国 际 民 用 航 空 组 织

工 作 文 件

A39-WP/19
EX/7
31/5/16

大会 — 第39届会议

执行委员会

议程项目 19：　简化手续和国际民航组织旅行者身份识别方案(ICAO TRIP)战略

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38届会议以来的使用情况。建立国际民航组织公钥簿，是为了支助成员国获取芯片中存储的公钥信息，以验证和核实电子护照。利用国际民航组织公钥簿验证电子护照，是对各国为开发此类旅行证件所做投资实行资本化的一个基本要素，有助于加强边境安保和简化手续，打击恐怖主义和犯罪，并促进全球可靠及高效的航空旅行。本文件结束时提出了下个三年期国际民航组织公钥簿工作方案的优先事项及其工作的预期成果。

行动：请大会：

a) 核准国际民航组织公钥簿的工作方案；和

b) 敦促国际民航组织所有成员国加入公钥簿，并积极使用国际民航组织公钥簿验证及核实电子护照。

战略目标：	本工作文件涉及战略目标C — 安保和简化手续。
财务影响：	无需额外资源，因为国际民航组织公钥簿由参加国缴费供资。
参考文件：	A38-WP/11号文件 C-WP/14264号文件 Doc 10022号文件：《大会有效决议》(截至2013年10月4日)

1. 背景

1.1 电子护照(ePassports)，也称作生物鉴别护照，在护照数据页包含一个内置电子芯片，其中存有照片，并且载有其他个人信息。电子护照使用公钥基础设施(PKI)技术，这种技术为各国提供了一种机制，可以检测芯片所存储信息是否已被涂改。由于芯片的信息应当与数据页的信息相同，因此，验证芯片数据还有助于发现证件实物上面的涂改。除护照信息外，电子护照芯片还存储从国家安全证书，即证件签署人证书(DSC)和国家签署证书当局(CSCA)证书中得出的该国特定的数字安全特征。这些数字签名对于每个国家的电子护照都是独一无二的，并且可以利用护照颁发国的公钥信息进行核实。

1.2 以新技术工作组(NTWG)为先锋的国际民航组织旅行者身份识别方案技术咨询组(TAG/TRIP)估计，现有 110 多个国家颁发的 5 亿多本电子护照正在流通使用。这对双边交换电子证书，以验证芯片所存储电子护照数字签名的可行性提出了质疑。

1.3 为此，应成员国的要求，在国际民航组织主持下于 2007 年 3 月创建了国际民航组织公钥簿(PKD)，以促进各国之间共享公钥信息。国际民航组织公钥簿是各类证书的一个中央存储库，它简化并便利对验证电子护照数字签名所需信息的多边交换。由于它在最大程度上将交换的数字信息量降至最低的同时确保互用性，因此，国际民航组织公钥簿发挥了一个核心经纪人的关键作用。附录 A 图 1 对交换过程做了说明。

2. 国际民航组织的作用

2.1 在国际民航组织总部运行、受公钥簿委员会监督、并且由国际民航组织公钥簿参加国供资的一个中立场所，被视为可提供可信、可集中访问来自所有成员国国家边境当局、航空器运营人和其他实体的资源，可以下载公钥用于核实作为身份证件的电子护照的真实性。

2.2 公钥簿委员会是负责国际民航组织公钥簿财务、技术和运行监督及管理的常设机构。根据 2008 年公钥簿谅解备忘录(MoU)的规定，该委员会由国际民航组织理事会任命的 15 名委员会成员组成。

2.3 国际民航组织的主要作用是充当信托代理人，而秘书处则担任委员会的秘书，负责为公钥簿委员会的工作提供运行和行政支助。

3. 国际民航组织公钥簿的目标

3.1 国际民航组织公钥簿的主要目标之一，就是协助其成员实现并保持对 Doc 9303 号文件：《机读旅行证件》所载公钥基础设施证书规范(第 12 部分)的遵守，以确保在边境管制点持续顺畅地进行电子护照的验证工作。

3.2 通过确保为开展这一验证过程提供及时可靠的信息，国际民航组织公钥簿简化并加强了边境管制点电子护照验证过程的程序，并促进了迅速安全的出入境活动。

3.3 国际民航组织公钥簿和电子护照还提供了一种方式，无需提前登记参加一项单独的方案便可以对边境管制实行自动化。自动化边境管制(ABCs)通道，要求使用譬如面部进行生物识别以便确认旅行者的身份。电子护照上的芯片包含了证件持有人的面部照片。因此，当边境管制系统通过国际民航组织公钥簿进行电子护照验证，以确认芯片数据的真实性和完好性时，该系统可以信赖该照片进行面部识别。

3.4 在某些情况下，目前流通的电子护照芯片的数据并不完全符合国际民航组织的规范。因此，国际民航组织公钥簿还与国际标准化组织(ISO)合作，实施了一项提供错误代码的机制，并确保各边境管制当局在读取不合规的电子护照时清楚地意识到这些问题。

3.5 国际民航组织公钥簿被公认是分发边境管制所需公共证书的一个宝贵工具和系统，并协助其成员核实其各类证书是否符合 Doc 9303 号文件的要求。国际民航组织大会第 38 届会议核准国际民航组织旅行者身份识别方案战略，突出强调了国际民航组织公钥簿在该战略主要要素之一：检查系统和工具中，对于高效且可靠地读取及核实机读旅行证件(MRTDs)的重要作用(参见附录 A 图 2)。

3.6 但是，目前需要进行电子护照验证的所有类型的证书，并非都可以通过国际民航组织公钥簿进行交换。属于可信渠道或可信来源的国家签署证书当局的证书，是根据 Doc 9303 号文件采用两种方式分发的：外交双边交换，或者通过国家签署证书当局总列表，但不直接通过国际民航组织公钥簿。许多国家已经发现通过双边交换获取国家签署认证当局的证书比较困难，并表示对加入国际民航组织编制和公布总列表的可能性感兴趣。

3.7 公布此类总列表[1]将使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。国际民航组织秘书处与公钥簿委员会已经商定近期内在公钥簿当中提供一个由国际民航组织签署和公布的总列表。这将是国际民航组织公钥簿为其参加国提供的另一项重要服务，它既符合文件签署当局的利益，又符合边境管制当局的利益。

4. 国际民航组织公钥簿的效益

4.1 由于持有电子护照的公民可以借助电子护照附带的简化手续的便利，因此各国可以通过加入国际民航组织公钥簿受益。例如：一些国家只允许具有各自国家可靠数字证书来源(如公钥簿)的电子护照持有人使用其自动化边境管制通道。边境管制当局加入国际民航组织公钥簿也有益，以便获取及时可靠的信息来源，协助验证电子护照。查验电子护照的真实性和有效性，有助于可靠和高效地简化旅行者的手续，因为它能够加快合法旅行者的出入境手续。

4.2 国际民航组织公钥簿被认为具有成本效益，因为相对于维持双边基础设施以连接所有电子护照颁发国所需整体投资而言，公钥簿成员的会费是很小的一部分，并且可以通过电子护照收费进行回收。虽然某些成本可能难以估算，并且国与国之间存在较大差异，但是将根据各国的反馈以及公钥簿实施工作中的经验，制定成本效益分析(CBA)以展示国际民航组织公钥簿的效益。

[1] 总列表是国家签署证书当局的证书目录，其自身是由签署国家编制并进行数字签署的。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的证书双边交换、鉴别证书真伪，而后汇编一份目录并用其国家证书对其进行签署。包含该国信任的所有国家签署证书当局证书的这一目录被称为总列表，可以被上传到国际民航组织公钥簿。而后，信任总列表签发国、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。

5. 参加的状况

5.1 自大会上届会议以来，又有 13 个成员国加入了国际民航组织公钥簿，使公钥簿参加国总数达到了 51 个，如附录 B 所列。尽管约 80%的流通电子护照是由国际民航组织公钥簿成员国颁发的，但电子护照颁发国的数量、国际民航组织公钥簿参加国的数量，以及在日常边境管制运行当中利用国际民航组织公钥簿的国家实体与非国家实体的数量之间仍有很大差距。一个主要挑战就是利用芯片提供的全部能力，扩大对电子护照的全面检查，从而扩展边境管制当局对国际民航组织公钥簿的使用，以便从电子护照的实用价值当中全面受益。

5.2 为了鼓励参加国际民航组织公钥簿，附件 9 —《简化手续》的第 25 次修订介绍了对公钥簿建议措施 3.9.1 的修改。目前，该建议措施被分为两项建议措施：一项针对证件签发机关，另一项则针对边境管制当局。国际民航组织强烈建议参加公钥簿，对附件 9 的修改强化了这一立场。

5.3 作为持续开展的一项推广措施，在挪威举办了第二次公钥簿边境日活动(2014 年 10 月)。除其他外，这是审议使用国际民航组织公钥簿进行电子护照查验与使用国际刑警组织失窃和遗失旅行证件(SLTD)数据库之间的差异，以及审议失窃和遗失旅行证件能否与公钥簿联在一起的一次建设性机会。使用国际刑警组织失窃和遗失旅行证件数据库，是国际民航组织旅行者身份识别方案战略互用应用的一部分，其中包含了支持检查业务的边境情报应用。根据公钥簿谅解备忘录所述，公钥簿不涉及电子护照中有关个人信息的交换，例如证件身份识别号码(DIN)，这是失窃和遗失旅行证件数据库强制必报数据集当中报告的数据之一。因此，公钥簿不提供使其能够与国际刑警组织失窃和遗失旅行证件数据库相连的交换个人信息证书的机制。同样，2013 年 10 月、2014 年和 2015 年在蒙特利尔举行的三次国际民航组织机读旅行证件专题讨论会上，以及在布基纳法索(2013 年 11 月)、乌兹别克斯坦(2014 年 4 月)、尼日尔(2015 年 1 月)、刚果共和国(2015 年 5 月)和肯尼亚(2015 年 11 月)举行的旅行者身份识别方案地区研讨会上，组织了公钥簿座谈会。这些座谈会的重点是参加公钥簿应采取的实际步骤。

6. 新的公钥簿运营人

6.1 在进行国际民航组织公钥簿运营人运行合同招标程序之后，于 2015 年 3 月，与作为公钥簿完整设计、开发和运行主承包商的 Bundesdruckerei GmbH 签署了提供国际民航组织公钥簿的合同。根据这项新的合同，新的公钥簿参加国的登记费将从 56000 美元降至 15900 美元。同样，现有参加国的年费也将减少。值得注意的是，随着公钥簿参加国数量的增加，各参加国支付的年费将随之减少(参见附录 A 图 3)。

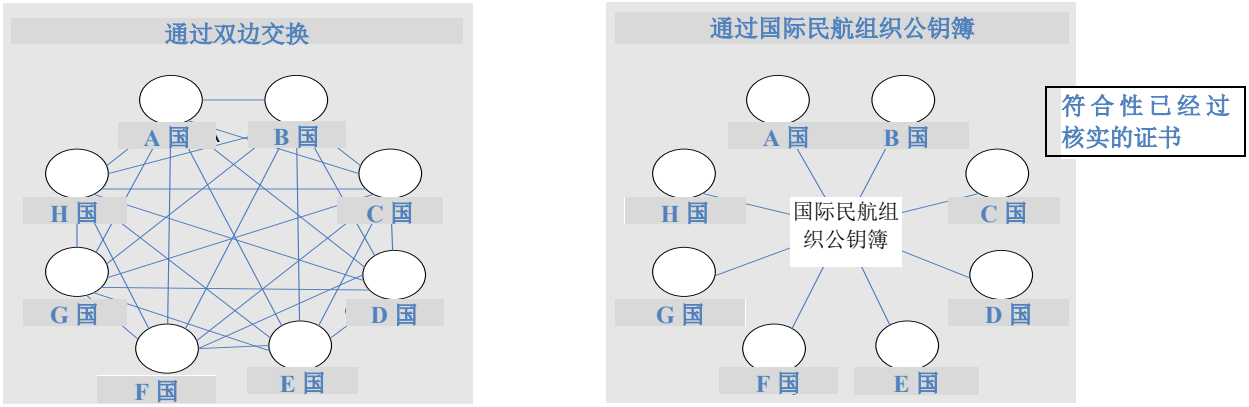
7. 优先事项和成果：2017 年至 2019 年

7.1 请大会根据附录 C 所述，核准已经得到理事会批准的下个三年期国际民航组织公钥簿的工作方案。

— — — — — — — —

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191个成员国，将需要进行36,290次双边交换，而与公钥簿仍然只需要2次交换。

注：DSCs：证件签署证书和CRLs：证书撤销列表

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

图 3. 登记费和年费

登记费(美元)		
2007 年至 2008 年	**2009 年至 2015 年**	**从 2016 年起**
85,000	**56,000**	**15,900**
年费(美元)		
公钥簿参加国数量	**2015 年及之前**	**从 2016 年起**
45-49	34,000	29,900
50-54	34,000	27,000
55-59	34,000	24,500

— — — — — — — —

附录 B

公钥簿参加国数量	公钥簿参加国及实体	加入日期	公钥簿参加国数量	公钥簿参加国及实体	加入日期
1	澳大利亚（公钥簿委员会成员）	19/03/2007	27	挪威	20/06/2011
2	新西兰（公钥簿委员会成员）	19/03/2007	28	保加利亚	12/10/2011
3	新加坡（公钥簿委员会成员）	19/03/2007	29	卢森堡	30/11/2011
4	联合王国（公钥簿委员会成员）	19/03/2007	30	瑞典（公钥簿委员会成员）	01/12/2011
5	日本（公钥簿委员会成员）	19/03/2007	31	联合国	14/06/2012
6	加拿大（公钥簿委员会成员）	19/03/2007	32	西班牙	10/07/2012
7	美国（公钥簿委员会成员）	02/11/2007	33	俄罗斯联邦	31/08/2012
8	德国	01/11/2007	34	马来西亚（公钥簿委员会成员）	09/11/2012
9	大韩民国	28/03/2008	35	阿根廷	13/12/2012
10	法国	19/06/2008	36	泰国	05/03/2013
11	中华人民共和国（公钥簿委员会成员）	26/11/2008	37	爱尔兰	08/03/2013
12	哈萨克斯坦共和国	19/12/2008	38	摩尔多瓦共和国	11/06/2013
13	印度	12/02/2009	39	比利时	31/10/2013
14	尼日利亚（公钥簿委员会成员）	13/04/2009	40	巴西（公钥簿委员会成员）	03/01/2014
15	瑞士（公钥簿委员会主席）	10/07/2009	41	卡塔尔	10/03/2014
16	乌克兰	30/10/2009	42	塞舌尔	14/03/2014
17	拉脱维亚	28/06/2010	43	乌兹别克斯坦	19/03/2014
18	捷克共和国	30/06/2010	44	菲律宾	21/03/2014
19	中国澳门	28/09/2010	45	伊朗（伊斯兰共和国）	18/05/2014
20	阿拉伯联合酋长国（公钥簿委员会成员）	25/10/2010	46	哥伦比亚	19/05/2015
21	中国香港	26/10/2010	47	罗马尼亚	03/02/2016
22	斯洛伐克共和国	23/11/2010	48	芬兰	26/02/2016
23	荷兰（公钥簿委员会成员）	08/12/2010	49	贝宁	03/03/2016
24	摩洛哥王国	29/12/2010	50	博茨瓦纳	05/04/2016
25	奥地利	31/12/2010	51	科威特	20/04/2016
26	匈牙利	15/02/2011			

— — — — — — — —

附录C

国际民航组织公钥簿工作方案

类别	优先事项	成果
国际民航组织的运行作用	优先事项 1：充当信托代理人。在持续的基础上恪尽职守，保持数字证书的完好性，并确保它们符合国际民航组织的标准以及 Doc 9303 号文件第 12 部分的规范。	确保公钥簿运行持续不断。
国际民航组织总列表	优先事项 2：通过国际民航组织公钥簿提供国际民航组织总列表服务，以便进一步支助电子护照验证的全球可互用性。	将为各国提供“一站式订购”的新服务，以验证电子护照的全部信息。
推广	优先事项 3：通过国家级信件以及组织公钥簿边境日等讲习班，或者结合旅行者身份识别方案专题讨论会及旅行者身份识别方案研讨会，加大推广力度。	提高对国际民航组织公钥簿的参与，并扩展对护照的全面检查，以使投资实现全面回报。
提高积极参与	优先事项 4：鼓励公钥簿所有成员积极上传和下载电子护照数据，以便提高边境管制点对照公钥簿验证电子护照的数量。	通过面向边境管制当局的有效行动计划，在边境管制中增加对国际民航组织公钥簿的积极使用。
加强秘书处对国际民航组织公钥簿的支助	优先事项 5：通过其他工具和资源，特别是通过制定成本效益分析，加强秘书处对公钥簿委员会和公钥簿参加国的支助。	确保公钥簿方案的需求得到满足，并确保向各国提供援助。

—完—