Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

A39-WP/19
EX/7
31/5/16

ASSEMBLÉE — 39e SESSION

COMITÉ EXÉCUTIF

Point 19 : Facilitation et Stratégie pour un programme OACI d'identification des voyageurs (ICAO TRIP)

FAITS NOUVEAUX CONCERNANT LE RÉPERTOIRE DE CLÉS PUBLIQUES (RCP) DE L'OACI

(Note présentée par le Conseil de l'OACI)

RÉSUMÉ ANALYTIQUE

La présente note rend compte de faits nouveaux concernant le Répertoire de clés publiques (RCP) de l'OACI et son utilisation depuis la 38e session de l'Assemblée de l'OACI. Le RCP de l'OACI a été établi dans le but d'aider les États membres à accéder aux informations sur les clés publiques stockées dans la puce afin de valider et d'authentifier les passeports électroniques. La validation des passeports électroniques en recourant au RCP de l'OACI est un élément essentiel pour tirer profit de l'investissement consenti par les États pour mettre au point de tels titres de voyage, contribuer à renforcer la sûreté et la facilitation aux frontières, pour combattre le terrorisme et le crime, et pour promouvoir la sécurité et l'efficacité des voyages aériens à l'échelle mondiale. La note conclut en proposant des ordres de priorité pour le programme des travaux relatifs au RCP de l'OACI ainsi que les résultats escomptés dans ce domaine durant le prochain triennat.

Suite à donner : L'Assemblée est invitée à :
a) approuver le programme de travail relatif au RCP de l'OACI ;
b) prier instamment tous les États membres de l'OACI d'adhérer au RCP et d'y recourir activement pour valider et authentifier les passeports électroniques.

Objectifs stratégiques :	La présente note de travail se rapporte à l'Objectif stratégique C — *Sûreté et facilitation.*
Incidences financières :	Aucune ressource supplémentaire n'est nécessaire car le RCP de l'OACI est financé par les redevances des participants.
Références :	A 38-WP/11 C-WP/14264 Doc 10022, *Résolutions de l'Assemblée en vigueur* (au 4 octobre 2013)

1. HISTORIQUE

1.1 Les passeports électroniques, également appelés passeports biométriques, contiennent une puce électronique intégrée où sont stockés la photographie du titulaire et d'autres renseignements personnels figurant sur la page de renseignements du document. Les passeports électroniques sont basés sur la technologie de l'infrastructure à clés publiques (ICP) qui offre un mécanisme permettant aux États de détecter toute modification des renseignements stockés dans la puce. Comme les renseignements sur la puce sont identiques aux informations figurant sur la page de renseignements, la validation des données de la puce contribue également à la détection de toutes altérations du document physique. Outre les renseignements d'identification, la puce d'un passeport électronique contient également une fonction de sécurité numérique propre à l'État émetteur qui découle des certificats de sûreté de cet État, à savoir le certificat de signataire de documents (DSC) et le certificat de l'autorité de certification signataire nationale (ACSN). Il s'agit de signatures numériques qui sont uniques aux passeports électroniques de chaque État et qui peuvent être vérifiées au moyen de renseignements figurant dans les clés publiques de l'État émetteur.

1.2 Le Groupe consultatif technique de l'OACI sur le programme d'identification des voyageurs (TAG/TRIP), dont le Groupe de travail des technologies nouvelles (NTWG) est le fer de lance, a estimé que plus d'un demi-milliard de passeports électroniques, émis par plus de 110 États, sont actuellement en circulation. Un tel nombre soulève la question de l'aspect pratique des échanges bilatéraux de signatures électroniques pour valider l'authenticité des signatures numériques stockées dans les puces de données des passeports électroniques.

1.3 En réponse à cette question, et à la demande des États membres, l'OACI a mis sur pied, en mars 2007, un Répertoire de clés publiques (RCP) dont l'objet est de faciliter le partage entre États de renseignements sur les clés publiques. Le RCP de l'OACI est un service central d'archivage de certificats qui simplifie et facilite l'échange multilatéral de renseignements de validation des signatures figurant dans les puces de données des passeports électroniques. Son rôle de centre de coordination est critique, puisqu'il assure l'interopérabilité tout en réduisant au minimum le volume de renseignements numériques échangés. Ce processus d'échange est illustré dans la figure 1 de l'Appendice A.

2. RÔLE DE L'OACI

2.1 Un emplacement neutre, situé et exploité au siège de l'OACI, supervisé par la Commission du répertoire de clés publiques et financé par les participants au programme RCP, est considéré comme constituant une ressource de confiance, centralement accessible, où les autorités frontalières des États, les exploitants d'aéronefs et autres entités de tous les États membres peuvent télécharger des clés publiques, aux fins de vérification de l'authenticité des passeports électroniques comme pièces d'identité.

2.2 La Commission du RCP de l'OACI, composée de 15 membres désignés par le Conseil de l'OACI, conformément aux dispositions du Protocole d'entente de 2008 sur le RCP, est l'organe permanent responsable de la surveillance et de la supervision financières, techniques et opérationnelles du RCP.

2.3 Le rôle principal de l'OACI est celui d'un agent de fiducie et le Secrétariat, qui remplit les fonctions de Secrétaire de la Commission du RCP, est également chargé d'apporter un soutien opérationnel et administratif aux travaux de la Commission.

3. LES BUTS DU RCP DE L'OACI

3.1 Le RCP de l'OACI a pour objectif principal, entre autres, d'aider ses membres à réaliser et à maintenir la conformité aux dispositions (Partie 12) du Doc 9303, *Documents de voyage lisibles à la machine* relatives aux certificats du RCP, pour permettre une validation constante et sans interruption des passeports électroniques aux points de contrôle frontaliers.

3.2 En assurant la disponibilité d'informations fiables en temps utile à l'appui du processus de validation, le RCP simplifie et renforce le processus de validation des passeports électroniques aux points de contrôle frontaliers, et il facilite la vitesse et la sûreté des mouvements transfrontaliers.

3.3 Par ailleurs, le RCP et les passeports électroniques offrent un moyen d'automatiser les contrôles frontaliers sans nécessiter d'inscription préalable à un programme distinct. Les portes des contrôles frontaliers automatisés (CFA) exigent l'utilisation d'un élément biométrique, comme le visage, pour confirmer l'identité du voyageur. La puce d'un passeport électronique contient la photographie du visage du détenteur du document. Lorsqu'un système de contrôle frontalier valide un passeport électronique au moyen du RCP pour confirmer l'authenticité et l'intégralité des données contenues dans la puce, il peut se fier sans réserve à une telle photographie pour la reconnaissance faciale.

3.4 Dans certains cas, toutefois, les données des puces de passeports électroniques actuellement en circulation ne sont pas totalement conformes aux spécifications de l'OACI. C'est pourquoi le RCP de l'OACI, en collaboration avec l'Organisation internationale de normalisation (ISO), a également mis en place un mécanisme d'affichage de codes d'erreur pour alerter les unités de contrôle frontalières des problèmes de sûreté durant la lecture d'un passeport électronique non conforme.

3.5 Le RCP est reconnu comme un outil et un système utiles pour diffuser les certificats publics requis aux points de contrôle frontaliers et pour aider les membres dans la vérification de la conformité des certificats aux dispositions du Doc 9303. L'approbation de la stratégie TRIP de l'OACI par la 38e session de l'Assemblée met en relief le rôle essentiel du RCP dans un des principaux éléments de la stratégie, à savoir les *Systèmes et outils d'inspection* aux fins d'une lecture et d'une vérification efficaces et sûres des documents de voyage lisibles à la machine (MRTD) (voir Appendice A, Figure 2)

3.6 Malheureusement, pour le moment, les types de certificats requis pour la validation des passeports électroniques ne se prêtent pas tous à un échange par recours au RCP de l'OACI. Les certificats de l'ACSN, qui constituent la base de confiance ou la clé de voûte du système, sont diffusés selon deux méthodes, conformément aux dispositions du Doc 9303 : par échange diplomatique bilatéral ou dans le cadre des listes de contrôle de l'ACSN, mais non pas par l'intermédiaire du RCP de l'OACI. De nombreux États, ayant des difficultés à acquérir des certificats d'ACSN par échange bilatéral, ont manifesté de l'intérêt pour une liste de contrôle compilée et publiée par l'OACI.

3.7 La publication d'une telle liste de contrôle[1] devrait permettre à d'autres États récepteurs d'obtenir un ensemble de certificats d'ACSN à partir d'une source unique (l'auteur de la liste de contrôle), plutôt que par des échanges bilatéraux avec chacune des autorités ou organisations figurant sur cette liste. Le Secrétariat de l'OACI et la Commission du RCP sont convenus de créer une liste de contrôle signée et publiée par l'Organisation qui sera disponible dans le RCP, dans un proche avenir. Cela constituera un autre service utile offert par le RCP à ses participants, qui servira aussi bien les intérêts des autorités émettrices de documents que ceux des autorités de contrôle aux frontières.

4. AVANTAGES DU RCP DE L'OACI

4.1 Les États bénéficieront de leur adhésion au RCP parce que leurs ressortissants détenteurs d'un passeport électronique peuvent tirer parti des avantages de la facilitation des passeports électroniques. Par exemple, certains États ne donnent accès à leurs portes CFA qu'aux détenteurs de passeports électroniques émis par des États dont les certificats numériques proviennent d'une source fiable, comme le RCP. De même, les autorités de contrôle frontalier ont intérêt à adhérer aux RCP de l'OACI pour pouvoir accéder à une source d'information fiable et rapide, aux fins de validation des passeports électroniques. La vérification de l'authenticité et de la validité des passeports électroniques contribue à la sûreté et à l'efficacité de la facilitation des voyageurs, en permettant d'accélérer le passage des frontières pour les voyageurs légitimes.

4.2 Le RCP est reconnu comme étant efficace par rapport aux coûts car les frais de cotisation des membres ne représentent qu'une fraction des investissements totaux requis pour le maintien d'une infrastructure bilatérale permettant de connecter tous les États émetteurs de passeports électroniques et peuvent être récupérés avec les frais de passeport électroniques. Comme certains coûts peuvent être difficiles à déterminer et les écarts peuvent être énormes d'un État à l'autre, une analyse des coûts et avantages sera effectuée sur la base des rétroactions et des expériences des États dans la mise en œuvre du RCP, afin de mettre en relief les avantages du RCP de l'OACI.

5. DEGRÉ DE PARTICIPATION

5.1 Depuis la dernière session de l'Assemblée, 13 autres États membres de l'OACI ont adhéré au RCP, portant à 51 le nombre total de participants, comme il est indiqué à l'Appendice B. Bien que 80 % des passeports électroniques en circulation soient délivrés par des États membres du RCP, on constate encore un écart important entre le nombre d'États émettant des passeports électroniques, le nombre de participants au RCP de l'OACI et le nombre d'États et d'entités non étatiques qui utilisent quotidiennement le RCP dans les opérations de contrôle frontalier. Le principal défi que le RCP doit résoudre est d'approfondir l'inspection complète des passeports électroniques en utilisant toutes les capacités offertes par la puce, et généraliser ainsi le recours au RCP de l'OACI par les autorités de contrôle frontalier pour tirer totalement parti de la valeur pratique des passeports électroniques.

---

[1] Une liste de contrôle est une liste de certificats d'ACSN produits par un État émetteur et portant sa signature numérique. En termes simples, un participant au PKD peut échanger bilatéralement des certificats d'ACSN avec plusieurs autres États, authentifier les certificats et en dresser la liste qu'il signera ensuite avec son certificat national. Cette liste, contenant tous les certificats d'ACSN auxquels l'État fait confiance, est appelée liste de contrôle et peut être téléchargée vers le PKD de l'OACI. Cette liste de contrôle pourra ensuite être téléchargée du PKD par d'autres utilisateurs qui font confiance à l'État émetteur de la liste de contrôle et qui souhaitent obtenir ces certificats.

5.2 Afin d'encourager la participation au RCP, une révision de la Pratique recommandée 3.9.1 est proposée dans l'Amendement n° 25 de l'Annexe 9 — *Facilitation*. Il s'agit de diviser la pratique recommandée en deux, pour obtenir une pratique visant les autorités de délivrance de documents de voyage et une seconde destinée aux autorités de contrôle frontalier. L'OACI recommande fermement la participation au RCP, en soulignant que la révision de l'Annexe 9 renforce cette position.

5.3 À titre de promotion continue, une deuxième Journée « RCP aux frontières » a été organisée en Norvège en octobre 2014. Ce fut, entre autres, une occasion constructive de se pencher sur les différences entre le recours au RCP de l'OACI pour la validation des passeports électroniques et l'utilisation de la base de données sur les documents de voyage volés ou perdus (SLTD) d'Interpol, et de déterminer s'il est possible de lier la base de données au RCP. L'utilisation de la base de données d'Interpol fait partie des *Applications interopérables* de la Stratégie TRIP de l'OACI, qui comprend des applications d'information frontalière à l'appui des opérations d'inspection. Comme il est indiqué dans son protocole d'accord, le RCP ne couvre pas l'échange de données personnelles connexes figurant dans les passeports électroniques, comme le numéro d'identification du document, qui est l'un des renseignements communiqués dans la série de données obligatoires de la base de données SLTD. Le RCP n'offre donc pas la possibilité d'échanger des certificats pour des renseignements personnels, ce qui aurait permis de le lier à la banque de données d'Interpol. De même, les sessions du RCP se sont tenues durant les trois derniers symposiums de l'OACI sur les MRTD, organisés à Montréal en octobre 2013, 2014 et 2015, et durant les séminaires régionaux TRIP tenus au Burkina Faso (novembre 2013), en Ouzbékistan (avril 2014), au Niger (janvier 2015), en République du Congo (mai 2015) et au Kenya (novembre 2015). Ces sessions portaient essentiellement sur les mesures pratiques d'adhésion au RCP.

6. NOUVEL EXPLOITANT DU RCP

6.1 À l'issue de l'appel d'offres de l'OACI pour l'octroi d'un contrat d'exploitation du RCP en mars 2015, le contrat d'exploitation du RCP a été signé avec Bundesdruckerei GmbH, comme entrepreneur principal chargé de la conception, du développement et de l'exploitation du RCP. Aux termes de ce nouveau contrat, les frais d'inscription pour les nouveaux participants au RCP baisseront de 56 000 USD à 15 900 USD, et les redevances annuelles des participants existants seront également réduites. Il convient de noter que les redevances annuelles des participants diminuent à mesure que le nombre d'adhérents augmente (Figure 3 de l'Appendice A).

7. PRIORITÉS ET PERSPECTIVES : 2017 – 2019

7.1 L'Assemblée est invitée à entériner le programme de travail du RCP de l'OACI pour le prochain triennat, qui a été approuvé par le Conseil et qui est décrit à l'Appendice C.

– – – – – – – – – – – –

APPENDICE A

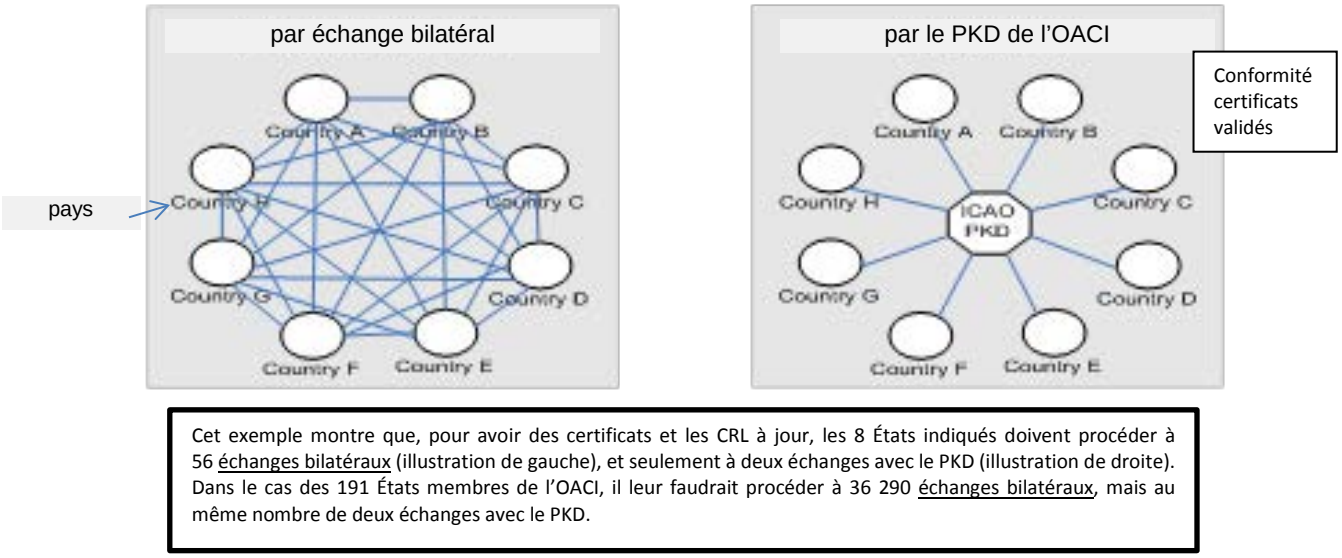

Figure 1. DIFFUSION DES CERTIFICATS

Note.— DSC : Certificat de signataire de documents et CRL = Liste de révocation de certificats

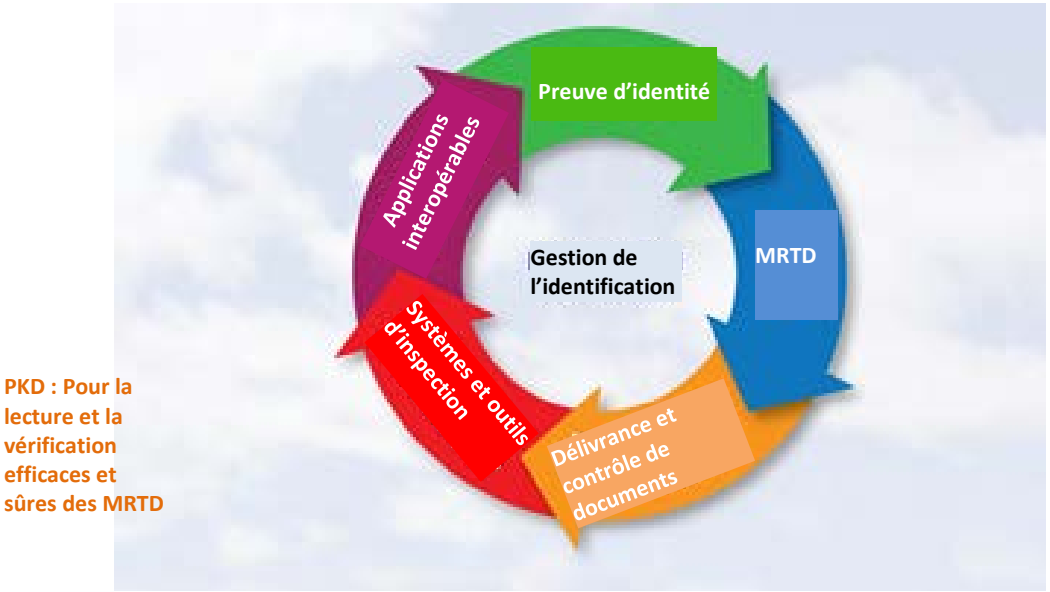

Figure 2. POSITION DU RCP DANS LA STRATÉGIE TRIP DE L'OACI

Frais d'inscription en USD		
2007 à 2008	**2009 à 2015**	**À partir de 2016**
85 000	56 000	15 900
Redevances annuelles en USD		
Nombre de participants au RCP	**2015 et années antérieures**	**À partir de 2016**
45-49	34 000	29 900
50-54	34 000	27 000
55-59	34 000	24 500

Figure 3. FRAIS D'INSCRIPTION ET REDEVANCES ANNUELLES

– – – – – – – – – – – –

APPENDICE B

Numéro du participant au RCP	États et entités participant au RCP	Date d'adhésion		Numéro du participant au RCP	États et entités participant au RCP	Date d'adhésion
1	Australie (Membre de la Commission du RCP)	19/3/2007		27	Norvège	20/6/2011
2	Nouvelle-Zélande (Membre de la Commission du RCP)	19/3/2007		28	Bulgarie	12/10/2011
3	Singapour (Membre de la Commission du RCP)	19/3/2007		29	Luxembourg	30/11/2011
4	Royaume-Uni (Membre de la Commission du RCP)	19/3/2007		30	Suède (Membre de la Commission du RCP)	1/12/2011
5	Japon (Membre de la Commission du RCP)	19/3/2007		31	Nations Unies	14/6/2012
6	Canada (Membre de la Commission du RCP)	19/3/2007		32	Espagne	10/7/2012
7	États-Unis d'Amérique (Membre de la Commission du RCP)	2/11/2007		33	Fédération de Russie	31/8/2012
8	Allemagne	1/11/2007		34	Malaisie (Membre de la Commission du RCP)	9/11/2012
9	République de Corée	28/3/2008		35	Argentine	13/12/2012
10	France	19/6/2008		36	Thaïlande	5/3/2013
11	Chine (République populaire de) (Membre de la Commission du RCP)	26/11/2008		37	Irlande	8/3/2013
12	République du Kazakhstan	19/12/2008		38	République de Moldova	11/6/2013
13	Inde	12/2/2009		39	Belgique	31/10/2013
14	Nigéria (Membre de la Commission du RCP)	13/4/2009		40	Brésil (Membre de la Commission du RCP)	3/1/2014
15	Suisse (Président de la Commission du RCP)	10/7/2009		41	Qatar	10/3/2014
16	Ukraine	30/10/2009		42	Seychelles	14/3/2014
17	Lettonie	28/6/2010		43	Ouzbékistan	19/3/2014
18	La République tchèque	30/6/2010		44	Philippines	21/3/2014
19	Macao, Chine	28/9/2010		45	Iran (République islamique d')	18/5/2014
20	Émirats arabes unis (Membre de la Commission du RCP)	25/10/2010		46	Colombie	19/5/2015
21	Hong Kong, Chine	26/10/2010		47	Roumanie	3/2/2016
22	République slovaque	23/11/2010		48	Finlande	26/2/2016
23	Pays-Bas (Membre de la Commission du RCP)	8/12/2010		49	Bénin	3/3/2016
24	Royaume du Maroc	29/12/2010		50	Botswana	5/4/2016
25	Autriche	31/12/2010		51	Koweït	20/4/2016
26	Hongrie	15/2/2011				

– – – – – – – – – – – –

APPENDICE C

PROGRAMME DE TRAVAIL DU RCP DE L'OACI

Catégories	Priorité	Résultat
Rôle opérationnel de l'OACI	Priorité 1 : Agir en qualité d'agent de fiducie. Prendre régulièrement les mesures voulues pour maintenir l'intégrité des certificats numériques et assurer leur conformité aux normes et pratiques recommandées du Doc 9303, Partie 12, de l'OACI.	Assurer le bon fonctionnement ininterrompu du RCP.
Liste de contrôle de l'OACI	Priorité 2 : Fournir les services d'une liste de contrôle de l'OACI par l'intermédiaire du RCP afin d'appuyer l'interopérabilité de la validation des passeports électroniques à l'échelle mondiale.	Nouveau service offrant aux États un guichet unique pour la validation de toutes les informations des passeports électroniques.
Promotion	Priorité 3 : Donner une emphase plus ciblée à la promotion, par l'envoi de lettres aux États et l'organisation d'ateliers similaires à la Journée RCP aux frontières ou dans le cadre de symposiums et de séminaires TRIP.	Augmenter la participation aux RCP de l'OACI et élargir l'inspection approfondie des passeports électroniques, afin d'assurer un bon rendement du capital investi.
Renforcement de la participation active	Priorité 4 : Encourager tous les membres du RCP à télécharger activement en amont et en aval des données sur les passeports électroniques, afin d'augmenter le nombre de validations de ces passeports via le RCP aux points de contrôle frontalier.	Renforcer l'utilisation active du RCP de l'OACI aux points de contrôle frontalier, dans le cadre d'un plan efficace visant les autorités de contrôle frontalier.
Renforcement du soutien du Secrétariat au RCP	Priorité 5 : Renforcer l'appui du Secrétariat à la Commission du RCP et aux participants en fournissant des outils et des ressources accrus, notamment par l'établissement de CBA.	Assurer que les besoins du RCP sont remplis et que les États reçoivent l'assistance nécessaire.

— FIN —