



ASSEMBLÉE — 42^e SESSION

COMITÉ EXÉCUTIF

Point 12 : Programmes de facilitation

POSSIBILITÉS D'AMÉLIORER LA MISE EN ŒUVRE DU RÉPERTOIRE DE CLÉS PUBLIQUES (RCP) ET DES PASSEPORTS ÉLECTRONIQUES DANS LES CONTRÔLES AUX FRONTIÈRES

[Note présentée par la République argentine avec l'appui du Belize, de la Bolivie (État plurinational de), du Chili, de la Colombie, de Cuba, de la République dominicaine, de l'Équateur, d'El Salvador, du Guatemala, du Honduras, de la Jamaïque, du Mexique, du Nicaragua, du Panama, du Pérou et de l'Uruguay]

RÉSUMÉ ANALYTIQUE

La mise en œuvre du répertoire de clés publiques (RCP) de l'Organisation de l'aviation civile internationale (OACI) et l'utilisation de passeports électroniques ont amélioré la sûreté et l'efficacité des contrôles aux frontières. Toutefois, des possibilités d'amélioration ont été mises en évidence qui, avec un soutien accru de l'OACI, pourraient faciliter la transition vers ces systèmes et leur intégration dans les pays qui se trouvent actuellement au stade du développement ou de la mise en œuvre.

Défis liés à la mise en œuvre du RCP :

- a) difficultés d'accès et d'utilisation du RCP : certains pays rencontrent des difficultés techniques et administratives pour intégrer le RCP dans leurs systèmes nationaux en raison d'un manque d'infrastructures ou d'expertise ;
- b) contraintes d'interopérabilité : l'absence de normes plus souples pour l'intégration avec d'autres infrastructures nationales crée des obstacles techniques à la validation des passeports,
- c) mise à jour et maintenance : certains pays ne téléchargent pas régulièrement les certificats et les listes de révocation de certificats, ce qui peut compromettre la sécurité et la fiabilité du système.

Suite à donner : L'Assemblée est invitée à demander à l'OACI de renforcer son rôle par les actions suivantes :

- a) assistance technique personnalisée : mettre en place des programmes spécifiques de formation et d'assistance technique pour les pays se trouvant au stade de la mise en œuvre, en accordant une attention particulière aux meilleures pratiques et à l'utilisation optimale du RCP ;
- b) plateforme de validation centralisée : étudier la possibilité de bâtir un système sécurisé de renseignements préalables concernant les voyageurs (RPCV) que les pays puissent utiliser pour consulter en ligne et en temps réel les certificats et les listes de révocation de certificats, comme solution complémentaire aux téléchargements courants ;
- c) coopération régionale : promouvoir l'intégration régionale au moyen d'accords de partage en matière d'infrastructures et de connaissances techniques afin de réduire les coûts et de faciliter l'adoption du RCP.

¹ Version en espagnol fournie par l'Argentine

<i>Objectifs stratégiques :</i>	La présente note de travail se rapporte aux objectifs stratégiques <i>Chaque vol est sûr et sécurisé et L'aviation assure une mobilité fluide, accessible et fiable pour tous.</i>
<i>Incidences financières :</i>	Les activités décrites dans la présente note dépendront de la disponibilité de ressources dans le budget ordinaire 2025-2026 et de contributions extrabudgétaires.
<i>Références :</i>	

1. INTRODUCTION

1.1 Lorsqu'un pays enregistre son autorité de certification signataire nationale (ACSN) dans le répertoire de clés publiques (RCP) de l'Organisation de l'aviation civile internationale (OACI), les points de contrôle frontaliers de ce pays et d'autres pays doivent prendre un certain nombre de mesures et utiliser les technologies appropriées pour tirer parti de la sécurité implicite des certificats signés pour les documents de voyage lisibles à la machine (DVLM) électroniques (DVLM-e).

1.1.1 Télécharger et gérer les certificats de l'ACSN et les certificats de signataire de document (CSD)

1.1.1.1 Les pays qui vérifient les documents de voyage doivent régulièrement télécharger les certificats d'ACSN et les certificats de signataire de document (CSD) à partir du RCP OACI.

1.1.1.2 L'ACSN est l'émetteur certifié qui délivre les CSD, qui sont les certificats utilisés pour signer les données sur les puces des passeports électroniques.

1.1.1.3 Note sur le CSD : il s'agit du certificat numérique délivré par l'ACSN au signataire du document. Le CSD contient la clé publique du signataire du document. Lorsqu'un passeport électronique est inspecté, le système d'inspection utilise la clé publique du CSD pour vérifier la signature numérique des données du passeport et s'assurer que les données n'ont pas été falsifiées et qu'elles proviennent de l'autorité de délivrance légitime.

1.1.2 Mettre à jour les bases de données des points de contrôle frontaliers

1.1.2.1 Les certificats téléchargés doivent être distribués à tous les systèmes d'inspection des documents aux aéroports, dans les ports et les autres points d'entrée.

1.1.3 Utiliser l'authentification passive

1.1.3.1 L'authentification passive vérifie l'intégrité des données contenues dans la puce du document de voyage ; aux points de contrôle, les lecteurs de passeport vérifient que les données stockées dans la puce n'ont pas été falsifiées en comparant la signature numérique au CSD correspondant.

1.1.4 Mettre en œuvre l'authentification active (facultatif)

1.1.4.1 Certains passeports électroniques utilisent l'authentification active pour empêcher le clonage de puce. Il s'agit d'un défi cryptologique entre le lecteur et la puce pour confirmer qu'elle est authentique et qu'il ne s'agit pas d'une copie.

1.1.5 Utiliser le contrôle d'accès étendu (EAC) (pour les données biométriques protégées)

1.1.5.1 Pour accéder aux données biométriques sensibles, telles que les empreintes digitales, les systèmes de contrôle aux frontières doivent utiliser l'EAC. L'EAC exige que les lecteurs disposent de certificats autorisés et échangent des clés pour vérifier les permissions d'accès aux données biométriques.

1.1.6 **Infrastructure à clé publique (ICP)**

1.1.6.1 Pour valider les certificats, il faut une infrastructure à clé publique (ICP) capable de vérifier la chaîne de confiance entre l'ACSN et le CSD ainsi que la signature de la puce. Il peut s'agir :

- a) des listes de révocation de certificats (CRL) pour détecter les certificats révoqués ;
- b) du protocole OCSP (Online Certificate Status Protocol) pour une validation en temps réel.

1.1.7 **Inspection des listes de documents de voyage volés ou perdus (SLTD)** de l'Organisation internationale de police criminelle (INTERPOL)

1.1.7.1 Les systèmes de contrôle aux frontières devraient également consulter les bases de données internationales, telles que la SLTD d'INTERPOL, pour détecter les documents de voyage déclarés perdus ou volés.

2. **RÉSUMÉ**

2.1 Pour que les services de contrôle aux frontières puissent bénéficier de la sécurité implicite des certificats de documents de voyage après l'adhésion d'un pays au RCP OACI, ils doivent :

- a) télécharger et mettre à jour régulièrement les certificats d'ACSN et les CSD à partir du RCP ;
- b) distribuer ces certificats aux systèmes de contrôle aux frontières ;
- c) mettre en œuvre l'authentification passive pour vérifier l'intégrité des données de la puce ;
- d) utiliser l'authentification active ou l'EAC selon le cas ;
- e) tenir à jour l'ICP pour valider la chaîne de confiance du certificat ;
- f) intégrer des outils de détection des documents perdus ou volés.

2.2 Ces mesures garantissent l'authenticité des passeports électroniques et préviennent la fraude documentaire lors des contrôles d'immigration.

2.3 L'utilisation incorrecte de l'infrastructure du RCP OACI pour vérifier l'authenticité des passeports électroniques ouvre la voie à plusieurs possibilités de fraude. Les fraudes les plus courantes sont notamment les suivantes.

2.3.1 **Usurpation d'identité à l'aide de passeports frauduleux**

2.3.1.1 Passeports entièrement contrefaits : des individus pourraient créer des passeports électroniques qui semblent authentiques mais qui contiennent de fausses informations biographiques et biométriques. En l'absence de vérification par rapport au RCP, qui permet de confirmer que le CSD est légitime et délivré par une autorité reconnue, ces documents falsifiés seraient plus difficiles à détecter.

2.3.1.2 Passeports modifiés : les passeports électroniques authentiques peuvent être falsifiés, en modifiant la photographie ou les informations biographiques dans la zone visuelle ou même sur la puce. En

l'absence de vérification de la signature numérique au moyen du RCP, ces modifications pourraient ne pas être détectées.

2.3.1.3 Utilisation frauduleuse de passeports authentiques : les passeports volés ou perdus peuvent être utilisés par des personnes autres que les titulaires légitimes. Si les systèmes de contrôle ne vérifient pas la validité du certificat de passeport au moyen du RCP (et éventuellement par rapport à des listes de documents volés ou perdus), la fraude sera plus facile.

2.3.2 **Manipulation des données de la puce**

2.3.2.1 Bien que les passeports électroniques comportent des mesures de sûreté, sans vérification du RCP, un pirate informatique disposant des outils appropriés pourrait altérer les données stockées sur la puce, y compris les informations biographiques et biométriques. La vérification au moyen du RCP garantit l'intégrité de ces données en confirmant la validité de la signature numérique.

2.3.3 **Réutilisation de l'identité**

2.3.3.1 Un individu pourrait tenter d'utiliser plusieurs passeports électroniques frauduleux sous différentes identités pour franchir les frontières à plusieurs reprises ou commettre d'autres délits. L'absence de vérification par rapport au RCP rend difficile la détection de ces incohérences au niveau international.

2.3.4 **Attaques contre la chaîne de confiance**

2.3.4.1 En l'absence de RCP comme point central de confiance, la vérification de l'authenticité des passeports dépend davantage des accords bilatéraux ou de la fiabilité des informations fournies par les différents pays. Cela rend le système plus vulnérable à l'infiltration par des certificats frauduleux si des normes de sûreté rigoureuses ne sont pas maintenues à l'échelle mondiale. Le RCP constitue une infrastructure solide pour atténuer ce risque.

2.3.5 En résumé, l'infrastructure du RCP est essentielle à l'établissement d'une chaîne de confiance mondiale pour l'authentification des passeports électroniques. Sans cela, les contrôles aux frontières sont beaucoup plus vulnérables à toute une série de fraudes sophistiquées qui exploitent la difficulté de vérifier l'authenticité des documents et l'identité des voyageurs internationaux. La mise en œuvre du RCP permet aux autorités de contrôle de confirmer qu'un passeport électronique a été délivré par une autorité légitime et que ses données n'ont pas été altérées.

3. **CONCLUSION**

3.1 Une mauvaise mise en œuvre du RCP OACI expose les contrôles aux frontières à un risque élevé de fraude documentaire, comme l'usurpation d'identité et la manipulation des données des passeports électroniques. L'absence de mise à jour et de vérification des certificats compromet la chaîne de confiance, ce qui porte atteinte à la sûreté mondiale. Pour atténuer ces risques, il est essentiel de renforcer l'assistance technique, d'améliorer l'interopérabilité et de créer des outils centralisés pour garantir une validation efficace et en temps réel.