantar una solución de la cual no tenga un total dominio y conocimiento.

2.3 ¿Por qué aplicar la tecnología de las TI en el Proceso de Identificación en Cuba?

La TI permite la impresión de datos de filiación en su exterior así como también una foto de su portador, de esta manera es posible la verificación de la identidad de su portador con una probabilidad de autenticidad similar a la que existe actualmente en nuestro país, en caso de que se use el lector para verificar los datos de la tarjeta porque así lo requiera la instancia que necesite comprobar la identidad del portador del documento, entonces esta probabilidad de autenticidad aumentaría tendiendo al 100%. Además en la UCI se encuentra el Centro de Identificación y Seguridad Digital, para el cual se hace esta investigación y sería el encargado de darle soporte y solución a la futura implantación de un sistema de identificación utilizando las TI.

Es por esto que se decide aplicar la tecnología de Tarjetas Inteligentes, en el sistema de identificación, ya que las TI ofrecen la seguridad necesaria para proteger dicho documento, el cual siempre estará en el servidor de cada oficina de registro, en manos de la persona y protegido por un PIN o por una característica biométrica digitalmente almacenada en la tarjeta.

2.4 ¿Qué ventajas traería introducir la tecnología TI en el proceso de identificación?

Se evitaría el excesivo manejo de papeles. Se podría almacenar más información sobre la persona, se evitaría en gran escala la falsificación del documento de identificación. Esta tarjeta es multiaplicación por tanto se puede vincular con el sistema de licencia de conducción, bancario, de salud dependiendo de la capacidad de almacenamiento de la tarjeta. En caso de no existir una conexión directa y teniendo un lector de este tipo de tarjetas se puede obtener la información necesaria de la persona.

2.5 Conclusiones:

Durante este capítulo se analizaron varios de los sistemas de identificación nacional que usan TI en el mundo, se identificaron sus semejanzas y diferencias entre ellos, también ventajas y desventajas de estos sistemas, se valoraron los resultados y se tomaron las características comunes que son aplicables a nuestro país, concluyendo que la opción más acertada para informatizar nuestro proceso de identificación es:

- Un sistema creado e implantado por personal del Centro de Identificación y Seguridad Digital.
- Utilizar tecnología TI como documento de identificación electrónico nacional.

CAPÍTULO 3: PROPUESTA DE SOLUCIÓN.

3.1 Introducción.

En este capítulo se describe la realización de los Casos de Usos, se definen los actores y trabajadores que participan en el negocio quedando explícitas las reglas del negocio, y se modela el negocio. Además se realiza la descripción de la propuesta del sistema a desarrollar, se hace un diagrama de casos de uso del sistema para un mejor entendimiento de la solución informática del mismo y se define actores y requerimientos tanto funcionales como no funcionales del sistema a desarrollar.

3.2 Información que se maneja.

En cuanto a la información de la persona se encuentran los datos de identificación de la misma: nombre y apellidos, fecha de nacimiento, dirección particular, estatura, peso y género.

Un carné de identidad, documento nacional de identidad (DNI), o cédula de identidad es un documento emitido por una autoridad administrativa competente para permitir la identificación personal de los ciudadanos.

El Documento Nacional de Identidad es el único documento de uso generalizado en todos los ámbitos a nivel nacional y referente obligado para la expedición de otros documentos.

Ventajas del DNI electrónico (DNIe).

El DNIe tiene grandes ventajas para el ciudadano:

Desde el punto de vista de la SEGURIDAD:

Mediante el DNIe se garantiza la identidad de los interlocutores de una comunicación telemática, ya sea para intercambio de información, acceso a datos o acciones o compra por Internet. Igualmente, mejorar la gestión del acceso a los espacios de trabajo, los ordenadores personales y a la información que contenga.

Usando el DNIe se intercambian mensajes con la certeza de que los interlocutores son quienes dicen ser y que la información intercambiada no ha sido alterada, además permite certificar los documentos digitales, mediante firmas digitales que aseguran la propiedad intelectual del autor.

Desde el punto de vista de la COMODIDAD:

Hacer trámites sin tener que aportar una documentación que ya exista: Una de las ventajas derivadas del uso del DNI electrónico y de los servicios basados en él será la práctica eliminación del papel en la tramitación. El ciudadano no tendrá que aportar una información que ya exista en otra Unidad de la Administración, evitándose pérdidas de tiempo.

Desde el punto de vista de la ERGONOMÍA:

El DNI electrónico es un documento más robusto. Está construido en policarbonato y tiene una duración prevista de unos diez años.

Descripción del DNI electrónico.

El DNI electrónico es una tarjeta de un material plástico, que incorpora un chip con información digital. Su tamaño, coincide con las dimensiones de las tarjetas de crédito comúnmente utilizadas (85,60 mm de ancho X 53,98 mm de alto).

Descripción física del DNI electrónico.

En una de las caras de la tarjeta se encuentran los siguientes elementos:

En el cuerpo central:

Elementos	Descripción
PRIMER APELLIDO	Primer apellido del ciudadano.
SEGUNDO APELLIDO	Segundo apellido del ciudadano.
NOMBRE	Nombre del ciudadano.
FECHA DE NACIMIENTO	Fecha de nacimiento del ciudadano.
VÁLIDO HASTA	Fecha de validez del documento.

En la esquina inferior izquierda:

Elementos	Descripción
DNI NUM	Número del Documento Nacional de Identidad del Ciudadano, seguido del carácter de verificación (Número de Identificación Fiscal).
Fecha de expedición	La fecha de expedición en formato DDMMAA.

Chip criptográfico, que contiene la siguiente información en formato digital:

Certificado electrónico para autenticar la personalidad del ciudadano.

Certificado electrónico para firmar electrónicamente, con la misma validez jurídica que la firma manuscrita.

Certificado de la Autoridad de Certificación emisora.

Claves para su utilización.

La plantilla biométrica de la impresión dactilar.

La fotografía digitalizada del ciudadano.

La imagen digitalizada de la firma manuscrita.

Datos de la filiación del ciudadano, correspondientes con el contenido personalizado en la tarjeta.

Elementos de seguridad del documento, para impedir su falsificación:

Medidas de seguridad físicas:

Visibles a simple vista (tintas ópticamente variables, relieves, fondos de seguridad).

Verificables mediante medios ópticos y electrónicos (tintas visibles con luz ultravioleta, micro escrituras)

Medidas de seguridad digitales:

Encriptación de los datos del chip

Acceso a la funcionalidad del DNIe mediante clave personal de acceso (PIN)

Las claves nunca abandonan el chip

La Autoridad de Certificación es el la Dirección General de la Policía

El reverso de la tarjeta contiene los siguientes elementos:

Información impresa (y visible a simple vista) sobre la identidad del ciudadano en la parte superior:

LUGAR DE NACIMIENTO

PROVINCIA-PAÍS

HIJO DE

DOMICILIO

LUGAR DE DOMICILIO

PROVINCIA-PAÍS

Proceso de transición del DNI a la TI como DNIe.

El proceso de transición del DNI al DNIe deberá ser de forma paulatina como la TI estará impresa en su exterior y teniendo la misma función del DNI permite cambiar sistemáticamente hacia el DNIe sin que se afecte el proceso de identificación actual. El MININT dispone de los recursos y el capital humano para efectuar esta transición en un plazo de 5 años emitiendo el DNIe para aquellos que cumplan 16 años o vayan a hacer algún cambio o actualización del documento y para los recién nacidos que requieren DNI.

La información almacenada en los archivos de la OCI se lleva al sistema y no se desechara esta información física, sino que se almacenara hasta 10 años.

Consejos y buenas prácticas con el DNI electrónico

Pérdida o sustracción del documento.

En caso de pérdida o sustracción del DNIe, el titular deberá denunciar el hecho en cualquier Estación de Policía, seguidamente deberá dirigirse a la Oficina del Carné de Identidad para proceder a la obtención de un nuevo documento.

Una vez en la Oficina del Carné de Identidad, deberá rellenar el impreso correspondiente y adjuntar una fotografía, que junto a su firma y su impresión dactilar, servirá de comprobación de su identidad.

Igualmente, se generarán nuevas claves y se expedirán nuevos certificados electrónicos.

Custodia de las claves privadas de los Certificados

La custodia de las claves privadas de los Certificados de Identidad Pública la realizan los ciudadanos titulares de las mismas. En ningún caso la Autoridad de Certificación guarda copia de la clave privada ya que esta no puede ser extraída de la tarjeta.

Las claves privadas del ciudadano se encuentran almacenadas en el procesador de la tarjeta criptográfica del DNIe. Con esto se consigue que las claves privadas no abandonen nunca el soporte físico del DNI, minimizando las posibilidades de poner en riesgo dichas claves.

Para el acceso a las claves y al certificado de firma el ciudadano deberá emplear una clave personal de acceso (PIN) generada en el momento de recibir su DNIe y que sólo él debe conocer.

En todo momento el ciudadano podrá modificar la clave personal de acceso en una Oficina de Expedición utilizando los puestos destinados a tal efecto (Puntos de Actualización del DNI electrónico).

3.3 Propuesta de arquitectura

Lenguajes de programación a utilizar

Java.

Java es un lenguaje de programación de alto nivel, orientado a objetos desarrollado por Sun Microsystems a principios de los años 90. Sun Microsystems liberó la mayor parte de sus tecnologías Java bajo la licencia GNU GPL, de acuerdo con las especificaciones del Java Community Process, de forma tal que el lenguaje Java de Sun se encuentra con la licencia GNU GPL / Java Community. El lenguaje es Independiente de la plataforma, lo que permite ejecutar programas escritos en el lenguaje Java de forma similar en cualquier tipo de hardware y su recolector automático de basura, es el responsable de gestionar el ciclo de vida de los objetos creados por el programador.

Java Card.

Java Card da al usuario la capacidad de programar aplicaciones que se ejecutan en la tarjeta de modo que ésta tenga una funcionalidad práctica en un dominio de aplicación específico, es un subconjunto del lenguaje Java.

Gestor de Base de Datos a utilizar

PostgreSQL.

La solución propuesta deberá manejar un gran número de datos, por lo que la propuesta más acertada es PostgreSQL, que es un sistema de gestión de base de datos objeto relacional de software libre, publicado bajo la licencia BSD, es el más adaptable a las necesidades, pues es capaz de soportar grandes volúmenes de datos con el mismo rendimiento.

3.4 Tipos de dispositivos, sistemas operativos y estándares.

Para la utilización del DNI electrónico es necesario contar con determinados elementos hardware y software que nos van a permitir el acceso al chip de la tarjeta y, por tanto, la utilización de los certificados contenidos en él.

El DNI electrónico requiere el siguiente equipamiento físico:

•Un lector de tarjetas inteligentes que cumpla el estándar ISO-7816. Existen distintas implementaciones, integrados en el teclado, externos (conectados vía USB) o a través de una interfaz PCMCIA.

Para elegir un lector que sea compatible con el DNI electrónico, verificar que al menos:

- Cumpla el estándar ISO 7816 (1, 2 y 3)
- Soporta tarjetas asíncronas basadas en protocolos T=0 (y T=1)
- Soporta velocidades de comunicación mínimas de 9.600 bps.
- Soporta los estándares:
  - ✓ API PC/SC (Personal Computer/Smart Card)
  - ✓ CSP (Cryptographic Service Provider, Microsoft)
  - ✓ API PKCS#11

Tarjetas inteligentes			
Distribuidora	Tarjeta	Características	Precio en Euros
C3PO	C3P2K	Tarjeta de memoria con doble sistema de seguridad: cabecera fija y PIN de acceso a escritura. 256 Bytes	1.24
C3PO	Crypto Memory	Tarjeta que combina los beneficios de las tarjetas de memoria con el protocolo T=0, permitiendo su aceptación en cualquier terminal de tarjetas inteligentes. Capacidad de 2Kbit.	2.12
C3PO	***WG10***	**Tarjeta micro procesada con diferentes capacidades, potente sistema de seguridad, gestión de monedero y criptografía simétrica (DES). Capacidades de 2Kbytes y 8Kbytes.**	**4.34**
C3PO	Criptonita	Tarjeta criptográfica con sistema de almacenamiento de certificados, sistema de alta seguridad y criptografía asimétrica (RSA). Capacidades de 16Kbytes y 32Kbytes.	11.21

La TI WG10 es la propuesta ya que es la que más se ajusta a las necesidades y contexto de esta solución.

Lector de tarjeta inteligente					
Modelo	Descripción	Alimentación	Ventajas	Inconvenientes	Precio
SmartLp2	Lector interno	Fuente de alimentación del ordenador	Fiable, robusto	Hay que "abrir" el PC para su instalación. No tienen soporte para Windows 2000 pc/sc.	57.40 €
SmartLp3	***Similar al anterior pero de tipo externo.***	***Conector PS/2***	***Igual de fiable y plug and play en windows 9x.***	***No.***	***35.70 €***
Cherry G83-6700	Teclado con lector de tarjeta incorporado.	Mismo puerto de teclado	Fácil de instalar.	Teclado de membrana. Si se rompe el teclado, tiramos también el lector.	67.00 ***€***
Teclado Keytronic	Teclado con lector de tarjeta incorporado.	Mismo puerto de teclado	Fácil de instalar.	Teclado de membrana. Si se rompe el teclado, tiramos también el lector. Ha dado problemas con algún periférico.	64.30 €
Towitoko ChipDrive	Lector externo miniatura	Del mismo puerto serie donde. Conector PS/2, y USB.	Económico. Multiplataforma.	Los que sacan la alimentación del mismo puerto serie, no han demostrado	37.00 €
Smarty	Se usan en la disquetera del equipo	Una pila de botón.	No utiliza ningún puerto de la PC.	Ha demostrado poca fiabilidad.	---------

Impresoras de tarjetas			
Marca	Modelo	Característica	Precio
Datacard	RL90	Ideal para control de acceso mediante proximidad o identificación de la persona. Cada impresora le permite la impresión de hasta 100 tarjetas por hora, aunado a una presentación y calidad excelente.	1353.30 €
Datacard	SP25	Funcionalidad de impresión sobre tarjetas re escribibles. El valor-precio de la Datacard SP25 combina alta calidad, con la impresión de tarjetas a todo color y la innovación de escribir sobre tarjetas re escribibles a un costo-beneficio muy atractivo e ideal para programas pequeños de identificación	1022.35 €
Evolis Tattoo	***Tatoo2***	***Personaliza en color o en monocromo las tarjetas vírgenes o pre impresas. Tattoo permite obtener resultados de calidad gracias a una resolución de 300 dpi y una excelente impresión. Imprime textos, logotipos, códigos de barras y fotografías según sus necesidades. La respuesta a las expectativas de las pequeñas organizaciones***	***920.22 €***
Overlandia	nisca c101	No solo ofrece una calidad de impresión nunca vista sino que además su driver permite una multitud de ajustes: contraste, brillo, separación de canales CMYK	1.690.00 €

Estimación de costo tecnológico				
Tecnología	Modelo	Precio unitario	Cantidad	Costo final
Tarjetas inteligentes	WG10	4.34 €	130 969 (Población de municipio La Lisa)	568405.46 €
Lector de tarjetas inteligentes	SmartLp3	35.70 €	3	107.10 €
Impresora de tarjetas inteligentes	Evolis Tattoo	920.22	2	1840.44 €
Total				570353 € 730736.26 usd 584589 cuc

La aplicación del DNIe evitará el manejo de papeles teniendo así un impacto ecológico, el DNI estará protegido por el entorno del chip y por un pin y la falsificación de este es casi imposible, se evitará tener que confeccionar un nuevo documento ya que la TI es reutilizable. Permitirá vincular el DNI con otros documentos y servicios, los ciudadanos se podrán identificar a través de la red. Se agilizará el proceso de emisión del documento al hacer una búsqueda informática en vez de manual.

3.5 Modelo del Negocio.

El modelo de negocio es una técnica para comprender los procesos de negocio de la organización y la determinación de los requisitos del futuro sistema. Dentro de los objetivos fundamentales de este flujo de trabajo están: comprender la estructura y la dinámica de la organización en la cual se va a implantar el sistema, comprender los problemas actuales de la organización e identificar las mejoras potenciales, asegurar que los consumidores, usuarios finales y desarrolladores tengan un entendimiento común del funcionamiento de la organización y derivar los requerimientos del sistema que va a soportar la organización.

3.5.1 Reglas del negocio.

- ✓ La persona solicita la creación del documento de identificación según su necesidad.
- ✓ El documento de identificación es creado por el oficial del registro de personas.
- ✓ En caso de fallecimiento de la persona su documento de identificación pierde su funcionalidad activa y se archiva el documento de inscripción en el archivo de fallecidos.
- ✓ El documento de identificación vence a los 10 años de su creación.
- ✓ Las personas deben portar el documento de identificación en trámites legales.

3.5.2 Justificación de Actores y Trabajadores del Negocio.

Actor: Es cualquier persona, individuo, grupo, entidad, organización, máquina o sistema de información externos; con los que el negocio interactúa. El término actor no es más que el rol que se juega cuando se interactúa con el negocio para beneficiarse de sus resultados por tanto no debe expresar una persona en especifico, por lo cual, no representa un usuario físico pues varios usuarios físicos pueden realizar el mismo papel en el negocio (rol), por otro lado, un mismo usuario puede actuar como diferentes actores (roles). El nombre de un actor del negocio debe ir de acorde al rol que este desempeñe dentro del negocio.

Actor	**Descripción**
Persona	Es el principal beneficiado con los resultados de los procesos de negocio y se encuentra en su derecho de obtener un

	documento de identificación con la calidad requerida.

Tabla 2.1. Descripción de los actores del negocio.

Trabajador: Definen el comportamiento y responsabilidades (rol) de un individuo, grupo de individuos, sistema automatizado (Software) o máquina, que trabajan en conjunto como un equipo dentro del proceso de negocio realizando las actividades que están comprendidas dentro del caso de uso. Ellos realizan las actividades y son propietarios de elementos. Estos trabajadores están dentro de la frontera del negocio y son los que posteriormente se convertirán en usuarios del sistema que se quiere construir. Cada trabajador del negocio debe definirse brevemente con su responsabilidad dentro del negocio.

Trabajador	**Descripción**
Oficial de Registro	Es el encargado de registrar los datos de la persona y de confeccionar el documento de identificación.

Tabla 2.2. Descripción de los trabajadores del negocio.

3.5.3 Diagrama de casos de uso (CU) del negocio.

El diagrama de casos de uso del negocio es un diagrama que describe los procesos de un negocio (casos de uso del negocio) y su interacción con elementos externos (actores), tales como socios y clientes, es decir, describe las funciones que el negocio pretende realizar y su objetivo básico es describir cómo el negocio es utilizado por sus clientes y socios.

Modelo de Objetos del Negocio

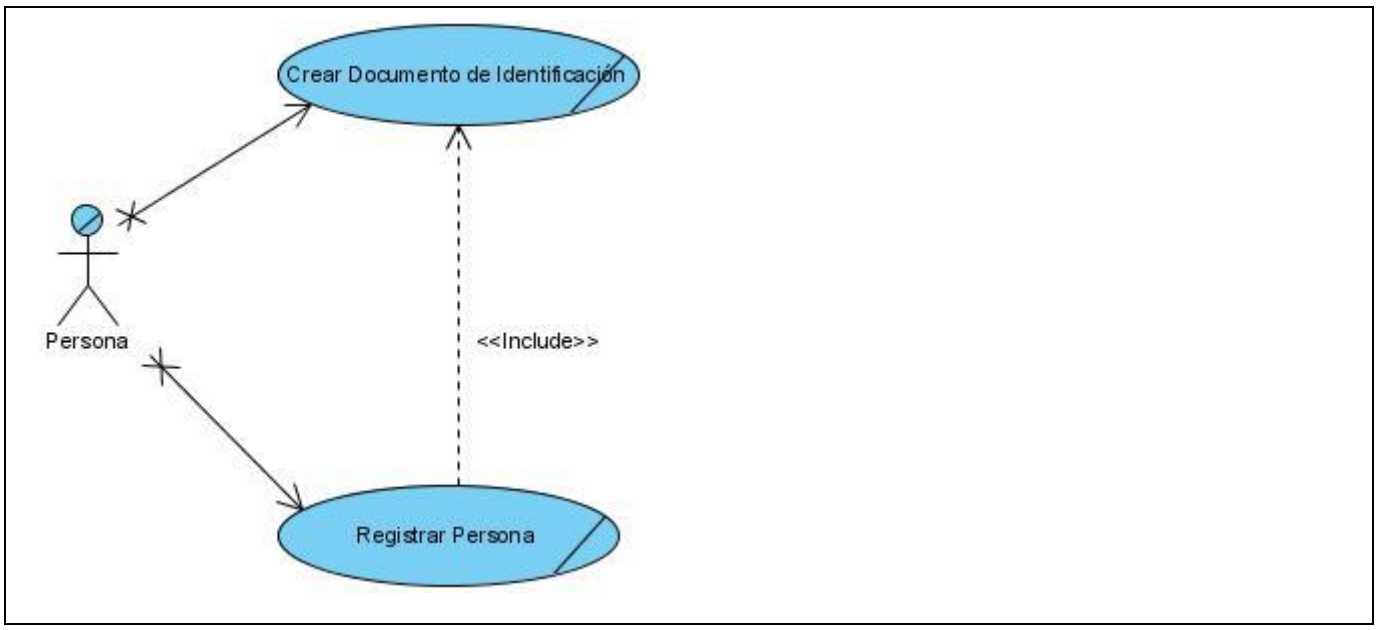


Figura 2.1: Diagrama de Casos de Uso del Negocio.

3.5.4 Descripción de los CU del Negocio.

Descripción del Caso de Uso del Negocio Registrar Persona.

CU del Negocio	Registrar Persona
Actores	Persona
Resumen	El Caso de Uso se inicia cuando una persona llega a la OCI y solicita un servicio, si es para registrar un recién nacido, la persona deberá identificarse y se le solicitan los datos necesarios. Si la persona necesita modificar algún dato personal entonces hay que crear un nuevo documento de inscripción y deshabilitar el anterior
CU asociados	Crear Documento de identificación

Acción del actor	**Respuesta del proceso de negocio**
1. La persona llega a la oficina de identificación y solicita la creación del documento de inscripción.	1.1 El oficial de registro solicita los datos de la persona.
2. Informa los datos solicitados.	2.1 El oficial busca a la persona según los datos ofrecidos 2.2 Verifica los datos. 2.3 Solicita la foto para la creación del documento de

	identificación.
3. Entrega la foto	3.1 EL oficial añade la foto al documento de inscripción.
4. Se toma las huellas digitales	4.1 El oficial archiva el documento de inscripción. 4.2 Realiza caso de uso asociado.
Otras secciones	Acción 2.2: No se le solicita la foto porque a los menores de edad no se les adjunta la foto al documento de inscripción. Acción 3.2: No se le toma las huellas digitales porque a los menores de edad no se les toman las huellas digitales.
Mejoras propuestas	Realizar de forma automática el llenado del documento de inscripción.

Descripción del Caso de Uso del Negocio Crear Documento de Identificación.

CU del Negocio	Crear Documento de Identificación.
Actores	Persona
Resumen	El Caso de Uso se inicia cuando una persona llega a la oficina de identificación y solicita un servicio por pérdida o deterioro del documento de identificación. Además es inicializado cuando a partir de la realización del caso de uso Registrar persona se crea el documento de identificación.
CU asociados	

Acción del actor	**Respuesta del proceso de negocio**
1. La persona llega a la oficina de identificación y solicita la creación del documento de identificación por pérdida o deterioro.	1.1 El oficial de registro solicita los datos de la persona.
2. Informa los datos solicitados.	2.1 El oficial registra los datos en el documento de inscripción. 2.2 El oficial solicita la foto.
3. Entrega la foto	3.1 EL oficial añade la foto al documento de inscripción.

	3.2 El oficial le toma las huella digitales a la persona.
4. Se toma las huellas digitales	4.1 El oficial archiva el documento de inscripción.
Otras secciones	
Mejoras propuestas	Realizar de forma automática el llenado del documento de inscripción.

3.5.5 Modelo de objetos.

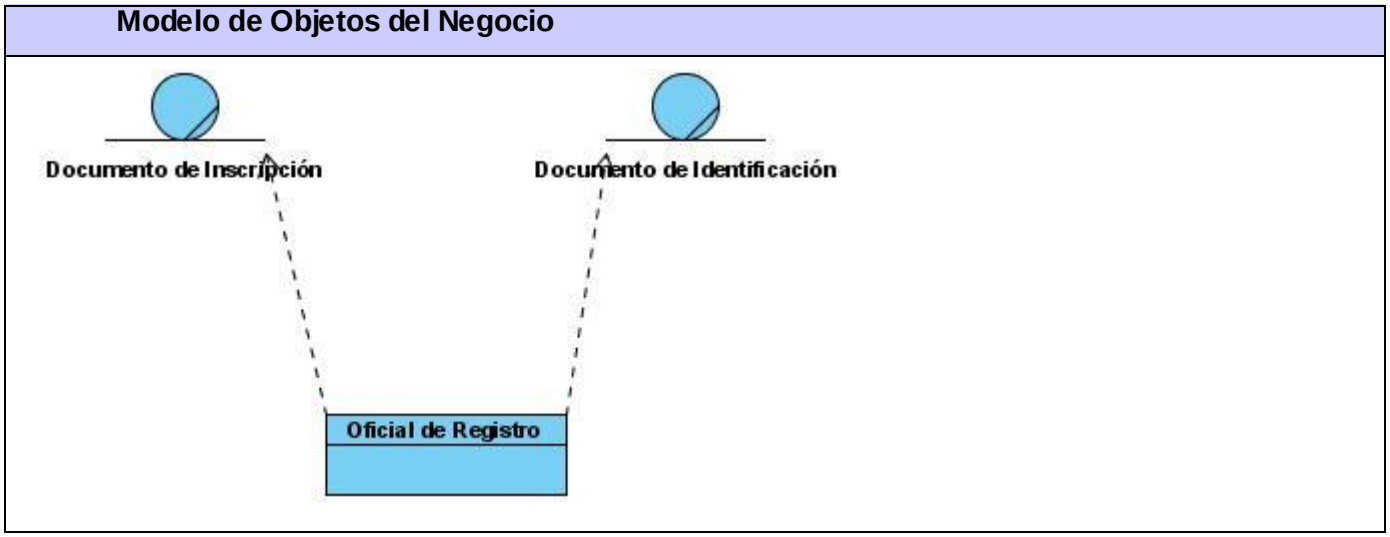


Figura 2.2: Modelo de Objetos del Negocio.

3.6 Propuesta del sistema.

3.6.1 Especificación de los Requerimientos de Software

Los requerimientos, también conocidos como requisitos, son condiciones o capacidades que tienen que ser alcanzadas o poseídas por un sistema o componente de un sistema para satisfacer un contrato, estándar u otro documento impuesto formalmente. Todas las ideas que los clientes, usuarios y miembros del equipo de proyecto tengan acerca de lo que debe hacer el sistema, deben ser analizadas como candidatas a requisitos. Los requisitos se pueden clasificar en: funcionales y no funcionales.

Requerimientos Funcionales.

Los requerimientos funcionales son capacidades o condiciones que el sistema debe cumplir; los mismos no alteran la funcionalidad del producto, esto quiere decir que los requerimientos funcionales se mantienen invariables sin importarle con que propiedades o cualidades se relacionen. En la realización

de los casos de uso del negocio se obtienen las actividades que serán objeto de automatización, estas actividades no son exactamente los requerimientos funcionales pero si son el punto de partida para identificar qué debe hacer el sistema.

A continuación se muestra el listado de los requerimientos funcionales del Documento de Identificación.

RF 1 Autenticar usuario.

RF 2 Registrar datos de la persona.

RF 3 Crear documento de identificación.

RF 4 Buscar persona.

RF 5 Obtener documento de identificación.

RF 6 Modificar datos de la persona.

RF 7 Modificar documento de identificación.

RF 8 Desactivar documento de identificación.

RF 9 Archivar los documentos desactivados de identificación de una Persona.

Algunos de los requerimientos funcionales se encuentran agrupados en un mismo caso de uso, el requerimiento Obtener documento de identificación está contenido en el caso de uso Buscar persona, al hacer una búsqueda de la persona se obtiene su documento de identificación. Los requerimientos funcionales Desactivar documento de identificación y Archivar los documentos desactivados de identificación de una persona se encuentran contenidos en el caso de uso Modificar documento de identificación, los restantes requerimientos conforman los casos de usos del sistema.

Requerimientos no Funcionales.

Los requerimientos no funcionales son propiedades o cualidades que el producto debe tener, debe pensarse en estas propiedades como las características que hacen al producto atractivo, usable, rápido o confiable.

Apariencia o interfaz externa.

- La aplicación deberá tener una interfaz externa amigable, que sea sencilla y fácil de entender por el usuario para así evitar que el usuario se pierda dentro de la aplicación.

Software.

- No hay restricciones en cuanto al sistema operativo a instalar puesto que la aplicación será multiplataforma.
- La Máquina Virtual de Java tiene que estar instalada.
- Los Drivers para los lectores de las tarjetas tienen que estar instalados.
- La Máquina Virtual de JavaCard que se ejecuta en la tarjeta debe coincidir con una versión igual o superior a la JCDK
- Gestor de Base de Datos: PostgreSql.

Hardware:

- Se debe contar con 256 MB de memoria RAM como mínimo, aunque lo ideal serian 512 MB.
- Procesadores Pentium IV.
- Lector de Tarjetas Inteligentes.
- Java Card.

Seguridad:

- *Confidencialidad*: Se requiere de un PIN para poder acceder a la información dentro de la Tarjeta y que el oficial de registro este autentificado. El oficial de registro es el único que puede modificar la información dentro del documento de identificación.
- *Disponibilidad*: La información siempre estará disponible ya que no se necesitan de conexiones online para poder acceder a la información.

Portabilidad:

- El sistema deberá funcionar en los sistemas operativos Windows y Linux, pero para ello se deberá tener instalada la máquina virtual de Java y los Drivers para los lectores de las tarjetas.

3.6.2 Modelo de CU del Sistema.

El modelado del sistema tiene como entrada principal los requisitos de software identificados, los que se agrupan en casos de usos que responde a las funcionalidades del sistema.

Definición de Actores del Sistema.

Ver Anexo 1.

Diagrama de CU del Sistema.

Un diagrama de casos de uso del sistema representa gráficamente los procesos y su interacción con los actores, describiendo lo que hace el sistema para cada tipo de usuario. Cada tipo de usuario se representa mediante uno o más actores, también se representa mediante uno o más actores cada sistema externo con el que interactúa el sistema, incluyendo los dispositivos.

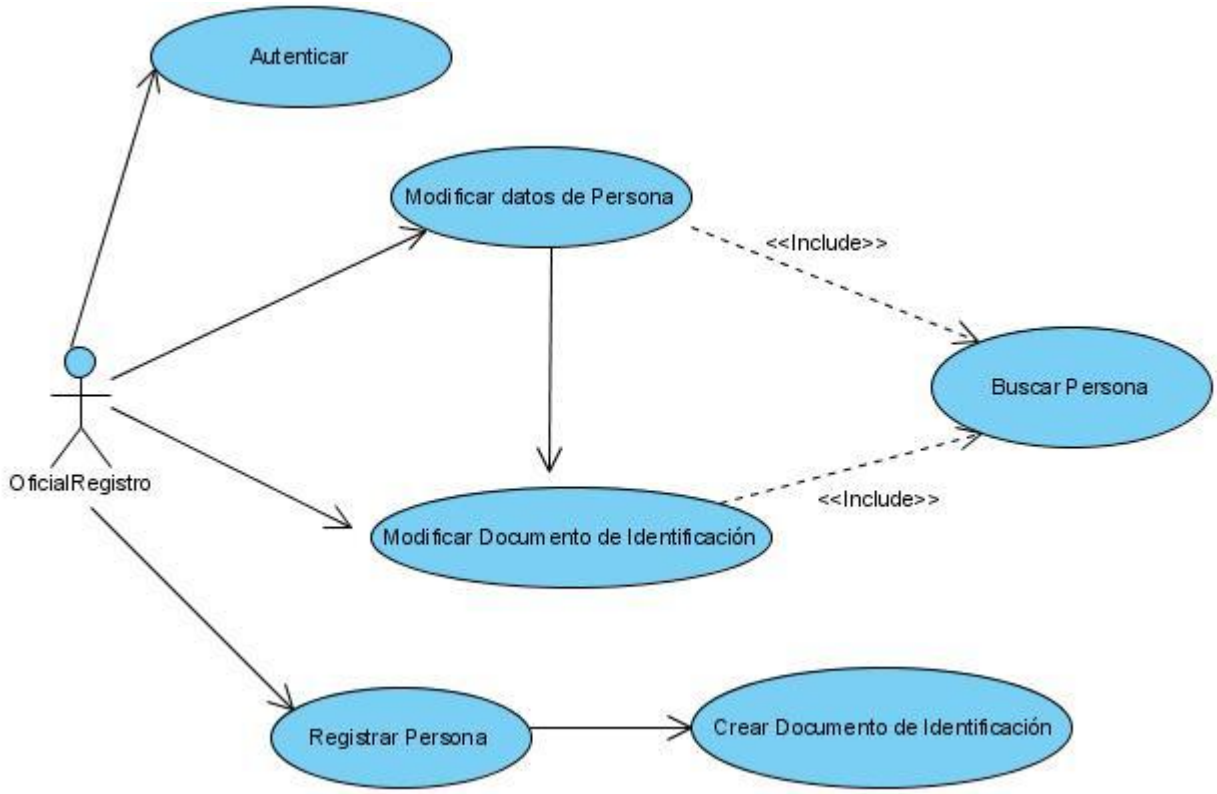


Figura 2.3: (Diagrama de Casos de Uso del Sistema).

3.6.2.1 Descripción de los CU del Sistema.

Una descripción de los casos de uso del sistema, detallando el flujo de los eventos y dejando claro todas las acciones que se realizan en el sistema, para lograr un mejor entendimiento de su funcionamiento.

Anexo 2: Descripción del Caso de uso del Sistema Buscar persona.

Anexo 3: Prototipo de interfaz de usuario Buscar Personas.

Anexo 4: Descripción del Caso de uso del Sistema Registrar Datos Persona.

Anexo 5: Prototipo de interfaz de usuario Registrar Datos de Personas.

Anexo 6: Descripción del Caso de uso del Sistema Modificar Datos Persona.

Anexo 7: Prototipo de interfaz de usuario Modificar Datos de Personas.

Anexo 8: Descripción del Caso de uso del Sistema Crear DNIe.

Anexo 9: Prototipo de interfaz de usuario Crear Documento

Anexo 10: Descripción del Caso de uso del Sistema Modificar documento de Identificación.

Anexo 11: Prototipo de interfaz de usuario Modificar Documento de Identificación.

Anexo 12: Descripción del Caso de uso Autenticar.

Anexo 13: Prototipo de interfaz de usuario Autenticar.

3.6.3 Diagramas de Clases del sistema

Diagrama de clases Gestionar Datos de Persona.

El oficial de registro interactúa con la clase interfaz persona donde va a introducir los datos de la persona, la clase controladora persona es la encargada de gestionar los datos introducidos y de almacenarlos en la clase persistente persona.

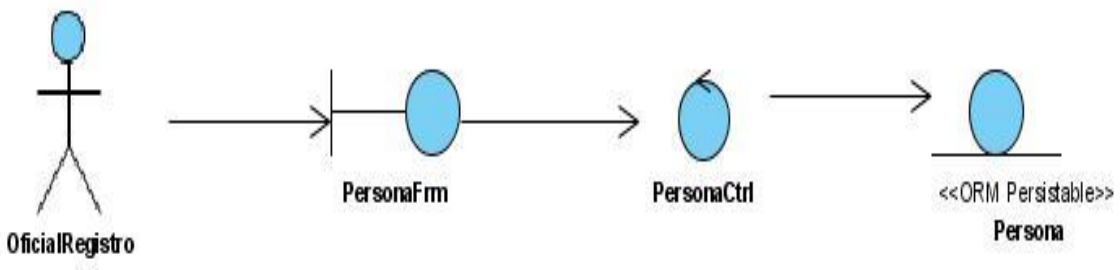
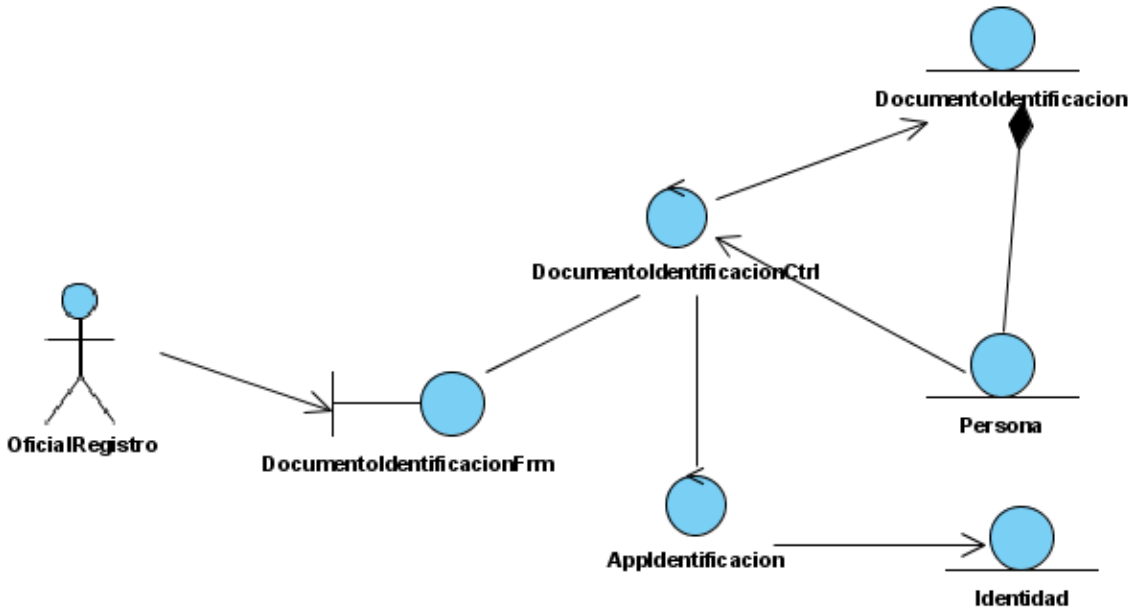


Diagrama de Clases 1: Gestionar Documento de Identificación.

El oficial de registro interactúa con la clase interfaz Documento Identificación (DI), la clase controladora DI gestiona los datos introducidos y los almacena en la clase persistente DI, la cual tiene una relación de uno a muchos con la clase entidad persona. La clase controladora DI interactúa con la clase controladora AppIdentificación (Apple de la tarjeta) y esta última clase gestiona los datos que va a ser almacenados en la clase persistente identidad.



3.7 Conclusiones:

En el transcurso de este capítulo se ha descrito el proceso de creación de un documento de identificación, donde se identificaron los roles, entidades u objetos del negocio, así como su relación

con este proceso. Esta descripción fue realizada mediante el modelado del negocio, para lo cual se elaboraron los modelos de casos de uso y objetos del negocio.

Después de haber realizado el modelado de negocio, se pudo lograr una mejor comprensión del problema que el sistema tiene que resolver.

Se realizó una propuesta de solución informática para informatizar el proceso de identificación de personas en Cuba utilizando tarjetas inteligentes java, esta propuesta constituye un paso relevante para la futura implementación de un sistema para el proceso de identificación de la OCI del municipio La Lisa.

CONCLUSIONES

Se constató la existencia de la problemática mediante consultas a especialistas y mediante una observación sistemática, consciente y objetiva del proceso de identificación de personas en Cuba.

Se realizó una propuesta de solución informática para informatizar el proceso de identificación de personas en Cuba utilizando tarjetas inteligentes java, esta propuesta constituye un paso relevante para la futura implementación de un sistema para el proceso de identificación de la OCI La Lisa. La tecnología que se propone es reutilizable para otras aplicaciones como son:

- ✓ Tarjeta de débito.
- ✓ Tarjeta de salud.

Se validó la propuesta según criterios de especialistas.

En el transcurso de este trabajo se describieron las características de los tipos de sistemas que se emplean para la identificación personal y se puntualizaron las tecnologías aplicadas, lo cual brindó los elementos para la selección del sistema y tecnología más adecuada al proceso actual de identificación en la Oficina del Carné de Identidad del municipio La Lisa.

Se analizaron los resultados de la implantación de sistemas de identificación personal existentes en el mundo y dio la medida de las diferencias y similitudes que pueden tener los datos en los documentos de identificación así como también del nivel de rechazo que causa la implantación de estos sistemas en la sociedad. Otro aporte de este análisis es que demostró la utilidad del uso de la tecnología TI que permite la integración con otros sectores sociales como la salud, el banco, y políticos donde tienen un uso acertado en el proceso electoral mediante el voto electrónico usando la firma digital en la tarjeta inteligente.

RECOMENDACIONES

- ✓ Desarrollar la cultura de la sociedad para el uso del DNIe.
- ✓ Sancionar la ley que reconozca la firma electrónica como homóloga de la firma manuscrita.
- ✓ Implementar e Implantar la tecnología TI como DNIe en Cuba.
- ✓ Integrar al DNIe la licencia de conducción y la tarjeta de salud.

BIBLIOGRAFÍA

1. Noticias jurídicas. [En línea] 2009. [Citado el: 5 de Mayo de 2009.] http://noticias.juridicas.com/base_datos/Admin/dudh.html.

2. **Ramón, Miguel A.** Apuntes de PoliciaCientifica I.-CICE. [En línea] 2006. [Citado el: 19 de Marzo de 2009.] http://campus.usal.es/~cise/software/PoliciaCientifica/TEMA2.pdf.

3. **Rojas, George.** [En línea] 29 de 12 de 2007. [Citado el: 6 de Marzo de 2009.] http://gjorge.wordpress.com/2007/12/29/arquitectura-de-un-sistema-biometrico-para-identificacion-personal.

4. **Justiniano, Ernesto.** [En línea] 2009. [Citado el: 2 de Mayo de 2009.] http://www.ernestojustiniano.org/foro/topic/que-son-los-sistemas-biomeacutetricos.

5. AP-ELECTRONICS.com. [En línea] 2007. [Citado el: 26 de Enero de 2009.] http://www.ap-electronics.com/tarjetas_inteligentes.asp?op=10.

6. International Organization for Standarization. [En línea] 2003. [Citado el: 17 de Marzo de 2009.] http://www.iso.org/iso/catalogue_detail?csnumber=31432.

7. CERES. [En línea] 6 de Junio de 2008. [Citado el: 29 de mayo de 2009.] http://www.cert.fnmt.es/index.php?cha=cit&sec=9&page=85&lang=es.

8. **Jesús Sánchez Orozco, José R. Sánchez Orozco, Benito Recuero Díaz, Francisco José Seva Mora, Álvaro Rendón Pérez.** [En línea] 20 de Mayo de 2004. [Citado el: 20 de Marzo de 2009.] http://www.dte.us.es/tec_inf/itis/peri_int/trabajos/.

9. Web electrónica club se. [En línea] 2004. [Citado el: 24 de Enero de 2009.] http://www.clubse.com.ar/download/pdf/notasrevistas06/nota01.htm.

10. **Madaglia, Diego.** [En línea] 2001. [Citado el: 03 de Febrero de 2009.] http://www.monografias.com/trabajos16/tarjetas-inteligentes/tarjetas-inteligentes.shtml.

11. **Carlos Alegría Galicía, Samuel Flores Sandoval, Augusto Dobeslao Hernández López.** Creación de un modelo de identificación de alumnos e integración de servicios utilizando smartcards y

tecnología java. Caso de estudio: Facultad de Ingeniería. [En línea] 2005. [Citado el: 12 de Enero de 2009.] http://cad.cele.unam.mx/~cerealito/html.

12. **García, Cristóbal Tárraga.** Laboratorio de Electrónica 2003/2004. [En línea] 2004. [Citado el: 22 de Febrero de 2009.] http://www.info-ab.uclm.es/labelec/Solar/Otros/ISO_7816/index.htm.

13. **Enrrique Vasquez Gallo, Carmen Sanches Avila.** *Sistemas nacionales de identificación electrónica en el entorno europeo y norteamericano.* Madrid : s.n., 2007.

14. **Daniel Perovich, Leonardo Rodríguez, Martín Varela.** [En línea] 2001. [Citado el: 7 de Enero de 2009.] http://www.fing.edu.uy/inco/grupos/mf/Proyectos/Grado/JavaCard/progjavacard.pdf.

15. Ampliación de Señales Aleatorias / Reconocimiento Biométrico. *Escuela Politécnica Superior - EPS.* [En línea] 2008. [Citado el: 15 de Abril de 2009.] http://arantxa.ii.uam.es/~jortega/Evaluacion_Biometricos_v1.pdf.

16. **Martínez, María Raquel.** El documento electrónico. [En línea] [Citado el: 27 de Avril de 2009.] http://bibliotecavirtual.clacso.org.ar/ar/libros/argentina/cijs/SEC1014.HTML.

17. **Group, Information Highway.** The Information Highway Group. [En línea] 2004. [Citado el: 03 de 02 de 2009.] http://www.ihg.net/java/X?cgi=index.pattern.

GLOSARIO DE TÉRMINOS

1. **Autenticación**: procedimiento de comprobación del acceso del solicitante al sistema.

2. **Certificado electrónico**: un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

3. **Ciudadano**: toda persona física con nacionalidad cubana que solicita la expedición o renovación de un Documento Nacional de Identidad ante un funcionario de la OCI.

4. **Clave Pública** y **Clave Privada**: la criptografía asimétrica en la que se basa la PKI emplea un par de claves en la que lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

5. **Número de identificación personal (PIN)**: Secuencia de caracteres que permiten identificar a una persona.

6. **Documento electrónico**: conjunto de registros lógicos almacenado en soporte susceptible de ser leído por equipos electrónicos de procesamiento de datos, que contiene información.

7. **Datos de filiación**: Datos asociados a una persona en particular que pueden estar comprendidos por nombre y apellidos, dirección particular, lugar de nacimiento.

8. **Número de identificación**: Número único asociado a una persona en particular.

9. **Documento Nacional de Identificación (DNI)**: Documento emitido por autoridades del gobierno que identifican a un ciudadano con datos de filiación y un número de identificación.

10. **Firma electrónica**: es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.

11. **Titular**: ciudadano para el que se expide un certificado de identidad pública.

12. **Identificación**: procedimiento de reconocimiento de la identidad de un solicitante o titular del DNIe y su certificado electrónico.

13. **Oficial del registro de personas**: la persona física o jurídica, autoridad pública, que encargado de crear el DNI y el DNIe.

ANEXOS

Anexo 1: Descripción del Actor dl sistema.

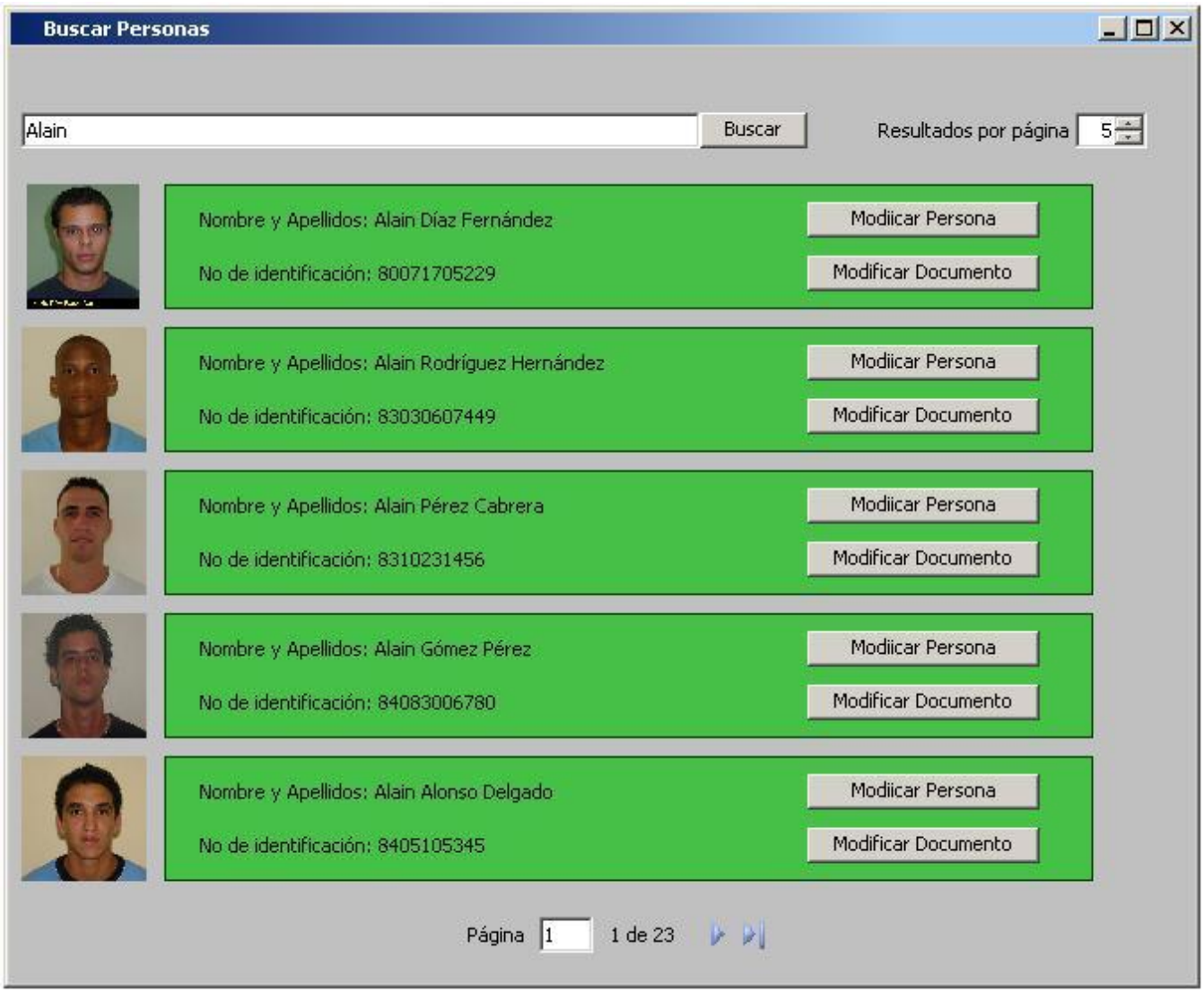
Nombre del actor	Descripción
Oficial del registro de personas	El oficial del registro de personas es el encargado de interactuar con el sistema para gestionar la información personal de los ciudadanos.

Tabla 3.1: Definición de actores del sistema.

Anexo 2: Descripción del Caso de uso del Sistema Buscar persona.

CASO DE USO		**Buscar Persona.**	
ACTORES	Oficial del registro de personas		
PROPÓSITO	Encontrar la persona.		
RESUMEN: El caso de uso se inicia cuando el oficial del registro de personas procede a buscar los datos de la persona, el sistema obtiene los datos de la persona contenidos en la tarjeta y con esta información busca, mostrándole al oficial del registro la información encontrada, terminando de esta forma el caso de uso.			
Precondiciones:	El oficial del registro de personas debe estar autenticado.		
CURSO NORMAL DE LOS EVENTOS.			
ACCIÓN DEL ACTOR		**RESPUESTA DEL PROCESO DEL SISTEMA**	
1	El oficial del registro de personas procede a buscar la Persona.	1.1	El sistema obtiene los datos de la persona almacenados en la tarjeta.
		1.2	El sistema busca los datos de la persona y muestra el resultado al oficial del registro. En caso de no encontrar los datos ir al 1.1 a
1.1 a Flujo alterno			
			El sistema muestra una excepción. Ir al 1
Prioridad	Crítico.		

Anexo 3: Prototipo de interfaz de usuario Buscar Personas.



Anexo 4: Descripción del Caso de uso del Sistema Registrar Datos Persona.

Caso de Uso del Sistema		Registrar Persona	
Actor	Oficial del registro de personas		
Propósito	Registrar los datos de la persona.		
Resumen: El caso de uso se inicia cuando el oficial del registro de personas entra los datos de la persona y procede a personalizar la Tarjeta, el sistema almacena los datos.			
Precondiciones:		El oficial del registro de personas debe estar autenticado.	
Curso normal de los eventos.			
ACCIÓN DEL ACTOR		**RESPUESTA DEL SISTEMA**	
1	El oficial de registro procede a registrar los datos de la persona.	1.1	El Sistema muestra el formulario, para que sean registrados los datos de la persona.
1	El oficial de registro de personas introduce los datos.	1.2	El Sistema almacena los datos de la persona. En caso de error conexión ir al 1.1 a En caso de que los datos insertados ya existan ir al 1.1 b
Prioridad		Crítico	
Flujo alterno 1.1 a		El sistema muestra una excepción. Ir al 1	
Flujo alterno 1.1 b		El sistema muestra un mensaje de advertencia. Ir al 1	

Anexo 5: Prototipo de interfaz de usuario Registrar Datos de Personas.

Anexo 6: Descripción del Caso de uso del Sistema Modificar Datos Persona.

Caso de Uso del Sistema		Modificar Persona	
Actor	Oficial del registro de personas		
Propósito	Actualizar los datos de la persona.		
Resumen: El caso de uso se inicia cuando el oficial del registro de personas modifica los datos de la persona y procede a personalizar la Tarjeta, el sistema almacena los datos.			
Precondiciones:	El oficial del registro de personas debe estar autenticado.		
Curso normal de los eventos.			
ACCIÓN DEL ACTOR		**RESPUESTA DEL SISTEMA**	
1	El oficial de registro procede a registrar los datos de la persona.	1.1	El Sistema muestra el formulario, para que sean registrados los datos de la persona que serán modificados.
1	El oficial de registro de personas introduce los datos.	1.2	El Sistema actualiza los datos almacenados. En caso de error conexión ir al 1.1 a En caso de que los datos insertados ya existan ir al 1.1 b
Prioridad		Crítico	
Flujo alterno 1.1 a		El sistema muestra una excepción. Ir al 1	
Flujo alterno 1.1 b		El sistema muestra un mensaje de advertencia. Ir al 1	

Anexo 7: Prototipo de interfaz gráfica Modificar Datos de Personas.

Anexo 8: Descripción del Caso de uso del Sistema Crear DNIe.

CASO DE USO DEL SISTEMA		**Crear Documento de Identificación.**	
ACTORES	Oficial del registro de personas		
PROPÓSITO	Crear el DNI electrónico.		
RESUMEN: El caso de uso se inicia cuando el oficial del registro de personas procede a crear el DNI electrónico, luego que se registra la persona el sistema le muestra el formulario, para que sean registrado los datos, se entra los datos de la persona y procede a crearle el DNIe, el sistema almacena los datos, terminando de esta forma el caso de uso.			
PRECONDICIONES	Tener una tarjeta conectada a la PC a través de un lector de tarjetas y una conexión a la Base de Datos del Sistema y estar autenticado previamente.		
POS CONDICIONES	Almacenar los datos en la Base de Datos del Sistema.		
CURSO NORMAL DE LOS EVENTOS.			
ACCIÓN DEL ACTOR		**RESPUESTA DEL SISTEMA**	
1	El oficial del registro de personas procede a crear el DNIe de la persona.	1.1	El Sistema después de registrar los datos de la persona muestra el formulario, para que sean registrados los datos del documento de identificación.
1	El oficial del registro de personas introduce los datos.	1.2	El sistema almacena los datos del DNI, creando de esta forma el DNIe en la tarjeta. En caso de error de conexión ir al 1.1 a
Prioridad	Crítico		
Flujo alterno 1.1 a			
	El sistema muestra una excepción. Ir al 1		

Anexo 9: Prototipo de interfaz de usuario Crear Documento de Identificación

Anexo 10: Descripción del Caso de Uso del Sistema modificar documento de Identificación.

CASO DE USO		**Modificar Documento de Identificación.**	
ACTORES	Oficial del registro de personas.		
PROPÓSITO	Actualizar información del DNIe.		
RESUMEN: En el caso de uso el oficial del registro de personas obtiene el documento de identificación de una persona para proceder a actualizar los datos del documento de identificación.			
Precondiciones:	El oficial del registro de personas debe estar autenticado.		
CURSO NORMAL DE LOS EVENTOS.			
ACCIÓN DEL ACTOR		**RESPUESTA DEL PROCESO DEL SISTEMA**	
1	El oficial del registro de personas procede a modificar el Documento de Identificación de la persona.	1.1	El sistema obtiene el documento de identificación y lo muestra en un formulario. En caso de error de conexión ir al 1.1 a
1	El oficial del registro de	1.2	El sistema actualiza el número del DNIe (DNI NUM), creando de

	personas introduce los datos del DNI a ser modificados.		esta forma un nuevo DNIe con los mismos datos del anterior pero con un nuevo DNI NUM, y almacenándolo en la BD y en la TI. En caso de error de conexión ir al 1.1 a
Prioridad	Crítico.		
Flujo alterno 1.1 a			
	El sistema muestra una excepción. Ir al 1		

Anexo 11: Prototipo de interfaz de usuario Modificar Documento de Identificación.

Anexo 12: Descripción del Caso de uso Autenticar usuario.

Caso de Uso del Sistema	Autenticar
Actor	Oficial del registro de personas
Propósito	Autenticarse
Resumen: El caso de uso se inicia cuando el oficial del registro de personas se identifica con el sistema mediante una clave.	
Precondiciones:	

Curso normal de los eventos.			
ACCIÓN DEL ACTOR		**RESPUESTA DEL SISTEMA**	
1	El oficial de registro procede a acceder al sistema.	1.1	El Sistema muestra el formulario para la autenticación.
1	El oficial de registro de personas introduce su clave.	1.2	El Sistema verifica la clave introducida se accede al sistema. En caso de no acceso ir al **1.1 a**
1.1 a Flujo alterno			
			El sistema muestra una excepción. Ir al 1
Prioridad		Secundario	

Anexo 13: Prototipo de interfaz de usuario Autenticar.