Organización de Aviación Civil Internacional

A42-WP/475[1]
EX/214
29/7/25

NOTA DE ESTUDIO

ASAMBLEA — 42º PERÍODO DE SESIONES

COMITE EJECUTIVO

Cuestión 12: Programas de Facilitación

PROPUESTA DE OPORTUNIDADES DE MEJORA EN LA IMPLEMENTACIÓN DEL DIRECTORIO DE CLAVES PÚBLICAS (PKD) Y PASAPORTES ELECTRÓNICOS EN CONTROLES FRONTERIZOS

(Nota presentada por Argentina apoyada por Belice, Bolivia (Estado Plurinacional de), Chile, Colombia, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay.)

RESUMEN

La implementación del Directorio de Claves Públicas (PKD) de la Organización de Aviación Civil Internacional (OACI) y el uso de pasaportes electrónicos (ePassports) han mejorado la seguridad y la eficiencia en los controles fronterizos. Sin embargo, se han detectado oportunidades de mejora que, con un mayor acompañamiento por parte de la OACI, podrían facilitar la transición e integración de estos sistemas en los países en desarrollo o en proceso de implementación.

Desafíos en la Implementación del PKD:

a) **Dificultades de acceso y utilización del PKD**: Algunos países encuentran desafíos técnicos y administrativos en la incorporación del PKD a sus sistemas nacionales, debido a la falta de infraestructura o conocimiento especializado.
b) **Falta de interoperabilidad**: La ausencia de estándares más flexibles para la integración con diferentes infraestructuras nacionales genera barreras técnicas en la validación de pasaportes.
c) **Actualización y mantenimiento**: Algunos países no realizan la descarga regular de certificados y listas de revocación, lo que puede comprometer la seguridad y confiabilidad del sistema.

Decisión de la Asamblea: Se invita a la Asamblea a solicitar a la OACI fortalecer su rol mediante las siguientes acciones:

a) **Asistencia Técnica Personalizada**: Establecer programas de capacitación y asistencia técnica específicos para los países en proceso de implementación, con enfoque en buenas prácticas y optimización del uso del PKD.
b) **Plataforma de Validación Centralizada**: Explorar la posibilidad de desarrollar una API segura para que los países puedan consultar en línea los certificados y listas de revocación en tiempo real, como una alternativa complementaria a las descargas periódicas.
c) **Cooperación Regional**: Fomentar acuerdos de integración regional que permitan compartir infraestructura y conocimiento para reducir costos y mejorar la eficiencia en la adopción del PKD.

Objetivos estratégicos:	Esta nota de estudio se relaciona con los objetivos estratégicos *Todos los vuelos son seguros y protegidos, La aviación brinda movilidad fluida, accesible y confiable para todo el mundo*.

[1] Versión en español proporcionada por Argentina.

Repercusiones financieras:	Las actividades referidas en este documento dependerán de los recursos disponibles en el Presupuesto del programa regular 2025-2026 o de contribuciones presupuestarias adicionales.
Referencias:	

1. INTRODUCCIÓN

1.1 Cuando un país publica su Country Signing Certificate Authority (CSCA) al Directorio de Claves Públicas (PKD) de la Organización de Aviación Civil Internacional (OACI), los puestos de control fronterizo de su país y de otros países deben realizar una serie de acciones y utilizar tecnologías adecuadas para aprovechar la seguridad implícita en los certificados firmados de los documentos de viaje electrónicos (eMRTD). Estas acciones incluyen:

1.1.1 Descarga y Gestión de Certificados CSCA y certificado de los firmantes de documentos (DSC)

1.1.1.1 Los países que verifican documentos de viaje deben descargar periódicamente los certificados CSCA y los certificado de los firmantes de documentos (DSC) de la PKD de la OACI.

1.1.1.2 El CSCA es el certificado raíz que emite los DSC, y los DSC son los certificados utilizados para firmar los datos en los chips de los pasaportes electrónicos.

1.1.1.3 Nota en el DSC: Este es el certificado digital emitido por la Autoridad de Certificación de Firma de País (CSCA) al Firmante del Documento. El DSC contiene la clave pública del Firmante del Documento. Cuando se inspecciona un pasaporte electrónico, el sistema de inspección utiliza la clave pública del DSC para verificar la firma digital en los datos del pasaporte, asegurando que los datos no han sido manipulados y que provienen de la autoridad emisora legítima.

1.1.2 Actualización de Bases de Datos en Puestos de Control Fronterizo

1.1.2.1 Los certificados descargados deben ser distribuidos a todos los sistemas de inspección de documentos en aeropuertos, puertos y otros puntos de entrada.

1.1.3 Uso de la Autenticación Pasiva (PA)

1.1.3.1 La Autenticación Pasiva permite verificar la integridad de los datos del chip del documento de viaje. En los puestos de control, los lectores de pasaportes verifican que los datos almacenados en el chip no han sido modificados, comprobando la firma digital con el DSC correspondiente.

1.1.4 Implementación de la Autenticación Activa (AA) (Opcional)

1.1.4.1 Algunos pasaportes electrónicos usan Autenticación Activa para evitar la clonación del chip. Esto implica un desafío criptográfico entre el lector y el chip para confirmar que el chip es auténtico y no una copia.

1.1.5 Uso de la Autenticación Extendida (EAC) (para datos biométricos protegidos)

1.1.5.1 Para acceder a datos biométricos sensibles, como huellas dactilares, los sistemas fronterizos deben usar EAC. La EAC requiere que los lectores tengan certificados autorizados y que se realicen intercambios de claves para verificar permisos de acceso a los datos biométricos.

1.1.6 **Infraestructura de Validación de Certificados (PKI)**

1.1.6.1 Para validar certificados, se necesita una infraestructura de clave pública (PKI) que pueda verificar la cadena de confianza desde el CSCA hasta el DSC y la firma del chip. Esto puede incluir:

a) Listas de Certificados Revocados (CRL) para detectar certificados revocados.

b) OCSP (Online Certificate Status Protocol) para validación en tiempo real.

1.1.7 **Uso de la Inspección de Listas de Documentos Perdidos y Robados (SLTD)** de la Organización Internacional de Policía Criminal (INTERPOL).

1.1.7.1 Los sistemas fronterizos también deben consultar bases de datos internacionales, como la SLTD de INTERPOL, para detectar documentos de viaje reportados como perdidos o robados.

2. SINTESIS

2.1 Para que los puestos fronterizos puedan usar la seguridad implícita en los certificados de los documentos de viaje tras la incorporación de un país a la PKD de la OACI, deben:

a) descargar y actualizar periódicamente los certificados CSCA y DSC desde la PKD;

b) distribuir estos certificados a los sistemas de inspección en fronteras;

c) implementar Autenticación Pasiva (PA) para verificar la integridad de los datos del chip;

d) usar AA o EAC según sea necesario;

e) mantener una infraestructura PKI para validar la cadena de confianza de los certificados; y

f) integrar herramientas de detección de documentos perdidos/robados.

2.2 Estas medidas garantizan la autenticidad de los pasaportes electrónicos y evitan fraudes documentales en el control migratorio;

2.3 Sin la correcta utilización de la infraestructura PKD (Public Key Directory) de la OACI para verificar la autenticidad de los pasaportes electrónicos, se abren diversas vías para la comisión de fraudes. Estos son algunos de los fraudes más comunes:

2.3.1 **Suplantación de identidad con pasaportes fraudulentos**

2.3.1.1 Pasaportes completamente falsificados: Individuos podrían crear pasaportes electrónicos que parecen auténticos pero que contienen información biográfica y biométrica falsa. Sin la verificación contra el PKD, que permite confirmar que el DSC es legítimo y ha sido emitido por una autoridad reconocida, estos documentos falsos serían más difíciles de detectar.

2.3.1.2 Pasaportes alterados: Se podrían manipular pasaportes electrónicos genuinos, alterando la fotografía o la información biográfica en la zona visual o incluso en el chip. Sin la verificación de la firma digital mediante el PKD, estas alteraciones podrían pasar desapercibidas.

2.3.1.3 Uso fraudulento de pasaportes auténticos: Personas que no son los titulares legítimos podrían utilizar pasaportes robados o perdidos. Si los sistemas de control no verifican la validez del certificado del pasaporte a través del PKD (y potencialmente contra listas de documentos robados o perdidos), el fraude sería más sencillo.

2.3.2 **Manipulación de los datos del chip**

2.3.2.1 Aunque los pasaportes electrónicos están diseñados con medidas de seguridad, sin la verificación del PKD, un atacante con las herramientas adecuadas podría intentar modificar los datos almacenados en el chip, incluyendo la información biográfica y la biométrica. La verificación del PKD asegura la integridad de estos datos al confirmar la validez de la firma digital.

2.3.3 **Reutilización de identidades**

2.3.3.1 Un individuo podría intentar utilizar múltiples pasaportes electrónicos fraudulentos con diferentes identidades para cruzar fronteras repetidamente o para cometer otros delitos. La falta de verificación contra el PKD dificulta la detección de estas inconsistencias a nivel internacional.

2.3.4 **Ataques contra la cadena de confianza**

2.3.4.1 Sin el PKD como punto central de confianza, la verificación de la autenticidad de los pasaportes se vuelve más dependiente de acuerdos bilaterales o de la confianza en la información proporcionada por cada país individualmente. Esto hace que el sistema sea más vulnerable a la infiltración de certificados fraudulentos si no se mantienen estándares de seguridad rigurosos a nivel global. El PKD establece una infraestructura robusta para mitigar este riesgo.

2.3.5 En resumen, la infraestructura PKD es crucial para establecer una cadena de confianza global en la autenticación de pasaportes electrónicos. Sin ella, los controles fronterizos son mucho más vulnerables a una variedad de fraudes sofisticados que explotan la dificultad de verificar la autenticidad de los documentos y la identidad de los viajeros a nivel internacional. La implementación del PKD permite a las autoridades de control confirmar que un pasaporte electrónico ha sido emitido por una autoridad legítima y que sus datos no han sido manipulados.

3. CONCLUSIONES

3.1 La implementación deficiente del PKD de la OACI expone a los controles fronterizos a un alto riesgo de fraudes documentales, como la suplantación de identidad y la manipulación de datos en pasaportes electrónicos. La falta de actualización y verificación de certificados compromete la cadena de confianza, debilitando la seguridad global. Para mitigar estos riesgos, es crucial fortalecer la asistencia técnica, mejorar la interoperabilidad y desarrollar herramientas centralizadas que garanticen una validación eficaz y en tiempo real.

— FIN —