Organisation de l'aviation civile internationale

FALP/5-WP/3
14/2/08

NOTE DE TRAVAIL

GROUPE D'EXPERTS DE LA FACILITATION (FALP)

CINQUIÈME RÉUNION

Montréal, 31 mars – 4 avril 2008

Point 3 : Autres amendements de l'Annexe 9

FACILITATION DES PASSAGERS ET LE RCP DE L'OACI

(Note présentée par la Commission du RCP OACI[*])

AVERTISSEMENT

Faute de ressources, seuls le sommaire, la suite à donner par le Groupe FAL et les amendements de l'Annexe 9 ont été traduits.

SOMMAIRE

L'inclusion de données biométriques dans les passeports électroniques offre la possibilité d'automatiser le processus de congé des passagers, notamment la confirmation d'identité et les vérifications initiales des listes d'alerte. Ces possibilités sont déjà exploitées dans un certain nombre de pays (ex : Singapour, Portugal et Australie). Néanmoins, l'automatisation de certains éléments du congé des passagers ne présente d'avantages pour la facilitation que si le niveau de confiance dans l'intégrité des passeports électroniques présentés comme pièces d'identité est élevé, tout comme le niveau de compréhension du processus de validation du RCP. La validation des passeports électroniques par le RCP est essentielle, car elle confirme qu'il s'agit de documents authentiques émis par une autorité émettrice de bon aloi et qui n'a pas fait l'objet d'altérations ultérieures. Ouvrir la puce d'un passeport électronique et en vérifier les données qui y sont inscrites sans passer par l'étape de validation ne donne pas le même degré de confiance que celui offert par la validation. Le RCP de l'OACI est le véhicule logique et préféré pour gérer l'échange des certificats numériques qui permet une validation efficace par le RCP des passeports électroniques présentés aux postes de contrôle frontaliers. Le RCP de l'OACI est devenu opérationnel en mars 2007.

Suite à donner par le Groupe FAL :

Le Groupe FAL est invité à examiner et à approuver les amendements de l'Annexe 9 présentés au paragraphe 3.1.

[*] Australie, Canada, États-Unis, Japon, Nouvelle-Zélande, Royaume-Uni et Singapour.

1. INTRODUCTION

1.1 The introduction of ePassports is intended to improve both aviation security, by combating identity fraud, and passenger safety/facilitation by offering an opportunity to improve the efficiency of aviation operations by enabling identification checks in passenger clearance processes at the primary control to be automated. Moreover, the security and process efficiency benefits of ePassports are equally applicable for international travel by sea and land.

1.2 An essential element in the introduction of ePassports is the implementation of a global system for ePassport validation achieved via the exchange of Public Key Infrastructure (PKI) certificates. The system is privacy enhancing. It does not require or involve any exchange of the personal data of passport holders and the validation transactions help combat identity theft.

2. DISCUSSION

2.1 The business case for validating ePassports is compelling. Border control authorities can confirm that the document held by the traveller:

· was issued by a *bona fide* authority.
· has not subsequently been altered.
· is not a copy (cloned document).
· if the document has been reported lost or has been cancelled, the validation check can confirm whether the document remains in the hands of the person to whom it was issued.

2.2 As a result, Passport issuing authorities can better engage border control authorities in all participating countries in identifying and removing from circulation bogus documents. It is important to stress that only by validating ePassports will the assurances set out at 2.1 above be met. Opening the ePassport chip without validating it does not provide that same level of assurance.

2.3 ePassport validation is therefore an essential element to capitalise on the investment made by States in developing ePassports to contribute to improved border security and safer air travel globally. Because the benefits of ePassport validation are collective, cumulative and universal, the broadest possible implementation of a scheme of ePassport validation is desirable.

2.4 The exchange of PKI certificates (and the exchange of the certificate revocation lists that are the essential recovery layer in the system) must be reliable and timely. The emerging consensus is that this exchange cannot be achieved by other than electronic means. Since the system of ePassport validation must also operate on an open ended, indefinite basis it is apparent that a central broker is required. ICAO is the logical candidate to perform this role because it is accepted globally as the agency responsible for setting and managing travel document standards.

2.5 The number of ePassports in circulation is approaching a tipping point where border control authorities will reap returns from the investments required in systems hardware and integration to support ePassport PKI validation. Validation of ePassports enables automation of identity and warning list checking of ePassport holders to be undertaken with confidence. Without PKI or alternative database validation checks and effective checks for lost and stolen passports, any such automation would be higher risk.

2.6 It is for all these reasons that the 2007 ICAO Assembly resolved to urge all ICAO ePassport issuing States to join the ICAO PKD.

3. SUITE À DONNER PAR LE GROUPE FAL

3.1 Le Groupe FAL est invité à examiner et à approuver les propositions d'amendement ci-après de l'Annexe 9 :

a) définitions des termes « Passeport électronique » et « Répertoire OACI de clés publiques (RCP) » à ajouter au Chapitre premier de l'Annexe 9 :

« ***Passeport électronique (ou PLM activé électroniquement) :*** Passeport lisible à la machine (PLM) conforme aux spécifications du Doc 9303, Volume 1 de la 1re Partie, qui incorpore en outre un circuit intégré sans contact permettant l'identification par des fonctions biométriques du titulaire du passeport, conformément aux spécifications du Doc 9303, Volume 2 de la 1re Partie. »

« ***Répertoire OACI de clés publiques (RCP OACI) :*** Base de données centrale servant, d'une part, de répertoire de certificats de signataire de documents (C_{SD}) (contenant les clés publiques du signataire de documents), de listes de contrôle de l'ANSC, de certificats de liaison de l'Autorité nationale de signature de certificat (CL_{ansc}) et de listes de révocation de certificats émis par les Participants, et d'autre part, de système de diffusion mondiale, maintenue par l'OACI au nom des Participants dans le but de faciliter la validation des données figurant dans les passeports électroniques. »

b) nouvelle Pratique recommandée à ajouter au Chapitre 3 de l'Annexe 9 :

3.9.1. « **Pratique recommandée.—** *Il est recommandé que les États contractants a) qui émettent ou ont l'intention d'émettre des passeports électroniques et/ou b) qui appliquent des mesures de vérification automatiques aux postes de contrôle frontaliers, adhèrent au Répertoire de clés publiques (RCP) de l'OACI. »*

— FIN —