RCCI Vol. 4, No. 1-2 ENERO- JUNIO, 2010 p. 65-68

Recibido: *Aceptado:*

Directorio de llaves públicas de la OACI

Alina Surós Vicente, Reynier Lester Claro Escalona

Universidad de las Ciencias Informáticas. Carretera a San Antonio de los Baños, km 2 ½. Torrens. Boyeros. Ciudad de La Habana. Cuba C.P.: 19370.
[asuros; rlclaro@uci.cu]

Resumen

Palabras clave: pasaporte electrónico, OACI/ICAO, autenticación pasiva, certificado.

Introducción

La utilización de las nuevas tecnologías en todas las facetas de la sociedad en la actualidad es una necesidad imperante ante el creciente aumento del terrorismo y la falsificación de identidades. El pasaporte como documento de identificación a nivel internacional de los ciudadanos no se ve exento, debido a la importancia de este documento en la seguridad de los estados.

La Organización Internacional de Aviación Civil (OACI/ICAO), es la entidad encargada de estudiar los problemas de la aviación civil internacional y promover los reglamentos y normas únicos en la aeronáutica mundial. La labor de la OACI en documentos de viaje de lectura mecánica comenzó en 1968, cuya actividad fundamental se dirigió a recomendaciones para que la libreta o tarjeta de pasaporte normalizada que fuera susceptible a la lectura mecánica con el objetivo de acelerar el despacho de pasajeros por los puestos de control de pasaporte. Continúa su labor en función de mejorar la confirmación de la identidad con los pasaportes, iniciándose en 1998 el estudio sistemático para la inclusión de características biométricas en el pasaporte que permitieran validar la identidad del ciudadano trayendo consigo la concesión de un nuevo documento: El pasaporte electrónico (pasaporte-e).

Este pasaporte incorpora un circuito integrado sin contacto, que contiene la información del ciudadano, en una estructura lógica de datos (LDS) organizada en grupos de datos (DG). Para asegurar la información contenida en el documento, la OACI ha establecido una serie de medidas de seguridad que pueden ser implementadas de manera opcional u obligatoria, se hará referencia en este trabajo a la única de ejecución obligatoria que es la autenticación pasiva. La autenticación pasiva consiste en almacenar en el objeto de seguridad del documento (SOD) la firma digital de los datos contenidos en el chip pasaporte. El sistema de inspección, que contenga la llave pública asociada firmante del documento, contenida en el certificado del firmante del documento (CDS), podrá verificar la firma del documento, validando así la autenticidad de los datos almacenados en el LDS.

Directorio de llaves públicas de la OACI (ICAO PKD)

Para la validación del pasaporte electrónico es imprescindible la verificación del SO_D, y podrá ser efectiva solamente si el país receptor del

pasaporte-e cuenta con los C_{DS} o los certificados de la autoridad de certificación de firma del país (C_{CSCA}) emisor del documento. Aunque los de C_{DS} de manera opcional pueden ser incluidos en el SO_D, si lo estuvieran, no se verificaría de esta manera la cadena de confianza, elemento requerido para que sea positiva dicha verificación.
Para poder validar la firma es necesario que el sistema de control fronterizo conozca:

- El certificado de la autoridad de certificación de país del estado emisor del documento C_{CSCA}. (No es necesario poseer este certificado si se poseen los C_{DS} válidos)
- El certificado del firmante del documento C_{DS} (aunque es opcional, usualmente se encuentra en el objeto de seguridad del documento, pero no hay garantía que este certificado sea emitido por la autoridad de certificación a nivel de país de la nación emisora).
- Las listas de revocación (CLR), para validar si estos certificados todavía son válidos o si han sido revocados.

En estos momentos surge la pregunta ¿Cómo puede un estado receptor conocer los C_{CSCA} y C_{DS} de todos los países emisores de pasaporte-e que deban ser validados en sus puntos de control fronterizo? Pues mediante dos vías: acuerdos bilaterales entre naciones o mediante la guía de llaves públicas de la OACI.

La Guía de llaves públicas de la OACI o ICAO *Public Key Directory* (ICAO PKD), en inglés, no es más que un directorio centralizado que funciona como intermediario de cada nación participante, donde serán publicados:

- Certificados de firmante de documento de las naciones participantes (C_{DS}).
- Listas de Revocación de certificados (CLR).
- C_{CSCA} enlazados a sus certificados (Consiste en el intercambio del nuevo C_{CSCA} firmándolo con la llave anterior del C_{CSCA}).
- Lista Maestra de C_{CSCA} (Lista firmada de C_{CSCA} recibidos mediante acuerdos bilaterales de otros estados).

Haciendo un análisis crítico de las vías mencionadas es evidente la ventaja del uso por las naciones del PKD, debido al dificultoso proceso de intercambio de datos entre países, la demora de actualización de los datos, por ejemplo cuando sea comprometida una llave, como se muestra en la Figura 1. Ejemplo de comunicaciones utilizando los dos modelos, intercambio bilateral y vía ICAO PKD.

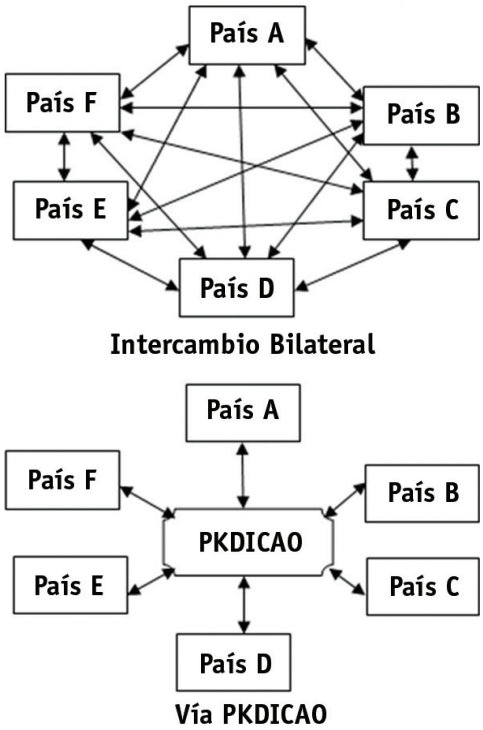

Figura 1. Ejemplo de comunicaciones utilizando los dos modelos, intercambio bilateral y vía ICAO PKD

Para el desarrollo e implementación del servicio de validación del ICAO PKD, la OACI/ICAO ha contratado a Netrust, Singapur. El sitio principal del PKD está situado en Singapur y su respaldo en Bangkok. El PKD se actualizará mediante el protocolo LDAP (*Lightweight Directory Access Protocol*) y está formada fundamentalmente por:

"Directorio de escritura": se envían los C_{DS} y CRL. Lista Maestra de C_{CSCA} de forma opcional. C_{CSCA} de enlace. Adicionalmente se envían los C_{CSCA} para validar los certificados de firmante del documento.
"Directorio de lectura": contiene los C_{DS}, que han sido previamente validados y a los que pueden acceder los estados receptores para obtener los certificados válidos, así como la Lista Maestra de C_{CSCA}. Este directorio es accesible de forma pública, en la página: https://pkddownloadsg.icao.int/. La guía de lectura tendrá un tamaño de 15-20 MB, por lo cual se recomienda su descarga y actualización diaria.

Vías de acceso al ICAO PKD

El ICAO PKD cuenta con dos vías de acceso una para los usuarios y otra para los Participantes. Los usuarios tendrán acceso a la zona de descarga del "directorio de lectura" únicamente. Los participantes contarán con un privilegio de

Vías de acceso al ICAO PKD

El ICAO PKD cuenta con dos vías de acceso una para los usuarios y otra para los Participantes. Los usuarios tendrán acceso a la zona de descarga del "directorio de lectura" únicamente. Los participantes contarán con un privilegio de acceso seguro a un puerto para descargar del PKD, estas credenciales no pueden ser compartidas y tendrán prioridad de descarga sobre el resto de los usuarios. Solo los participantes tendrán acceso a la capacidad del PKD de consulta y búsqueda de C_{DS} individuales Lista Maestra de los C_{CSCA}, Certificados de enlace de C_{CSCA} o CRL y al "directorio de escritura".

Los países participantes del PKD son: Nueva Zelanda, Australia, Estados Unidos, Alemania, Francia, Japón, Gran Bretaña, Canadá, República de Corea, Singapur.

Uso Público del ICAO PKD

La Guía de llaves públicas en su directorio de descargas contiene la lista de certificados de C_{DS} y CLR en un fichero y la Lista de Maestra de C_{CSCA}

Home ICAO PKD Download Page

Download the latest LDIF(.ldif) file

Serial Number	Description	Version	Size	Download
1	The latest collection of Document Signing Certificates(DSCs) and Certificate Revocation Lists(CRLs) to verify electronic passports.	000131	3786.0 KB	
2	The latest collection of CSCA Master Lists.	000002	15.0 KB	

Figura 2. Zona de Descarga del ICAO PKD

Conclusiones

Es de vital importancia para los países contar con elementos para comprobar la autenticidad de un pasaporte electrónico, pues sin este primer paso, la información obtenida del chip, no puede considerarse válida.

Para esta validación es necesario contar con los certificados C_{CSCA} o C_{DS} de los países emisores de documentos, dichos certificados se pueden obtener mediante acuerdos bilaterales o a través del ICAO PKD, donde evidentemente la segunda variante es la más efectiva puesto que está centralizada la información y por tanto su procesamiento así como regularidad de actualización sería mucho mayor, ahorrando costos y esfuerzos.

Deberán crearse por cada nación las condiciones tecnológicas para adquirir vía ICAO PKD los C_{DS} así como las listas maestras de C_{CSCA}, con altos niveles de actualización, para en cada punto de control migratorio poder validar los pasaportes-e que sean presentados, aumentando la seguridad en los trámites migratorios y en la admisión de los ciudadanos al país.

Referencias

Braur, D. E. (2009). PKD Board Annual Report 2009. OACI/ICAO.

Markus Hartmann, S. K. (2009, 05 20). A Primer on the ICAO Public Key Directory . OACI/ICAO.

OACI/ICAO. (2006). Documento 9303. Parte 1 Pasaportes de lectura mecánica. Volumen 2 Especificaciones para pasaportes electrónicos con capacidad de identificación biométrica.

OACI/ICAO. Procedures for the ICAO Public Key Directory.