Foire aux questions

(23 août 2013)

i. Qu’est-ce que le Répertoire de clés publiques (RCP) ?

Le RCP de l’OACI est la plateforme centrale qui permet de gérer à l’échelle mondiale l’échange de certificats et de listes de révocation de certificats. Ces certificats et listes de révocation servent à valider la signature électronique des données figurant dans la puce d'identification par radiofréquence (RFID) des passeports électroniques et autres documents de voyage électroniques lisibles à la machine (DVLM électroniques). Le contenu du RCP est pré-validé et peut être téléchargé gratuitement.

ii. Quelle est la valeur ajoutée du RCP ?

Avec le nombre croissant d’États émettant des passeports électroniques, le RCP garantit

la simplicité et la rapidité du processus d’échange entre les États. Le RCP est crucial pour réduire au minimum le volume de certificats et de listes de révocation de certificats échangés, afin de permettre des téléchargements et téléversements rapides et de vérifier la conformité aux normes techniques en vue d’assurer et de maintenir l’interopérabilité.

iii. Pourquoi est-il important que l’OACI appuie le RCP ?

L’OACI a publié le Document 9303, qui est la principale publication de référence pour les passeports électroniques et autres DVLM électroniques basés sur les normes ISO. Compte tenu des compétences et de la réputation de l’OACI, l’appui dont jouit le RCP est tout à fait naturel et s’imposait de lui-même.

iv. Qui sont les participants au RCP ?

La liste des participants au RCP figure sur le site web du RCP, à l’adresse suivante :

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

(voir « RCP de l’OACI – État opérationnel actuel »)

v. Où peut-on trouver l’Avis de participation ?

L’Avis de participation peut être téléchargé du site web du RCP, à l’adresse suivante :

<http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU(includeslanguageversion(s))/NoticeofParticipation-Model.pdf>

(voir « Procédures du Répertoire de clés publiques de l’OACI »)

vi. Où peut-on trouver l’Avis d’inscription ?

L’Avis d’inscription peut être téléchargé du site web du RCP, à l’adresse suivante :

<http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU(includeslanguageversion(s))/NoticeofRegistration-Model.pdf>

(voir « Procédures du Répertoire de clés publiques de l’OACI »)

Le barème des redevances du RCP peut être téléchargé du site web du RCP, à l’adresse suivante <http://www.icao.int/Security/FAL/PKD/Documents/PKDFinanceDocuments/B-Fin-123-PKD%20Fee%20Schedule%202016.pdf>

: (voir « Barème des redevances du RCP »)

viii. Quelles sont les redevances d’usage ?

Le contenu du RCP peut être téléchargé intégralement, sans frais, en accédant simplement et rapidement à la page web <https://pkddownloadsg.icao.int/>). Toutefois les procédures de contrôle frontalier ou autres applications similaires suivies par les États ou les entités non étatiques qui ne participent pas au RCP peuvent nécessiter le recours à d’autres moyens d’accéder au RCP. L’installation et le maintien de ce genre d’accès exigent une intervention permanente de l’exploitant du RCP et le Protocole d’entente prévoit l’établissement de redevances d’usage pour couvrir les coûts émergents. Le barème des redevances du RCP contient tous les renseignements détaillés.

ix. Qu’entend-on par participation active ?

Une fois l’Avis de participation soumis et les droits d’inscription payés, c’est-à-dire une fois que la participation a pris effet, le participant peut connecter son RCP national au RCP central. Le processus est appuyé par l’exploitant du RCP. À l’issue de cette phase préparatoire, le participant peut commencer à télécharger et téléverser les contenus entre son RCP et le RCP central et il devient ainsi « actif ».

x. Quels sont les contenus que le RCP permet de télécharger ?

Le RCP offre au téléchargement des certificats de signataire de documents (CSD) et des listes de révocation de certificats (LRC), ainsi que des listes de contrôle des certificats ANSC.

xi. Comment peut-on vérifier les passeports électroniques avec le RCP ?

La vérification du passeport électronique se fait au moyen d’une chaîne complète de confiance. La chaîne de confiance repose sur la vérification de la signature électronique de la puce RFID qui est comparée au certificat de signataire de documents (CSD). Elle prévoit également la validation du CSD au moyen du certificat ANSC du pays émetteur. Il s’agit de prouver que tous les éléments de certificat utilisés n’apparaissent pas sur les listes de révocation de certificats (LRC) en vigueur.

xii. Le RCP permet-il d’accéder aux empreintes digitales figurant dans les passeports électroniques ?

Non. Bien que la vérification des signatures des passeports électroniques et l’accès aux empreintes digitales dans les passeports électroniques soient fondés sur la technologie de l’infrastructure des clés publiques (ICP), il est impossible d’accéder aux empreintes digitales au moyen du contenu du RCP.

Une fois que sa participation a pris effet, un participant au RCP dispose d’un délai de

15 mois pour participer activement. Les droits annuels d’une participation active couvrent le coût des activités (voir « Barème des redevances du RCP »).

xiv. Quels avantages y a-t-il à offrir le RCP sur Internet ?

L’échange de certificats et de listes de révocation doit être fiable et effectué en temps utile. Il ne peut pas se faire autrement que par voie électronique. Toutes les mesures appropriées habituelles sont prises pour protéger le RCP contre des attaques par Internet.

xv. Y a-t-il des risques de télécharger des virus ou d’autres programmes malveillants du

RCP ?

Non. Le contenu du RCP est constitué de fichiers de texte qui ne contiennent aucun script ou code d’exécution.

xvi. Où peut-on trouver d’autres informations ?

Le site web du RCP à l’adresse <http://www.icao.int/Security/FAL/PKD/Pages/default.aspx>

contient des renseignements de base pour une première lecture, ainsi que de nombreux documents téléchargeables pour une étude plus poussée. On peut également prendre contact avec le Secrétariat de l’OACI ([ICAO-PKD@ICAO.INT](mailto:ICAO-PKD@ICAO.INT)) ou le Président la Commission du RCP. Il y a même un lien pour soumettre des plaintes ou des observations.

xvii. Le RCP permet de vérifier les signatures numériques dans les puces des passeports électroniques. Comment peut-on s’en servir pour détecter la fraude basée sur la ressemblance ?

Les systèmes biométriques modernes sont capables de comparer en quelques secondes une image faciale entreposée dans un passeport électronique et une image en temps réel du visage d’une personne. Les écarts mêmes légers, typiques des cas de fraude par ressemblance, sont détectés systématiquement, et les personnes visées sont dirigées vers une inspection secondaire.

Le RCP permet la vérification de la signature de la puce d’un passeport électronique pour déterminer l’intégrité des données de la puce, notamment les éléments biométriques. La validation de la puce est essentielle si le contrôle repose sur l’image faciale entreposée dans la puce, surtout aux points de contrôle frontalier qui accueillent des volumes élevés de passagers.

xviii. Le RCP offre-t-il la possibilité d’échanger des certificats aux fins d’accès aux empreintes digitales ?

Le Protocole d’entente du RCP ne couvre pas l’échange de certificats de vérificateur de documents et d’informations connexes sur les données biométriques secondaires dans les passeports électroniques.

xix. Quelle est la valeur ajoutée du RCP pour les États émetteurs de passeports électroniques qui n’appliquent pas de mesures de contrôle frontalier automatisé ?

Une participation active au RCP permet à un État de vérifier les documents de voyage des États participant au RCP. Cela veut dire que les ressortissants de ces États peuvent bénéficier de formalités frontalières facilitées lorsqu’ils voyagent, ce qui représente un avantage concret.

xx. Pourquoi le RCP contient-il des données non conformes aux normes ?

Il y a des passeports électroniques valides en circulation qui ont été délivrés avant que ne prennent effet les nombreuses mesures adoptées par la Commission du RCP pour améliorer la qualité des données. Comme ces passeports ne peuvent être échangés aisément, il faut indiquer clairement les données utilisées pour leur production qui doivent faire l’objet d’une attention particulière durant la validation de la signature de la puce.

xxi. Quelles sont les mesures prises par la Commission du RCP pour améliorer la qualité des données du RCP ?

Les contenus non conformes aux normes téléversés par les participants au RCP ne sont acceptés qu’après avoir été dûment examinés par la Commission du RCP. Un tel examen découle de l’engagement de rectifier toute non-conformité durant une période de transition maximale de six mois. Après cette période de transition, les contenus présentant la même non-conformité seront rejetés. Les participants au RCP peuvent envoyer à l’avance à

l’exploitant du RCP des certificats ANSC ou des certificats de liaison ANSC préalablement à une importation ou un téléversement à des fins de vérification de conformité.

xxii. Que signifie l’expression « moyens diplomatiques strictement protégés (diffusion hors-bande) » ?

La diffusion peut se faire par échanges diplomatiques personnels, valise diplomatique ou toute autre procédure ou moyen similaire. Elle peut également se faire par courrier électronique, site web, etc., sous réserve que le destinataire soit tenu de vérifier l’intégrité du certificat reçu hors-bande, en utilisant par exemple un condensé numérique cryptographique imprimé qui lui aurait été envoyé préalablement par courrier diplomatique.

xxiii. Les certificats ANSC peuvent-ils être publiés sur le site web d’un État sans que cela constitue une infraction aux normes de l’OACI ?

Les certificats sont des informations publiques et en tant que telles, ils peuvent être publiés sur un site web sans que cela constitue une infraction aux normes de l’OACI.

xxiv. Où peut-on trouver des informations techniques pour téléverser des contenus au RCP ?

Toutes les questions techniques et leurs réponses se trouvent dans les documents qui sont envoyés à tous les participants par le Bureau RCP de l’OACI et l’exploitant du RCP. Ces documents peuvent également être téléchargés du site web du RCP. Veuillez consulter en particulier le Règlement du RCP et les Procédures du RCP. On peut aussi télécharger à partir du site web DVLM le Supplément du Doc 9303, qui contient des informations à jour sur les spécifications relatives aux DVLM.

xxv. Comment peut-on différencier les certificats ANSC, les certificats de signataire de documents (CSD) et les listes de révocation de certificats (LRC) de la Chine, de Hong Kong, Chine, et de Macao, Chine ?

Il y a trois points de délivrance de passeports en Chine :

i) un pour la Chine continentale, ii) un pour Hong Kong, Chine, et iii) un pour Macao, Chine.

Ces points de délivrance utilisent le même code de pays ISO 3166 (soit C = CN) dans les certificats ANSC, les CSD et les LRC. En conséquence, les certificats et les LRC sont tous stockés dans le RCP sous le même groupe portant le code de pays « CN ». Les autorités de contrôle frontalier peuvent différencier l’origine des entrées en utilisant à la fois le code de pays (C) et d’organisation (O). Le tableau ci-après montre les attributs des certificats des trois points de délivrance en question.

|  |  |  |
| --- | --- | --- |
| Chine | Macao, Chine | Hong Kong, Chine |
| C = CN | C = CN | C = CN |
| O = Gouvernement chinois | O = RAS Macao | O = Hong Kong Chine |

xxvi. Pourquoi payer pour participer au RCP alors qu’on peut utiliser les listes de contrôle sans frais ?

Les listes de contrôle du RCP couvrent une grande partie de la communauté de pays délivrant des passeports électroniques dans le monde, en termes de certificats ANSC. Ces certificats ANSC permettent de vérifier la chaîne de certificats de l’émetteur du passeport électronique. Les utilisateurs des listes de contrôle qui ne participent pas au RCP doivent cependant tenir compte des éléments suivants:

- La diffusion des certificats de signataire de documents (CSD) et des listes de révocation de certificats (LRC) d’un État reste une question en suspens pour les utilisateurs des listes de contrôle.

- Même si un utilisateur de listes de contrôle construit son unique base de confiance sur une liste centrale téléchargée du RCP, il doit néanmoins gagner la confiance

de l’émetteur de listes de contrôle qui, lui, sera toujours un participant au RCP.

- Les participants au RCP ne sont pas obligés de publier des listes de contrôle ni d’inclure certains certificats ANSC dans ces listes. Ils ne sont pas tenus non plus de mettre à jour les listes de contrôle dans un certain délai après l’émission de nouveaux certificats ANSC. En conséquence, un utilisateur qui se fie uniquement à des listes de contrôle risque d’accepter des certificats ANSC qui ne sont pas ou ne sont plus disponibles.

- Il est vrai que ceux qui ne participent pas au RCP ne payent pas de redevances.

Par contre, les téléchargements qu’ils font sont manuels et non pas automatiques (cf. Barème de redevances du RCP). Cela signifie une intervention humaine continue et un traitement post-téléchargement, qui représentent une différence financière moins élevée que l’on croit entre les participants et les non-participants.

- L’Annexe 9 à la Convention de Chicago contient une pratique recommandée selon laquelle les États contractants de l’OACI qui délivrent ou envisagent de délivrer des passeports électroniques et/ou de mettre en place des moyens automatisés de contrôle frontalier des passeports électroniques devraient

participer au RCP. En outre, le RCP bénéficie du soutien politique de l’OSCE, de l’UE et du G8.

xxvii. En quoi consistent les dispositions de réduction des droits ?

Les droits du RCP sont réduits à mesure que la participation augmente.

Comme il est prévu dans le contrat d’exploitation, les droits de l’exploitant du RCP feront l’objet d’une réduction dès que le nombre de participants au RCP atteindra 31. En conséquence, à compter du 1er janvier 2014, les droits de l’exploitant du RCP seront réduits, passant de 43 000 $US à 34 000 $US. Le contrat d’exploitation prévoit une autre réduction lorsque le RCP atteindra 65 participants.

xxviii. Une autorité de contrôle frontalier peut-elle participer au RCP ?

Oui, une autorité de contrôle frontalier peut participer au RCP. L’article 2.1 du Protocole d’entente du RCP stipule que « tout État contractant de l’OACI » (c’est-à-dire tout État qui a ratifié la Convention de Chicago) qui émet ou envisage d’émettre des DVLM électroniques peut participer au RCP. Le Protocole ne précise pas quelle entité nationale doit se charger de la participation. Il convient cependant de noter qu’une seule entité par État sera chargée d’exécuter le Protocole d’entente et s’engager à s’acquitter des tâches connexes au nom de l’État. Il revient donc à l’État intéressé de prendre la décision souveraine de désigner l’entité nationale qui sera chargée d’exécuter le Protocole. La pratique recommandée figurant au paragraphe 3.9.1 de l’Annexe 9 – Facilitation à la Convention de Chicago encourage expressément les autorités de contrôle frontalier qui appliquent des mesures de vérification automatisée des passeports électroniques à participer au RCP.

– – – – –