



大会 — 第 41 届会议

执行委员会

题目编号 13: 简化手续方案

国际民航组织公钥簿 (PKD) 的进展情况

(由国际民航组织理事会提交)

执行摘要

国际民航组织公钥簿 (PKD) 是支撑使用电子机读旅行证件 (eMRTDs) 的国际基础设施的一个组成部分, 并促进共享作为全球电子机读旅行证件生态系统之一部分所必需的公钥证书。自大会第 40 届会议以来, 由于新参与者不断加入、所包含的数据越来越多, 并且增加了新的服务, 令公钥簿系统不断演进。目前, 正在对核验旅行健康证明的未来支助进行审议, 同时正在探讨今后是否能够供私营部门实体加以使用。

行动: 请理事会:

- a) 虑及公钥簿的发展和管理是 2023 年至 2025 年国际民航组织业务计划的一个优先事项, 如第 5 节所述, 批准国际民航组织公钥簿下一个三年期的优先事项和工作方案;
- b) 敦促所有国际民航组织成员国加入国际民航组织公钥簿; 和
- c) 要求参加国际民航组织公钥簿的所有国家将所有适当的信息上传到该系统, 并充分利用所提供的服务。

战略目标:	本工作文件涉及战略目标 — 安保和简化手续。
财务影响:	国际民航组织公钥簿工作方案的资金来自参与者的费用。本文件所及的与公钥簿相关的具体活动资金由公钥簿基金直接提供。与通用基础设施或能力发展相关的其他活动将依据经常预算下的额外预算或自愿捐助的情况而定。
参考文件:	Doc 10140 号文件: 《大会有效决议》(截至 2019 年 10 月 4 日) 附件 9 — 《简化手续》(第十五版) 关于参与电子机读旅行证件国际民航组织公钥簿和分摊费用的谅解备忘录 Doc 9303 号文件: 机读旅行证件 (第 8 版) A40-WP/6 号文件: 国际民航组织公钥簿的进展情况 A40-WP/8 号文件: 国际民航组织旅行者身份识别方案 (TRIP) 战略的进展情况 A41-WP/10 号文件: 国际民航组织旅行者身份识别方案 (TRIP) 战略的进展情况

1. 背景

1.1 电子机读旅行证件（eMRTDs），以数字格式编码与个人旅行相关的身份信息，增强旅行安保和便利性。国际民航组织发布了各种电子旅行证件格式的规范，包括电子护照、数字旅行证书（DTC）和可见数字印章（VDS）（参见 A41-WP/10 号文件（国际民航组织旅行者身份识别方案（ICAO TRIP）战略的进展情况））。所有格式都规定存储数据应用数字签名，在对签名进行适当验证后确保文件的真实性和数据的完整性。验证签名有赖于相关公钥的可用性。

1.2 随着越来越多的国家发行电子机读旅行证件，以及对其定期和及时交换的要求变得愈加严格，通常作为公钥证书共享的密钥，其双边交换也变得极具挑战性。参与电子机读旅行证件签发和验证的国家当局通过网络进行集中共享，极大地促进了多边交换。在此基础上，国际民航组织于 2007 年建立了公钥簿，以便各国间共享公钥证书。

1.3 过去几年，随着越来越多的国家开始签发电子护照（目前有超过 145 个国家签发电子护照）、电子签证（欧洲联盟已于 2022 年授权使用可见数字印章格式签发电子签证），以及基于国际民航组织非限制环境可见数字印章规范的健康证明，并且随着各国开始审议通过签发数字旅行证书以实现护照簿的非实物化，公钥簿已成为全球电子机读旅行证件的一个日益重要的组成部分。这导致自国际民航组织大会第 40 届会议以来，公钥簿及其相关框架出现了本文件第 2 节和第 3 节所述的演变，以及为确保认识到该系统的价值而进行的大量外联。迅速发展的环境还要求审议公钥簿系统如何在近期发展的基础上保持敏捷性并继续提供最大的价值。第 5 节概述了发展方面的优先事项。

2. 监管框架和参与状况

2.1 《国际民用航空公约》附件 9 —《简化手续》第 28 次修订于 2021 年 2 月 28 日生效，标准 3.9.2 作为国际民航组织公钥簿相关的首个标准（参见 SL 2020/71）被增加到该附件。它要求参加国际民航组织公钥簿的国家上传所有必要的公共密钥数据，用以验证它们发给公钥簿的所有电子护照。它补充了现有的建议措施，即在边境签发电子旅行证件和检查电子旅行证件的机构应该加入公钥簿。

2.2 公钥簿的资金完全出自均摊费用的参与者的捐款。因此，年费随着公钥簿参与者数量的增加而减少。2022 年，参与者支付 7,096.25 美元以分担国际民航组织的费用，并支付了 18,000.00 美元作为其应支付给使用国际民航组织公钥簿的私营行业运营商的份额，共计 25,096.25 美元（2019 年为 29,853.23 美元）。附录 A 所示为自 2015 年以来不断降低的费用。2021 年 3 月对运营商现有合同进行修订，合同期再延长五年，从而保证这一费用结构将适用于提供现有服务，直至 2026 年。

2.3 与以往任何三年期相比，在 2019-2021 年期间，有更多的国家开始参与公钥簿，这证明了该系统的现有价值。2019 年，8 个成员国（白俄罗斯、波斯尼亚和黑塞哥维那、克罗地亚、埃及、印度尼西亚、意大利、乌干达和坦桑尼亚联合共和国）加入了公钥簿；2020 年，4 个成员国（孟加拉国、厄瓜多尔、卢旺达和多哥）加入；2021 年，7 个成员国（加纳、莱索托、墨西哥、蒙古、尼泊尔、苏丹和越南）加入，公钥簿参与者总数达到 82 个。参与者完整名单见附录 B。

3. 新服务的开发

3.1 2020年3月，国际民航组织通过公钥簿发布了首份国际民航组织总列表。这份总列表提供了电子机读旅行证件签发国的信任根（“CSCA”）公钥证书，为电子机读旅行证件验证提供了所需的最基本公钥可信来源。它是在联合国通行证电子护照信任根下签署的，允许接收方验证其真伪和完整性。附录C列出了截至2021年12月其证书被列入总列表的实体。

3.2 2021年12月启动了一项试点计划，授权参与旅行连续体的私营行业实体在其运营中可以使用从公钥簿获得的数据。该计划的推出反映了此类实体在旅行连续体中的公私伙伴关系日益深入的参与，以及为它们提供正确验证电子机读旅行证件手段的相关重要性。它还鼓励私营行业主体为本国解决动荡时期出现的意外挑战及时提供方案。向15家公司提供了公钥簿数据的使用授权。在6个月试点后，所获信息将被用于下一步工作。

3.3 为支持核验健康证明发送所需公钥材料（根据理事会航空恢复工作队（CART）的建议和世界卫生组织（WHO）的指南），鉴于世卫组织指南指出健康证明应基于利用现有能力的公钥基础设施签发，如国际民航组织公钥簿，公钥簿委员会对公钥簿中实施新的健康分支情况进行了审查。与此同时，根据新的服务交付模式，建立了一个新的国际民航组织健康总列表，卢森堡负责重要信息技术基础设施的国家机构 INCERT 作为合作伙伴参与了该模式，使国际民航组织或成员国无需承担任何费用便可以迅速推出新的解决办法。

4. 外联和加强援助

4.1 在2020年5月11日（关于新的国际民航组织总列表）和2022年1月26日（关于私营行业使用试点项目）举行的非正式通报会上，向理事会重点介绍了公钥簿的进展情况。公钥簿委员会主席在第16届国际民航组织旅行者身份识别方案研讨会（2021年5月25-27日）上介绍了国际民航组织总列表，同时国际民航组织举行了公钥簿研讨会和/或在各种国际虚拟活动上作了介绍。在国际民航组织旅行者身份识别方案技术咨询小组的新技术工作组会议上做了多次介绍，确保规范制定和公钥簿操作实施之间持续保持一致。

4.2 2020年6月19日发布的国际民航组织公钥簿的新国际民航组织主列表国家信函 EC 6/8.3-20/68，向成员国通报了新的国际民航组织总列表。

4.3 公钥簿委员会于2020年11月批准了一项新的公钥簿能力建设计划——公钥簿“数据质量辅导”计划（附录D）。该方案将公钥簿参与者与经验丰富的教练配对，这些教练将帮助他们与更广泛的电子机读履行证件实施活动进行对接并正确使用公钥簿。委员会选择蒙古作为教练计划的第一个受训方，辅导工作已于2021年12月开始。

5. 2023–2025年三年期的优先事项

5.1 电子机读旅行证件是航空运输简化手续创新的一个基本组成部分，并支助与无缝隙、非接触式旅行程序相关的技术和进程创新。在这方面对电子证件的全面核验至关重要。因此，公钥簿必须是2023年至2025年三年期国际民航组织业务计划中安保和简化手续战略目标下所开展工作的基石。这就要求所有签发或接收电子机读旅行证件的国家对其予以全面使用。

5.2 新冠疫情凸显，现有能力必须落实到位，确保做好应对意外挑战的准备，同时这些能力本身必须具有适应性。

5.3 因此，请大会按照下一个三年期的以下优先事项，支持国际民航组织公钥簿：

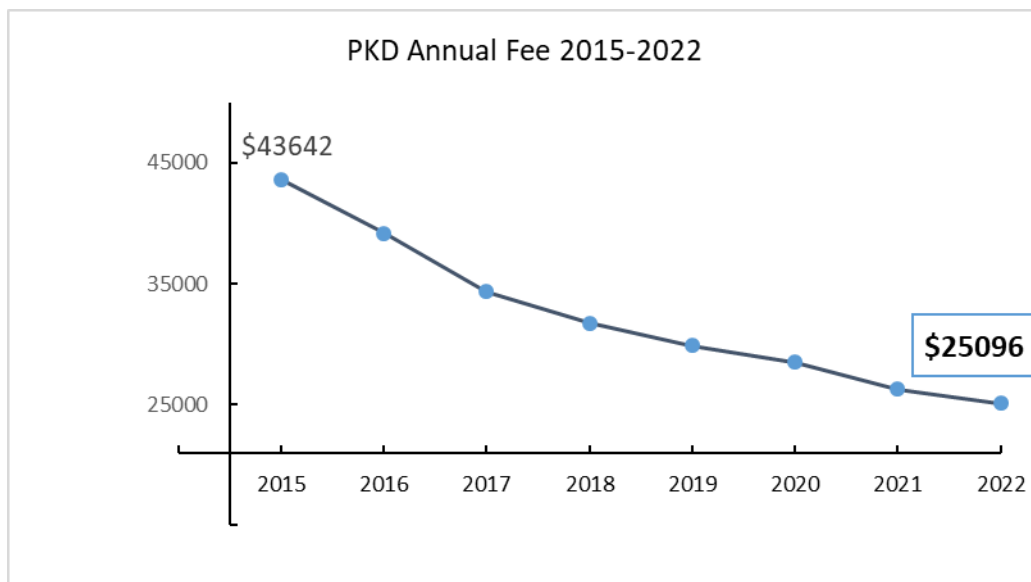
- a) 保证公钥簿运营不间断和系统完整性的维护；
- b) 扩大公钥簿活动，增加交换证书数量；
- c) 赋权私营行业使用公钥簿数据为国家和航空利益相关方服务；
- d) 通过数据质量辅导计划、外联活动以及与旅行者身份识别技术咨询小组及其小组的合作，改善公钥簿的使用并遵守国际民航组织电子机读旅行证件标准和规范；和
- e) 确保为续签现有公钥簿运营合同做好准备，确保系统今后持续运营和经济高效的发展。

5.4 在根据目前的财务模式或获取额外资源得出财务可行性结论之前，还请大会核准下列优先事项：

- a) 在国际民航组织公钥簿设立一个新的健康分支，支持发送基于公钥簿的健康证明相关的公共密钥材料，从而更好地确保全球互操作性；和
- b) 增强实施能力，适应或改进服务，尤其是通过使用内部开发资源，应对外部挑战和需求。

5.5 根据 2023 年至 2025 年业务计划所载的相关关键绩效指标，请大会敦促所有成员国加入公钥簿，并要求参与公钥簿的成员国根据国际民航组织附件 9 的标准 3.9.2，向国际民航组织公钥簿上传对其电子机读旅行证件进行全面核验所需的全部资料，并充分利用其中包含的数据，因为充分利用这些数据对于实现旅客的非接触式处理、增强简化手续方面的技术和进程创新，并且对于提高应对未来挑战的稳健性非常重要。

APPENDIX A



The decrease in annual fees for PKD participants in the period from 2015 to 2022

APPENDIX B
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		42	Seychelles	14/03/2014
2	New Zealand (PKD Board Member)	19/03/2007		43	Uzbekistan	19/03/2014
3	Singapore (PKD Board Member)	19/03/2007		44	Philippines	21/03/2014
4	United Kingdom (PKD Board Member)	19/03/2007		45	Iran (Islamic Republic of)	18/05/2014
5	Japan (PKD Board Member)	19/03/2007		46	Colombia	19/05/2015
6	Canada (PKD Board Member)	19/03/2007		47	Romania	03/02/2016
7	United States of America (PKD Board Member)	02/11/2007		48	Finland	26/02/2016
8	Germany	01/11/2007		49	Benin	03/03/2016
9	Republic of Korea	28/03/2008		50	Botswana	05/04/2016
10	France (PKD Board Member)	19/06/2008		51	Kuwait	20/04/2016
11	People's Republic of China (PKD Board Member)	26/11/2008		52	Georgia	25/05/2016
12	Republic of Kazakhstan	19/12/2008		53	Türkiye	30/09/2016
13	India	12/02/2009		54	Iceland	30/09/2016
14	Nigeria (PKD Board Member)	13/04/2009		55	Oman	22/12/2016
15	Switzerland (PKD Board Member)	10/07/2009		56	Turkmenistan	13/02/2017
16	Ukraine	30/10/2009		57	Peru	28/02/2017
17	Latvia	28/06/2010		58	Barbados	29/03/2017
18	Czechia	30/06/2010		59	Panama	19/10/2017
19	Macao SAR, China	28/09/2010		60	European Union	07/11/2017
20	United Arab Emirates	25/10/2010		61	Mali	28/06/2018
21	Hong Kong SAR, China	26/10/2010		62	Côte d'Ivoire	19/07/2018
22	Slovakia	23/11/2010		63	Serbia	28/12/2018
23	The Netherlands (PKD Board Member)	08/12/2010		64	Italy	26/03/2019
24	Kingdom of Morocco (PKD Board Member)	29/12/2010		65	Croatia	01/04/2019
25	Austria	31/12/2010		66	Uganda	12/06/2019

26	Hungary	15/02/2011		67	Bosnia & Herzegovina	08/07/2019
27	Norway	20/06/2011		68	Egypt	09/08/2019
28	Bulgaria	12/10/2011		69	Indonesia	30/08/2019
29	Luxembourg (Chairperson of PKD Board)	30/11/2011		70	Belarus	01/10/2019
30	Sweden	01/12/2011		71	United Republic of Tanzania	20/11/2019
31	United Nations	14/06/2012		72	Bangladesh	29/06/2020
32	Spain (PKD Board Member)	10/07/2012		73	Togo	02/07/2020
33	Russian Federation	31/08/2012		74	Ecuador	17/07/2020
34	Malaysia	09/11/2012		75	Rwanda	23/07/2020
35	Argentina	13/12/2012		76	Sudan	12/01/2021
36	Thailand	05/03/2013		77	Lesotho	21/04/2021
37	Ireland	08/03/2013		78	Mexico	14/06/2021
38	Republic of Moldova	11/06/2013		79	Ghana	13/10/2021
39	Belgium	31/10/2013		80	Nepal	18/10/2021
40	Brazil	03/01/2014		81	Viet Nam	17/12/2021
41	Qatar	10/03/2014		82	Mongolia	29/12/2021

APPENDIX C
LIST OF eMRTD ISSUING ENTITIES WITH CERTIFICATES IN THE ICAO MASTER LIST
(FEBRUARY 2022)

Argentina	Hungary	Republic of Kazakhstan
Australia	Iceland	Republic of Korea
Austria	India	Republic of Moldova
Barbados	Indonesia	Romania
Belarus	Iran, Islamic Republic of	Russian Federation
Belgium	Ireland	Rwanda
Benin	Italy	Singapore
Botswana	Japan	Slovakia
Brazil	Kingdom of Morocco	Spain
Bulgaria	Kuwait	Sweden
Canada	Latvia	Switzerland
China	Luxembourg	Thailand
Hong Kong SAR, China	Malaysia	Türkiye
Macao SAR, China	Mexico	Turkmenistan
Colombia	Netherlands	Ukraine
Côte d'Ivoire	New Zealand	Uganda
Czechia	Nigeria	United Arab Emirates
Ecuador	Norway	United Kingdom
European Union	Oman	United Nations
Finland	Panama	United Republic of Tanzania
France	Peru	United States of America
Germany	Philippines	Uzbekistan
Ghana	Qatar	

APPENDIX D

The ICAO PKD Data Quality Coach Initiative

During the 26th meeting of the PKD Board, a proposal was made regarding the appointment of volunteer data quality (DQ) coaches who could be paired with different new PKD members or those struggling to come up to speed with PKD usage in order to provide the necessary help. The initiative was foreseen as a means of boosting the quality of data in the PKD (in terms of completeness as well as usability) and encouraging new participants. Subsequent to the meeting, the Vice-Chairperson of the Board collaborated with the Secretariat to refine the concept and elaborate procedural rules related to the program. A proposal outlining the concept and the approach to implementation was put to the Board and approved at the 27th meeting, with an immediate mandate given to the Secretariat to launch the program through collection of the names of coaches from PKD Board members and dissemination of a request to States (both PKD participants and those who had expressed an intention to join) to ascertain their interest in participating).

Data quality coaches are Member State experts with deep knowledge of PKI. They are fluent in English and normally able to communicate in another language of potential use in outreach to States (e.g. French, Spanish, Russian, Arabic). Eight coaches were nominated by national PKD Board members following an open call from the Secretariat and all were approved by the Board for the period of 2020/2021. Renewed calls will be launched on an annual basis.

States who express their interest in participating provide an outline of their reasoning and their requirements using an online form. The Board assesses the candidatures on an annual basis based on established criteria – their location in a region of priority as identified in the PKD Strategy, the possible availability of other support resources for that State (e.g. from the OSCE), the eagerness on the part of the identified States to engage in the initiative and the suitability of DQ coaches available. Currently, it is anticipated that one or two States will receive coaching each year. In 2021, the Board selected Mongolia and Cameroon as candidates for coaching. Mongolia have recently initiated the coaching program subject for a period of 12 months from December 2021.

In the first months of each partnership, remote contact between the State, the DQ coach and the ICAO secretariat will be established. Any issues with national organizational arrangements might also be identified and remedied at this stage. In later months, each State should host a dedicated 3 to 4 day visit by the coach, should such an effort be deemed appropriate by the coach. Where feasible, he/she may be supported by members of the ICAO secretariat and/or DQ coaching team in order to provide continuity of experience across different visits. The visit will be followed by all further outreach necessary to ensure continuity of effective operations going forward. The outreach should normally be fully concluded in a single calendar year.

It is emphasized that the appointed DQ coaches are intended to support the receiving State in their efforts to appropriately make use of their PKD participation. The coach is not intended to execute work on behalf of the State. It is incumbent on the receiving State to have the appropriate organizational setup and capacities necessary to execute the work intended. Indeed, the initial outreach in the early part of the year is intended to assure the availability of the necessary resources at national level. In case that the receiving State cannot be in a position to execute the necessary work identified by the DQ coach, work with that State in the defined year will cease. The Secretariat and DQ coaching team will provide a dedicated report to the PKD Board each year.

The activities are fully funded through the PKD “Reserve Fund” (i.e. Development and Implementation Fund). The main costs foreseen are the travel costs and daily allowances of the DQ coach and any Secretariat/DQ coaching team attending the country visits.