El pasaporte electrónico

Electronic passport

Alina Surós Vicente

Universidad de las Ciencias Informáticas, (UCI)

asuros@vnz.uci.cu

Resumen

Debido a la internacionalidad del documento pasaporte pudiera deducirse que si cada estado estableciera indistintamente los elementos a contener en el pasaporte entonces sería muy difícil el entendimiento de este tipo de documento fuera de los países donde ha sido emitido.

La Organización Internacional de Aviación Civil (OACI), establece una serie de normas que se encuentran enfocadas a los documentos de viaje de lectura mecánica con el objetivo de acelerar el despacho de los pasajeros en los puntos de control fronterizos. Sin embargo, la demanda de datos extras, tales como los elementos biométricos y visas electrónicas no es satisfecha. La OACI con el fin de ampliar la capacidad de almacenamiento del pasaporte ha implementado varios esfuerzos, siendo el uso de un chip la tecnología más aceptada y con mejores resultados.

Los pasaportes electrónicos aumentan la capacidad de almacenamiento de los pasaportes e incorporan nuevas medidas de seguridad electrónica.

Palabras clave: biometría, chip, pasaporte.

Abstract

Due to passport's internationality could realize that if every country manage the value of the data in this document, it would be very difficult to understand by other nations.

International Civil Aviation Organization (ICAO), set up norms focused on the Machine Readable Travel Documents in order to improve border control process. Nevertheless the demand of extra data, such as biometrics and electronic visa is not satisfied. ICAO in pos to extend store capacity have done many effort, being chip technology the most accepted and with the best result.

The electronic passport increases the storage and new security features.

Keywords*:* biometric, chip, Passport.

Introducción

La tecnología, como el terrorismo, ha cambiado dramáticamente el mundo en los últimos tiempos. El resultado de la necesidad de la mejora de la seguridad internacional también ha tenido un impacto significativo en los documentos oficiales de identificación. Sin embargo la falsificación y alteración de la legitimad de los documentos de identificación siempre ha sido un problema.

La amenaza de actos de terrorismo internacionales tales como el 11 de septiembre, requiere que las medidas de seguridad sean constantemente refinadas y aumentadas con el fin de minimizar absolutamente la oportunidad de individuos de cruzar la frontera con credenciales falsas.

Desde diciembre del 2001 la Organización Internacional de Aviación Civil (OACI), encargada de estudiar los problemas de la aviación civil internacional y promover los reglamentos y normas únicos en la aeronáutica mundial, ha estado evaluando las tecnologías de encriptación y qué rol pueden desempeñar en la autenticación de los documentos de seguridad y en la incorporación de biometría dentro de los documentos de viaje, lo cual provee un fuerte apoyo en la validación del portador del documento con datos autocontenidos en el mismo, unido al creciente uso de un alto volumen de tecnologías avanzadas que permiten el almacenamiento de estos elementos biométricos, tales como el chips sin contacto.

Pasaporte electrónico

El pasaporte es el documento de identificación internacional de los miembros de una nación. Si este documento cumple con las especificaciones que figuran en el doc. 9303, parte 1 de la OACI, es el llamado "Pasaporte de Lectura Mecánica" (PLM). El PLM está normalmente elaborado en forma de libreta (tamaño ID-3) y cuenta con una zona de lectura mecánica comprendida en dos líneas de texto OCR-B de 44 caracteres cada una.

La OACI establece una serie de especificaciones a las que deben ajustarse los PLM para que sean compatibles e intercambiables mundialmente empleando tanto medios visuales (lectura ocular) como la lectura mecánica, tratando de satisfacer los distintos requisitos de las leyes y costumbres de los Estados y lograr el más alto nivel de normalización posible dentro de los requisitos divergentes. Las especificaciones sientan las normas para pasaportes que, al ser expedidos por un Estado u organización y aceptados por otro Estado receptor, pueden emplearse para fines de viaje. Los datos que constarán en los PLM en forma legible, tanto visualmente cómo los métodos de captación óptica de caracteres, se presentan en 7 zonas que se enumeran a continuación.

Las zonas I a VI constituyen la zona de inspección visual (ZIV), mientras que la zona VII es la zona de lectura mecánica (ZLM).

Zona I **Encabezamiento**
Zona II **Datos personales (obligatorios y opcionales)**
Zona III **Datos del documento (obligatorios y opcionales)**
Zona IV **Firma**
Zona V **Elemento de codificación**
Zona VI **Datos Opcionales**
Zona VII **Zona obligatoria de lectura mecánica (ZLM)**
Zona de Inspección Visual

En la Figura 1 se especifica el orden en que se pueden acomodar los datos en la hoja de datos del PLM.

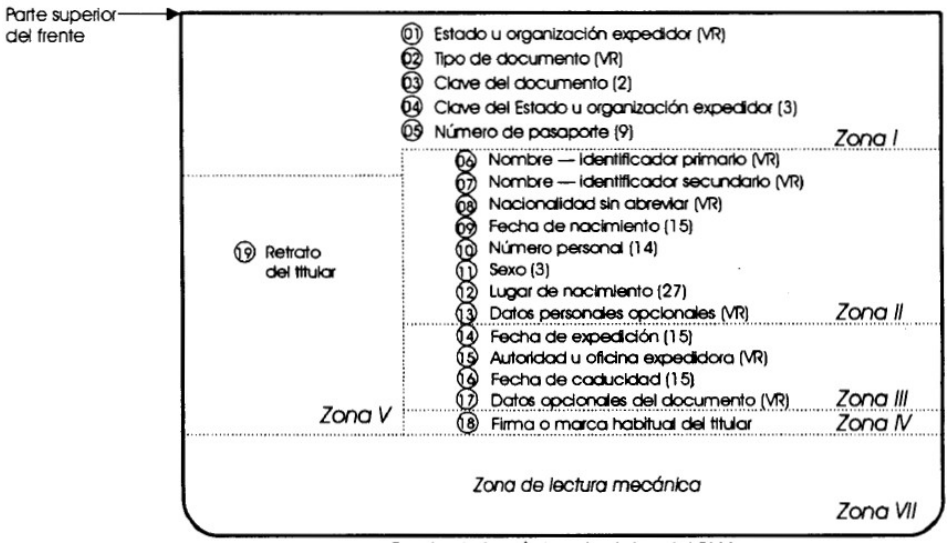

Fig. 1. Orden de los datos de la Página del Pasaporte de Lectura Mecánica.

Zona de Lectura Mecánica

La zona de lectura mecánica deberá ser escrita con caracteres OCR-B permitiendo la lectura mecánica a partir del reconocimiento óptico de los caracteres. En la Figura 2 se ilustra los elementos que componen el código OCR-B.

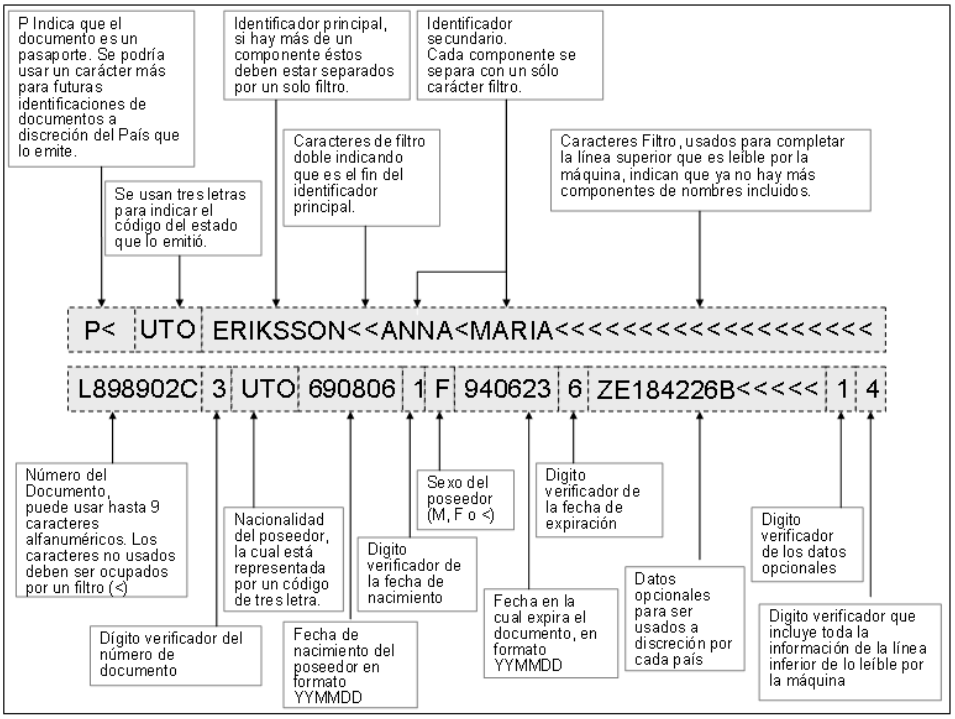

Fig. 2. Código OCR-B.

Pasaporte Electrónico

El Pasaporte Electrónico, es el PLM que incorpora un chip y se identifica con el símbolo que se muestra en la Figura 3.

Fig. 3. Símbolo del Pasaporte Electrónico.

Chip

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

Interoperatibilidad global: al chip 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 a un oficial de inspección o que sea 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 si solo. La razón es que si contiene fuente de energía, no sería posible que durara el tiempo de vida esperado del PLM que es de 10 años. El lector es el que provee la energía para comunicarse con el chip.

El circuito integrado está formado por el chip y una antena, Figura 3.

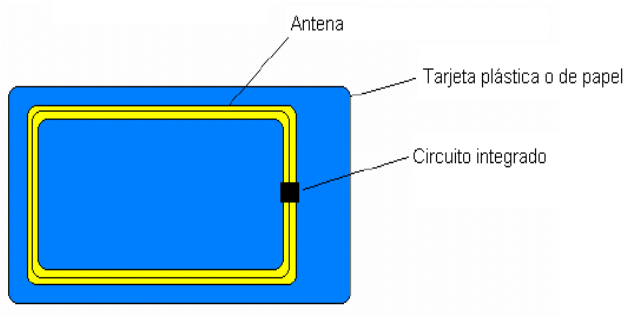

Fig. 4. Estructura del Chip.

Estructura de Datos (LDS)

Los datos al ser almacenados en el chip requieren una estructura de datos estandarizada para habilitar una interoperatibilidad global para PLM facilitando que todas las naciones tengan conocimiento de cómo está estructurado el documento. EL LDS está conformado por elementos de datos (DE) 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 (DG), cada uno de ellos está identificado con un número, como se muestra en la Tabla 1.

Tabla 1. Distribución de los grupos de datos dentro del chip.

Grupo	Nombre
DG1	Detalles almacenados en la ZLM: Tipo de Documento Estado Emisor Nombre Número de Documento Dígito de Verificación - Número de Documento Nacionalidad Fecha de Nacimiento Dígito de Verificación - Fecha de Nacimiento Sexo Fecha de Expiración Dígito de verificación - Fecha de Expiración Datos Opcionales Dígito de verificación - Datos Opcionales Dígito de verificación compuesto
DG2	Rostro codificado
DG3	Huellas codificadas
DG4	Ojos codificados
DG5	Imagen Facial
DG6	Reservado para uso futuro
DG7	Imagen de la firma
DG8	Características de los datos
DG9	Características de la estructura
DG10	Características de la sustancia
DG11	Detalles personales adicionales
DG12	Detalles adicionales del documento
DG13	Detalles opcionales
DG14	Reservado para uso futuro
DG15	Información de la llave para la autenticación activa
DG16	Persona a notificar
DG17	Control automatizado fronterizo
DG18	Visa Electrónica
DG19	Registro de viaje

Estructura de ficheros

Los datos en el chip están almacenados en el sistema de ficheros definido por la ISO 7816-4. Los ficheros están organizados jerárquicamente en ficheros dedicados (DF) y ficheros elementales (EF). Los DF contienen los ficheros elementales y otros ficheros dedicados. Y un fichero maestro (MF), determinado por el sistema operativo, que será la raíz del sistema de ficheros.

Cada grupo de datos consiste en una serie de datos dentro de una plantilla y será almacenado en un EF separado. La estructura y codificación de los datos está definida en la ISO 7816-4 y 7816-6. Cada dato posee una identificación Tag, que es especificada en un código hexadecimal. Cada dato contenido dentro de un grupo de datos posee una única Tag, longitud y valor, como se muestra en la Figura 5.

Data Group	EF Name	Short EF identifier	FID	Tag
Common	EF.COM	'1E'	'01 1E'	'60'
DG1	EF.DG1	'01'	'01 01'	'61'
DG2	EF.DG2	'02'	'01 02'	'75'
DG3	EF.DG3	'03'	'01 03'	'63'
DG4	EF.DG4	'04'	'01 04'	'76'
DG5	EF.DG5	'05'	'01 05'	'65'
DG6	EF.DG6	'06'	'01 06'	'66'
DG7	EF.DG7	'07'	'01 07'	'67'
DG8	EF.DG8	'08'	'01 08'	'68'
DG9	EF.DG9	'09'	'01 09'	'69'
DG10	EF.DG10	'0A'	'01 0A'	'6A'
DG11	EF.DG11	'0B'	'01 0B'	'6B'
DG12	EF.DG12	'0C'	'01 0C'	'6C'
DG13	EF.DG13	'0D'	'01 0D'	'6D'
DG14	EF.DG14	'0E'	'01 0E'	'6E'
DG15	EF.DG15	'0F'	'01 0F'	'6F'
DG16	EF.DG16	'10'	'01 10'	'70'
Security Data	$EF.SO_D$	'1D'	'01 1D'	'77'

Fig. 5. Ficheros en el Chip.

El EF.COM almacena los datos comunes que corresponden fundamentalmente a la organización de los datos dentro del chip. El Identificador corto del fichero es 30 ('1E'). Cada grupo de datos deberá ser almacenado en un EF accesible por un identificador corto del fichero. El EF deberá tener nombre de fichero que se corresponderá con el grupo de datos que contenga, el nombre del fichero EF que contiene los datos de seguridad se denomina EF.SOD.

Ejemplo de valores de objeto de datos. Tabla 2.

Tabla 2. Ejemplo de los valores en el EF.COM

Tag	L	Valor
'5F01'	04	Número de versión con formato aabb, donde aa define la versión del LDS y bb define el nivel al cual se ha actualizado
'5F36'	06	Versión de Unicode con formato aabbcc, donde aa define la mayor versión, bb define la menor versión y cc define el nivel del release
‘5C’	X	Lista de Tag. Lista de todos los grupos presentes

El siguiente ejemplo indica la implementación del LDS versión 1.7, usando la versión Unicote 4.0.0 teniendo los grupos 1 (tag ‘61’), 2 (tag ‘75’), 4 (tag ‘76’), and 12 (tag ‘6C’) presentes.

En este ejemplo está escrito en rojo el valor del Tag, en azul la longitud y los valores en negro.

‘60’’16’
'5F01''04'0107
'5F36''06'040000
‘5C’‘04’’6175766C’

Conjunto de Comandos

El mínimo de comandos soportados por los PLM son:

-SELECT FILE
-READ BINARY

Los parámetros de estos comandos son obligatorios y opcionales. Todos los comandos, formatos y sus códigos de retorno están definidos en la ISO 7816-4. Está reconocido que comandos adicionales serán necesarios para cargar y actualizar la información de:

- GET _CHALLENGE
- EXTERNAL_AUTHENTICATE
- PSO_MSE
- PSO_CDS
- VERIFY_CERTIFICATE

Seguridad

La OACI propone varios mecanismos de seguridad para el PLM. De ellos algunas son de cumplimiento obligatorio u opcional según decisión del país emisor. Estos mecanismos se mencionan a continuación.

Autenticación Pasiva

Es de uso obligatorio

Beneficios

Prueba que el contenido del SO_D y el LDS son auténticos y no ha sido cambiado**.**

Deficiencias

No previene la copia exacta o sustitución del chip ni los accesos no autorizados.

Para poder realizar la autenticación pasiva de los datos almacenados en el chip, el sistema de inspección debe conocer la información de la llave pública del estado emisor del documento. Este método consiste en verificar la firma digital del objeto de seguridad contenido en el chip.

Autenticación Activa

Es de uso opcional

Beneficios

Previene la copia del SO_D y prueba que se está leyendo un chip auténtico y que no ha sido sustituido.

Deficiencias

Adiciona complejidad y requiere procesamiento del chip.

Consiste en leer la ZLM, luego comparar el hash de la ZLM con el almacenado en el SO_D para comprobar que corresponden al mismo documento, luego lee la llave pública para la autenticación activa almacenada en el chip y lo compara con el almacenado en el SO_D, comprobando así que la llave es auténtica. Finalmente se establece un challenge\response entre el chip y el lector.

Control de Acceso Básico

Es de uso opcional

Beneficios

Previene la lectura no autorizada y que se escuche la comunicación entre el PLM y el sistema de inspección.

Deficiencias

No previene la copia exacta o sustitución del chip. Adiciona complejidad y requiere procesamiento del chip**.**

El control de acceso básico comienza con la lectura óptica o visual de la ZLM para derivar las llaves de acceso básicas del documento para después de un efectivo challenge\response se establece un canal seguro de comunicación.

Control de Acceso Extendido

Es de uso opcional

Beneficios

Previene el acceso no autorizado a los datos biométricos adicionales. Previene la lectura no autorizada a los datos biométricos adicionales.

Deficiencias

Requiere el manejo de una llave adicional. No previene la copia exacta o sustitución del chip. Adiciona complejidad y requiere procesamiento del chip.

Este método lo decide el estado emisor y su especificación es conocida en otros estados mediante acuerdos bilaterales.

Encriptación de Datos

Es de uso opcional

Beneficios

Asegura los elementos biométricos adicionales. No requiere procesamiento del chip.

Deficiencias

Requiere una compleja desencriptación y manejo de llaves. No previene la copia exacta o sustitución del chip. Adiciona complejidad.

Este método lo decide el estado emisor y su especificación es conocida en otros estados mediante acuerdos bilaterales.

Sistema automatizado para la emisión de Pasaporte Electrónico

Este tipo de documento requiere una infraestructura tecnológica necesaria para la captura de datos e imágenes de los ciudadanos, validación de identidad, personalización del documento y entrega, pasos fundamentales para la emisión de pasaporte, ilustrados en la Figura 6. Cada uno de estos componentes se concibe de forma independiente, funcionando de forma modular.

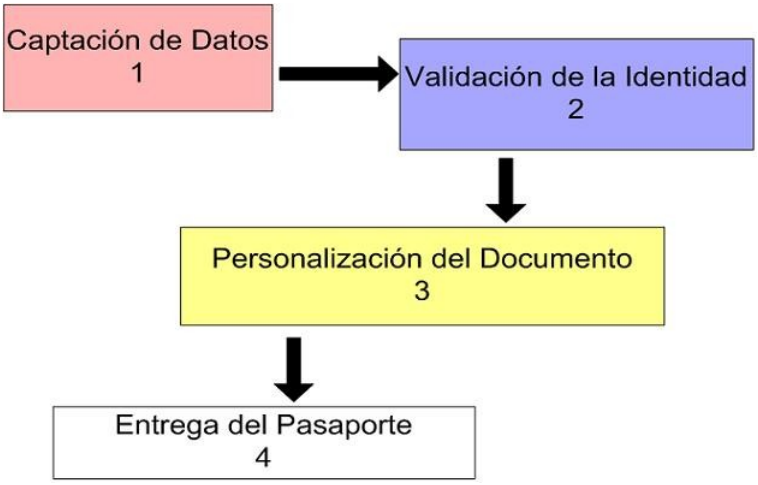

Fig. 6 Pasos para la emisión de pasaporte.

Captura de Datos

En este momento se inicia el trámite de 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 OACI.

Verificación de la Identidad

Los métodos de verificación de la identidad se centran en la verificación biométrica (identificación o verificación de 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 huella digital por diversas ventajas que ofrece frente a otras tecnologías.

Personalización del Documento

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

Personalización Eléctrica. Se refiere a la escritura de los datos en el chip.
Personalización Óptica. Se personalizan los datos que se encuentran en la ZIV.

En este paso guardan gran relación el tipo de documento con la impresora debido al tipo de material con que esté conformada la hoja de datos del documento.

La personalización sugiere la OACI 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.

Entrega del documento

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 que realmente al portador y que los datos almacenados sean suficientes y cuenten con la calidad necesaria para hacer la verificación biométrica.

Conclusiones

Es de vital importancia para una nación contar con un documento de viaje seguro, debido al impacto que tiene en la seguridad nacional la ocurrencia de actos terroristas o la entrada de ciudadanos con documentos falsos al país. Una de las formas de mejorar esta situación es la implementación de un sistema para la emisión de Pasaporte Electrónico como documento de viaje.

Referencias Bibliográficas

Tom A.F. Kinneging. PKI Digital Signatures For Machine Readable Travel Documents. 2004.

ICAO TAG MRTD/NTWG Development Of A Logical Data Structure – LDS For Optional Capacity Expansion Technologies. 2004

ICAO TAG MRTD/NTWG Use of Contactless Integrated Circuits In Machine Readable Travel Documents.

ICAO TAG MRTD/NTWG. Biometrics deployment of machine readable travel documents. 2004.

http://es.wikipedia.org/wiki/Organizaci%C3%B3n_de_Aviaci%C3%B3n_Civil_Internacional

http://www.bioidentidad.com/FAQ_biometria.htm