



## APERÇU



### Tirer pleinement profit des nouvelles technologies

Chaque passeport électronique contient une puce électronique intégrée où sont stockés la photo et les renseignements personnels du titulaire qui apparaissent sur la page de données du passeport. Les passeports électroniques utilisent la technologie de l'infrastructure à clés publiques (ICP), qui empêche la falsification des informations stockées sur la puce.

Outre les renseignements sur le titulaire, la puce du passeport électronique contient une caractéristique de sûreté numérique particulière connue sous le nom de signature numérique, qui est tirée des certificats de sûreté du pays, à savoir les certificats de signataires de documents (DSC) et le certificat d'AC signataire nationale (CSCA). Ces signatures numériques sont uniques à chaque passeport et pays et peuvent être vérifiées au moyen des certificats de clés publiques du pays émetteur. Lorsque le passeport électronique est scanné et lorsque les données de la puce sont lues, sa signature numérique authentifiée indique aux autorités frontalières que l'information de la puce est authentique, qu'elle a été émise et signée par le pays concerné et qu'elle n'a pas été falsifiée.

### Travailler ensemble

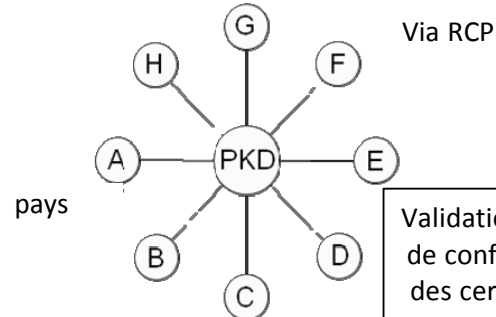
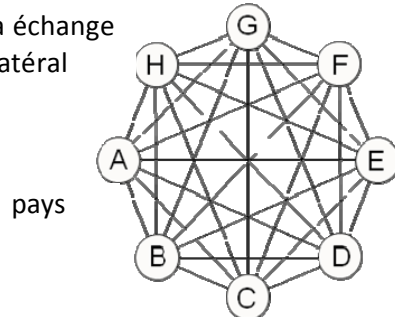
Pour pouvoir les utiliser efficacement, les autorités frontalières et autres doivent avoir accès aux certificats de sûreté de tous les pays qui émettent des passeports électroniques. C'est pourquoi l'Organisation de l'aviation civile internationale (OACI) a créé un système qui facilite le partage des renseignements sur les clés publiques entre les pays, à savoir le Répertoire de clés publiques (RCP) de l'OACI. Tous les participants au RCP peuvent y insérer régulièrement leurs CSCA, DSC, listes des certificats révoqués (LCR) et listes maîtresses en donnant également accès aux certificats de sûreté validés de tous les participants au RCP qui y ont téléchargé les données nécessaires.

Le RCP est un système organisé, simple, sûr et économique de partage de renseignements validés à jour. Sans le RCP, les pays doivent s'adresser l'un à l'autre pour échanger en toute sécurité leurs DSC et LCR et le partage de certificats, qui demanderait ainsi des centaines de transactions et d'heures de travail, peut grâce au RCP s'accomplir en deux échanges seulement – le transfert et le téléchargement de renseignements validés. En outre, les listes maîtresses disponibles, qui contiennent les CSCA validés d'autres pays, vous donnent accès aux CSCA même si l'échange initial de CSCA n'a pas été fait avec tous les pays.

---



## APERÇU

Via échange  
bilatéral

Un autre avantage précieux que le RCP offre à ses participants est un service de validation de conformité des certificats. L'assurance mondiale de conformité et d'origine du certificat permet de faciliter la vérification du document de voyage et de faire en sorte que les voyages se déroulent sans problèmes.

Le RCP de l'OACI ne contient de renseignements personnels sur aucun titulaire de passeport et ne donne pas accès aux éléments biométriques secondaires de la puce du passeport comme les empreintes digitales.

### Ouvrir les portes aux voyageurs

Tous les pays, et pas seulement les participants au RCP, peuvent y accéder gratuitement<sup>1</sup>. Ce répertoire de partage de renseignements permet aux autorités frontalières de tous les pays qui ont mis leur infrastructure de contrôle frontalière en contact avec le RCP de valider rapidement les passeports électroniques, ce qui facilite grandement l'entrée des voyageurs légitimes. Ce système aide aussi toutes les nations à travailler ensemble pour combattre la fraude de passeports et contribuer à la sécurité nationale et internationale.

Pour de plus amples renseignements, prière de consulter le site web du RCP :

<http://www.icao.int/Security/FAL/PKD/Pages/default.aspx>

ou de contacter le :

Bureau du Répertoire de clés publiques de l'OACI

[ICAO-PKD@ICAO.INT](mailto:ICAO-PKD@ICAO.INT)

<sup>1</sup> L'accès gratuit est conçu pour des téléchargements occasionnels et non pas pour le contrôle frontalier, qui exige une intervention régulière de l'opérateur RCP, et n'offre pas d'appui technique.