**Universidad de las Ciencias Informáticas**

**Facultad 1**

# **Título:** Applet y su componente middleware para la gestión de información en los pasaportes electrónicos

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

**Autores**: Nelson Hernández Guerra

Adrián Martínez Pérez

**Tutor:** Ing. Marvin Márquez Peralo

**Co-tutor:** Ing. Pedro E. Novales Hernández

**Consultante:** Msc. Adonis Cesar Legón Campo

"Ciudad de La Habana. Junio, 2011"

## DECLARACIÓN DE AUTORÍA

Declaro que somos los únicos autores de este trabajo y autorizamos al Centro de Identificación y Seguridad Digital de la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.

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

| | |
|---|---|
| _____ | _____ |
| Nelson Hernández Guerra | Ing. Marvin Márquez Peralo |
| _____ | _____ |
| Adrián Martínez Pérez | Ing. Pedro E. Novales Hernández |

**Datos de Contacto**

---

**Síntesis de los Tutores:**

- Marvin Márquez Peralo. Ingeniero en Ciencias Informáticas, graduado de la Universidad de Ciencias Informáticas. *Presenta* dos años de experiencia en el desarrollo de componentes de software.
- Pedro Enrique Novales Hernández. Ingeniero en Ciencias Informáticas, graduado de la Universidad de Ciencias Informáticas. *Presenta* dos años de experiencia en el desarrollo de componentes de software.

## AGRADECIMIENTO

*Agradezco a mis padres por ayudarme a lograr mis sueños, por darme en todo momento su amor, apoyo incondicional y por su preocupación. Agradecerles por enseñarme a ser una mejor persona en cada momento de mi vida. A mis hermanas por llenar con todo su cariño y amor aquellos momentos que estuvimos juntos, Mimi, Minerva, Dayi las quiero mucho. Agradecerle a mi madrastra Yordan por todo su amor y apoyo en momentos difíciles, a mi padrastro Rogelio por sus consejos, apoyo y amor por mí y por mi madre.*

*Agradezco a mis abuelos por su cariño, amor y por darme unos padres maravillosos, a mis tíos por su apoyo, Pedro, Ana, Maria, Virtudes, Bradis, Elvio, Roli, David, Lazaro, Regla y Dario, así como a mis primos y primas por compartir buenos momentos Marlon, Daiky, Wilfre, Daylien, Dachel, Francisco, Reinaldo, Darnier, Yane, Helen, Milisa, Claudia, Yilian, Yulexis y Alexander a todos muchas gracias.*

*No quisiera dejar de mencionar a Yanet, Mariela, Manolo, Mayte, Isabel así como a todos aquellos profesores Marvin, Dayron, Ander, Katerina, Vismar, Teddy y a mis mejores amigos Adrian, Alejandro, Oren, Dariel, Alberto, Rayner, Reynier, Felix y Andres que de una forma u otra me ayudaron a llegar hoy hasta aquí, a todos les agradezco por siempre.*

*A la Universidad por darme la oportunidad de graduarme y de conocer personas extraordinarias de todas las provincias de nuestro país.*

*A mi compañero de tesis (Adrian alias ¨el manga¨) por comprenderme, soportarme y compartir buenos momentos.*

*A todos los que no menciono que me ayudaron en la realización de este trabajo y en que yo fuera mejor persona… Muchas Gracias*

*Nelson H.G*

*Primeramente agradecer de todo corazón a mis padres, por apoyarme en la mayoría de las cosas y tratar de hacerme entender cuando mi cabezota iba por caminos incorrectos. No tengan ninguna duda que aunque se me hace difícil expresar mis sentimientos, junto a Lisi, son lo que más quiero en este mundo.*

*A mi hermanita Lisi, la mejor de todas las personas que he conocido, gracias por darme clases de moralidad y amistad, consciente e inconscientemente.*

*A mi abuela Eloina por apoyarme desde siempre sin importar nada de lo que haga y también por hacer la mejor comida del mundo, espero que te mejores.*

*A Alexis, por siempre estar junto a la familia como el mejor amigo que hemos tenido, gracias por ayudarme en la tesis y por ser mi ejemplo a seguir en muchas cosas.*

*A mi primo Islay, el mejor de todos los primos y una de las personas que siempre me ha apoyado y ha creído que puedo llegar lejos.*

*A todos mis amigos que han arrastrado conmigo desde hace un montón de tiempo, Pepe, El rubio, Vladiux, Yoendri, Rony, Mario, Boris, Patricia y Claudia, todos compañeros de armas en montones de locuras en mi oscuro tiempo de friki.*

*A los montones de amigos que he conocido en esta universidad, en especial al flaco, Oren, Onnier, Ariel, Robert, Guillermo, Reinier y Dariem.*

*A todos mis amigos fanes al anime, el manga y los juegos de rol, con los cuales he pasado montones de gratos momentos en la mella todos los jueves.*

*A mis amigos de Jagüey Norlys, Pipa, Vladi, Yuri e Ivan.*

*A mis subordinados en la revista Kuro Sora, por aguantarme como según me catalogan, un director tirano (al menos el tiempo que duro).*

*A mis pupilos directos, los cuales he tratado de culturizar desde que conocí, pero la sangre indígena que cargan siempre entorpece el procedimiento, Eduardo, Felix, Leonardo y Jose Alberto.*

*A mi compañero de tesis, que se incluye en la mayoría de los apartados anteriores, pero hay que dedicarle unas líneas especiales para que no se siente inferior, nada que al final logramos sacar lo que pensamos anclado al abismo.*

*A la mayoría de los integrantes del proyecto, por darnos su apoyo y ayuda cuando ellos mismos tenían gran cantidad de trabajo. En especial a Ander que pese a toda la carga que arrastraba supo dedicarnos algo de tiempo.*

*A nuestro tutores, en especial a Marvin por guiarnos en la realización de este trabajo.*

*A todas las personas que nos ayudaron en nuestro trabajo y he olvidado mencionar.*

*Muchas Gracias*

**DEDICATORIA**

*Quiero dedicar mi trabajo de Diploma a mis padres, a mis hermanas, a mi madrastra y a mi padrastro. A mi familia en general, a mi novia y a todos lo que de una forma u otra me ayudaron a estar aquí hoy, a todos muchas gracias.*

*A mi familia por el amor incondicional y el apoyo*

*Que me han dado.*

*Los Quiero…*

*Nelson*

*Dedico mi trabajo de diploma a muchísimas personas, pero en especial*

*A mis padres, a mi hermanita y a mi abuela, gracias por apoyarme*

*De todas las maneras posibles para seguir adelante.*

*Los quiero un montón…*

*Adrián*

## RESUMEN

Seguridad y portabilidad son las características que definen a la tecnología de tarjetas inteligentes que en los últimos años se ha destacado como la más ideal en el campo de la identificación digital. El pasaporte como documento de identidad con una necesidad de seguridad elevada ha optado por la utilización de la misma, creándose los llamados pasaportes electrónicos.

La utilización de los pasaportes electrónicos ha ido en aumento en los últimos tiempos, por lo que se han definido diversos estándares a seguir por los estados que utilicen dicho tipo de documento, permitiendo así una interoperabilidad entre todos los sistemas que sigan las especificaciones.

Por todo esto, los diversos estados del mundo han decidido comenzar con la utilización de esta novedosa y prometedora tecnología. Aunque en nuestro país aún no se ha realizado un cambio hasta este nuevo tipo de pasaporte, se tiene la necesidad de poseer un sistema propio para un posterior uso en los puertos internacionales, así como para implementar en la República Bolivariana de Venezuela, en la cual parte del sistema actual es desarrollado y atendido por Cuba.

El presente trabajo de diploma presenta un estudio sobre los actuales sistemas que utilizan pasaportes electrónicos o impliquen la tecnología de tarjetas inteligentes usada en los mismos. Teniendo como base todo el análisis realizado en la investigación, se desarrolló un prototipo de un sistema multiplataforma para interactuar con los pasaportes electrónicos y terminales que sigan los estándares definidos por la International Civil Aviation Organization (ICAO). El actual documento recoge toda la información resultante de nuestra investigación, presentándose características de otros sistemas actualmente implementados o en desarrollo, así como la descripción del diseño y la arquitectura seguida. Se describen los estándares que guiaron el desarrollo del sistema, así como las tecnologías utilizadas y los artefactos generados en el mismo.

**ÍNDICE**

AGRADECIMIENTO ..... III

DEDICATORIA ..... VI

RESUMEN ..... VII

ÍNDICE ..... VIII

INTRODUCCIÓN ..... 1

CAPÍTULO 1: FUNDAMENTACIÓN TEÓRICA SOBRE PASAPORTES ELECTRÓNICOS Y LAS TARJETAS INTELIGENTES ..... 6

1.1. Desarrollo de los pasaportes como documentos de identidad ..... 6

1.2. Pasaporte de lectura mecánica. ..... 7

1.3. Pasaportes Electrónicos ..... 9

1.4. Seguridad en los pasaportes electrónicos ..... 15

1.5. Tarjetas Inteligentes ..... 22

1.6. Conceptos Fundamentales ..... 24

1.7. Estándares ..... 25

1.8. Tecnología usada. ..... 29

1.9. Conclusiones. ..... 32

CAPITULO 2: DESCRIPCIÓN DE LA PROPUESTA DE SOLUCIÓN PARA UN APPLET Y SU COMPONENTE MIDDLEWARE ..... 33

2.1. Modelo de dominio. ..... 33

2.2. Glosario de términos del Modelo de dominio. ..... 34

2.3. Historias de usuario ..... 35

2.4. Requerimientos no funcionales. ..... 39

2.5. Metáfora ..... 40
2.6. Arquitectura ..... 41
2.7. Plan de entregas ..... 43
2.8. Estimación de tiempo. ..... 43
2.9. Plan de iteraciones. ..... 44
2.10. Estudio de Factibilidad ..... 44
2.11. Conclusiones ..... 52
CAPÍTULO 3: IMPLEMENTACIÓN Y PRUEBAS DEL APPLET PARA PASAPORTE ELECTRÓNICO Y SU COMPONENTE MIDDLEWARE ..... 53
3.1 Iteraciones a primera liberación ..... 53
3.2 Tareas de ingeniería ..... 54
3.3 Diseño de la solución ..... 55
3.4 Descripción del diseño ..... 55
3.5 Descripción del flujo de proceso: Solicitud de un servicio ..... 57
3.6 Fase de producción ..... 58
3.7 Pruebas unitarias ..... 58
3.8 Pruebas de aceptación ..... 59
3.9 Conclusiones ..... 63
CONCLUSIONES ..... 64
RECOMENDACIONES ..... 65
BIBLIOGRAFÍA CITADA ..... 66
BIBLIOGRAFÍA CONSULTADA ..... 67
GLOSARIO DE TÉRMINOS ..... 68

ANEXOS ..... 69
Anexo 1: Datos obligatorios y opcionales definidos para la LDS. ..... 69
Anexo 2: Plan de Entregas. ..... 70
Anexo 3: Multiplicadores de esfuerzo (factores de costo). ..... 70
Anexo 4: Factores de escala. ..... 71
Anexo 5: Entradas y Salidas externas. ..... 71
Anexo 6: Archivos lógicos internos. ..... 72
Anexo 7: Archivos externos de interfaces. ..... 72
Anexo 8: Puntos función desajustados. ..... 73
Anexo 9: Tablas de las tareas de la ingeniería. ..... 73
Anexo 10: Tarjetas CRC. ..... 81

## ÍNDICE DE FIGURAS

Figura 1: Logotipo de pasaporte-e .....10
Figura 2: Estructura del chip .....11
Figura 3: Pasos para la emisión de pasaporte .....13
Figura 4: Modelo de Dominio del Sistema.....33
Figura 5: Distribución de los componentes.....41
Figura 6: Diagrama de arquitectura.....42
Figura 7: Sub-fases de la fase Iteraciones a primera liberación. .....53
Figura 8: Diagrama de componentes. .....56
Figura 9: Diagrama de Secuencia "Leer pasaporte electrónico".....57
Figura 10: Datos obligatorios y opcionales definidos para la LDS. .....69

## ÍNDICE DE TABLAS

Tabla 1: Método de seguridad básico ..... 21
Tabla 2: HU1 Gestión de la comunicación. ..... 36
Tabla 3: HU2 Permitir la autenticación activa y pasiva. ..... 37
Tabla 4: HU3 Permitir la autenticación mediante el control de acceso básico. ..... 37
Tabla 5: HU4 Gestionar la información en el documento de viaje electrónico. ..... 38
Tabla 6: HU5 Gestionar el sistema de ficheros. ..... 39
Tabla 7: Estimación de tiempo de las historias de usuario. ..... 43
Tabla 8: Plan de iteraciones. ..... 44
Tabla 9: Cálculo de las líneas de código. ..... 49
Tabla 10: Distribución de las tareas de ingeniería por iteraciones. ..... 55
Tabla 11: HU1_CP1 - Gestión de la comunicación. ..... 60
Tabla 12: HU3_CP2 – Permitir la autenticación mediante el control de acceso básico. ..... 60
Tabla 13: HU4_CP3 – Gestionar la información en el pasaporte electrónico. ..... 61
Tabla 14: HU5_CP4 – Gestionar el sistema de ficheros. ..... 62
Tabla 15: HU2_CP5 – Permitir la autenticación activa y pasiva. ..... 62
Tabla 16: Plan de entregas. ..... 70
Tabla 17: Multiplicadores de esfuerzo (factores de costo). ..... 70
Tabla 18: Factores de escala. ..... 71
Tabla 19: Entradas externas. ..... 71
Tabla 20: Salidas externas. ..... 72
Tabla 21: Archivos lógicos internos. ..... 72
Tabla 22: Archivos externos de interfaces. ..... 72
Tabla 23: Puntos función desajustados. ..... 73
Tabla 24: HU1_T1 Detectar lector conectado. ..... 73
Tabla 25: HU1_T2 Establecer conexión con el pasaporte electrónico. ..... 74
Tabla 26: HU1_T3 Cerrar conexión con el pasaporte electrónico. ..... 74
Tabla 27: HU3_T1 Obtener los datos del código de barra de la zona de lectura mecánica. ..... 75

Tabla 28: HU3_T2 Decodificar la clave del código de barra y compararla con la clave almacenada en el chip. ..... 75
Tabla 29: HU3_T3 Permitir o negar la comunicación en dependencia del resultado de la verificación de la clave. ..... 76
Tabla 30: HU3_T4 Cifrar la comunicación entre el lector y el chip. ..... 76
Tabla 31: HU4_T1 Leer los datos almacenados en el documento electrónico de viaje. ..... 77
Tabla 32: HU4_T2 Modificar los datos almacenados en el documento electrónico de viaje. ..... 77
Tabla 33: HU4_T3 Eliminar los datos almacenados en el documento electrónico de viaje. ..... 78
Tabla 34: HU5_T1 Crear un EF.SOD para la autenticidad/integridad de los datos del pasaporte electrónico. ..... 78
Tabla 35: HU5_T2 Definir los grupos de datos obligatorios y opcionales. ..... 79
Tabla 36: HU2_T1 Generar clave personalizada del chip. ..... 79
Tabla 37: HU2_T2 Cifrar clave. ..... 80
Tabla 38: HU2_T3 Generar fichero con los códigos hash de todos los archivos almacenados. ..... 80
Tabla 39: HU2_T4 Generar firma digital usando los códigos hash almacenados en el fichero y la firma digital del país expedidor. ..... 81
Tabla 40: CRC middleware – AAEvent. ..... 81
Tabla 41: CRC middleware – BACEntry. ..... 81
Tabla 42: CRC middleware – BACEvent. ..... 82
Tabla 43: CRC middleware – CBEFFDataGroup. ..... 82
Tabla 44: CRC middleware - MRZInfo. ..... 83
Tabla 45: CRC middleware – FaceInfo. ..... 83
Tabla 46: CRC middleware - Passport. ..... 85
Tabla 47: CRC middleware – PassportApduService. ..... 85
Tabla 48: CRC middleware – PassportPersoService. ..... 86
Tabla 49: CRC applet – PassportApplet. ..... 86
Tabla 50: CRC applet – FileSystem. ..... 87
Tabla 51: CRC applet – PassportCrypto. ..... 87

## INTRODUCCIÓN

Desde siempre el comercio y la migración han sido piezas clave en el desarrollo de los pueblos. Con el paso del tiempo fue necesario controlar los movimientos y actividades de las personas alrededor del mundo, debido a las entradas ilegales de agentes espías. Fue durante la Primera Guerra Mundial donde los gobiernos introdujeron los requisitos de los documentos de viaje en la frontera por razones de seguridad, estos controles pronto se convirtieron en una característica institucionalizada de los viajes internacionales, donde los gobiernos reafirmaron el derecho a controlar la entrada y salida de las personas por los territorios nacionales e internacionales bajo su control. Estos controles con el paso de los años se mantuvieron y se convirtieron en un procedimiento estándar.

Pronto se otorgó a estos documentos de viaje una especie de cuaderno o cuadernillo, donde se insertaban las autorizaciones de otros países para ingresar y salir de ellos, que se denominaron visados o visas; al mismo tiempo se le dio al documento validez internacional, la cual siempre fue sujeta a la condición de que los países se reconozcan entre sí. La normalización de los documentos de viaje se produjo en 1980, bajo los auspicios de la ICAO, surgiendo así diferentes tipos de documentos de viaje, dentro de los que están el Documento Nacional de Identidad (DNI) y el pasaporte.

Dentro de los pasaportes aparecen diversos tipos entre los que están: pasaporte ordinario, también llamado pasaporte turístico, pasaporte oficial, llamado pasaporte del servicio y el pasaporte diplomático. Como consecuencia de la diversificación de los pasaportes, ICAO recomienda a los gobiernos nacionales diferentes estándares como son los documentos de viaje de lectura mecánica 9303 en sus tres partes, Logical Data Structure (LDS), Public Key Infrastructure (PKI), así como el uso de los circuitos integrados sin contacto en los documentos de viaje de lectura mecánica, además el formato que debe regir los pasaportes, los cuales incluyen el nombre del país, un símbolo nacional, una descripción del documento (pasaporte, pasaporte oficial, pasaporte diplomático), si es un pasaporte electrónico el símbolo que lo identifica, una página de título nombrando el país, seguido por una página con los datos del titular y páginas en blanco disponibles para que los países extranjeros incluyan visas y estampen las entradas así como las salidas.

Con el desarrollo de las Tecnologías de la Informática y las Comunicaciones (TIC) y en un esfuerzo por hacer pasaportes más seguros, en Malasia en el año 1998 aparecen los primeros pasaportes electrónicos, los que incluyen una tarjeta inteligente sin contacto, con comunicación por Radio Frequency Identification (RFID). Estos pasaportes-e *(*pasaportes electrónicos*)* incluyen un circuito integrado que almacena la información que se encuentra impresa en la página del Pasaporte de Lectura Mecánica (PLM) que contiene los datos del titular; así como puede sostener una firma digital, datos para asegurar la integridad del pasaporte y datos biométricos.

Con la introducción de esta nueva tecnología en los pasaportes, la seguridad de los mismos se fortaleció, pero no fue hasta después del 11 de septiembre del 2001 por causa del atentado terrorista a las Torres Gemelas, que se intensificó a nivel mundial el uso de los pasaportes-e. Se aumentó la seguridad en los nuevos pasaportes electrónicos con la ejecución de diferentes métodos como Basic Access Control (BAC), Passive Authentication (PA), Extended Access Control (EAC), y Active Authentication (AA). Estas nuevas medidas permiten que los pasaportes no sean falsificados o manipulados, Tanto así que actualmente más de 190 países optan por el uso de los pasaportes electrónicos.

En la hermana República Bolivariana de Venezuela hoy en día se hace uso de un sistema para este tipo de pasaporte, el cual fue desarrollado por Cuba y Alemania. Donde el Centro de Identificación y Seguridad Digital (CISED) de la Universidad de las Ciencias Informática (UCI) se encarga de verificar y gestionar la información, mientras que la empresa alemana Bundes Druckerei, es la encargada del desarrollo de un middleware y de un applet que es instalado en el chip integrado al pasaporte electrónico, así como de la impresión y personalización del mismo, lo que lleva a la siguiente situación problémica: existe una dependencia tecnológica con este sistema, dificultando la realización de pruebas unitarias debido al desconocimiento del funcionamiento interno del mismo.

Con el análisis de lo antes expuesto y con el fin de darle solución a la situación problemática existente, este trabajo plantea el siguiente problema científico: ¿Cómo gestionar la información presente en los pasaportes electrónicos?

Para dar solución al problema científico se asume como objeto de estudio**:** el proceso de gestión de información almacenada en los pasaportes electrónicos. Se desarrolló como campo de acción: la creación

de un applet y su componente middleware para la gestión de la información almacenada en los pasaportes electrónicos en la República Bolivariana de Venezuela.

Por lo que el objetivo general de esta investigación es: desarrollar un applet y su componente middleware que permitan gestionar la información presente en los pasaportes electrónicos.

A partir del análisis del objetivo general se derivaron los siguientes objetivos específicos:

- Realizar un estudio de las soluciones existentes para la gestión de la información en los pasaportes electrónicos.
- Identificar estándares existentes para la comunicación con tarjetas inteligentes y la organización de la información en los pasaportes electrónicos.
- Realizar el análisis, diseño e implementación de los componentes Applet y un Middleware multiplataforma que posibiliten la gestión de la información en los pasaportes electrónicos.
- Desarrollar un prototipo de aplicación para la lectura y personalización de los pasaportes electrónicos.

Para darle cumplimiento a los objetivos antes mencionados se definen las siguientes tareas:

- Estudiar soluciones existentes para la gestión de la información en los pasaportes electrónicos.
- Estudiar estándares ISO/IEC 14443, ISO/IEC-7816 sobre la tecnología de tarjetas inteligentes y los estándares 9303, LDS del ICAO para pasaportes electrónicos.
- Elaborar la documentación y diagramas de ingeniería de software necesarios para el análisis y diseño de la solución.
- Desarrollar un applet y su componente middleware multiplataforma para gestionar la información en los pasaportes electrónicos en la República Bolivariana de Venezuela.
- Proponer un prototipo de aplicación para la lectura y personalización de los pasaportes electrónicos, el cual empleará el applet y middleware desarrollados.

- Realizar las pruebas de calidad al prototipo de aplicación propuesto, así como pruebas al applet y middleware.

Esta investigación defiende la idea de: la implementación de un applet y su componente middleware para aplicar en la República Bolivariana de Venezuela, que permitirá gestionar la información en los pasaportes electrónicos y ganar independencia tecnológica.

Los siguientes métodos científicos sustentaran la investigación:

Teórico:

El método Histórico-Lógico posibilito obtener conocimiento sobre la evolución y el desarrollo de los diferentes elementos asociados a las tecnologías de tarjetas inteligentes y de los pasaportes electrónicos.

Se utilizó el método de la Modelación para crear abstracciones de los diferentes elementos a lo largo de la investigación, como fueron los diagramas de dominio, diagrama de componente y diagrama de secuencia, los cuales nos ayudaron en la comprensión y simplificación del trabajo.

El método Analítico-Sintético nos permitió la comprobación y utilización de fuentes bibliográficas de las cuales seleccionamos y sintetizamos información que nos fue útil para la realización de nuestro tema.

Empírico:

La Observación como método de forma pasiva nos proporcionó una visión detallada sobre los diferentes elementos que utilizamos, permitiéndonos visualizar de forma directa diferentes herramientas y equipos, para el uso de la tecnología de tarjetas inteligentes y pasaportes electrónicos.

## .Estructura de la tesis

El trabajo se encuentra estructurado de la siguiente forma:

**Capítulo 1. Fundamentación teórica sobre pasaportes electrónicos y las tarjetas inteligentes:** Este capítulo contiene una base teórica para entender el problema planteado, en él se describen los conceptos fundamentales relacionados con aplicaciones Applet y Middleware además de hacer referencia a las tecnologías relacionadas con los pasaportes electrónicos.

**Capítulo 2. Descripción de la propuesta de solución para un applet y su componente middleware:** Se presentan las fases de Exploración y Planificación definidas por la metodología Extreme Programming (XP) para dar solución al problema científico, se identifica el modelo de dominio, las historias de usuarios y los requisitos no funcionales, se realizan el plan de iteraciones y plan de entregas, así como sobre la estimación de cuán factible será el desarrollo del sistema.

**Capítulo 3. Implementación y pruebas del applet para pasaporte electrónico y su componente middleware:** Se muestra el modelo de implementación, el modelo de despliegue y las técnicas usadas durante la implementación, además del diseño de los casos de prueba.

# CAPÍTULO 1: FUNDAMENTACIÓN TEÓRICA SOBRE PASAPORTES ELECTRÓNICOS Y LAS TARJETAS INTELIGENTES

El presente capítulo se aborda variados aspectos sobre los pasaportes, más específicamente los pasaportes electrónicos, la seguridad de los mismos y su uso actual en los países del mundo. También el capítulo cuenta con varios apartados dedicados a la tecnología de tarjetas inteligentes en los que entre otros se incluye la seguridad lógica y física de las mismas. Se hace mención a las tecnologías mayormente usadas para desarrollar aplicaciones para las tarjetas inteligentes, así como los diversos estándares para regirse a la hora de trabajar con dicha tecnología y ser aplicada en los pasaportes.

## *1.1. Desarrollo de los pasaportes como documentos de identidad*

Un pasaporte es un documento personal, individual e intransferible con validez internacional, que certifica a su titular (en ciertos países también a sus descendientes directos e incluso a sus cónyuges), expedido por las autoridades de su respectivo país, que acredita un permiso o autorización legal para que salga o ingrese al mismo, por los puertos internacionales. Los elementos que son incluidos en el pasaporte son el carnet de identidad, nombre, fecha de nacimiento, sexo, lugar de nacimiento o cualquier otro dato que el país de procedencia desee agregar. Un pasaporte por lo general da derecho al titular del pasaporte para regresar al país que haya expedido el pasaporte. El derecho a la protección consular se deriva de los acuerdos internacionales y el derecho a regresar surge de las leyes del país emisor. Un pasaporte no representa el derecho o el lugar de residencia del titular del pasaporte en el país que haya expedido el pasaporte. (Organización de Aviación Civil Internacional, 2006)

El formato de un pasaporte estándar incluye el nombre del país emisor, en la portada del pasaporte, un símbolo nacional, una descripción del documento (por ejemplo, pasaporte, pasaporte oficial, pasaporte diplomático), y si el pasaporte es biométrico el símbolo que lo clasifica. En el interior hay una página de título, también de denominación del país. Esto es seguido por una página de datos, en la que se dispone de información sobre el portador y la autoridad de expedición. Hay páginas en blanco para los países extranjeros para colocar los visados, y proceder al sellado de las entradas y salidas. Los pasaportes

tienen designadores numéricos o alfanuméricos ("número de serie") asignados por la autoridad expedidora y los estándares del pasaporte son recomendados a los gobiernos nacionales por la ICAO.

Un pasaporte contiene un mensaje oficial emitido por el país que expide dicho documento. El mensaje que generalmente está cerca del frente o al final del pasaporte, solicita que al portador del pasaporte le sea permitido pasar libremente, y otras peticiones, como que en caso de necesidad, al portador se le conceda ayuda. Las leyes típicas sobre pasaportes declaran que los mismos son propiedad del estado, y pueden ser limitados o revocados en cualquier momento, generalmente en los argumentos especificados.

Los países tienen diversos estilos en las estampillas para las entradas y las salidas, para facilitar la identificación de los movimientos de personas. El color de la tinta puede también proporcionar la información sobre los movimientos. En Hong Kong, antes e inmediatamente después de la transferencia en 1997 de la soberanía, las estampillas de la entrada y de la salida eran idénticas en todos los puertos de la entrada, pero los colores diferenciaron. El aeropuerto estampa la tinta negra, la tierra estampa la tinta roja, y el mar estampa la tinta púrpura. En varios países las estampillas o su color son diferentes si la persona llegó en un coche o como pasajero del autobús/del barco/del tren/del avión.

### *1.2. Pasaporte de lectura mecánica.*

La ICAO en el 2005 aprueba una nueva norma por la contratación de 188 Estados los cuales deben expedir los nuevos pasaportes de lectura mecánica (PLM) con arreglo al Doc. 9303, Parte 1, Volumen 1 y opcionalmente Volumen 2, donde se definen las especificaciones a las que deben ajustarse los pasaportes de lectura mecánica, para hacer posible el intercambio mundial de los datos empleando tanto medios visuales (lectura ocular) como la lectura mecánica (reconocimiento óptico de caracteres). Como mínimo, el PLM contendrá los datos obligatorios especificados en estos volúmenes, en el formato normalizado prescrito.

El pasaporte de lectura mecánica cumple con las especificaciones que figuran en el Doc. 9303, Parte 1, Volumen 1, y opcionalmente, Volumen 2. Está normalmente elaborado en forma de libreta (tamaño-ID-3) con páginas que contienen información sobre el titular, el estado u organización expedidores, páginas para visados y otras anotaciones. La información de lectura mecánica está comprendida en dos líneas de texto Optical Character Recognition (OCR-B), de 44 caracteres cada una. Estas especificaciones permiten

que el PLM tenga forma de tarjeta independiente de tamaño ID-1; como se especifica en el Doc. 9303. (Organización de Aviación Civil Internacional, 2006)

La página de datos del pasaporte de lectura mecánica tiene una dimensión fija, donde se presentan en formato estándar datos visuales y de lectura mecánica. La cual puede colocarse en el anverso o reverso de una página interior adyacente a la cubierta o en la parte interior de la cubierta anterior o posterior en el pasaporte. El visado de lectura mecánica (VLM), se conoce como autorización de entrada, la cual se ajusta a las especificaciones que figuran en el Doc. 9303, Parte 2. Por lo común el visado de lectura mecánica, se adjunta a una página de visado del pasaporte. Existe también un visado de lectura mecánica de tamaño normal (Formato - A) (VLM-A), ajustándose a las dimensiones especificadas en el Doc. 9303, Parte 2, cuyo tamaño cubre por completo la página de visados del pasaporte.

Las especificaciones técnicas para los pasaportes de lectura mecánica se presentan en dos secciones:

**Sección III-** Especificaciones técnicas para los elementos de seguridad que han de incorporarse en la libreta en el momento de fabricación y personalización, conjuntamente con especificaciones relativas a la seguridad de las instalaciones en las que se realizan tales operaciones, además de métodos seguros para la auditoría y la expedición. ( Organización de Aviación Civil Internacional, 2006)

**Sección IV-** Especificaciones técnicas aplicables a todos los pasaportes de lectura mecánica. (Organización de Aviación Civil Internacional, 2006)

Dentro de las especificaciones necesarias que figuran en el Doc. 9303 Parte 1, Volumen 2 para los estados que expidan pasaporte electrónico, se encuentra la incorporación de la identificación biométrica al pasaporte. Para los cuales existen especificaciones obligatorias u opcionales para el estado expedidor a efectos de asegurar que su pasaporte y los medios de personalización del titular legítimo del documento, están protegidos contra acciones fraudulentas. Se proporcionan especificaciones obligatorias para la seguridad física que ha de brindarse en los locales donde se producen y personalizan los pasaportes, así como la inspección y control del personal que participa en tales operaciones. Los pasaportes se diseñarán para incorporar garantías contra acciones fraudulentas durante su período de validez.

El estado expedidor puede incorporar en su pasaporte uno o más elementos de seguridad que exijan el uso de un equipo de detección para establecer y verificar su presencia dentro del tiempo normal del

trámite de despacho de inmigración. Por consiguiente, los estados tienen la plena libertad de escoger ninguno, uno o más de los elementos verificables por una máquina para ayudar a la verificación del documento, pero tales elementos serán para su uso propio o bilateral convenido. ( Organización de Aviación Civil Internacional, 2006)

El estado que expida el pasaporte de lectura mecánica se cerciorará de que los locales donde se imprima, encuaderne, personalice y expida el pasaporte sean altamente seguros, así como que las personas que trabajan en ellos cuenten con una autorización de seguridad apropiada. Se debe proporcionar una seguridad apropiada para los pasaporte en el tránsito entre instalaciones y desde la instalación al titular del pasaporte. El estado que introduzca un nuevo diseño en el PLM debe informar a los otros estados sobre los detalles del nuevo pasaporte, incluyendo los elementos de seguridad evidentes, mediante especímenes personalizados para utilizarlos como referencia en el departamento del estado receptor encargado de verificar la autenticidad de los pasaportes. Los estados deberían proporcionar información específica sobre pasaportes extraviados o robados (como por ejemplo el número del pasaporte o el número de libreta) a la base de datos central de la International Criminal Police Organization (INTERPOL) en el momento oportuno y con arreglo a procedimientos convenidos. Esto comprende detalles sobre cualquier PLM no personalizado que pueda ser robado de una instalación de producción o expedición o en tránsito. ( Organización de Aviación Civil Internacional, 2006)

### *1.3. Pasaportes Electrónicos*

El pasaporte electrónico también conocido como pasaporte biométrico, es un documento de identidad que combina el papel y una tarjeta inteligente que se comunica por radiofrecuencia. El mismo usa la biometría para autentificar la ciudadanía de los viajeros. La incorporación del minúsculo chip RFID en el documento permite tanto almacenar información adicional como duplicar la que se encuentra impresa en la página que contiene los datos del titular del pasaporte, permitiendo a través de una infraestructura de clave pública la certificación de la veracidad de los datos contenidos en él, haciendo virtualmente imposible forjar identidades falsas.

Un pasaporte electrónico debe ajustarse totalmente a las especificaciones proporcionadas en el Doc. 9303, Parte 1, Volumen 1 así como, Volumen 2. El pasaporte-e tiene un período de validez el cual queda a discreción del estado expedidor, el que recomienda un período de validez que no supere los 10 años.

Los Estados podrían considerar un período más breve para permitir la actualización progresiva del pasaporte-e a medida que evoluciona la tecnología. Todos los pasaportes-e llevarán el símbolo siguiente (figura 1)

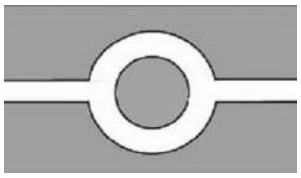

**Figura 1: Logotipo de pasaporte-e**

El símbolo solo puede aparecer en un PLM que contenga una micro plaqueta sin contacto, con capacidad de almacenamiento de datos de por los menos 32 KB, los datos codificados según el Doc. LDS, una imagen del rostro del titular, así como todos los datos ingresados protegidos con una firma digital. A menos que un pasaporte no se ajuste a estos requisitos mínimos, y no presente dicho símbolo el cual aparecerá en la cubierta anterior del pasaporte-e cerca del borde superior o del inferior de la cubierta, no será catalogado como pasaporte-e. El símbolo debe regirse por las dimensiones recomendadas en el Doc. 9303, Parte 1, Volumen 2.

El chip utilizado en los PLM, es un chip sin contacto, que cumple con la International Organization for Standardization (ISO) 14443 (proximidad entre 0 – 10 cm); las razones por las que se seleccionó este estándar son:

**Interoperatibilidad global**: al operar por radiofrecuencia (RF) hay diferentes bandas de RF usadas, pero la definida en la 14443 está disponible mundialmente. El uso de un estándar también prevé el uso de implementaciones propietarias.

**Diferentes métodos de inspección en la frontera**: pudiera ser que el portador del documento lo presente ante un oficial de inspección o un sistema automático, mediante el cual el chip es interrogado y se otorga o deniega automáticamente el permiso de entrada. La proximidad seleccionada admite cualquiera de estos dos tipos de inspección.

**El lector del chip:** solamente es necesario que requieran chips conformes a la ISO 14443 A y B.

En el PLM, el chip es pasivo, lo que significa que no contiene fuente de energía por sí solo. La razón para esto es que si contiene fuente de energía, no sería posible que durara el tiempo de vida esperado del PLM que es de 10 años, lo cual se logra siendo el lector el que provee la energía para comunicarse con el chip. El circuito integrado está formado por el chip y una antena, figura 2.

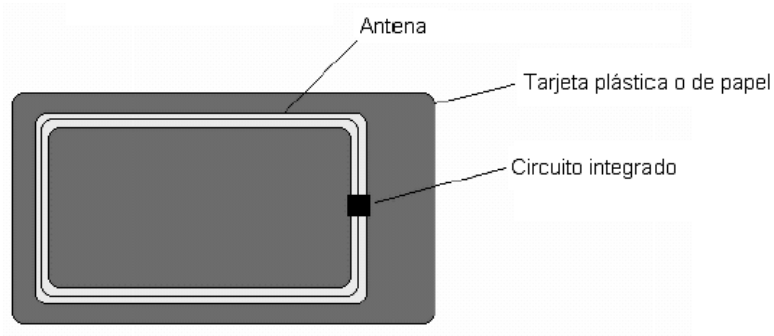


**Figura 2: Estructura del chip**

Los datos al ser almacenados en el chip requieren de una estructura lógica de datos estandarizada para habilitar una interoperatibilidad global para los PLM, facilitando que todas las naciones tengan conocimiento de cómo está estructurado el documento. El LDS está conformado por elementos de datos (ED) de uso obligatorio u opcional y un orden agrupado en elementos de datos. Dentro del LDS, los elementos de datos se agrupan según su organización lógica y son definidos como grupo de datos (GD), cada uno de ellos está identificado con un número. ( Organización de Aviación Civil Internacional, 2006)

Los datos en el chip están almacenados en el sistema de ficheros definidos por la ISO 7816-4. Los ficheros están organizados jerárquicamente empezando por el fichero maestro (FM), determinado por el sistema operativo, que será la raíz del sistema de ficheros compuestos por los ficheros dedicados (FD) y ficheros elementales (FE). Los FD contienen los ficheros elementales y otros ficheros dedicados. Cada grupo de datos consiste en una serie de datos dentro de una plantilla y será almacenado en un FE separado. La estructura y codificación de los datos está definida en la ISO 7816-4 y 7816-6. Cada dato posee una identificación, que es especificada en un código hexadecimal. Cada dato contenido dentro de un grupo de datos posee una única identificación, longitud y valor.

El FE.COM almacena los datos comunes que corresponden fundamentalmente a la organización de los datos dentro del chip. El identificador corto del fichero es 30 (IE). Cada grupo de datos deberá ser

almacenado en un FE accesible por un identificador corto del fichero. El FE deberá tener el nombre del fichero que se corresponderá con el grupo de datos que contenga, el nombre del fichero FE que contiene los datos de seguridad se denomina FE.SOD. (Organización de Aviación Civil Internacional, 2006)

El mínimo de comandos soportados por los PLM son:

- SELECT FILE
- READ BINARY

Los parámetros de estos comandos son obligatorios u opcionales. Todos los comandos, formatos y sus códigos de retorno están definidos en la ISO 7816-4.

La ICAO propone varios mecanismos de seguridad para el PLM, de ellos algunos son de cumplimiento obligatorio y otros opcionales, según decisión del país emisor. Estos mecanismos se mencionan a continuación:

- Autenticación Pasiva
- Autenticación Activa
- Control de Acceso Básico
- Control de Acceso Extendido
- Encriptación de Datos

Estos tipos de documentos requieren una infraestructura tecnológica necesaria para la captura de datos e imágenes de los ciudadanos, validación de la identidad, personalización del documento y entrega del mismo, paso fundamental para la emisión del pasaporte, ilustrado en la Figura 3. Cada uno de estos componentes se concibe de forma independiente, funcionando de forma modular.

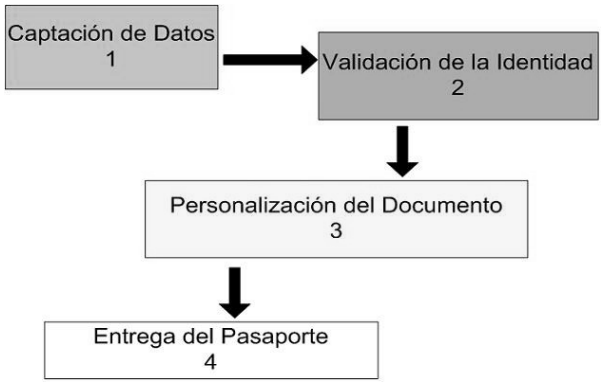


**Figura 3: Pasos para la emisión de pasaporte**

Para la captura de datos se inicia el trámite del pasaporte y se captan los datos del ciudadano y su foto, además de los elementos biométricos que decida incluir el estado emisor. Durante la captura de datos e imágenes es importante tener en cuenta que la foto cumpla con las características que establece la ICAO.

Los medios de verificación de la identidad se centran en la verificación biométrica (identificación o verificación de la identidad en forma automatizada, de seres humanos vivos, haciendo uso de sus características fisiológicas o de comportamiento) de los ciudadanos de forma automatizada, debido a que: se logra el aumento de los niveles de productividad y se minimiza el error humano y la corrupción. Entre las tecnologías biométricas comerciales más usadas resaltan la biometría dactilar, el reconocimiento facial, la geometría de la mano, el reconocimiento de iris, el reconocimiento dinámico de firma, el reconocimiento de voz, el reconocimiento de cadencia de digitación y la geometría de dedos. La más usada a nivel mundial es la biometría dactilar por diversas ventajas que ofrece frente a otras tecnologías. (Organización de Aviación Civil Internacional, 2006)

La personalización de este tipo de documento cuenta con dos factores:

- Personalización Eléctrica: se refiere a la escritura de los datos en el chip. (Organización de Aviación Civil Internacional, 2006)
- Personalización Óptica: Se personalizan los datos que se encuentran en la zona de inspección visual (ZIV). (Organización de Aviación Civil Internacional, 2006)

La personalización sugiere que sea de forma centralizada, por medidas de seguridad y control del documento. Incluye los procesos de personalización, control de la calidad, empaquetado, embalado y envío al ciudadano o a la oficina donde se inició el trámite. Durante el proceso de entrega se cierra el trámite correspondiente al ciudadano, en este momento podría hacerse el chequeo biométrico según los datos almacenados en el documento para asegurarse de que realmente pertenecen al portador, que los datos almacenados sean suficientes y cuenten con la calidad necesaria para la verificación biométrica.

### *1.3.1. Pasaporte Venezolano*

Es el documento expedido a los ciudadanos venezolanos, que les identifica y les permite viajar fuera del territorio de Venezuela. Desde julio de 2007, Venezuela empieza a expedir pasaporte biométrico, el cual contiene un chip RFID en el que se registra, además de los datos alfanuméricos del titular, información adicional como una fotografía o huellas dactilares. De acuerdo con las leyes vigentes en Venezuela, todos los pasaportes antiguos (sin datos biométricos), son válidos hasta su fecha de expiración, con la excepción del antiguo pasaporte de color azul, que ya no es válido para viajar a los Estados Unidos de América. Actualmente, el pasaporte venezolano es de color borgoña o vino tinto, con la inscripción del nombre oficial de la nación (República Bolivariana de Venezuela) y el escudo de armas en color dorado.

### *1.3.2. Pasaporte Canadiense*

Canadá no se queda detrás en cuanto a tecnologías por lo que ha introducido recientemente la biometría en el uso de los pasaportes. Los pasaportes incluyen un chip que contiene una imagen de la persona y la información personal tal como el nombre y la fecha de nacimiento entre otros datos. En el presupuesto federal 2008, el Ministro de las finanzas anunció que el pasaporte electrónico será introducido en 2011.

Esta tecnología se está utilizando en los pasos de frontera que tienen lectores electrónicos que puedan leer el chip en las tarjetas y verificar la información presente en la misma y en el pasaporte. Este método tiene como objetivo el aumentar la eficacia de la exactitud para identificar a las personas en el paso de la frontera.

### *1.3.3. Pasaporte estadounidense*

Para los Estados Unidos después de los ataques del 11 de septiembre de 2001, por causa de los cuales el nivel de la seguridad se convirtió en una máxima prioridad, los extranjeros que deseen viajar a los Estados Unidos deben poseer un pasaporte biométrico por su alta seguridad en el control de las fronteras. El Departamento del estado ahora publica pasaportes biométricos solamente, aunque los pasaportes sin las virutas siguen siendo válidos para la totalidad de sus períodos respectivos. Los Estados Unidos de América ahora publican pasaportes biométricos solamente.

### *1.3.4. Java Machine Readable Travel Documents*

En un estudio del arte de nuestro trabajo de diploma encontramos una aplicación libre para los pasaportes electrónicos llamada Java Machine Readable Travel Documents (JRMTD) la cual cumple con las normas especificadas por la ICAO. Este proyecto brinda ayuda, soporte y herramientas para los interesados en crear proyectos y aplicaciones acerca de los pasaportes electrónicos, lo cual nos sirvió de base para la realización de nuestro trabajo.

## *1.4. Seguridad en los pasaportes electrónicos*

En los últimos años se han reportado gran cantidad de falsificaciones, fraudes y copias ilegales de pasaportes como consecuencia del incremento en la delincuencia internacional y la inmigración ilegal, se ha agudizado la preocupación por la seguridad de los documentos de viaje y por lo que podría hacerse para mejorar su resistencia a las adulteraciones o a un uso indebido. Con este objetivo los asesores técnicos de la ICAO, decidieron que sería conveniente publicar un conjunto de “normas mínimas de seguridad recomendadas” como orientación para todos los Estados que expidan documentos de viaje de lectura mecánica (DVLM).

Los estados expedidores son responsables de los materiales empleados en la creación de los documentos, los métodos de impresión de seguridad y de protección y de los procesos de formación de imágenes y acabado que intervienen para personalizar y proteger los datos personales del documento.

Dentro de los principios básicos para la seguridad de los PLM están:

- La producción de las libretas de pasaportes que incluyen los procesos de personalización debe llevarse a cabo en un ambiente seguro y controlado que cuente con las medidas de seguridad apropiadas para impedir el acceso no autorizado a las instalaciones. (Organización de Aviación Civil Internacional, 2006)

- Deberá hacerse una conciliación completa con los registros que se lleven para dar cuenta de todos los materiales que hayan sido usados. (Organización de Aviación Civil Internacional, 2006)

- Los materiales empleados en la producción de PLM deberán ser de variedades controladas y obtenerse exclusivamente de proveedores de materiales de seguridad auténticos. Conviene usar materiales destinados sólo a aplicaciones de alta seguridad y evitar materiales que el público generalmente puede conseguir en el mercado abierto. (Organización de Aviación Civil Internacional, 2006)

- Se deben elegir bien la combinación de elementos, materiales y técnicas de seguridad de manera que sean compatibles entre sí y protejan el documento durante su vida útil. (Organización de Aviación Civil Internacional, 2006)

- La incorporación de elementos de seguridad y métodos que sirvan de protección contra reproducciones y alteraciones no autorizadas y otras formas de modificación fraudulenta. Para ello se han integrado elementos ocultos (secretos) ideados de manera que su autenticación sólo pueda hacerse mediante examen forense o por expertos empleando equipos de verificación especiales. (Organización de Aviación Civil Internacional, 2006)

Los elementos, técnicas y otras medidas de seguridad se clasifican según las etapas de los procesos de producción, personalización y según los componentes de los documentos de viajes que se crearon mediante dichos procesos: 1) materiales del sustrato; 2) impresión de seguridad; 3) protección contra las reproducciones; 4) técnicas de personalización. Se recomienda a los Estados expedidores que incorporen todos los elementos o medidas de seguridad básicas, después de evaluar a fondo los riesgos a los que están expuestos sus documentos de viajes, seleccionen de la lista varios elementos y medidas de seguridad adicionales. Salvo que se indique, puede suponerse que los elementos de seguridad se aplican

a todas las partes de un documento de viaje y a todas las páginas interiores de un pasaporte, incluida la página de datos personales, las últimas hojas, así como las páginas de los visados. Hay que asegurarse que los elementos no interfieran en la lectura mecánica del PLM.

**Materiales del sustrato**

- Papel empleado en las páginas de un documento de viaje.
- Papel u otro sustrato en forma de etiqueta empleado en la página de datos personales de un documento de viaje.
- Aspectos de seguridad del papel empleado en el reverso de la cubierta de la libreta de pasaporte.
- Sustratos plásticos.

**Impresión de seguridad**

- Fondo e impresión del texto.
- Tintas.
- Numeración.
- Medidas especiales de seguridad para uso con páginas no laminadas de datos personales.
- Medidas especiales de seguridad para uso con tarjetas de plástico.

**Protección contra las reproducciones**

- Necesidad de una protección contra las reproducciones,
- Métodos de protección contra las reproducciones.

**Técnica de personalización**

- Personalización de documentos.
- Protección contra alteraciones.

- Elección de la tecnología para crear el documento.
- Protección contra la sustitución de la fotografía y la alteración de los datos de la página de datos personales de las libretas de pasaportes, las tarjetas de viajes o los visados.

**Otras medidas de seguridad para las libretas de pasaportes**

- Colocación de la página de datos personales.
- Sustitución de una página completa.
- Página de visados.
- Supresión de sellos y desprendimiento de etiquetas en los pasaportes, incluida la eliminación de datos de la página de observaciones.
- Protección contra el robo y uso indebido de documentos en blanco genuinos o de los componentes de los documentos.

En el Doc. 9303 no se especifica un método de verificación con ayuda de máquina de interfuncionamiento mundial, puesto que basarse en un elemento único para verificar la autenticidad entraña un elevado riesgo de que el método se vea comprometido. Entre los tipos de elementos de verificación de documentos con ayuda de máquina tenemos tres categorías principales de elementos de seguridad verificables por lectores adecuadamente diseñados, los cuales son:

- Elemento estructura: es un elemento de seguridad que contiene algún tipo de información verificable sobre la base la constitución física del elemento.
- Elemento sustancia: entraña la identificación de una característica definida de una sustancia utilizada en la construcción del elemento.
- Elemento datos: la imagen visible de la página de datos del PLM puede contener información oculta que puede detectarse mediante un dispositivo adecuado incorporado al lector.

Dentro de las medidas de seguridad que se tienen que tener en cuenta están los riesgos de fraude relacionados con el proceso de solicitud y expedición de pasaportes. Estos peligros son consecuencias de las ventajas que pueden obtenerse con la posesión de un pasaporte del Estado expedidor que pueda utilizarse para confirmar la identidad y ciudadanía del titular. En el Doc. 9303, Parte 1, Volumen 1 se detallan las medidas recomendadas contra el fraude, los procedimientos para combatir solicitudes fraudulentas así como el control que se debe tener en las instalaciones expedidoras.

La comparación de un DVLM equipado con una microplaqueta sin contacto y un DVLM tradicional muestra dos diferencias:

- Los datos almacenados en la plaqueta pueden leerse electrónicamente sin abrir el documento (despumado).
- La comunicación no cifrada entre una plaqueta y un lector puede escucharse furtivamente a una distancia de varios metros.

Existen medidas físicas posibles para impedir el despumado, éstas no se aplican a la escucha furtiva. Por consiguiente se opta por implantar un mecanismo de control de acceso básico, es decir, un mecanismo de control de acceso que en efecto requiere el conocimiento del titular del DVLM de que los datos almacenados en la plaqueta son leídos de forma segura. El mecanismo de control de acceso básico impide el despumado así como la escucha furtiva. Este mecanismo tiene como objeto proteger la confidencialidad y reconocer los derechos de los viajeros a dicha protección mediante la prevención del despumado y la escucha furtiva. El control de acceso es opcional, si se implanta el mecanismo asegurará que el contenido de la microplaqueta sólo puede leerse después de que el titular ha ofrecido a sabiendas su DVLM.

La seguridad de las características biométricas adicionales para el acceso a los datos personales se logra de dos maneras: cifrado de datos o control de acceso extendido. El control de acceso extendido es opcional, es similar al mecanismo de control de acceso de básico ya descrito, no obstante, para el control de acceso ampliado se utiliza un conjunto de claves de acceso extendido al documento en lugar de las

claves de acceso básico al documento (KENC y KMAC). El Control de acceso extendido exige capacidades de procesamiento en la microplaqueta del DVLM.

La restricción del acceso a las características biométricas adicionales también puede efectuarse mediante el cifrado de las mismas. Para poder descifrar los datos cifrados, el sistema de inspección deberá contar con una clave de descifrado. La definición del algoritmo de cifrado/descifrado y las claves que han de utilizarse quedan a discreción del Estado que las implante.

Además de la autenticación pasiva mediante firmas digitales, los estados pueden optar por una seguridad adicional, utilizando formas más complejas de proteger la microplaqueta y sus datos. Las opciones presentadas en la Tabla 1 pueden combinarse adecuadamente para lograr una seguridad adicional con arreglo a las normas ISO existentes.

| Método | Expedidor | Ventajas | Deficiencias |
|---|---|---|---|
| Autenticación pasiva | Obligatorio | Prueba que el contenido de la SOD y la LDS son auténticos y no se han modificado. | No impide una copia exacta o sustitución de plaqueta.<br>No impide acceso no autorizado.<br>No impide despumado. |
| MÉTODOS DE SEGURIDAD AVANZADOS | | | |
| Comparación de la zona de lectura mecánica (ZLM) convencional (OCR-B) y ZLM basada en plaqueta (LDS) | Opcional | Prueba que el contenido de la microplaqueta y el DVLM físico se corresponden. | Añade complejidad (menor).<br>No impide una copia exacta de la microplaqueta y del documento convencional. |
| Autenticación activa | Opcional | Impide la copia del SOD y prueba que ha sido leído de la plaqueta auténtica. | Añade complejidad.<br>Requiere plaquetas con |

| | | | |
|---|---|---|---|
| | | Prueba que la plaqueta no ha sido sustituida. | procesador. |
| Control de acceso de base | Opcional | Impide despumado y uso impropio.<br><br>Impide escucha furtiva de las comunicaciones entre DVLM y sistema de inspección (cuando se usa para establecer un canal de sesión cifrado.) | No impide una copia exacta o sustitución de plaquetas (también exige copiar el documento convencional).<br><br>Añade complejidad.<br><br>Requiere microplaqueta con procesador. |
| Control de acceso ampliado | Opcional | Impide acceso no autorizado a las características biométricas adicionales.<br><br>Impide despumado de características biométricas adicionales. | Exige gestión de claves adicionales.<br><br>No impide una copia exacta o sustitución de plaqueta (también exige copia del documento convencional).<br><br>Añade complejidad.<br><br>Requiere microplaqueta con procesador. |
| Cifrado de datos | Opcional | Protege características biométricas adicionales.<br><br>No exige microplaqueta con procesador. | Exige gestión de claves de descifrado complejas.<br><br>No impide una copia exacta o sustitución de la microplaqueta.<br><br>Añade complejidad. |

**Tabla 1: Método de seguridad básico**

Los DVLM expedidos por Estados que aplican métodos de seguridad avanzados se ajustarán plenamente a las normas ICAO que satisfacen las normas de interfuncionamiento mundial.

## *1.5. Tarjetas Inteligentes*

El origen de las tarjetas inteligentes se remonta a los primeros años de la década del 70 del siglo XX, pero no fue hasta los años 90 con la llegada de las tarjetas Subscriber Identity Module (SIM).

Las tarjetas inteligentes (Smartcards) son tarjetas pequeñas similares a las de crédito bancario, pero que a diferencia de estas contienen en su interior un chip, por lo que también se les conoce como tarjetas con circuito integrado (TCI). La presencia de dicho circuito posibilita la ejecución de cierta lógica programada, de ahí que se utilice el adjetivo "inteligente" en su denominación. Por su parte el plástico que contiene la tarjeta puede ser impreso para contener información adicional y visible para los humanos acerca del portador o la entidad que las emite. Los adelantos tecnológicos sucedidos a lo largo de estos años han propiciado un auge en el desarrollo y utilización de las tarjetas inteligentes, las cuales ya no sólo se utilizan en el campo de la telefonía celular o en el comercio electrónico sino también para los pasaportes electrónicos. Las tarjetas pueden ser clasificadas según la forma en que se comunican, la capacidad del chip, la estructura del sistema operativo o el tamaño de la misma.

En la actualidad algunos países han comenzado a utilizarla como documento de identificación debido a la seguridad tanto física como lógica que brindan las Tarjetas Inteligentes, almacenando en cada una de las tarjetas información personal referente a un individuo, así como, de algunos servicios que brindan dichas naciones. Otra importante aplicación en la que son usadas las Smartcards en la actualidad es la firma digital de documentos, o sea que permiten almacenar un certificado digital de forma segura dentro de la tarjeta y firmar con él documentos electrónicos sin que en ningún momento el certificado (y más concretamente su clave privada) salgan del almacenamiento seguro en el que están confinados, ya que sirve no solo para validar la identidad de los mismos sino también para centralizar la información que de ellos se desea controlar.

### *1.5.1 Seguridad en las tarjetas inteligentes.*

La seguridad es una de las propiedades más importantes de las tarjetas inteligentes y se aplica a múltiples niveles y con diferentes mecanismos. Las medidas de protección van desde los elementos empleados en el material de la tarjeta, así como las características usadas en la impresión gráfica que dificultan la reproducción y alteración de las mismas, hasta reglas que se establecen para el acceso a la información contenida en el chip, según sus niveles de confidencialidad.

### *1.5.2 Seguridad Física.*

El conjunto de medidas de seguridad que se pueden implementar para un documento de identidad se dividen en diferentes niveles:

**Nivel 1:** Perceptibles mediante la vista al observar el documento. No requieren de herramientas especiales, por lo cual no es necesario entrenamiento. Pueden ser de conocimiento público.

. **Nivel 2:** Características escondidas que son visibles mediante equipos simples de luz ultravioleta. No requieren de un entrenamiento especial de los oficiales de seguridad.

**Nivel 3:** Características de seguridad que requieren de un entrenamiento al personal y de un equipamiento especial para detectarlas, por ejemplo: un microscopio o lupas especiales.

. **Nivel 4:** Características de un alto nivel de seguridad sobre las que sólo tienen conocimiento el personal requerido y que únicamente pueden verse mediante un equipamiento en un laboratorio especializado.

### *1.5.3 Seguridad Lógica*

En las tarjetas se implementan distintos niveles de seguridad sobre los ficheros en dependencia de la importancia de la información contenida en ellos. Algunos elementos de seguridad son:

- Especificación de un conjunto de reglas para ejecutar comandos o acceder a datos, las cuales se denominan Condiciones de Acceso.
- Mensajería segura para la autenticación e integridad del intercambio de datos entre la tarjeta y los lectores.
- Protección de la información por claves que deben presentarse a la tarjeta y son verificadas por su sistema operativo.
- Contador de confirmación para evitar agresiones repetidas contra los valores secretos.
- Mecanismos de autenticación mutua de la tarjeta y los terminales para garantizar que sólo elementos autorizados puedan tener acceso a la información.

- Funciones criptográficas que permiten los procesos de firma digital para prevenir repudios.
- Utilización de la infraestructura de llave pública.
- Verificación biométrica por parte de la tarjeta.

## *1.6. Conceptos Fundamentales*

### *1.6.1 Applet*

Es una aplicación pequeña o un componente de una aplicación que se ejecuta en el ámbito de otro programa. Los applets son desarrollados con la utilización de la tecnología Java card y en dependencia del contexto de trabajo pueden ser ejecutadas en tarjetas inteligentes.

### *1.6.2 Middleware*

El middleware es un software de conectividad que funciona como una capa de abstracción, posicionada entre la de aplicación y las inferiores, dando como resultado el funcionamiento de aplicaciones de plataformas diferentes. Se suele usar para intercambiar información entre dichos sistemas, permitiendo conectarse a través de interfaces de alto nivel. Entre sus funciones se destacan:

- Funciona con componentes heterogéneos de hardware y software.
- Brinda un estándar de interfaces para los desarrolladores, dando mucha facilidad a la hora de integrar, reutilizar, adaptar e ínteroperar.
- Facilita el trabajo y la colaboración entre aplicaciones diferentes, suministrando componentes y servicios comunes a las mismas.

### *1.6.3 APDU*

Application Protocol Data Unit (APDU), es la unidad básica para la comunicación entre los lectores y las tarjetas inteligentes. Se dividen en dos tipos, APDU Command y APDU Response. La estructura de los mismos se encuentra definida en el estándar ISO 7816.

### *1.6.4 Java Card*

Es una tecnología que permite la ejecución de Applets en tarjetas inteligentes y dispositivos similares. Java card también brinda la posibilidad de programar aplicaciones que se ejecutan en la tarjeta a modo que esta tenga una funcionalidad práctica para un dominio especifico.

La primera tarjeta que usa esta tecnología fue presentada en 1997. Los productos de Java card están basados en la plataforma de Java card. Las características más importantes de la misma son el alto grado de portabilidad y de seguridad que brinda.

Java card tiene la finalidad de definir un estándar de tarjeta inteligente para funcionar en diferentes tarjetas inteligentes.

### *1.6.5 Java Card Runtime Environment*

El Java Card Runtime Environment (JCRE) incluye la Java Card Virtual Machine (JCVM) junto a todos los servicios y clases de la Application Programming Interface (API). Sobre el mismo se cargan y ejecutan los Applets. La diferencia más marcada entre un Java Virtual Machine (JVM) estándar y el JCVM es el tiempo de vida, siendo el de la última igual al tiempo de vida de la tarjeta, por lo cual los objetos pueden mantener su estado en varias secciones, siendo esto una de sus funciones más importantes.

## *1.7. Estándares*

### *1.7.1 Doc. 9303*

El Doc. 9303 es un estándar para ciertos tipos de documentos de viajes, cuenta con tres partes y ha sido aprobado por la ICAO con carácter de normas ISO 7501-1, 7501-2 y 7501-3.

El documento propone algunas normas para hacer funcionales y seguros los pasaportes de lectura mecánica (incluyendo los electrónicos) en cualquier estado. Se definen especificaciones a las que deben

ajustarse, elementos de seguridad física y lógica. Medidas para la elaboración de los documentos, la transportación y la personalización de los mismos, así como el formato que deben llevar, las dimensiones, la calidad y el posicionamiento de los elementos en el documento. Con respecto a los pasaportes electrónicos se proponen algunos métodos de seguridad lógica, en los cuales se incluye la infraestructura de clave pública, así como la estructura lógica que deben tener los datos dentro del circuito integrado para que puedan ser leídos desde cualquier sistema que se ajuste a dichas normas.

### *1.7.2 Doc. LDS*

Para permitir el interfuncionamiento mundial de los lectores de tarjetas inteligentes, se necesita una estructura lógica de datos guiada por las mismas especificaciones. El documento LDS nos brinda las normas necesarias para permitir que todos los pasaportes que se ajusten al estándar puedan ser funcionales en todos los estados que igualmente cumplan las especificaciones.

LDS defiende la estructura lógica de los datos almacenados dentro del chip del pasaporte. Proporciona detalles sobre la capacidad de la información, posicionamiento de los datos en la estructura de archivos y define medidas de seguridad para proteger la información interna del pasaporte. Existen especificaciones sobre los datos que son de orden obligatorio si se desea seguir el estándar, así como otras opcionales (Ver Anexo 1)

### *1.7.3 ISO 14443*

El estándar ISO 14443 se relaciona con las tarjetas electrónicas, este estándar define los parámetros a seguir por las tarjetas de proximidad que utilizan el sistema RFID, componentes que deben incluir la misma, frecuencia por la que debe operar la antena incluida en el sistema RFID, así como el comportamiento del lector con respecto a la tarjeta.

El estándar cuenta con cuatro partes donde son descritos dos tipos de tarjetas: A y B. Se muestran las diferencias de las mismas en cuanto a los métodos de modulación, codificación de los planes o el protocolo de inicialización de los procedimientos. Así como la descripción del protocolo T=CL usado para el intercambio de datos.

### *1.7.4 ISO 7816*

Con el objetivo de crear aplicaciones para tarjetas inteligentes que pudiesen funcionar con terminales de diversos fabricantes se crearon un conjunto de especificaciones las cuales conforman el ISO 7816. En el mismo se definen características físicas, eléctricas, lógicas, de seguridad, estructura de datos y protocolos de comunicación. Estos estándares se complementan con los ISO 7810 e ISO 7811.

El estándar ISO 7816 está compuesto por 15 partes:

- Parte 1: Características físicas.
- Parte 2: Tamaño y localización de los contactos.
- Parte 3: Señales electrónicas y protocolos de transmisión.
- Parte 4: Organización, seguridad y comandos para el intercambio de información.
- Parte 5: Sistema de numeración y procedimiento de registro para los identificadores de aplicación.
- Parte 6: Interoperabilidad en los elementos de datos para el intercambio.
- Parte 7: Interoperabilidad en los comandos de la tarjeta.
- Parte 8: Comandos para operaciones de seguridad.
- Parte 9: Comandos para la gestión de la tarjeta.
- Parte 10: Señales electrónicas para tarjetas síncronas.
- Parte 11: Verificación de la identidad personal a través de métodos biométricos.
- Parte 12 Tarjetas con contactos. Interfaz eléctrica Universal Serial Bus (USB) y procedimientos operativos.
- Parte 13: Comandos de administración de aplicaciones en múltiples aplicaciones entorno.
- Parte 15: Aplicación de información criptográfica.

### *1.7.5 PC-SC*

Personal Computer / Smart Card (PC/SC) son un conjunto de especificaciones para facilitar la comunicación entre las tarjetas inteligentes, las computadoras y los lectores de tarjetas inteligentes. Define un API de programación que permite a los desarrolladores trabajar con lectores de diversos fabricantes de una misma manera.

Hasta la fecha existen nueve partes, en las cuales se encuentran detalles sobre la interoperabilidad de los dispositivos, interfaces de programación o información de diseño:

- Parte 1. Introducción y visión general de la arquitectura.
- Parte 2. Requisitos de interoperabilidad para las tarjetas y los lectores.
- Parte 3. Requisitos de interoperabilidad para los lectores.
- Parte 4. Consideraciones de diseño de los lectores e información de referencia.
- Parte 5. Definición de la interfaz del Resource Manager.
- Parte 6. Definición de la interfaz del Service Provider.
- Parte 7. Consideraciones de diseño para el desarrollo de aplicaciones
- Parte 8. Recomendación para la implementación de servicios de seguridad y privacidad con tarjetas inteligentes
- Parte 9. Lectores con capacidades extendidas

### *1.7.1 PKCS*

Public Key Cryptography Standards (PKCS) se refiere a un grupo de especificaciones técnicas desarrollados por RSA, Netscape con ayuda de otros desarrolladores y expertos en sistemas de seguridad de todo el mundo. Los mismos tienen como fin uniformizar los protocolos y procedimientos de la criptografía pública, así como acelerar su despliegue. PKCS está incluido en diversos estándares como serian Secure Sockets Layer (SSL), Public-Key Infrastructure X.509 (PKIX), Secure Electronic Transaction (SET) o X9. Actualmente está dividido en 15 documentos, que van desde PKCS #1 a PKCS #15.

- PKCS #1: Estándar criptográfico RSA
- PKCS #2: Incluido ahora en PKCS #1
- PKCS #3: Estándar de intercambio de claves Diffie-Hellman
- PKCS #4: Incluido ahora en PKCS #1
- PKCS #5: Estándar de cifrado basado en contraseñas

- PKCS #6: Estándar de sintaxis de certificados extendidos
- PKCS #7: Estándar sobre la sintaxis del mensaje criptográfico
- PKCS #8: Estándar sobre la sintaxis de la información de clave privada
- PKCS #9: Tipos de atributos seleccionados
- PKCS #10: Estándar de solicitud de certificación
- PKCS #11: Interfaz de dispositivo criptográfico ("Cryptographic Token Interface" o cryptoki)
- PKCS #12: Estándar de sintaxis de intercambio de información personal
- PKCS #13: Estándar de criptografía de curva elíptica
- PKCS #14: Generación de número pseudo-aleatorios
- PKCS #15: Estándar de formato de información de dispositivo criptográfico

## *1.8. Tecnología usada.*

### *1.8.1 Metodología.*

Extreme Programming (XP) o programación extrema es una metodología dentro de la ingeniería de software, más específicamente pertenece al reciente grupo de las llamada metodologías ágiles siendo una de las más destacadas dentro del mismo. La misma propone nuevas técnicas de desarrollo y comunicación en el proceso de desarrollo de software.

Las técnicas y principios fundamentales que XP sigue son:

- Un desarrollo incremental e iterativo: pequeñas y continuas mejoras.
- Pruebas unitarias continuas y de integración: se realizan pruebas por cada una de las clases creadas, añadidas o modificadas, pruebas funcionales, pruebas de regresión y pruebas realizadas por parte del cliente para asegurar el cumplimiento de los requisitos.
- Programación en dúos o cuartetos: dependiendo del tamaño del proyecto y el número de desarrolladores con que se disponga se pude usar dos o cuatro personas. Las tareas serán llevadas a cabo en conjunto en un mismo puesto de trabajo. El código es escrito, revisado y discutido al mismo tiempo, dando menos posibilidad a errores.
- El cliente se integra al equipo de trabajo, siendo él mismo un integrante más, así se tiene la certeza de desarrollar lo que el cliente desea y como lo desea.

- No existen módulos asignados a trabajadores específicos, todos los trabajadores pueden colaborar en cualquier módulo, dando esto como resultado un dominio total del sistema por todo el equipo.
- El código es desarrollado de la manera más sencilla posible.

### *1.8.2 Lenguaje de modelación visual.*

Unified Modeling Language (UML) es un lenguaje gráfico estandarizado el cual se utiliza para construir, documentar, especificar y visualizar un sistema de software. UML describe un plano del sistema, en el cual se incluyen aspectos conceptuales y concretos. El mismo puede ser utilizado en cualquier metodología ya que es independiente del ciclo de desarrollo a seguir.

### *1.8.3 NetBeans como entorno de desarrollo.*

NetBeans es un robusto Integrated Development Environment (IDE) que actualmente tiene una gran aceptación, el mismo es producto gratis, libre y de código abierto. El cual está totalmente programado en el lenguaje java. Es una herramienta que brinda facilidades para programar, en especial en el lenguaje java, aunque no se limita solo al uso de este lenguaje, en el mismo es posible desarrollar aplicaciones en la mayoría de los lenguaje existentes. Permite la integración de módulos y plug-ins desarrollados para aplicaciones específicas. Existen diversos paquetes de mejoras que pueden ser incluidos, agregando herramientas de desarrollo visual en Service Oriented Architecture (SOA), orientación a servicios web, modelado UML o esquemas Extensible Markup Language (XML).

### *1.8.4 Lenguaje de programación Java.*

Java es un lenguaje orientado a objetos y de alto nivel, fue creado por Sun Microsystems. Recoge los elementos típicos en el resto de los lenguajes de programación, agregando variadas ventajas como son la sencillez a la hora de desarrollar en el mismo y la portabilidad de las aplicaciones creadas.

Java ha sido pensado para soportar aplicaciones que serán ejecutadas en diversos entornos. Esto es posible ya que el mismo genera bytecode, usándolos como lenguaje intermedio y siendo indiferente de la arquitectura, el código pasa al intérprete de Java el cual realiza las acciones para que la aplicación sea compactible con las diversas plataformas hardware y software.

### *1.8.5 Developer Suite Gemalto.*

Developer Suite Gemalto es una herramienta que nos brinda un ambiente adecuado para el desarrollo de Applets, además cuenta con un simulador de tarjetas pudiendo probar las funcionalidades de los Applets, con esto podemos tener la seguridad de que nuestro Applet sea totalmente funcional antes de ser instalado en la tarjeta inteligente.

### *1.8.6 Altova UModel.*

Altova UModel se utiliza para interpretar y crear diseños software utilizando la potencia de UML. El mismo trae soporte para la mayoría de los tipos de diagramas UML. Mediante el diseño de la aplicación o a través de sus planos puede generar código en los lenguajes Java y C#, también permite realizar ingeniería inversa, de código a diagramas, así como completar códigos y modelos generados. Es compatible con modelos de otras aplicaciones, es una herramienta eficiente y muy fácil de usar.

## 1.9. *Conclusiones.*

- En el presente capítulo se realizó un análisis de las tecnologías relacionadas con tarjetas inteligentes, la organización de la información en los pasaportes electrónicos, así como su aplicación en los mismos.

- Con el estudio de soluciones existentes se han tenido en cuenta las medidas de seguridad y debilidades con que cuentan los sistemas actuales, tomando las ventajas de los mismos llevándolas a la solución.

- Se realizó un estudio de los estándares por los cuales se rigen los sistemas de pasaportes electrónicos basados en tecnología de tarjetas inteligentes.

- Para facilitar el desarrollo del sistema se ha propuesto un grupo de tecnologías: la metodología de desarrollo XP (Extreme Programming), la herramienta UModel Altova para la modelación visual del problema utilizando UML, la plataforma de desarrollo NetBeans la cual nos brinda un robusto ambiente visual, Java y Java card como lenguajes de programación. Con la utilización de las mismas se asegura trabajar en un entorno sencillo, seguro y confiable.

# CAPITULO 2: DESCRIPCIÓN DE LA PROPUESTA DE SOLUCIÓN PARA UN APPLET Y SU COMPONENTE MIDDLEWARE

A lo largo del capítulo se muestran las fases de planificación y exploraciones definidas en la metodología de desarrollo XP, así como la representación de los diversos artefactos generados en cada una de ellas, siendo estas etapas importantes para establecer en detalles de alto nivel que se desea hacer y cómo hacerlo, así como una apreciación de cuán viable puede llegar a ser el proyecto, decidiendo con esto la continuidad del mismo.

## *2.1. Modelo de dominio.*

Teniendo en cuenta el problema científico que la plataforma pretende resolver, se ha procedido a crear un modelo de dominio. El mismo permite identificar los principales conceptos sociales y tecnológicos del entorno en que se desarrolla la plataforma, así como las relaciones entre ellos.

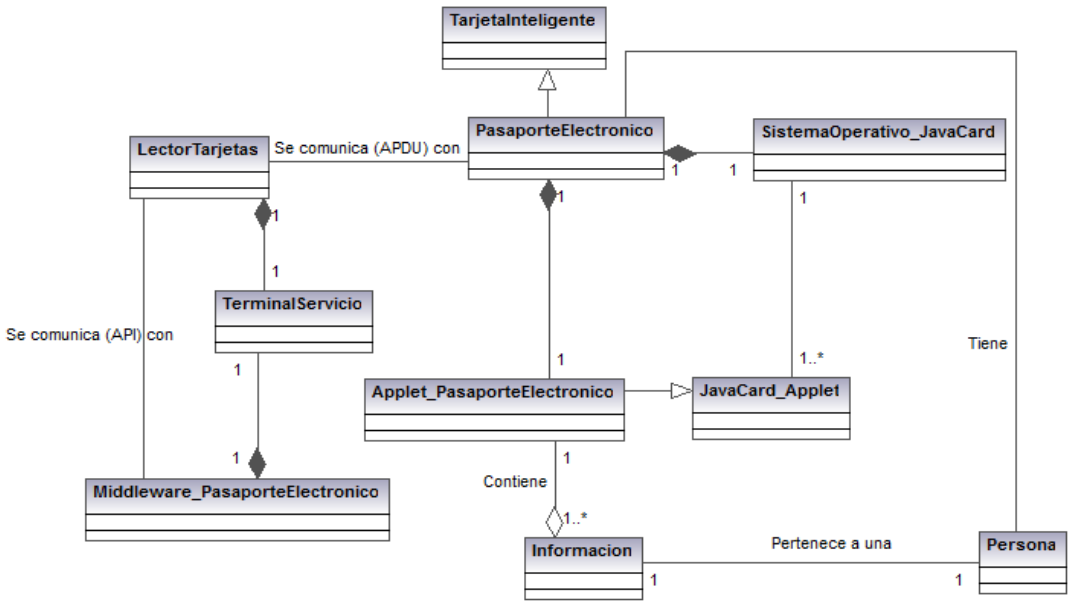


**Figura 4: Modelo de Dominio del Sistema**

## *2.2. Glosario de términos del Modelo de dominio.*

### Tarjeta Inteligente

Es un dispositivo de plástico similar en tamaño y otros estándares físicos a las tarjetas de crédito, presenta un circuito integrado, el mismo puede ser de sólo memoria o contener un microprocesador con un sistema operativo que le permita una serie de funcionalidades:

- Almacenar información.
- Encriptar información.
- Leer y escribir datos, al igual que un ordenador.

### *SistemaOperativo_JavaCard*

La tecnología Java card combina parte del lenguaje de programación Java con un entorno de ejecución optimizado para tarjetas inteligentes y similares. El objetivo de la tecnología Java card es llevar los beneficios del desarrollo de software en Java al mundo de las tarjetas inteligentes.

### *PasaporteElectrónico*

Es una tarjeta inteligente que contiene tecnología Java card, contiene datos de identificación de su portador y permite una mayor automatización de los procesos de identificación, logrando una mayor seguridad y efectividad de forma simple.

### *JavaCard_Applet*

Los Applets son las aplicaciones que corren embebidas en una Java card. Dichas aplicaciones interactúan en todo momento con el JCRE utilizando los servicios que éste brinda, e implementan la interfaz definida en la clase abstracta javacard.framework.Applet.

### *Applet_PasaporteElectronico*

Es una aplicación implementada en Java card, instalada dentro de la tarjeta inteligente la cual permite gestionar la información que se almacene dentro del pasaporte electrónico.

### *Información*

Son datos referentes al portador del documento electrónico de viaje y son almacenados en el mismo.

### *Middleware_PasaporteElectronico*

Es un componente que funciona como capa de traducción entre el Applet_PasaporteElectronico y otro sistema, permitiendo una mejor comprensión de las respuestas obtenidas por la comunicación establecida con la aplicación instalada en el documento electrónico de viaje (Applet).

### *TerminalServicio*

Es un punto en una computadora donde se instalan todas las condiciones para poder interactuar con la solución. Entre los elementos indispensables también podemos citar, los lectores PC/SC.

### *LectorTarjetas*

Es un lector compatible con el estándar PC/SC, el cual define la comunicación entre el Applet_PasaporteElectronico y el Middleware_PasaporteElectronico, sin realizarle modificaciones a ambas aplicaciones.

### *Persona*

Portador del documento electrónico de viaje.

## *2.3. Historias de usuario*

Las historias de usuarios se utilizan en la metodología XP para describir los requisitos de una forma menos detallada y desde la perspectiva del cliente. Una historia de usuario debe responder a las preguntas: ¿Quién se beneficia?, ¿Qué se quiere? y ¿Cuál es el beneficio?

**HU Gestión de la comunicación**

| **Historia de Usuario** | |
|---|---|
| **Número:** HU1 | **Usuario:** Desarrollador |
| **Nombre historia:** Gestión de la comunicación | |
| **Prioridad en negocio:** Alta | **Riesgo en desarrollo:** Baja |
| **Puntos estimados:** 2 | **Iteración asignada:** 1 |
| **Programador responsable:** Marvin Márquez Peralo, Adrián Martínez Pérez, Nelson Hernández Guerra | |
| **Descripción:** Permitirá la comunicación mediante el estándar PC/SC, obteniendo los lectores disponibles conectados a la terminal y estableciendo la conexión con el documento de viaje electrónico. Permitirá además enviar comandos APDU y obtener los APDU de respuesta del pasaporte electrónico. | |
| **Observaciones:** | |

**Tabla 2: HU1 Gestión de la comunicación.**

**HU Permitir la autenticación activa (AA) y pasiva (AP)**

| **Historia de Usuario** | |
|---|---|
| **Número:** HU2 | **Usuario:** Desarrollador |
| **Nombre historia:** Permitir la autenticación activa y pasiva | |
| **Prioridad en negocio:** Alta | **Riesgo en desarrollo:** Baja |
| **Puntos estimados:** 2 | **Iteración asignada:** 2 |

| |
|---|
| **Programador responsable:** Marvin Márquez Peralo, Adrián Martínez Pérez, Nelson Hernández Guerra |
| **Descripción:** Permitirá la autenticación activa y la autenticación pasiva con el pasaporte electrónico para la verificación del chip. |
| **Observaciones:** |

**Tabla 3: HU2 Permitir la autenticación activa y pasiva.**

## HU Permitir la autenticación mediante el control de acceso básico (BAC)

| **Historia de Usuario** | |
|---|---|
| **Número:** HU3 | **Usuario:** Desarrollador |
| **Nombre historia:** Permitir la autenticación mediante el control de acceso básico | |
| **Prioridad en negocio:** Alta | **Riesgo en desarrollo:** Alta |
| **Puntos estimados:** 2 | **Iteración asignada:** 1 |
| **Programador responsable:** Marvin Márquez Peralo, Adrián Martínez Pérez, Nelson Hernández Guerra | |
| **Descripción:** Permitirá la autenticación mediante el mecanismo de control de acceso básico con el pasaporte electrónico para el establecimiento de un canal seguro con el terminal. | |
| **Observaciones:** | |

**Tabla 4: HU3 Permitir la autenticación mediante el control de acceso básico.**

**HU Gestionar información**

| **Historia de Usuario** | |
|---|---|
| **Número:** HU4 | **Usuario:** Desarrollador |
| **Nombre historia:** Gestionar la información en el pasaporte electrónico. | |
| **Prioridad en negocio:** Alta | **Riesgo en desarrollo:** Media |
| **Puntos estimados:** 2 | **Iteración asignada:** 1 |
| **Programador responsable:** Marvin Márquez Peralo, Adrián Martínez Pérez, Nelson Hernández Guerra | |
| **Descripción:** Permitirá verificar las condiciones de acceso en el pasaporte electrónico para posteriormente escribir, leer y mostrar la información contenida en el mismo. | |
| **Observaciones:** | |

**Tabla 5: HU4 Gestionar la información en el documento de viaje electrónico.**

**HU Gestionar el sistema de ficheros**

| **Historia de Usuario** | |
|---|---|
| **Número:** HU5 | **Usuario:** Desarrollador |
| **Nombre historia:** Gestionar el sistema de ficheros. | |
| **Prioridad en negocio:** Alta | **Riesgo en desarrollo:** Media |
| **Puntos estimados:** 2 | **Iteración asignada:** 1 |
| **Programador responsable:** Marvin Márquez Peralo, Adrián Martínez Pérez, Nelson Hernández Guerra | |

| |
|---|
| **Descripción:** Permitirá crear el sistema de ficheros así como escribir y gestionar la seguridad de cada uno de los grupos de datos que lo componen. |
| **Observaciones:** |

**Tabla 6: HU5 Gestionar el sistema de ficheros.**

## *2.4. Requerimientos no funcionales.*

**Usabilidad**

- Se utiliza el middleware para lograr una mayor comodidad en su integración con la aplicación existente.
- El entrenamiento de usuarios normales y avanzados tendrá una duración de 3 días.

**Fiabilidad**

- La solución estará disponible las 24horas del día durante todo el año.

**Seguridad**

- El Applet debe ser capaz de realizar sus operaciones de manera eficiente, garantizando que las funcionalidades se realicen correctamente
- El Applet debe recuperarse en caso de producirse una falla.
- La información contenida en la tarjeta, será objeto de cuidadosa protección contra la corrupción y estados inconsistentes.

**Soporte**

- Se redactará un manual de usuarios, un sistema de ayuda y un manual de procedimientos, para garantizar la independencia de los usuarios finales y documentar el uso del producto desarrollado.

**Restricciones de diseño**

- El middleware debe ser independiente del sistema operativo y ser completamente funcional en los principales sistemas operativos existentes en el mercado: Microsoft Windows, Mac OS y Linux.

- El middleware debe ser compatible con cualquier lector de tarjetas que cumpla con el estándar PC/SC.
- Para el correcto funcionamiento de la aplicación se requiere el uso de Java Development Kit (JDK) versión 6.0 o superior.
- El sistema debe ser diseñado para interactuar con dispositivos compatibles con el estándar LDS.

**Interfaces Software**

- Se utilizarán interfaces de otras aplicaciones, como las interfaces definidas en Java card Development Kit (JCDK), para facilitar el desarrollo de Applets.

**Interfaces de Comunicación**

- Comunicación con lectores de tarjetas inteligentes mediante el estándar PC/SC ganando interoperabilidad de la solución.

### *2.5. Metáfora.*

La metáfora es algo que sin la necesidad de grandes o específicas explicaciones cualquier persona puede comprender. XP sugiere usarla para dar una sencilla y clara explicación de la finalidad del proyecto así como guiar la arquitectura y estructura del mismo. Es de vital importancia que el cliente y los desarrolladores estén de acuerdo y conozcan la metáfora a usar para así poder trabajar y discutir en los mismos términos de una forma más precisa y de dominio de todos.

El sistema para pasaportes electrónicos funcionará en todos los centros donde se cuente con lectores de tarjetas inteligentes con comunicación por radiofrecuencias mientras los mismos hayan sido diseñados siguiendo los estándares que ICAO redactó para la normalización de esta tecnología. El sistema está compuesto por un applet, el cual se usará para personalizar el chip (personalización eléctrica) por radiofrecuencia insertado en el pasaporte, así como un middleware que funciona como protocolo para la comunicación entre las aplicaciones. El applet tiene la funcionalidad de modificar, adicionar o eliminar datos sobre el titular del pasaporte.

## *2.6. Arquitectura*

La siguiente propuesta de la plataforma para la gestión de información en los pasaportes electrónicos basa su implementación en una arquitectura simple cliente/servidor conocida como arquitectura de 2 capas. Teniendo en cuenta las características de la plataforma, cuyo principal papel es mediar entre la aplicación a desarrollar y el lector de pasaporte, se identifica una capa estación (cliente) que contiene la aplicación la cual implica al middleware. En segundo lugar se tiene la capa Lector (servidor), donde se encuentra el applet el cual contiene toda la información del titular del pasaporte electrónico.

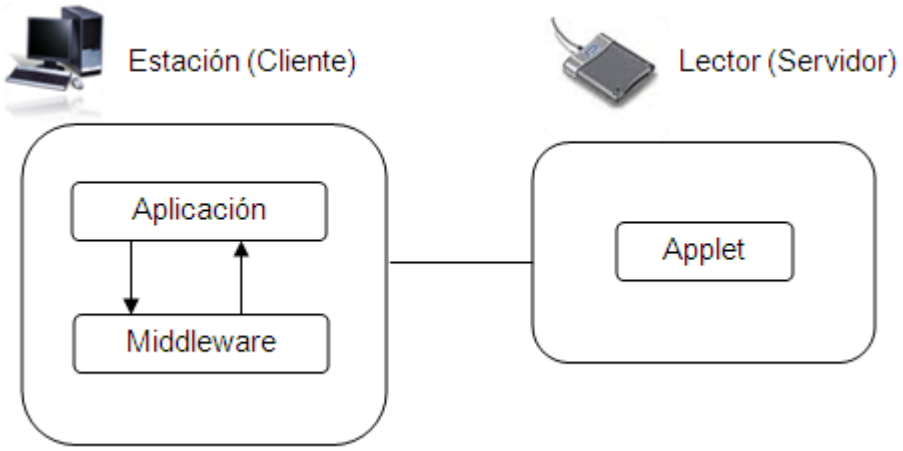


**Figura 5: Distribución de los componentes.**

Las arquitecturas en capas son muy utilizadas para el desarrollo de aplicaciones en la actualidad por las grandes ventajas que proporcionan. El principal objetivo que persigue es reducir dependencias entre artefactos, situándolos en capas lógicas, donde cada capa depende del servicio prestado por la inferior y presta un servicio a la superior, proporcionando a los desarrolladores ventajas en cuanto al mantenimiento y reutilización de estos componentes.

A continuación se muestra un diagrama de la arquitectura base en tres capas del sistema:

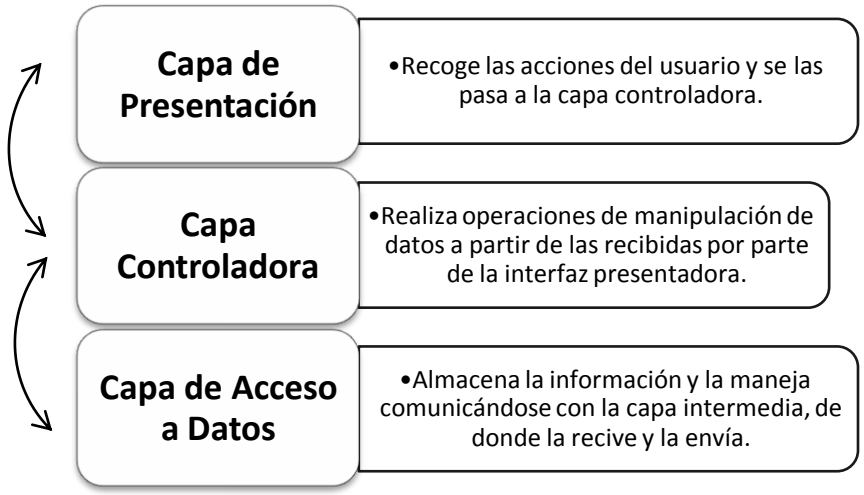


**Figura 6: Diagrama de arquitectura.**

**Capa de presentación**

Esta es la capa que interactúa con el usuario, es la encargada de modelar como se recogerán y mostrarán los datos del proceso asistencial, así como de la apariencia que tendrá la interfaz visual. Esta se comunica con la capa controladora o *middleware* a la cual envía todas las solicitudes, y las muestra cuando estas hayan sido procesadas. En el sistema que será desarrollado posteriormente esta capa se llamará MiddlewareNA.

**Capa controladora**

La capa controladora representa las clases del sistema, es la encargada de darle solución a las historias de usuario, en esta es donde se implementan las restricciones que deberá cumplir la aplicación. Se comunica con la capa de presentación para recibir las solicitudes del usuario, las envía a la capa de acceso a datos y envía las respuestas a la capa de presentación después del procesamiento de la solicitud. En el sistema que será desarrollado posteriormente esta capa se llamará: Middleware.

**Capa de acceso a datos**

Esta capa contendrá una aplicación donde estará almacenada la información referente al paciente, y esta será la encargada del manejo de dicha información. La misma se comunicará con la capa intermediaria, de donde recibe la solicitud de guardar información o de mostrarla. En el sistema que será desarrollado posteriormente esta capa se llamará *applet* ThisPassport.

## *2.7. Plan de entregas.*

Después que las historias de usuarios son elaboradas por los clientes, se desarrollará el plan de entregas. En el mismo se establecen las historias de usuarios agrupadas en entregas y con cierto orden de prioridad. El plan de entregas será resultado de una reunión en la cual participan los desarrolladores y clientes, los clientes seleccionarán según sus necesidades las historias de usuarios más importantes y los desarrolladores proponen el tiempo que pueden tardarse para el desarrollo de cada una. Con esto queda listo el cronograma de entregas en el cual también se deciden las fechas para liberar las versiones funcionales del producto. (Ver Anexo 2)

## *2.8. Estimación de tiempo.*

Los programadores se encargan de estimar el tiempo que cada historia de usuario puede tomarles para el desarrollo de la misma. El valor del tiempo se expresa en semanas y en un principio no es totalmente exacto, pero con el transcurso de las iteraciones y el desarrollo del producto se irá acercando a la realidad. (Ver Anexo 3)

| **Historia de Usuario** | **Estimación** |
|---|---|
| Gestión de la comunicación | 1 |
| Permitir la autenticación mediante el control de acceso básico | 2 |
| Gestionar la información en el documento de viaje electrónico | 1 |
| Gestionar el sistema de ficheros | 2 |
| Permitir la autenticación activa y pasiva | 2 |
| **Total** | **8** |

**Tabla 7: Estimación de tiempo de las historias de usuario.**

### *2.9. Plan de iteraciones.*

Las historias de usuarios son desarrolladas y probadas en un ciclo de iteración en correspondencia con el orden establecido anteriormente. Se realiza un plan de duración de las iteraciones en el cual se muestra el orden y la duración de la implementación de cada historia de usuario. Se han definido cinco historias de usuario para dos iteraciones con una duración total de ocho semanas.

| **Iteración** | **No. HU** | **Historia de Usuario** | **Duración Estimada** |
|---|---|---|---|
| Iteración 1 | HU1 | Gestión de la comunicación | 6 semanas |
| | HU3 | Permitir la autenticación mediante el control de acceso básico | |
| | HU5 | Gestionar la información en el documento de viaje electrónico | |
| | HU6 | Gestionar el sistema de ficheros | |
| Iteración 2 | HU2 | Permitir la autenticación activa y pasiva | 2 semanas |

**Tabla 8: Plan de iteraciones.**

### *2.10. Estudio de Factibilidad*

Una de las tareas de mayor importancia en la planificación de proyectos de software es la estimación, la cual consiste en determinar, con cierto grado de certeza, los recursos de hardware y software, costo, tiempo y esfuerzo necesarios para el desarrollo de los mismos. Para lo cual se utilizó Constructive Cost Model (COCOMO II) como modelo de estimación de costos. Este modelo permite realizar estimaciones en función del tamaño del software, y de un conjunto de factores de costo y de escala. Los factores de costo describen aspectos relacionados con la naturaleza del producto, hardware utilizado, personal involucrado, y características propias del proyecto.

#### *2.10.1 Estimación de esfuerzo*

COCOMO II está compuesto por tres modelos denominados: Composición de aplicación, Diseño temprano y Post-arquitectura. Éstos surgen como respuesta a la diversidad del mercado actual y debido a

las necesidades y características de la plataforma se ha utilizado una combinación de los dos últimos. (COCOMO II Jongmoon Baik, 2000)

El modelo Diseño Temprano se usa en las etapas tempranas de un proyecto de software, cuando se conoce muy poco del tamaño del producto a ser desarrollado, de la naturaleza de la plataforma, del personal a ser incorporado al proyecto o detalles específicos del proceso a utilizar. Este modelo podría emplearse tanto en productos desarrollados en sectores Generadores de Aplicación, Sistemas Integrados o Infraestructura.

El modelo Post-Arquitectura se aplica en la etapa de desarrollo propiamente dicho, después que se define la arquitectura del sistema, y en la etapa de mantenimiento. Este modelo utiliza:

- Puntos Función y/o Líneas de Código Fuente para estimar tamaño, con modificadores que contemplan el rehúso, con y sin traducción automática, y el "desperdicio" (breakage). (COCOMO II Jongmoon Baik, 2000)
- Un conjunto de 17 atributos, denominados factores de costo, que permiten considerar características del proyecto referentes al personal, plataforma de desarrollo, etc., que tienen injerencia en los costos. (COCOMO II Jongmoon Baik, 2000)
- Cinco factores que determinan un exponente, que incorpora al modelo el concepto de deseconomía y economía de escala 10. Estos factores reemplazan los modos Orgánico, Semi acoplado y Empotrado del modelo COCOMO II. (COCOMO II Jongmoon Baik, 2000)

El esfuerzo necesario para concretar un proyecto de desarrollo de software, cualquiera sea el modelo empleado, se expresa en meses/persona (PM) y representa los meses de trabajo de una persona a tiempo completo, requeridos para desarrollar el proyecto. El modelo de Diseño Temprano ajusta el esfuerzo nominal usando siete factores de costo. La fórmula para el cálculo de la estimación del esfuerzo es la siguiente:

$PM_{estimado} = PM_{nominal} \times \prod_{i=1}^{7} EMi$

Donde:

$PM_{nominal} = A \times (KSLOC)^{B}$

Donde:

***PM estimado:*** es el esfuerzo nominal ajustado por 7 factores, que reflejan otros aspectos propios del proyecto que afectan al esfuerzo necesario para la ejecución del mismo, expresado en meses/personas.

***KSLOC:*** es el tamaño del software a desarrollar expresado en miles de líneas de código fuente.

***A:*** es una constante que captura los efectos lineales sobre el esfuerzo de acuerdo a la variación del tamaño, (A= 2.45).

***B:*** es el factor exponencial de escala, toma en cuenta las características relacionadas con las economías y deseconomías de escala producidas cuando un proyecto de software incrementa su tamaño.

***EMi***: corresponde a los factores de costo que tienen un efecto multiplicativo sobre el esfuerzo, llamados Multiplicadores de esfuerzo.

Los modelos de estimación de costos del software a menudo tienen un factor exponencial para considerar los gastos y ahorros relativos de escala encontrados en proyectos de software de distinto tamaño. B se usa para capturar estos efectos y es calculado con la ecuación:

$$B = 0.91 + 0.01 \times \sum_{j=1}^{5} SF_j$$

**Si B < 1.0** El proyecto presenta ahorros de escala.

**Si B = 1.0** Los ahorros y gastos de escala están equilibrados.

**Si B > 1.0** El proyecto presenta gastos de escala.

Un factor de escala de un proyecto, SFj, se calcula sumando todos los factores y se usa para determinar el exponente de escala, B.

Sustituyendo valores en la fórmula anterior nos queda que B = 1.0778.

### *2.10.2 Métricas*

El modelo COCOMO II usa puntos función y/o líneas de código fuente como base para medir tamaño en el modelo de estimación de diseño temprano. Los Puntos función procuran cuantificar la funcionalidad de un sistema de software. La meta es obtener un número que caracterice completamente al sistema. Son útiles estimadores ya que están basados en información que está disponible en las etapas tempranas del ciclo de vida del desarrollo de software. (COCOMO II Jongmoon Baik, 2000)

### *2.10.3 Puntos función*

Los Puntos Función procuran cuantificar la funcionalidad de un sistema de software. La meta es obtener un número que caracterice completamente al sistema. Son útiles estimadores ya que están basados en información que está disponible en las etapas tempranas del ciclo de vida del desarrollo de software. COCOMO II considera solamente puntos de función no ajustados). La fórmula de Albretch (Albretch, 1979) para calcular los puntos función, es la siguiente:

FP = UFP X TCF

Donde:

**FP**: Puntos función

**UFP**: Puntos función no ajustados

**TCF**: Factor de complejidad técnica

Para calcular los UFP, se deben identificar los siguientes tipos de ítems:

- Entradas Externas: Entrada de datos del usuario o de control que ingresan desde el exterior del sistema para agregar y/o cambiar datos a un archivo lógico interno.
- Salidas Externas: Salida de datos de usuario o de control que deja el límite del sistema de software.
- Archivo Lógicos Internos (Archivos): Incluye cada archivo lógico, es decir cada grupo lógico de datos que es generado, usado, o mantenido por el sistema de software.
- Archivos Externos de Interface (Interfaces): Archivos transferidos o compartidos entre sistemas de software.
- Solicitudes Externas: Combinación única de entrada-salida, donde una entrada causa y genera una salida inmediata, como un tipo de solicitud externa.

Una vez identificados los ítems se clasifican de acuerdo con el grado de complejidad en: bajo, promedio o alto. Se asigna un peso a cada ítem según el tipo y el grado de complejidad correspondiente. Finalmente los UFP son calculados mediante la sumatoria de los pesos de todos los ítems identificados.

$$\mathrm{UFP} = \sum_{i=1}^{15} (\mathrm{Cantidad_Items_Tipo}_i)\ \mathrm{X}\ (\mathrm{Peso})$$

Para el cálculo del Factor de complejidad técnica, TCF, se considera la siguiente fórmula:

$$\mathrm{TCF} = 0.65 + 0.01\ \mathrm{X} \sum_{\mathrm{i}=1}^{14} \mathrm{F_i}$$

Donde los *F i* corresponden a los pesos asignados a los siguientes factores:

F1: Mecanismos de recuperación y back-up confiables

F2: Comunicación de Datos

F3: Funciones de Procesamiento Distribuido

F4: Performance

F5: Configuración usada rigurosamente

F6: Entrada de datos on-line

F7: Factibilidad Operativa

F8: Actualización de archivos on-line

F9: Interfaces Complejas

F10: Procesamiento Interno Complejo

F11: Reusabilidad

F12: Fácil Instalación

F13: Soporte de múltiples instalaciones

F14: Facilidad de cambios y amigabilidad

Los pesos se consideran dentro de una escala de 0 a 5, descripta a continuación:

0: Sin influencia

1: Incidental

2: Moderado

3: Medio

4: Significativo

5: Esencial

Estas 14 características consideran aspectos como reusabilidad, complejidad, confiabilidad, etc., contemplados por COCOMO II a través de los factores de costo. Es por ello que este modelo utiliza los UFP como métrica de determinación de tamaño. Despejando de la fórmula original se tiene un total de 50 puntos de función sin ajustar, equivalentes a los puntos función.

### *2.10.4 Líneas de código*

El tamaño de una aplicación se mide en unidades de líneas de código fuente, este valor en COCOMO II puede estimarse a partir de puntos de función sin ajustar convirtiendo a SLOC y luego dividiendo por 1000.

Si se opta por utilizar los Puntos función sin ajustar para determinar el tamaño del proyecto, éstos deben convertirse en líneas de código fuente en el lenguaje de implementación (ensamblador, lenguajes de alto nivel, lenguajes de cuarta generación, etc.) para evaluar la relativamente concisa implementación por puntos de función. (COCOMO II Jongmoon Baik, 2000)

| **Características** | **Valor** |
|---|---|
| Puntos de función desajustados | 50 |
| Lenguaje Java | 29 |
| Líneas de código fuente | 1450 |
| Miles de líneas de código fuente | 1,450 (KSLOC) |

**Tabla 9: Cálculo de las líneas de código.**

Una vez calculados los elementos necesarios, se procede al cálculo del Esfuerzo nominal del proyecto con la fórmula anteriormente planteada, quedando que:

$$\mathrm{PM}_{\mathrm{nominal}} = 2.45 \text{ x } 1.450^{1.0778}$$

$$\mathrm{PM}_{\mathrm{nominal}} = 4.74 \text{ meses/persona}$$

Derivándose del resultado anterior se encuentra el esfuerzo estimado del proyecto quedando:

$\mathrm{PM}_{\mathrm{estimando}} = 4.74 \text{ x } 0.76$

$\mathrm{PM}_{\mathrm{estimando}} = 3.60 \text{ meses/persona}$

### *2.10.5 Estimación de tiempo de desarrollo*

La ecuación inicial para los tres modelos de COCOMO II es:

TDEV = [3.0 x $\mathrm{PM}_{*}^{(0.33+0.2 \text{ x } (\mathrm{B}-1.01))}$] x $\frac{\mathrm{SCED\%}}{100}$

Donde:

***TDEV:*** es el tiempo en meses que transcurre desde la determinación de los requerimientos a la culminación de una actividad que certifique que el producto cumple con las especificaciones.

$\boldsymbol{PM_{*}}$***:*** es el esfuerzo expresado en meses/personas, calculado sin tener en cuenta el multiplicador de esfuerzo ***SCED.***

***B:*** es el Factor de escala.

***SCED%:*** es el porcentaje de compresión/expansión del cronograma.

Aplicando la fórmula anterior queda que:

TDEV = [3.0 x $3.60^{(0.33+0.2 \text{ x } (\mathrm{B}-1.01))}$] x 1

TDEV= 3.41meses

El tiempo y esfuerzo de desarrollo se consideran mucho más próximos a la realidad al utilizar el modelo COCOMO II, se destaca el hecho de que para proyectos pequeños resulta efectivo el lograr un prototipo rápido como técnica de cumplimiento a los requisitos, que si bien al inicio demanda de un esfuerzo y tiempo adicional, esto se ve claramente compensado al momento de desarrollar el producto final.

### *2.10.6 Costos y beneficios.*

El desarrollo de un producto trae aparejado un costo de producción, el cual debe ser justificado de acuerdo con los beneficios que el mismo reporta. La solución propuesta no incurre en grandes gastos, ya que no ha sido necesario invertir en equipamiento técnico pues es proporcionado por la Universidad de las Ciencias Informáticas, por lo que se concluye que su desarrollo es factible.

El desarrollo de la aplicación fue hecha en el lenguaje Java, el cual tiene como ventaja independencia de plataforma, ámbito dinámico, etc., Esto evitará que el usuario tenga que instalar aplicaciones en la

Personal Computer (PC) cliente, lo que hace más cómodo el uso de la plataforma. La aplicación no se ha concebido con fines comerciales inmediatos, pero es un software independiente que pueda comercializarse en un futuro reportando beneficios monetarios al Centro de Identidad y Seguridad Digital y en general a la Universidad de Ciencias Informáticas.

## *2.11. Conclusiones*

- Se analizaron los principales conceptos y sus relaciones quedando reflejados en el Modelo de dominio, que brindó una visión más clara de los componentes de la solución.
- Los principales artefactos logrados fueron las Historias de usuario, obteniendo una visión clara y objetiva de los requerimientos del cliente. También se generó el Plan de iteraciones, y el Plan de entrega, determinado ocho semanas como tiempo máximo para la realización de la solución, divididas en dos iteraciones.
- Se definió la arquitectura que seguirá la solución.
- Mediante la utilización del Modelo Constructivo de Costes (COCOMO II) se realizó un estudio sobre la factibilidad del proyecto.

# CAPÍTULO 3: IMPLEMENTACIÓN Y PRUEBAS DEL APPLET PARA PASAPORTE ELECTRÓNICO Y SU COMPONENTE MIDDLEWARE

En el siguiente capítulo se muestra mediante representaciones gráficas la implementación de la solución, enfocándose en el diagrama de componentes, el diagrama de clases y el diagrama de secuencia. Se visualiza el proceso seguido en las fases “Iteraciones a primera liberación” y “Producción” definidas por la metodología de desarrollo XP. Se ofrece un panorama del funcionamiento del sistema así como los componentes primarios y sus relaciones.

## *3.1 Iteraciones a primera liberación*

Se comienza a realizar el Plan de iteraciones, desarrollando en cada iteración las subfases correspondientes al Diseño, la realización de las pruebas unitarias, la codificación de la solución y la recodificación. Al terminar esta fase el cliente podrá comenzar con las pruebas de aceptación y en caso de existir fallos deberá mostrar un orden de prioridad para su corrección o resolución.

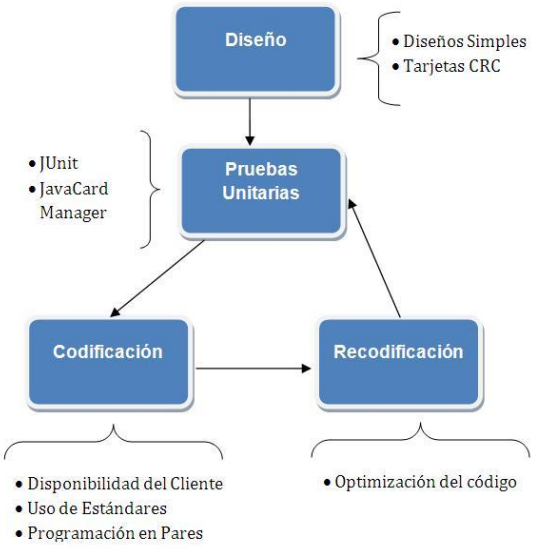


**Figura 7: Sub-fases de la fase Iteraciones a primera liberación.**

### *3.2 Tareas de ingeniería*

Al inicio de la primera iteración se debe tener claro qué es lo que se debe codificar. Las historias de usuarios describen a un alto nivel lo que se necesita implementar, pero no brindan los detalles suficientes para poder hacer una codificación correcta de lo que se necesita. Por lo que se dividen todas las historias de usuarios en tareas de programación, las mismas especifican con detalle lo que deben realizar los programadores para cada una de las historias de usuarios.

En el Plan de Iteraciones se han definidos dos iteraciones en las que están agrupadas todas las historias de usuarios. En la siguiente tabla se muestran las tareas en las que han sido desglosadas las historias de usuarios y la iteración a la que pertenecen. (Ver Anexo)

| **Iteración** | **Historia de Usuario** | **Tarea** |
|---|---|---|
| **1** | Gestión de la comunicación | - Detectar lector conectado.<br>- Establecer conexión con el pasaporte electrónico.<br>- Cerrar conexión con el pasaporte electrónico. |
| | Permitir la autenticación mediante el control de acceso básico | - Obtener los datos del código de barra de la zona de lectura mecánica.<br>- Decodificar la clave del código de barra y compararla con la clave almacenada en el chip.<br>- Permitir o negar la comunicación en dependencia del resultado de la verificación de la clave.<br>- Cifrar la comunicación entre el lector y el chip. |
| | Gestionar la información en el documento de viaje electrónico | - Leer los datos almacenados en el documento electrónico de viaje.<br>- Modificar los datos almacenados en el documento electrónico de viaje.<br>- Eliminar los datos almacenados en el documento electrónico de viaje. |
| | Gestionar el sistema de ficheros | - Crear un EF.SOD para la autenticidad e integridad |

| | | |
|---|---|---|
| | | de los datos del pasaporte electrónico.<br><br>- Definir los grupos de datos obligatorios y opcionales. |
| **2** | Permitir la autenticación activa y pasiva | - Generar clave personalizada del chip.<br><br>- Cifrar clave.<br><br>- Generar fichero con los códigos hash de todos los archivos almacenados.<br><br>- Generar firma digital usando los códigos hash almacenados en el fichero y la firma digital del país expedidor. |

**Tabla 10: Distribución de las tareas de ingeniería por iteraciones.**

## *3.3 Diseño de la solución*

Después de tener divididas las historias de usuarios en tareas estas deben ser transformadas a código, para esto se llevan a cabo encuentros donde se presentan las tarjetas Class Responsibility Collaboration (CRC), las mismas dan una idea de la cantidad de clases a implementar, las responsabilidades de las mismas, todo esto siempre a un alto nivel. Las tarjetas CRC deben ser simples, describiendo la responsabilidad de una clase en pocas frases así como las clases con las que interactúa.

La metodología XP propone algunos principios para agilizar el proceso de desarrollo, simplicidad en el diseño, ya que es mucho más rápido de realizar y mucho menos complejo de entender. El uso de tarjetas CRC logra la contribución de todo el equipo al diseñar la solución. Se recomienda mantener las funcionalidades extras alejadas del trabajo primario, ya que las mismas no son tan necesarias y hacen perder mucho tiempo.

## *3.4 Descripción del diseño*

En el Diagrama de Componentes que a continuación se muestra, se relacionan los componentes y paquetes de la arquitectura del middleware. En la solución se implementó el “MiddlewareEPass.jar” el cual contiene todas las funcionalidades que presenta el middleware, este a su vez utiliza un paquete “cu.uci.proiden.smartcards”, que contiene un componente “TerminalCardServicie.java” encargado de implementar un servicio en la tarjeta del pasaporte para el envío de APDU a un terminal con el Java

Community Process (JCP) y el uso de un kit de desarrollo de software que permitirá la comunicación con cualquier lector para un pasaporte electrónico.

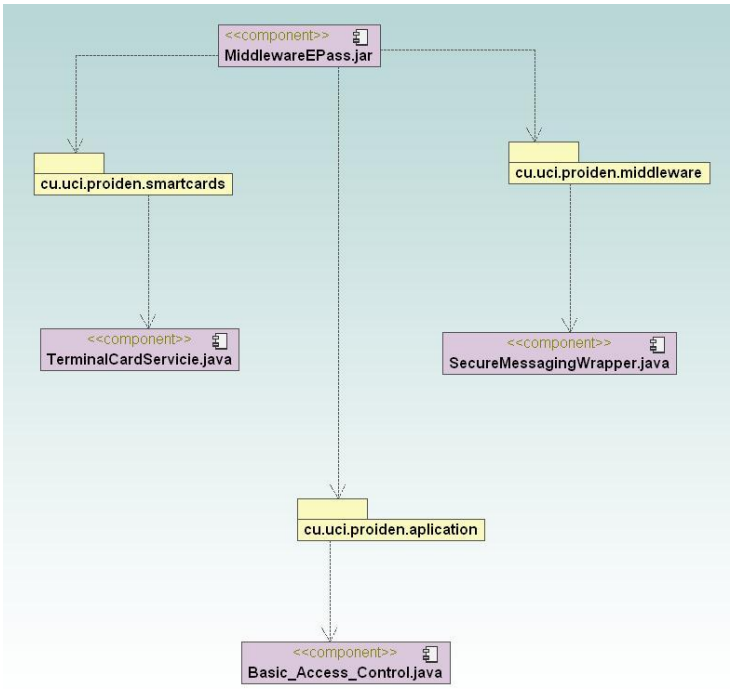


**Figura 8: Diagrama de componentes.**

El Paquete “cu.uci.proiden.middleware” incluye un componente “SecureMessagingWrapper.java” que posibilitará la protección del contenedor para la mensajería segura para el APDU, desde el tamaño del envío APDU y APDU respuesta, hasta el ksEnc de la clave de sesión para el cifrado y el ksMac de la clave de sesión para Mac.

El “MiddlewareEPass.jar” contiene otro paquete “el cu.uci.proiden.aplication” en el cual el componente “Basic_Access_Control” es el encargado de activar el servicio de lectura con el pasaporte, para la posterior comunicación con el applet de dicho pasaporte electrónico, permitiendo acceder a los datos que están almacenados en el applet y es el responsable del cierre automático del servicio en caso de quitar el pasaporte del lector o alejarlo fuera del área establecida por el lector.

### *3.5 Descripción del flujo de proceso: Solicitud de un servicio*

El proceso más importante que ejecuta la aplicación es atender la solicitud de un servicio hecha por un usuario.

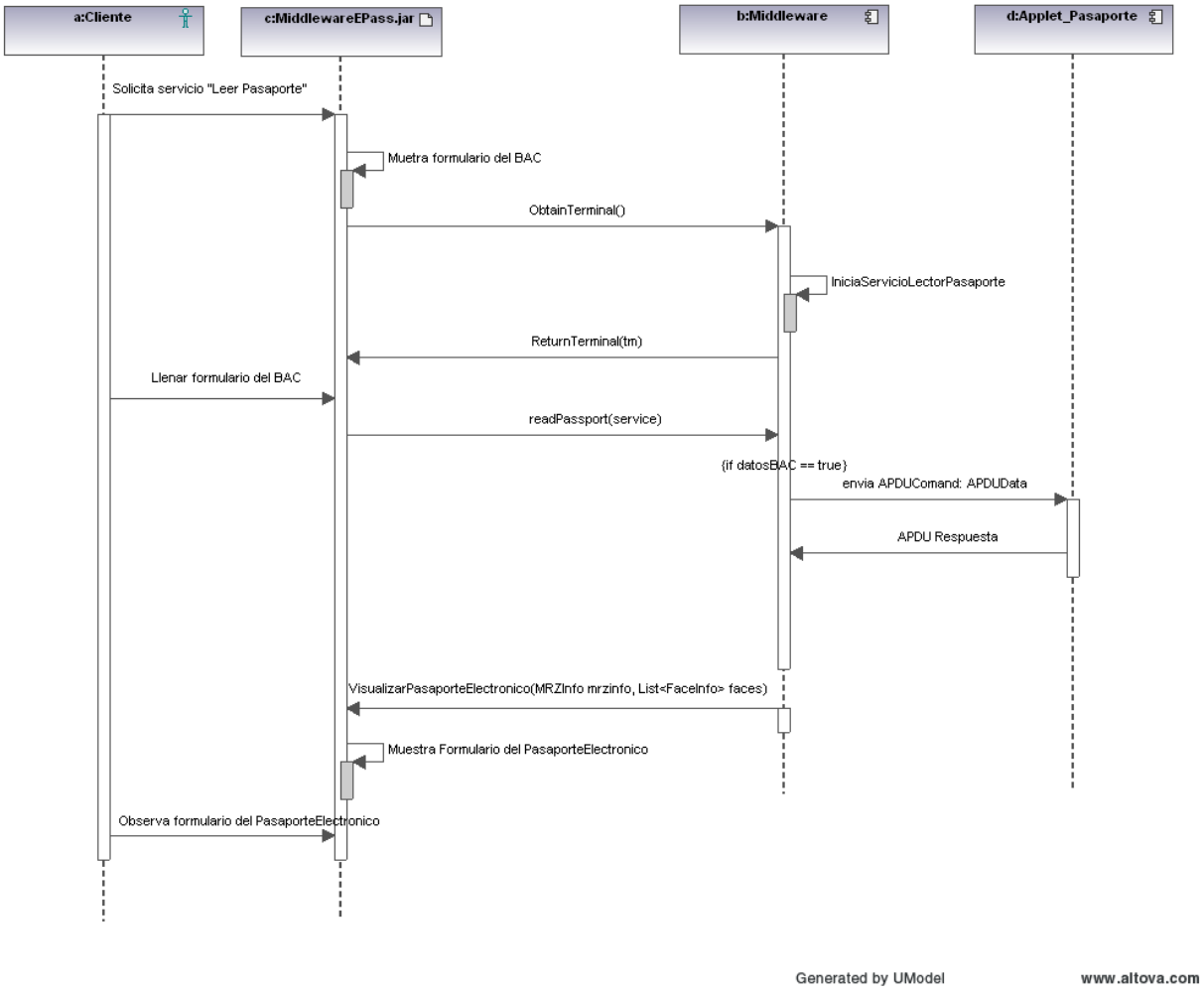


**Figura 9: Diagrama de Secuencia "Leer pasaporte electrónico".**

### *3.6 Fase de producción*

La fase de producción requiere de pruebas adicionales y revisiones de rendimiento antes de que el sistema sea trasladado al entorno del cliente. Al mismo tiempo, se deben tomar decisiones sobre la inclusión de nuevas características a la versión actual, debido a cambios durante esta fase. Las ideas que han sido propuestas y las sugerencias son documentadas para su posterior implementación, por lo que, el perfeccionamiento de código sólo fue posible a través de un grupo de pruebas unitarias automatizadas que aseguraron la ejecución correcta del sistema en todo el período de desarrollo. Se realizó una gran cantidad de pruebas para verificar que nuestro código esté correcto. Estas pruebas normalmente tienen que ser realizadas varias veces y se ven afectadas por los cambios que introducimos conforme vamos desarrollando. Las pruebas del sistema se dividieron en dos grupos: pruebas unitarias, encargadas de verificar el código y diseñadas por los programadores, y pruebas de aceptación o pruebas funcionales destinadas a evaluar si al final de una iteración se consiguió la funcionalidad requerida diseñadas por el cliente final.

### *3.7 Pruebas unitarias*

Los programadores continuamente escriben pruebas unitarias antes de empezar a codificar lo cual hará más sencillas y efectivas las pruebas finales, se corren reiteradamente a lo largo de todo el proyecto, asegurando siempre el funcionamiento correcto; así se evitan las ambigüedades y los requerimientos quedan afinados en la prueba. Mientras que el cliente especifica las pruebas funcionales.
Para realizar una prueba unitaria óptima prueba unitaria se debe cumplir con varios requisitos como:

- Automatizables
- Completas
- Repetibles o reutilizables
- Independientes
- Profesionales

El objetivo de estas pruebas es aislar cada parte del programa y mostrar que las partes individuales son correctas, las cuales van a proporcionar una mejora en la documentación del código, una clara separación de la interfaz y la implementación, los errores están más acotados y son más fáciles de localizar. Para la

realización de estas pruebas se utilizaron las siguientes herramientas: JUnit versión 4.5 integrada al netbeans IDE versión 6.9 y JCardManager del developer Suite versión 3.2.

La ausencia de las pruebas unitarias implica tener que invertir una gran cantidad de horas en sesiones de corrección de código al momento de integrar el código con el sistema existente.

### *3.8 Pruebas de aceptación*

El cliente define las pruebas de aceptación para cada historia de usuario al principio de cada iteración, por tal motivo son más importantes que las pruebas unitarias dado que significan el grado de satisfacción del cliente con el producto desarrollado, por esto, el cliente es la persona adecuada para diseñar las pruebas de aceptación. Las pruebas de aceptación son pruebas de caja negra definidas por el cliente para cada historia de usuario, y tienen como objetivo asegurar que las funcionalidades del sistema cumplen con lo que se espera de ellas. En efecto, las pruebas de aceptación corresponden a una especie de documento de requerimientos en XP, ya que marcan el camino a seguir en cada iteración, indicándole al equipo de desarrollo hacia donde tiene que ir y en qué puntos o funcionalidades debe poner el mayor esfuerzo y atención. Permiten al cliente saber cuando el sistema funciona, y que los programadores conozcan que es lo que resta por hacer.

| **Caso de prueba de aceptación** | |
|---|---|
| **Código de caso de prueba:** HU1_CP1 | **Nombre de la historia de usuario:** Gestión de la comunicación |
| **Responsable de la prueba:** Adrian Martínez Pérez | |
| **Descripción de la prueba:** Prueba de funcionalidad para listar los lectores conectados, enviar comandos APDU y obtener los APDU de respuesta. | |
| **Condiciones de ejecución:** Debe existir algún lector conectado. | |
| **Entrada/Pasos de ejecución:**<br>• El usuario se registra en la aplicación.<br>• Se reconoce automáticamente el lector para leer el pasaporte electrónico.<br>• Envió de comandos APDU al pasaporte electrónico.<br>• Recibir APDU de respuesta desde el pasaporte electrónico. | |

| |
|---|
| **Resultado esperado:**<br>Reconocer satisfactoriamente el lector, así como enviar y recibir datos mediantes APDU. |
| **Evaluación de la prueba:** Prueba Satisfactoria. |

**Tabla 11: HU1_CP1 - Gestión de la comunicación.**

| **Caso de prueba de aceptación** | |
|---|---|
| **Código de caso de prueba:** HU3_CP2 | **Nombre de la historia de usuario:** Permitir la autenticación mediante el control de acceso básico |
| **Responsable de la prueba:** Adrian Martínez Pérez | |
| **Descripción de la prueba:** Prueba de funcionalidad para verificar la comunicación con el terminal mediante un canal seguro. | |
| **Condiciones de ejecución:** Debe existir algún lector conectado para leer la zona de lectura mecánica o introducir los datos de la zona de lectura mecánica manualmente. | |
| **Entrada/Pasos de ejecución:**<br>• Recibir los datos de la zona de lectura mecánica enviados desde el lector.<br>• Generar clave mediante los datos de la zona de lectura mecánica.<br>• Comprobar la clave generada con la almacenada en el chip del pasaporte electrónico.<br>• Permitir la comunicación cifrando los datos. | |
| **Resultado esperado:**<br>Obtención y autenticación de la clave de la zona de lectura mecánica y permitir la comunicación segura con la terminal. | |
| **Evaluación de la prueba:** Prueba Satisfactoria. | |

**Tabla 12: HU3_CP2 – Permitir la autenticación mediante el control de acceso básico.**

| Caso de prueba de aceptación | |
|---|---|
| **Código de caso de prueba:** HU4_CP3 | **Nombre de la historia de usuario:** Gestionar la información en el pasaporte electrónico. |
| **Responsable de la prueba:** Adrian Martínez Pérez | |
| **Descripción de la prueba:** Prueba de funcionalidad para verificar la gestión de la información almacenada en el pasaporte electrónico. | |
| **Condiciones de ejecución:** Debe existir comunicación con la terminal mediante un canal seguro. | |
| **Entrada/Pasos de ejecución:**<br>• El usuario hace una solicitud de servicio.<br>• El middleware inicia la comunicación enviando el primer comando APDU al applet del pasaporte electrónico.<br>• Se reciben los datos del applet mediante un APDU de respuesta.<br>• Según la solicitud de servicio escogida por el usuario, se gestionan los datos del pasaporte electrónico.<br>• Se muestran los resultados al usuario. | |
| **Resultado esperado:**<br>Leer y modificar satisfactoriamente la información almacenada en los pasaportes electrónicos. | |
| **Evaluación de la prueba:** Prueba Satisfactoria. | |

**Tabla 13: HU4_CP3 – Gestionar la información en el pasaporte electrónico.**

| Caso de prueba de aceptación | |
|---|---|
| **Código de caso de prueba:** HU5_CP4 | **Nombre de la historia de usuario:** Gestionar el sistema de ficheros. |
| **Responsable de la prueba:** Adrian Martínez Pérez | |
| **Descripción de la prueba:** Prueba de funcionalidad para verificar la estructura lógica de los datos almacenados en el pasaporte electrónico. | |
| **Condiciones de ejecución:** Debe existir comunicación con la terminal mediante un canal seguro y recibir un comando APDU de respuesta del applet del pasaporte electrónico. | |
| **Entrada/Pasos de ejecución:**<br>• Lectura del árbol jerárquico del fichero maestro (FM).<br>• Verifica que los ficheros elementales FE que almacena los datos dentro del chip | |

| |
|---|
| cumplan con el estándar LDS. |
| **Resultado esperado:**<br>Verificar que el sistema de fichero esté organizado de la forma FM- FD- FE y que la información esté distribuida siguiendo las especificaciones del estándar LDS. |
| **Evaluación de la prueba:** Prueba Satisfactoria. |

**Tabla 14: HU5_CP4 – Gestionar el sistema de ficheros.**

| **Caso de prueba de aceptación** | |
|---|---|
| **Código de caso de prueba:** HU2_CP5 | **Nombre de la historia de usuario:** Permitir la autenticación activa y pasiva |
| **Responsable de la prueba:** Adrian Martínez Pérez | |
| **Descripción de la prueba:** Prueba de funcionalidad para verificar el identificador del chip del pasaporte electrónico y prevenir la modificación de los datos a los usuarios no autorizados. | |
| **Condiciones de ejecución:** El lector debe tener acceso a todas las llaves públicas de todos los países. | |
| **Entrada/Pasos de ejecución:**<br>• Verificar la existencia de la firma contenida en el chip del pasaporte electrónico.<br>• Se obtiene la firma digital generada mediante los códigos hash de los ficheros almacenados en el pasaporte electrónico y la del país expedidor.<br>• Comparar las firmas para asegurar la autenticidad de los datos almacenados en el pasaporte electrónico. | |
| **Resultado esperado:**<br>Verificar que sea posible la autenticidad tanto del chip como de los datos almacenados en el pasaporte electrónico. | |
| **Evaluación de la prueba:** Prueba Satisfactoria. | |

**Tabla 15: HU2_CP5 – Permitir la autenticación activa y pasiva.**

## *3.9 Conclusiones*

- En el capítulo se desarrollaron importantes diagramas para mostrar la implementación de la solución, siendo estos el diagrama de componentes y el diagrama de secuencia.
- El desglose de las historias de usuario en tareas de la ingeniería fue una buena práctica que mostró a los programadores las funcionalidades específicas a implementar.
- El desarrollo de la solución fue guiado y verificado por las pruebas unitarias que permitió el desarrollo y diseño del software.

  Se realizaron pruebas de aceptación para asegurar la funcionalidad del sistema coinciden con las historias de usuarios.

## CONCLUSIONES

- El sistema desarrollado permitió la comunicación entre la aplicación y un pasaporte electrónico, utilizando el componente middleware como capa de comunicación.
- Las tecnologías utilizadas permitieron el desarrollo de la solución.
- El Middleware desarrollado cuenta con un grupo de clases que le posibilitan la creación de comandos APDU para cada uno de los requerimientos de la solución.
- El Applet cumple con el mecanismo de control de acceso básico, así como la verificación de las condiciones de acceso a los ficheros elementales, lo que garantiza la seguridad para poder acceder a los datos del pasaporte electrónico.
- Con el uso de tecnologías Java se logró una aplicación multiplataforma, completamente funcional en los principales sistemas operativos existentes en el mercado.

## RECOMENDACIONES

Se recomienda:

- Realizar las pruebas de aprobación a la historia de usuario relacionada con la personalización del pasaporte electrónico.
- Realizar la implementación del mecanismo de seguridad control de acceso extendido, así como pruebas al mismo.
- Implementar una solución utilizando la plataforma .Net.
- Desarrollar una interfaz que permita mediante la utilización de las librerías implementadas mostrar las huellas digitales almacenadas en el applet del pasaporte electrónico.

## BIBLIOGRAFÍA CITADA


**2009.** *Global Platform.* [En línea] 2009. www.globalplatform.org.

**Almeida Sotolongo, Dayron y Sáez Vilar, Joel. 2009.** *Solución para el control de acceso a la información de las entidades externas, en la cédula de identificación electrónica de la República Bolivariana de Venezuela.* 2009.

**COCOMO II Jongmoon Baik. 2000.** *Model Difinition Manual.* 2000.

**e-Passport System. Solutions, Integrales. 2010.** 2010.

**Fernández Santana, Vismar y Pereda Viñolo, Katerina. 2010.** *Plataforma para el desarrollo de servicios en línea utilizando tarjetas inteligentes.* 2010.

**Gemalto. 2006.** *GemBorder Applet.* 2006.

**GlobalPlatform. 2003.** *Card Specification, Version 2.1.1.* 2003.

**ISO/IEC. 2005.** *info_isoiec7816-4{ed2.0}en.pdf.* 2005.

**Organización de Aviación Civil Internacional. 2006.** *Documento de viaje de lectura mecánica, Parte2, Volumen 1.* s.l. : OACI, 2006.

**—. 2006.** *Documentos de viaje de lectura mecánica, Parte 2.* 2006.

**Pérez Costa, Michel Rafael y Fernández Leyva, Luis. 2008.** *Sistema de Administración de Tarjetas Inteligentes y Aplicaciones para la Cédula de Identidad Electrónica de la República Bolivariana de Venezuela.* 2008.

**Sánchez Véjar, Néstor Alonso. 2008.** *Control Acceso.* 2008.

**Sharykin, Raman. 2006.** *Java Card Programming.* 2006.

**Sun Microsystems, Inc. 2003.** *Application Programming Interface.* [Java Card™ Platform, Version 2.2.1] 2003.

**Toyserkani, Ali. 2007.** *Java Card Technology.* 2007.

## BIBLIOGRAFÍA CONSULTADA


**2009.** *Global Platform.* [En línea] 2009. www.globalplatform.org.

**Almeida Sotolongo, Dayron y Sáez Vilar, Joel. 2009.** *Solución para el control de acceso a la información de las entidades externas, en la cédula de identificación electrónica de la República Bolivariana de Venezuela.* 2009.

**COCOMO II Jongmoon Baik. 2000.** *Model Difinition Manual.* 2000.

**e-Passport System. Solutions, Integrales. 2010.** 2010.

**Fernández Santana, Vismar y Pereda Viñolo, Katerina. 2010.** *Plataforma para el desarrollo de servicios en línea utilizando tarjetas inteligentes.* 2010.

**Gemalto. 2006.** *GemBorder Applet.* 2006.

**GlobalPlatform. 2003.** *Card Specification, Version 2.1.1.* 2003.

**ISO/IEC. 2005.** *info_isoiec7816-4{ed2.0}en.pdf.* 2005.

**Organización de Aviación Civil Internacional. 2006.** *Documento de viaje de lectura mecánica, Parte2, Volumen 1.* s.l. : OACI, 2006.

**—. 2006.** *Documentos de viaje de lectura mecánica, Parte 2.* 2006.

**Pérez Costa, Michel Rafael y Fernández Leyva, Luis. 2008.** *Sistema de Administración de Tarjetas Inteligentes y Aplicaciones para la Cédula de Identidad Electrónica de la República Bolivariana de Venezuela.* 2008.

**Sánchez Véjar, Néstor Alonso. 2008.** *Control Acceso.* 2008.

**Sharykin, Raman. 2006.** *Java Card Programming.* 2006.

**Sun Microsystems, Inc. 2003.** *Application Programming Interface.* [Java Card™ Platform, Version 2.2.1] 2003.

**Toyserkani, Ali. 2007.** *Java Card Technology.* 2007.

## GLOSARIO DE TÉRMINOS

**FE:** Fichero elemental.

**FD:** Fichero dedicado.

**FM:** Fichero maestro.

**PKI:** Infraestructura de Llave Pública.

**PLM:** Pasaporte de Lectura Mecánica

**DVLM:** Documento de Viaje de Lectura Mecánica.

**PKCS:** Estándar Criptográfico de Llave Pública.

**Framework:** Es una estructura de soporte definida en la cual otro proyecto de software puede ser organizado y desarrollado.

**Applet:** Aplicación que se ejecutan dentro de las tarjetas inteligentes para gestionar la información almacenada.

## ANEXOS

### Anexo 1: Datos obligatorios y opcionales definidos para la LDS.

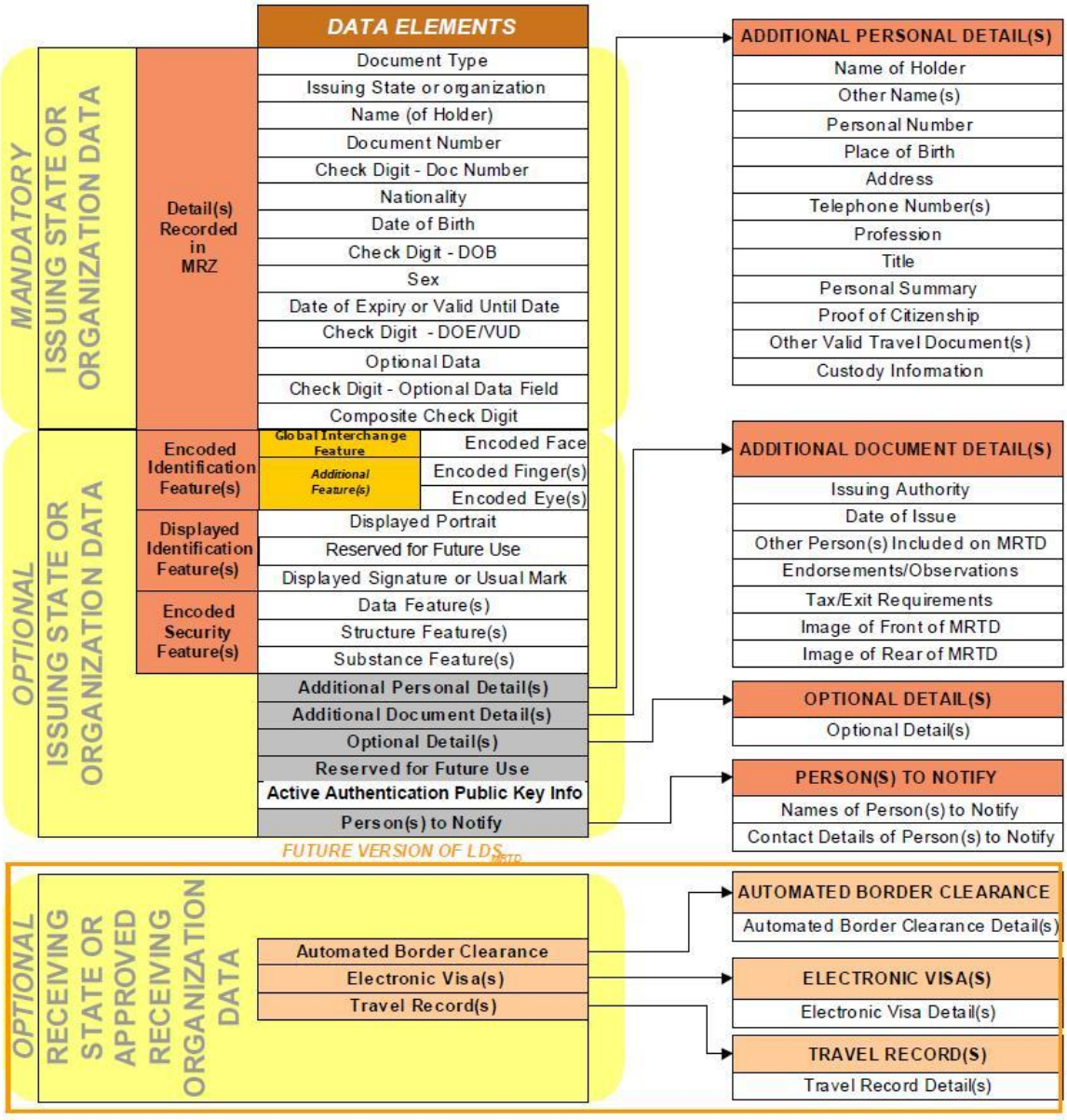


**Figura 10: Datos obligatorios y opcionales definidos para la LDS.**

## Anexo 2: Plan de Entregas.

| Entregable | Fin Iteración 1 | Fin Iteración 2 |
|---|---|---|
| **Applet y middleware para pasaportes electrónicos** | Enero 2010 | Mayo 2011 |

**Tabla 16: Plan de entregas.**

## Anexo 3: Multiplicadores de esfuerzo (factores de costo).

| Nombre | Abreviatura | Valor | Justificación |
|---|---|---|---|
| **Confiabilidad del producto y Complejidad.** | RCPX | 1.30 | El sistema presenta un nivel de complejidad alto. |
| **Reusabilidad requerida.** | RUSE | 1.07 | El nivel de reusabilidad es alto. |
| **Dificultad de la plataforma.** | PDIF | 0.87 | Uso de la memoria y almacenamiento bajo, plataforma estable. |
| **Experiencia del personal.** | PREX | 0.87 | El nivel de experiencia en el uso del lenguaje y la plataforma de trabajo es alto. |
| **Aptitud del personal.** | PERS | 0.83 | La capacidad del personal es alta. |
| **Facilidades.** | FCIL | 0.87 | Se utilizan herramientas de modelación que facilitan el trabajo y entornos de desarrollo integrados. |
| **Cronograma de desarrollo requerido.** | SCED | 1.00 | Se utilizó el tiempo planificado para el desarrollo del sistema. |
| **Total(EM)** | | **0.76** | |

**Tabla 17: Multiplicadores de esfuerzo (factores de costo).**

## Anexo 4: Factores de escala.

| Nombre | Valor | Justificación |
|---|---|---|
| **PREC** | 3.72 | Es un proyecto sin muchos precedentes. |
| **FLEX** | 3.04 | Posee cierta flexibilidad de desarrollo (se cuenta con acuerdos de requerimientos preestablecidos) |
| **TEAM** | 1.1 | Interacciones entre los miembros del equipo altamente cooperativas. |
| **RESL** | 4.24 | Se identifican pocos riesgos críticos pero no existen las herramientas para resolverlos. |
| **PMAT** | 4.68 | El nivel de madurez de la organización es utilizada para generar el resultado de la evaluación según CMM es Nivel 2. |
| **Total (SFj)** | **16.78** | |

**Tabla 18: Factores de escala.**

## Anexo 5: Entradas y Salidas externas.

### Tablas de estimación de los Puntos función sin ajustar.

| Nombre de la entrada externa | Cantidad de ficheros | Cantidad de elementos de datos | Clasificación (simple/medio/complejo) |
|---|---|---|---|
| **Aplicaciones contenidas dentro de la tarjeta.** | 1 | 1 | Simple |
| **Middleware.** | 1 | 1 | Simple |
| **Total** | | **2** | |

**Tabla 19: Entradas externas.**

| Nombre de la salida externa | Cantidad de ficheros | Cantidad de elementos de datos | Clasificación (simple/medio/complejo) |
|---|---|---|---|
| **Comandos APDU enviados a la tarjeta.** | 1 | 1 | Simple |
| **Respuestas APDU enviados al middleware.** | 1 | 1 | Simple |
| **Total** | | **2** | |

**Tabla 20: Salidas externas.**

## Anexo 6: Archivos lógicos internos.

| Nombre del fichero interno | Cantidad de elementos de registro | Cantidad de elementos de datos | Clasificación (simple/medio/complejo) |
|---|---|---|---|
| **PassportApplet** | 1 | 1 | Simple |
| **Total** | | **1** | |

**Tabla 21: Archivos lógicos internos.**

## Anexo 7: Archivos externos de interfaces.

| Nombre de la interfaz interna | Cantidad de elementos de registro | Cantidad de elementos de datos | Clasificación (simple/medio/complejo) |
|---|---|---|---|
| **BERTLVScanner** | 1 | 1 | Simple |
| **KeyStore** | 1 | 1 | Simple |
| **PassportCrypto** | 1 | 1 | Simple |
| **Total** | | **3** | |

**Tabla 22: Archivos externos de interfaces.**

## Anexo 8: Puntos función desajustados.

| Elementos | Simple | | Medio | | Complejo | | Subtotal |
|---|---|---|---|---|---|---|---|
| | No | Peso | No | Peso | No | Peso | |
| **Entradas externas** | 2 | 3 | 0 | 4 | 0 | 6 | 6 |
| **Salidas externas** | 2 | 4 | 0 | 5 | 0 | 7 | 8 |
| **Archivos lógicos internos** | 3 | 7 | 0 | 10 | 0 | 15 | 21 |
| **Solicitudes externas** | 0 | 3 | 0 | 4 | 0 | 6 | 0 |
| **Archivos externos de interfaces** | 3 | 5 | 0 | 7 | 0 | 10 | 15 |
| **Total** | | | | | | | **50** |

**Tabla 23: Puntos función desajustados.**

## Anexo 9: Tablas de las tareas de la ingeniería.

| **Tarea de ingeniería** | |
|---|---|
| **Número de tarea:** HU1_T1 | **Historia de usuario:** Gestión de la comunicación |
| **Nombre:** Detectar lector conectado. | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Adrián Martínez Pérez | |
| **Descripción:**<br>Accediendo a la Winscard.dll se obtiene el lector conectado a la terminal para posteriormente comenzar la comunicación. | |

**Tabla 24: HU1_T1 Detectar lector conectado.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU1_T2 | **Historia de usuario:** Gestión de la comunicación |
| **Nombre:** Establecer conexión con el pasaporte electrónico. | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Adrián Martínez Pérez | |
| **Descripción:**<br>Después de detectar el lector se procede a iniciar la conexión con el chip incluido en el pasaporte. | |

**Tabla 25: HU1_T2 Establecer conexión con el pasaporte electrónico.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU1_T3 | **Historia de usuario:** Gestión de la comunicación |
| **Nombre:** Cerrar conexión con el pasaporte electrónico | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Adrián Martínez Pérez | |
| **Descripción:**<br>Al terminar de realizar la comunicación entre el lector y el pasaporte, la misma debe ser cerrada adecuadamente. | |

**Tabla 26: HU1_T3 Cerrar conexión con el pasaporte electrónico.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU3_T1 | **Historia de usuario:** Permitir la autenticación mediante el control de acceso básico |
| **Nombre:** Obtener los datos del código de barra de la zona de lectura mecánica | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Adrián Martínez Pérez | |
| **Descripción:**<br>El lector envía los datos previamente obtenidos de la zona de lectura mecánica hacia el pasaporte para que los mismos sean verificados y así otorgar el permiso para iniciar la comunicación de forma segura. | |

**Tabla 27: HU3_T1 Obtener los datos del código de barra de la zona de lectura mecánica.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU3_T2 | **Historia de usuario:** Permitir la autenticación mediante el control de acceso básico |
| **Nombre:** Decodificar la calve del código de barra y comprarla con la clave almacenada en el chip | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Adrián Martínez Pérez | |
| **Descripción:**<br>Los datos obtenidos del lector son decodificados mediante el algoritmo pertinente hasta obtener una clave, la misma será comparada con otra clave almacenada en el chip para asegurar su veracidad. | |

**Tabla 28: HU3_T2 Decodificar la clave del código de barra y compararla con la clave almacenada en el chip.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU3_T3 | **Historia de usuario:** Permitir la autenticación mediante el control de acceso básico |
| **Nombre:** Permitir o negar la comunicación en dependencia del resultado de la verificación de la clave | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Adrián Martínez Pérez | |
| **Descripción:**<br>En caso de que las claves comparadas sean similares el pasaporte permitiría al lector la comunicación, en caso contrario se termina la conexión. | |

**Tabla 29: HU3_T3 Permitir o negar la comunicación en dependencia del resultado de la verificación de la clave.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU3_T4 | **Historia de usuario:** Permitir la autenticación mediante el control de acceso básico |
| **Nombre:** Cifrar la comunicación entre el lector y el chip. | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Adrián Martínez Pérez | |
| **Descripción:**<br>Si anteriormente las claves correspondían se dará paso a comenzar la comunicación de una forma cifrada asegurando un canal seguro. | |

**Tabla 30: HU3_T4 Cifrar la comunicación entre el lector y el chip.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU4_T1 | **Historia de usuario:** Gestionar la información en el documento de viaje electrónico |
| **Nombre:** Leer los datos almacenados en el documento electrónico de viaje | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Adrián Martínez Pérez | |
| **Descripción:**<br>Siguiendo la elección del usuario se procede a leer los datos almacenados en el pasaporte y a mostrarlos en la interface de la aplicación cliente. | |

**Tabla 31: HU4_T1 Leer los datos almacenados en el documento electrónico de viaje.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU4_T2 | **Historia de usuario:** Gestionar la información en el documento de viaje electrónico |
| **Nombre:** Modificar los datos almacenados en el documento electrónico de viaje | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Adrián Martínez Pérez | |
| **Descripción:**<br>Siguiendo la elección del usuario se procede a leer los datos almacenados en el pasaporte y a mostrarlos en la aplicación cliente. Después se modifican los datos en la interface de la aplicación cliente y los cambios son enviados hacia el pasaporte realizando la modificación de los datos almacenados. | |

**Tabla 32: HU4_T2 Modificar los datos almacenados en el documento electrónico de viaje.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU4_T3 | **Historia de usuario:** Gestionar la información en el documento de viaje electrónico |
| **Nombre:** Eliminar los datos almacenados en el documento electrónico de viaje | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Adrián Martínez Pérez | |
| **Descripción:**<br>Siguiendo la elección del usuario se procede a leer los datos almacenados en el pasaporte y a mostrarlos en la aplicación cliente. Después se eliminan los datos en la interface de la aplicación cliente y los cambios son enviados hacia el pasaporte realizando el borrado de los datos almacenados. | |

**Tabla 33: HU4_T3 Eliminar los datos almacenados en el documento electrónico de viaje.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU5_T1 | **Historia de usuario:** Gestionar el sistema de ficheros |
| **Nombre:** Crear un EF.SOD para la autenticidad e integridad de los datos del pasaporte electrónico | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Nelson Hernández Guerra | |
| **Descripción:**<br>Se crea el fichero elemental SOD detallando aspectos referentes a la estructura y posicionamiento de la información en el árbol jerárquico de ficheros, así como elementos de seguridad. | |

**Tabla 34: HU5_T1 Crear un EF.SOD para la autenticidad/integridad de los datos del pasaporte electrónico.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU5_T2 | **Historia de usuario:** Gestionar el sistema de ficheros |
| **Nombre:** Definir los grupos de datos obligatorios y opcionales | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Nelson Hernández Guerra | |
| **Descripción:**<br>Se define la posición y la capacidad que ocuparán los datos a almacenar en el pasaporte, estructurando los obligatorios y opcionales a ficheros específicos. | |

**Tabla 35: HU5_T2 Definir los grupos de datos obligatorios y opcionales.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU2_T1 | **Historia de usuario:** Permitir la autenticación activa y pasiva |
| **Nombre:** Generar clave personalizada del chip | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Nelson Hernández Guerra | |
| **Descripción:**<br>Se genera una clave que diferenciará al chip de todos los demás haciéndolo único y pudiendo puede probar su legitimidad. | |

**Tabla 36: HU2_T1 Generar clave personalizada del chip.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU2_T2 | **Historia de usuario:** Permitir la autenticación activa y pasiva |
| **Nombre:** Cifrar clave | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Nelson Hernández Guerra | |
| **Descripción:**<br>La clave generada es cifrada mediante un algoritmo. | |

**Tabla 37: HU2_T2 Cifrar clave.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU2_T3 | **Historia de usuario:** Permitir la autenticación activa y pasiva |
| **Nombre:** Generar fichero con los códigos hash de todos los archivos almacenados | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Nelson Hernández Guerra | |
| **Descripción:**<br>Se guardan en el fichero FE.SOD todos los códigos hash de los archivos de almacenamiento de información dentro del chip. | |

**Tabla 38: HU2_T3 Generar fichero con los códigos hash de todos los archivos almacenados.**

| | |
|---|---|
| | **Tarea de ingeniería** |
| **Número de tarea:** HU2_T4 | **Historia de usuario:** Permitir la autenticación activa y pasiva |
| **Nombre:** Generar firma digital usando los códigos hash almacenados en el fichero y la firma digital del país expedidor | |
| **Tipo:** Desarrollo | **Puntos Estimados:** 2 |
| **Fecha inicio:** | **Fecha fin:** |
| **Responsable:** Nelson Hernández Guerra | |
| **Descripción:**<br>Usando los códigos hash almacenados en el fichero SOD y la firma digital del país expedidor se genera una nueva firma digital para detectar la modificación de los archivos. | |

**Tabla 39: HU2_T4 Generar firma digital usando los códigos hash almacenados en el fichero y la firma digital del país expedidor.**

## Anexo 10: Tarjetas CRC.

| **AAEvent** | |
|---|---|
| **Responsabilidades** | **Colaboradores** |
| - Verifica la autenticidad del chip mediante una clave única cifrada. | - java.security.PublicKey<br>- java.util.EventObject<br>- cu.uci.proiden.data.Hex |

**Tabla 40: CRC middleware – AAEvent.**

| **BACEntry** | |
|---|---|
| **Responsabilidades** | **Colaboradores** |
| - Crear una llave para el Control de Acceso Básico. | - java.text.SimpleDateFormat<br>- java.util.Date |

**Tabla 41: CRC middleware – BACEntry.**

| BACEvent | |
|---|---|
| **Responsabilidades** | **Colaboradores** |
| - Realiza el Control de Acceso Básico. | - java.util.EventObject |

**Tabla 42: CRC middleware – BACEvent.**

| CBEFFDataGroup | |
|---|---|
| **Responsabilidades** | **Colaboradores** |
| - Crea un fichero en el que se define la estructura jerárquica de los archivos que almacenan los datos biométricos. | - java.io.ByteArrayInputStream<br>- java.io.DataInputStream<br>- java.io.IOException<br>- java.io.InputStream<br>- java.util.ArrayList<br>- java.util.List<br>- cu.uci.proiden.tlv.BERTLVInputStream<br>- cu.uci.proiden.middleware. DataGroup |

**Tabla 43: CRC middleware – CBEFFDataGroup.**

| MRZInfo | |
|---|---|
| **Responsabilidades** | **Colaboradores** |
| - Se crea una estructura de los datos que deben ser almacenados en la zona de lectura mecánica del pasaporte electrónico. | - java.io.ByteArrayOutputStream<br>- t java.io.DataInputStream<br>- java.io.DataOutputStream<br>- java.io.IOException<br>- java.io.InputStream<br>- java.text.SimpleDateFormat<br>- java.util.ArrayList<br>- java.util.Collection<br>- java.util.Date<br>- java.util.GregorianCalendar |

| | |
|---|---|
| | - java.util.StringTokenizer<br>- cu.uci.proiden.data.Country<br>- cu.uci.proiden.data.Gender |

**Tabla 44: CRC middleware - MRZInfo.**

| FaceInfo | |
|---|---|
| **Responsabilidades** | **Colaboradores** |
| - Se crea una estructura para el almacenamiento de la imagen del titular del pasaporte electrónico. | - java.awt.Rectangle<br>- java.awt.image.BufferedImage<br>- java.io.ByteArrayInputStream<br>- java.io.ByteArrayOutputStream<br>- java.io.DataInputStream<br>- java.io.DataOutputStream<br>- java.io.IOException<br>- java.io.InputStream<br>- java.io.OutputStream<br>- java.util.Collection<br>- java.util.Iterator<br>- javax.imageio.ImageIO<br>- javax.imageio.ImageReadParam<br>- javax.imageio.ImageReader<br>- javax.imageio.ImageWriteParam<br>- javax.imageio.ImageWriter<br>- javax.imageio.stream.ImageInputStream<br>- javax.imageio.stream.ImageOutputStream<br>- cu.uci.proiden.data.Gender |

**Tabla 45: CRC middleware – FaceInfo.**

| Passport | |
|---|---|
| **Responsabilidades** | **Colaboradores** |
| - Se genera la zona de lectura mecánica.<br>- Se crean todos los grupos de ficheros.<br>- Lectura de los ficheros.<br>- Llamadas a los mecanismos de seguridad.<br>- Clase controladora del sistema. | - cu.uci.proiden.data.Country<br>- cu.uci.proiden.data.Gender<br>- java.io.BufferedInputStream<br>- java.io.ByteArrayInputStream<br>- java.io.ByteArrayOutputStream<br>- java.io.IOException<br>- java.io.InputStream<br>- java.io.PipedInputStream<br>- java.io.PipedOutputStream<br>- java.security.PrivateKey<br>- java.util.ArrayList<br>- java.util.HashMap<br>- java.util.List<br>- java.util.Map<br>- cu.uci.proiden.smartcards.CardFileInputStream<br>- cu.uci.proiden.smartcards.CardServiceException<br>- java.math.BigInteger<br>- java.security.GeneralSecurityException<br>- java.security.KeyPair<br>- java.security.KeyPairGenerator<br>- java.security.MessageDigest<br>- java.security.PublicKey<br>- java.security.cert.X509Certificate<br>- java.util.Calendar |

| | |
|---|---|
| | - java.util.Collections<br>- java.util.Date<br>- java.util.TreeMap; |

**Tabla 46: CRC middleware - Passport.**

| PassportApduService | |
|---|---|
| **Responsabilidades** | **Colaboradores** |
| - Encargada de crear la estructura del APDU. | - java.security.GeneralSecurityException<br>- javax.crypto.Cipher<br>- javax.crypto.Mac<br>- javax.crypto.SecretKey<br>- javax.crypto.spec.IvParameterSpec<br>- javax.smartcardio.CommandAPDU<br>- javax.smartcardio.ResponseAPDU<br>- cu.uci.proiden.smartcards.CardService<br>- cu.uci.proiden.smartcards.CardServiceException<br>- cu.uci.proiden.smartcards.APDUListener<br>- cu.uci.proiden.smartcards.ISO7816<br>- cu.uci.proiden.data.Hex |

**Tabla 47: CRC middleware – PassportApduService.**

| PassportPersoService | |
|---|---|
| **Responsabilidades** | **Colaboradores** |
| - Crea la estructura y almacena los datos en la tarjeta del pasaporte electrónico.<br>- Genera los datos necesarios para realizar | - java.io.IOException<br>- java.io.InputStream<br>- java.text.SimpleDateFormat |

| | |
|---|---|
| el control de acceso básico utilizando los datos de la zona de lectura mecánica. | - java.util.Date<br>- javax.smartcardio.CommandAPDU<br>- javax.smartcardio.ResponseAPDU<br>- cu.uci.proiden.smartcards.CardService<br>- cu.uci.proiden.smartcards.CardServiceException<br>- cu.uci.proiden.smartcards.ISO7816<br>- cu.uci.proiden.tlv.BERTLVObject |

**Tabla 48: CRC middleware – PassportPersoService.**

| **PassportApplet** | |
|---|---|
| **Responsabilidades** | **Colaboradores** |
| - Selecciona, instala y procesa los comandos APDU enviados al applet, así como los comandos APDU respuesta al lector del pasaporte electrónico.<br>- Clase controladora del sistema. | - FileSystem.java<br>- PassportCrypto.java<br>- PassportInit.java<br>- CVCertificate.java<br>- KeyStore.java<br>- JCOP41PassportCrypto.java |

**Tabla 49: CRC applet – PassportApplet.**

| **FileSystem** | |
|---|---|
| **Responsabilidades** | **Colaboradores** |
| - Estructura y crea el sistema de ficheros del applet e implementa métodos para la | |

| | |
|---|---|
| lectura de los mismos. | |

**Tabla 50: CRC applet – FileSystem.**

| **PassportCrypto** | |
|---|---|
| **Responsabilidades** | **Colaboradores** |
| - Encargada de codificar el APDU respuesta y decodificar el comando APDU. | - PassportUtil.java<br>- KeyStore.java |

**Tabla 51: CRC applet – PassportCrypto.**