国 际 民 用 航 空 组 织

工 作 文 件

HLCAS-WP/8
6/6/12

高级别航空保安会议（HLCAS）

2012 年 9 月 12 日至 14 日，蒙特利尔

议程项目 7：机读旅行证件（MRTD）方案，预报旅客资料（API）和旅客姓名记录（PNR）的作用

公钥簿（PKD）

（由秘书处提交）

摘要

本文件介绍了国际民航组织公钥簿（PKD）的情况。目前，公钥簿包含 30 个参加方，国际民航组织鼓励所有成员国加入公钥簿，以加强电子护照查验的效率和有效性。

行动：请高级别航空保安会议核准第 6 段所载的建议。

1. 引言

1.1 电子护照（ePassport）又称生物识别护照，与传统的机读护照（MRP）类似，但包含一个用护照资料页所载的相同信息进行编码的电子芯片。电子芯片采用了数字签名，因此提高了安全性，并提供更多保护以防篡改，从而减少了欺诈的风险。

1.2 电子护照的益处完全取决于其芯片上所包含的生物识别及个人信息。反过来，芯片上的信息只有在能够被迅速且可靠验证的情况下才有用。据估计，目前有 93 个国家签发的 3 亿 5 千万本电子护照处于使用之中。这便带来了双边交流电子签名可行性，以保证芯片所存储电子护照数据签名有效性的问题。

1.3 为此，由国际民用航空组织（ICAO）主办，并应各成员国的要求，建立了公钥簿。公钥簿是一个数字签名的存储中心，简化并便利了电子护照芯片签名验证信息的多边交流。

2. 国际民航组织的作用

2.1 机读旅行证件技术咨询组（TAG/MRTD）建议，国际民航组织应担任建立公钥簿的指定组织。这项建议是根据本组织作为机读旅行证件标准的拟定者的长期历史记录、其作为联合国一个专门机构的国际地位，及其在文件保安方面重大利益的基础上提出的。由公钥簿委员会进行监督并由电子护照签发国家进行供资的一个中立网站，被视为提供一个受信赖的来源，所有成员国中的政府检查机构、航空公司及其他实体，都可以从其下载正在使用的所有公钥，用来核实护照作为身份文件的真伪。

2.2 公钥簿委员会对公钥簿中心的监督，为电子护照的保安提供了一个合作、互用的制度，参与其中的国际民航组织所有成员国均可对其进行访问。具有同等重要意义的是首先查验旅行者护照、担任“前线”的航空器运营人可访问其核心的一个公钥簿。作为防止涂改或伪造护照、或假冒者使用被盗护照的一个手段，公钥簿提供了一种高度有效的保安措施。

2.3 公钥簿委员会是常设机构，负责国际民航组织的公钥簿。它由国际民航组织理事会根据公钥簿谅解备忘录（MoU）的规定任命的 15 名成员组成。公钥簿委员会负责国际民航组织公钥簿的财务及运行监督。

2.4 国际民航组织的主要作用，就是作为一个托管代理，验证数字签名的来源及其数据的完好性，并保护公共密钥。验证来源意味着确定数字签名或公共密钥是由适当当局签发的。国际民航组织还负责向公钥簿委员会提供运行及行政支助。

3. 国际民航组织公钥簿的益处

3.1 国际民航组织公钥簿促进电子旅行证件验证系统的全球互用性。它作为一个中央代理，管理各种证书及证书吊销目录的多边交流，将其用来验证电子护照芯片内的数字签名。利用公钥簿，对电子护照芯片上的数据进行篡改或补充的任何企图，都会在查验时被即刻发现。目前，公钥簿被当作实施《机读旅行证件》（Doc 9303 号文件）中所制定规范的一项无可替代的宝贵工具。

3.2 对公钥簿的参与，确保了提供适时信息，以便验证电子护照的真伪，从而简化并加强边境管制通道的电子护照查验过程的保安，并会带来便利迅速安全的过境流动。只有当边境管制工作中使用电子护照读取器时，才能够证实电子护照的真实性未被涂改或伪造。

3.3 公钥簿具有较高的成本效益和效率。目前，一次性注册费是 56,000 美元。还有一项经常性年费约 56,000 美元，用来涵盖公钥簿运营人的运行成本（43,000 美元）及国际民航组织的行政费用（13,000 美元）。考虑到维护一项双边基础设施，以便与所有电子护照签发国相连接，以及部署电子读取器的所需投资，这些年费是十分轻微的。通过公钥簿共享此类数据，简化了验证过程，并减少了相关的行政费用，同时遵守了各项国际标准。而且，随着更多国家成为参加方，各项费用会进一步降低。

4. 参与

4.1 在 2011 年中，有五个国家 —— 保加利亚、匈牙利、卢森堡、挪威和瑞典 —— 加入了公钥簿。加上澳大利亚、奥地利、加拿大、中国、捷克共和国、法国、德国、中国香港特别行政区、印度、日本、哈萨克斯坦、拉脱维亚、中国澳门特别行政区、摩洛哥、荷兰、新西兰、尼日利亚、大韩民国韩国、新加坡、斯洛伐克、瑞士、乌克兰、阿拉伯联合酋长国、联合王国和美国，现有 30 个公钥簿参加方。

4.2 尽管如此，电子护照签发国的数量与公钥簿参加方的数量之间，仍然存在巨大差距。公钥簿所面临的主要挑战就是扩大参与，以便各国能够对其正在加入一个可行的全球解决办法充满信心。

4.3 作为一项正在推广的有效措施，2011 年 9 月于蒙特利尔举行的国际民航组织机读旅行证件（MRTDs）、生物识别和安全标准第七次专题讨论会暨展览会期间，组织了一次公钥簿讲习班。在卡塔尔（2011 年 11 月）、新加坡（2011 年 12 月）和巴西（2012 年 4 月）举行的机读旅行证件地区研讨会期间，举办了类似的活动。各讲习班的出席人数较多，并得到了如何加入公钥簿的实际步骤方面的指导。

5. 运行和行政

5.1 公钥簿是在成本回收的财务模式基础上开发和运行的，完全由来自参与公钥簿的各国付费提供支助。

5.2 为了公钥簿的完整设计、开发和运行，已于 2006 年将一份合同授予 Netrust。公钥簿已于 2007 年 3 月开始运行，并且公钥簿的服务是向所有参加方提供的，并向世界各地的其他商业和一般用户提供。与 Netrust 签订的运行合同已圆满结束，并得到了国际民航组织和公钥簿委员会的验收。

5.3 2011 年 12 月 31 日结束的合同，已另外续延三年，于 2012 年 1 月 1 日起生效。经续延的运行合同的一个主要特点，就是一旦公钥簿的有效参加方数量达到 31 个，将把目前 43,000 美元的公钥簿运行费，减少约 12,000 美元，降到每个参加方每年 31,000 美元左右。公钥簿的有效参加方数量达到 65 个时，预计将再次减少费用。

5.4 2012 年，国际民航组织与公钥簿有关的工作人员费用、旅行、职业责任保险，将由 2011 年国际民航组织经常方案预算的盈余供资。这项供资将减少本年度公钥簿参加方的费用。经过预算方面的审议后，可能还会保证 2013 年对公钥簿的类似供资。

5.5 公钥簿的管理和行政工作，引发在 2011 年举行了 3 次公钥簿委员会会议。按照谅解备忘录的要求，根据必要情况改进并扩展了确保公钥簿平稳运行的行政、财务和技术制度方面的效率。这包括但不限于关于公钥簿委员会的组成及财务条例方面的决定。

6. 结论和建议

6.1 请高级别航空保安会议建议各国：

a) 参加公钥簿；

b) 签发电子护照；和

c) 使用电子护照读取器实施自动化边境管制查验。

—完—