Preguntas frecuentes

(23 de agosto de 2013)

i. ¿Qué es el Directorio de claves públicas (PKD)?

El PKD de la OACI es la plataforma central para administrar el intercambio de certificados y listas de revocación de certificados a nivel mundial. Esos certificados y listas de revocación de certificados se usan para validar la firma electrónica de los datos contenidos en el chip RFID de ePassports (pasaportes electrónicos) y otros eMRTD (documentos electrónicos de lectura automatizada). El contenido del PKD está previamente validado y se puede descargar de forma gratuita.

ii. ¿Cuál es el valor agregado del PKD?

A medida que más Estados introducen los ePassports, el PKD garantiza que el proceso de intercambio entre los Estados se mantenga simple y rápido. El PKD es esencial

para minimizar el volumen de certificados y las listas de revocación de certificados que se intercambian, con el fin de garantizar las descargas y cargas oportunas y manejar el cumplimiento de las normas técnicas para garantizar que se logre y se mantenga la interoperabilidad.

iii. ¿Por qué es importante que OACI respalde el PKD?

La OACI emite el Documento 9303 como la referencia central para ePassports y otros eMRTD según las normas ISO. Los conocimientos especializados y la reputación de la OACI constituyen la base para que el PKD sea una consecuencia natural y evidente para la cual no existe alternativa comparable.

iv. ¿Quiénes son los participantes del PKD?

Los participantes del PKD aparecen indicados en el sitio web del PKD.

<http://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx>

(consulte "ICAO PKD – Current Operational Status")

v. ¿Dónde puedo encontrar el Aviso de participación?

El Aviso de participación se puede descargar del sitio web del PKD.

[http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU(includeslanguageversion(s))/NoticeofParticipation-Model.pdf](http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU%28includeslanguageversion%28s%29%29/NoticeofParticipation-Model.pdf)

(consulte "Procedures for the ICAO Public Key Directory")

vi. ¿Dónde puedo encontrar el Aviso de registro?

El Aviso de registro se puede descargar del sitio web del PKD.

[http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU(includeslanguageversion(s))/NoticeofRegistration-Model.pdf](http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU%28includeslanguageversion%28s%29%29/NoticeofRegistration-Model.pdf)

(consulte "Procedures for the ICAO Public Key Directory")

Se puede descargar el esquema de tarifas del PKD en su sitio web.

<http://www.icao.int/Security/FAL/PKD/Documents/PKDFinanceDocuments/B-Fin-123-PKD%20Fee%20Schedule%202016.pdf>

(consulte "PKD Fee Schedule")

viii. ¿Qué son las tarifas de usuario?

Se puede descargar todo el contenido del PKD en forma gratuita usando el acceso web simple y rápido (<https://pkddownloadsg.icao.int/>). Sin embargo, es posible que el control fronterizo que operan los Estados o entidades no estatales que no participan en el PKD requieran acceso versátil a PKD. Dado que la instalación y mantenimiento de este tipo de acceso requiere acción permanente del operador de PKD, el Memorando de Entendimiento permite que la definición de

tarifas del usuario cubran los costos que surjan. El esquema de tarifas del PKD

contiene los detalles.

ix. ¿Qué significa participación activa?

Después de que se ha presentado un Aviso de participación y se ha pagado la Tarifa de registro, es decir, después de que la participación se haya hecho efectiva, un participante del PKD se prepara para conectar su PKD nacional con el PKD central. El Operador del PKD lo asiste en ese proceso. Después de esta fase preparatoria, el participante de PKD comienza a cargar y descargar el contenido previsto desde y hacia el PKD y mediante este procedimiento se hace 'activo'.

x. ¿Qué contenido ofrece el PKD para descargar?

El PKD ofrece Certificados del firmante del documento (DSC) y Listas de revocación de certificados (CRL), al igual que Listas maestras (ML) de Certificados CSCA para descargar.

xi. ¿Cómo compruebo los ePassports con el PKD?

El ePassport se debe comprobar usando una cadena de confianza completa. Esta cadena de confianza consiste en una comprobación de firma electrónica de los datos del chip de RFID usando el Certificado del firmante del documento (DSC). Además, comprende la validación del DSC contra el Certificado de CSCA correspondiente al país emisor. Se debe probar que la totalidad del material de certificados usados no aparece en las actuales Listas de revocación de certificado (CRL).

xii. ¿Es posible obtener acceso a huellas digitales en ePassports con el PKD?

No. Aunque las comprobaciones de ePassports y el acceso a huellas digitales en ePassports usan tecnología de infraestructura de clave pública (PKI), es imposible obtener acceso a huellas digitales usando el contenido del PKD.

xiii. ¿Qué es el plazo de 15 meses?

Después de que la participación se hace efectiva, un participante del PKD tiene un plazo de 15 meses para iniciar la participación activa. Con la participación activa, la

tarifa anual se extiende para cubrir los costos de la actividad (consulte Esquema de tarifas del PKD).

xiv. ¿Cuáles son las ventajas de ofrecer el PKD a través de Internet?

El intercambio de certificados y listas de revocación de certificados debe ser confiable y puntual. Este intercambio sólo se puede realizar con medios electrónicos. Se adoptan todas las medidas adecuadas para proteger el PKD de los ataques en Internet.

xv. ¿Existe un riesgo de descargar virus u otro software maliciosos del PKD?

No. El contenido del PKD consiste en archivos de texto que no contienen ningún script o código ejecutable.

xvi. ¿Dónde puedo encontrar información adicional?

El sitio web de PKD es <http://www.icao.int/Security/FAL/PKD/Pages/default.aspx> contiene información para una primera lectura, al igual que numerosos documentos descargables para un estudio detallado. Se puede establecer contacto con la Secretaría de la OACI ICAO-PKD@ICAO.INT o el Presidente del Consejo de PKD. Además, existe un vínculo para presentar quejas o comentarios.

xvii. El PKD se usa para comprobar firmas digitales en chips de ePassport. ¿Cómo eso puede ayudar a detectar fraude de dos personas que se parecen?

Los sistemas biométricos modernos pueden comparar una imagen facial almacenada en un ePassport y la imagen de captura en vivo del rostro de una persona en unos pocos segundos. Incluso se pueden dirigir a la inspección secundaria las pequeñas desviaciones comunes para el fraude de dos personas que se parecen.

La comprobación de firma del chip de ePassport basada en PKD determina la integridad de los datos del chip, incluida la biométrica. La validación del chip es esencial si usted depende de la imagen facial almacenada en el chip, en particular, en escenarios de control fronterizo que reciben grandes volúmenes de pasajeros.

xviii. ¿El PKD ofrece una instalación para intercambiar certificados para acceso a huellas digitales?

El Memorando de Entendimiento (MoU) de PKD no cubre el intercambio de Certificados de verificador del documento ni la información relacionada correspondiente a biométrica secundaria.

xix. ¿Cuál es el valor agregado del PKD para los Estados que emiten ePassport sin control fronterizo automatizado?

Participación activa en el PKD significa que otros Estados pueden verificar documentos de viaje de Estados participantes usando el PKD. Esto significa que los ciudadanos de ese Estado pueden disfrutar del cruce de fronteras facilitado mientras viajan, lo cual es un beneficio tangible para los ciudadanos.

Existen ePassports válidos en circulación que se emitieron antes de que entraran en vigencia las numerosas medidas del Consejo del PKD para mejorar la calidad de los datos. Dado que dichos ePassports no se pueden intercambiar fácilmente, se debe indicar claramente cuáles datos usados durante la producción del ePassport necesitan atención especial durante la validación de la firma del chip.

xxi. ¿Qué medida toma el Consejo del PKD para mejorar la calidad de los datos del PKD?

En caso en que los participantes del PKD intenten cargar contenido contrario a la norma, esto sólo se considerará después de la adecuada consideración del Consejo del PKD. El proceso de consideración incluye el compromiso de rectificar el no cumplimiento dentro de un período de transición máximo de seis meses. Después del período de transición, se rechazará el contenido que muestre nuevamente el mismo contenido de incumplimiento. Los Participantes del PKD podrán enviar certificados de CSCA o Certificados de enlace de CSCA al Operador del PKD, antes de una importación o carga para probar el cumplimiento.

xxii. ¿A qué se refiere ‘medios diplomáticos estrictamente seguros (distribución fuera de banda)’?

Esta distribución puede realizarse mediante intercambio personal, valija diplomática o cualquier otro procedimiento o medio similar. También se puede realizar por correo electrónico, sitio web, etc., siempre que el destinatario esté obligado a verificar la integridad del certificado recibido mediante comunicación fuera de banda; por ejemplo, con un hash criptográfico que se ha enviado por correo diplomático.

xxiii. ¿Los Certificados CSCA se pueden publicar en el sitio web de un estado o esto sería un incumplimiento de las normas de la OACI?

Los certificados son información pública y como tales, se pueden publicar en un sitio web. Esto no es un incumplimiento de las normas de la OACI.

xxiv. ¿Dónde puedo obtener información técnica para cargar contenido al PKD?

Todas las preguntas técnicas se responderán leyendo la documentación que la oficina del PKD y el Operador del PKD le enviarán una vez que se convierta en un Participante del PKD. Es posible que también desee comprobar la documentación del PKD para descargar en el sitio web del PKD. Específicamente, consulte los Reglamentos del PKD y los Procedimientos del PKD. Además, descargue el Suplemento del Doc 9303, disponible en el sitio web de MRTD. Este contiene la información más actualizada sobre las especificaciones de MRTD.

xxv. ¿Cómo distinguir los Certificados CSCA, Certificados del firmante del documento (DSC) y Listas de revocación de certificado (CRL) de China continental; Hong Kong, China; y Macao, China?

Hay tres lugares emisores de pasaportes en China:

i) uno para China continental,

ii) uno para Hong Kong, China y iii) uno para Macao, China.

Comparten el mismo Código de país ISO 3166 (es decir, C = CN) en los Certificados CSCA, DSC y CRL. Por lo tanto, la totalidad de estos certificados y CRL se almacena bajo la misma división con el Código de país “CN” en el PKD. Las autoridades de control fronterizo pueden distinguir las entradas usando el Código de país (C) y Organización (O) con el fin de diferenciar los certificados y CRL de los tres lugares emisores. La comparación de los atributos de los certificados de China continental; Hong Kong, China; y Macao, China es la siguiente.

|  |  |  |
| --- | --- | --- |
| China | Macao, China | Hong Kong, China |
| C = CN | C = CN | C = CN |
| O = Gobierno chino | O = RAE de Macao | O = Hong Kong China |

xxvi. ¿Por qué pagar por la participación en el PKD si puedo usar Listas maestras en forma gratuita?

Las Listas maestras del PKD cubren una parte significativa de la comunidad emisora mundial de ePassport en términos de Certificados CSCA. Dichos Certificados CSCA permiten la verificación de la cadena de certificados del emisor de ePassport respectivo. Sin embargo, un usuario de Listas maestras que no participa en el PKD debe tener presente lo siguiente:

- La distribución de los Certificados del firmante del documento (DSC) y las Listas de revocación de certificado (CRL) se mantienen como un tema abierto para los usuarios de las Listas maestras.

- Si el único estabilizador de confianza es una Lista maestra descargada del PKD, no obstante, un usuario de Listas maestras debe tener confianza en el emisor de la Lista maestra, que siempre será un participante del PKD.

- Los participantes del PKD no tienen ninguna obligación de emitir Listas maestras o incluir ciertos Certificados CSCA en las Listas maestras. Los participantes del PKD tampoco tienen la obligación de actualizar las Listas maestras dentro de cierto período después que se emiten nuevos Certificados CSCA. Por lo tanto, depender únicamente de las Listas maestras significa aceptar la posibilidad de que los Certificados CSCA no se encuentren disponibles por un período más breve o más prolongado.

- Es cierto que los participantes no PKD no pagan ninguna tarifa de PKD. Sin embargo, las descargas de los participantes no PKD por lo general se realizan en forma manual más que automática (cf. Esquema de tarifas del PKD). Esto requiere intervención humana permanente y procesamiento posterior a la descarga, lo cual significa que la diferencia financiera entre la participación y la no participación en el PKD es más pequeña que lo esperado.

- Es una Práctica recomendada en el Anexo 9 de la Convención de Chicago que los Estados contratantes que emiten o intentan emitir ePassports o implementar en comprobaciones automatizadas de los controles fronterizos en ePassports deben participar en el PKD. Además, el PKD disfruta de apoyo político de OSCE, la UE y el G8.

xxvii. ¿En qué consiste la disposición de reducción de tarifa?

Dado el crecimiento en la participación, las tarifas del PKD se han reducido.

Como se preveía en el contrato operacional, se esperaba una reducción de las tarifas del Operador del PKD, una vez que el PKD alcanzara los 31 participantes en el PKD. Como resultado, a partir del 1 de enero de 2014 la tarifa del Operador del PKD se

reducirá de US $43.000 a US $34.000. El Contrato operacional prevé una nueva reducción una vez que el PKD alcance los 65 Participantes.

xxviii. ¿Puede participar en el PKD una autoridad de control fronterizo?

Sí, una autoridad de control fronterizo puede participar en el PKD. Según el Artículo

2.1 de PKD MoU, cualquier "Estado contratante de la OACI" (es decir, un Estado que haya ratificado la Convención de Chicago) que emita o intente emitir eMRTD puede participar en el PKD. El MoU no aborda expresamente qué entidad dentro del Estado relacionado tiene que iniciar la participación. Sin embargo, cabe notar que sólo puede haber una entidad por Estado que ejecute el MoU y se comprometa con las iniciativas relacionadas con este, en nombre de ese Estado relacionado. Por lo tanto, el Estado relacionado tiene una decisión soberana sobre cuál entidad interna designar para ejecutar el MoU. Las Normas y métodos recomendados 3.9.1 en el Anexo 9 - Facilitación para la Convención de Chicago, recomiendan explícitamente la participación en el PKD en caso de controles fronterizos con comprobaciones automatizadas de los ePassports.

**-----**