International Civil Aviation Organization

FALP/5-WP/3
14/02/08

WORKING PAPER

FACILITATION PANEL (FALP)

FIFTH MEETING

Montréal, 31 March to 4 April 2008

Agenda Item 3: Other amendments to Annex 9

PASSENGER FACILITATION AND THE ICAO PKD

(**Presented by the ICAO PKD Board**[*])

SUMMARY

The inclusion of biometric information in ePassports creates the opportunity for automating aspects of the passenger clearance process, including confirmation of identity and primary checking against alerts. These opportunities are already being exploited in a number of countries (e.g. Singapore, Portugal and Australia). However, the facilitation benefits of automating aspects of passenger processing can only be gained where there is a high level of confidence in the integrity of the ePassport being presented as evidence of identity and a level of understanding of how this can be achieved through the PKI validation process. ePassport PKI validation is essential as it confirms that the document is a genuine issue from a *bona fide* issuing authority that has not subsequently been altered. Opening the ePassport chip and comparing the data on the chip without the validation step does not provide the level of assurance that validation provides. The ICAO PKD is the logical and preferred vehicle for managing the exchange of the digital certificates that enable effective ePassport PKI validation to be undertaken at border controls. The ICAO PKD became operational in March 2007.

Action by the FAL Panel:

The FAL Panel is invited to consider and agree to the amendments to Annex 9 set out in Paragraph 3.1.

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.

[*] Australia, Canada, Japan, New Zealand, Singapore, United Kingdom and United States

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. ACTION BY THE FAL PANEL

3.1 The FAL Panel is invited to consider and agree to the following proposed amendments to Annex 9:

a) Definitions for the terms “ePassport” and “ICAO Public Key Directory (PKD)” be inserted in Chapter 1 of Annex 9 as follows:

“***ePassport (or Electronically enabled MRP)*:** A Machine Readable Passport (MRP) conforming to the specifications of Volume 1 of Part 1 of Doc 9303, which additionally incorporates a contactless integrated circuit including the capability of biometric identification of the MRP holder confirming to the specifications in Volume 2 of Part 1 of Doc 9303.”

*"**ICAO Public Key Directory (ICAO PKD):*** the central database serving as the repository of Document Signer Certificates (C_{DS}) (containing Document Signer Public Keys), CSCA Master List, Country Signing CA Link Certificates(lC_{CSCA})and Certificate Revocation Lists issued by Participants, together with a system for their distribution worldwide, maintained by ICAO on behalf of such Participants in order to facilitate the validation of data in ePassports."

b) A new Recommended Practice be inserted in Chapter 3 of Annex 9, as follows:

3.9.1 "**Recommended Practice.—** *Contracting States (a) issuing or intending to issue ePassports; and/or (b) implementing at border controls automated checks on ePassports should join the ICAO Public Key Directory (PKD).*"

— END —