MINISTERIAL CONFERENCE ON AVIATION SECURITY AND FACILITATION IN AFRICA

WINDHOEK, NAMIBIA, 4-8 April 2016

Agenda item 1.6: Introduction to Public Key Directory (PKD)

THE ICAO PUBLIC KEY DIRECTORY (PKD)

(Presented by the Secretariat)

SUMMARY
The ICAO PKD was established to support Member States in gaining access to public key information stored in the chip to validate and authenticate ePassports. The validation of ePassports through the use of the ICAO PKD is an essential element in capitalizing on the investment made by States in developing such travel documents, contributing to improved border security and facilitation, combatting terrorism and crime, and promoting secure and efficient air travel globally. This paper describes the ICAO PKD tool and explains the benefits for States to use this valuable inspection tool.
ACTION REQUIRED: The Ministerial Conference on Aviation Security and Facilitation in Africa is invited to endorse the recommendations in paragraph 7.
REFERENCE(S):

1. BACKGROUND

1.1 Electronic passports (ePassports), also known as biometric passports, contain an embedded electronic chip that stores the photograph and other personal information found on the passport data page. ePassports use Public Key Infrastructure (PKI) technology, which provides a mechanism for States to detect if the information stored on the chip has been altered. As the information on the chip is to be the same as the information on the data page, validating the chip data also contributes to detecting alterations on the physical document. In addition to the passport information, an ePassport chip stores a State-specific digital security feature which is derived from the State's security certificates, i.e. Document Signer Certificate (DSC) and Country Signing Certificate

Authority (CSCA) certificate. These digital signatures are unique to each State's ePassport and can be verified using the public key information of the passport-issuing State.

1.2 It has been estimated by the ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP), spearheaded by the New Technologies Working Group (NTWG), that there are more than half a billion ePassports in circulation today, issued by over 110 States. This has brought into question the practicability of bilaterally exchanging electronic certificates to validate ePassport digital signatures stored on the chips.

1.3 In response, and at the request of Member States, the ICAO Public Key Directory (PKD) was created in March 2007 under the aegis of ICAO to facilitate the sharing of public key information between States. The ICAO PKD is a central repository of certificates that simplifies and facilitates the multilateral exchange of the information required to validate the digital signatures on ePassports. The ICAO PKD plays a critical role as a central broker, as it ensures interoperability while minimizing the volume of digital information being exchanged. Appendix A, Figure1, illustrates the exchange process.

2. ROLE OF ICAO

2.1 A neutral site, located and operated at ICAO Headquarters, overseen by the PKD Board and funded by ICAO PKD participants was deemed to provide a trusted, centrally accessible resource from which State border authorities, aircraft operators and other entities in all Member States might download public keys for the purpose of verifying the authenticity of ePassports, which are documents of identity.

2.2 The PKD Board is the standing body responsible for financial, technical and operational oversight and supervision of the ICAO PKD. It comprises 15 board members that are appointed by the Council of ICAO, consistent with the provisions of the 2008 PKD Memorandum of Understanding (MoU).

2.3 The main role of ICAO is to act as a Trust Agent, and the Secretariat, acting as the Secretary of the Board, is responsible for providing operational and administrative support to the work of the PKD Board.

3. THE ICAO PKD GOALS

3.1 One of the major goals of the ICAO PKD is to assist its members to achieve and maintain compliance with Doc 9303, *Machine Readable Travel Documents*, specifications (Part 12) for PKI certificates in order to assure continuous and smooth ePassport validation at border control points.

3.2 By ensuring that timely and reliable information is available to undertake this validation process, the ICAO PKD simplifies and enhances the process of the ePassport validation process at border control points, and facilitates fast and secure cross-border movement.

3.3 The ICAO PKD and ePassports also provide a means of automating border control without requiring pre-enrolment in a separate program. Automated Border Controls (ABCs) gates require the use of a biometric, such as the face, to confirm the identity of the traveller. The chip on the ePassport includes the facial photograph of the document holder. Therefore, when a border control system performs ePassport validation through the ICAO PKD, which confirms the authenticity and integrity of the data on the chip, the system can confidently rely on the photograph for facial recognition.

3.4 In some instances, the chip data of ePassports currently in circulation are not fully compliant with ICAO specifications. Therefore, the ICAO PKD, in cooperation with the International Organization for Standardization (ISO), has also implemented a mechanism to make error codes available ensuring that border control authorities are aware of these issues when reading a non-compliant ePassport.

3.5 The ICAO PKD is recognized as a valuable tool and system for distributing the public certificates needed by border control and assisting its members by verifying that their certificates conform to the requirements of Doc 9303. The endorsement of the ICAO TRIP Strategy by the 38th Session of the ICAO Assembly highlighted the essential role of the ICAO PKD within one of the Strategy's main elements, *Inspection Systems and Tools* for the efficient and secure reading and verification of Machine Readable Travel Documents (MRTDs) (see Appendix A, Figure 2).

3.6 However, currently not all of the types of certificates required to perform ePassport validation can be exchanged through the ICAO PKD. CSCA certificates, which are the trust root or trust anchor, are distributed according to Doc 9303 via two methods: diplomatic bilateral exchange or through CSCA Master Lists, but not directly through the ICAO PKD. Many States have found it challenging to acquire CSCA certificates through bilateral exchange and have expressed interest in the possibility of a Master List compiled and published by ICAO.

3.7 The publication of such a Master List[1] would enable other receiving States to obtain a set of CSCA certificates from a single source (the Master List issuer) rather than undertake direct bilateral exchange with each of the issuing authorities or organizations represented on that list. The ICAO Secretariat and the PKD Board have agreed to make a Master List signed and published by ICAO available in the PKD in the near future. This will be an additional valuable service of the ICAO PKD for its participants, which will serve both the interests of document issuing authorities and the border control authorities.

4. BENEFITS OF THE ICAO PKD

4.1 States benefit from joining the ICAO PKD because citizens holding ePassports can take advantage of the facilitation benefits of ePassports. For instance, some States only allow access to their ABC gates for ePassport holders for whom a reliable source of digital certificates from their States (such as PKD) is available. Border control authorities also have an interest in joining the ICAO PKD to gain access to timely and reliable source of information to assist in validating ePassports. Checking the authenticity and validity of ePassports contributes to secure and efficient traveller facilitation as it enables to expedite the border crossing of legitimate travellers.

4.2 The ICAO PKD is considered cost-effective because the fees for PKD membership are a fraction of the overall investment required to maintain a bilateral infrastructure to connect to all ePassport-issuing States and may be recovered through ePassport fees. Although some costs may be difficult to estimate and are significantly different from one State to another, a cost-benefit analysis (CBA) based on States' feedback and experiences in PKD implementation will be developed to showcase the ICAO PKD benefits.

[1] A Master List is a list of CSCA certificates that has itself been produced and digitally signed by an issuing State. In simple terms, a PKD participant may bilaterally exchange CSCA certificates with a number of other States, authenticate the certificates, then assemble a list and sign it with its national Certificate. This list containing all the CSCAs that the State trusts is called a Master List and can be uploaded to the ICAO PKD. This Master List can then be downloaded from the ICAO PKD by others who trust the country that has issued the Master List and wish to obtain those CSCA certificates.

5. STATUS OF PARTICIPATION

5.1 Since January 2016, four additional Member States joined the ICAO PKD, bringing the total number of PKD participants to 49, as listed in Appendix B. Although approximately 80 per cent of the ePassports in circulation are issued by ICAO PKD Member States, there continues to be a significant gap between the number of ePassport-issuing States, the number of ICAO PKD participants and the States and non-State entities using the ICAO PKD in day-to-day border control operations. A major challenge is to expand the full inspection of ePassports using all of the capability that the chip provides, and thereby expand the use of the ICAO PKD by border control authorities to fully benefit from the practical value of ePassports.

5.2 With a view to encouraging participation in the ICAO PKD, Amendment 25 to Annex 9 – *Facilitation*, presented a revision to the PKD Recommended Practice 3.9.1. The Recommended Practice is now divided into two Recommended Practices: one aimed at document issuers and one for border control authorities. ICAO strongly recommends PKD participation, and the revision of Annex 9 reinforces this position.

5.3 As a measure for on-going promotion, a second PKD Border Day was held in Norway (October 2014). Among other things, it was a constructive opportunity to review the differences between using the ICAO PKD in ePassport validation and using the Interpol Stolen and Lost Travel Documents (SLTD) database, and whether the SLTD could be linked to the PKD. The use of the Interpol SLTD database is part of the ICAO TRIP Strategy's *Interoperable Applications*, which include border intelligence applications that support inspection operations. As stated in the PKD MoU, the PKD does not cover the exchange of related personal information in ePassports, such as the Document Identification Number (DIN), one of the data reported in the mandatory dataset of the SLTD database. Therefore, the PKD does not offer a facility for exchanging certificates for personal information allowing it to be linked to the Interpol SLTD database. Similarly, PKD sessions were organized during the past three Symposia on ICAO MRTDs held in Montréal in October 2013, 2014 and 2015, and during TRIP Regional Seminars held in Burkina Faso (November 2013), Uzbekistan (April 2014), Niger (January 2015), Republic of the Congo (May 2015) and Kenya (November 2015). These sessions focused on practical steps to take to join the PKD.

6. NEW PKD OPERATOR

6.1 Following an ICAO tender procedure for an operational contract for the PKD operator, in March 2015 the contract for the provision of the ICAO PKD was signed with Bundesdruckerei GmbH as prime contractor for the complete design, development and operation of the PKD. Under this new contract, the registration fees for new PKD participants will decrease from USD 56 000 to USD 15 900 and similarly, the annual fees for existing participants will be reduced. It is noteworthy that as the number of PKD participants increases, the annual fee paid by each participant decreases (see Appendix A, Figure 3).

7. ACTION REQUIRED BY THE MEETING

7.1 The meeting is invited to recommend that :

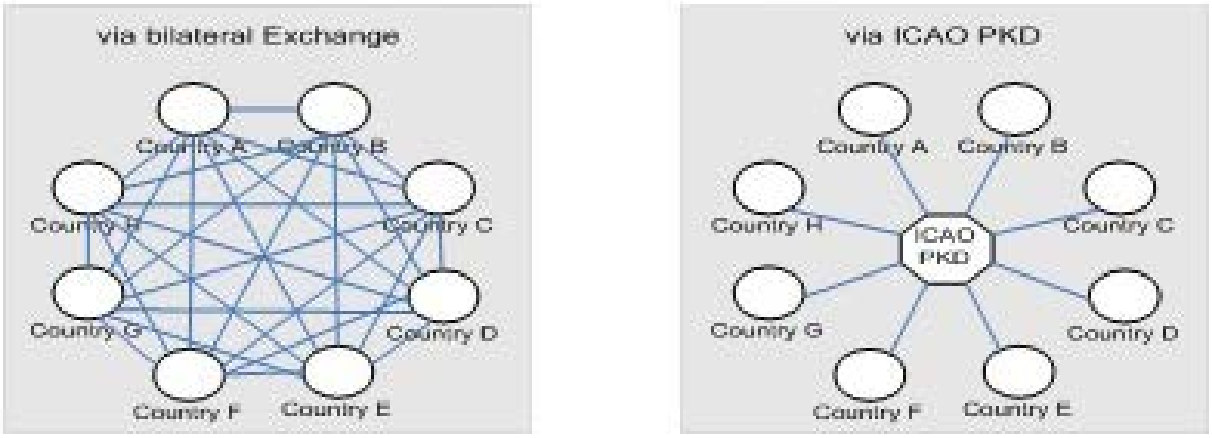
a) African States should endeavor to join the ICAO PKD as a means to prevent fraud in order to neutralize the activities and other forms of cross-border criminality; and

b) African States should actively use the ICAO PKD to authenticate and validate ePassports.

— — — — — — — —

APPENDIX A

Figure 1 - DISTRIBUTION OF CERTIFICATES



This example shows 8 States requiring 56 bilateral exchanges (left) or 2 exchanges with the PKD (right) to be up to date with DSCs and CRLs. In case of 191 ICAO States 36,290 bilateral exchanges would be necessary while there are still 2 exchanges with the PKD.

Note. — DSCs: Document Signer Certificate and CRLs: Certificate Revocation List

Figure 2 - PKD POSITION IN THE ICAO TRIP STRATEGY

Figure 3 - REGISTRATION FEE AND ANNUAL FEE

Registration Fee in US dollars		
2007 to 2008	**2009 to 2015**	**From 2016**
85,000	**56,000**	**15,900**

Annual Fee in US dollars		
No. of PKD Participants	**2015 and Earlier**	**From 2016**
45-49	34,000	29,900
50-54	34,000	27,000
55-59	34,000	24,500

PKD Participant Number	PKD Participating States and Entities	Joining Date
1	Australia (PKD Board Member)	19/03/2007
2	New Zealand (PKD Board Member)	19/03/2007
3	Singapore (PKD Board Member)	19/03/2007
4	United Kingdom (PKD Board Member)	19/03/2007
5	Japan (PKD Board Member)	19/03/2007
6	Canada (PKD Board Member)	19/03/2007
7	United States of America (PKD Board Member)	02/11/2007
8	Germany	01/11/2007
9	Republic of Korea	28/03/2008
10	France	19/06/2008
11	People's Republic of China (PKD Board Member)	26/11/2008
12	Republic of Kazakhstan	19/12/2008
13	India	12/02/2009
14	Nigeria (PKD Board Member)	13/04/2009
15	Switzerland (Chair of PKD Board)	10/07/2009
16	Ukraine	30/10/2009
17	Latvia	28/06/2010
18	The Czech Republic	30/06/2010
19	Macao, China	28/09/2010
20	United Arab Emirates (PKD Board Member)	25/10/2010
21	Hong Kong, China	26/10/2010

22	Slovak Republic	23/11/2010
23	The Netherlands (PKD Board Member)	08/12/2010
24	Kingdom of Morocco	29/12/2010
25	Austria	31/12/2010
26	Hungary	15/02/2011
27	Norway	20/06/2011
28	Bulgaria	12/10/2011
29	Luxembourg	30/11/2011
30	Sweden (PKD Board Member)	01/12/2011
31	United Nations	14/06/2012
32	Spain	10/07/2012
33	Russian Federation	31/08/2012
34	Malaysia (PKD Board Member)	09/11/2012
35	Argentina	13/12/2012
36	Thailand	05/03/2013
37	Ireland	08/03/2013
38	Republic of Moldova	11/06/2013
39	Belgium	31/10/2013
40	Brazil (PKD Board Member)	03/01/2014
41	Qatar	10/03/2014
42	Seychelles	14/03/2014
43	Uzbekistan	19/03/2014
44	Philippines	21/03/2014

45	Iran (Islamic Republic of)	18/05/2014
46	Colombia	19/05/2015
47	Romania	03/02/2016
48	Finland	26/02/2016
49	Republic of Benin	04/03/2016

— END —