



WORKING PAPER

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Facilitation Programmes

DEVELOPMENTS PERTAINING TO THE ICAO PUBLIC KEY DIRECTORY (PKD)

(Presented by the Council of ICAO)

EXECUTIVE SUMMARY

This paper reports on the developments pertaining to the ICAO Public Key Directory (PKD) and its use since the 39th Session of the ICAO Assembly. The ICAO PKD was established to support States in gaining access to public key information required to validate and authenticate ePassports. The validation of ePassports through the use of the PKD is an essential element in capitalizing on the investment made by States in developing such travel documents, contributing to improved border security, combatting terrorism and crime, and facilitating air travel globally. This paper concludes by proposing the PKD work programme for the next triennium detailing the priorities and their expected outcome.

Action: The Assembly is invited to:

- a) support the ICAO PKD operation and development priorities for the next triennium as indicated in 5.1.; and
- b) urge all ICAO Member States to join and actively use the ICAO PKD.

<i>Strategic Objectives:</i>	This working paper relates to Strategic Objective — <i>Security and Facilitation</i> .
<i>Financial implications:</i>	No additional resources required for PKD operation as the ICAO PKD work programme is funded by participant fees. Expanded activities beyond the ones listed in paragraph 5.1 are subject to the availability of additional budget under the regular programme or voluntary contributions.
<i>References:</i>	Doc 10075, <i>Assembly Resolutions in Force</i> (as of 6 October 2016) A40-WP/7, Benefits of Participation in the ICAO Public Key Directory (PKD) A40-WP/8, Developments pertaining to the ICAO Traveller Identification Programme (ICAO TRIP) Strategy

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 a passport data page. These passports use Public Key Infrastructure (PKI) technology, which prevents the information stored on the chip from being altered. Information on the chip, in turn, is only useful if it can be validated quickly and securely. This has brought into question the practicability of bilaterally exchanging electronic signatures that vouch for the validity of ePassport data signatures stored on the data chips.

1.2 Although issuing ePassports is not an Annex 9 – *Facilitation* Standard, it is recommended that the introduction of ePassports by a State goes hand in hand with participation to the ICAO Public Key Directory (PKD). States participating to the ICAO PKD are provided real time assurance that ePassports are genuine and unaltered, while facilitating the passenger travel process. The ICAO PKD is a central repository of certificates created to facilitate the sharing of public key information (PKI) between States, and allows States to minimize the volume of digital information being exchanged on a bilateral basis. To take full benefit of PKD participation, border control authorities should be invited to use it actively in order to gain access to a reliable source of information to validate ePassports. Appendix A illustrates the benefits of the PKD exchange process and shows how the PKD is part of the ICAO Traveller Identification Programme (ICAO TRIP) strategy.

2. THE REGULATORY FRAMEWORK AND PARTICIPATION STATUS

2.1 With a view to encouraging participation in the ICAO PKD, Amendment 26 to Annex 9, effective since 23 October 2017, introduced a new Recommended Practice (RP) 3.35.5, in addition to the existing ones RP 3.9.1 and RP 3.9.2, that are targeting those ICAO Member States utilizing Automated Border Control (ABC) systems. This new RP encourages the use of the information available through the ICAO PKD as a means to validate ePassports by comparing the facial recognition to the ePassport holder's photograph.

2.2 As per the PKD operational contract signed in April 2016, the PKD annual fee steadily decreases as the number of PKD participants increases (Appendix B refers). For 2019, the PKD annual fees have been established at US \$7,353 for ICAO for the PKD management and US \$22,500 for the operator for maintaining the infrastructure, totalling US \$29,853 (compared to US \$31,755 in 2018).

2.3 In the course of 2018, three Member States (Côte d'Ivoire, Mali and Serbia) joined the PKD, and as of June 2019, three Member States (Croatia, Italy and Uganda) joined, bringing the total number of PKD participants to 66. A complete list of participants is provided in Appendix C.

2.4 Although 88 per cent of the ePassports in circulation are issued by 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 PKD in day-to-day border control operations. The major challenge facing the PKD is to expand participation so that a majority of States can benefit of this inspection system and its future improvements that will enhance both global aviation security and travel facilitation.

3. ONGOING OUTREACH AND ASSISTANCE

3.1 As a measure for on-going promotion, PKD sessions were held during the 14th ICAO TRIP Symposium (23-25 October 2018) and the TRIP regional seminar held in Brasilia (5 to 7 June 2018). The dedicated session on the PKD aimed to provide more information on effectively running and implementing a national PKD (NPKD) system in order to effectively authenticate and validate ePassport. Presentations and discussions highlighted the role and value of the ICAO PKD, its benefits and deployment options for ePassport validation, as well as the advantages of using PKD in conjunction with ABCs for ePassport validation.

3.2 State letter EC 6/8.3-16/70, *ICAO Public Key Directory*, issued on 25 July 2016, informed Member States of the new ICAO PKD fees and the change in service provider. States were urged to join the ICAO PKD and also requested to reply to a questionnaire on the use of the PKD at border control. As of 30 November 2018, 51 responses were received, 42 of which were from PKD Participants (Appendix D refers). Although the deadline to answer was set at 15 September 2016, the States which have not replied continued to be encouraged to do so.

3.3 A preliminary analysis of the replies to the questionnaire on the use of the PKD at border control demonstrated that for the Member States participating in the PKD:

- 86 per cent have an Information Technology (IT) infrastructure to conduct ePassport validation;
- 56 per cent obtain the required certificates from the ICAO PKD;
- 64 per cent validate all ePassport at border control;
- 59 per cent of respondents use ABCs for border clearance process; and
- 41 per cent mentioned a decrease in waiting time.

Based on the States' responses, there is a constant increase in the number of travellers using ABCs between 2011 and 2015 with an average processing time of approximately 24 seconds. The number of replies received from non-PKD participants is too low to allow a significant analysis.

3.4 A study conducted by the New Technology Working Group (NTWG) of the Technical Advisory Group on TRIP (TAG/TRIP) identified 135 Member States issuing ePassports as detailed in Appendix E. In order to ensure an increased participation to the ICAO PKD, the Secretariat sent letters in July 2018 to 73 Member States identified by this study as issuing ePassports but not yet PKD participants (Appendix F refers). As of May 2019, eight responses were received with positive intention on joining the PKD in the near future and requesting additional information on the administrative steps in becoming a member, and since then additional letters were sent to States which have been identified as issuing ePassports.

4. RECENT PKD DEVELOPMENTS AND EXPLORATION OF POSSIBLE FUTURE USE

4.1 At the request of ICAO PKD Participants, the PKD Board, the Office of Legal Affairs of the United Nations (UN) and the Secretariat have been working together in order to develop and implement the ICAO Master List as described in Appendix G. This Master List, to be issued as ICAO intellectual property and under the ICAO brand, is expected to be an enhancement to the ICAO PKD and would increase its value for participants as well as contribute to its long-term relevance and sustainability.

This additional service is yet another incentive for States that are not participants to the ICAO PKD to join, as it will provide a “one-stop shop” for all ePassport validation. The Master List is planned to be launched in the first half of 2019, once the cooperation agreement with the UN is signed.

4.2 Expanding the use of the PKD by allowing PKD participants to exchange additional certificates, such as electronic visas and also enabling commercial entities to access the PKD data, is being currently reviewed by the PKD Board. In doing so, the PKD Board is analyzing the feasibility and the associated policies development that would allow commercial entities to access the PKD data.

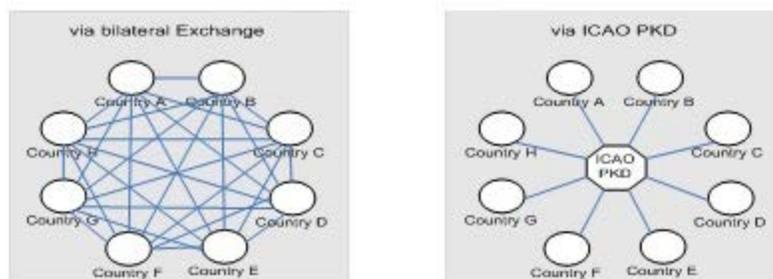
5. **PKD OPERATION AND DEVELOPMENT PRIORITIES FOR THE 2020 – 2022 TRIENNIUM**

5.1 The Assembly is invited to support the ICAO PKD operation and development priorities for the next triennium, under the work programme which has been approved by the Council, as described below:

- Assurance of uninterrupted PKD operations, by acting as a trust agent and exercising due diligence on an ongoing basis to maintain the integrity of the digital certificates;
- Development of a new ICAO Master List service that will provide States with a “one-stop shop” for the validation of all ePassport information, to support the global interoperability of ePassport validation;
- Ensurance of compliance with ICAO standards and specifications by increasing States participation in the PKD through promotion via workshops, seminars and symposia;
- Increase in active use of the PKD at border controls, with the support of the new Border and Aviation Engagement subgroup of the TAG/TRIP;
- Expansion of the activities of the PKD to exchange additional certificates, and enabling commercial entities to access the PKD data; and
- Provision of additional ICAO secretariat support needed for the PKD Board and PKD participants that could be identified during the 2020-2022 triennium would be met by means of additional resources to be funded by the PKD Fund.

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 193 ICAO States, 37,056 bilateral exchanges would be necessary while there are still 2 exchanges with the PKD.

Figure 2. PKD POSITION IN THE ICAO TRIP STRATEGY



APPENDIX B

ICAO PKD FEE SCHEDULE BASED ON ACTIVE PARTICIPATION

Active Participants¹	Operator Fees (US \$)	ICAO Fees² (US \$)	Total Annual Fees (US \$)
50 Participants	27,000.00	9,118.00	36,118.00
55 Participants	24,500.00	8,289.10	32,789.10
60 Participants	22,500.00	7,598.33	30,098.33
65 Participants	20,900.00	7,013.85	27, 913.85
70 Participants	19,250.00	6,512.86	25,762.86

¹A participant is considered as active as soon as the Participant becomes uploading and downloading the PKI certificates to and from the PKD. If no upload or download occurs within the time span of 15 months from the date of joining the PKD, the participant is considered as active and would pay the full Operator Fee.

²The ICAO Fees calculated based on the ICAO annual budget for managing and operating the PKD which is shared among all PKD Participants. For the purpose of this table, the 2019 ICAO budget of US\$455,900.00 is used and shared among the corresponding number of Participants for each row of the first column of the table in order show the decrease in the annual fee with the increase in participation and as the 2020 budget is not yet estimated (assuming that there will be 70 active PKD participants in 2020) the 2019 fee of US \$6,512 per participant is used for 70 and more participants.

**APPENDIX C
LIST OF ICAO PKD PARTICIPATING STATES AND ENTITIES**

PKD Participant Number	PKD Participating States and Entities	Joining Date	PKD Participant Number	PKD Participating States and Entities	Joining Date
1	Australia (PKD Board Member)	19/03/2007	34	Malaysia	09/11/2012
2	New Zealand (PKD Board Member)	19/03/2007	35	Argentina	13/12/2012
3	Singapore (PKD Board Member)	19/03/2007	36	Thailand	05/03/2013
4	United Kingdom (PKD Board Member)	19/03/2007	37	Ireland	08/03/2013
5	Japan (PKD Board Member)	19/03/2007	38	Republic of Moldova	11/06/2013
6	Canada (PKD Board Member)	19/03/2007	39	Belgium	31/10/2013
7	United States of America (PKD Board Member)	02/11/2007	40	Brazil	03/01/2014
8	Germany	01/11/2007	41	Qatar	10/03/2014
9	Republic of Korea	28/03/2008	42	Seychelles	14/03/2014
10	France (PKD Board Member)	19/06/2008	43	Uzbekistan	19/03/2014
11	People's Republic of China (PKD Board Member)	26/11/2008	44	Philippines	21/03/2014
12	Republic of Kazakhstan	19/12/2008	45	Iran (Islamic Republic of)	18/05/2014
13	India	12/02/2009	46	Colombia	19/05/2015
14	Nigeria (PKD Board Member)	13/04/2009	47	Romania	03/02/2016
15	Switzerland (PKD Board Member)	10/07/2009	48	Finland	26/02/2016
16	Ukraine	30/10/2009	49	Benin	03/03/2016
17	Latvia	28/06/2010	50	Botswana	05/04/2016
18	Czechia	30/06/2010	51	Kuwait	20/04/2016
19	Macao SAR, China	28/09/2010	52	Georgia	25/05/2016
20	United Arab Emirates	25/10/2010	53	Turkey	30/09/2016
21	Hong Kong SAR, China	26/10/2010	54	Iceland	30/09/2016
22	Slovakia	23/11/2010	55	Oman	22/12/2016
23	The Netherlands (PKD Board Member)	08/12/2010	56	Turkmenistan	13/02/2017
24	Kingdom of Morocco (PKD Board Member)	29/12/2010	57	Peru	28/02/2017
25	Austria	31/12/2010	58	Barbados	29/03/2017
26	Hungary	15/02/2011	59	Panama	19/10/2017
27	Norway	20/06/2011	60	European Union	07/11/2017
28	Bulgaria	12/10/2011	61	Mali	28/06/2018
29	Luxembourg (Chairperson of PKD Board)	30/11/2011	62	Côte d'Ivoire	19/07/2018
30	Sweden	01/12/2011	63	Serbia	28/12/2018
31	United Nations	14/06/2012	64	Italy	26/03/2019
32	Spain (PKD Board Member)	10/07/2012	65	Croatia	01/04/2019
33	Russian Federation	31/08/2012	66	Uganda	12/06/2019

APPENDIX D

Replies to State letter EC 6/8.3 – 16/70 received as of 15 May 2019

		Subject: ICAO Public Key Directory (PKD)	
		Action Required:	
		a) provide information concerning State plans to join the ICAO PKD, if applicable, by 15 September 2016; and	
		b) provide information on whether the State uses the PKD for ePassport validation at border controls, when applicable, by 15 September 2016.	
State	Reply Date	State	Reply Date
Australia (PKD)	06/10/2016	Luxembourg (PKD)	18/08/2016
Austria (PKD)	02/10/2017	Macao SAR, China (PKD)	02/09/2017
Belgium (PKD)	21/03/2017	Mali (PKD)	08/01/2018
Bulgaria (PKD)	26/04/2017	Malaysia (PKD)	15/03/2017
Cameroon	23/09/2016	Netherlands (PKD)	26/09/2016
Canada (PKD)	13/09/2016	New Zealand (PKD)	25/09/2016
Chile	23/09/2016	Oman (PKD)	26/09/2017
China (PKD)	03/10/2017	Qatar (PKD)	20/03/2017
Colombia (PKD)	28/09/2016	Republic of Moldova (PKD)	22/05/2018
Czechia (PKD)	16/09/2016	Romania (PKD)	22/09/2017
Denmark	14/11/2016	Russian Federation (PKD)	12/10/2017
Egypt	16/11/2016	Seychelles (PKD)	26/09/2016
Estonia	31/08/2016	Singapore (PKD)	26/08/2016
Finland (PKD)	28/09/2016	Slovakia (PKD)	04/10/2016
France (PKD)	06/12/2016	Slovenia	28/10/2016
Georgia (PKD)	18/10/2016	Spain (PKD)	05/10/2016
Germany (PKD)	27/09/2016	Sweden (PKD)	17/10/2016
Hong Kong SAR, China (PKD)	17/03/2017	Switzerland (PKD)	05/10/2016
Hungary (PKD)	13/12/2017	Thailand (PKD)	16/05/2018
Iceland (PKD)	18/10/2016	Turkey (PKD)	30/10/2017
Ireland (PKD)	24/04/2018	Turkmenistan (PKD)	19/04/2018
India (PKD)	27/09/2017	United Kingdom (PKD)	20/12/2017
Iran (PKD)	26/09/2017	United Republic of Tanzania	24/03/2017
Japan (PKD)	20/09/2016	United States (PKD)	16/10/2016
Jordan	23/04/2018	Venezuela	01/12/2016
Latvia (PKD)	11/10/2016		

APPENDIX E

REGIONAL BREAKDOWN OF STATES ISSUING ePASSPORTS

Region	Number of Member States	Number of Member States issuing ePassports	Percentage (%) Regional % (Global %)
Asia and Pacific (APAC) ³	39	21	53.85 (10.88)
Eastern and Southern African (ESAF)	24	14	58.33 (7.25)
European and North Atlantic (EUR/NAT)	56	55	98.21 (28.50)
Middle East (MID)	15	9	60 (4.66)
North American, Central American and Caribbean (NACC)	22	7	31.82 (3.63)
South American (SAM)	13	9	69.23 (4.66)
Western and Central African (WACAF)	24	20	83.33 (10.36)
Total	193	135	(69.95)

³ Although Hong Kong (China) and Macao (China) are issuing ePassports they are not counted as ICAO Member States.

APPENDIX F
LIST OF STATES IDENTIFIED AS ISSUING ePASSPORTS BUT NOT YET PKD
PARTICIPANTS (as of 12 June 2019)

1	Albania	38	Liberia
2	Algeria	39	Lithuania
3	Andorra	40	Madagascar
4	Armenia	41	Maldives
5	Azerbaijan	42	Malta
6	Bahamas	43	Mauritania
7	Bosnia Herzegovina	44	Monaco
8	Brunei	45	Mongolia
9	Burkina Faso	46	Montenegro
10	Burundi	47	Mozambique
11	Cambodia	48	Namibia
12	Cameroon	49	North Macedonia
13	Cabo Verde	50	Pakistan
14	Central African Republic	51	Paraguay
15	Chile	52	Poland
16	Comoros	53	Portugal
17	Congo	54	San Marino
18	Congo, Democratic Republic of the	55	Senegal
19	Cyprus	56	Sierra Leone
20	Denmark	57	Slovenia
21	Egypt	58	Solomon Islands
22	Equatorial Guinea	59	Somalia
23	Estonia	60	South Africa
24	Fiji	61	South Sudan
25	Gabon	62	Sri Lanka
26	Gambia	63	St. Kitts and Nevis
27	Ghana	64	St. Vincent and the Grenadines
28	Greece	65	Sudan
29	Grenada	66	Tajikistan
30	Guinea	67	Timor-Leste
31	Guinea-Bissau	68	Togo
32	Indonesia	69	United Republic of Tanzania
33	Iraq	70	Uruguay
34	Israel	71	Venezuela
35	Kenya	72	Zimbabwe
36	Lebanon		
37	Lesotho		

APPENDIX G

Country Signing Certificate Authority (CSCA) Master List

The only way to correctly validate ePassports is to have the validation keys available from trusted sources. Each ePassport should be checked against both their *document* verification key and *country* verification key. Currently, ICAO PKD is supporting the global interoperability of ePassport validation by acting as a central broker to manage the exchange of the document validation keys which are updated on a regular basis during the year, while the *country* validation keys are only shared through diplomatic channels.

Even though they are changed relatively infrequently, States are reporting great difficulty exchanging the *country* validation keys bilaterally. A neutral repository of these country validation keys will be a tool that States can use to fulfil notably their obligations under the Security Council resolutions, related to Aviation Security and Facilitation.

There is an existing mechanism in place for States to share their own collection of other State *country* validation keys. This mechanism is called a Master List.

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 Master List signing 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.

The publication of a Master List enables 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 greater the number of Master Lists available, the more beneficial because lists can be downloaded and compared to other lists.

Given ICAO's status as a specialized agency of the United Nations, the ICAO Country Signing Certificate Authority (CSCA) Master List is being developed. A pre-requisite for this ICAO Master List is to have it counter-signed with a CSCA in order to be interoperable with border systems. As the UN issues electronic Laissez-Passers and holds one of the non-State CSCAs in the PKD, ICAO sought the assistance of the UN and proposed to use the UN CSCA for the sole purpose of countersigning the ICAO Master List.