Autenticación y perspectivas futuras mediante Identificadores Digitales

Vazquez Hess, Matías Román

2013

cad 1503/0124

Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Autenticación y perspectivas futuras mediante Identificadores Digitales

SUBTEMA

Fortalezas y debilidades.
Robo de identidad, ataques a la intimidad y a la privacidad, falsificación de documentación, estafas...

Autor: Ing. Matías Román Vazquez Hess
Tutor del Trabajo Final: Ing. Pagola Hugo

Año de Presentación: 2015
Cohorte: 2013

Declaración Jurada de Origen de los Contenidos:

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Firma:
Nombres y Apellidos: Matías Román Vazquez Hess
DNI: 30.406.007

Resumen

Cada día, mayor es la multiplicidad e interrelación que presentan los individuos de forma electrónica en diversos tipos de relaciones presenciales. Donde la proliferación de sistemas específicos es más común, logrando hacer que los procesos de negocios sean más eficientes y eficaces, pero también más vulnerables.

Debido a la falta de conciencia referida a la seguridad de la información operada, los mismos quedan expuestos de manera desmedida, siendo cada individuo objeto potencial de un sin fin de ataques, a su persona electrónica; es decir, a los identificadores digitales los cuales identifican física y digitalmente su identidad.

El avance de las ciencias y la tecnología, resulta muy positivo; pero si las mismas no son medidas o controladas y administradas o gestionadas conforme a las buenas practicas; la información que manejan, puede ser explotada por entes o seres mal intencionados con el propósito general de causar un daño u obtener un beneficio. Entonces, para reducir la probabilidad de pérdida de información y saber dónde estamos parados se analizara e informara sobre su uso y funcionamiento, tratando de minimizar los riesgos, resguardando al máximo posible la información electrónica a operar por cada individuo, tanto en la actualidad como en un futuro inmediato.

Palabras clave: Identificadores Digitales, Pasaporte Electrónico, Pasaporte Biométrico, RFID, tecnología vulnerable, control masivo, monitoreo global.

Índice

Prólogo

A Dios, quien es mi fortaleza en los momentos difíciles.

A mis Padres, Griselda y Carlos.

A todo aquel que me honra al leer estas páginas, dado que honra una parte de mí.

Matías R. Vz H.

Nómina de abreviaturas y acrónimos

AA, del inglés: Active Authentication; en castellano: Autentificación Activa.

Auto ID, del inglés: Automatic IDentification; y del castellano: Identificación Automática.

BAC, del inglés: Basic Access Control; en castellano: Control de Acceso Básico.

CA, del inglés: Certification Authority; en castellano: Autoridad de Certificación (**AC**).

CCRA, del inglés: Common Criteria Recognition Arrangement; en castellano: Criterios Comunes de Cumplimiento Reconocido.

CE, Comisión Europea.

CRL, del inglés: Certificate Revocation List; en castellano: Lista de Revocación de Certificados (**LRC**).

DE, del inglés: Data Elements; y del castellano: Elementos de Datos.

DF, del inglés: Dedicated Files; y del castellano: Ficheros Dedicados.

DG, del inglés: Data Group; y del castellano: Grupo de Datos.

DNI, Documento Nacional de Identidad.

DSA, del inglés: Digital Signature Algorithm; y en castellano: Algoritmo de Firma Digital.

EAC, del inglés: Extended Access Control; en castellano: Control de Acceso Extendido o Mejorado.

ECDSA, del inglés: Elliptic Curve Digital Signature Algorithm; en castellano: Algoritmo de Firma Digital de Curva Elíptica.

EF, del inglés: Elementary Files; y del castellano: Ficheros / Archivos Elementales.

EIS, del inglés: European Information Society; en castellano: Sociedad Europea de la Información.

FIDIS, del inglés: Future of Identity in the Information Society; en castellano: Futuro de la Identidad en la Sociedad de la Información.

IC, del inglés: Integrated Circuit; y del castellano: Circuito Integrado (**CI**), también referido como Chip o en algunos casos Microchip.

ICAO, del inglés: International Civil Aviation Organization: en castellano: Organización de Aviación Civil Internacional (**OACI**).

IEC, del inglés: International Electrotechnical Commission; en castellano: Comisión Electrotécnica Internacional (**CEI**).

ISO, Organización Internacional de Normalización.

LDS, del inglés: Logical Data Structure; y del castellano: Estructura de Datos Lógica.

MF, del inglés: Master File; y del castellano: Fichero Maestro o Archivo Principal.

MRP, del inglés: Machine Readable Passport; y del castellano: Pasaporte de Lectura Mecánica (**PLM**).

MRTD, del inglés: Machine Readable Travel Document; y del Castellano: Documento de Viaje de Lectura Mecánica (**DVLM**).

MRZ, del inglés: Machine Readable Zone; y del castellano: Zona de Lectura Mecanizada (**ZLM**).

OCR, del inglés: Optical Character Recognition; en castellano: Reconocimiento Óptico de Caracteres (**ROC**).

PA, del inglés: Passive Authentication; en castellano: Autenticación Pasiva.

PACE, del inglés: Password Authenticated Connection Establishment; en castellano: Establecimiento de Conexión Autenticada por Contraseña.

PIN, del inglés: Personal Identification Number; en castellano: Número de Identificación Personal. Comunmente denominada también como: passnumber, contraseña, clave, código secreto.

PKD, del inglés: Public Key Directory; en castellano: Directorio de Clave Pública (**DCP**).

PKI, del inglés: Public Key Infraestructure; y del castellano: Infraestructura de Clave Pública.

PRADO, del inglés: Public Register of Authentic Identity and Travel Documents OnLine; del castellano: Registro Público de Documentos Auténticos de Identidad y de Viaje en Red.

RFID, del inglés: Radio Frequency IDentification; y del castellano: Identificación por Radio Frecuencia.

RSA, algoritmo criptográfico de clave pública, nombrado así por los apellidos de sus inventores: Rivest, Shamir y Adleman.

SAC, del inglés: Supplemental Access Control; en castellano: Control de Acceso Suplementario.

SC, del inglés: Smart Card; y del castellano: Tarjeta Inteligente.

SHA, del inglés: Secure Hash Algorithm; del castellano: Algoritmo de Hash Seguro.

SO_D, del inglés: Document Security Object; del castellano: Objeto de Seguridad del Documento.

SSCD, del inglés: Secure Signature Creation Device; en castellano: Dispositivo Seguro de Creación de Firma (**DSCF**).

SUBE, Sistema Único de Boleto Electrónico.

TAG, anglicismo del inglés, trasladado al castellano y utilizado como significado de etiqueta, identificador o baliza, genéricamente.

td"x", del inglés: Size "x" Machine Readable Official Travel Document; y del castellano: Tamaño "x" del Documento de Viaje de Lectura Mecánica Oficial (**dv**). Corresponde a los diferentes tamaños a leer del documento de viaje, los cuales pueden ser: td1, td2 y td3 respectivamente.

UE, Unión Europea.

VIZ, del inglés: Visual Inspection Zone; y del castellano: Zona de Inspección Visual (**ZIV**).

Cuerpo introductorio

Introducción

Desde hace tiempo que la necesidad de mejores y más sofisticadas medidas de seguridad es de primordial importancia. La autenticación de usuarios y los métodos de autorización necesitan distinguir entre ellos y aún más, mediante factores complementarios para asegurar que la persona adecuada obtiene la información correcta. Por ello, las perspectivas futuras mediante Identificadores Digitales permiten acreditar física y digitalmente la identidad de una persona en particular. Donde por lo general, su soporte físico consta de una tarjeta inteligente[1] (SC, Smart Card en inglés) conteniendo un soporte electrónico; el cual cuenta con ciertas especificaciones brindándole una robustez aceptable tanto dentro de su aspecto tangible como intangible, refiriéndonos con este último a su seguridad implícita dentro de este, y de su operatividad en equilibrio en cuanto a una relación costo beneficio aceptable.

El soporte electrónico, es decir, su chip criptográfico, es incrustado dentro del soporte físico con el objeto de servir como herramienta de autenticación y firma electrónica en algunos casos según su soporte de uso, y a través de su interacción según corresponda. Donde el chip básicamente, permite alojar un certificado electrónico el cual indica que la autoridad emisora de la autenticación y la firma electrónica está autorizada para realizar ciertos actos determinados, de forma colaborativa; es decir interactuando de forma multipropósito con diferentes servicios a tal fin y según corresponda.

Desde el punto de vista del ciudadano común, la interoperabilidad que le permite hoy día el soporte electrónico como identificador digital, implementado por ejemplo en el SUBE[2] (Sistema Único de Boleto Electrónico, en Capital Federal y Gran Buenos Aires), el pasaporte electrónico y próximamente el nuevo DNI electrónico en la República Argentina, entre otros tantos; brinda la certeza de poder realizar una transacción de forma segura, no invasiva y con ahorro de tiempo y costos, integrando diversas plataformas y servicios de forma colaborativa e interoperable. Además puede consultar datos de carácter personal y, con la firma digital, podría operar en comercio electrónico de manera confiable y legal.

Entonces, podríamos decir que la implantación de estos identificadores electrónicos, permiten un gran paso para el desarrollo de la sociedad de la información, pues incrementa la seguridad en las transacciones autorizadas a tal fin, y propicia un mayor desarrollo del gobierno electrónico, entre otros y según sea el caso.

Sin embargo, para que todo esto sea posible es necesario capacitar a la sociedad en las ventajas y peligros sobre el uso de esta nueva tecnología utilizada ya en la segunda guerra mundial[3], y muy explotada hace algún tiempo, de diversas maneras, denominada RFID[4] o Identificación por Radio Frecuencia.

Por esto, los sistemas simples de autenticación de usuarios, basados en usuario y contraseña, son insuficientes porque no proporcionan la suficiente granularidad entre los sistemas, pueden resultar tediosos, y ser fácilmente robados, compartidos y violados; lo cual no quiere decir que los identificadores digitales no pueden ser vulnerados ni mucho menos, pero conjugando estos con sistemas más sofisticados de autenticación de usuarios como ser Infraestructura de Clave Pública[5] (PKI), y sistemas biométricos entre otros proporcionan un incremento en los niveles de seguridad a expensas de la usabilidad y los costos que conllevan.

Por otro lado, el hardware especifico como tarjetas inteligentes[1] (SC) y demás dispositivos, permite cierta portabilidad, pero obliga a los usuarios a adquirir y llevar consigo dispositivos adicionales con funcionalidad limitada, la cual provoca además disminución de popularidad de la solución. Entonces, los usuarios quieren ser capaces de tener varias claves para su uso con múltiples partes de confianza; quieren poder utilizar sus llaves en cualquier lugar sin preocuparse por su compromiso, en definitiva, lo que se busca es la capacidad de permitir un entorno móvil o portátil capaz de utilizar claves de forma segura y flexible en múltiples entornos de confianza, pero fundamentalmente, bajo un entorno lo menos invasivo posible, para lograr un alto grado de aceptación entre sus usuarios.

En la actualidad esto es posible mediante la conjugación de diversas tecnologías las cuales le dieron forma y nombre a lo que hoy conocemos como Documentos Electrónicos o análogamente Identificadores Digitales.

Objetivos

Es el objetivo del presente trabajo de investigación, generar conciencia sobre la utilización de identificadores digitales, y su integración multipropósito, conociendo las potenciales debilidades y limitaciones de su arquitectura, para lograr de esta manera, resguardar los accesos de cualquier mecanismo indeseable, inoportuno, impropio y no autorizado; adquiriendo de acuerdo a su análisis, mayor confianza sobre el sistema involucrado, o todo lo contrario.

Además se busca que el análisis realizado, sirva como guía de buenas prácticas para el usuario final, sobre la seguridad e inseguridad detectada, sus implicancias sobre el medio y, la legislación aplicable según corresponda, con el mero fin de generar conciencia y advertir sobre el uso de la tecnología.

Alcance

Se realiza un enfoque analítico sobre las inseguridades que presenta particularmente el pasaporte biométrico, como identificador digital en la actualidad, realizando un resumen de algunas de las principales características necesarias para esclarecer términos y conceptos tratados dentro del documento.

No se pretende demostrar que las implementaciones analizadas no son seguras, sino por el contrario, se trata de dar a conocer probables vulnerabilidades o riesgos de este tipo particular de sistemas. Se limita su enfoque a las fortalezas y debilidades que este identificador presenta. Sobre estas últimas, es decir sus inseguridades, se desarrollara su relación directa con la privacidad, dada su exposición; además de realizar un análisis local, y global.

El análisis se limita a la utilización del Documento 9303[6] de la Organización de Aviación Civil Internacional[7] [8] (OACI) bajo la denominación "Documentos de Viaje de Lectura Mecánica" (MRTD / DVLM), como marco de referencia internacional.

Cuerpo principal

Identificadores Digitales

En la actualidad, debido a la continua exposición y al caudal de información existente, es necesario la evolución de esta, en sentido de pasar de simples repositorios de información impresa a verdaderos centros digitales de información. El salto del mundo análogo al mundo digital, prevé según la ley de Moore[9] [10] hace ya más de 50 años, que la capacidad de procesamiento de la información se duplica en promedio cada 18 a 24 meses, mientras que sus costos caen a la mitad. Entonces, para poder llevar a cabo esto se debe poder utilizar los mecanismos provistos por las nuevas tecnologías con el fin de satisfacer las necesidades informacionales de un mundo cada vez más exigente.

Ante tal situación, los centros de información tienden a desarrollar una serie de estrategias que centran su atención hacía un nuevo horizonte digital que permite la organización de esta gran masa de información, con el supuesto propósito de facilitar el acceso, aumentar la seguridad y reducir los tiempos; lo que permitiría una recuperación de forma práctica, eficiente y no invasiva fundamentalmente.

Por lo cual, podríamos decir que un identificador es una serie de pequeñas secuencias de caracteres alfanuméricos que identifica recursos genéricamente, como ser: documentos, imágenes, archivos, servicios, y demás; haciendo que éstos se encuentren disponibles y donde sus funciones principales son:

1. Proporcionar datos acerca de la identificación del documento,
2. Desarrollar la forma de localizarlos,
3. Recuperar la información que contiene, para generar nuevo conocimiento.

Entonces, es aquí donde definimos un identificador digital (análogamente documento electrónico[11]) como un documento cuyo soporte material es algún dispositivo electrónico o magnético, portable que permite identificar a una persona unívocamente y en el que el contenido está codificado mediante algún tipo de código digital, que puede ser leído, interpretado, o reproducido, mediante el soporte de detectores de magnetización. Contiene información del titular del mismo así como información que es de utilidad para determinar la validez del mismo y el nombre de su autoridad emisora. Para ello, cada identificador digital

tiene un periodo de validez. Es posible ver información detallada de un identificador, tal como todos los datos del titular del mismo, o la cadena de emisión de certificados. Los detalles del titular de un identificador digital pueden incluir varios datos, tales como su dirección de correo electrónico, su organización o su documento de identidad por ejemplo.

En esta oportunidad, los identificadores digitales (electrónicos) a analizar particularmente será el Pasaporte Electrónico. De manera análoga, tanto sea este, como sus similares documentos que incorporan identificadores digitales como por ejemplo, el Boleto Electrónico y Documento de Identidad Electrónico, la gran parte de estos, se relacionan por compartir la misma tecnología: RFID[4] [Para mayor información, ver Anexo: Tecnología Aplicada] como medio de transporte de la información almacenada. Por ello, vale aclarar que el enfoque del presente trabajo de investigación no tiene por objeto profundizar sobre la tecnología RFID[4] en su máxima expresión sino solo lo necesario y suficiente para poder comprender y analizar en profundidad los identificadores digitales antes detallados.

Figura 1. Ejemplo genérico de Identificador digital[12]

Pasaporte Electrónico

Desde hace tiempo, los organismos de seguridad y estados del mundo buscan medios para lograr identificar rápidamente a los individuos que transitan sus territorios de forma centralizada y aggiornada a los tiempos que corren.

Luego del ataque a las Torres Gemelas[13] de Nueva York, en el año 2001 en los Estados Unidos; quedo expuesto el modo en que cualquier terrorista o similar transita por cualquier aeropuerto y frontera del mundo sin ser siquiera detectado. Por lo cual, las agencias de seguridad de diferentes estados, se vieron necesitadas y de manera urgente, incrementar las medidas de control en sus fronteras. Aquí es donde se produce la necesidad de incorporar algún mecanismo el cual permita aumentar la seguridad y velocidad de identificación de cada individuo básicamente y de manera clara y sencilla, por lo cual se decide incorporar a los pasaportes físicos, un soporte tecnológico, como lo es el chip RFID[4], para permitir identificar de forma digital y de manera global, el tránsito de una persona particular.

Figura 2. Ilustración genérica de visado de pasaporte convencional[14]

Características

Generalidades

También conocido como pasaporte biométrico[15] o pasaporte digital (Ver Figura 3), es un documento de identidad que además del uso de papel de seguridad, contiene una lámina de policarbonato[16] con un circuito electrónico[17] incrustado en ella, y que usa la biometría[18] para autentificar a los viajeros.

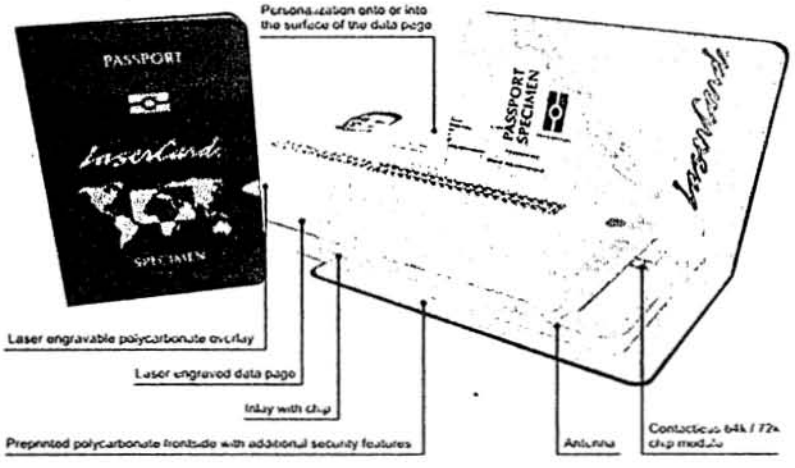


Figura 3. Ilustración de pasaporte electrónico genérico[19]

La incorporación de un minúsculo chip RFID[4] en el documento permite almacenar información adicional como también duplicar la que se encuentra impresa en la página que contiene los datos del titular del mismo, permitiendo mediante PKI[5], la certificación de la veracidad de los datos contenidos en él, haciéndolo en teoría infalsificable. Para mayor información, ver Anexo: Patentes.

Apariencia

En el caso particular del nuevo pasaporte electrónico argentino[20] (Ver Figura 5), vigente desde el 15/6/2012, y aprobado desde el 13/6/2012[21] por la Resolución 1474/2012[22] de la Dirección Nacional del Registro Nacional de las Personas; contiene un código alfanumérico el cual reemplaza el tradicional número de DNI[23] y algunos otros cambios relacionados con su seguridad. De acuerdo a información dada a conocer por el ministerio del Interior[24] [25] [26] [27], el documento cumple con las máximas medidas de seguridad exigidas a nivel internacional, por lo cual, se estaría teóricamente en condiciones de comenzar a pedir excepciones de visa en países como Estados Unidos, Canadá o Australia por ejemplo.

Figura 4. Nuevo pasaporte AR[28]

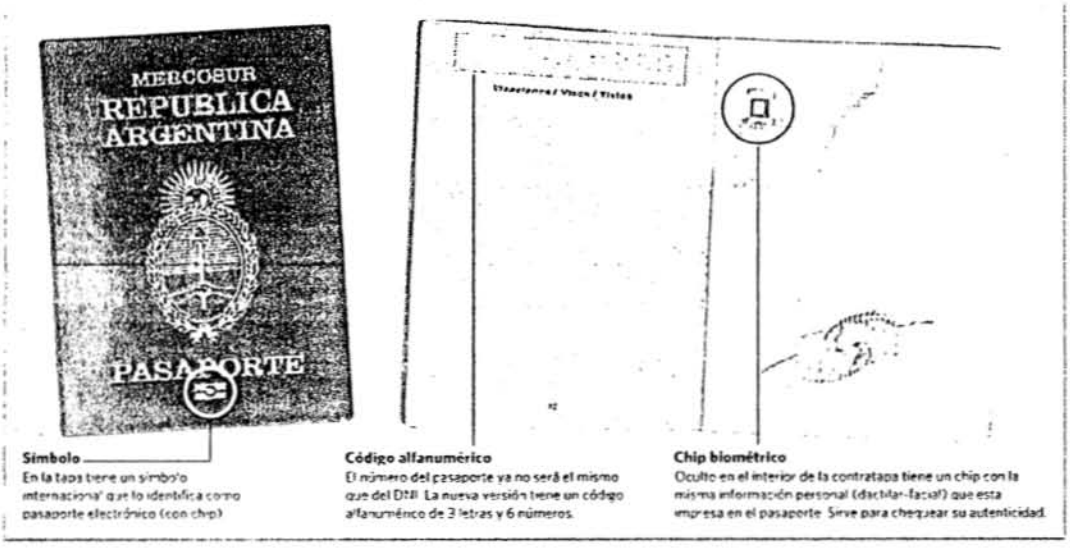


Figura 5. Infografía del nuevo pasaporte electrónico argentino[29]

Más allá del aumento en su costo[21], relacionado directamente a la tecnología que utiliza, la novedad más importante es el chip incorporado en la contratapa del documento, juntamente con una antena para su comunicación pasiva y sin contacto (Ver Figura 6). En ese pequeño chip RFID[4] están guardados los datos biométricos del portador; es decir, la información facial, dactilar y de identidad; siendo la misma que figura en las primeras páginas, pero digital.

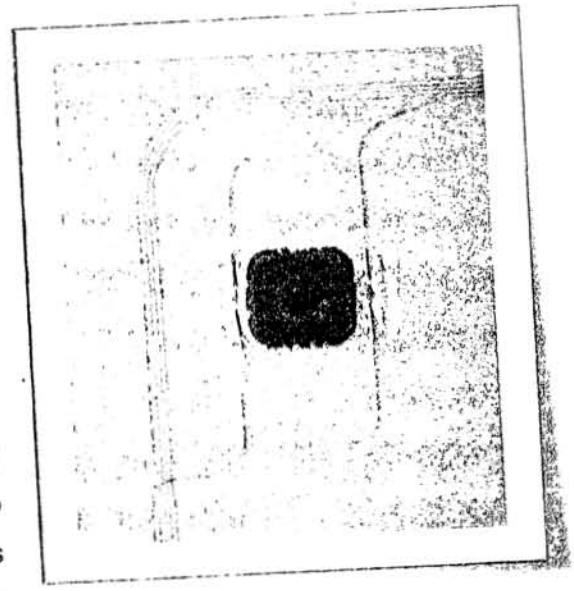


Figura 6. Ampliación de Chip RFID[4] y antena, contenido dentro de la contratapa interna de un pasaporte británico[30]

Este tipo de documentos, se pueden identificar genéricamente mediante un símbolo en su portada (Ver Figura 7), más específicamente un símbolo de micro plaqueta contenida, el cual indica visualmente que es un documento de viaje de lectura mecánica electrónico (con capacidad de identificación biométrica). Contiene un CI[31] (Circuito Integrado) sin contacto, con capacidad de almacenamiento de datos, como todos los pasaportes de los estados que adoptaron y usan esta tecnología, de acuerdo a las normas internacionales de la Organización de Aviación Civil Internacional[7] [8].

Figura 7. Símbolo identificador de pasaporte biométrico internacional[32]

Con respecto a Latinoamérica[33], la región consta de 20 países de los cuales solo 15 de ellos emiten este tipo de documento y los mismos son: Argentina, Bolivia, Brasil, Chile, Colombia, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela. En el caso particular de Argentina, a diferencia de los demás países de la región, se emite con una validez de 10 años[34], a diferencia del resto que lo emite por 5 años.

Componentes

Chip RFID sin contacto físico

Para el almacenamiento y el tratamiento de datos, se utiliza un circuito integrado[31] sin contacto o de proximidad (microchip) que se incorpora, por ejemplo, a pasaportes, y documentos de identidad genéricamente. Este microchip, que en la mayoría de los casos no resulta visible, va conectado a una antena para permitir su comunicación dado que el mismo es sin contacto físico (inalámbrico), por lo cual el único medio para accederlo, es a través de un lector de ondas electromagnéticas (radiofrecuencia - RFID[4]). Para iniciar la transmisión, el chip tiene que estar cerca del lector. El contenido protegido del chip se puede leer a una distancia teórica de 0-10 cm de acuerdo a las especificaciones. Puede ir embebido (Ver Figura 8) en una gruesa lámina de plástico, en el interior de la cubierta del documento o en una página especial de policarbonato. Para preservar la seguridad de los datos, en la zona de lectura mecanizada (ZLM) [Para mayor información, ver Anexo: Lectura Mecanizada - MRTD = DVLM / MRZ = ZLM] opcionalmente, se puede aplicar un control de acceso básico (donde el lector solo puede leer el chip una vez que este ha sido activado mediante una clave personal de acceso PIN validada [Ver: Mecanismos de protección - BAC]).

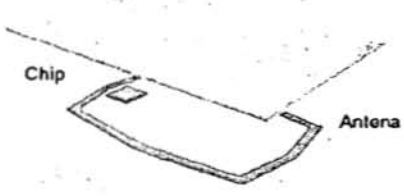


Figura 8. Chip y antena RFID[35]

Un control de acceso ampliado (autenticación del terminal) se aplica como salvaguarda, mediante una firma digital (para la que se emplea la infraestructura de clave pública[5] de la OACI[7] [8]) protegiendo la autenticidad y la integridad de los datos almacenados, obligatoriamente [Ver: Mecanismos de protección - PA].

Seguridad del identificador del pasaporte

La Organización Internacional de Aviación Civil[7] [8], de ahora en adelante OACI (o ICAO, por sus siglas en inglés: International Civil Aviation Organization); 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, donde los pasaportes electrónicos aumentan la capacidad de almacenamiento de los pasaportes tradicionales e incorporan nuevas medidas de seguridad electrónica.

Desde diciembre del 2001, la OACI[7] [8] es la encargada de estudiar los problemas de la aviación civil internacional y promover reglamentos y normas únicos en la aeronáutica mundial. La cual ha incorporado tecnologías de encripción y autenticación a 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.

Figura 9. Logo de la OACI[36]

La descripción así como las características básicas del chip se hallan descritas en el Documento 9303[37] [38] de la OACI[7] [8] bajo la denominación: "Documentos de viaje de lectura mecánica". Esta organización, también denominada Organización Internacional de Aeronáutica Civil, es una agencia de la Organización de las Naciones Unidas[39] [40] creada en el año 1944 por la Convención de Chicago[41] [42] para estudiar los problemas de la aviación civil internacional y promover reglamentos y normas únicos en la aeronáutica a nivel mundial.

Características Generales

Los datos biométricos obligatorios y normalizados que se utilizan en la actualidad son el reconocimiento facial, siendo opcional en algunos casos el reconocimiento de huellas dactilares, y el reconocimiento de iris entre otros métodos más invasivos. Los mismos fueron adoptados después de la evaluación de diferentes tipos de biometría, donde la OACI[7] [8] define los formatos de archivos biométricos y protocolos de comunicación que se deben utilizar en los mismos, como se mencionó con anterioridad; su interoperabilidad y método de normalización de la información.

Los datos personales se almacenan en un microchip embebido (CI) dentro del mismo documento. De conformidad con las especificaciones de la OACI[7] [8], el chip debe contener mínimamente, los datos incluidos en la zona de lectura mecanizada (en inglés, MRZ: Machine Readable Zone) [Para mayor información, ver Anexo: Lectura Mecanizada - MRTD = DVLM / MRZ = ZLM] de la página de datos biográficos del pasaporte y la imagen facial a modo de identificador biométrico interoperable.

Los datos biométricos contenidos en el microchip pueden compararse con las características biométricas de su titular y con los datos que figuran en la página de datos personales. Esto puede realizarse, de forma manual, empleando un lector de documentos, o también de manera automática, mediante un sistema de barreras electrónicas. Como salvaguarda, se utiliza una firma digital para proteger la autenticidad y la integridad de los datos almacenados. La tecnología utilizada es la denominada infraestructura de clave pública (del inglés PKI[5]) impuesta por el organismo regulador. La firma digital puede ser utilizada por autoridades de control para garantizar que los datos contenidos en el chip fueron expedidos por una autoridad de confianza.

Especificaciones

El pasaporte es el documento de identificación internacional de los miembros de una nación. Si este cumple con las especificaciones que figuran en el documento 9303[37] [38], parte 1, versión 2 de la OACI[7] [8], 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[43] de 44 caracteres cada una.

La OACI[7] [8] establece una serie de especificaciones a las que deben ajustarse los PLM para que sean interoperables empleando tanto medios visuales (lectura ocular) como la lectura mecánica, tratando de satisfacer los distintos requisitos de las leyes y costumbres de los distintos 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 (siete) 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	Descripción	Tipo
I	Encabezamiento	ZIV
II	Datos personales (obligatorios y opcionales)	ZIV
III	Datos del documento (obligatorios y opcionales)	ZIV
IV	Firma	ZIV
V	Elemento de codificación	ZIV
VI	Datos opcionales	ZIV
VII	Zona de Lectura Mecánica obligatoria	ZLM

Tabla 1. Especificación de Zonas de un PLM

Zona de Inspección Visual

A continuación, se especifica el orden en que se pueden acomodar los datos en la hoja de datos del PLM.

Para mayor información, ver Anexo: Medidas de seguridad verificables por medios mecánicos.

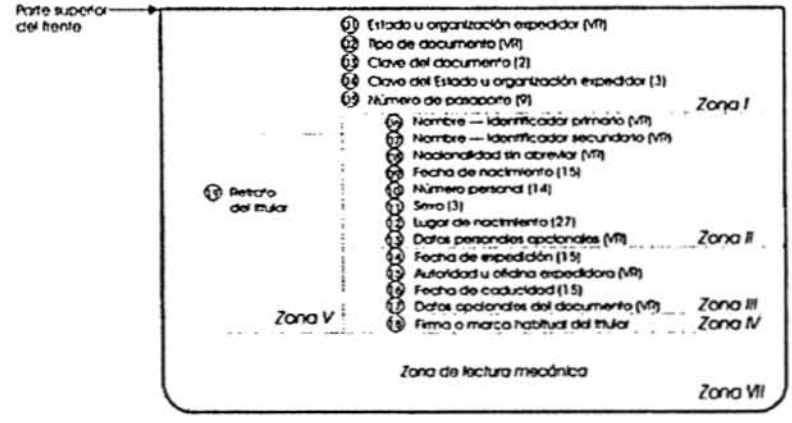


Figura 10. Esquema genérico de datos de la página del PLM de la OACI[7] [8]

Zona de Lectura Mecánica

La zona de lectura mecánica deberá ser escrita con caracteres OCR-B[43] permitiendo la lectura mecánica a partir del reconocimiento óptico de los caracteres. A continuación se ilustran los elementos que componen el código OCR-B[43] (Ver Cuadro 1). Para mayor información, ver Anexo: Lectura Mecanizada - MRTD = DVLM / MRZ = ZLM.

MRZ Im Format td-3 (MRP, machine readable passport)

```
P<D<<ADENAUER<<KONRAD<HERMANN<JOSEPH<<<<<<<<
1234567897D<<7601059M6704115<<<<<<<<<<<<<<2
```

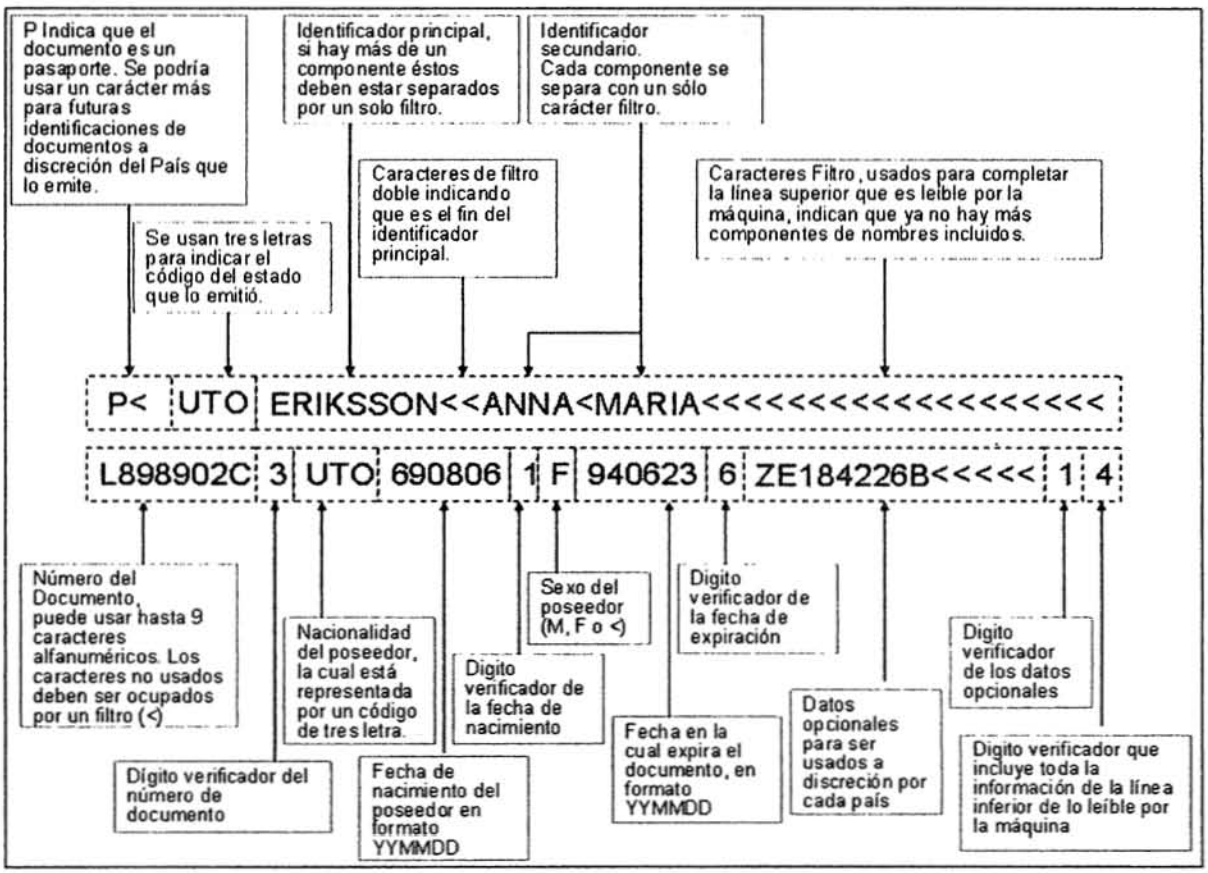
MRZ Im Format td-2

```
IDD<<ADENAUER<<KONRAD<HERMANN<JOSEPH
1234567897D<<7601059M6704115<<<<<<<2
```

MRZ Im Format td-1

```
IDD<<1234567897<<<<<<<<<<<<<<<
7601059M6704115D<<<<<<<<<<<<<2
ADENAUER<<KONRAD<HERMANN<JOSEP
```

Figura 11. Distintos tipos de formatos de la Zona de Lectura Mecánica[44]



Cuadro 1. Código OCR-B[43]

Características Técnicas

De acuerdo a las especificaciones mínimas internacionales, el circuito integrado del chip debe ser sin contacto físico, y tiene que poder almacenar como mínimo 32 kilobytes en una memoria de almacenamiento tipo EEPROM[45], quedando a criterio discrecional del estado expedidor su capacidad máxima, donde los 32kB quedan reservados exclusivamente para el almacenamiento obligatorio de la imagen del rostro, que de acuerdo a las especificaciones de normalización y compresión utilizara de 15 a 20kB, quedando el resto para el almacenamiento de los datos (ZLM) y los elementos necesarios para asegurar los mismos.

La interfaz de comunicación se ejecuta de acuerdo a la norma ISO / IEC 14443[46], Tipo A o B, y su tarjeta de identificación debe cumplir la norma ISO / IEC 7816-4/5/6[47], garantizando así su interoperabilidad entre los diferentes estados y fabricantes.

Los datos obligatorios deberán contener los datos de la zona de lectura mecánica, del grupo de datos 1 (DG1), [Ver: Estructura de datos] y la imagen del rostro del titular, del grupo de datos 2 (DG2), [Ver: Estructura de datos] además de un objeto de seguridad ($EF.SO_D$) necesario para la validación de la integridad de los datos contenidos [Ver: Estructura de ficheros].

Su vida normal debe conseguir una duración de 5 a 10 años, por lo que se debe realizar una cuidadosa selección de los materiales empleados en su construcción.

La codificación y comprensión de imágenes se adhiere a la norma ISO / IEC 10918:1994[48], mientras que su representación a la norma ISO / IEC 15444[49].

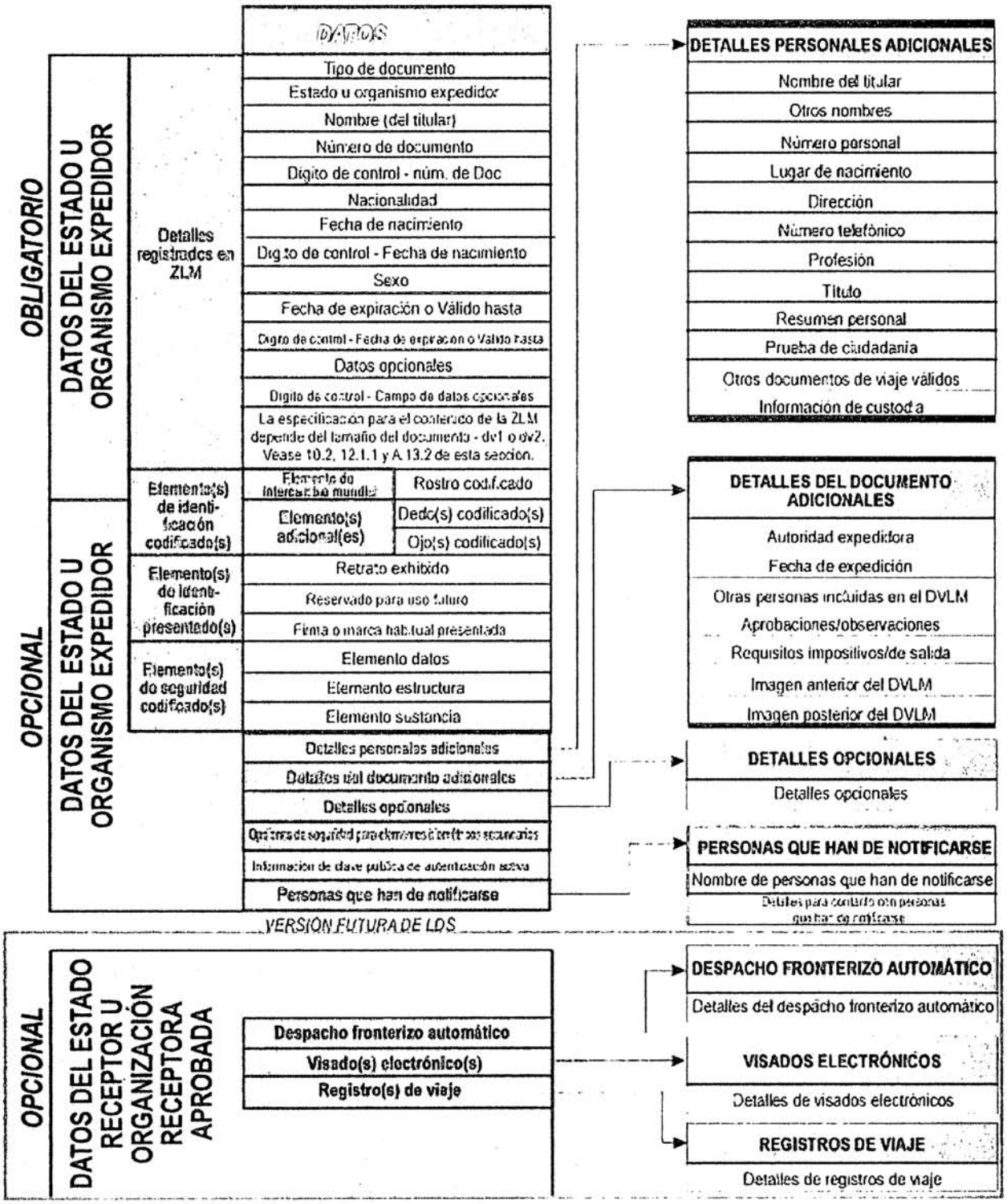
Se utiliza codificación Unicode: UTF-8[50] según norma ISO / IEC 10646[51]. Para interoperabilidad se debe cumplir además con la ISO / IEC 10373-6, para la conformidad con la norma ISO / IEC 14443[46].

Se reconocen los siguientes formatos para el tipo de imagen específica:

Imagen exhibida	Propietario del formato
Imagen del rostro	ISO / IEC 10918, opción JFIF
Dedo	ANSI / NIST-ITL 1-2000
Firma / marca habitual	ISO / IEC 10918, opción JFIF

Tabla 2. Especificación de los tipos de formatos de imagen

Datos contenidos



Cuadro 2. Datos obligatorios y opcionales definidos por OACI[7] [8] según documento 9303[37] [38]

Estructura de datos

Los datos al ser almacenados en el chip requieren de una estructura de datos estándar para una interoperabilidad global para PLM, facilitando que todos los estados tengan conocimiento de cómo está estructurado el documento. La estructura de datos lógica (LDS), está conformada por elementos de datos (DE) de uso obligatorio u opcional y un orden agrupado en elementos de datos.

Dentro de la LDS, los elementos de datos se agrupan según su organización lógica y son definidos como grupos de datos (DG), donde cada uno de ellos está identificado con un número, como se muestra a continuación:

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

Tabla 3. Distribución de los grupos de datos dentro del chip

Estructura de ficheros

Los datos en el chip están almacenados en el sistema de ficheros definido por la ISO 7816-4[52]. Los ficheros están organizados jerárquicamente en ficheros dedicados (DF) y ficheros elementales (EF). Los DF contienen los ficheros

elementales y otros ficheros dedicados. Mientras que un fichero maestro (MF), determinado por el sistema operativo, 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[52] y 7816-6[53 54] respectivamente. Cada dato posee una etiqueta (Tag), que es especificada en un código hexadecimal. Donde cada dato contenido dentro de un DG, posee un único identificador (Tag), entre otros datos, como se muestra a continuación:

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'

Tabla 4. Ficheros contenidos 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 el nombre de fichero que se corresponderá con el grupo de datos que contenga, donde el nombre del fichero EF que contiene los datos de seguridad se denomina EF.SO_D.

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 códigos de retorno están definidos en la ISO 7816-4[52].

Está reconocido que comandos adicionales serán necesarios para cargar y actualizar la información de:

- GET _CHALLENGE
- EXTERNAL_AUTHENTICATE
- PSO_MSE
- PSO_CDS
- VERIFY_CERTIFICATE

Algoritmos utilizados

Los estados deberán utilizar para la generación de firmas mediante el mecanismo de autenticación activa, el estándar ISO / IEC 9796-2:2002[55].

Para la utilización de firma de país, en su CA; claves de firma de documentos y cuando corresponda, los estados deberán optar por uno de los algoritmos indicados a continuación:

- **RSA:** Los Estados que implementen el algoritmo RSA[56] para generación de firmas y verificación de certificados y el objeto de seguridad del documento (SO_D) deberán utilizar el RFC 3447[57].
  La RFC 3447[57] especifica dos mecanismos de firma, RSASSA-PSS y RSASSA-PKCS1 v15.
  Por lo que se recomienda:
  - ✓ Que el tamaño mínimo del módulo n, para las claves de CA de firma de país que utilizan RSA[56] sea de 3072 bits.
  - ✓ Que el tamaño mínimo del módulo n, para las claves de firma de documentos que utilizan RSA[56] sea de 2048 bits.
  - ✓ Que el tamaño mínimo del módulo n, para claves de autenticación activa que utilizan RSA[56] sea de 1024 bits.
- **DSA:** Los Estados que implementen el algoritmo DSA[58] para generación o verificación de firma utilizaran FIPS186-2[59]. La especificación actual para DSA FIPS186-2 sólo apoya 1024 longitudes de clave.
  Por lo que se recomienda:

- ✓ Que el tamaño mínimo de los módulos p y q, para claves de CA de firma de país que utilicen DSA[58] sea de 3072 y 256 bits, respectivamente.
- ✓ Que el tamaño mínimo de los módulos p y q, para claves del firmante de documentos que utilizan DSA[58] sea de 2048 y 224 bits respectivamente.
- ✓ Que el tamaño mínimo de los módulos p y q, para claves de autenticación activa que utilizan DSA[58] sea de 1024 y 160 bits, respectivamente.

- **DSA de curva elíptica:** Los Estados que implementes el algoritmo ECDSA[60] para generación o verificación de firma utilizaran ANSI x9.62[61], e ISO /IEC 15946[62]. Los parámetros de domino de curva elíptica utilizados para generar el par de claves ECDSA[60] deben describirse explícitamente en los parámetros de la clave pública.

  Por lo que se recomienda:
  - ✓ Que el tamaño mínimo para las claves de CA de firma de país que utilicen ECDSA[60] sea de 256 bits.
  - ✓ Que el tamaño mínimo para claves del firmante de documentos que utilizan ECDSA[60] sea de 224 bits.
  - ✓ Que el tamaño mínimo para claves de autenticación activa que utilizan ECDSA[60] sea de 160 bits.
- **Algoritmos de condensación (Hash):** Los algoritmos de condensación permitidos son SHA-I, SHA-224, SHA-256, SHA-384 y SHA-512. Donde debería seleccionarse un algoritmo de condensación de tamaño apropiado para el algoritmo de firma utilizado.

Mecanismos de protección

Los pasaportes digitales, se encuentran equipados con ciertos mecanismos de protección, los cuales no todos son implementados como tampoco todos estos son de carácter obligatorios según la normativa internacional antes mencionada[37] [38]; donde los mecanismos opcionales quedan a criterio del estado emisor en su aplicación. A continuación se describen y detallan los mismos:

- Sistema de firma digital de datos o autenticación pasiva: PA, en inglés: Passive Authentication. Previene la modificación de los datos contenidos en el chip. Utilizando un sistema criptográfico de claves públicas y privadas estableciendo la integridad de los mismos. El chip contiene un archivo que almacena valores hash de todos los archivos almacenados en este (imagen, huella digital, y demás) y una firma digital de estos valores hash. La firma digital se realiza mediante una clave de firma de documentos que a su vez está firmado por una clave de país, estado o nación. Si se modifica un archivo en el chip (por ejemplo, la imagen), esto puede ser detectado dado que el valor hash no es correcto. Entonces, los lectores deben tener acceso a todas las claves públicas de los países utilizados para comprobar si la firma digital es generada por un país de confianza. El sistema es muy seguro, sin embargo sólo un porcentaje minoritario de puntos de control, tiene acceso al banco de claves públicas internacional para validar la autenticidad de los datos[63]. Por eso el grupo "The Hacker's Choice" pudo pasar por válido el pasaporte de Elvis Presley en Amsterdam[95] [Ver Análisis de factibilidad de la explotación real de debilidades: Riesgos y Ataques]. El uso de este mecanismo es obligatorio.

- Sistema anti-rastreo[64]: también denominado chip no rastreable o similar. Su implementación permite responder a cada solicitud realizada al chip RFID[4] en cuestión, con un número de identificador al azar diferente en cada solicitud. Esto potencialmente permite evitar el rastreo del chip, de forma tal que no pueda ser rastreable un pasaporte a partir de una operación elemental de lectura; es decir, cambia el valor devuelto, por lo cual el detector malicioso no sabe si se trata del mismo pasaporte. A pesar de esto, se demostró[65] que se podría hacer un seguimiento, e incluso conocer el país de origen[66] [Ver Análisis de factibilidad de la explotación real de debilidades: Riesgos y Ataques]. Particularmente, el uso del mecanismo de números de identificación aleatorios es opcional y no obligatorio.

- Sistema de control de acceso básico: BAC[67], Basic Access Control en inglés. Implementa un sistema de encripción de datos básico, utilizando

una clave o PIN creada a partir de algunos datos del pasaporte. Funcionalmente protege el canal de comunicación entre el chip y el lector mediante el cifrado de la información transmitida, donde antes de que los datos puedan ser leídos desde el chip, el lector tiene que proporcionar una clave que se obtiene a partir de la zona de lectura mecánica: como por ejemplo, la fecha de nacimiento, la fecha de caducidad y el número de documento. Varios especialistas vulneraron el sistema obteniendo fácilmente el PIN a partir de los datos públicos [Ver Análisis de factibilidad de la explotación real de debilidades: Riesgos y Ataques]. Específicamente, la utilización del presente mecanismo es también opcional y no obligatorio.

- Sistema de autentificación activa: AA, Active Authentication en inglés; también denominado sistema anti clonado. Permite guardar una clave privada oculta en el hardware que no puede modificarse de ninguna forma, ni tampoco leerse directamente, permitiéndole al chip realizar comprobaciones de integridad de los datos. Marc Witterman y Jeroen van Beek[68] demostraron que, según el modelo de chip, podía hacerse un bypass a esta comprobación y modificar los datos de todas formas [Ver Análisis de factibilidad de la explotación real de debilidades: Riesgos y Ataques]. Su utilización es opcional y no obligatorio.

- Sistema de control de acceso extendido o mejorado: EAC[69], Extended Access Control de acuerdo a su sigla en inglés. Es un sistema que no sólo verifica la autenticidad del chip, sino que también la del sistema receptor (lector), para establecer una comunicación segura. También usa un sistema de encriptado menos vulnerable que el BAC[67]. Se introdujo para proteger los datos biométricos sensibles en los pasaportes de algunos países como la huella digital o escaneo del iris [Ver Análisis de factibilidad de la explotación real de debilidades: Riesgos y Ataques]. La utilización del mecanismo es opcional, salvo para la emisión de documentos dentro de la UE (Unión Europea), donde su uso es obligatorio a partir de julio de 2009.

- Sistema físico de aislamiento del chip: o también conocido como blindaje del chip (anti-skimming o anti-fraude), de acuerdo a su interpretación. Básicamente y mediante una lámina metálica en ambas tapas del pasaporte se bloquea el acceso al chip cuando el pasaporte está cerrado (Ver Figura 12); lo cual impide una lectura no autorizada. Países como los EE.UU.[70] han integrado una malla metálica muy delgada en la portada del pasaporte para actuar como escudo cuando la cubierta del pasaporte está cerrado [Ver Análisis de factibilidad de la explotación real de debilidades: Riesgos y Ataques]. Más allá de esto, su utilización es opcional y no obligatoria.

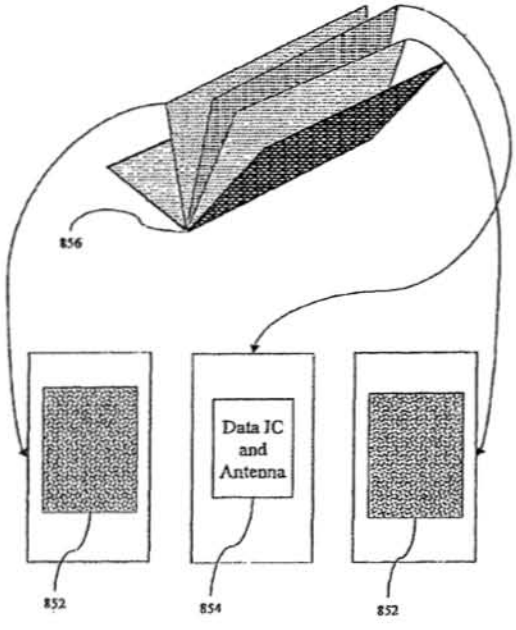


Figura 12. Blindaje metálico utilizado por los EE.UU. para evitar lecturas del pasaporte cuando este se encuentra cerrado (Las capas numeradas en la figura como 852, corresponden a la malla metálica utilizada de forma obligatorio por los EE.UU. en la emisión de sus documentos digitales, dificultando su lectura al estar el mismo cerrado, de acuerdo a la patente accedida)[71]

Inspección fronteriza

En la mayoría de los controles fronterizos (Ver Figura 13) del mundo, para lograr reducir el tiempo de espera de los pasajeros, aumentar el tráfico de los mismos y su seguridad, se utiliza un sistema automático (Ver Figura 14), y colaborativo el cual es interoperable[72] mediante pasaporte biométrico, documento electrónico o similar identificador digital, según sea el caso. El ciudadano está pasando la puerta, exhibiendo su pasaporte electrónico. Un sistema de inspección escanea la zona de lectura mecánica de la página de datos para derivar una clave criptográfica para tener acceso a la tarjeta inteligente sin contacto.

Tan pronto como se leen todos los grupos de datos del chip, el sistema de inspección verifica la autenticidad de los datos para asegurar la validez del chip

del pasaporte electrónico actual, contra la lectura mecánica realizada. Por otro lado, y de forma simultánea, el sistema de reconocimiento facial escanea el rostro del ciudadano para obtener una imagen de su cara.

De esta forma, la imagen obtenida en tiempo real, es comparada con la imagen facial biométrica almacenada en el chip del pasaporte. Si las dos imágenes son similares; es decir, si el resultado arroja una similitud o coincidencia, y el pasaporte electrónico no está en la lista negra y se validan los datos mecánicos contra los biométricos, el ciudadano puede pasar la puerta sin mayores inconvenientes. Vale aclarar, que existen mecanismos alternativos de lectura y comparación biométrica, por lo cual no necesariamente se debe limitar el método.

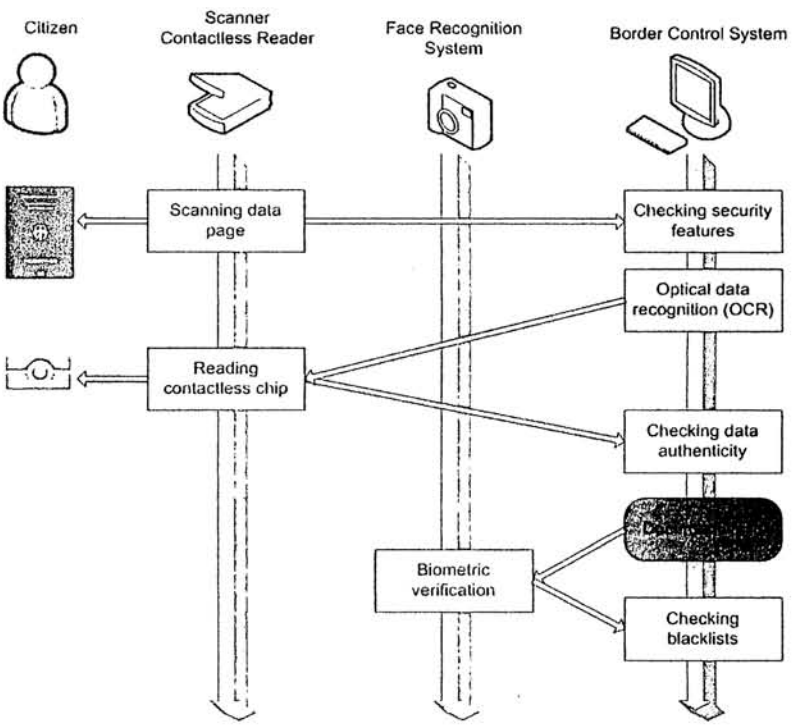


Figura 13. Proceso de control genérico de frontera[73]

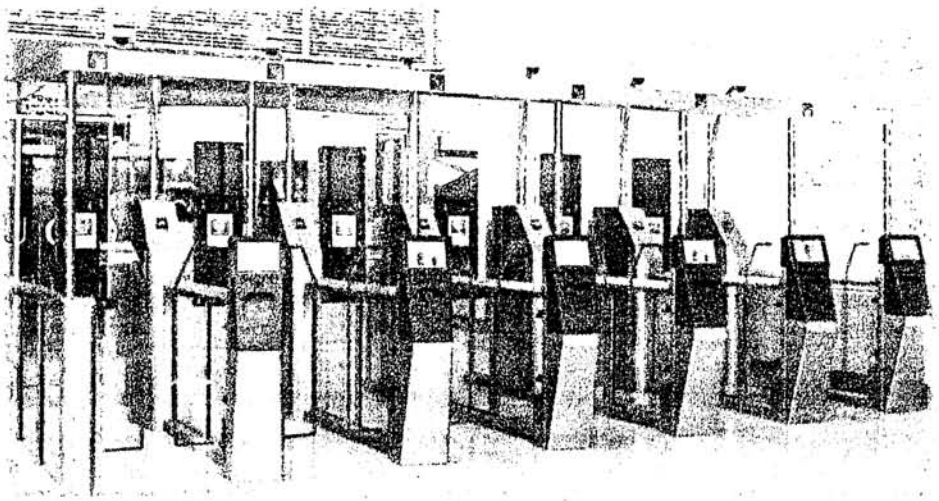
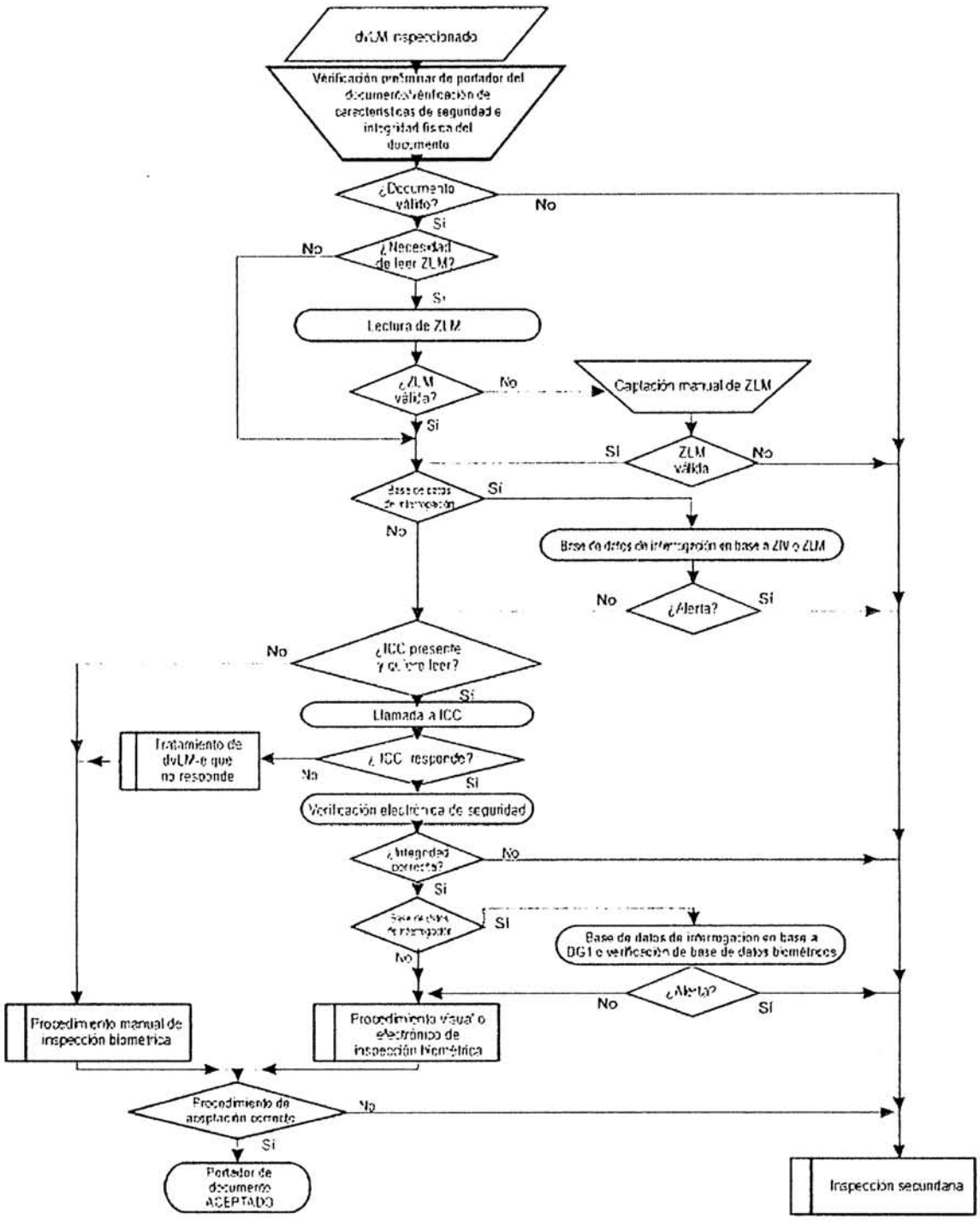


Figura 14. Sistema Automatizado de Control de Fronteras del aeropuerto de Munich[74]

Procedimiento de lectura

A continuación, se ilustra el procedimiento de lectura de un PLM antes de la verificación biométrica del titular, e incluyendo esta:



Cuadro 3. Procedimiento de lectura de PLM de la OACI[7] [8] según documento 9303[37] [38]

Inseguridad del identificador del pasaporte

Vulnerabilidades: medidas de inseguridad del entorno

Los pasaportes biométricos, digitales, inteligentes o como sea que se los pueda denominar, incorporan un identificador digital materializado como vimos con anterioridad, a través de un chip sin contacto con tecnología RFID[4]. Esta tecnología, realiza una emisión de radio en la que transmite los datos que guarda en el chip que contiene, en un área determinada (dependiendo de la frecuencia RFID[4] empleada y de la antena) que puede ir de centímetros a metros, cuando se expone a un campo magnético. La señal emitida puede ser sintonizada por cualquier lector RFID[4], dentro del radio de alcance, lo cual constituye una vulnerabilidad; es decir, una fuga de información que facilita que se pueda realizar el clonado del mismo, además de permitir su rastreo y vigilancia, afectando así la privacidad del portador.

La adopción actual del método de lectura de datos automático, no se puede negar que es práctica y muy rápida, dado que permite la lectura a distancia y en donde en muchos casos y mediante puertas biométricas por ejemplo, se realiza la comparación del rostro biométrico almacenado en el pasaporte con el rostro capturado en tiempo real, entre otras prácticas realizadas[75] [76], pero más allá de esto, claro está que la vulnerabilidad antes enunciada hace a este potencialmente inseguro y viola los derechos de su portador, es decir, no resguardando su privacidad.

Amenazas a la seguridad

Gestión de claves:

Claves de CA

Para proteger las claves privadas, se recomienda la utilización de dispositivos de soporte físico seguros para la generación de firmas, es decir, el SSCD (del inglés: Secure Signature-Creation Device), o en español: Dispositivo Seguro de Creación de Firma; genera nuevos pares de claves, almacena y destruye, después de su expiración y bajo condiciones de seguridad, la clave privada correspondiente. Para proteger contra ataques al SSCD incluyendo ataques de canal lateral (como por ejemplo: temporización, consumo de energía, emisión electromagnética, o inyección de fallas) y ataques contra el generador

de número aleatorio, se recomienda utilizar SSCD que hayan sido certificados y validados por un órgano de certificación que se ajuste a CCRA (del inglés: Common Criteria Recognition Arrangement) con arreglo a un perfil de protección de Criterios Comunes[77] (CC[78], del inglés, Common Criteria) alineado con EAL 4+[79] (del inglés: Evaluation Assurance Nivel 4+; en español: Aseguramiento de Evaluación Nivel 4+), del tipo SOF High (Strength of Function, High), es decir, un TOE (Target of Evaluation); nivel de evaluación alto.

Al distribuir certificados de CA de firma de país, autofirmados por medios diplomáticos, debe ejercerse extremo cuidado en impedir la inserción de un certificado falso. Además, se recomienda que los Estados almacenen en condiciones de seguridad los certificados de CA de firma de país recibidos y accesibles por dispositivos lectores en forma también segura. Para proteger contra ataques al dispositivo lector, se recomienda utilizar dispositivos lectores que sean certificados y validados por un órgano de certificación que se ajuste a CCRA con arreglo a un adecuado perfil de protección de Criterios Comunes[77] como EAL 4+[79] SOF High.

Claves de autenticación activa

Se recomienda generar pares de claves para autenticación activa en forma segura. Como la clave privada se almacena en el CI[31] sin contacto de memoria segura y el soporte físico del circuito integrado sin contacto debe resistir ataques durante todo el periodo de validez del DVLM (Documento de Viaje de Lectura Mecánica con un CI[31] sin contacto incorporado y con capacidad para utilizarse con fines de identificación biométrica del portador bajo normas específicas del Documento 9303[37] [38], parte 3 de la OACI[7] [8]), se recomienda utilizar un CI[31] sin contacto que sean certificados y validados por un órgano de certificación que se ajuste a CCRA[77] [78] con arreglo a un perfil de protección de Criterios Comunes[77] adecuado con EAL 4+[79] SOF High.

Respecto a la tecnología de CI[31] empleada, influye en la longitud de clave máxima de las claves utilizadas dentro del CI[31] sin contacto para autenticación activa. Muchos CI[31] sin contacto no soportan actualmente longitudes de clave que excedan un nivel de seguridad de 80 bits, lo que fue el motivo de elegir este valor como mínimo recomendado. Este es un nivel de seguridad relativamente

bajo comparado con su período de validez en el DVLM. Por consiguiente, se recomienda utilizar claves más largas, si el CI[31] sin contacto las soporta.

Los Estados que utilicen el mecanismo de autenticación activa para validar un DVLM extranjero también deberían saber que no se ha especificado mecanismo de revocación para las claves de autenticación activa comprometidas.

Ataques de negación de servicio

Deben considerarse ataques de negación de servicio cuando los Estados se basen en el directorio para distribución de certificados del firmante de documentos y CRL[80] (Certificate Revocation List o Lista de Revocación de Certificados). Estos ataques no pueden impedirse, por consiguiente se recomienda que el certificado del firmante de documentos requerido para validar el objeto de seguridad del documento también se incluya en el propio objeto de seguridad del documento. Los Estados receptores deberán utilizar el certificado del firmante de documentos proporcionado.

Para distribuir bilateralmente las CRL[80] se recomienda establecer canales múltiples (como por ejemplo: Internet, teléfono, fax, correo, etc.) con otros Estados y confirmar la recepción de las CRL[80] recibidas.

Amenazas de clonado

La reproducción de los datos firmados almacenados en el CI[31] sin contacto es posible. Los Estados preocupados por la posibilidad de que se copien datos de sus ciudadanos en otro CI[31] sin contacto deberían implantar la autenticación activa que asegure que dichos intentos puedan detectarse.

Autenticación pasiva

La autenticación pasiva no impide la copia de los datos almacenados en el CI[31] sin contacto. En consecuencia, es posible sustituir el CI[31] sin contacto de un DVLM por un CI[31] sin contacto falso donde se almacenan los datos copiados del CI[31] sin contacto de otro DVLM. Por lo cual, los Estados receptores deberán verificar que los datos leídos del CI[31] sin contacto pertenecen verdaderamente al DVLM presentado. Esto puede realizarse comparando el DG1 almacenado en el CI[31] sin contacto con la ZLM impresa en el DVLM. Si el DG1 y la ZLM se

corresponden y el objeto de seguridad del documento es válido, y el DVLM presentado no ha sido manipulado en forma no autorizada (no es falsificado), entonces puede considerarse que el DVLM y los datos almacenados en el CI[31] sin contacto se corresponden verdaderamente.

Autenticación activa

La autenticación activa dificulta la sustitución del CI[31], pero no lo hace imposible; el DVLM presentado por el falsificador al sistema de inspección podría estar equipado con un CI[31] especial. Este CI[31] funciona básicamente como intermediario con el CI[31] sin contacto genuino emplazado en un lugar diferente: es decir, el CI[31] se comunica con el falsificador, el falsificador se comunica con otro falsificador y el otro falsificador tiene acceso (temporario) al CI[31] sin contacto genuino. El sistema de inspección no está en condiciones de saber que ha autenticado un CI[31] sin contacto realmente genuino. Este ataque se denomina: Ataque de gran maestro de ajedrez.

Amenazas a la confidencialidad / intimidad

Control de negación de acceso

El uso de CI[31] sin contacto de proximidad ya minimiza los riesgos para la confidencialidad dado que los dispositivos lectores deben estar muy cerca de los CI[31] sin contacto y, por consiguiente, no se considera que la extracción de información sea una amenaza grave. No obstante, la escucha furtiva en un sistema de comunicaciones existente entre un CI[31] sin contacto y un lector es posible desde una distancia mayor. Por lo cual, los Estados que quieran tratar esta amenaza deberían implantar el sistema físico de aislamiento del chip, o también conocido como blindaje del chip (anti-skimming o anti-fraude).

Control de acceso de base

Las claves de acceso de base utilizadas para autenticar el lector y establecer las claves de sesión para cifrar comunicaciones entre el CI[31] sin contacto y el lector se generan a partir del número de documento de 9 (nueve) dígitos, la fecha de nacimiento y la fecha de expiración. Así pues, la entropía de las claves es relativamente baja. Para un DVLM con validez de diez años la entropía es, como máximo, de 56 bits. Con conocimiento adicional (por ejemplo,

edad aproximada del titular o relaciones entre el número de documento y la fecha de expiración) la entropía desciende aún más. Debido a la entropía relativamente baja, en principio un falsificador podría registrar una sesión cifrada, calcular las claves de acceso de base mediante fuerza bruta a partir de la autenticación, obtener las claves de sesión y descifrar la sesión registrada. No obstante, esto todavía requiere un considerable esfuerzo con respecto a la obtención de los datos de otras fuentes.

Autenticación activa: trazas de datos

En el protocolo de prueba-respuesta utilizado para la autenticación activa, el CI[31] sin contacto firma una cadena de bits que ha sido escogida en forma pseudo aleatoria por el sistema de inspección. Si un Estado receptor utiliza la fecha, hora y lugar actuales para generar su cadena de bits en forma impredecible pero verificable (como por ejemplo, utilizando un soporte físico seguro), una tercera parte puede confirmar posteriormente de que el firmante estaba en determinada fecha y hora en determinado lugar.

Amenazas criptográficas

Las longitudes de clave mínimas recomendadas, se han seleccionado para que el descifrado de dichas claves requiera cierto esfuerzo (supuesto), independientemente del algoritmo de firma empleado.

Tipo de clave	Nivel de seguridad
CA de firma de país	128 bits
Firmante del documento	112 bits
Autenticación activa	80 bits

Tabla 5. Longitudes de clave mínimas recomendadas por la OACI[7 8]

Progreso computacional

Según la Ley de Moore[9 81 82], el poder computacional se duplica cada 18 a 24 meses en promedio. No obstante, la seguridad del algoritmo de firma no está influenciada solamente por el poder computacional; los progresos en matemática, ósea el criptoanálisis y la disponibilidad de nuevos métodos de procesamiento no estándar, como por ejemplo, el empleo de computadoras cuánticas, también debe tenerse en cuenta.

Debido a los largos periodos de validez de las claves es muy difícil formular predicciones con respecto a los progresos matemáticos y la disponibilidad de dispositivos de computación no estándar. Por consiguiente, las recomendaciones para longitudes de clave se basan principalmente en el poder computacional extrapolado. Por lo cual, los Estados deberían revisar a menudo las longitudes de clave de sus propios DVLM y también de los DVLM recibidos por las razones antes mencionadas.

La generación de pares de claves en forma especial puede mejorar la actuación general del algoritmo de firma, pero también pueden explotarse para criptoanálisis en el futuro. Por consiguiente, deberían evitarse dichos pares de claves especiales.

Colisiones de condensación

Cuando no es posible encontrar otro mensaje que produzca el mismo valor condensado que un mensaje determinado, es considerablemente más sencillo encontrar dos mensajes que produzcan el mismo valor de condensación; lo que se puede denominar comúnmente como: Paradoja de nacimiento[83].

En general, todos los mensajes que han de firmarse se producen por el propio firmante de documentos. Por consiguiente el encontrar colisiones de condensación no ayuda mucho a un falsificador. No obstante, si las fotografías proporcionadas por el solicitante en forma digital son aceptadas por el firmante de documentos sin una modificación aleatoria adicional, es posible el siguiente ataque:

- Dos personas comparten sus fotografías digitales. Entonces voltean en forma aleatoria un pequeño número de bits reiteradamente en cada fotografía hasta que dos fotografías producen el mismo valor de condensación.
- Ambas personas solicitan un nuevo DVLM utilizando la fotografía manipulada. Cada persona puede ahora utilizar el DVLM de la otra persona siempre que sea posible sustituir la fotografía digital en el CI sin contacto (por ejemplo, mediante la sustitución de la plaqueta).

La función de condensación SHA-1 sólo proporciona 80 bits de seguridad con respecto a colisiones de condensación. Así pues, es considerable más

sencillo encontrar una colisión de condensación que descifrar la clave del firmante de documentos que proporciona 112 bits de seguridad, por ende, siempre que las colisiones de condensación sean objeto de preocupación (por ejemplo, como se describió anteriormente), no se recomienda utilizar SHA-1 como función de condensación.

Análisis de factibilidad de la explotación real de debilidades: Riesgos y Ataques

Podemos definir como riesgo, al daño probable o remanente según corresponda, sobre un activo si se encontrara este desprotegido; es decir, la exposición a una amenaza la cual explota una vulnerabilidad provocando directamente el riesgo. Por lo cual, decimos que amenaza es un daño potencial a un activo y vulnerabilidad es la debilidad de un activo que puede ser aprovechada por una amenaza. Por lo cual, hace tiempo que se logró explotar la vulnerabilidad existente en los pasaportes biométricos.

A continuación se detallaran algunas de las explotaciones de vulnerabilidades más conocidas sobre pasaportes digitales, comprobando de manera fehaciente las amenazas de seguridad que estos presentan.

En 2005 Marc Witterman mostró que se podía romper la clave necesaria para la lectura del chip con un mecanismo de protección BAC[67] incorporado. Posteriormente, en 2006 Adam Laurie escribió una aplicación de software, aplicando de esta forma uno de los ataques de Witterman. Donde, el acceso a información pública permite reducir significativamente el número de claves posibles. Laurie demostró el ataque mediante la lectura del chip del pasaporte británico de una reportera del periódico Daily Mail en un sobre cerrado[84] [85]. Un dato no menor, es que algunos pasaportes biométricos, no utilizan el mecanismo de protección BAC[67], por lo cual esto permite al atacante, leer el contenido del chip sin proporcionar una clave, haciendo que el ataque sea más sencillo dado que no se debe sortear el mecanismo básico de control de acceso como medio de protección.

Tiempo después, Jeroen van Beek[68], más precisamente por el año 2008, demostró que los mecanismos de seguridad opcionales se pueden desactivar mediante la eliminación de su presencia desde el archivo índice del pasaporte[86].

Esto permite a un atacante quitar los mecanismos de protección, como por ejemplo el AA. El ataque está documentado en el suplemento del Documento 9303[6] bajo la nomenclatura: R1-p1_v2_sIV_0006[87], y puede ser resuelto mediante parches de software del sistema de inspección. Es importante mencionar, que el suplemento del documento 9303[6], presenta características vulnerables, donde a su implementación, resulta un proceso de inspección vulnerable.

En 2007, Luks Grunwald[88] presentó un ataque aprovechando las nuevas vulnerabilidades que introducía el sistema mejorado de control de acceso (EAC[69]), que le permitía bloquear permanentemente el chip, volviendo inutilizable el pasaporte. Se estableció que si una clave EAC[69], necesaria para la lectura de huellas y la actualización de certificados, es comprometida, un atacante podría subir un certificado falso con una fecha de emisión a futuro. Donde el acceso al chip es afectado hasta alcanzar la fecha futura.

Un equipo conformado por la Universidad de Radboud[89] y por la Universidad de Lausitz[90] respectivamente, demostró que es posible determinar el país de origen de un pasaporte sin conocer la clave necesaria para leerlo[66], burlando así el mecanismo de protección anti-rastreo. Básicamente esto se puede lograr mediante los mensajes de error generados por el chip, donde una tabla de búsqueda resultante permite a un atacante determinar el origen del pasaporte.

Sin ir más lejos, en 2008 nuevamente el experto holandés llamado Jeroen van Beek[68 91], y contratado por el diario The Times[92], en menos de una hora, usando una lectora de RFID[4] de unos pocos dólares, accedió a los datos biométricos contenidos en dos pasaportes británicos entregados por el diario antes mencionado, y modificó a su intención la información, clonando un chip RFID[93] con los supuestos datos de Osama Bin Laden, demostrando que los sistemas de autenticación activa (AA) podían ser desactivados.

Claro está que no se había realizado ninguna proeza, sólo se había repetido lo que otros expertos alemanes habían hecho en cinco minutos para la BBC[94] ya en 2006.

Nuevamente, en julio de 2009[95], el grupo de hackers alemanes conocido como The Hacker's Choice[96], logra explotar la vulnerabilidad existente en el pasaporte, descifrando así cómo leer la información contenida en el chip RFID[4]

de un supuesto inviolable pasaporte europeo confeccionado bajo estándares internacionales antes mencionados. Se logra materializar el hecho, clonando y cambiando algunos datos del chip, y renombrándolo como "Elvis Presley", con demás datos biométricos. Para comprobar fehacientemente y documentar el suceso, en el aeropuerto de Ámsterdam y con el chip clonado, probaron en una máquina inteligente su lectura, donde el dispositivo inmediatamente reconoció sin inmutarse la imagen del titular del pasaporte, "Elvis Presley", y no detectó nada anómalo en el mismo. Los crackers[97], generaron información válida a su antojo para insertarla en el chip de un pasaporte, documentando lo sucedido en video[98] posteriormente subido a internet, donde además publicaron un tutorial[99] y el código del software empleado, junto a un artículo: "El riesgo de los Pasaportes inteligentes y el RFID" [100].

Tom Chothia[101] y Vitaly Smirnov, en el 2010, demostraron en un congreso criptográfico cómo podía hacerse el seguimiento de un pasaporte individual, aún sin conocer las llaves criptográficas y vulnerando los sistemas que en teoría impiden que el pasaporte sea rastreable, mediante él envió específico de solicitudes BAC[64] [65].

Kevin Mahaffey[102], demostró en un video[175] que si el pasaporte esta mínimamente abierto (como podría ocurrir en el interior de la cartera de una dama por ejemplo), el mismo, puede ser accedido. Más allá de que el pasaporte sigue siendo vulnerable a ataques en situaciones habituales como por ejemplo, cuando se lo abre en la mesa de entrada de un hotel, en un banco, o situación similar, y donde el mismo incluye el mecanismo de físico de aislamiento del chip implementado obligatoriamente por los EE.UU.

Las intervenciones antes mencionadas, fueron noticia pero no tuvieron reflejada la importancia que causo su efecto el cual podría ser tomado como falsificación de documento público[103], por lo menos en lo que respecta a la jurisdicción de la República Argentina la cual tiene una pena de prisión de 1 a 8 años, según corresponda [Ver Legalidad e Implicancias...].

De todas formas los muchachos de The Hacker's Choice no reinventaron la rueda ni mucho menos, sino que se limitaron a utilizar las herramientas desarrolladas por los especialistas para sus demostraciones[104], y disponibles en la red de redes, como por ejemplo, la desarrollada por Adam Laurie sugestivamente llamada RFIDIOt[105].

Inseguridad de los mecanismos

La OACI[7] [8] propone varios mecanismos de seguridad para el PLM, donde de ellos algunos son de cumplimiento obligatorio y otros no; siendo de carácter opcional según decisión del estado emisor. A continuación se detalla por cada uno de ellos según corresponda el análisis correspondiente de los mecanismos en cuestión:

Mecanismo:	Autenticación pasiva o Sistema de firma digital de datos [PA: Passive Authentication]
Implementación:	Obligatoria
Pros:	Prueba que el contenido del SO_D y el LDS son auténticos y no ha sido cambiado.
Contras:	No previene la copia exacta de los datos almacenados o la sustitución del chip ni los accesos no autorizados.
Detalles:	Para poder realizar la autenticación pasiva de los datos almacenados en el chip, el sistema de inspección debe conocer la información de la clave pública del estado emisor del documento. Este método consiste en verificar la firma digital del objeto de seguridad contenido en el chip.

Tabla 6. Mecanismo de protección: PA

Mecanismo:	Sistema anti-rastreo o Chip no rastreable [Chip Untraceable]
Implementación:	Opcional
Pros:	Acota el universo de ataques de rastreo.
Contras:	No previene efectivamente el seguimiento de un pasaporte, donde incluso se puede conocer hasta el país de origen.
Detalles:	Permite responder a cada solicitud realizada al chip, con un número de identificador al azar diferente en cada solicitud; lo que potencialmente permite evitar el rastreo del chip, a partir de una operación elemental de lectura. Entonces, al cambiar el valor devuelto, el detector malicioso no sabe si se trata del mismo pasaporte.

Tabla 7. Mecanismo de protección: Chip Untraceable

Mecanismo:	Control de acceso extendido o Sistema mejorado de control de acceso [EAC[69]: Extended Access Control]
Implementación:	Opcional
Pros:	Previene el acceso y lectura no autorizado de los datos biométricos adicionales.
Contras:	Requiere el manejo de una clave adicional. No previene la copia exacta o sustitución del chip. Adiciona complejidad y requiere procesamiento del chip.
Detalles:	Este método lo decide el estado emisor y su especificación es conocida en otros estados mediante acuerdos bilaterales.

Tabla 8. Mecanismo de protección: EAC

Mecanismo:	Control de acceso básico o Sistema básico de control de acceso [BAC[67]: Basic Access Control]
Implementación:	Opcional
Pros:	Previene la lectura no autorizada y que se escuche la comunicación entre el PLM y el sistema de inspección, asegurando los elementos biométricos adicionales. Todavía requiere un considerable esfuerzo con respecto a la obtención de los datos de otras fuentes para lograr el quiebre criptográfico del mecanismo.
Contras:	No previene la copia exacta o sustitución del chip. Adiciona complejidad y requiere procesamiento del chip.
Detalles:	El control de acceso básico comienza con la lectura óptica o visual de la ZLM para derivar las claves de acceso básicas del documento para después de un efectivo desafío – respuesta (challenge – response) se establezca un canal seguro de comunicación.

Tabla 9. Mecanismo de protección: BAC

Mecanismo:	Autenticación activa o Sistema de autentificación activa [AA: Active Authentication]
Implementación:	Opcional
Pros:	Previene la copia del SO_D y prueba que se está leyendo un chip auténtico y que no ha sido sustituido, minimizando los ataques de clonado del chip.
Contras:	Adiciona complejidad y requiere procesamiento del chip. No se ha especificado mecanismo de revocación para las claves de autenticación activa comprometidas.
Detalles:	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. Posteriormente, lee la clave pública para la autenticación activa almacenada en el chip y lo compara con el almacenado en el SO_D, comprobando así que la clave es auténtica. Finalmente se establece un desafío – respuesta (challenge – response) entre el chip y el lector.

Tabla 10. Mecanismo de protección: AA

Mecanismo:	Sistema físico de aislamiento del chip o Blindaje del chip [Anti-Skimming o Anti-Fraude]
Implementación:	Opcional
Pros:	No adiciona complejidad ni tampoco requiere procesamiento del chip.
Contras:	Este escudo no previene los accesos no autorizados cuando la cubierta del pasaporte no está cerrada en su totalidad, es decir, al 100%.
Detalles:	Una lámina metálica en ambas tapas del pasaporte, bloquea el acceso al chip cuando el pasaporte está cerrado; lo cual impide una lectura no autorizada. Este método lo decide el estado emisor y su especificación es conocida en otros estados mediante acuerdos bilaterales.

Tabla 11. Mecanismo de protección: Anti-Skimming

Novedades

Recientemente, la OACI[7] [8] ha incorporado un nuevo mecanismo a su set de seguridad, denominado por el acrónimo SAC, el cual será explicado y analizado a continuación:

Control de Acceso Suplementario[106]

SAC, de su contracción del inglés: Supplemental Access Control, es básicamente un conjunto de funciones de seguridad particulares, que especifica el Establecimiento de conexión autenticada por contraseña (PACE: del inglés Password Authenticated Connection Establishment). El cual complementa y mejora el control de acceso básico (BAC), correspondiente a la versión 1 de PACE (PACE v1). Por lo tanto, PACE[107] v2, es la articulación de BAC + SAC a grandes rasgos, evitando dos tipos de ataques:

- Skimming: ataque que consiste en la lectura del chip sin acceso físico al documento y sin la aprobación de su titular. Antes de leer el chip, el sistema de inspección tiene que saber algunos datos que se imprime en el documento (por ejemplo, la ZLM) o una clave (PIN) que se conoce solamente por el titular, lo que significa que tiene nivel superior de seguridad al momento de realizar la inspección; mientras BAC sólo funciona con llaves cortas impresas en la ZLM del documento, PACE v2 permite el uso de números de acceso o PIN.
- Espionaje: ataque que comienza registrando los datos intercambiados entre el lector y el chip, para ser analizados con posterioridad. El sistema de control utiliza PACE v2 para establecer un canal de comunicación seguro con el chip sin contacto, mediante el uso de criptografía fuerte, ofreciendo una excelente protección.

Con la implementación de PACE comienza la tercera generación de pasaportes electrónicos. Esta novedosa y última generación de pasaportes, se hace de implementación obligatoria, para miembros de la UE, a finales de 2014. Por otro lado, es importante mencionar, que los Estados, en función de la interoperabilidad global, no deberán implementar PACE sin implementar BAC, y los sistemas de inspección deben implementar PACE y utilizarlo solo si es compatible con el chip DVLM de su Estado.

Para mayor detalle, a partir de la versión 1.1[108] de abril de 2014, correspondiente al Informe Técnico de Control de Acceso Suplementario (SAC), de la OACI, se presenta el protocolo de autenticación de chip como una alternativa a la autenticación activa y la integra con PACE, donde el logro de un nuevo protocolo (PACE-CAM), permite la ejecución más rápida y eficaz que ejecutando los protocolos separados.

Mecanismo:	Control de acceso suplementario [SAC: Supplemental Access Control]
Implementación:	Obligatoria solo para la CE a partir de diciembre 2014 y opcional para el resto de los estados miembros.
Pros:	Pace v2, es interoperable con pasaportes Pace v1 (básicamente que soporten BAC), integra diversos mecanismos de seguridad existentes y nuevos, logrando un funcionamiento eficiente por ser más rápido y eficaz, limitando aún más el universo de ataques al chip, previniendo la lectura no autorizada y limitando la escucha de la comunicación.
Contras:	Limita aún más la copia exacta o sustitución del chip, pero no la previene totalmente. Adiciona más complejidad y requiere procesamiento del chip indefectiblemente.
Detalles:	Es un mecanismo muy reciente y solo el tiempo podrá decir si es la solución necesaria al acceso no autorizado a la información contenida.

Tabla 12. Mecanismo de protección: SAC

Legalidad e Implicancias...

La actual exposición de los datos privados contenidos en identificadores digitales, como ser los datos biométricos de identidad, los cuales son de carácter sensibles y privados, implica un problema donde los seres humanos deben ser distinguidos y se deben respetar, dado que los datos personales de un individuo deben ser preservados en todo momento por ser susceptibles de derechos. Entonces, en tanto y en cuanto existe la posibilidad de vulneración de un derecho a la privacidad de una persona, la decisión sobre la implementación de un mecanismo o sistema debería recaer no solo en los responsables del proyecto sino sobre el sujeto soberano de derecho también, donde por alguna extraña razón no ha sido el caso y lo más llamativo es que la implementación a la cual se refiere la presente investigación presenta prácticamente soberanía sobre todo

el planeta tierra, o más precisamente sobre algo más de 90 países alrededor del mundo al día de hoy [Ver Contexto Global].

Volviendo al tema, se puede justificar en un "estado de excepción", pasar por alto ciertas consideraciones razonables a ciertas garantías. Pero, siendo que por definición, el estado de excepción no es permanente sino excepcional, en cualquier proceso bajo condiciones normales, la decisión debería someterse a deliberación pública: es decir, debería pasar por el Congreso de la Nación.

Concretamente, la cruda realidad indica que la gravedad del problema radica en la posibilidad de cometer un delito con la información recolectada, como el robo de identidad[109] [110] (también conocido como suplantación de identidad), la falsificación de documentación[111], ataques contra la intimidad[112] y estafas[113]; siendo la recolección de la misma, realizada sin el consentimiento de su titular. Esto último, es decir, el uso sin autorización, viola el derecho a la privacidad[114] [115] de toda persona, además de poner en riesgo la autonomía de la misma en tanto se le impide tener un control adecuado sobre sus datos personales y sensibles como sus datos biométricos (rostro, iris, huella y demás). Donde su potencial utilización implicaría una cesión de hecho de la información cedida a terceros, quienes la podrían compilar e integrar en bases de datos con fines comerciales e ilícitos.

Particularmente, en Argentina, el derecho a la imagen (captura biométrica de rostro) reconoce protección jurídica mediante distintos instrumentos, entre los cuales está el Art. 31 de la Ley 11.723[116] de Derechos de Autor. Texto que establece como excepción que: "*Es libre la publicación del retrato cuando se relacione con fines científicos, didácticos y en general culturales, o con hechos o acontecimientos de interés público o que se hubieran desarrollado en público*". Por lo cual, en el hipotético caso de no existir tal finalidad determinada por la ley, se estaría incurriendo en un acto no lícito, el cual estaría penado por la ley.

En lo que respecta a la alteración de un documento público[117], referida a la falsificación[111] del mismo, el derecho argentino[118] prevé una pena de prisión de 1 (uno) a 8 (ocho) años, según corresponda, enmarcado dentro del Código Penal[119] [120] bajo el artículo 292, del Capítulo III, referido a Falsificación de documentos en general de la Ley 11.179[103], modificada por la Ley 24.410[121]; texto que indica: "*El que hiciere en todo o en parte un documento falso o adultere uno verdadero, de modo que pueda resultar perjuicio, será reprimido con*

reclusión o prisión de uno a seis años, si se tratare de un instrumento público y con prisión de seis meses a dos años, si se tratare de un instrumento privado. Si el documento falsificado o adulterado fuere de los destinados a acreditar la identidad de las personas, la pena será de tres a ocho años. Están equiparados a los documentos destinados a acreditar la identidad de las personas, aquellos que a tal fin se dieren a las cédulas de identidad expedidas por autoridad pública competente, las libretas cívicas o de enrolamiento y los pasaportes".

Las consecuencias de actos delictivos o ilícitos sobre la captura no autorizada de información personal y sensible de cada portador de un identificador digital, claramente viola el derecho a la privacidad. Con la negación del problema, por parte de los estados, no sería de extrañar que luego se cometan decenas de delitos con la información recolectada.

Si para los estados, el pasaporte electrónico es "infalsificable e inteligente", pero la realidad y los ataques indican y demuestran que no es así, se plantean ciertos interrogantes como: ¿quién nos protege ante los posibles problemas que implica esto? ¿Qué sucede en el caso de ser una víctima de clonación, fraude o robo de identidad? ¿Quién garantiza que nuestros datos personales son realmente privados? ¿Análogamente dudar del pasaporte electrónico, sería como dudar de una prueba de ADN? Por último, ¿quién nos protege de la "no inteligencia" del pasaporte inteligente? Y finalmente, ¿cuándo la ciudadanía va a reaccionar y accionar contra la violación a sus derechos? La verdad, son interrogantes para muchos de los cuales no hay respuestas de momento clarificadoras o que realmente justifiquen su utilización.

Ahora bien, el incremento en el control desmedido sobre la ciudadanía de manera global empieza a impactar sobre los ciudadanos los cuales reaccionan en contra. Tal es el caso de Giorgio Agamben[122], filósofo italiano renunció en 2004 a una posición en la Universidad de Nueva York, al negarse a pasar por los nuevos requisitos biométricos para la visa de este país. Actitud similar a la de Stallman[123], que tuvo probablemente su última visita a la República Argentina según dicen por el fichaje biométrico del sistema SIBIOS[124] [125] [126] [127] [128] [129].

Claro está que existe un horizonte, donde la tecnología se convierte en una herramienta de control[130] para su portador. Donde el verdadero fin, se trata de enmascarar políticamente con otras sutiles vetas que aporta está llegando a

través del perfeccionamiento de una población controlada digitalmente[131], y en su gran mayoría ignorante y poco reactiva; mucho menos proactiva.

Ahora bien, la teoría supuestamente indica que bajo una democracia, el controlado es el gobernante, y el controlador el gobernado, es decir, el pueblo es soberano. Lamentablemente, existe un largo trecho entre la teoría y la práctica, donde muchas veces en situaciones como estas, suele abrirse una brecha y la realidad, es la única que muestra qué tan ajustada está aquella teoría, demostrando como se invierten los roles de cada jugador.

En este punto, es donde el "pasaporte electrónico" y su correspondiente enrolamiento biométrico no desentona con el resto de políticas globales sobre vigilancia y recolección de datos por los gobiernos de la mayor parte del mundo[132]. A pesar de las trágicas experiencias, y no solo de propia historia, la estrategia parece apuntar en una única y muy clara dirección: más control para todos[133], aunque de a poco hay sociedades que comienzan a reaccionar y sus gobiernos deben dar marcha atrás en algunos casos, hasta tanto se consiga un nivel aceptable de seguridad en este tipo de documentos.

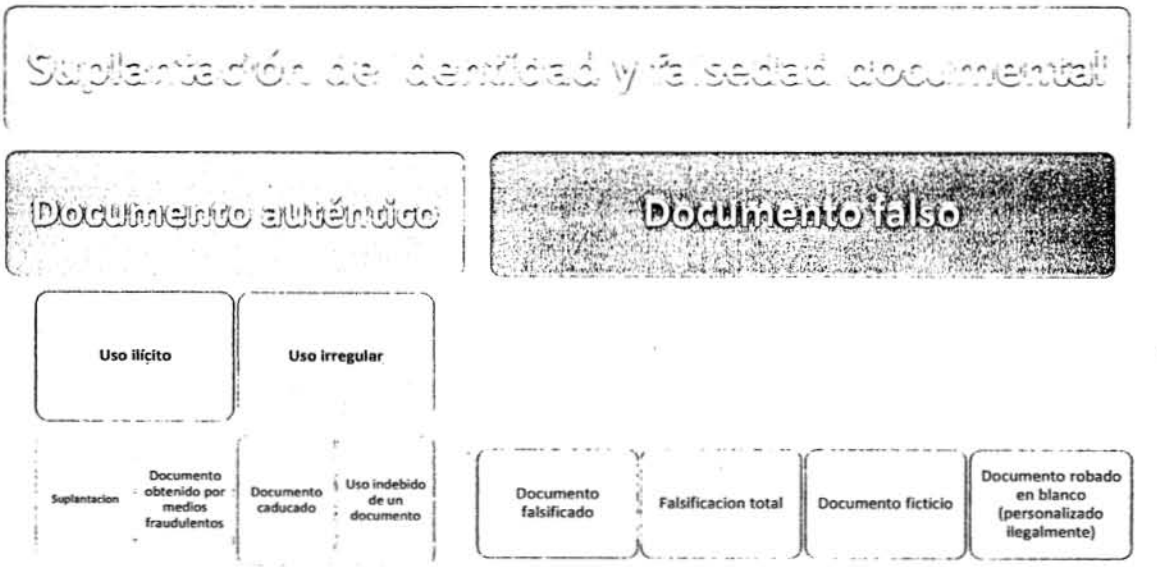
En cuanto a estrategias, en el ámbito nacional, la Secretaría de Transporte, la cual administraba la base de datos de SUBE, paso de la órbita del Ministerio de Infraestructura al Ministerio del Interior[134], el cual maneja los documentos y pasaportes electrónicos[135]. El tema ahora será saber con qué fin cierto se realizó el cambio, centralizando así los identificadores digitales Argentinos en un único ministerio.

Contexto Global

En la mayoría de los países donde se encuentra implementado el pasaporte digital, se cuestionan y se protesta en mayor o menor medida por la falta de información sobre lo que contiene específicamente el chip de este, y su impacto en las libertades civiles de sus ciudadanos, es decir, su impacto directo sobre la privacidad. Dado que como vimos con anterioridad, el problema radica en los datos que se transfieren con su tecnología inalámbrica RF, la que puede convertirse en una gran vulnerabilidad al no estar controlada como hasta el momento. Puesto que como se fue desarrollando a lo largo del presente análisis, cualquier individuo puede obtener información de una persona sin una conexión

física, sino que también puede permitir a cualquier persona con el equipo necesario llevar a cabo la tarea. Por lo tanto, si la información personal no se encuentra ofuscada podría terminar en las manos equivocadas.

Ahora bien, a fin de poder identificar dentro del contexto global y a grandes rasgos la suplantación de identidad y la falsedad documental, se definirán los siguientes conceptos detallados a continuación, según la Comunidad Europea, conjuntamente con Islandia, Noruega y Suiza, de acuerdo a Prado (Public Register of Authentic Identity and Travel Documents OnLine, o Registro Público de Documentos Auténticos de Identidad y de Viaje en Red), organizado por la Secretaria General de la Unión Europea[136]. Los conceptos a detallar, y el cuadro a continuación (ver Cuadro 4), ha sido aprobado por la Red de Análisis del Riesgo de Falsedades Documentales de la Unión Europea (EDF-ARA 2012 Ref. R023) y también es utilizado por Frontex[137] [138] [139]. Para mayor información, ver Anexo: Suplantación de identidad y falsedad documental.



Cuadro 4. Suplantación de identidad y falsedad documental[140]

Jurisprudencia internacional

La jurisprudencia internacional, constituye una fuente primaria de conocimiento en el estudio y comprensión del Derecho Internacional Público,

conjuntamente con las normas convencionales, la doctrina y la práctica; ofreciendo la posibilidad de poner de manifiesto cuál es la práctica generalmente seguida por los Estados, como prueba de una norma general del Derecho Internacional.

Referido esto, podemos mencionar normativa[141] vigente sobre medidas de seguridad y datos biométricos para los pasaportes y documentos de viaje emitidos por los Estados miembros, la cual lleva a plantear cuestiones semejantes a las ya planteadas en anteriores dictámenes, donde el punto siempre es la protección de los datos y la necesidad de procedimientos de recuperación en caso de fallo. Por ello, puntualmente la Unión Europea, ha introducido exenciones por razón de la edad de las personas o de su posibilidad de proporcionar las impresiones dactilares, y también por el intento de adoptar una orientación coherente entre los distintos instrumentos que tratan asuntos similares, como situaciones no contempladas en un primer momento, referidos a niños y personas mayores.

Ahora bien, y por mencionar algunas sentencias[142], referidas a la posesión de documentos falsos con intenciones espurias, en el Reino Unido, contamos con varios casos donde la pena máxima incurre en 10 años, de acuerdo a los agravantes como ser: la naturaleza del documento, intención, cantidad de documentos, ganancia financiera u otros.

Mitigación

La "Declaración de Budapest" [143] [144], un documento votado por unanimidad por un comité de expertos agrupados en FIDIS[145] ("Future of Identity in the Information Society") un consorcio de reconocidas universidades europeas[146], integrado por investigadores en una red de excelencia multidisciplinaria y transnacional deja al descubierto el análisis exhaustivo realizado, dando a conocer las medidas de implementación inmediatas a fin de tratar de reducir los riesgos hasta tanto se diseñe e implemente un nuevo sistema de seguridad integrado, o se re-diseñe el sistema actual. También, en Estados Unidos, otro comité de expertos convocado por la propia Homeland Security[147]

emitió un reporte[148] similar donde advierte los problemas de seguridad y privacidad.

Figura 15. Protector con bloqueador de RFID[149]

Argentina[150] sin dudas puede aportar valor agregado en el registro biométrico masivo de su población, que por costumbre y tradición no cuestiona ni resiste el fichaje como tampoco la toma de datos biométricos. Si nos guiamos por el cuidado que últimamente los organismos del estado han puesto en preservar los datos personales como es el caso de la AFIP[151], o el propio padrón electoral[152] [153], por dar solo algunos pocos ejemplos, la mejor alternativa seria que cada uno trate de resguardar sus datos como mejor le parezca. Para ello a continuación se plantean sugerencias alternativas de protección, las cuales no garantizan un resguardo de la privacidad del 100% pero reducen considerablemente el riesgo.

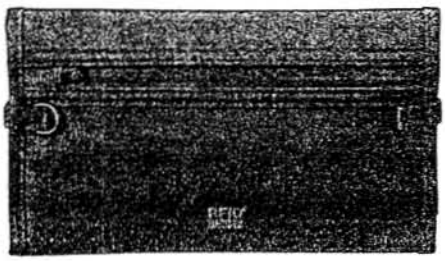


Figura 16. Cartera protectora contra RFID[154]

Recientemente[155], la empresa Betabrand[156], dedicada a la confección y comercialización de indumentaria, ha fabricado unos vaqueros y una chaqueta en colaboración con la conocida empresa Norton[157] que tienen una característica muy especial: en su interior incorpora un material que bloquea señales inalámbricas por lo que protegen a tarjetas o documentos RFID[4] cuya información puede ser sustraída sin que nos demos cuenta[158] [159].

Figura 17. Jean RFID[4] Blocking[160]

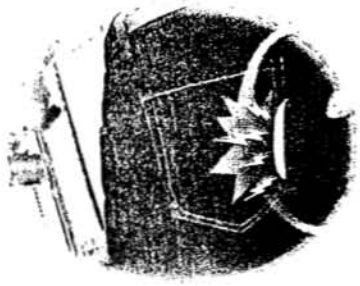


Figura 18. Pocket Blocking[161]

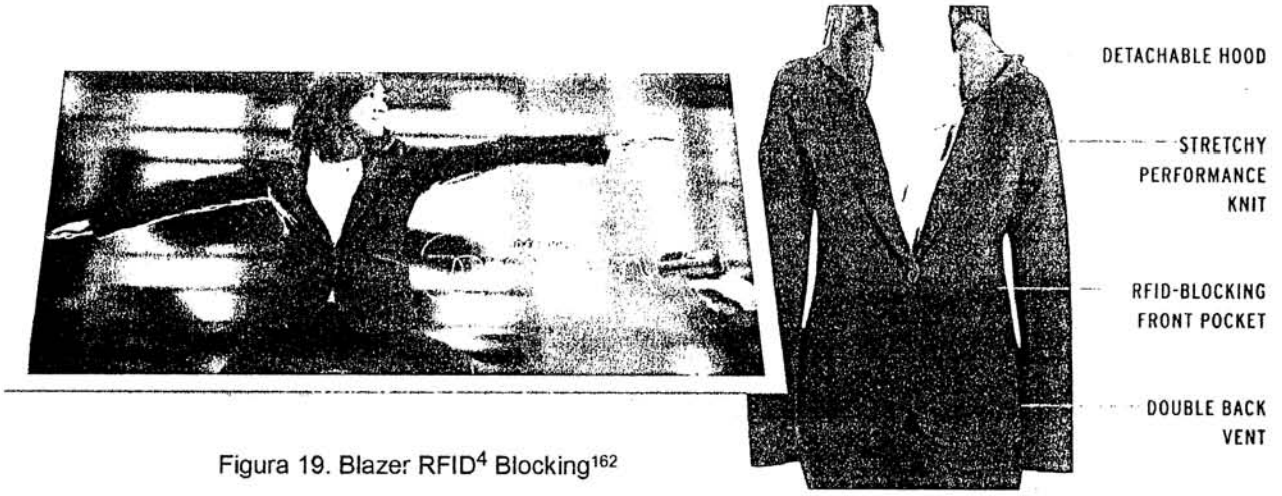


Figura 19. Blazer RFID[4] Blocking[162]

Figura 20. Blazer RFID[4] Blocking[163]

Por otro lado, en el caso de las carteras, fabricantes como Disklabs[164] también ofrecen "mochilas de Faraday" (basadas en el concepto teórico de jaulas de Faraday[165]) que bloquean señales y que por ejemplo usan ciertos cuerpos de seguridad para almacenar teléfonos móviles que decomisan a sospechosos de delitos. Así pues, para lograr tener algo más de tranquilidad a la hora de llevar documentación sensible de este tipo, la indumentaria y accesorios con estos bolsillos reforzados o una buena cartera basada en este tipo de tejido pueden ser una buena alternativa, por no decir la mejor. Para mayor información, ver Anexo: Alternativa ingeniosa pero no 100% efectiva.

Para ampliar algo más la propuesta, y con el reciente descubrimiento de los programas de monitorización masiva de la NSA, últimamente se han provocado muchas suspicacias, y algunos fabricantes tratan de aprovechar esto para promocionar productos que teóricamente nos ayudan a proteger nuestra privacidad. Uno de ellos es el llamado: Blackout Pocket, de la empresa Scottevest[166], un singular bolsillo fabricado con un tejido especial "anti-RFID" que permite protegernos ante el robo de datos de forma inalámbrica y también del seguimiento de nuestros dispositivos móviles.

Figura 21. Blackout Pocket RFID[4] nivel II[167]

El principio de cualquiera de estos productos, es análogo a la famosa jaula de Faraday[165]: el material del que está fabricado el bolsillo protege por ejemplo a nuestro pasaporte electrónico y hace que las antenas del exterior o señales, no puedan llegar o salir del mismo.

Particularmente Scottevest[168] comercializa tres niveles de protección, donde el primero, nos protege de robos de datos vía RFID[4]; el segundo además agrega la protección de señales de redes móviles y de la recepción GPS. Por último, el tercer nivel está solo al alcance de cuerpos de seguridad, agencias gubernamentales y organizaciones especializadas, y curiosamente el fabricante no da más datos sobre un nivel de protección que parece especialmente elevado.

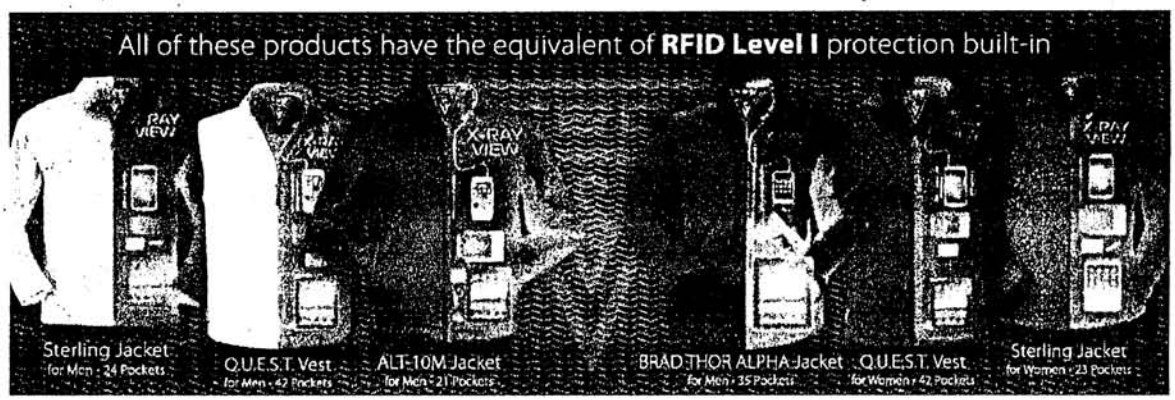


Figura 22. Gama de productos con protección RFID[4] nivel I[169]

Contramedidas...

El principio de la cuestión se relaciona directamente con las características del chip para poder ser leído a distancia, convirtiéndolo esto en su principal inconveniente. Lamentablemente, de igual manera que los dispositivos de lectura de las autoridades correspondientes pueden leer la información contenida en el pasaporte, otros receptores también pueden hacerlo, lo que da lugar a la explotación de la vulnerabilidad, donde la información personal del pasaporte pasa a estar al alcance de cualquier individuo con capacidad de capturar este tipo de información omitiendo la buena fe. En vías de subsanar el inconveniente (emparcharlo más precisamente), los expertos de agencias gubernamentales tuvieron la brillante idea de cubrir el pasaporte con una "Jaula de Faraday" [165], es decir una malla o lámina metálica que impide en teoría que el chip pueda ser leído, a menos por supuesto que el mismo sea abierto. Pero esta protección, sumada a herramientas de encripción, no

resultaron ser demasiado efectivas hasta el momento, dado que: "si tiene un chip RFID[4] es hackeable" [170]. Países como EE.UU. han integrado este tipo de mecanismo como una barrera adicional, la cual no es de implementación obligatoria, y sugiere un aislamiento físico del chip.

Aceptación de uso

Análisis y actualidad

Ante las contundentes vulnerabilidades expuestas anteriormente, el sistema debería haber sido descartado por ser inseguro básicamente. Pero a expensas de ello, se continuó en su utilización y lejos de una solución, dado que en principio no se afronta ni reconoce necesariamente el problema[171] de manera oficial por ninguna administración.

Cuando se empezó a especular con pasaportes RFID[4], durante la administración de George Bush[172], los expertos advirtieron las implicancias y riesgos a la seguridad y amenazas a la privacidad. Bruce Schneier[173], uno de los principales referentes en el campo de la seguridad y la criptografía escribió en 2004: "*... los viajeros que lleven pasaportes con RFID[4] estarán transmitiendo su identidad. Piensen por un minuto lo que esto significa. Sus pasaportes irán transmitiendo continuamente su nombre, nacionalidad, edad, dirección y cualquier cosa que esté en el chip RFID. Esto significa que cualquier persona con un lector puede aprender esa información, sin el conocimiento o el consentimiento del titular del pasaporte. ... Es una clara amenaza a la intimidad y la seguridad personal...*" [174].

Ahora bien, incluyendo que la mayoría de los pasaportes actualmente incluyen más datos biométricos sensibles, como la huella digital y el rostro de forma obligatoria según la norma de especificación 9303[6], y opcionalmente puede incluir demás datos biométricos como ser iris; esto compromete directamente la identidad e integridad de su portador, quedando a las buenas de su acechador el uso que le dé a los datos capturados potencialmente hablando.

Por lo cual, la implementación por parte de los gobiernos de una fallida e inadecuada arquitectura de seguridad, han forzado a los ciudadanos a adoptar nuevos pasaportes legibles por maquinas (DVLM), que disminuyen dramáticamente la seguridad y la privacidad, y aumentan el riesgo del robo de

identidad. En pocas palabras, la implementación actual del pasaporte biométrico utiliza tecnologías y estándares que no están concebidos para su propósito.

Por otro lado, el especialista alemán Luks Grunwald[88], expuso en 2006 la vulnerabilidad del sistema clonando un pasaporte, donde le siguió Kevin Mahaffey[102] desde Los Ángeles mostrando un video[175] sobre cómo el pasaporte podía ser leído inclusive estando apenas entreabierto, y el especialista Adam Laurie que clonó un pasaporte británico en una demo para Daily Mail[84]. Como se puede ver, varios son los casos a los que le siguieron hasta el hartazgo las vulnerabilidades de esta tecnología [Ver Análisis de factibilidad de la explotación real de debilidades: Riesgos y Ataques], muchas veces antes de implementarse: donde la premisa básica es que los pasaportes son crackeados[176] por especialistas y en muchos casos, antes de comenzar a emitirse por lo cual su implementación no corresponde a la lógica sino que está supeditada a otros factores. Por lo que el debate trasciende el ámbito de la seguridad, llegando a varios medios masivos, como The Guardian[177], The Washington Post[178] y El Mundo[179], entre otros; los cuales se hicieron eco del problema aumentando su exposición mediante la publicación de artículos críticos[180], y convocando a especialistas para que realizaran demostraciones sobre las vulnerabilidades, como se comentó anteriormente.

Argentina

En los tiempos en que vivimos y no solo en la República Argentina, la clase política es vulnerable a dejarse llevar, por la inexperiencia de implementaciones a nivel mundial y más particularmente por no tener competencia sobre el caso (falta de capacidad). Por lo que la picardía de agregar inteligencia al nuevo pasaporte argentino, puede que nos conduzca a un camino sin retorno, en el cual se aumenta la vigilancia[181] sobre el individuo sin controlar su portación intransferible atacada por el robo de identidad; donde hubiese sido correcto dudar y debatir el tema como corresponde.

Argentina estuvo a tiempo de aprovechar toda la experiencia mundial de los últimos años, analizando los problemas relativos a la privacidad, y las vulnerabilidades comprobadas de seguridad, para su correspondiente rediseño o en su defecto su rechazo, donde al fin y al cabo se terminó por copiar una no tan buena idea. El anuncio[182] oficial fue realizado por el Ministro del Interior,

donde entre otras cosas afirmo lo siguiente en conferencia de prensa: "*La validación de la identidad de la persona se hace mediante dos vías, mediante el escaneo del mismo, y a partir de la identificación de los datos biométricos y biográficos de una persona, que aparecen en una pantalla, y que están encriptados en el chip, lo que hace que este pasaporte sea inviolable. ...esto tiene que quedar en claro, es un pasaporte absolutamente seguro...*" [24].

Aparentemente la actualización del pasaporte, tiene su objetivo en cumplir con los estándares fijados por el "Visa Waiver Program"[183] [184], el cual abre la posibilidad de entrar a los EE.UU. sin tramitar visa, siendo en la región Chile[185] [186] [187] el único país habilitado a tal fin hasta el momento.

Contexto mundial

Allá por 1998, Malasia introdujo por primera vez el pasaporte electrónico en el mundo; el cual contenía texto, una foto y una huella digital. Todo se almacenaba en un único archivo de datos en un chip electrónico de 8 kB.

En la actualidad más de 90 países ya incorporaron en sus pasaportes un chip RFID[4], lo que da un estimado de 500 millones de pasaportes electrónicos en circulación[188]. Si bien esta cifra es aun relativamente baja en comparación con la cifra aproximada de 125 millones de pasaportes tradicionales que se emiten en todo el mundo cada año, los pasaportes electrónicos son el futuro de los documentos de identidad de viajes.

Esto es demasiada información dando vueltas por el mundo y la seguridad de los mismos está supeditada a la OACI[7] [8], en conjunto con los estados miembros, que lo tienen muy en cuenta, y continuamente organizan seminarios para revisar y discutir sobre estos temas.

Se evidencia un claro interés en que todos los países adopten este sistema, y parece que el tiempo apremia, dado que cada vez son más los estados que lo adoptan.

Constantemente se trabaja en mejorar la seguridad digital, y en el diseño de los documentos. No es casual que algunos pasaportes tengan por ejemplo un recubrimiento metálico en las tapas para protegerlo de las ondas de radiofrecuencia (la conocida Jaula de Faraday[165]) para impedir acceder a la información si el pasaporte está cerrado. También en algunos casos, dependiendo del país emisor, se ha instalado el chip en la página de datos

personales o agregado una página central especialmente para contener el chip. Mantener la seguridad es un trabajo difícil ya que teniendo en cuenta que los pasaportes en su gran mayoría tienen una duración promedio de entre 5 y 10 años, donde en este universo conviven varios tipos de seguridad, siendo algunos más vulnerables que otros.

Para cualquier estado, la implementación de un programa como este, requiere una importante inversión para aprovechar todas las ventajas de la verificación de identidad biométrica.

Todos los pasaportes electrónicos deben llevar una copia del certificado PKI[5] del emisor, pero estos certificados también se intercambian entre los países participantes, junto con las listas de revocación, enumerando los certificados que ya no son válidos. Este proceso de cambio, que debe ser digno de confianza, es un elemento esencial de la infraestructura de los sistemas de pasaporte electrónico.

Gestión de las relaciones individuales para obtener esta información de todos los otros países que emiten es una tarea compleja. Para facilitar el creciente número de pasaportes electrónicos, la OACI[7] [8] ha establecido un intercambio global llamado Directorio de Clave Pública (PKD) para ayudar a las autoridades de control fronterizo a gestionar el proceso de forma rápida y eficaz. El DCP OACI[7] [8] actúa como un intermediario central para gestionar el intercambio de certificados y listas de revocación de certificados entre los países. Los estados participantes depositan los datos que otros estados necesitan con el fin de asegurarse de que sus pasaportes electrónicos son auténticos. Es importante destacar que el DCP de la OACI[7] [8] sólo contiene información que confirma si la firma en el pasaporte electrónico es auténtico y que los datos no han sido manipulados.

Figura 23. Logo del Directorio de Clave Publica

Sin el DCP, cada país debe intercambiar la información pertinente de manera bilateral; por ejemplo, el intercambio de información entre sólo ocho países requiere 56 intercambios bilaterales. El DCP OACI[7] [8] reduce este número a sólo dos intercambios cuando un país deposita su información, y cuando recibe datos con respecto a todos los demás miembros.

Sorprendentemente, a pesar del creciente número de pasaportes electrónicos, sólo 37 países son actualmente los abonados al DCP de la OACI[7] [8]. Los países que utilizan el sistema son los emisores de tres cuartas partes de todos los pasaportes electrónicos en circulación y para ellos está demostrando ser una herramienta de gestión eficaz para sus agencias de expedición de pasaportes, lo que les permite compartir su información basada en certificados en previsión de su uso en otros lugares.

Para lograr una interoperabilidad de los pasaportes electrónicos a escala global, todo el mundo tiene que estar moviéndose en la misma dirección, y lamentablemente ese no es el escenario actual. Aunque los EE.UU. y Europa están liderando el camino en términos de emisión de pasaportes electrónicos, y países como África, América Central y América del Sur aún tienen que comprometerse con la nueva la tecnología; pero especialmente en el mundo del sub desarrollo, que enfrenta una serie de desafíos diferentes, incluyendo guerras civiles, desplazamientos de la población, la sequía, el hambre, la falta de salud y la escasez de agua, la búsqueda de inversiones en nuevas tecnologías de identidad no es una prioridad.

Entonces, un elemento importante en la validación del pasaporte electrónico, el DCP de la OACI[7] [8] está ayudando a mejorar la seguridad fronteriza y los viajes internacionales, permitiendo a la interoperabilidad mundial, estar un paso más cerca; pero para llegar a la etapa en que todos los beneficios están siendo cosechados en todo el mundo, esto demandara mucho tiempo.

A continuación, se detallan los estados que incorporaron la tecnología biométrica en sus pasaportes y demás datos recopilados, de manera informativa[189] [190]:

#	Estado	Desde...	Costo estimado	Validez
1	Albania	5/2009	€ 50	**10** años
2	Alemania	11/2005	€ 59 / 38	**10** / 6 años
3	Arabia Saudita	6/2006	-	-
4	Argentina	6/2012	€ 36	**10** años
5	Armenia	7/2012	-	**10** años
6	Australia	10/2005	-	**10** / 5 años
7	Austria	7/2006	€ 76 / 30 / Free	**10** / 5 / 2 años
8	Azerbaiyán	9/2013	-	-
9	Bélgica	10/2004	€ 71 / 41	5 años
10	Bolivia	-	-	5 años

11	Bosnia y Herzegovina	10/2009	€ 21	5 años
12	Brasil	12/2006	€ 80	5 años
13	Brunei	2/2007	-	-
14	Bulgaria	3/2010	€ 20 / 10	5 años
15	Canadá	7/2013	-	-
16	Chile	9/2013	-	-
17	Chipre	12/2010	€ 70	**10** años
18	Colombia	-	-	5 años
19	Corea del Sur	8/2008	€ 43	**10** años
20	Croacia	7/2009	€ 53	**10** / 5 años
21	Dinamarca	8/2006	-	**10** / 5 años
22	Egipto	2/2007	-	-
23	Emiratos Árabes Unidos	2011	-	-
24	Eslovaquia	1/2008	€ 34 / 29 / 27	**10** / 5 / 2 años
25	Eslovenia	8/2006	€ 42 / 36 / 32	**10** / 5 / 3 años
26	España	8/2006	€ 25	**10** / 5 años
27	Estados Unidos	10/2004	-	-
28	Estonia	5/2007	€ 29	5 años
29	Filipinas	8/2009	-	-
30	Finlandia	8/2006	€ 48 / 65	5 años
31	Francia	4/2006	€ 89 / 86 / 42 / 17	**10** / 5 años
32	Ghana	1/2014	-	-
33	Grecia	8/2006	€ 85 / 74	5 / 2 años
34	Guatemala	-	-	5 años
35	Honduras	-	-	5 años
36	Hong Kong	2/2007	-	-
37	Hungría	8/2006	€ 49 / 26	**10** / 5 años
38	India	6/2008	-	-
39	Indonesia	1/2011	€ 52 / 32	5 años
40	Irak	4/2009	€ 16	-
41	Irán	7/2007	€ 29	-
42	Irlanda	10 / 2006	€ 80 / 27 / 16 / free	**10** / 5 / 3 años
43	Islandia	5/2006	-	-
44	Israel	7/2013	-	2 años
45	Italia	10/2006	€ 116	**10** / 5 / 3 años
46	Japón	3/2006	-	-
47	Kosovo	5/2011	-	-
48	Letonia	11/2007	€ 22	**10** / 5 / 2 años
49	Lituania	8/2006	€ 48 / 24	**10** / 5 / 2 años
50	Luxemburgo	8/2006	€ 30 / 20	5 / 2 años
51	Macao	9/2009	-	-
52	Macedonia	4/2007	€ 22	-
53	Malasia	1998	-	-
54	Maldivas	7/2006	-	-
55	Malta	10/2008	€ 70 / 35	**10** / 5 años
56	Marruecos	2008	€ 27	-

57	Mauritania	5/2011	€ 90	5 años
58	México	-	-	5 años
59	Moldavia	1/2008	€ 45	7 / 4 años
60	Montenegro	2008	€ 40	-
61	Nicaragua	-	-	5 años
62	Nigeria	2007	-	-
63	Noruega	2005	€ 50	-
64	Nueva Zelanda	11/2005	-	-
65	Países Bajos	8/2006	€ 85 / 67	**10** / 5 años
66	Pakistán	2004	-	-
67	Panamá	-	-	5 años
68	Paraguay	-	-	5 años
69	Perú	-	-	5 años
70	Polonia	8/2006	€ 106 / 36	**10** / 5 años
71	Portugal	7/2006	€ 65	5 / 2 años
72	Qatar	4/2008	-	-
73	Reino Unido	3/2006	€ 205 / 170 / 108	**10** / 5 años
74	Republica Checa	9/2006	-	**10** / 5 años
75	República Dominicana	5/2004	-	-
76	República Gabonesa	1/2014	-	-
77	República Popular de China	1/2011	-	-
78	Rumania	12/2008	€ 59 / 25	5 / 3 / 1 años
79	Rusia	2006	€ 70	-
80	Serbia	7/2008	€ 32	**10** / 5 / 3 años
81	Singapur	8/2006	-	-
82	Somalia	10/2006	€ 78	-
83	Sudán	5/2009	€ 78	7 / 5 años
84	Sudán del Sur	1/2012	-	5 años
85	Suecia	10/2005	-	5 años
86	Suiza	9/2006	-	5 años
87	Tailandia	5/2005	-	-
88	Taiwán	12/2008	-	**10** / 5 / 3 años
89	Tayikistán	2/2010	-	-
90	Togo	8/2009	-	-
91	Túnez	2017	-	-
92	Turkmenistán	7/2010	-	-
93	Turquía	6/2010	-	**10** años
94	Ucrania	1/2013	-	-
95	Uruguay	-	-	5 años
96	Uzbekistán	6/2009	-	-
97	Venezuela	7/2007	-	-

Tabla 13. Información general de los estados que incorporan pasaporte biométrico

Luego de haber detallado los orígenes de implementación del pasaporte electrónico a nivel mundial, a continuación se enumeran algunos de los Estados que no fueron nativos OACI[7] [8] y / o que aún no lo son también:

#	Estado	Desde...	OACI
1	Ghana	-	No
2	Hong Kong	2008	Si
3	Malasia	2/2010	Si
4	Pakistán	2012	Si
5	República Dominicana	-	No
6	República Gabonesa	-	No
7	Tailandia	8/2005	Si

Tabla 14. Detalle de estados no nativos OACI[7] [8]

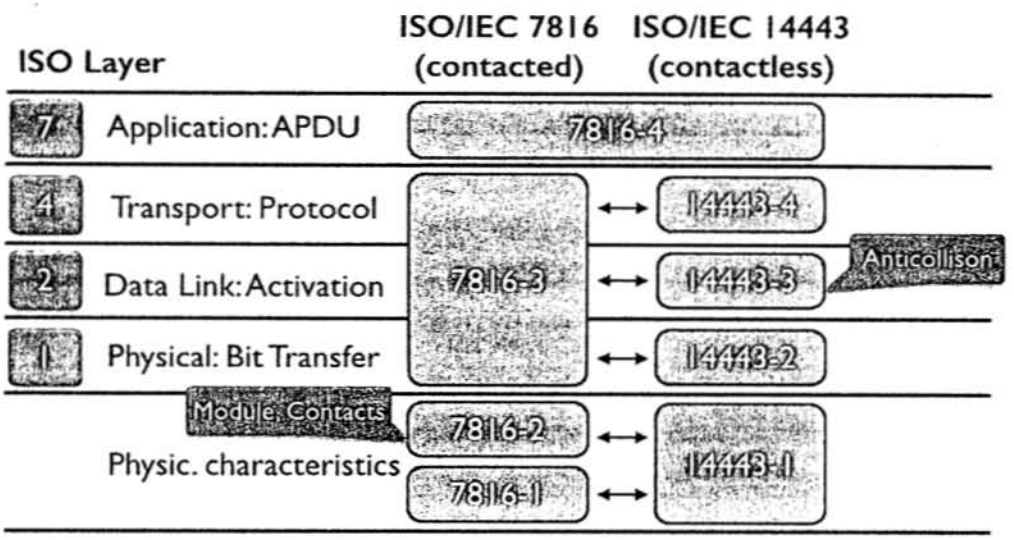
Futuro e Interoperabilidad

El futuro de la identidad en la Sociedad de la Información (FIDIS[191]); por medio de una investigación realizada por un equipo de la red de expertos en seguridad del EIS: del inglés European Information Society, y financiados por la Unión Europea, se han manifestado en contra del régimen de pasaporte electrónico, puesto que los mismos disminuyen dramáticamente la seguridad y aumentan el riesgo de robo de identidad.

La mayoría de las medidas de seguridad están diseñadas contra los ciudadanos y no son de confianza; sin tener en cuenta los peligros a los que se enfrenta al momento de ser verificado, por estados no confiables, como las organizaciones no gubernamentales corruptas, o que utilizan una mala implementación de sus sistemas electrónicos, no seguros[192]. Por lo que nuevas soluciones criptográficas se están proponiendo para mitigar las amenazas de robo masivo de identidad, las cuales son objeto de estudio científico, pero no se han aplicado todavía en la mayoría de los pasaportes biométricos.

Por lo general, esta tecnología se basa en estándares y normas internacionales. Por lo cual, este identificador digital particular, es decir, el pasaporte electrónico, en un futuro cercano, incorporara un mecanismo complementario de seguridad, conocido como el Control de Acceso Suplementario (SAC: del inglés Supplemental Access Control) o Establecimiento de conexión autenticada por contraseña (PACE: del inglés Password

Authenticated Connection Establishment), basado en las normas internacionales ISO. Por ello, a continuación la siguiente figura muestra las normas análogas pertinentes de la ISO para tarjetas inteligentes con y sin contacto:



Cuadro 5. Normas de tarjetas inteligentes análogamente interoperables con y sin contacto en el modelo de capas ISO[193]

La OACI[7] [8] ha publicado una actualización; la versión 2.06[194] con aclaraciones de su informe técnico del protocolo de transmisión de radiofrecuencia, centradas en pruebas de conformidad y pruebas de protocolo para los pasaportes electrónicos de aplicación de protocolos BAC[67] y SAC, correspondientes a la versión uno del PACE (PACE v1).

Es por ello que la interoperabilidad del pasaporte electrónico es necesaria a fin de verificar si la próxima generación de sus tarjetas inteligentes en los pasaportes electrónicos con el nuevo protocolo de Control de Acceso Complementario (SAC) como un reemplazo del mecanismo de Control de Acceso Básico[67] (BAC), el cual fue diseñado en el comienzo de este siglo y será reemplazado por SAC en diciembre 2014 en algunas regiones. Donde SAC, especifica el tipo de protocolo PACE que se utilizara para autenticar el acceso. PACE, fue desarrollado principalmente por BSI[195] y también se utiliza en las tarjetas de identificación alemanas emitidas desde noviembre de 2010: TR-03110[196].

Durante el Seminario Regional[197] de la OACI[7] [8] sobre documentos de viaje de lectura mecánica en Madrid del pasado 25 al 27 de junio de 2014, se realizó

una prueba de interoperabilidad para los pasaportes electrónicos con control de acceso Complementario (SAC). Este protocolo, está reemplazando el BAC[67], que se utiliza en los pasaportes electrónicos y será obligatoria en la UE a partir de diciembre de 2014. SAC es el mecanismo propuesto para asegurar que sólo las personas autorizadas pueden leer de forma inalámbrica información del chip RFID[4] de un pasaporte electrónico. SAC también se conoce como PACE v2; mientras que PACE v1 se utiliza como un protocolo básico en la tarjeta de identificación alemana. Para mayor información, ver Anexo: Prueba de interoperabilidad.

Conclusiones

Los chips RFID[4] presentan un problema inherente: el llevar información sensible en un formato vulnerable. Más aun, implementando e integrando esta tecnología en algo tan sensible como son los identificadores digitales, pero de validez documental; es decir al ser utilizado como documento electrónico para la identificación de un individuo, según sea el caso. Por lo cual el portador de un identificador digital, lleva consigo la exposición de datos sensibles dentro del entorno transitado, siendo el medio propiamente dicho inseguro dadas las condiciones expuestas. Lo que queda a criterio de interpretación personal, es si el diseño fue realizado adrede para forzar la exposición de los datos al dominio público o no, puesto que da que pensar que los gobiernos de varios estados, permiten la exposición colaborativa de los datos de sus ciudadanos a expensas de la invasión de su privacidad y lo que esto implica y conlleva.

Por lo cual, se plantean ciertos interrogantes como por ejemplo: ¿Qué sentido tiene la incorporación de este chip, si agrega un problema en vez de una solución, y si necesita realmente ser bloqueado o encriptado? ¿Cuál es la ventaja de introducir información electrónica dudosa? Esto, equivale a volver a escribir los datos del pasaporte en otra página, pero en vez de usar tinta ¡usando un lápiz que se puede modificar! Entonces, ¿si los datos electrónicos son menos confiables, qué seguridad extra aportan? Por último, ¿si sólo pueden leerse cuando el pasaporte está abierto, por qué no usar los datos impresos y listo?

Claro está, que esta tecnología necesita evolucionar para llegar a un nivel aceptable de seguridad y confianza; dado que la actualidad de este identificador digital genera muchas dudas. Particularmente, refiriéndome a la República Argentina, esta adopta el pasaporte electrónico en 2012 justificando en aquel momento, que son 56 países en el mundo los que ya utilizan biometría en el control de sus fronteras y cada día se suman más a esta exigencia para habilitar la exención de visados para el ingreso así como por el uso de sistemas automáticos de control fronterizo. No obstante lo anterior, los avances tecnológicos y la modernización en materia de técnicas de personalización, incorporación y encriptación de datos biométricos han significado un salto de calidad y seguridad en lo que hace a la emisión de Pasaportes Electrónicos o biométricos en el mundo, teniendo como resultado el establecimiento de nuevos estándares y requerimientos por parte de Organismos Internacionales expertos.

El problema central de este tipo de implementaciones, es la privacidad, desde la perspectiva social. Dado que: "la seguridad de la identidad solo es viable si se acompaña de las correctas políticas que garanticen el correcto uso de las mismas en el marco de los derechos humanos y resguardando la privacidad de los datos que estos sistemas resguardan" [198].

La biometría, como tantas herramientas, depende de cómo se implemente y utilice. Por lo cual la preocupación sobre la privacidad de los datos es uno de los mayores objetivos y preocupaciones. En este punto, podemos observar decenas de documentos, estándares y buenas prácticas de cómo recolectar la información biométrica, procesarla, almacenarla y verificarla. Métodos de protección de las comunicaciones, así como de portabilidad de las mismas a través de diferentes identificadores digitales. Pero lo que quizás más preocupa aun, es la falta de transparencia, donde no se le informa a la persona a la cual se le recogen estos datos, que información le será requerida, y menos aún, el método, el almacenamiento y su seguridad, permitiendo esto lograr una audibilidad a futuro. Puesto que cumpliendo mínimamente con estos aspectos, y con la correspondiente campaña de difusión, el ciudadano ya estará mucho más seguro de que la utilización de estas herramientas por parte de los diferentes estados, le otorgan la seguridad necesaria para respaldar su única e irrepetible identidad, y con ello, sus derechos básicamente.

Por lo tanto, garantizar la privacidad, y transparencia a través de la apertura tecnológica, son claves y puntos centrales, dado que nos permite conocer, entender y brindar mayor información de cómo son tratados nuestros datos, y así entender cómo esta herramienta sumada a las demás tecnologías, pueden agilizar muchos trámites, y fundamentalmente, darnos mayor confianza.

Ahora bien, avocándonos a cuestiones de seguridad y puntualmente al problema de la privacidad, podemos remarcar que en contraste con los documentos de identidad tradicionales, los datos pueden ser accedidos de forma remota, transparente e interactivamente desde distancias de hasta 10 metros. Esto se ve agravado por las vulnerabilidades de control de acceso, las cuales son susceptibles al riesgo de ubicación, donde la autenticación de los datos por terceros autorizados y no autorizados, permite el seguimiento de las personas, por ejemplo cuando residan como turista en un país extranjero. Por lo que el uso

de datos biométricos es explotable por sectores público y privado con propósitos particulares, como una violación de los principios de privacidad de su portador.

Específicamente, los mecanismos de seguridad actuales de estos identificadores, cubren sólo partes de un concepto como la seguridad. BAC[67] fue presentado originalmente como una solución eficaz de control de acceso, mientras que más recientemente EAC[69] se ha presentado como una versión mejorada. Sin embargo, ambos son simplemente insuficiente, para el control de acceso para el usuario, en infinidad de situaciones. Por esto y reactivamente de forma mitigante, recientemente se está en proceso de suplantación de estos mecanismos por uno nuevo denominado SAC, actualizando sus soportes a PACE v2 respectivamente con el único fin de agregar un parche y acotar el universo de seguridad, el cual aún sigue siendo amplio. Es importante mencionar, que en los países no europeos sólo se encuentra implementado el BAC[67] con un nivel de seguridad significativamente más bajo, y actualmente solo la UE, obligatoriamente desde este diciembre último implementa SAC.

Una serie de amenazas teóricas, científicamente demostradas y debilidades conceptuales han sido publicadas y detalladas. Las cuales hasta ahora, no han sido cubiertas por perfiles de protección, directrices y normas técnicas o implementaciones existentes. Donde lo más significativo es:

- La biometría en los DVLM actualmente no puede ser revocada, puesto que las características biométricas de los usuarios, no se pueden cambiar fácilmente, por lo que los datos biométricos "robados" pueden ser objeto de abuso por un largo período de tiempo.
- La gestión de claves es insuficiente con BAC[67].
- Es factible, el espionaje de la comunicación realizada entre la etiqueta RFID[4] y el lector, utilizando debilidades criptográficas documentadas para descubrir datos, lo que es cada vez más frecuente hoy día[199].
- Clonación de identificadores RFID[76].
- El abuso de la lectura a distancia de los identificadores RFID[4].

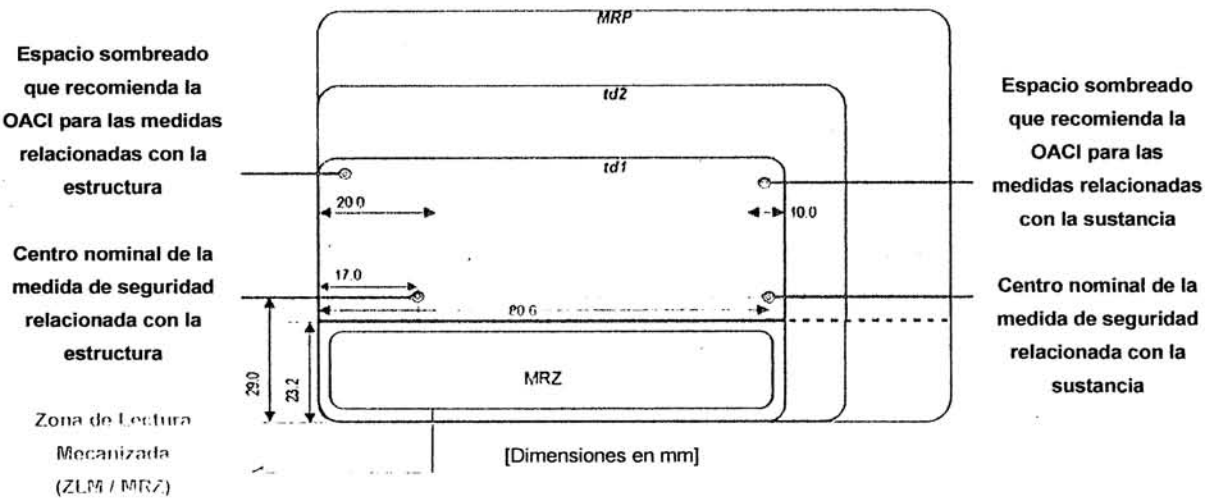
La combinación de estas amenazas y debilidades pone la seguridad y privacidad de sus portadores en significativo riesgo, especialmente cuando se considera el uso disperso geográficamente y larga vida útil de estos, en la que puede llegar a tener una validez de hasta diez años, lo cual aumenta potencialmente aún más su riesgo.

Anexo

El presente anexo tiene como finalidad, explicar y ampliar según corresponda, los términos técnicos y específicos que se usan en la presente investigación, como así también fomentar su uso razonable y correcto, aplicando la terminología específica para lograr una comprensión clara y eficaz.

Medidas de seguridad verificables por medios mecánicos

Las medidas de seguridad verificables por medios mecánicos de un documento son medidas de seguridad que pueden ser leídas y verificadas por una máquina (lectores de documentos), y que permiten autenticar un documento de viaje o de identidad mediante la detección o medición de determinadas propiedades físicas de elementos o estructuras del documento, a la vez que ayudan a comprobar la identidad del titular del documento.



Cuadro 6. Hoja genérica de datos[200]

Lectura Mecanizada - MRTD = DVLM / MRZ = ZLM

Las especificaciones de los documentos de viaje de lectura mecanizada según la OACI[7] [8] aplican para el cruce de fronteras. De acuerdo con estas normas, la página de datos personales de un documento de viaje de lectura mecanizada se divide en dos zonas distintas:

- Una Zona de Inspección Visual (ZIV), que contiene la denominación del documento, la fotografía del titular, datos personales y datos sobre la expedición y la validez.
- Una Zona de Lectura Mecanizada (ZLM), que incluye parte de la información de la zona de inspección visual.

La ZLM, incluye parte de la información de la ZIV en forma de una secuencia de caracteres alfanuméricos y el símbolo "<" dispuestos en dos o tres líneas. Esta secuencia de caracteres se lee con un lector de documentos para facilitar las inspecciones de los documentos de viaje (OCR).

Formato de la zona de lectura mecanizada:

- Formato ID1/td1: 86 (85,6) x 54 (53,98) mm. Tres líneas de 30 caracteres cada una, situadas en el reverso del documento.
- Formato ID2/td2: 105 x 74 mm. Dos líneas de 36 caracteres cada una, situadas en la parte inferior de la página de datos personales o visado.
- Formato ID3/td3: PLM 125 x 88 mm. Dos líneas de 44 caracteres cada una, situadas en la parte inferior de la página de datos personales.

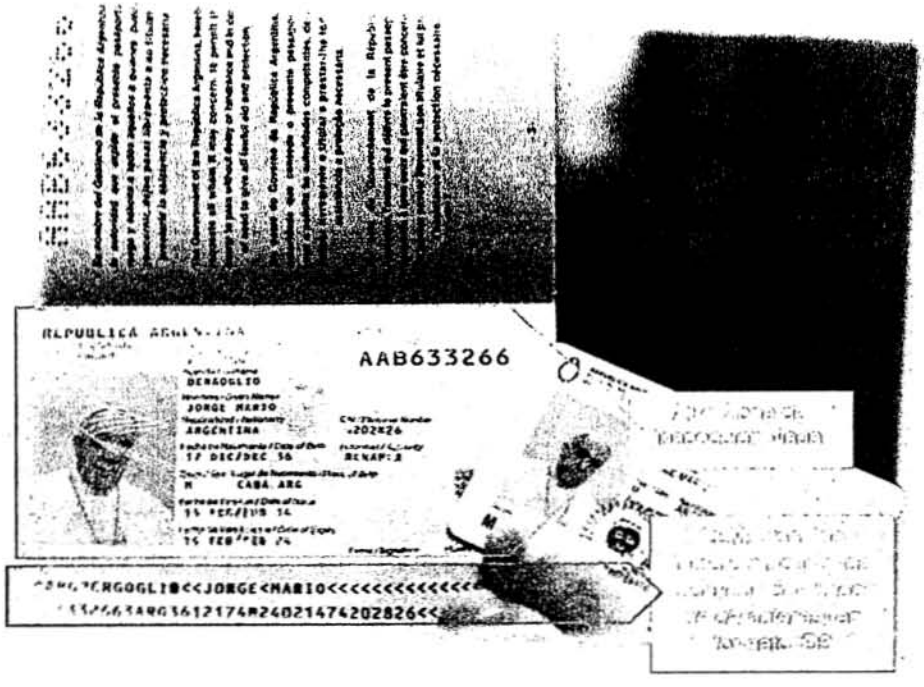


Figura 24. Ejemplo de hoja de datos del PLM del Papa[201]

Tecnología Aplicada

Definiciones

RFID[4] es la sigla de "Radio Frequency IDentification", que en castellano se traduce como "Identificación por Radiofrecuencia".

Figura 25. Ilustración genérica de Chip RFID[202]

Es básicamente un sistema de almacenamiento y recuperación de datos remotos, que puede utilizar dispositivos denominados etiquetas, tarjetas y transponders. Su propósito fundamental es transmitir la identidad de un objeto (similar a un número único de serie) mediante ondas de radio. Estas tecnologías se agrupan dentro de las denominadas Auto ID[203] (Automatic IDentification en inglés, o identificación automática). Las etiquetas RFID[4] (RFID Tag) (Ver Figura 25) son dispositivos pequeños, similares a una pegatina, que pueden ser adheridas o incorporadas a un producto, un animal o una persona. Contienen antenas para permitir recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID[4].

Existen dos tipos de etiquetas, las cuales pueden ser pasivas, y son las que no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren. Una de las ventajas del uso de radiofrecuencia (en lugar, por ejemplo, de usar infrarrojos) es que no se requiere visión directa entre el emisor y el receptor.

Evolución y Funcionamiento

Es una tecnología que data de antes de la segunda guerra mundial[3] [204], producto de una convergencia entre dos inventos: el radar y la transmisión radiofónica.

La patente[205] que corresponde al RFID[4] pasivo tal como lo conocemos hoy, corresponde a Charles Walton[206] y se le otorgó en 1983. Ya en los años 50 y 60, se desarrollaron los primeros sistemas RFID[207] utilizados en instalaciones militares.

Figura 26. Caravanas RFID[208]

Una de sus primeras aplicaciones civiles, a partir de su comercialización en la década del ochenta, fue el etiquetado de animales (Ver Figura 26) y mercaderías. La realidad indica que tecnología que en un comienzo se usaba para identificar y controlar aviones (Ver Figura 27), camiones, productos y luego ganado a grandes rasgos, en la actualidad se la utiliza análogamente, con seres humanos.

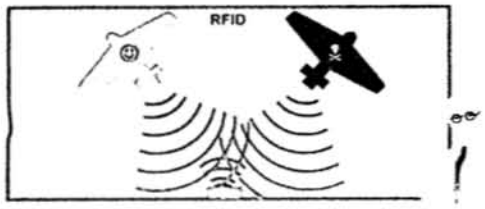


Figura 27. Sistema de identificación de avión amigo o enemigo utilizado en la segunda guerra mundial[209]

Los chips RFID[4], han evolucionado en el tiempo (Ver Figura 28); y funcionan (Ver Figura 29) a grandes rasgos de la siguiente manera: son excitados por una onda de radiofrecuencia, a la cual "responden" emitiendo (con diferente alcance según sea el tipo de RFID[4]) la información que contienen, generalmente un número de identificación. Es decir, con un dispositivo especial (que en la actualidad es de bajo costo) y donde se detecta la presencia de un objeto con un chip RFID[4] en el entorno, se puede obtener la información que contiene el mismo.

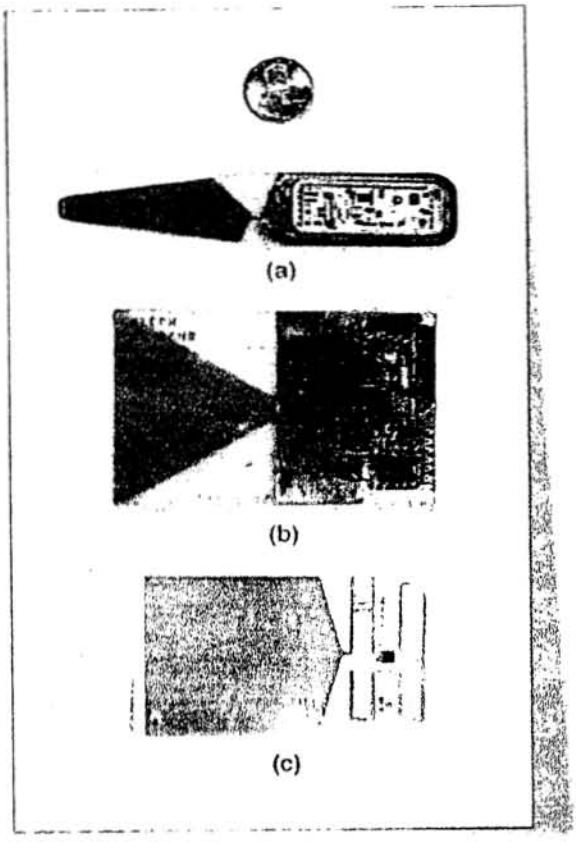


Figura 28. TAGs RFID[4] en evolución con el paso del tiempo. Imagen (a) de 12 bytes en 1976, Imagen (b) de 128b en 1987 e imagen (c) de 1024b en 1999; donde disminuye el tamaño del chip con relación a la etiqueta[210]

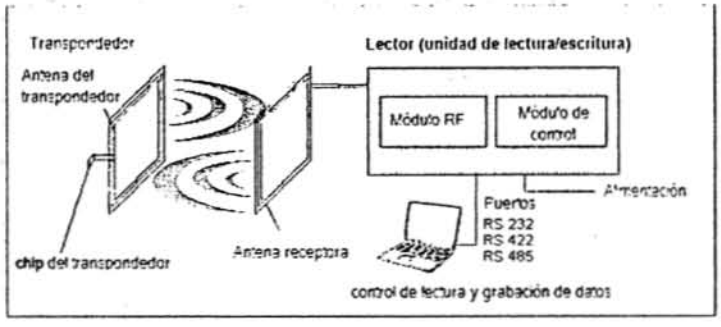


Figura 29. Diagrama de funcionamiento RFID[4] general[211]

Pasaporte Electrónico

Patentes

Las patentes de documentos de identificación inteligente o pasaporte inteligente, describen un sistema de implementación para estos. Además muestran ilustrativamente la incrustación que incluye los componentes de seguridad física necesarios para tal fin, y que pueden ser insertos en cualquier pasaporte estándar, convirtiéndolo en un pasaporte inteligente.

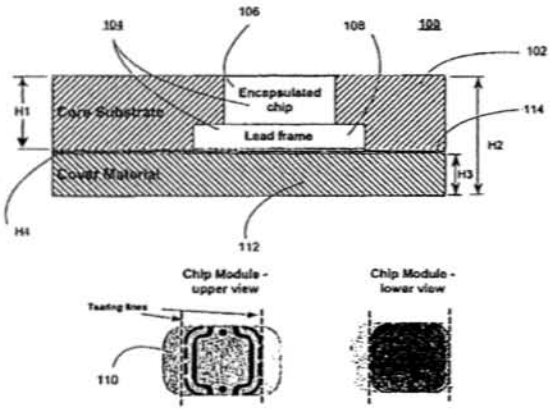


Figura 30. Corte transversal de la incrustación del microchip[212]

El diseño de patente tomado como referencia y de manera genérica es funcionalmente flexible ya que ofrece un alojamiento basado en las normas internacionales existentes y emergentes en el campo de los documentos inteligentes, particularmente sobre los pasaportes biométricos, donde el mismo responde a las especificaciones generales de la OACI[7] [8], y particularmente al diseño de los EE.UU. para su fabricación e implementación, por incorporar a diferencia del resto de los estados, una malla metálica en sus tapas, (Ver Figura 31) obligatoriamente.

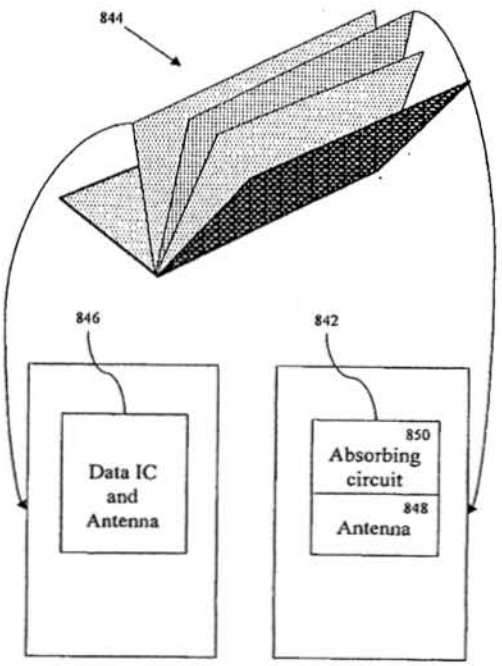


Figura 31. Vista esquemática de elementos de absorción 842 (anti-skimming), adyacentes al microchip y su antena, para obstruir la propagación de ondas electromagnéticas de cualquier lector externo cuando el pasaporte se encuentra cerrado 844, mediante la absorción de la radiación 850 (self-tuning) a través de antena 848; evitando así la lectura del módulo de identificación 846[213]

Estas normas incluirán los requisitos de interoperabilidad global, fiabilidad técnica, funcionalidad y durabilidad, bajo estándares incluidos en un chip sin

contacto incrustado o inserto dentro del pasaporte digital. El microchip sin contacto puede ser provisto por una variedad de fabricantes, de acuerdo con la norma ISO 14443[46] A / B o ISO 15693[214], y puede ser inserto en su portada o en una página de datos, conteniendo además la antena.

La información digital en el chip será firmada criptográficamente para evitar la falsificación. Las necesidades de almacenamiento biométricos previstas incluyen 12 kB (kilo-bytes) para el rostro, 10 kB para una huella digital, 30 kB para el iris y 5 kB para la información plana general. Por lo cual, serán necesarios 32 o 64 kB. El tamaño requerido de antena es la misma que en tarjetas de crédito[215]. La incrustación tiene que ser reforzada mecánicamente para proteger el chip y la antena. El pasaporte inteligente tiene que ser legible por un lector sin contacto que soporte ISO 14443[46] A y B.

La presente invención permite alojar un chip interoperable de diferentes fabricantes, como por ejemplo, Philips P5CT072[216] 72K E 2 PROM, o un ST Micro Electronics ST19XR34[217] 34K E 2 PROM.

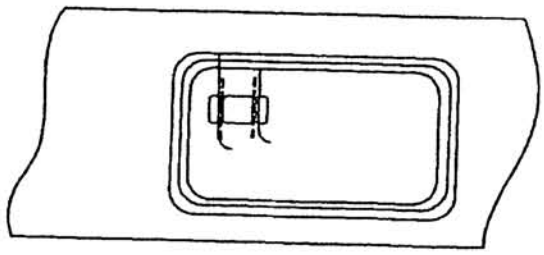


Figura 32. Incrustación del microchip[218]

Esta patente, incorpora un módulo de identificación inteligente incluyendo un módulo de chip sin contacto y una antena. El módulo de identificación inteligente es operativo para almacenar e intercambiar información de identificación personal sin contacto con un lector externo; y un elemento de aislamiento del chip para la prevención del robo no autorizada de la información (obligatorio solo para EE.UU.), el cual no es ni más ni menos que un escudo eléctrico conductor dispuesto de manera adyacente al módulo de identificación inteligente, para evitar el robo no autorizada de la información almacenada en el documento mientras está siendo leído por un elemento de lectura (Ver: Mecanismos de protección - Sistema físico de aislamiento del chip, incluido por EE.UU. en sus pasaportes de forma opcional a las normas internacionales).

De acuerdo con las características de la invención, el elemento absorbente está configurado para resonar a la frecuencia de las ondas electromagnéticas, siempre y cuando este se encuentre abierto, donde el elemento absorbente es un elemento magnético absorbente.

En el caso de encontrarse cerrado el mismo, incluye un elemento electrónico de desplazamiento de fase configurado para transmitir una señal que está fuera de fase con las ondas electromagnéticas generando de ese modo al menos una interferencia con las ondas electromagnéticas y el ruido en el canal.

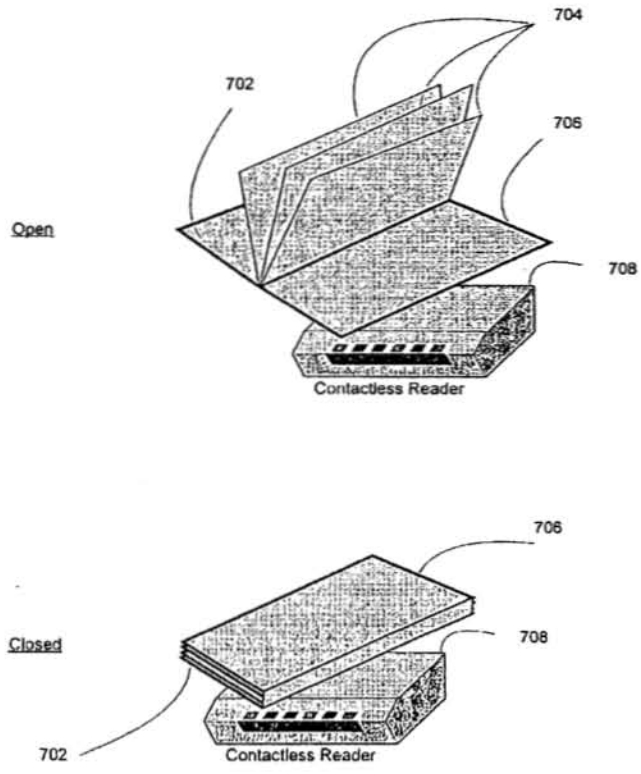


Figura 33. Muestra por un lado, la primera sección de la cubierta externa 702, varias páginas 704, y una segunda sección de la cubierta 706; donde el pasaporte se encuentra abierto y sobre un lector sin contacto 708, de tal manera que el escudo de la cubierta 702 no impide la comunicación entre el lector y el chip. Donde la siguiente ilustración, muestra un pasaporte cerrado (702 + 706), por ende con el escudo de protección de lectura sin contacto activo, evitando potencialmente el robo de información de un lector 708[219]

De acuerdo con las enseñanzas de la presente invención, también se proporciona un sistema de procesamiento de identificación personal electrónica para el procesamiento de la información con un lector externo, comprendiendo el sistema: un lector de documentos de identificación personal configurado para leer la información desde el documento de identificación personal electrónica inteligente; un terminal de procesamiento configurado para el envío de comandos para el lector y para la validación de la información del documento; y un enlace de comunicación que une operativamente el lector y el terminal de procesamiento, donde además, cada uno de los involucrados incluyen un codificador y decodificador para que los datos transmitidos se interpreten de manera segura.

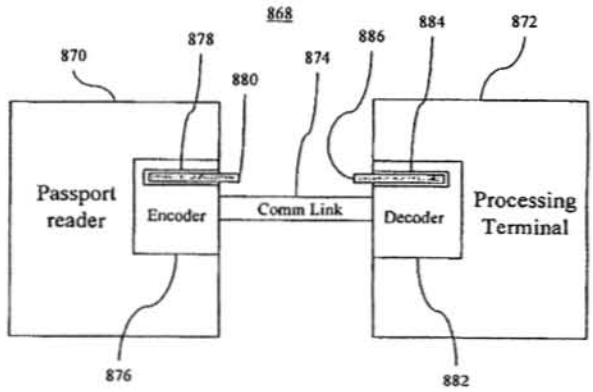


Figura 34. Vista esquemática del sistema de procesamiento de información del pasaporte construido y operable de acuerdo a la presente patente[220]

Contexto Global

Suplantación de identidad y falsedad documental

Documento Autentico

Código de documento

Los códigos de documento que se utilizan para los documentos auténticos están formados por una serie de elementos específicos:

Por ejemplo, el código "FRA-AO-01001" se compone de:

"FRA" para Francia, el país del documento	3 letras del código de país
"A" para Pasaporte (pasaporte nacional)	Clase de documento
"O" para Ordinario	Tipo de documento
"01001" (5 dígitos); los dos primeros ("01")	Número de documento
los tres últimos ("001")	Número de versión

Tabla 15. Ejemplo especifico de un código de documento de la UE

En la base prado no se describen todas las clases y tipos de documento. Para describir un documento falso, se emplea el mismo código de documento que el que corresponde al documento auténtico, seguido inmediatamente entre paréntesis del número de orden que dicho documento ocupa en la serie de documentos falsos detectados del mismo tipo:

Por ejemplo: "FRA-AO-01001 (3)" correspondería al tercer caso de documento falso detectado dentro del tipo de documento "FRA-AO-01001".

Uso ilícito

- Suplantación: Una persona, denominada suplantador, engaña apoderándose de una personalidad, identidad o nombre simulado. Los suplantadores usan siempre documentos auténticos, de modo que también puede hablarse de suplantación o usurpación en el caso de un pasaporte auténtico que contenga un visado o un sello falso, o en el caso de un visado auténtico en un pasaporte falsificado.
- Documento obtenido por medios fraudulentos: esta categorización corresponde tanto a los documentos auténticos que han sido solicitados aportando documentos acreditativos falsos o falsificados como a los documentos auténticos expedidos de forma fraudulenta.

Uso irregular

- Documento caducado: corresponde a la caducidad del mismo ("Válido hasta") documento.
- Uso indebido de un documento: Incluye los casos en que hay sospechas de que un documento va a usarse indebidamente. A modo de ejemplo, se puede utilizar como un visado de un estudiante para inmigrar, aunque su titular tiene desde el principio la intención de trabajar en el país; esta sección sobre uso indebido de documentos incluye también, los titulares de un documento de residencia diplomático que pueden usar legalmente ese tipo de permiso en lugar de un visado (en caso de que este sea necesario).

Documento Falso

En contraposición a las descripciones de las medidas de seguridad de los documentos auténticos, el término genérico: Documento Falso, es utilizado para describir los siguientes tipos de documentos:

- Documento falsificado: es la alteración no autorizada de un documento; donde se modifica el estado original de un documento auténtico expedido legalmente.
- Falsificación total: es la copia o reproducción no autorizada de un documento de seguridad auténtico. Este término se utiliza para indicar "falsificaciones completas" únicamente, es decir, documentos falsos fabricados enteramente (y no parcialmente) por un falsificador.
- Documento ficticio: Los documentos ficticios comprenden toda una serie de documentos que carecen de base legal y que por lo general no intentan reproducir ningún documento auténtico. Donde el documento ficticio tiene la apariencia de un documento oficial, pero la diferencia sustancial radica en que no es expedido por una autoridad o una institución existentes y oficialmente reconocidas por un Estado u organización de Derecho internacional, por lo que no tiene validez jurídica. Dentro de estos podemos hacer las siguientes distinciones:
    - Documento de fantasía: En los documentos de fantasía aparece el nombre de países u organizaciones imaginarios y el expedidor no

es ni un Estado reconocido por el Derecho internacional ni una institución autorizada.

- Documento de camuflaje: Son los documentos que aseguran proceder de países u organizaciones que han dejado de existir o que han cambiado de nombre.
- Otros tipos de documentos ficticios: Son por ejemplo, documentos, visados o sellos que llevan el nombre de un Estado u organización existentes pero que no corresponden a ningún documento real del país u organización internacional en cuestión y no debe confundirse con el documento falsificado, ni con la falsificación total.

- Documento robado en blanco: es aquel documento expedido ilegalmente, es decir de forma fraudulentamente, y corresponde a la sustracción de un documento auténtico virgen y posterior personalización por una persona no autorizada (falsificador).

Alternativa ingeniosa pero no 100% efectiva

Un novedoso e inteligente rediseño sobre esta tecnología, de acuerdo a la empresa Peratech[221], reduciría el riesgo actual del robo de identidad. El dueño toma una decisión consciente para autorizar la lectura de la información mediante la validación física sobre el dispositivo, donde un material muy delgado y sensible a la presión actúa como un interruptor integrado en el circuito y se lamina en el mismo.

Figura 35. Pasaporte biométrico actual[222]

Sólo cuando el interruptor está presionado por el propietario del dispositivo este se activará. Esta tecnología RFID[4] para control de acceso sin contacto, estaría disponible para pasaportes y tarjetas de crédito, siendo el fabricante antes mencionado innovador en materiales diseñados para soluciones de tecnología táctil, explicó David Lussey, CTO de Peratech.

El interruptor es incluso más delgado que el chip que le permite ser fácilmente integrado en un pase de la tarjeta de crédito, pasaporte o similar. El

material no tiene partes móviles y no requiere espacio de aire entre los contactos y es lo suficientemente robusto para durar muchos años. Esto hace que sea muy fiable y apto para su integración en los diseños electrónicos más delgados y de uso intensivo. De esta manera, se permite un mayor control sobre la información a compartir, dado que se limita el uso a la autorización física del propietario.

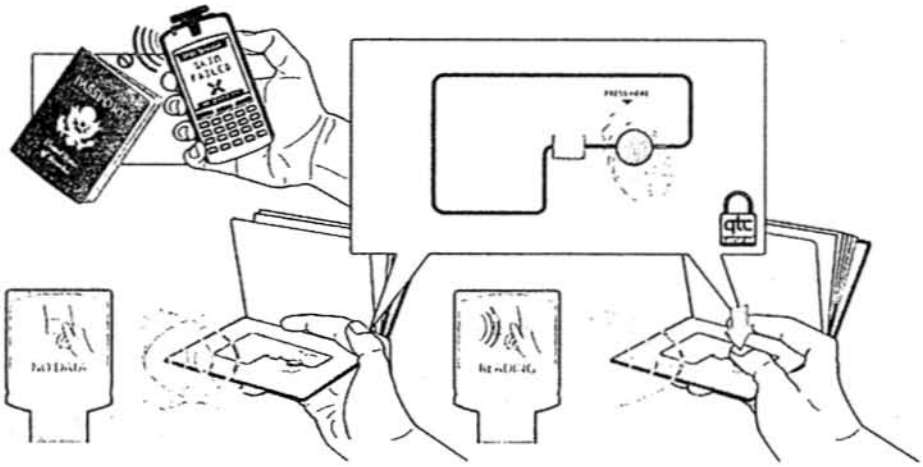


Figura 36. Rediseño de Pasaporte biométrico con tecnología QTC[223]

Futuro e Interoperabilidad

Prueba de interoperabilidad

Una prueba de interoperabilidad, es similar a un Plugtest[224] realizado por ejemplo por ETSI. Es un evento en el que los dispositivos; en este caso: pasaporte electrónico, sistemas de inspección y herramientas de prueba para los mismos, se ponen a prueba para la interoperabilidad con estándares emergentes. Este procedimiento permite a todos los proveedores, poner a prueba sus dispositivos contra otros dispositivos. Además, existe la posibilidad de realizar múltiples tipos de pruebas y así lograr la conformidad aplicada en las herramientas de prueba como GlobalTester[225] por ejemplo. Este procedimiento, logra reducir los esfuerzos y permite analizar el fracaso completo de los dispositivos como los pasaportes electrónicos o sistemas de inspección. En la actualidad, no existe un estándar de pruebas, como así tampoco están bien establecidas las especificaciones de las pruebas disponibles, tanto para los pasaportes electrónicos como para los sistemas de inspección. Por lo que los editores de estas especificaciones de prueba son la BSI[226] (Oficina Federal de

Seguridad Informática Alemana, del inglés: Federal Office for Information Security) o la OACI[227].

La Comisión Europea (CE) y la OACI[7] [8], organizo una prueba de interoperabilidad SAC en Madrid a finales de junio de 2014. El objetivo de esta prueba fue asegurar que los países europeos están listos para lanzar el protocolo de Control de Acceso Suplementario, respectivamente PACE v2; y donde los siguientes países participaron en la prueba: Alemania, Australia, Austria, Bélgica, Bosnia Herzegovina, Eslovenia, España, Finlandia, Francia, Islandia, Italia, Japón, Noruega, Países Bajos, Portugal, República Checa, Suecia y Suiza.

La prueba de interoperabilidad[228] SAC, también estaba abierta a la industria; por los cual, los siguientes proveedores participaron con sus soluciones de pasaporte electrónico:

- 3M
- Arjowiggins
- Athena
- De La Rue
- EDAPS
- Gemalto
- Giesecke & Devrient
- IRIS
- Masktech
- Oberthur
- PwPw
- Safran Morpho
- Toshiba

Cada participante tuvo la oportunidad de presentar un máximo de dos conjuntos diferentes de pasaportes con diferentes implementaciones. En total hubo 52 muestras disponibles durante la sesión de prueba. Todos los pasaportes electrónicos se pusieron a prueba en dos procedimientos diferentes: Prueba crossover y prueba de conformidad. Había tres laboratorios de pruebas (Keolabs, TÜViT + HJP Consultoría y UL) que participan en la prueba de interoperabilidad[229].

Durante la prueba de conformidad, los tres laboratorios de prueba realizaron 21.282 casos de prueba completa. Casi el 3% de los casos de prueba falló durante la prueba de conformidad.

Índices específicos

Índice de Figuras

Índice de Tablas

Índice de Cuadros

Bibliografía general

¿Cuál es el mejor pasaporte de América Latina?, El Comercio, http://elcomercio.pe/vamos/noticias/cual-mejor-pasaporte-america-latina-noticia-1728053 (Consultada el 29/10/2014)

Biometrías 2, Thill, Eduardo, Jefatura de Gabinete de Ministros - Presidencia de la Nación, http://www.biometria.gov.ar/media/74948/biometrias2.pdf (Consultada el 15/11/2014)

Biometric Passport, Wikipedia, http://en.wikipedia.org/wiki/Biometric_passport (Consultada el 9/9/2014)

Biometrics: PET or PIT?, FIDIS, http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables2/fidis-WP3-del3.16-biometrics-PET-or-PIT.PDF (Consultada el 28/12/2014)

BtB, Biometría y pasaportes, Elisa Paoletti, http://www.btb.termiumplus.gc.ca/tpv2guides/guides/caleid/index-eng.html?lang=eng&lettr=indx_autr8fq9MkNqa2sc&page=9O8D9yYVSasA.html (Consultada el 25/11/2014)

Carlos Zavaleta Pellat, Abogado especializado en temas de migración, https://www.youtube.com/watch?v=fwUvHeStcWs (Consultada el 2/10/2014)

Combining Biometric Authentication with Privacy-Enhancing Technologies, ACM, http://dl.acm.org/citation.cfm?id=1422942 (Consultada el 17/12/2014)

Consejo de la Unión Europea, Anexo PRADO; Seguridad de los documentos - Medidas de seguridad y otros términos técnicos conexos, http://register.consilium.europa.eu/doc/srv?l=ES&t=PDF&gc=true&sc=false&f=ST%2010329%202007%20REV%202 (Consultada el 8/11/2014)

Consejo de la Unión Europea, Glosario PRADO; Términos técnicos relacionados con las medidas de seguridad y con los documentos de seguridad en general, http://prado.consilium.europa.eu/es/glossarypopup.html (Consultada el 8/12/2014)

Contactless RFID Tag Measurements, Omicron Lab, http://www.omicron-lab.com/fileadmin/assets/application_notes/App_Note_RFID_Resonance_Frequency_V2_0.pdf (Consultada el 2/1/2015)

Dirección Nacional de Migraciones, Ministerio del Interior y Transporte, Área de Análisis Documental, Curso de Documentología, Guía básica de terminología aplicada, http://www.belgranomun.gov.ar/web/wp-

content/uploads/2013/04/GUIA-DOCUMENTOLOGIA-AAD-2013.pdf
(Consultada el 13/11/2014)

Doc 9303, Machine Readable Travel Documents, ICAO, http://www.icao.int/publications/pages/publication.aspx?docnum=9303
(Consultada el 1/7/2014)

El pasaporte electrónico, Alina Surós Vicente, http://publicaciones.uci.cu/index.php/SC/article/viewFile/48/49 (Consultada el 25/11/2014)

E-passport security, https://www.os3.nl/2008-2009/epassport_eng (Consultada el 19/8/2014)

ePassports reloaded, Jeroen van Beek, BlackHat USA 2008, https://www.blackhat.com/presentations/bh-usa-08/van_Beek/bh_us_08_van_Beek_ePassports_Reloaded_Slides.pdf
(Consultada el 3/12/2014)

E-Passports, Erik Poll, Digital Security Group, Radboud University Nijmegen, http://www.iom.int/seguridad-fronteriza/lit/bio/epassport.pdf (Consultada el 14/9/2014)

ETSI White Paper No. 7, Testing ePassport Readers using TTCN-3, Jean-Marc Chareau , Laurent Velez, Zdenek Riha, http://blog.protocolbench.org/wp-content/uploads/2014/08/WP7_ePassport_Interoperability_FINAL.pdf
(Consultada el 26/11/2014)

ICAO ePassport issuing States Participants in Public Key Directory (PKD), ICAO, http://gis.icao.int/epassport/ (Consultada el 4/3/2015)

ICAO Machine Readable Travel Documents Programme, ICAO, http://www.icao.int/Security/mrtd/Pages/default.aspx (Consultada el 2/8/2014)

ICAO, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, http://www.icao.int/security/mrtd/downloads/technical%20reports/technical%20report.pdf (Consultada el 19/9/2014)

Identificadores Digitales: una herramienta que apoya la recuperación de información, http://eprints.rclis.org/10599/1/indentificadores.pdf (Consultada el 9/10/2014)

Implementing The ePassport int spain: lessons learnt, Carlos Gomez, R&D Project Engineer, FNMT-RCM, http://www.icao.int/Meetings/mrtd-brazil2012/Documents/Gomez_session-2.pdf (Consultada el 29/1/2015)

JMRTD, Java implementation of the Machine Readable Travel Document, http://jmrtd.org/about.shtml (Consultada el 17/11/2014)

Machine Reading Options for td1 size MRtds, NTWG, ICAO, http://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-20/TagMrtd-20_Pres_TD-1_Broekhaar-wp20.pdf (Consultada el 14/2/2015)

NFC Passport Reader, https://play.google.com/store/apps/details?id=nl.novay.nfcpassportreader&hl=en_GB (Consultada el 4/11/2014)

NXP, Preventing fraud in ePassports and eIDs Security protocols for today and tomorrow, Markus Mösenbacher, http://www.nxp.com/documents/other/75017377.pdf (Consultada el 23/1/2015)

OIM, Sistemas sobre Pasaportes y Visas, Sección 3.1, http://www.crmsv.org/documentos/IOM_EMM_Es/v3/V3S01_CM.pdf (Consultada el 1/12/2014)

Present the Secure ID from, Laser Card, http://www.weldonn.com/laser/ (Consultada el 9/1/2015)

Protección RFID, http://www.proteccionrfid.com/ (Consultada el 21/11/2014)

Proyecto Sube, Arquitectura y Recursos para el desarrollo del servicio de transporte por medio de la tarjeta sube, http://prezi.com/yp5hoyumhmok/proyecto-sube/ (Consultada el 8/9/2014)

Pseudonymous Mobile Identity Architecture Based on Government-Supported PKI, ACM, http://dl.acm.org/citation.cfm?id=1422938 (Consultada el 7/10/2014)

Radio-electronics.com, Resources and analysis for electronic engineers, RFID coupling techniques - backscatter, capacitive, inductive, http://www.radio-electronics.com/info/wireless/radio-frequency-identification-rfid/coupling-backscatter-inductive-capacitive.php (Consultada el 25/11/2014)

RFID: Tecnología, aplicaciones y perspectivas; LIBERA, http://www.libera.net/uploads/documents/whitepaper_rfid.pdf (Consultada el 13/12/2014)

Rodríguez Carrión, A., Lecciones de Derecho Internacional Público, 2ª edición, Tecnos S.A., Madrid, 1990.

Sistemas de identificación por radiofrecuencia, Luis Miguel Blázquez del Toro, http://www.it.uc3m.es/jmb/RFID/rfid.pdf (Consultada el 14/1/2015)

Small Tech, Big Issues, RFID implants, http://web.cecs.pdx.edu/~harry/ethics/Student-Slides/Greg-Nielsen%20-%20RFID%20Implants.pdf (Consultada el 27/10/2014)

Smart identification document, CN 101002214 A; Patentes, http://www.google.com/patents/CN101002214A (Consultada el 22/10/2014)

Smart identification document, CN 101002214 B; Patentes, http://www.google.com/patents/CN101002214B (Consultada el 22/10/2014)

Smart identification document, US 20050274794 A1; Patentes, http://www.google.com/patents/US20050274794 (Consultada el 22/10/2014)

Smart Identification Document, US 20080272196 A1; Patentes, http://www.google.com/patents/US20080272196 (Consultada el 22/10/2014)

Smart identification document, US 7243840 B2; Patentes, http://www.google.com/patents/US7243840 (Consultada el 22/10/2014)

Smart identification document, US 7905415 B2; Patentes, http://www.google.com/patents/US7905415 (Consultada el 22/10/2014)

Tamper-free and forgery-proof passport and methods for providing same, US 20060005050 A1; Patentes, http://www.google.com/patents/US20060005050 (Consultada el 2/11/2014)

Tecnología de identificación por radiofrecuencia (RFID): aplicaciones en el ámbito de la salud, Informe de vigilancia tecnológica, http://www.madrimasd.org/informacionidi/biblioteca/publicacion/Vigilancia-tecnologica/descargar_documentos/fichero.asp?id=VT13_RFID.pdf (Consultada el 20/1/2015)

The history of RFID, JEREMY LANDT, http://detaco.ir/attachments/RFID-en2.pdf (Consultada el 29/12/2014)

The Use of RFID for Human Identification, A DRAFT REPORT from DHS Emerging App lications and Technology Subcommittee to the Full Data Privacy and Integrity Advisory Committee, Version 1.0; Homeland Security, http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf (Consultada el 26/10/2014)

Bibliografía específica

[1]http://es.wikipedia.org/wiki/Tarjeta_inteligente (Consultada el 30/11/2014)
[2]http://es.wikipedia.org/wiki/Sistema_%C3%9Anico_de_Boleto_Electr%C3%B3nico (Consultada el 30/11/2014)
[3]http://es.wikipedia.org/wiki/RFID#Historia (Consultada el 21/9/2014)
[4]http://es.wikipedia.org/wiki/RFID (Consultada el 12/8/2014)
[5]http://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica (Consultada el 3/9/2014)
[6]http://www.icao.int/publications/pages/publication.aspx?docnum=9303 (Consultada el 30/11/2014)
[7]http://es.wikipedia.org/wiki/Organizaci%C3%B3n_de_Aviaci%C3%B3n_Civil_Internacional (Consultada el 30/8/2014)
[8]http://www.icao.int/Pages/default.aspx (Consultada el 30/11/2014)
[9]http://es.wikipedia.org/wiki/Ley_de_Moore (Consultada el 5/10/2014)
[10]http://en.wikipedia.org/wiki/Moore%27s_law (Consultada el 27/8/2014)
[11]http://es.wikipedia.org/wiki/Documento_electr%C3%B3nico (Consultada el 3/10/2014)
[12]http://www.redusers.com/noticias/wp-content/uploads/2013/06/bagtag-650x450.jpg (Consultada el 7/8/2014)
[13]http://es.wikipedia.org/wiki/Atentados_del_11_de_septiembre_de_2001 (Consultada el 30/11/2014)
[14]http://www.fabio.com.ar/images/reviews24/pasaportes_s.jpg (Consultada el 5/11/2014)
[15]http://es.wikipedia.org/wiki/Pasaporte_biom%C3%A9trico (Consultada el 17/11/2014)
[16]http://es.wikipedia.org/wiki/Policarbonato (Consultada el 4/12/2014)
[17]http://es.wikipedia.org/wiki/Circuito_electr%C3%B3nico (Consultada el 26/10/2014)
[18]http://es.wikipedia.org/wiki/Biometr%C3%ADa (Consultada el 10/9/2014)
[19]http://www.weldonn.com/laser/lasercards_files/image014.jpg (Consultada el 29/11/2014)
[20]http://www.clarin.com/sociedad/pasaporte-ahora-electronico-cuesta_0_719928149.html (Consultada el 25/11/2014)
[21]http://infoleg.mecon.gov.ar/infolegInternet/anexos/195000-199999/198662/norma.htm (Consultada el 12/10/2014)
[22]http://www.boletinoficial.gob.ar/DisplayPdf.aspx?s=BPBCF&f=20120618 (Consultada el 14/11/2014)
[23]http://es.wikipedia.org/wiki/Documento_Nacional_de_Identidad_(Argentina) (Consultada el 30/11/2014)
[24]http://www.youtube.com/watch?v=JwePHFSrAbM (Consultada el 6/10/2014)
[25]http://www.telam.com.ar/nota/28554/ (Consultada el 19/7/2014)
[26]http://prensa.argentina.ar/2012/06/15/31583-randazzo-presento-el-nuevo-pasaporte-electronico.php (Consultada el 14/11/2014)
[27]http://prensa.argentina.ar/2012/06/18/31631-tiene-vigencia-el-nuevo-pasaporte-electronico.php (Consultada el 14/11/2014)
[28]http://mininterior.gov.ar/NuevoPasaporte/img/banner-pasaporte.png (Consultada el 21/10/2014)
[29]http://www.clarin.com/sociedad/nuevo-pasaporte_CLAFIL20120616_0002.jpg (Consultada el 8/10/2014)
[30]http://es.wikipedia.org/wiki/Pasaporte_biom%C3%A9trico#mediaviewer/Archivo:Biometric_passport_RFID_chip_high_res.png (Consultada el 2/2/2015)
[31]http://es.wikipedia.org/wiki/Circuito_integrado (Consultada el 24/11/2014)
[32]http://es.wikipedia.org/wiki/Pasaporte_biom%C3%A9trico#mediaviewer/Archivo:EPassport_logo.svg (Consultada el 2/1/2015)
[33]http://es.wikipedia.org/wiki/Am%C3%A9rica_Latina (Consultada el 20/12/2014)

[34]http://infoleg.mecon.gov.ar/infolegInternet/anexos/175000-179999/179846/norma.htm (Consultada el 2/10/2014)
[35]http://akrocard.com/userfiles/image/MifareDIAGRAMA.jpg (Consultada el 2/11/2014)
[36]http://www.icao.int/Design/img/Logo_EN.png (Consultada el 28/11/2014)
[37]http://www.icao.int/publications/Documents/9303_p1_v2_cons_es.pdf (Consultada el 28/11/2014)
[38]http://www.icao.int/publications/Documents/9303_p3_v2_cons_es.pdf (Consultada el 28/11/2014)
[39]http://es.wikipedia.org/wiki/Organizaci%C3%B3n_de_las_Naciones_Unidas (Consultada el 2/10/2014)
[40]http://www.un.org/es/ (Consultada el 2/9/2014)
[41]http://es.wikipedia.org/wiki/Convenio_sobre_Aviaci%C3%B3n_Civil_Internacional (Consultada el 24/11/2014)
[42]http://www.icao.int/secretariat/legal/List%20of%20Parties/Chicago_ES.pdf (Consultada el 28/11/2014)
[43]http://en.wikipedia.org/wiki/OCR-B (Consultada el 15/2/2015)
[44]http://upload.wikimedia.org/wikipedia/commons/a/a8/Adenauer_MRZ_2.jpg (Consultada el 06/02/2015)
[45]http://en.wikipedia.org/wiki/EEPROM (Consultada el 30/11/2014)
[46] http://en.wikipedia.org/wiki/ISO/IEC_14443 (Consultada el 7/9/2014)
[47]http://es.wikipedia.org/wiki/ISO_7816 (Consultada el 27/10/2014)
[48]http://www.iso.org/iso/catalogue_detail.htm?csnumber=18902 (Consultada el 28/10/2014)
[49]http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50410 (Consultada el 28/10/2014)
[50]http://en.wikipedia.org/wiki/UTF-8 (Consultada el 15/2/2015)
[51]http://en.wikipedia.org/wiki/Universal_Character_Set (Consultada el 15/2/2015)
[52]http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=54550 (Consultada el 29/10/2014)
[53]http://es.wikipedia.org/wiki/ISO_7816#7816-6:_Interoperabilidad_en_los_elementos_de_datos_para_el_intercambio (Consultada el 9/1/2015)
[54]http://www.iso.org/iso/catalogue_detail.htm?csnumber=38780 (Consultada el 29/10/2014)
[55]http://www.iso.org/iso/catalogue_detail.htm?csnumber=35455 (Consultada el 29/10/2014)
[56]http://es.wikipedia.org/wiki/RSA#Algoritmo_RSA (Consultada el 22/1/2015)
[57]https://www.ietf.org/rfc/rfc3447.txt (Consultada el 22/1/2015)
[58]http://es.wikipedia.org/wiki/DSA (Consultada el 22/1/2015)
[59]http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.pdf (Consultada el 22/1/2015)
[60]http://es.wikipedia.org/wiki/ECDSA (Consultada el 22/1/2015)
[61]http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.62%3A2005 (Consultada el 22/1/2015)
[62]http://www.iso.org/iso/catalogue_detail.htm?csnumber=46541 (Consultada el 22/1/2015)
[63]Directorio de Claves Públicas de la OACI (PKD), https://pkddownloadsg.icao.int/ICAO/pkdLDIFDownload.jsp (Consultada el 3/12/2014)
[64]http://www.theregister.co.uk/2010/01/26/epassport_rfid_weakness/ (Consultada el 2/9/2014)
[65]http://www.cs.bham.ac.uk/~tpc/Papers/PassportTrace.pdf (Consultada el 12/10/2014)
[66]http://www.cs.ru.nl/~erikpoll/papers/nluug.pdf (Consultada el 12/10/2014)
[67]http://en.wikipedia.org/wiki/Basic_access_control (Consultada el 15/10/2014)
[68]http://www.dexlab.nl/epassports.html (Consultada el 10/2/2015)
[69]http://en.wikipedia.org/wiki/Extended_Access_Control (Consultada el 29/9/2014)

[70]http://www.newscientist.com/article/dn8227-metal-shields-and-encryption-for-us-passports.html#.U97Dm_I5OSo (Consultada el 21/10/2014)
[71]http://patentimages.storage.googleapis.com/US7905415B2/US07905415-20110315-D00015.png (Consultada el 20/10/2014)
[72]http://www.heise.de/newsticker/meldung/Automatisches-Grenzkontrollsystem-fuer-Flughaefen-1940534.html (Consultada el 15/11/2014)
[73]http://upload.wikimedia.org/wikipedia/commons/8/8c/Border-Control-Process.png (Consultada el 6/11/2014)
[74]http://3.f.ix.de/imgs/18/1/1/8/0/0/1/2/140224_easypass_muc_img.jpg_jsessionid_F3F5FDC0BE85B3476970B3392208BEF4.2_cid297-5aa09277acf0b18a.jpeg (Consultada el 2/12/2014)
[75]https://www.eff.org/deeplinks/2012/06/biometrics-national-id-passports-false-sense-security (Consultada el 7/10/2014)
[76]http://archive.wired.com/science/discoveries/news/2006/08/71521 (Consultada el 4/11/2014)
[77]http://en.wikipedia.org/wiki/Common_Criteria (Consultada el 24/11/2014)
[78]http://www.commoncriteriaportal.org/cc/ (Consultada el 24/11/2014)
[79]http://en.wikipedia.org/wiki/Evaluation_Assurance_Level (Consultada el 23/11/2014)
[80]http://es.wikipedia.org/wiki/Lista_de_revocaci%C3%B3n_de_certificados (Consultada el 25/11/2014)
[81]http://web.eng.fiu.edu/npala/EEE6397ex/Gordon_Moore_1965_Article.pdf (Consultada el 25/11/2014)
[82]http://www.computerhistory.org/semiconductor/timeline/1965-Moore.html (Consultada el 25/11/2014)
[83]http://es.wikipedia.org/wiki/Paradoja_del_cumplea%C3%B1os (Consultada el 24/1/2015)
[84]http://www.dailymail.co.uk/news/article-440069/Safest-passport-fit-purpose.html (Consultada el 20/10/2014)
[85]http://www.computerweekly.com/news/2240079096/Expert-cracks-biometric-passport-data (Consultada el 11/11/2014)
[86]http://www.blackhat.com/presentations/bh-europe-09/VanBeek/BlackHat-Europe-2009-VanBeek-ePassports-Mobile-slides.pdf (Consultada el 18/11/2014)
[87]http://www.iom.int/seguridad-fronteriza/lit/icao/supplementtoicaodoc9303-release7.pdf (Consultada el 2/12/2014)
[88]https://www.dc414.org/download/confs/defcon15/Speakers/Grunwald/Presentation/dc-15-grunwald.pdf (Consultada el 2/11/2014)
[89]http://www.ru.nl/english/ (Consultada el 11/2/2015)
[90]http://de.wikipedia.org/wiki/Hochschule_Lausitz (Consultada el 11/2/2015)
[91]http://arstechnica.com/security/2008/08/faking-passport-rfid-chips-for-120/ (Consultada el 2/1/2015)
[92]http://www.timesonline.co.uk/tol/news/uk/crime/article4467098.ece (Consultada el 2/7/2014)
[93]http://tecnologia.elpais.com/tecnologia/2008/08/06/actualidad/1218011282_850215.html (Consultada el 27/9/2014)
[94]http://news.bbc.co.uk/2/hi/programmes/click_online/6182207.stm (Consultada el 16/11/2014)
[95]http://www.zdnet.com/blog/storage/elvis-your-e-passport-is-ready/542 (Consultada el 2/9/2014)
[96]http://en.wikipedia.org/wiki/The_Hackers_Choice (Consultada el 2/10/2014)
[97]http://es.wikipedia.org/wiki/Cracker (Consultada el 2/10/2014)
[98]https://www.youtube.com/watch?v=0u4pg_XwNk8 (Consultada el 3/10/2014)
[99]https://www.thc.org/thc-epassport/ (Consultada el 2/9/2014)
[100]https://www.thc.org/index.php?/archives/4-The-Risk-of-ePassports-and-RFID.html (Consultada el 2/9/2014)
[101]http://www.cs.bham.ac.uk/~tpc/ (Consultada el 10/02/2015)
[102]http://www.rsaconference.com/speakers/kevin-mahaffey (Consultada el 08/02/2015)

[103]Código Penal de la Nación Argentina, Capitulo III, Falsificación de documentos en general, Articulo 292, http://www.infoleg.gov.ar/infolegInternet/anexos/15000-19999/16546/texact.htm#26 (Consultada el 5/10/2014)
[104]http://www.theregister.co.uk/2008/09/30/epassport_hack_description/ (Consultada el 7/10/2014)
[105]http://rfidiot.org/ (Consultada el 7/11/2014)
[106]http://en.wikipedia.org/wiki/Supplemental_access_control (Consultada el 7/12/2014)
[107]https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/Keesing_10_09_Introducing_the_PACE_solution_pdf.pdf?__blob=publicationFile (Consultada el 06/02/2015)
[108]http://www.icao.int/Meetings/TAG-MRTD/TagMrtd22/TAG-MRTD-22_WP05.pdf (Consultada el 12/2/2015)
[109]http://es.wikipedia.org/wiki/Robo_de_identidad (Consultada el 7/12/2014)
[110]http://www.jus.gob.ar/datos-personales/ejerce-tus-derechos/robo-de-identidad.aspx (Consultada el 7/12/2014)
[111]http://es.wikipedia.org/wiki/Falsificaci%C3%B3n (Consultada el 7/12/2014)
[112]http://es.wikipedia.org/wiki/Derecho_a_la_intimidad (Consultada el 7/12/2014)
[113]http://es.wikipedia.org/wiki/Estafa (Consultada el 7/12/2014)
[114]http://es.wikipedia.org/wiki/Privacidad (Consultada el 7/12/2014)
[115]http://es.wikipedia.org/wiki/Leyes_sobre_privacidad (Consultada el 7/12/2014)
[116]http://infoleg.mecon.gov.ar/infolegInternet/anexos/40000-44999/42755/texact.htm (Consultada el 2/11/2014)
[117]http://es.wikipedia.org/wiki/Documento_p%C3%BAblico (Consultada el 7/12/2014)
[118]http://es.wikipedia.org/wiki/Derecho_argentino (Consultada el 7/12/2014)
[119]http://es.wikipedia.org/wiki/C%C3%B3digo_penal (Consultada el 7/12/2014)
[120]http://www.infoleg.gov.ar/infolegInternet/anexos/15000-19999/16546/texact.htm (Consultada el 7/12/2014)
[121]http://infoleg.mecon.gov.ar/infolegInternet/anexos/0-4999/791/norma.htm (Consultada el 23/9/2014)
[122]http://es.wikipedia.org/wiki/Giorgio_Agamben (Consultada el 7/12/2014)
[123]http://es.wikipedia.org/wiki/Richard_Stallman (Consultada el 7/12/2014)
[124]http://www.vialibre.org.ar/2012/04/23/control-para-todos/ (Consultada el 19/11/2014)
[125]http://es.wikipedia.org/wiki/Sistema_Federal_de_Identificaci%C3%B3n_Biom%C3%A9trica_para_la_Seguridad_(SIBIOS) (Consultada el 2/12/2014)
[126]https://www.eff.org/deeplinks/2012/01/biometrics-argentina-mass-surveillance-state-policy (Consultada el 6/10/2014)
[127]http://www.infoleg.gov.ar/infolegInternet/anexos/195000-199999/197800/norma.htm (Consultada el 3/10/2014)
[128]http://www.lanacion.com.ar/1597521-por-que-julian-assange-acusa-a-la-argentina-de-espionaje (Consultada el 2/9/2014)
[129]http://www.lanacion.com.ar/1635928-que-es-sibios-el-sistema-que-tiene-bajo-la-lupa-a-40-millones-de-argentinos (Consultada el 11/11/2014)
[130]http://www.youtube.com/watch?feature=player_embedded&v=Uk8x3V-sUgU (Consultada el 2/12/2014)
[131]http://www.catedrahendler.org/doctrina_in.php?id=36 (Consultada el 2/1/2015)
[132]http://www.vialibre.org.ar/2012/01/10/biometria-en-argentina-la-vigilancia-masiva-como-politica-de-estado/ (Consultada el 2/8/2014)
[133]http://www.plazademayo.com/2012/04/control-para-todos/ (Consultada el 21/9/2014)
[134]http://www.telam.com.ar/nota/27600/ (Consultada el 7/10/2014)
[135]http://www.mininterior.gov.ar/inicio/index.php (Consultada el 19/8/2014)
[136]http://prado.consilium.europa.eu/ (Consultada el 2/11/2014)
[137]http://frontex.europa.eu/ (Consultada el 12/2/2015)
[138]http://europa.eu/about-eu/agencies/regulatory_agencies_bodies/policy_agencies/frontex/index_es.htm (Consultada el 12/2/2015)

[139]http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33216_es.htm (Consultada el 12/2/2015)
[140]http://prado.consilium.europa.eu/ES/glossaryPopup.html#_192_1 (Consultada el 20/12/2014)
[141]http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52008XX0806(01) (Consultada el 29/12/2014)
[142]http://www.cps.gov.uk/legal/s_to_u/sentencing_manual/possession_of_a_false_identity_documents_with_improper_intent/ (Consultada el 29/12/2014)
[143]http://www.fidis.net/press-events/press-releases/budapest-declaration/ (Consultada el 5/1/2014)
[144]http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.en.20061106.pdf (Consultada el 2/1/2015)
[145]http://www.fidis.net/ (Consultada el 9/1/2015)
[146]http://www.fidis.net/about/consortium/ (Consultada el 9/1/2015)
[147]http://www.rfidjournal.com/articles/view?2360 (Consultada el 27/12/2014)
[148]http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf (Consultada el 2/12/2014)
[149]http://www.containerstore.com/catalogimages/164718/RfidBlockingPassportSleeve10060661_x.jpg (Consultada el 21/11/2014)
[150]http://derechoaleer.org/blog/2011/01/haciendo-el-panoptico-genetico-de-buenos-aires.html (Consultada el 28/10/2014)
[151]http://enlacedigital.com.ar/i/afip-datos-fiscales-comprometidos-filtracion-de-informacion-publica (Consultada el 20/11/2014)
[152]http://www.iprofesional.com/notas/173236-Denuncian-que-las-fotografas-de-los-nuevos-DNI-pueden-caer-en-manos-de-delincuentes-informticos (Consultada el 4/10/2014)
[153]http://blog.segu-info.com.ar/2013/10/la-adc-pidio-la-justicia-que-se-retiren.html (Consultada el 2/9/2014)
[154]http://images.containerstore.com/catalogimages/189540/10062971TravelWalletRFID_backview_x.jpg?height=312&width=312 (Consultada el 17/10/2014)
[155]http://www.bbc.com/news/technology-30513497 (Consultada el 2/1/2015)
[156]http://www.betabrand.com/ (Consultada el 9/1/2015)
[157]http://www.norton.com/ (Consultada el 9/1/2015)
[158]https://www.youtube.com/watch?v=G11xHMvhq3E (Consultada el 5/1/2015)
[159]http://www.betabrand.com/mens-rfid-blocking-pocket-norton-denim-jeans.html (Consultada el 5/1/2015)
[160]http://static1.betabrands.com/story/wp-content/uploads/2014/11/xRFID-Ready-Jeans-M-PANTS-SPEC.png.pagespeed.ic.-G9tFJ66z7.png (Consultada el 9/1/2015)
[161]http://www.betabrand.com/media/catalog/product/cache/1/image/1150x673/0dc2d03fe217f8c83829496872af24a0/r/e/xready_jeans_protected_by_norton_27.jpg.pagespeed.ic.Gw6TR5mLAX.jpg (Consultada el 9/1/2015)
[162]http://static1.betabrands.com/story/wp-content/uploads/2014/11/xRFID-Blazer-W-TOPS-SPEC.png.pagespeed.ic.DVvXhduYNl.png (Consultada el 9/1/2015)
[163]http://static2.betabrands.com/media/catalog/product/cache/1/image/1150x673/0dc2d03fe217f8c83829496872af24a0/w/o/xwork_it_blazer_protected_by_norton_8_3.jpg.pagespeed.ic.mwQoNYyvsm.jpg (Consultada el 9/1/2015)
[164]http://disklabs.com/products/faraday-bags (Consultada el 9/1/2015)
[165]http://es.wikipedia.org/wiki/Jaula_de_Faraday (Consultada el 8/11/2014)
[166]http://www.scottevest.com/v3_store/BP.shtml (Consultada el 10/1/2015)
[167]http://www.scottevest.com/media/img/page_blackout_pocket.jpg (Consultada el 10/1/2015)
[168]http://www.scottevest.com/ (Consultada el 9/1/2015)
[169]http://www.scottevest.com/media/img/rfid_built_in.jpg (Consultada el 10/1/2015)
[170]https://www.google.com.ar/search?q=si+tiene+un+chip+RFID,+es+hackeable&hl=es&gws_rd=ssl (Consultada el 12/8/2014)

[171]http://www.aietech.com/leblog/2007/2/6/le-scandale-du-passeport-rfid.html (Consultada el 28/11/2014)
[172]http://en.wikipedia.org/wiki/George_W._Bush (Consultada el 13/2/2015)
[173]http://en.wikipedia.org/wiki/Bruce_Schneier (Consultada el 3/12/2014)
[174]https://www.schneier.com/essays/archives/2004/10/does_big_brother_wan.html (Consultada el 2/11/2014)
[175]https://www.youtube.com/watch?v=-XXaqraF7pI (Consultada el 7/9/2014)
[176]http://news.virginia.edu/node/4321?id=4321 (Consultada el 18/9/2014)
[177]http://www.theguardian.com/technology/2006/nov/17/news.homeaffairs (Consultada el 2/10/2014)
[178]http://voices.washingtonpost.com/securityfix/2008/09/tool_lets_users_change_their_p.html?hpid=sec-tech (Consultada el 4/11/2014)
[179]http://www.elmundo.es/navegante/2006/03/07/esociedad/1141744987.html (Consultada el 10/10/2014)
[180]http://www.economist.com/node/14066895/print?story_id=14066895 (Consultada el 25/11/2014)
[181]https://www.eff.org/deeplinks/2012/01/biometrics-argentina-mass-surveillance-state-policy (Consultada el 6/9/2014)
[182]https://www.youtube.com/watch?v=KmEd962EvE8 (Consultada el 12/9/2014)
[183]http://en.wikipedia.org/wiki/Visa_Waiver_Program (Consultada el 9/11/2014)
[184]http://elcomercio.pe/vamos/noticias/cual-mejor-pasaporte-america-latina-noticia-1728053 (Consultada el 14/11/2014)
[185]http://www.lanacion.cl/gobierno-confirma-que-chile-entro-en-programa-de-excepcion-de-visa-a-eeuu/noticias/2013-06-03/163623.html (Consultada el 19/8/2014)
[186]http://www.emol.com/noticias/nacional/2014/03/10/648893/vicepresidente-de-eeuu-anuncia-que-programa-visa-waiver-se-adelanta-para-este-mes.html (Consultada el 22/10/2014)
[187]http://www.latercera.com/noticia/politica/2013/06/674-526500-9-pinera-confirma-ingreso-de-chile-a-programa-que-permite-viajar-a-eeuu-sin-visa.shtml (Consultada el 23/10/2014)
[188]http://www.delarue.com/insight-and-innovation/inter-operability-of-epassports.aspx (Consultada el 7/1/2015)
[189]http://en.wikipedia.org/wiki/Passports_of_the_European_Union#Overview_of_passports_issued_by_28_Member_States (Consultada el 11/1/2015)
[190]http://en.wikipedia.org/wiki/Biometric_passport#Countries_using_biometric_passports (Consultada el 11/1/2015)
[191]http://en.wikipedia.org/wiki/Budapest_Declaration_on_Machine_Readable_Travel_Documents (Consultada el 16/9/2014)
[192]https://www.opendemocracy.net/media-edemocracy/egovernment_3254.jsp#/thc-epassport/ (Consultada el 8/10/2014)
[193]http://blog.protocolbench.org/wp-content/uploads/2013/11/ISO-Layer_SmartCard.png (Consultada el 13/1/2015)
[194]http://www.icao.int/Security/mrtd/Downloads/Technical%20Reports/NEW%20TRs%20post%20TAG%2022/TR%20-%20RF%20and%20Protocol%20Testing%20Part%203%20V2.06.pdf (Consultada el 8/11/2014)
[195]https://www.bsi.bund.de (Consultada el 24/2/2015)
[196]https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110.html (Consultada el 15/1/2015)
[197]http://www.icao.int/Meetings/mrtd-madrid-2014/Pages/default.aspx (Consultada el 27/12/2014)
[198]http://www.biometria.gov.ar/editoriales/2012/08/08/avances-de-la-biometria-en-america-latina-una-herramienta-mas-para-garantizar-la-identidad-y-la-democracia.aspx (Consultada el 17/1/2015)
[199]http://www.beel.org/epass/epass-kapitel6-fazit.pdf (Consultada el 18/1/2015)

[200]http://prado.consilium.europa.eu/es/glossaryPopup_files/image114.jpg (Consultada el 8/12/2014)
[201]http://bucket3.clanacion.com.ar/anexos/fotos/52/1841652w300.jpg (Consultada el 5/1/2015)
[202]http://www.wirelessvisionme.com/attachments/Image/RFID-Tag.jpg?1382194802615 (Consultada el 21/12/2014)
[203]http://en.wikipedia.org/wiki/Automatic_identification_and_data_capture (Consultada el 20/11/2014)
[204]http://gs1ec.org/contenido/index.php?option=com_content&view=article&id=53:secretos-rfid&Itemid=58 (Consultada el 2/11/2014)
[205]http://www.google.com/patents/US4384288 (Consultada el 20/10/2014)
[206]http://en.wikipedia.org/wiki/Charles_Walton_(inventor) (Consultada el 8/10/2014)
[207]http://www.rfidjournal.com/articles/view?1338 (Consultada el 3/11/2014)
[208]http://www.leaderproducts.com.au/images/256.jpg (Consultada el 2/11/2014)
[209]http://gs1ec.org/contenido/images/stories/epc/rfid_origen.jpg (Consultada el 2/10/2014)
[210]http://autoid.mit.edu/pickup/RFID_Papers/008.pdf (Consultada el 2/12/2014)
[211]http://www.valentin-carl.com/media/produkte/etikettendrucker/rfid/rfid_function_es.gif (Consultada el 4/2/2015)
[212]http://patentimages.storage.googleapis.com/US7243840B2/US07243840-20070717-D00001.png (Consultada el 3/11/2014)
[213]http://patentimages.storage.googleapis.com/US7243840B2/US07243840-20070717-D00000.png (Consultada el 21/10/2014)
[214]http://en.wikipedia.org/wiki/ISO/IEC_15693 (Consultada el 2/1/2015)
[215]http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=4751818 (Consultada el 3/12/2014)
[216]http://www.win.tue.nl/pinpasjc/docs/cards-docs/jcop41/sfs085513.pdf (Consultada el 18/1/2015)
[217]http://pdf.datasheetcatalog.com/datasheet2/8/0iju3cuk5z1qaqfihjdzgw1pip3y.pdf (Consultada el 18/1/2015)
[218]http://patentimages.storage.googleapis.com/US7243840B2/US07243840-20070717-D00004.png (Consultada el 20/10/2014)
[219]http://patentimages.storage.googleapis.com/US7243840B2/US07243840-20070717-D00012.png (Consultada el 22/10/2014)
[220]http://patentimages.storage.googleapis.com/US7243840B2/US07243840-20070717-D00019.png (Consultada el 21/9/2014)
[221]http://www.peratech.com/rfid.html (Consultada el 26/9/2014)
[222]http://www.peratech.com/assets/images/pr/RFIDBiometricPassport_SkimStory.jpg (Consultada el 26/9/2014)
[223]http://www.peratech.com/assets/images/pr/RFIDBiometricPassport_QTCSecured_WithSkimmer.jpg (Consultada el 17/10/2014)
[224]http://www.etsi.org/services/plugtests (Consultada el 15/1/2015)
[225]http://www.globaltester.org/ (Consultada el 15/1/2015)
[226]https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03105/TR-03105_Part3_2_V1_4.html (Consultada el 14/1/2015)
[227]http://www.icao.int/Meetings/mrtd-madrid-2014/Pages/InteroperabilityTest.aspx (Consultada el 14/1/2015)
[228]http://www.securitydocumentworld.com/article-details/i/11644/ (Consultada el 13/1/2015)
[229]http://www.icao.int/Meetings/mrtd-madrid-2014/Documents/31_InteropResults_Test2014.pdf (Consultada el 12/1/2015)