International Civil Aviation Organization
ICAO South American Regional Office
Eleventh Meeting of the Civil Aviation Authorities of the SAM Region (RAAC/11)
(Santiago, Chile, 6 – 8 May 2009)

Agenda Item 6: Other matters

ICAO PUBLIC KEY DIRECTORY

(Presented by the Secretariat)

SUMMARY

The administration of the ICAO Public Key Directory (ICAO PKD) is one of the expected outputs of Strategic Result JF-1 in ICAO's current Business Plan. The PKD system contributes to:

- facilitation of traffic of persons and goods;
- improved security for travelers; and
- promotion of efficient border crossing.

1. Introduction

1.1 The Public Key Directory Memorandum of Understanding (PKD MoU) came into effect on 8 March 2007. To date, out of the sixteen States who have sent ICAO Participation Notices to the PKD, fourteen States have paid their registration fee and have become participants in the PKD. They are: Australia, Canada, China, France, Germany, India, Japan, Kazakhstan, Korea (Republic of), New Zealand, Nigeria, Singapore, United Kingdom and United States.

1.2 The PKD participants believe that ICAO is the most appropriate host for the PKD. Having ICAO as a central broker minimizes the volume of exchange of certificates among the States and, as a United Nations agency, the Organization represents the best vehicle for achieving a sustainable global scheme.

1.3 The PKD allows document inspectors of ePassports at borders throughout the world to access the Directory and use the public keys to validate ePassports. Validating ePassports with these public keys reveals manipulations of the contactless chip integrated in the passport. As the number of States issuing ePassports has grown to above 60 worldwide, the alternative of each State managing on a bilateral basis, the exchange of certificates and lists with all other States would become unimaginable. The PKD's central role is critical in minimizing the volume of certificates being exchanged, ensuring timely uploads and managing adherence to technical standards with a view to ensuring interoperability is achieved and maintained.

1.4 During the year 2008, four PKD Board meetings were held in: Christchurch, New Zealand (Feb 2008); Montréal, Canada (May and October 2008) and Bern, Switzerland (in September 2008). In 2009, there was a PKD Board meeting held in Brussels, Belgium (23 to 24 March 2009). These meetings resulted in a review of the technical amendments to the PKD MoU as well as amendment proposed by China. In addition, further refinements to the Public Key

Infrastructure (PKI) Validation approach were discussed. The budget for 2009 was approved and extensive discussions and negotiations of the Operational Contract were handled leading to the signing of the Operational Contract in December 2008, officially launching the ICAO PKD into the operational phase.

2. Participation in the PKD

2.1 Participation in the ICAO PKD has been growing. States that have most recently joined are China, India, Kazakhstan and Nigeria, while Moldova and Cyprus have sent their Notice of Participation in the ICAO PKD, but have not yet paid their Registration Fee.

2.2 The first fifteen States to join the ICAO PKD and are current with their fee payment constitute the PKD Board, while beyond fifteen states, membership will rotate.

2.3 Pursuant to Section 3 of Appendix C of the PKD MoU, Germany took over the chairmanship of the PKD Board from Australia for a one-year term during the sixth PKD Board meeting in May 2008 and was re-elected during the seventh meeting in March 2009.

2.4 The major challenge facing the ICAO PKD is the expansion of its membership so that other States considering membership can be confident they are joining a viable, global solution.

3. Technical Design

3.1 The PKD is a database into which digital signatures containing public keys from States issuing ePassports can be deposited, and from which States and airlines might download into their own systems for use in the inspection and verification of authenticity of the passports presented to them. The ICAO PKD is designed to provide a centralized distribution of electronic keys for decryption of the digital signatures on data loaded by issuing States on the integrated circuit chips (ICs) to be imbedded into these passports.

3.2 Germany proposed an amendment to the PKD Board, which was approved, advocating a modified approach to ePassport validation. The modified approach is based on countersigning the Country Signing CA certificates of issuing States by other States, and distributing the countersigned CSCA certificates via the ICAO PKD to support, but not to replace, bilateral distribution of self-signed certificates.

3.3 Subsequently, detailed work refined the modified approach to ePassport PKI validation by the introduction of the concept of “CSCA Master List” to replace the earlier proposed CSCA Cross Certificates. A “CSCA Master List” is a list of CSCAs that is produced by a State and is relied on in the inspection process. Compiling this list is based on diplomatic exchanges and subsequent verification processes. A State may countersign, and publish in the ICAO PKD, its Master List of received certificates as part of the diplomatic exchange. A State may, at its own discretion, choose to rely upon the information on the CSCA Master List to verify the received certificates.

3.4 As a result of this proposal, and the participants’ experiences to date, the PKD Board proposed changes to the PKD MoU which were approved by the Council of ICAO in November 2008.

4. **Cost of participation**

4.1 A number of countries have expressed the view that the level of the ICAO PKD Registration and Annual fees is an obstruction to membership.

4.2 With the signing of the Operational Contract in December 2008, and the ICAO Council approval, the registration fee has been reduced from U.S. $85,000 to U.S. $56,000.

4.3 The annual fee is inversely related to the number of participants. The higher the number of participants, the lower the annual fee. Annual Fee is set to recover ICAO and Operator's operating costs. As of January 2009, the annual fee set by the PKD Board was US $74 200 for a full year of activity and is pro-rated to take into account the time of joining.

5. **Action by RAAC/11**

5.1 The RAAC/11 Meeting is invited to note this information paper.

— END —