HLCAS-WP/8
6/6/12

International Civil Aviation Organization

WORKING PAPER

HIGH-LEVEL CONFERENCE ON AVIATION SECURITY (HLCAS)

Montréal, 12 to 14 September 2012

Agenda Item 7: The role of the Machine Readable Travel Document (MRTD) Programme, Advance Passenger Information (API) and Passenger Name Record (PNR)

THE PUBLIC KEY DIRECTORY (PKD)

(Presented by the Secretariat)

SUMMARY

This paper presents information on the ICAO Public Key Directory (PKD). Currently, the PKD comprises 30 participants, and ICAO encourages all Member States to join the PKD to enhance the efficiency and effectiveness of ePassport checks.

Action: The High-level Conference on Aviation Security is invited to endorse the recommendations in paragraph 6.

1. INTRODUCTION

1.1 An electronic passport (ePassport), also known as a biometric passport, is similar to a traditional Machine Readable Passport (MRP) but contains an electronic chip that is encoded with the same information found on the data page of a passport. The electronic chip is digitally signed and, therefore, increases security, providing greater protection against tampering, thus reducing the risk of fraud.

1.2 An ePassport is only as good as the biometric and biographic information contained on its chip. Information on the chip, in turn, is only useful if it can be validated quickly and securely. It is estimated that 350 million ePassports are in circulation today, issued by 93 States. This has brought into question the practicability of bilaterally exchanging electronic signatures that vouch for the validity of ePassport data signatures stored in the chip.

1.3 In response, under the aegis of the International Civil Aviation Organization (ICAO) and at the request of Member States, the PKD was established. The PKD is a central repository of digital signatures that simplifies and facilitates multilateral exchanges of ePassport chip signature validation information.

2. ICAO ROLE

2.1 The Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) recommended that ICAO be the designated organization to establish the PKD. This recommendation was based on the Organization’s long track record as the developer of MRTD Standards, its international stature as a United Nations specialized agency, and its substantial interest in document security. A neutral site overseen by the PKD Board and funded by the ePassport issuing States was deemed to provide a trusted resource from which government inspection agencies, airlines, and other entities in all Member

States might download all public keys in circulation for the purpose of verifying the authenticity of passports as documents of identity.

2.2 The oversight of a central PKD by the PKD Board provides a cooperative, interoperable regime for ePassport security that is accessible to all ICAO participating Member States. Of equal importance is a PKD that is centrally accessible to aircraft operators that serve on the "front line" as the first to examine the passports of travelers. As a means of preventing the alteration or counterfeiting of passports, or the use of stolen passports by imposters, the PKD provides a highly effective security measure.

2.3 The PKD Board is the standing body responsible of the ICAO PKD. It is composed of 15 Members that are appointed by the Council of ICAO consistent with the provisions of the PKD Memorandum of Understanding (MoU). The PKD Board is responsible for the financial and operational oversight of the ICAO PKD.

2.4 The main role of ICAO is to act as a Trust Agent, validating the sources and data integrity of the digital signatures, and safeguarding public keys. Validating the source means determining that a digital signature or a public key was issued by the proper authority. ICAO also has the responsibility to provide operational and administrative support to the PKD Board.

3. BENEFITS OF THE ICAO PKD

3.1 The ICAO PKD promotes the global interoperability of the validation system for electronic travel documents. It acts as a central broker, managing the multilateral exchange of certificates and certificate revocation lists, which are used to validate the digital signature on the chip within an ePassport. With the use of the PKD, any attempt to alter or add to data on a chip in an ePassport is immediately detected when checks are made. Today, the PKD is recognized as a valuable instrument, without a sensible alternative, for implementing the specifications established in *Machine Readable Travel Documents* (Doc 9303).

3.2 PKD participation ensures that timely information is available to validate ePassport authenticity, thereby simplifying and enhancing the security of the ePassport validation process at border control points, and with the result of facilitating fast and secure cross-border movement. It is only when using an ePassport reader at border control that the authenticity of the ePassport can be confirmed as not having been altered or counterfeit.

3.3 The PKD is cost-effective and efficient. Currently, the one-time registration fee is US $56,000. There is also a recurring annual fee of approximately US $56,000, used to cover the PKD Operator costs of operation (US $43,000) and ICAO administrative costs (US $13,000). These annual fees are quite minor, considering the investment required to maintain a bilateral infrastructure to connect to all ePassport issuing States and to deploy electronic readers. Sharing such data via the PKD streamlines the validation process and reduces related administrative costs, while adherence to international standards is achieved. As well, costs are further reduced as more States become participants.

4. PARTICIPATION

4.1 In the course of 2011, five States – Bulgaria, Hungary, Luxembourg, Norway and Sweden – joined the PKD. Together with Australia, Austria, Canada, China, Czech Republic, France, Germany, Hong Kong Special Administrative Region China, India, Japan, Kazakhstan, Latvia, Macao Special Administrative Region China, Morocco, the Netherlands, New Zealand, Nigeria, Republic of Korea, Singapore, Slovakia, Switzerland, Ukraine, the United Arab Emirates, the United Kingdom and the United States, there are currently 30 PKD participants.

4.2 Nevertheless, there is still a significant gap between the number of ePassport-issuing States and the number of PKD participants. The major challenge facing the PKD is to expand participation so that States can be confident they are joining a viable, global solution.

4.3 As an effective measure of ongoing promotion, a PKD workshop was organized during the Seventh Symposium and Exhibition on ICAO Machine Readable Travel Documents (MRTDs), Biometrics and Security Standards, held in Montréal in September 2011. Similar events were organized during MRTD Regional Seminars held in Qatar (November 2011), Singapore (December 2011) and Brazil (April 2012). The workshops enjoyed high attendance and were directed towards practical steps on how to join the PKD.

5. OPERATION AND ADMINISTRATION

5.1 The PKD has been developed and operated on a cost-recovery financial model, fully supported by fees from States participating in the directory.

5.2 For the complete design, development and operation of the PKD, a contract was awarded to Netrust in 2006. The PKD started operations in March 2007, and PKD services are provided to all participants, and to other commercial and general users around the world. The operational contract with Netrust was successfully completed and accepted by ICAO and the PKD Board.

5.3 The contract ending 31 December 2011 has been extended for another three years effective 1 January 2012. A major feature of the extended operational contract is the reduction of the PKD operations fee, currently US $43,000, by approximately US $12,000 to reach around US $31,000 per participant and per year once the number of active PKD participants reaches 31. Another reduction is expected when the number of active PKD participants reaches 65.

5.4 For 2012, ICAO PKD-related staff costs, travel, and professional liability insurance will be funded by the 2011 ICAO Regular Programme Budget surplus. This funding will reduce costs for the PKD participants in the current year. Subject to budgetary considerations, similar funding for the PKD could be secured in 2013 as well.

5.5 The management and administrative work of the PKD resulted in three meetings of the PKD Board in 2011. The efficiency of the administrative, financial and technical regime that ensures the smooth operation of the PKD as required by the Memorandum of Understanding has been refined and extended where necessary. This includes, but is not limited to, the determination of the composition of the PKD Board and the financial regulations.

6. RECOMMENDATIONS

6.1 The HLCAS is invited to recommend that States:

a) participate in the PKD;

b) issue ePassports; and

c) implement automated border control checks using ePassport readers.

— END —