



## CONFÉRENCE MINISTÉRIELLE SUR LA SÛRETÉ ET LA FACILITATION DE L'AVIATION EN AFRIQUE

(WINDHOEK) NAMIBIA, 4-8 Avril 2016)

**Point 1.6 de l'ordre du jour: Présentation du répertoire OACI des clés publiques (PKD)**

### RÉPERTOIRE DE L'OACI DES CLÉS PUBLIQUES (PKD)

*(Note présentée par le Secrétariat)*

#### SOMMAIRE

Le répertoire OACI des clés publiques (PKD) a été établi pour permettre aux États membres d'accéder aux informations des clés publiques stockées dans la puce servant à valider et à authentifier les passeports électroniques. La validation des passeports électroniques au moyen du PKD de l'OACI est un élément essentiel pour capitaliser l'investissement consenti par les États dans la confection des documents de voyage, contribuer à l'amélioration de la sûreté et de la facilitation aux frontières, lutter contre le terrorisme et le crime et promouvoir au plan mondial un voyage aérien efficace et en toute sécurité.

Cette note décrit par ailleurs l'outil PKD de l'OACI et explique les avantages procurés aux États par l'utilisation de ce précieux mode d'inspection.

**SUITE À DONNER:** La Conférence ministérielle sur la sûreté et la facilitation de l'aviation en Afrique est invitée à faire siennes les recommandations formulées au paragraphe 7.

#### RÉFÉRENCES:

### 1. GENÈSE

1.1 Les passeports électroniques (ePassports), connus également sous l'appellation de passeports biométriques contiennent une puce électronique encastrée qui stocke la photo et d'autres renseignements personnels qui se trouvent sur la page des données du passeport. Les passeports électroniques des clés publiques (PKI), qui fournissent un mécanisme permettant aux États de déceler si les renseignements stockés dans la puce ont été modifiés. Comme les renseignements contenus dans la puce sont censés être les mêmes que dans la page de données, en validant les données de la

puce on contribue également à déceler si le document physique a été modifié. Outre les informations du passeport, la puce des passeports électroniques contient le trait sùreté numérique propre à l'État qui découle des certificats de sùreté nationale, à savoir le certificat du signataire du document (DSC) et le certificat du pays du destinataire (CSCA). Ces signatures numériques sont propres au passeport électronique et spécifiques à chaque État et peuvent se vérifier par les renseignements des clés publiques de l'État ayant vérifié les passeports.

1.2 Le groupe technique consultatif de l'OACI sur le programme d'identification des voyageurs (TAG/TRIP) dont le précurseur a été le Groupe de travail des nouvelles technologies (NTWG), estime qu'il y a plus d'un demi-milliard de passeports électroniques en circulation actuellement, émis par plus de 110 États. Cela soulève la question de la faisabilité de l'échange au plan bilatéral de certificats électroniques pour valider les signatures numériques des passeports électroniques stockés dans les puces.

1.3 À la requête des États membres, le répertoire OACI des clés publiques PKD a été créé en mars 2007 sous l'égide de l'OACI afin de faciliter le partage entre États des informations contenues dans les clés publiques. Le PKD de l'OACI est le dépositaire central des certificats qui simplifient et facilitent l'échange au plan multilatéral des renseignements servant à valider les signatures numériques sur les passeports électroniques. Le PKD de l'OACI joue un rôle déterminant en tant que courtier central du fait qu'il assure l'interopérabilité tout en réduisant au minimum le volume des informations numériques échangées. À l'appendice A, le tableau illustre le processus d'échange.

## **2. RÔLE DE L'OACI**

2.1 Un site neutre, situé et exploité au siège de l'OACI supervisé par le comité directeur du PKD et financé par les adhérents du PKD de l'OACI est réputé de fournir une ressource fiable avec accès central à partir de laquelle les autorités des frontières nationales, les exploitants d'aéronefs et d'autres entités des États membres peuvent télécharger les clés publiques afin de vérifier l'authenticité des passeports qui sont des pièces d'identité.

2.2 Le comité directeur du PKD est un organe permanent chargé de la supervision financière, technique et opérationnelle et du contrôle du PKD de l'OACI. Il comprend 15 administrateurs de l'OACI, conformément aux dispositions du mémorandum d'entente de 2008 sur le PKD.

2.3 Le principal rôle de l'OACI est d'agent fiduciaire et de secrétariat en assurant les fonctions de secrétaire de comité directeur chargé de fournir un soutien administratif et technique au travail dudit comité.

## **3. L'OBJECTIF DU PKD DE L'OACI**

3.1 L'un des principaux objectifs du PKD de l'OACI est d'aider ses membres à se conformer aux dispositions du Doc 9303, *Documents de voyage lisibles à la machine (partie 12)*, pour les certificats PKI afin d'assurer la validation continue et harmonieuse des passeports électroniques aux points de contrôle frontalier.

3.2 En veillant à ce que les informations fiables soient disponibles à temps pour entamer ce processus de validation, le PKD de l'OACI simplifie et améliore les processus de validation des passeports électroniques aux points de contrôle frontalier et facilite des mouvements transfrontaliers rapides et sécurisés.

3.3 Le PKD de l'OACI et les passeports électroniques offrent également un moyen de contrôle automatisé aux frontières sans qu'il soit besoin d'adhérer à un programme distinct. Les portiques de contrôle automatisé aux frontières ABC nécessitent le recours à la biométrie, par exemple la face peut confirmer l'identité d'un voyageur. La puce dans le passeport électronique comprend la photo de face du titulaire du document. Par conséquent, lorsqu'un système de contrôle frontalier procède à la validation du passeport électronique au moyen du PKD de l'OACI, qui confirme l'authenticité et l'intégrité des données dans la puce, le système peut en toute confiance se fier à la photo pour une reconnaissance de visu.

3.4 Dans certains cas, les données de la puce des passeports électroniques actuellement en circulation ne sont pas tout à fait conformes aux spécifications de l'OACI. Par conséquent, le PKD de l'ICAO, en coopération avec l'Organisation internationale de normalisation (ISO) a déjà mis en place un mécanisme permettant de rendre disponibles les codes d'erreur en s'assurant que les autorités chargées du contrôle aux frontières sont sensibilisées à la question au moment de lire un passeport électronique non conforme.

3.5 Le PKD de l'OACI est reconnu comme étant un outil et un système précieux de répartition de certificats publics nécessaires aux contrôles aux frontières. Il aide ses membres en s'assurant que leurs certificats sont conformes aux spécifications du Doc 9303. Le fait que la 38<sup>ème</sup> Assemblée de l'OACI a entériné la stratégie TRIP de l'OACI montre le rôle capital du PKD de l'OACI dans le cadre d'un des principaux éléments de la stratégie «Outils et systèmes d'inspection» pour une lecture et une vérification efficaces et sécurisées de documents de voyage lisibles à la machine (MRTD) (Appendice, Tableau2).

3.6 Toutefois, actuellement, ce ne sont pas tous les types de certificats permettant de valider un passeport électronique qui peuvent être échangés grâce au PKD de l'OACI. Les certificats CSCA qui sont l'essence ou la pierre angulaire de la confiance sont répartis conformément aux spécifications du Doc 9303 en vertu de deux méthodes: l'échange au plan bilatéral par voie diplomatique ou par le fichier maître de la CSCA, mais pas directement à travers le PKD de l'OACI. Nombre d'États trouvent difficile d'acquérir les certificats de CSCA par voie d'échange au plan bilatéral et ont manifesté l'intérêt en un fichier maître compilé et publié par l'OACI.

3.7 La publication d'un tel fichier maître<sup>1</sup> permettrait aux autres États récepteurs d'obtenir un jeu de certificats CSCA d'une source unique (l'émetteur du fichier maître) plutôt que d'entreprendre au plan bilatéral un échange avec chacune des autorités ou organisations émettrices représentées dans ce fichier. Le Secrétariat de l'OACI et le Comité directeur sont convenus de faire signer le fichier maître et de le faire publier par l'OACI afin qu'il soit disponible dans le répertoire PKD dans un proche avenir. Ce sera là un autre précieux service que le PKD rendra à ses participants, qui servira à la fois les intérêts des autorités émettant les documents et ceux des autorités chargées des contrôles aux frontières.

#### 4. AVANTAGES PROCURÉS PAR LE RÉPERTOIRE OACI DES CLÉS PUBLIQUES (PKD)

4.1 Les États ont intérêt à adhérer au PKD de l'OACI parce que leurs ressortissants détenteurs de passeports électroniques peuvent tirer parti des avantages de la facilitation procurés par ce type de passeport. Par exemple, certains États n'autorisent l'accès à leurs portails ABC qu'aux détenteurs de passeports électroniques pour lesquels une source sûre de certificats numériques de leurs États tel que le (PKD) sont disponibles. Les autorités chargées des contrôles aux frontières ont également intérêt à adhérer au PKD pour pouvoir accéder à temps à une source d'informations fiables leur permettant de valider les passeports électroniques. Vérifier l'authenticité et la validité de passeports électroniques contribue à faciliter la tâche aux voyageurs comme cela permet d'accélérer le passage aux frontières des voyageurs légitimes.

4.2 On estime que le PKD de l'OACI est rentable parce que les droits d'adhésion représentent une infime partie de l'investissement global nécessaire au maintien d'une infrastructure bilatérale servant à relier tous les États qui délivrent des passeports électroniques et ce cout peut être recouvre dans les frais du passeport. Même si certains coûts sont difficiles à évaluer et varient sensiblement d'un État à un autre, une analyse de coûts-rentabilité (CBA) fondée sur la rétroaction et les expériences des États dans la mise en œuvre du PKD sera effectuée dans le cadre d'une étude de cas démontrant les avantages du PKD de l'OACI.<sup>2</sup>

#### 5. ÉTATS DE PARTICIPATION

5.1 Depuis janvier 2016, quatre autres États membres ont adhère au PKD de l'OACI, soit un total de 49 adhérents, tel qu'il ressort de l'Appendice B. Même si environ 80 pourcent des passeports électroniques en circulation sont délivrés par des États membres de l'OACI participant au PKD, il existe toujours un énorme fossé entre le nombre d'États délivrant des passeports électroniques, le nombre d'États adhérents du PKD et celui des États et des entités privées qui ont recours quotidiennement au PKD de l'OACI dans leurs opérations de contrôle aux frontières. Il y a un grand défi à relever, à savoir vulgariser l'inspection intégrale des passeports électroniques en s'appuyant sur toute la capacité qu'offre la puce électronique et ce faisant, vulgariser l'utilisation du PKD de l'OACI par les autorités chargées des contrôles aux frontières afin de tirer pleinement parti de la valeur pratique des passeports électroniques.

5.2 Afin d'encourager la participation au PKD de l'OACI, l'Amendement 25 à l'Annexe 9 – *Facilitation*, a proposé une modification à la Pratique recommandée 3.9.1 sur le PKD. Cette Pratique recommandée est scindée en deux Pratiques recommandées: l'une s'adressant aux émetteurs de documents, et l'autre destinée aux autorités chargées des contrôles aux frontières. L'OACI recommande fortement d'adhérer au PKD et l'amendement à l'Annexe 9 étaye cette position.

5.3 En guise de mesure de promotion en cours, une deuxième session axée sur les contrôles aux frontières grâce au PKD s'est tenue en Norvège en octobre 2014. Ce fut notamment une opportunité constructive d'examiner les différences entre utiliser le PKD de l'OACI pour valider un passeport électronique et utiliser la base de données d'INTERPOL des documents de voyage volés et perdus (SLTD), et la question de savoir si la base de données SLTD peut être reliée au PKD. L'utilisation de la base de données SLTD d'Interpol fait partie de la stratégie TRIP de l'OACI

---

<sup>1</sup>Un fichier maître est une liste de certificats CSCA produite et signée numériquement par un État émetteur. En termes simples un adhérent au PKD peut échanger au plan bilatéral des certificats CSCA avec un certain nombre d'autres États, authentifier les certificats, ensuite dresser une liste et la signer avec son certificat national. Cette liste contenant tous les CSCA en qui l'État a confiance est dénommée fichier maître et peut être chargé dans le PKD de l'OACI. Ce fichier maître peut être téléchargé à partir de PKD de l'OACI par d'autres États qui ont confiance en l'État ayant publié le fichier maître en question et qui souhaitent obtenir lesdits certificats CSCS

*Applications Interopérables*, qui comprend les applications aux informations confidentielles aux frontières à l'appui des opérations d'inspection. Tel qu'énoncé dans le mémorandum d'entente (MoU) sur le PKD, le PKD ne couvre pas l'échange des renseignements personnels dans les passeports électroniques, tels que le code d'identification du document (DIN), l'une des données contenues dans la base de données obligatoires relatives à la base de données SLTD. Par conséquent, le PKD n'offre pas la possibilité d'échange de certificats pour l'échange de renseignements personnels pouvant être versés dans la base de données SLTD d'Interpol. Des sessions sur le PKD ont également été organisées lors des trois derniers Symposiums portant sur les MRTD de l'OACI tenus à Montréal en 2013, 2014 et 2015 et lors de séminaires régionaux sur TRIP tenus au Burkina Faso (Novembre 2013), au Ouzbékistan (Avril 2014), au Niger (Janvier 2015), en République du Congo (Mai 2015) et au Kenya (Novembre 2015). Ces sessions ont mis l'accent sur les mesures pratiques permettant d'adhérer au PKD de l'OACI.

## **6. NOUVEL EXPLOITANT DU PKD**

6.1 A la suite du lancement par l'OACI d'un appel d'offres en vue de l'adjudication d'un marché opérationnel pour un exploitant du PKD en mars 2015, le marché relatif à la fourniture du PKD de l'OACI a été conclu avec la firme Bundesdruckerei GmbH en qualité d'entrepreneur principal pour la conception totale, l'élaboration et l'exploitation du PKD. Au titre de ce nouveau marché, les droits d'adhésion pour les nouveaux participants du PKD vont baisser, pour passer de 56,000 \$ÉU à 15,900 \$ÉU et de la même façon, les droits annuels des anciens adhérents vont baisser. Il convient de noter qu'il y a augmentation du nombre d'adhérents au PKD et que les droits annuels versés par chaque adhérent connaissent une baisse (voir Appendice A, Tableau 3).

## **7. SUITE À DONNER**

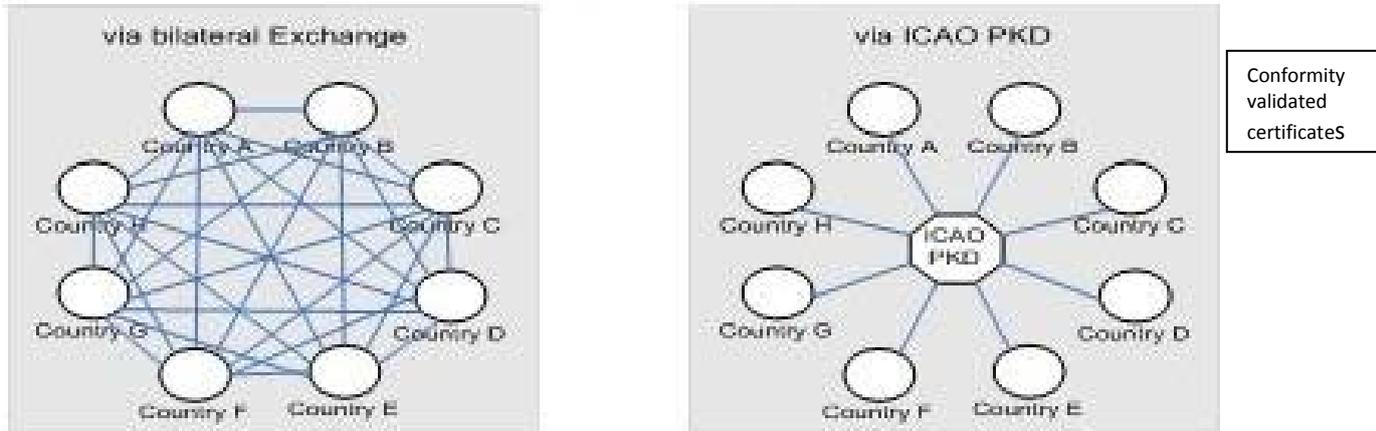
7.1 La réunion est invitée à recommander:

- a) Que les États africains veillent à participer au Répertoire OACI des clés publiques (PKD) en tant que moyen de prévention de la fraude afin de contrer les activités et autres formes de criminalité transfrontalière; et
- b) Que les États africains utilisent fréquemment le PKD de l'OACI pour authentifier et valider les passeports électroniques/biométriques.

-----

APPENDICE A

Illustration 1 – RÉPARTITION DES CERTIFICATS



Cet exemple montre 8 États nécessitant 56 échanges bilatéraux (à gauche) ou 2 échanges avec le PKD (à droite) pour être en règle avec DSC et CRL. Dans le cas des 191 États membres de l'OACI, 36,290 échanges bilatéraux seront nécessaires.

Note. — DSC: Certificat du signataire du document et CRL : Liste d'annulation de certificats.

**Illustration 2 - POSITION DU PKD DANS LA STRATÉGIE TRIP DE L'OACI**



**Tableau 3 – DROITS D’ADHÉSION ET DROITS ANNUELS**  
(Le Tableau ci-dessous ne peut pas être modifié – Le Traducteur)

<b>Registration Fee in US dollars</b>		
<b>2007 to 2008</b>	<b>2009 to 2015</b>	<b>From 2016</b>
<b>85,000</b>	<b>56,000</b>	<b>15,900</b>

<b>Annual Fee in US dollars</b>		
<b>No. of PKD Participants</b>	<b>2015 and Earlier</b>	<b>From 2016</b>
45-49	34,000	29,900
50-54	34,000	27,000
55-59	34,000	24,500

No. d'adhérent au PKD	États et entités participant au PKD	Date d'adhésion
1	Australie (Administrateur du PKD )	19/03/2007
2	Nouvelle Zélande (Administrateur du PKD )	19/03/2007
3	Singapour (Administrateur du PKD )	19/03/2007
4	Royaume-Uni (Administrateur du PKD )	19/03/2007
5	Japon (Administrateur du PKD )	19/03/2007
6	Canada (Administrateur du PKD )	19/03/2007
7	États-Unis d'Amérique (Administrateur du PKD)	02/11/2007
8	Allemagne	01/11/2007
9	République de Corée	28/03/2008
10	France	19/06/2008
11	République populaire de Chine (Administrateur du PKD )	26/11/2008
12	République du Kazakhstan	19/12/2008
13	Inde	12/02/2009
14	Nigéria (Administrateur du PKD )	13/04/2009
15	Suisse (Président du Comité directeur du PKD)	10/07/2009
16	Ukraine	30/10/2009
17	Latvie	28/06/2010
18	République tchèque	30/06/2010

19	Macao, Chine	28/09/2010
20	Émirats Arabes Unis (Administrateur du PK)	25/10/2010
21	Hong Kong, Chine	26/10/2010
22	République slovaque	23/11/2010
23	Pays-Bas (Administrateur du PKD)	08/12/2010
24	Royaume du Maroc	29/12/2010
25	Autriche	31/12/2010
26	Hongrie	15/02/2011
27	Norvège	20/06/2011
28	Bulgarie	12/10/2011
29	Luxembourg	30/11/2011
30	Suède (Administrateur du PKD)	01/12/2011
31	Nations Unies	14/06/2012
32	Espagne	10/07/2012
33	Fédération de Russie	31/08/2012
34	Malaisie (Administrateur du PKD)	09/11/2012
35	Argentine	13/12/2012
36	Thaïlande	05/03/2013
37	Irlande	08/03/2013
38	République de Moldovie	11/06/2013

39	Belgique	31/10/2013
40	Brésil (Administrateur du PKD)	03/01/2014
41	Qatar	10/03/2014
42	Seychelles	14/03/2014
43	Ouzbekistan	19/03/2014
44	Philippines	21/03/2014
45	Iran (République islamique)	18/05/2014
46	Colombie	19/05/2015
47	Roumanie	03/02/2016
48	Finlande	26/02/2016
49	République du Bénin	04/03/2016

— FIN —