Organización de Aviación Civil Internacional

NOTA DE ESTUDIO

A40-WP/7
EX/4
5/7/19
(Nota de información)

ASAMBLEA — 40º PERÍODO DE SESIONES

COMITÉ EJECUTIVO

Asunto núm. 14: Programas de facilitación

BENEFICIOS DE PARTICIPAR EN EL DIRECTORIO DE CLAVES PÚBLICAS (PKD) DE LA OACI

(Nota presentada por el Consejo de la OACI)

RESUMEN

En esta nota se presenta información sobre el Directorio de claves públicas (PKD) de la OACI y se destacan los beneficios que obtendrán los Estados al participar en él. El directorio se estableció para apoyar a los Estados con el propósito de que tengan acceso a la información de claves públicas que se requiere para validar y autentificar los pasaportes electrónicos (pasaportes-e). Es un componente esencial de la estrategia para el Programa OACI de identificación de viajeros (TRIP), ya que sirve de apoyo en hacer eficientes y rentables los procesos de lectura y verificación de documentos de viaje. La verificación de los pasaportes-e utilizando los correspondientes certificados de la infraestructura de claves públicas puede proporcionar a las autoridades de control fronterizo la certeza de que los documentos de viaje son genuinos y no están alterados, lo que a su vez autentifica la información biométrica que figura en los pasaportes-e y permite automatizar lo relativo al proceso de despacho fronterizo. La validación de los pasaportes-e es un elemento fundamental para capitalizar la inversión de los Estados en crear esos documentos de viaje, con lo que se contribuye a mejorar la seguridad fronteriza, a combatir el terrorismo y el delito y a promover en el mundo viajes aéreos seguros. Como el PKD de la OACI cubre al mismo tiempo las necesidades de seguridad de la aviación y de facilitación, utilizar el directorio ayudará a llenar los vacíos de seguridad de los sistemas de control fronterizo de los países y, a la vez, a mejorar la experiencia de los viajeros en sus desplazamientos. El PKD actualmente cuenta con 66 participantes. La OACI alienta a todos los Estados miembros a incorporarse en el PKD y usarlo activamente para mejorar la eficiencia y eficacia del proceso de validación de pasaportes-e.

Objetivos estratégicos:	Esta nota de estudio se relaciona con el Objetivo estratégico de *Seguridad de la aviación y facilitación.*
Repercusiones financieras:	No se requieren recursos adicionales.
Referencias:	C – DEC 216/2 *Documentos de viaje de lectura mecánica* (Doc 9303) (Séptima edición) Novedades relativas al Directorio de claves públicas (PKD) de la OACI, A40-WP/6 Novedades relativas a la estrategia del Programa OACI de identificación de viajeros (TRIP), A40-WP/8

1. ANTECEDENTES

1.1 Un pasaporte electrónico (pasaporte-e) es un pasaporte de lectura mecánica (MRP) que cuenta con un microprocesador con circuito integrado (CI) y datos encriptados donde se almacena la información biográfica del titular que está visible en la segunda página del pasaporte. Cuando el Estado expedidor personaliza un pasaporte-e, éste queda asegurado y, por lo tanto, no puede modificarse, con lo que se agrega a los MRP un nivel de seguridad.

1.2 Además de la información biográfica del viajero que figura en la página del pasaporte que contiene los datos, en el microprocesador del pasaporte-e (Apéndice A) se almacenan elementos de seguridad digital que son específicos de un Estado y que se conocen como firma digital del Estado. Estas firmas digitales son únicas de cada Estado y se encuentran almacenadas de manera segura en el microprocesador del pasaporte-e como objeto de seguridad del documento (SOD), de modo que pueden verificarse mediante la Infraestructura de clave pública (PKI) del Estado expedidor. En el Apéndice B se muestra la manera de interconectar la expedición y la verificación de un pasaporte-e y de confirmar la autentificación mediante el Directorio de claves públicas (PKD) de la OACI. Cuando se escanea un pasaporte-e y se leen los datos del microprocesador, la firma digital autentificada que aparece en el pasaporte indica a las autoridades fronterizas que esos datos son auténticos, que el pasaporte-e fue expedido por el Estado y que no ha sido alterado.

1.3 Esta autentificación, usualmente conocida como validación del pasaporte-e, es el proceso de validar la autenticidad e integridad de un pasaporte-e verificando la firma digital en el microprocesador. Para que el puesto de control fronterizo de un Estado receptor autentifique el pasaporte-e de un viajero extranjero, el Estado receptor debe tener acceso a cierta información del Estado expedidor.

1.4 Existen más de 140 Estados y entidades que no son Estados, como las Naciones Unidas, que actualmente expiden pasaportes-e o documentos de viaje de lectura mecánica electrónicos (eMRTD), y hay unos 1 000 millones de esos pasaportes en circulación. Si bien las firmas digitales de un Estado pueden intercambiarse en forma bilateral, el número cada vez mayor de Estados que expiden pasaportes-e y el correspondiente alto volumen de esos pasaportes en circulación podrían dar origen a un sistema altamente complejo e ineficiente que podría retrasar el proceso de facilitación y dar lugar a errores. Se creó el PKD de la OACI a fin de que constituyera un repositorio central para intercambiar la información que se necesita para autentificar los pasaportes-e. Por lo tanto, este directorio ofrece una manera eficiente para que los Estados carguen su propia información y descarguen la de otros Estados con el fin de utilizarla en los controles fronterizos para fortalecer tanto la facilitación como la seguridad de la aviación. No todos los Estados que expiden pasaportes-e participan en el PKD, como se puede observar en el Apéndice C.

2. LA FUNCIÓN DEL PKD EN LA ESTRATEGIA PARA EL PROGRAMA OACI DE IDENTIFICACIÓN DE VIAJEROS (TRIP)

2.1 En la Estrategia TRIP de la OACI se aplica un enfoque que consiste en cinco elementos interconectados que ayudan a los Estados a establecer y confirmar la identidad de los viajeros. Los cinco elementos son complementarios y se refuerzan mutuamente. La identificación eficaz de los viajeros ayuda a optimizar los beneficios económicos, sociales y políticos de los viajes internacionales, manejar los riesgos de seguridad y responder a las amenazas en las fronteras, ya que permite dirigir mejor los recursos hacia las personas de interés.

2.2 Juntos, los elementos del Programa TRIP de la OACI permiten a los Estados identificar a los viajeros y llevar a cabo evaluaciones de riesgos de viajeros específicos, principalmente enlazando los sistemas y herramientas de inspección (IST) y las aplicaciones interoperables (IA). La recopilación de

información sobre los viajeros completa el ciclo del TRIP de la OACI ya que contribuye a proporcionar pruebas adicionales de la identidad de los extranjeros que ingresan en los Estados.

2.3 Los sistemas y herramientas de inspección permiten a las autoridades fronterizas capturar, verificar y registrar los datos sobre viajeros que figuran en los documentos de viaje de lectura mecánica (MRTD). Los controles que se aplican a los titulares de los documentos de viaje pueden llevarse a cabo en diferentes fases del viaje: antes de la salida, antes de la llegada, a la entrada, durante la estancia y a la salida. Esos controles se refuerzan intercambiando mundialmente los datos sobre los pasajeros y de sus documentos de viaje, lo que se logra mediante aplicaciones interoperables. Estos dos elementos de los cinco que integran la Estrategia TRIP de la OACI se relacionan directamente con la gestión del control fronterizo (BCM). Los sistemas de control fronterizo (BCS) que emplean los Estados integran las aplicaciones interoperables con los sistemas y herramientas de inspección.

2.4 Los sistemas y herramientas de inspección capturan, verifican, cotejan y registran los datos contenidos en los MRTD y sobre los viajeros, en tanto que las aplicaciones interoperables permiten compartir a escala mundial los datos sobre los viajeros y sus documentos de viaje. La integración de los IST con las IA en los BCS nacionales permite realizar evaluaciones de riesgos de los viajeros durante las diferentes fases de su viaje. Esta evaluación se basa en la identificación de los viajeros mediante la nueva información que los Estados de tránsito y destino van obteniendo en cada fase del viaje. En el Apéndice D, se describen los elementos del TRIP de la OACI, algunos componentes de los IST y las IA y la manera en que estos interactúan con las diferentes fases del viaje de un viajero típico.

2.5 Para que la gestión del control fronterizo sea eficiente, es fundamental que los elementos de datos del MRTD se lean con eficacia utilizando MRTD y MRTD-e normalizados e interoperables que cumplan las especificaciones técnicas descritas en *Documentos de viaje de lectura mecánica* (Doc 9303) (https://www.icao.int/publications/pages/publication.aspx?docnum=9303). Los Estados deberían aplicar plenamente estas especificaciones técnicas a fin de garantizar la interoperabilidad y la obtención de los beneficios conexos en materia de seguridad de la aviación y facilitación.

3. BENEFICIOS DEL USO DEL PKD DE LA OACI EN LAS FRONTERAS

3.1 Desde el punto de vista del Estado expedidor, el uso de tecnologías modernizadas de expedición con infraestructuras de PKI y redes seguras está fortaleciendo la confianza en los pasaportes expedidos por el Estado y la participación en iniciativas internacionales en materia de seguridad de la aviación. Además, permite la flexibilidad para iniciativas más recientes, como la autorización de viaje electrónica (eTA), las puertas de control fronterizo automatizado (ABC) y todas las herramientas modernas disponibles basadas en la tecnología de pasaportes-e. Para que se puedan aprovechar plenamente los beneficios de ser miembro del PKD, el uso del PKD debería ir acompañado de inspecciones fronterizas más exhaustivas.

3.2 En 2014, el Consejo de Seguridad de las Naciones Unidas adoptó la resolución 2178 en la que, en particular: “Reafirma que todos los Estados deberán impedir la circulación de terroristas mediante controles fronterizos eficaces y controles de la emisión de documentos de identidad y de viaje, y mediante la adopción de medidas para evitar la falsificación, la alteración ilegal y la utilización fraudulenta de documentos de identidad y de viaje”. La incorporación de los Estados miembros en el PKD de la OACI y el uso de esta herramienta pueden ayudar a los Estados a poner en práctica la resolución del Consejo de Seguridad, ya que se reconoce que constituye un instrumento valioso, y actualmente no se cuenta con una alternativa viable. Desde el punto de vista de los Estados, es una medida proactiva que contribuye a mejorar la experiencia de viaje de los pasajeros y a combatir el terrorismo internacional.

3.3 Si no se cuenta con capacidad para validar los datos electrónicos de un pasaporte-e en una frontera extranjera, el documento de viaje debe tratarse exactamente como se trata un MRP y no ofrece seguridad adicional. El PKD de la OACI hace posible la validación de los pasaportes-e de forma simple, rápida y rentable. Sólo el uso de un lector de pasaportes-e precargado con datos PKD puede confirmar, en los puntos de control fronterizo, la autenticidad del microprocesador de datos de un pasaporte-e. Por lo tanto, el uso de la herramienta PKD en las fronteras garantiza que se disponga en forma oportuna de información para validar la autenticidad de dicho documento. Este proceso simplifica el proceso de validación de pasaportes-e en las fronteras y facilita un movimiento transfronterizo rápido y seguro al permitir la pronta detección de microprocesadores falsos o que no cumplen los requisitos.

3.4 Desde la perspectiva de un Estado expedidor de pasaportes-e, es importante asegurarse de que las autoridades fronterizas de todo el mundo validen sus pasaportes-e. Las cuotas de participación en el PKD son bajas, en comparación con la inversión que se requiere para mantener una infraestructura bilateral que conecte a todos los participantes que expiden pasaportes-e. Al compartirse los datos por medio del canal PKD, se reducen los costos administrativos conexos de un enfoque bilateral. Asimismo, las cuotas de participación en el PKD disminuyen conforme va aumentando la cantidad de participantes en ese directorio.

3.5 El uso del PKD en las fronteras genera gran confianza en la seguridad física y electrónica de los pasaportes-e. Se pueden cotejar la página física del pasaporte, que contiene los datos, y los datos del microprocesador mediante una inspección visual; además, se puede aplicar el reconocimiento facial a una fotografía del pasajero que llega. Así, si la inspección se realiza correctamente, los impostores y falsificadores enfrentan numerosas dificultades para el ingreso.

3.6 Participar en el PKD de la OACI ofrece acceso prioritario a las agencias de control fronterizo del Estado expedidor. Con la validación de los pasaportes-e de conformidad con la Parte 12 del Doc 9303, la autoridad de control fronterizo tiene confianza en que el documento de viaje inspeccionado ha sido expedido por las autoridades competentes y que la información registrada en él no ha sido alterada. En el Doc 9303, Parte 12, se detallan las especificaciones de la PKI, que es un componente importante para la seguridad general de los MRTD, ya que ahí se dan los requisitos que necesitan los especialistas en tecnología de la información que tienen la tarea de desarrollar el sistema de PKI nacional (NPKI) para los Estados y se cubren, entre otros, temas sobre funciones y responsabilidades, gestión de claves, mecanismos de distribución y confianza y validación en la PKI. La herramienta PKD de la OACI brinda acceso fiable y rentable a la NPKI publicada por otros Estados, lo que posibilita la validación rigurosa de los pasaportes-e.

3.7 Asimismo, la participación en el PKD permite a un Estado expedidor de pasaportes-e compartir sus experiencias con otros Estados y beneficiarse de la experiencia de esos Estados, así como adquirir las eficiencias del intercambio multilateral de datos y facilitar los viajes internacionales de sus propios ciudadanos.

3.8 Por último, es importante destacar que la Junta del PKD está finalizando una Lista maestra, que se prevé que esté disponible a finales de 2019, lo que representa una parte importante que se añade a los servicios que actualmente ofrece el PKD de la OACI.

4. CONCLUSIONES

4.1 Participar en el PKD de la OACI debería ser parte del fortalecimiento de la gestión nacional de la identidad en su conjunto. Resulta fundamental impedir que los delincuentes obtengan un pasaporte-e genuino utilizando una identidad falsa y es indispensable entrelazar los sistemas de expedición con los datos del registro civil.

4.2 La introducción del PKD debería prepararse en forma adecuada. Los Estados deberían garantizar que se cumplan las especificaciones de la OACI desde un principio. Los Estados necesitan considerar las fases administrativas nacionales e internacionales y las cuestiones técnicas relacionadas con la integración de su sistema en el PKD de la OACI. En el Apéndice E se detallan los pasos prácticos para la implantación del PKD de la OACI.

4.3 Gracias a las normas y los métodos recomendados y las especificaciones de la OACI, cada Estado tiene ahora la oportunidad de beneficiarse de este marco, que ha creado un sistema verdaderamente interoperable a escala global para leer y verificar pasaportes en las fronteras internacionales.

4.4 Esto constituye una contribución importante a la seguridad de la aviación en el mundo y facilita los procesos de inmigración en los aeropuertos, así como en las fronteras terrestres y marinas. La capacidad de agregar características biométricas, como imágenes del rostro, al microprocesador sin contacto de los MRP demuestra que el nivel de seguridad ha aumentado sustancialmente. Ahora, depende de las agencias de gestión fronteriza de todo el mundo que su infraestructura se modernice para así poder leer estas características y utilizarlas en los sistemas fronterizos con la finalidad de verificar la identidad de los portadores de los documentos.

— — — — — — — — —

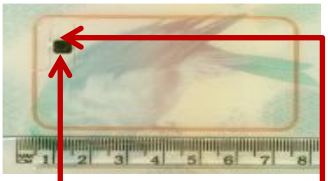
APÉNDICE A

¿QUÉ ES UN PASAPORTE-E?

La OACI define el pasaporte-e como un pasaporte de lectura mecánica (MRP) que cuenta con un microprocesador con circuito integrado (CI) sin contacto donde se almacenan los datos de la página de datos del MRP, una medición biométrica del titular del pasaporte y un objeto de seguridad para proteger los datos con una tecnología criptográfica, y que se ajusta a las especificaciones del Doc 9303-4.

MRP

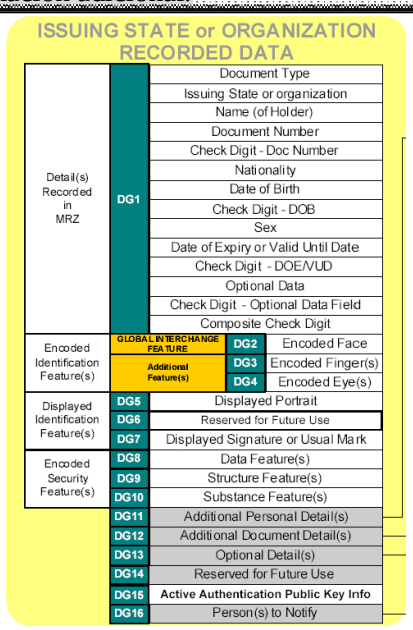
Microprocesador



Estructura lógica de datos (LDS)

Firma digital del Estado

La LDS contiene datos biográficos y biométricos obligatorios (rostro en la imagen) e información adicional.



La validación correcta de la firma digital del Estado expedidor en el microprocesador de un pasaporte electrónico indica la autenticidad e integridad de los datos registrados en la parte de la LDS del microprocesador.

— — — — — — — —

APÉNDICE B

DE LA EXPEDICIÓN A LA VERIFICACIÓN DEL PASAPORTE-E EN LA FRONTERA: LA CADENA DE CONFIANZA

Expedición de un pasaporte-e para un ciudadano del Estado A

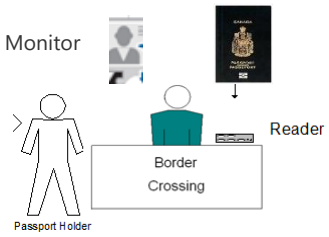
Pasos de verificación cuando el ciudadano del Estado A llega a la frontera del Estado B

Paso 1:

- Los datos de la ZLM no son más que una representación de parte de la información impresa en la página de datos, lo que permite que las computadoras lean con precisión, por medios electrónicos, la información impresa.
- El funcionario escanea el pasaporte con un lector para leer la ZLM, que permite acceder al microprocesador del pasaporte-e.
- La ZLM contiene una clave que se utiliza para acceder al microprocesador; solo se permite que el microprocesador se comunique con el lector si la clave coincide.
- Si coincide, se obtienen los datos y la fotografía y se prosigue con el Paso 2 de la verificación.

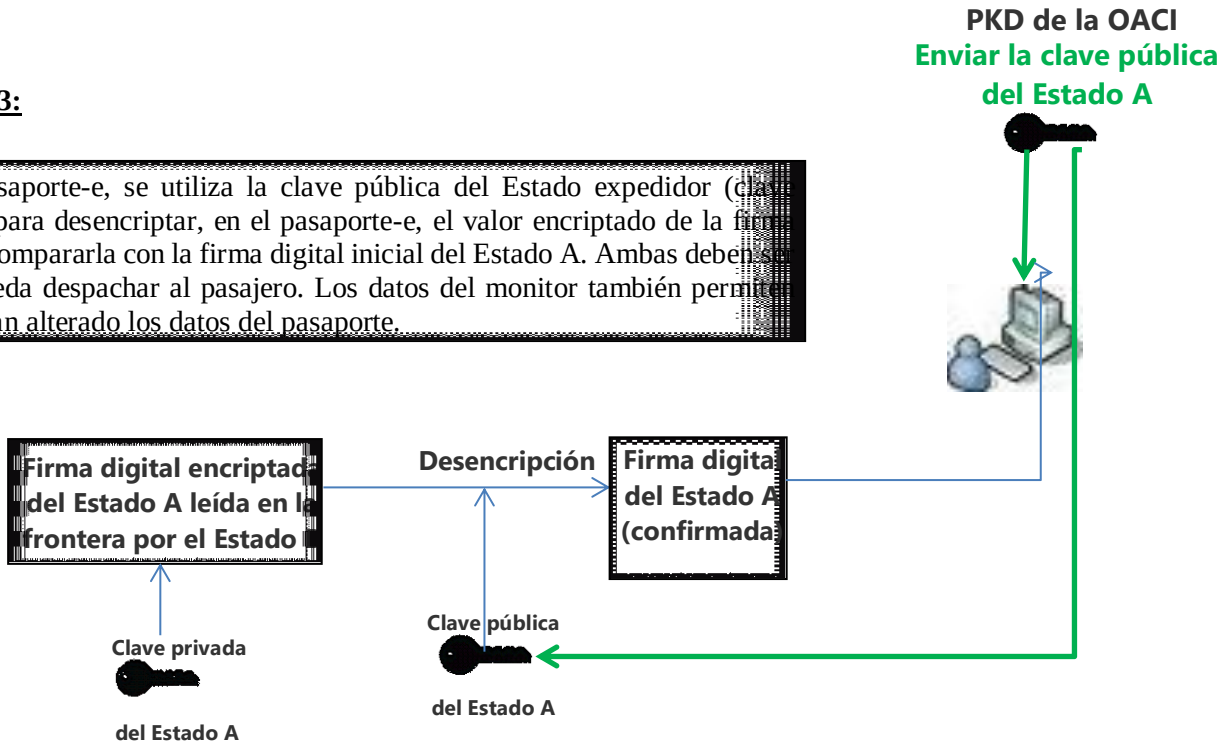
Paso 2:

Se abre el microprocesador y el funcionario verifica que el aspecto del titular coincide con la fotografía del pasaporte, así como los datos y la fotografía del microprocesador del pasaporte, que aparecen en el monitor. El siguiente paso consiste en verificar que el pasaporte haya sido expedido por una autoridad competente y que no haya sufrido modificaciones desde su expedición.



Paso 3:

Para autentificar el pasaporte-e, se utiliza la clave pública del Estado expedidor (clave pública del Estado A) para desencriptar, en el pasaporte-e, el valor encriptado de la firma digital del Estado A y compararla con la firma digital inicial del Estado A. Ambas deben ser iguales para que se pueda despachar al pasajero. Los datos del monitor también permiten verificar que no se hayan alterado los datos del pasaporte.

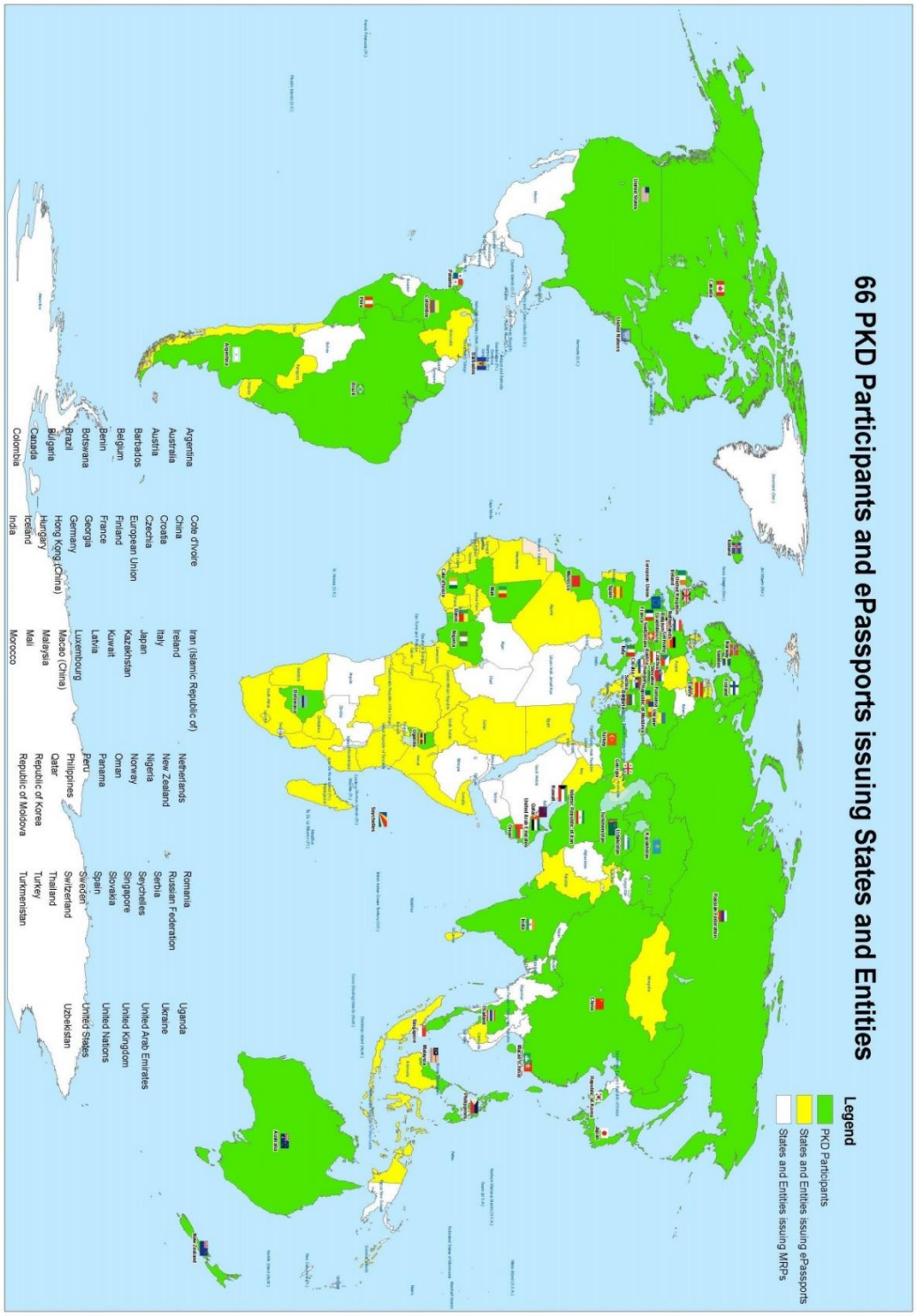


El PKD de la OACI tiene la función de validar la autenticidad de la clave pública de cada Estado; si eso no ocurre, todo el conjunto de datos del pasaporte-e podría haber sido falsificado. Esto se confirma por medio de la ceremonia oficial de importación de la clave pública de cada participante en el PKD. No obstante, el PKD de la OACI no garantiza la identidad del titular del pasaporte, sino que solo garantiza que los datos del pasaporte-e no hayan sufrido modificaciones desde que fueron producidos por un productor específico.

— — — — — — — —

APÉNDICE C

ESTADOS Y ENTIDADES EXPEDIDORES DE PASAPORTES-E Y PARTICIPANTES EN EL PKD

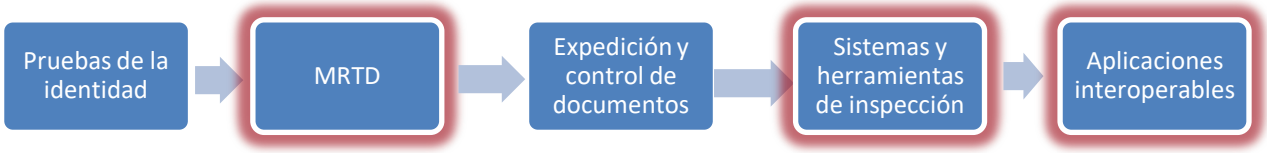


— — — — — — — —

APÉNDICE D

LA ESTRATEGIA TRIP DE LA OACI Y LA GESTIÓN DEL CONTROL FRONTERIZO

Los cinco elementos de la estrategia TRIP de la OACI: tres de ellos están vinculados al uso del PKD

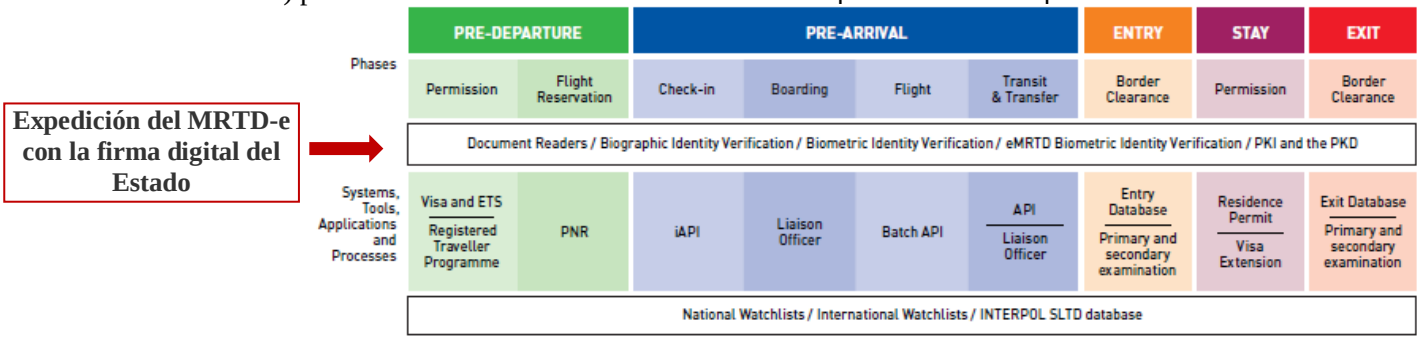


En la tabla que figura a continuación se destacan algunos ejemplos de los diferentes componentes de los elementos cuarto y quinto de la Estrategia TRIP de la OACI

SISTEMAS Y HERRAMIENTAS DE INSPECCIÓN	APLICACIONES INTEROPERABLES
Visas y sistemas electrónicos de viaje (ETS)	Sistema de información anticipada sobre los pasajeros (API) y API interactivo (iAPI)
Lectores de documentos	Datos del registro de nombres de los pasajeros (PNR)
Infraestructura de clave pública (PKI)	Infraestructura de clave pública (PKI)
Directorio de claves públicas de la OACI (PKD)	Directorio de claves públicas de la OACI (PKD)
Verificación de identidad biográfica	Verificación de identidad biométrica del MRTD-e
Verificación de identidad biométrica	Base de datos de documentos de viaje robados y perdidos (SLTD) de la Interpol
Listas nacionales de vigilancia	Listas internacionales de vigilancia
Bases de datos de entrada y salida	Controles fronterizos automatizados (ABC)
Controles fronterizos automatizados (ABC)	

Las diferentes fases del viaje de un pasajero

La preparación para el uso de la herramienta PKD de la OACI debería comenzar en la fase previa a la salida, cuando se expide el MRTD-e (2º elemento del TRIP). En la fase de entrada, se emplearía la herramienta PKD de la OACI (4º elemento del TRIP) para autentificar el MRTD-e, y su interoperabilidad (5º elemento del TRIP) permitiría vincular el MRTD-e con las otras aplicaciones interoperables.



EN TODAS LAS FASES DEL VIAJE: Se utilizan los lectores de documentos para capturar de modo fiable y eficiente los datos relativos a la identidad del pasajero. Se efectúan las verificaciones de identidad biográfica con los datos leídos en los documentos de viaje. Si están disponibles, la verificación de identidad biométrica y la autenticación de la PKI, facilitadas por la herramienta PKD, contribuyen a asegurar la identificación del pasajero. Una vez establecida la identidad del pasajero con un nivel adecuado de confianza, un Estado puede consultar la base de datos de documentos de viaje robados y perdidos (SLTD) de la Interpol y las listas nacionales e internacionales de vigilancia para fundamentar la evaluación de riesgos del viajero.

— — — — — — — —

APÉNDICE E

PASOS PRÁCTICOS PARA INCORPORARSE EN EL PKD DE LA OACI

1) Examen de la legislación nacional: Es fundamental llevar a cabo un examen exhaustivo de la legislación nacional antes de incorporar los pasaportes electrónicos y participar en el PKD de la OACI.

2) Definición de funciones y responsabilidades e implementación de un NPKD: Los Estados tienen la responsabilidad de garantizar la calidad del material que intercambian a través del PKD de la OACI. Para ello, es necesario que las funciones y responsabilidades de las partes interesadas nacionales estén definidas con claridad y que se cumplan y mantengan las normas técnicas. Esto se aplica, en especial, a los directorios de claves públicas nacionales (NPKD) que cargarán y descargarán certificados hacia y desde el PKD de la OACI y la CSCA.

3) Incorporación en el PKD de la OACI: El paso inicial para un Estado consiste en firmar el Memorando de acuerdo (MoU) del PKD con la OACI. Luego se dispone de un plazo de 15 meses para conectar el NPKD con el PKD de la OACI e iniciar la carga y descarga activa. Los Estados que deseen incorporarse en el PKD de la OACI deberían consultar a la Secretaría los detalles del proceso de inscripción.

4) Integración del NPKD con el PKD de la OACI: El paso final consiste en la plena integración del NPKD del Estado con el PKD de la OACI. Esto incluye la carga y descarga por los NPKD de certificados y listas de revocación hacia y desde el PKD de la OACI.

— FIN —