国 际 民 用 航 空 组 织

工 作 文 件

A40-WP/6
EX/3
26/6/19

大会 — 第 40 届会议

执行委员会

议程项目 14：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

本文件报告了国际民航组织公钥簿（PKD）的进展情况，及其自国际民航组织大会第 39 届会议以来的使用情况。国际民航组织公钥簿的建立是为了支持各国获取验证和核实电子护照所需的公钥信息。使用公钥簿验证电子护照是各国从开发这种旅行证件的投资中获益，以利加强边境安保、打击恐怖主义和犯罪以及促进全球航空旅行的一个关键要素。文件最后提出公钥簿在下一个三年期的工作方案，其中说明各个优先事项及其预期成果。

行动：请大会：

a) 支持 5.1 中所述下一个三年期国际民航组织公钥簿运行和发展优先事项；和

b) 敦促所有国际民航组织成员国加入并积极使用国际民航组织公钥簿。

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：	公钥簿运行无需额外资源，因为国际民航组织公钥簿工作方案由参加国缴费供资。超出第 5.1 段所列的扩展活动取决于经常方案中是否有额外预算可用或者是否有自愿捐助。
参考文件：	Doc 10075号文件：《大会有效决议》（截至2016年10月6日） A40-WP/7号文件：参加国际民航组织公钥簿（PKD）的益处 A40-WP/8：有关国际民航组织旅行者身份识别方案（ICAO TRIP）战略的进展情况

1. 背景

1.1 电子护照（ePassports） — 也称为生物特征护照，其中嵌入了电子芯片，用于储存护照资料页的照片和其他个人信息。这种护照使用公钥基础设施（PKI）技术，防止存储在芯片中的信息遭到更改。反过来，芯片上的信息也只有能被快速和安全地验证才会有用。这对双边交换电子签名，证明存储在数据芯片上的电子护照数据签名有效性的方法是否实际可行提出了质疑。

1.2 虽然签发电子护照不是附件 9 — 《简化手续》的一个标准，但建议采用电子护照的国家也同时参加国际民航组织公钥簿（PKD）。参加国际民航组织公钥簿的国家在对旅客旅行提供便利的同时，还对电子护照真实无误、未被改动提供了实时保证。国际民航组织公钥簿是为促进各国之间共享公钥信息（PKI）而创建的一个证书中央存储库，并使各国尽量减少双边交换数字信息的流量。为了充分利用参加公钥簿的好处，应邀请边境管制当局积极使用公钥簿，为验证电子护照获得可靠的信息来源。附录 A 说明公钥簿交换进程的效益，并显示公钥簿如何成为国际民航组织旅行者身份识别方案（TRIP）战略的一部分。

2. 监管框架和参与状况

2.1 为鼓励参加国际民航组织公钥簿，自 2017 年 10 月 23 日起生效的附件 9 第 26 次修订除针对那些利用自动边境控制（ABC）系统的国际民航组织成员国的现有建议措施（RP）3.9.1 和建议措施 3.9.2 外，还提出了新的建议措施 3.35.5。这个新的建议措施鼓励使用国际民航组织公钥簿提供的信息，将其作为将面部识别与电子护照持有人的照片进行对比来验证电子护照的手段。

2.2 依照 2016 年 4 月签署的公钥簿运营合同，公钥簿的年费随着参加公钥簿的国家数目增多而稳步下降（见附录 B）。2019 年，国际民航组织为管理公钥簿设定的年费为 7 353 美元，运营商维持基础设施的费用为 22 500 美元，共计 29 853 美元（2018 年为 31 755 美元）。

2.3 在 2018 年，有三个成员国（科特迪瓦、马里和塞尔维亚）加入了公钥簿，截至 2019 年 6 月，又有三个成员国（克罗地亚、意大利和乌干达）加入，使得参加公钥簿的国家总数达到 66 个。附录 C 提供了参加国家的完整名单。

2.4 尽管 88%的流通电子护照是由公钥簿成员国签发的，但电子护照发放国的数量与国际民航组织公钥簿参加国的数量以及在日常边防管制活动中使用公钥簿的国家与非国家实体的数量之间仍有很大差距。公钥簿面临的主要挑战是扩大参加范围，以便大多数国家都能受益于这一检查系统及其未来的改进，从而加强全球航空安保和旅行便利。

3. 目前的外联活动和援助

3.1 作为一项正在进行的推广措施，在第十四次国际民航组织旅行者身份识别方案（TRIP）研讨会（2018 年 10 月 23 日至 25 日）和在巴西利亚举行的旅行者身份识别方案地区研讨会（2018 年 6 月 5 日至 7 日）期间举行了公钥簿会议。关于公钥簿问题的专门会议旨在提供有关有效运行和实施国家公钥簿（NPKD）系统的更多信息，以便有效核实和验证电子护照。会议的发言和讨论强调了国际民航组织公钥簿的作用和价值、使用电子护照验证的好处和部署方案以及在自动化边境管制（ABCs）中使用公钥簿查验电子护照的便利之处。

3.2 2016年7月25日发布的关于国际民航组织公钥簿的EC 6/8.3 – 16/70号国家级信件向成员国通报了新的国际民航组织公钥簿费用和服务提供商的改变。它敦促各国加入国际民航组织公钥簿，并要求回答关于在边境管制中使用公钥簿的调查问卷。截至2018年11月30日，共收到51份答复，其中42份来自参加公钥簿的国家（见附录D）。虽然答复的截止日期是2016年9月15日，但没有作出答复的国家仍可提出答复。

3.3 对在边境管制中使用公钥簿的调查表的答复进行初步分析表明，在参加公钥簿的成员国中：

- 86%的成员国拥有信息技术（IT）基础设施进行电子护照验证；
- 56%的成员国从国际民航组织公钥簿获得所需的证书；
- 64%的成员国在边境管制中查验所有电子护照；
- 59%的回复者在边境清关程序中使用自动化边境管制（ABCs）；和
- 41%的成员国提到等待时间减少。

根据各国的答复，2011年至2015年期间使用自动化边境管制（ABCs）的旅行者人数不断增加，平均处理时间约为24秒。从非公钥簿参加国收到的答复数量太少，无法进行重要分析。

3.4 旅行者身份识别方案技术咨询小组（TAG/TRIP）的新技术工作组（NTWG）进行的一项研究确定了发放电子护照的135个成员国，详情见附录E。为了确保更多地参与国际民航组织公钥簿，秘书处于2018年7月向这项研究确定的73个发放电子护照但尚未参加公钥簿的成员国发送了信函（见附录F）。截至2019年5月，收到8份答复，其中表示有意在不久的将来加入公钥簿，并要求提供关于成为成员的行政步骤的补充资料，之后又向被确定发放电子护照的国家发送了额外信函。

4. 公钥簿的最近发展和探索未来的可能用处

4.1 应参与国际民航组织公钥簿的国家的要求，公钥簿委员会、联合国法律事务厅和国际民航组织秘书处一直在共同努力，以便制定和实施附录G所述的国际民航组织总列表。将作为国际民航组织的知识产权并在国际民航组织名下发布的这份总列表预计将加强国际民航组织公钥簿，并将为参与国家增加其价值以及促进其长期相关性和可持续性。这项额外服务是促使尚未加入国际民航组织公钥簿的国家加入其中的一项激励措施，因为它将为所有电子护照验证提供“一站式服务”。一旦与联合国的合作协议得到签署，计划将于2019年上半年发布总列表。

4.2 公钥簿委员会目前正在审查通过允许公钥簿参与国家交换额外证书（如电子签证）并允许商业实体取用公钥簿数据，扩大公钥簿的使用范围。在这方面，公钥簿委员会正在分析允许商业实体取用公钥簿数据的可行性和制定相关的政策。

5. 2020－2022 三年期公钥簿运行和发展优先事项

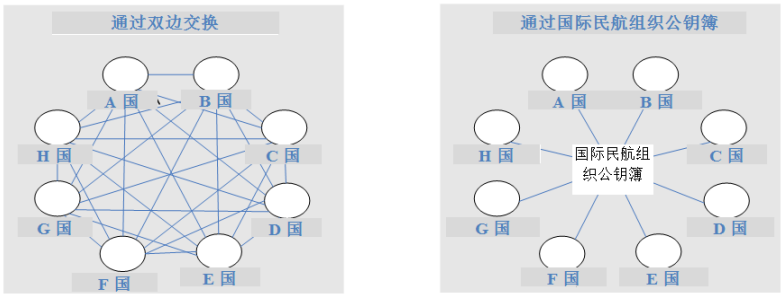
5.1 请大会支持理事会已经核准的工作方案下国际民航组织公钥簿下一个三年期的运行和发展优先事项如下：

- 充当信托代理人，持续尽职地维持数字证书的完整性，从而确保公钥簿不间断运行；
- 发展新的国际民航组织总列表服务，为各国提供验证所有电子护照信息的“一站式”服务，以支持电子护照验证的全球互操作性；
- 通过讲习班、研讨会和专题讨论会进行推广使更多国家参与公钥簿，从而确保遵守国际民航组织的标准和规范；
- 借助旅行者身份识别方案技术咨询小组（TAG/TRIP）新设立的边境和航空接触小组，增加公钥簿在边防管制中的积极使用；
- 扩大公钥簿的使用范围，允许交换额外证书并允许商业实体取用公钥簿数据；和
- 通过公钥簿基金可提供的额外资源为 2020－2022 三年期间可确定的公钥簿委员会和公钥簿参加国家提供额外的国际民航组织秘书处支持。

— — — — — — — —

附录 A

图 1. 证书的分发



本范例表明，为获取目前的证件签署人证书和证书撤销列表，8个国家需要进行56次双边交换（左图），或者与公钥簿进行2次交换（右图）。如果是国际民航组织的193个成员国，将需要进行37 056次双边交换，而与公钥簿仍然只需要2次交换。

图 2. 公钥簿在国际民航组织旅行者身份识别方案战略中的位置

— — — — — — — — —

附录 **B**

国际民航组织基于积极参与程度设定的公钥簿使用收费表

积极参加国家 [1]	运营商收费（美元）	国际民航组织收费 [2]（美元）	年费总额（美元）
50 个参加国	27 000.00	9 118.00	36 118.00
55 个参加国	24 500.00	8 289.10	32 789.10
60 个参加国	22 500.00	7 598.33	30 098.33
65 个参加国	20 900.00	7 013.85	27 913.85
70个参加国	19 250.00	6 512.86	25 762.86

— — — — — — — — —

[1] 一旦参加国从公钥簿（PKD）上传或下载公钥基础设施（PKI）证书就被视为积极参与。如果在加入公钥簿之日起15个月内没有上传或下载，则参加国被视为积极参与并将支付全额运营商费用。

[2] 国际民航组织收费根据国际民航组织管理和运行公钥簿的年度预算计算，由所有公钥簿参加国分担。就本表而言，采用了2019年国际民航组织的预算455 900.00美元，在表格第一栏每行相应数量的参加国之间分担，以显示随着参加国数量增加而年费减少。鉴于2020年预算尚未估算（假设2020年将有70名积极的公钥簿参参加国），对于70名和70名以上参加国，采用了2019年费，即每个参加国6 512美元。

附录C

国际民航组织公钥簿参加国家和实体名单

公钥簿 参加国编号	公钥簿参加国和实体	加入日期	公钥簿 参加国编号	公钥簿 参加国和实体	加入日期
1	澳大利亚 （公钥簿委员会成员）	19/03/2007	34	马来西亚	09/11/2012
2	新西兰 （公钥簿委员会成员）	19/03/2007	35	阿根廷	13/12/2012
3	新加坡 （公钥簿委员会成员）	19/03/2007	36	泰国	05/03/2013
4	联合王国 （公钥簿委员会成员）	19/03/2007	37	爱尔兰	08/03/2013
5	日本 （公钥簿委员会成员）	19/03/2007	38	摩尔多瓦共和国	11/06/2013
6	加拿大 （公钥簿委员会成员）	19/03/2007	39	比利时	31/10/2013
7	美利坚合众国 （公钥簿委员会成员）	02/11/2007	40	巴西	03/01/2014
8	德国	01/11/2007	41	卡塔尔	10/03/2014
9	大韩民国	28/03/2008	42	塞舌尔	14/03/2014
10	法国 （公钥簿委员会成员）	19/06/2008	43	乌兹别克斯坦	19/03/2014
11	中华人民共和国 （公钥簿委员会成员）	26/11/2008	44	菲律宾	21/03/2014
12	哈萨克斯坦共和国	19/12/2008	45	伊朗伊斯兰共和国	18/05/2014
13	印度	12/02/2009	46	哥伦比亚	19/05/2015
14	尼日利亚 （公钥簿委员会成员）	13/04/2009	47	罗马尼亚	03/02/2016
15	瑞士 （公钥簿委员会成员）	10/07/2009	48	芬兰	26/02/2016
16	乌克兰	30/10/2009	49	贝宁	03/03/2016
17	拉脱维亚	28/06/2010	50	博茨瓦纳	05/04/2016
18	捷克	30/06/2010	51	科威特	20/04/2016
19	中国澳门特别行政区	28/09/2010	52	格鲁吉亚	25/05/2016
20	阿拉伯联合酋长国	25/10/2010	53	土耳其	30/09/2016
21	中国香港特别行政区	26/10/2010	54	冰岛	30/09/2016
22	斯洛伐克	23/11/2010	55	阿曼	22/12/2016
23	荷兰 （公钥簿委员会成员）	08/12/2010	56	土库曼斯坦	13/02/2017
24	摩洛哥王国 （公钥簿委员会成员）	29/12/2010	57	秘鲁	28/02/2017
25	奥地利	31/12/2010	58	巴巴多斯	29/03/2017
26	匈牙利	15/02/2011	59	巴拿马	19/10/2017
27	挪威	20/06/2011	60	欧洲联盟	07/11/2017
28	保加利亚	12/10/2011	61	马里	28/06/2018
29	卢森堡 （公钥簿委员会主席）	30/11/2011	62	科特迪瓦	19/07/2018
30	瑞典	01/12/2011	63	塞尔维亚	28/12/2018
31	联合国	14/06/2012	64	意大利	26/03/2019
32	西班牙 （公钥簿委员会成员）	10/07/2012	65	克罗地亚	01/04/2019
33	俄罗斯联邦	31/08/2012	66	乌干达	12/06/2019

— — — — — — — —

附录 D

截至 2019 年 5 月 15 日收到的对 EC 6/8.3 – 16/70 号国家级信件收到的答复

	题目：国际民航组织公钥簿（PKD）
	要求： a) 在 2016 年 9 月 15 日以前，酌情提供有关加入国际民航组织公钥簿的国家计划的信息；和 b) 在 2016 年 9 月 15 日以前，酌情提供国家在边境控制中是否使用公钥簿进行电子护照验证的信息。

国家	答复日期	国家	答复日期
澳大利亚（公钥簿）	06/10/2016	卢森堡（公钥簿）	18/08/2016
奥地利（公钥簿）	02/10/2017	中国澳门特别行政区（公钥簿）	02/09/2017
比利时（公钥簿）	21/03/2017	马里（公钥簿）	08/01/2018
保加利亚（公钥簿）	26/04/2017	马来西亚（公钥簿）	15/03/2017
喀麦隆	23/09/2016	荷兰（公钥簿）	26/09/2016
加拿大（公钥簿）	13/09/2016	新西兰（公钥簿）	25/09/2016
智利	23/09/2016	阿曼（公钥簿）	26/09/2017
中国（公钥簿）	03/10/2017	卡塔尔（公钥簿）	20/03/2017
哥伦比亚（公钥簿）	28/09/2016	摩尔多瓦共和国（公钥簿）	22/05/2018
捷克（公钥簿）	16/09/2016	罗马尼亚（公钥簿）	22/09/2017
丹麦	14/11/2016	俄罗斯联邦（公钥簿）	12/10/2017
埃及	16/11/2016	塞舌尔（公钥簿）	26/09/2016
爱沙尼亚	31/08/2016	新加坡（公钥簿）	26/08/2016
芬兰（公钥簿）	28/09/2016	斯洛伐克（公钥簿）	04/10/2016
法国（公钥簿）	06/12/2016	斯洛文尼亚	28/10/2016
格鲁吉亚（公钥簿）	18/10/2016	西班牙（公钥簿）	05/10/2016
德国（公钥簿）	27/09/2016	瑞典（公钥簿）	17/10/2016
中国香港特别行政区（公钥簿）	17/03/2017	瑞士（公钥簿）	05/10/2016
匈牙利（公钥簿）	13/12/2017	泰国（公钥簿）	16/05/2018
冰岛（公钥簿）	18/10/2016	土耳其（公钥簿）	30/10/2017
爱尔兰（公钥簿）	24/04/2018	土库曼斯坦（公钥簿）	19/04/2018
印度（公钥簿）	27/09/2017	联合王国（公钥簿）	20/12/2017
伊朗（公钥簿）	26/09/2017	坦桑尼亚联合共和国	24/03/2017
日本（公钥簿）	20/09/2016	美国（公钥簿）	16/10/2016
约旦	23/04/2018	委内瑞拉	01/12/2016
拉脱维亚（公钥簿）	11/10/2016		

— — — — — — — —

附录 E

按地区分列签发电子护照的国家

地区	成员国数目	签发电子护照的成员国数目	百分率 (%) 地区% （全球%）
亚洲和太平洋（APAC）地区 [3]	39	21	53.85 (10.88)
东部和南部非洲（ESAF）地区	24	14	58.33 (7.25)
欧洲和北大西洋（EUR/NAT）地区	56	55	98.21 (28.50)
中东（MID）地区	15	9	60 (4.66)
北美、中美和加勒比（NACC）地区	22	7	31.82 (3.63)
南美（SAM）地区	13	9	69.23 (4.66)
西部和中部非洲（WACAF）地区	24	20	83.33 (10.36)
共计	193	135	(69.95)

— — — — — — — — —

[3] 尽管香港（中国）和澳门（中国）都发放电子护照，但它们没有被作为国际民航组织成员国计入。

附录 F

发放电子护照但没有参加国际民航组织公钥簿的国家名单

1	阿尔巴尼亚	37	莱索托
2	阿尔及利亚	38	利比里亚
3	安道尔	39	立陶宛
4	亚美尼亚	40	马达加斯加
5	阿塞拜疆	41	马尔代夫
6	巴哈马	42	马耳他
7	波斯尼亚和黑塞哥维那	43	毛里塔尼亚
8	文莱	44	摩纳哥
9	布基纳法索	45	蒙古
10	布隆迪	46	黑山
11	柬埔寨	47	莫桑比克
12	喀麦隆	48	纳米比亚
13	佛得角	49	北马其顿
14	中非共和国	50	巴基斯坦
15	智利	51	巴拉圭
16	科摩罗	52	波兰
17	刚果	53	葡萄牙
18	刚果民主共和国	54	圣马力诺
19	塞浦路斯	55	塞内加尔
20	丹麦	56	塞拉利昂
21	埃及	57	斯洛文尼亚
22	赤道几内亚	58	所罗门群岛
23	爱沙尼亚	59	索马里
24	斐济	60	南非
25	加蓬	61	南苏丹
26	冈比亚	62	斯里兰卡
27	加纳	63	圣基茨和尼维斯
28	希腊	64	圣文森特和格林纳丁斯
29	格林纳达	65	苏丹
30	几内亚	66	塔吉克斯坦
31	几内亚比绍	67	东帝汶
32	印度尼西亚	68	多哥
33	伊拉克	69	坦桑尼亚联合共和国
34	以色列	70	乌拉圭
35	肯尼亚	71	委内瑞拉
36	黎巴嫩	72	津巴布韦

— — — — — — — —

附录 G

国家签署证书当局（CSCA）总列表

正确查验电子护照的唯一方法是从可信来源得到验证密钥。对每份电子护照应核对其证件验证密钥和国家验证密钥。目前，国际民航组织公钥簿通过担当中央中介管理证件验证密钥（一年中定期更新）的交换来支持电子护照查验的全球互用性，而国家验证密钥只通过外交渠道分享。

即使国家验证密钥相对较少改变，但各国报告在双边交换国家验证密钥方面有很大困难。一个中立的国家验证密钥储存库将成为各国可用来履行其安理会决议下有关航空安保和简化手续的义务的工具。

已有一个已到位的现行机制让各国分享自己的他国国家验证密钥集。这一机制被称为总列表。

总列表是国家签署证书当局证书的列表，该列表本身由签发国制作并进行数字签署。简言之，公钥簿参加国可以与若干其他国家进行国家签署证书当局证书的双边交换、鉴别证书真伪，然后汇编一份列表并用其国家总列表签署证书对其进行签署。包含该国信任的所有国家签署证书当局的这一列表被称为总列表，可以被上传到国际民航组织公钥簿。之后，信任该总列表签发国并且希望获取那些国家签署证书当局证书的其他国家可以从国际民航组织公钥簿下载这一总列表。

公布此类总列表使得其他接收国家通过单一渠道（总列表签发人）获得一套国家签署证书当局的证书，而不用与该表所列的每个签发当局或组织直接进行双边交换。可用的总列表数量越多越有益，因为可以下载列表并与其他列表进行比较。

鉴于国际民航组织作为联合国的专门机构，现在正在编制国际民航组织的国家签署证书当局（CSCA）总列表。编制这份国际民航组织总列表的一项先决条件是它得到国家签署证书当局（CSCA）的会签，以便与边境系统实现互用。由于联合国签发电子通行证（Laissez-Passers）并且是公钥簿中非国家签署证书当局之一，国际民航组织寻求联合国的协助并提议以联合国的国家签署证书当局来会签国际民航组织的总列表。

— 完 —