国 际 民 用 航 空 组 织

工 作 文 件

A40-WP/7
EX/4
5/7/19
信息文件
(Information paper)

大会 — 第 40 届会议

执行委员会

议程项目 14：简化手续方案

参加国际民航组织公钥簿(PKD)的益处

(由国际民航组织理事会提交)

执行摘要

本文件介绍了国际民航组织公钥簿(PKD)的信息，强调了各国加入国际民航组织公钥簿所带来的益处。建立国际民航组织公钥簿是为了支持各国获取验证和认证电子护照所需的公钥信息。它是国际民航组织旅行者身份识别方案(TRIP)战略的重要组成部分，因为它支持以高效和具有成本效益的方式读取和核证旅行证件的程序。使用相关的公钥基础设施证书对电子护照进行核证，可以为边境管制当局提供旅行证件真实且未经改动的保证，从而认证电子护照中包含的生物识别信息，并允许边境清关过程各方面的自动化。电子护照的核证是利用各国在制定此类旅行证件方面投资的一个基本要素，有助于改善边境安保，打击恐怖主义和犯罪并促进全球航空旅行的安保。由于国际民航组织公钥簿同时满足简化手续和安保需求，利用国际民航组织公钥簿将有助于消除国家边境管制系统安保方面的差距，同时增强旅行者在旅途中的体验。公钥簿目前包括 66 个参加方。国际民航组织鼓励所有成员国加入并积极使用公钥簿，以提高电子护照验证的效率和有效性。

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：	无需额外资源。
参考文件：	C - DEC 216/2 号决定 Doc 9303 号文件(第 7 版)《机读旅行证件》 A40-WP/6 号文件：国际民航组织公钥簿(PKD)的发展情况 A40-WP/8 号文件：国际民航组织旅行者身份识别方案(ICAO TRIP)战略的发展情况

1. 背景

1.1 电子护照(ePassport)是一种机读护照(MRP)，内嵌带有加密数据的集成电路(IC)芯片，存储与其持有人相关的护照第 2 页上可见的个人信息。当发行国对电子护照进行个人化时，护照被锁定，因此无法修改，从而为机读护照增加了一层安保保障。

1.2 除护照资料页上的旅行者个人信息外，电子护照芯片(附录 A)还存储国家特定的数字安保特性，称为国家数字签名。这些数字签名是每个国家独有的，作为证件安保对象(SOD)可靠地存储在电子护照的芯片中，使其可以通过签发国的公钥基础设施(PKI)核证。附录 B 列出了如何在电子护照的签发和核证之间建立关联性，以及如何使用国际民航组织公钥簿(PKD)对其认证进行确认。当扫描电子护照并读取芯片数据时，其经过认证的数字签名告诉边境管理机构芯片上的数据是真实的，且是由国家签发的，且没有被更改过。

1.3 这一认证通常称为电子护照验证，是通过核证芯片上的数字签名来验证电子护照的真实性和完整性的过程。接收国边境管制机构若要对外国旅行者的电子护照进行认证，则接收国必须能够获取签发国的某些信息。

1.4 目前有 140 多个国家和非国家实体(如联合国)在签发电子护照或电子机读旅行证件(eMRTDs)，有约 10 亿电子护照在流通中。虽然国家数字签名可以双边交换，但是签发电子护照的国家越来越多，相应大量的电子护照在流通之中，这将导致产生一个高度复杂无效的系统，可能造成简化手续~~该~~过程延误并产生错误。建立国际民航组织公钥簿是为了将其作为交换认证电子护照所需信息的中央信息库。因此，公钥簿为各国提供了高效的手段，上载自己的信息和下载其他国家的信息供在边境管制中加以使用，以加强简化手续与安保。如附录 C 所示，并不是所有签发电子护照的国家都是公钥簿参加方。

2. 公钥簿在国际民航组织旅行者身份识别方案(TRIP)战略中的作用

2.1 国际民航组织旅行者身份识别方案战略采用的方法包括五个相互关联的要素，帮助各国建立和确认旅行者的身份。这五个要素是相辅相成的。有效的旅行者身份识别有助于优化国际旅行的经济、社会和政治益处，也有助于管理安保风险并通过更好地将资源用于相关人员来回应边境威胁。

2.2 国际民航组织旅行者身份识别方案的各要素共同发挥作用，使各国能够识别旅行者并进行有针对性的旅行者风险评估，特别是通过将检查系统和工具(IST)与可互用的应用(IA)联系起来做到这一点。收集旅行者信息更是提供了关于进入各国的外国人的身份证明，从而使国际民航组织旅行者身份识别方案周期得以完整。

2.3 检查系统和工具使边境当局能够采集、核证和记录机读旅行证件(MRTD)中包含的旅行者数据。可以在旅程的不同阶段对旅行证件持有人进行控制：出发前、到达前、入境、停留和出境。通过可互用的应用实现关于旅行者及其旅行证件的全球数据共享，从而增强了这些控制。国际民航组织旅行者身份识别方案战略五个要素中的这两个与边境管制管理(BCM)直接相关。 各国使用的边境控制系统(BCS)将可互用的应用与检查系统和工具整合在一起。

2.4 检查系统和工具(IST)采集、核证、匹配和记录机读旅行证件包含的旅行者数据，而可互用的应用可以在全球范围共享旅行者及其旅行证件的数据。将检查系统和工具与可互用的应用整合到国家边境控制系统中，就可以在旅行者旅程的不同阶段进行旅行者风险评估。通过使用过境国和目的地国在旅程的每个阶段可获得的新信息来识别旅行者，从而作出这种评估。附录 D 载有国际民航组织旅行者身份识别方案要素的描述、检查系统和工具及可互用的应用下的一些项目及其与典型的旅行者旅程的不同阶段的互动方式。

2.5 高效边境管制管理的基础是通过使用符合国际民航组织 Doc 9303 号文件《机读旅行证件》技术规范(网址为 https://www.icao.int/publications/pages/publication.aspx?docnum=9303)的标准化互用式机读旅行证件和电子机读旅行证件，有效地读取机读旅行证件数据要素。各国应遵守和充分应用这些技术规范，以确保实现互用性，并切实获得相关的安保和简化手续益处。

3. 在边境使用公钥簿的益处

3.1 从签发国角度来看，使用具有安全可靠的网络和 PKI 基础设施的现代化签发技术，既可增强对于该国所签发的护照的信任也可加大对于国际安保举措的参与。此外，还可带来灵活性，以便能够实施电子旅行许可(ETA)、自动边境管制(ABC)门等较新举措和以电子护照技术为基础的所有可用现代工具。为了充分发挥成为公钥簿成员的益处，使用公钥簿应该与加强边境检查相结合。

3.2 2014 年，联合国安理会(UNSC)通过了第 2178 号决议，其中特别声明：“重申所有国家应通过有效的边境管制和签发身份证和旅行证件方面的管制，并通过防止伪造、假造或冒用身份证和旅行证件的措施，防止恐怖分子和恐怖集团的流动”。加入和使用国际民航组织公钥簿可以帮助各成员国实施这项安理会决议，因其被认为是一种宝贵的工具，目前没有可行的替代方案。从国家的角度而言，这是的一种积极做法，既有助于加强旅客的旅行体验也有助于打击国际恐怖主义。

3.3 如果没有能力在外国边境验证电子护照中的电子数据，则旅行证件必须完全视同机读护照，不提供额外的安保。国际民航组织公钥簿提供了一种简单、快速和具有成本效益的方法来验证电子护照。 只有在边境管制点使用预先加载了公钥簿数据的电子护照阅读器，才能确认电子护照数据芯片的真实性。因此，参加公钥簿可确保及时提供信息以验证电子护照的真实性。这一过程简化了边境上的电子护照验证过程，并通过迅速检测受损或错误的芯片，便利快速可靠的跨境移动。

3.4 从电子护照签发国的角度来看，重要的是确保世界各地的边境当局验证其电子护照。与维持用于连接所有电子护照签发参加方的双边基础设施所需的投资相比，公钥簿成员费用较低。通过公钥簿渠道共享数据可以减少双边做法的相关管理成本。此外，随着公钥簿参加方数量增加，公钥簿费用会减少。

3.5 在边境使用公钥簿可为电子护照的实物和电子安保提供强有力的信任。可将实物资料页和芯片数据与可视检查相匹配，而人脸识别可应用于到达旅客的照片；这样，如果检查得当，冒充者和伪造者入境就面临多重障碍。

3.6 参加国际民航组织公钥簿为签发国的边境管制机构提供首次获取服务。根据 Doc 9303 号文件第 12 部分的规定对电子护照进行核证可让边境当局相信，所审查的旅行证件是由有关当局签发的并且证件上记录的信息未被篡改。Doc 9303 号文件第 12 部分细述了 PKI 的规范，这是机读旅行证件整体安保中一个非常重要的组成部分，因其提供了负责为各国制定国家公钥基础设施（NPKI）系统的信息技术专家所需的要求，涵盖的题目包括作用和职责、密钥管理、分发机制、PKI 信任和验证。国际民航组织的公钥簿工具提供对其他国家公布的国家公钥基础设施的可靠和具有成本效益的访问，并得以进行扎实的电子护照验证。

3.7 此外，成为公钥簿的参加方使得电子护照签发国能够与其他国家分享经验并从其经验中受益，同时获得多边数据交换的高效率，并便利其本国公民的国际旅行。

3.8 最后值得指出的是，公钥簿委员会正在最后确定一份主列表，预计将于 2019 年底提供，这将大大补充国际民航组织公钥簿目前提供的服务。

4. 结论

4.1 加入国际民航组织公钥簿应该是加强国家身份管理总体工作的一部分。防止犯罪分子以虚假身份获得真正的电子护照是一项至关重要的工作，必需将签发系统与民事登记数据相互关联。

4.2 应该为公钥簿的推行做好妥善的准备。各国应从一开始就确保遵守国际民航组织的规范。各国需要处理相关的国家和国际行政步骤及技术问题，以将其系统整合到国际民航组织公钥簿之中。关于实施国际民航组织公钥簿的实际步骤，详细说明载于附录 E。

4.3 由于国际民航组织的标准、建议措施和规范，今天每个国家都有机会受益于这一框架，该框架创建了一个真正的全球可互用系统，用于在国际边境读取和核证护照。

4.4 这一系统是对全球安保的一项重大贡献，并为机场、陆地和海洋边界的移民进程提供了便利。在机读护照的非接触式芯片中添加面部影像等生物识别特征，表明安保水平已显著提高。现在要由全世界的边境管理机构来升级其基础设施，以便能够读取这些特征并在边境系统中用其核证持有者的身份。

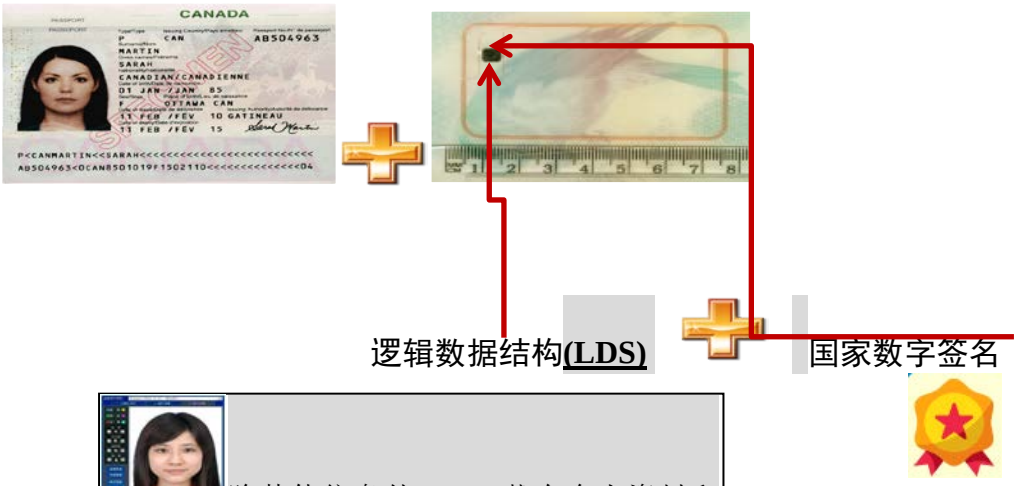
— — — — — — — —

附录A

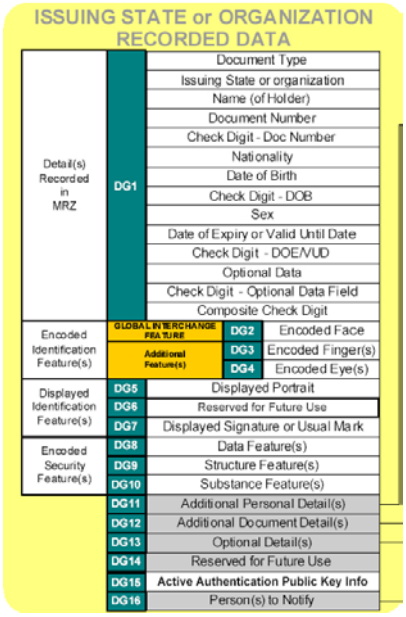
什么是电子护照?

国际民航组织将电子护照定义为一种内置非接触式集成电路(IC)芯片的机读护照(MRP)，该芯片储存有机读护照资料页的数据，护照持有人的生物特征测量结果和一个用密码技术保护数据的安全对象，并符合Doc 9303号文件第4 部分所载规范。

机读护照　　芯片



除其他信息外，LDS载有个人资料和强制性生物识别数据(人脸图像)。



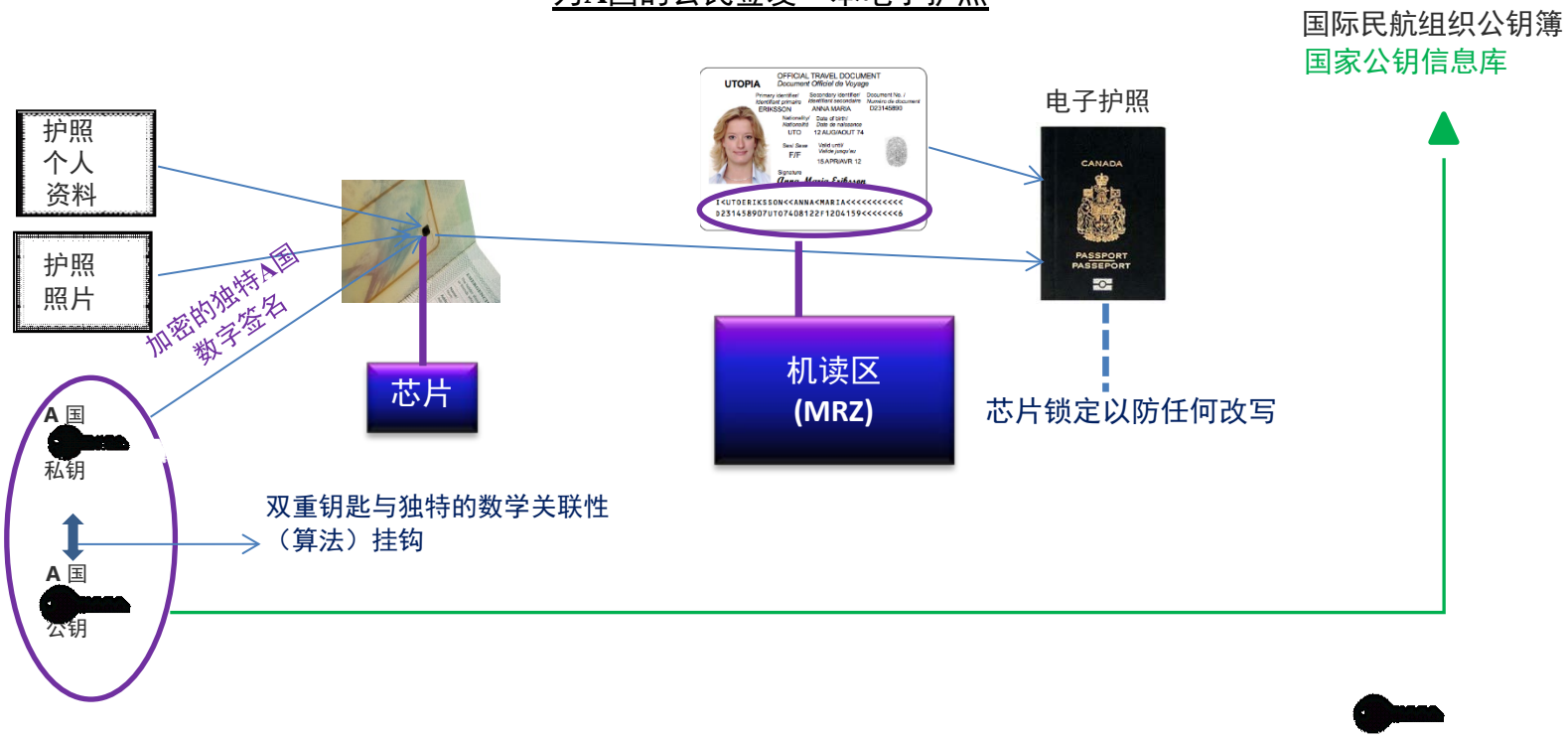
正确验证电子护照芯片中的签发国数字签名，指向置于芯片LDS部分之中的数据的真实性和完好性。

— — — — — — — —

附录B

从电子护照的签发到其在边境的核证：信任链

为A国的公民签发一本电子护照



A国公民到达B国边境时的检查步骤

第1步

机读区(MRZ)数据只不过呈现资料页上某些印制信息，使计算机能以电子方式准确地阅读印制信息。

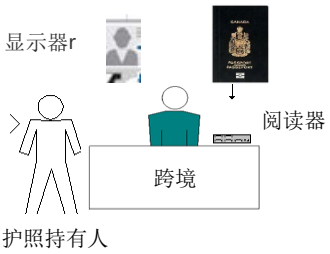
官员在阅读器上对护照进行扫描以阅读MRZ，使电子护照的芯片得到访问。

MRZ的内容载有一把用来访问芯片的钥匙，只有在钥匙匹配时才允许芯片与阅读器进行交流。

如果匹配，数据和照片得到检索，检查进行到第2步。

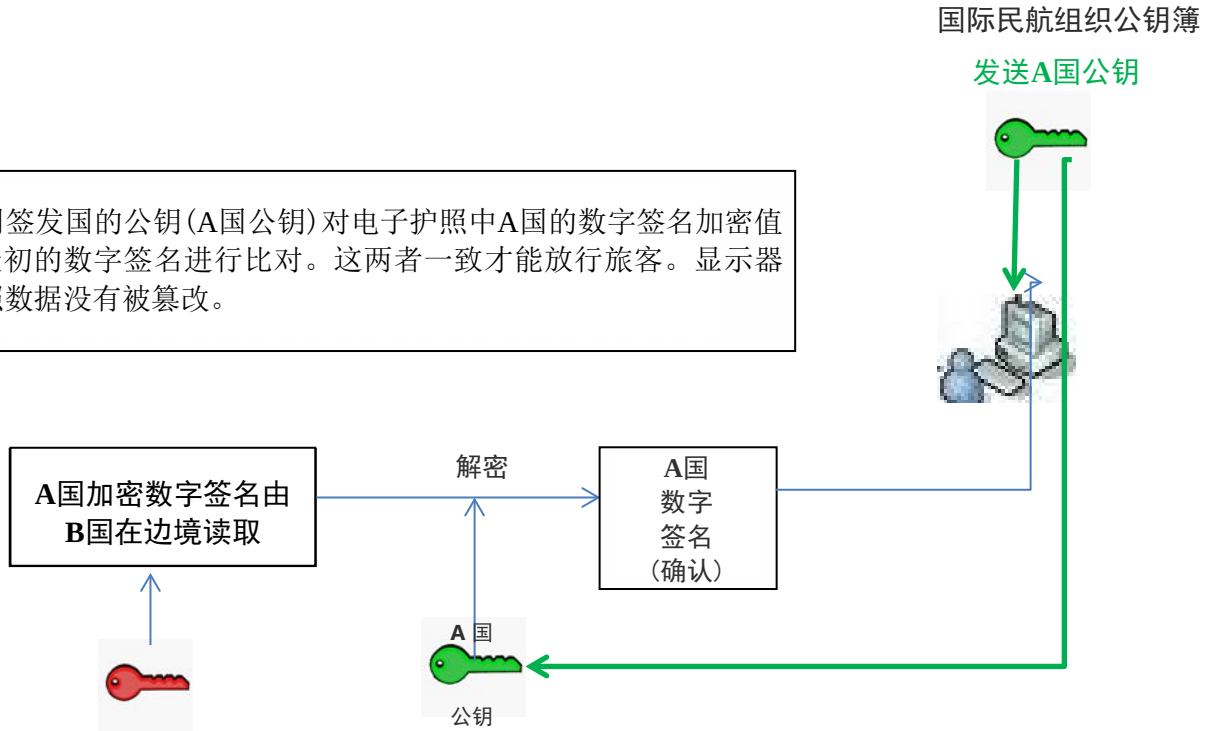
第2步

芯片被打开，官员核对持有人是否与护照上的照片以及显示器上展示的护照芯片中的数据和照片相匹配。下一步包括确认护照是由合法当局签发的，且在签发后没被篡改过。



第3步

为了认证电子护照，用签发国的公钥(A国公钥)对电子护照中A国的数字签名加密值进行解密，并与A国最初的数字签名进行比对。这两者一致才能放行旅客。显示器上的数值也要确认护照数据没有被篡改。

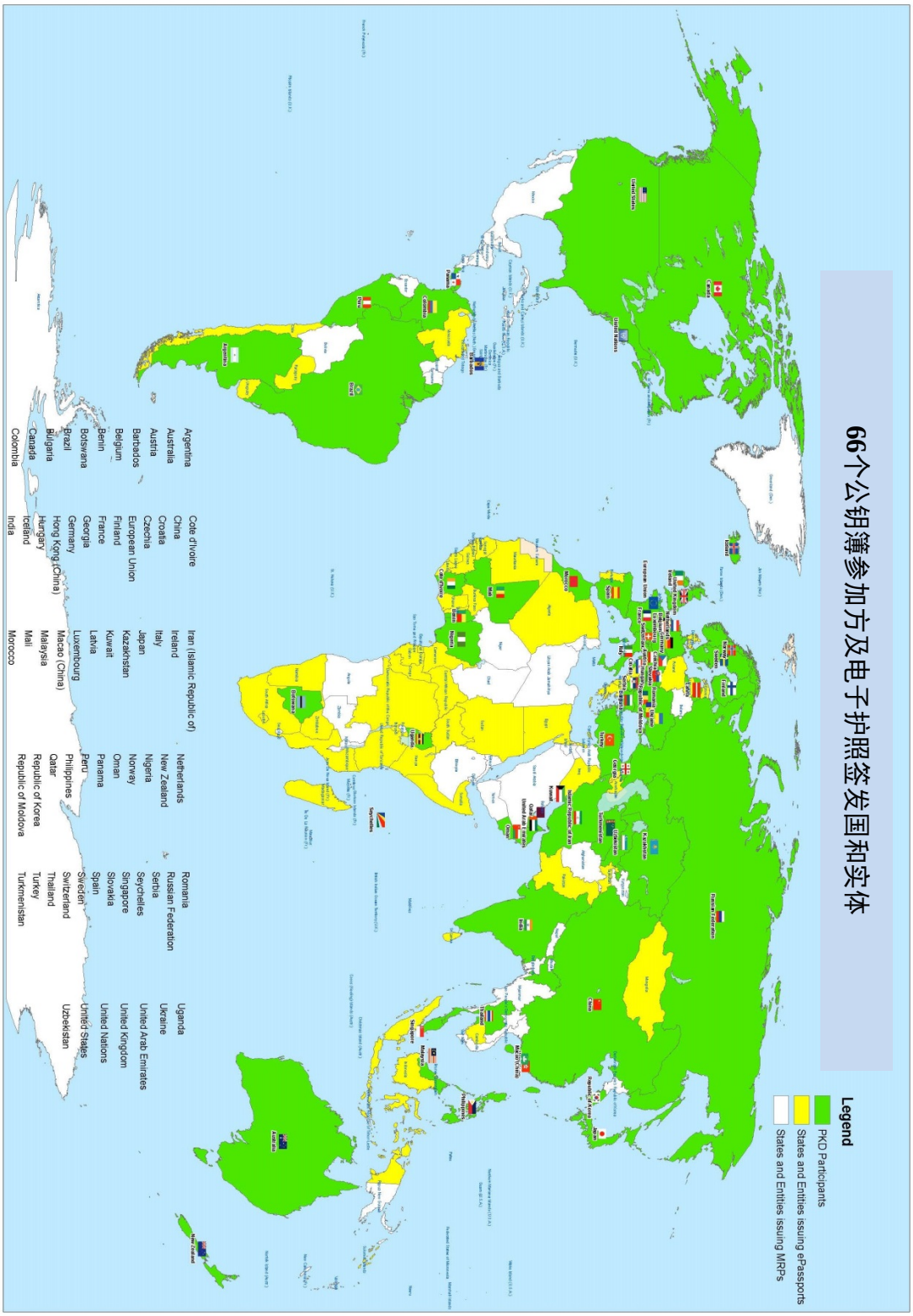


国际民航组织公钥簿的作用是验证每个国家公钥的真实性，否则电子护照的整套数据就可能是伪造的。这一点通过每一公钥簿参加方公钥的正式输入仪式加以确认。但是，国际民航组织公钥簿不保证护照持有人的身份，只保证电子护照中的数据自其由某个特定的出品人推出后未做改变。

— — — — — — — —

附录C

签发电子护照的国家和实体及公钥簿参加方

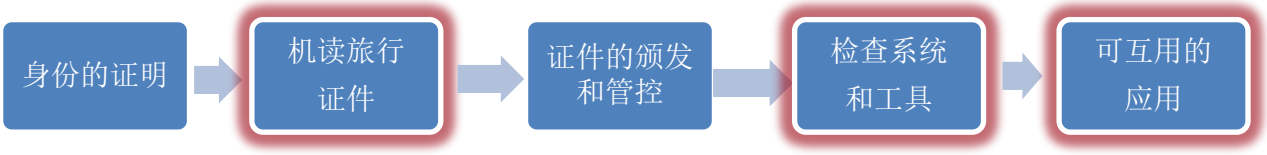


— — — — — — — — —

附录D

国际民航组织旅行者身份识别方案(TRIP)战略和边境管制管理

国际民航组织旅行者身份识别方案战略五大要素:其中三个与公钥簿的使用相关

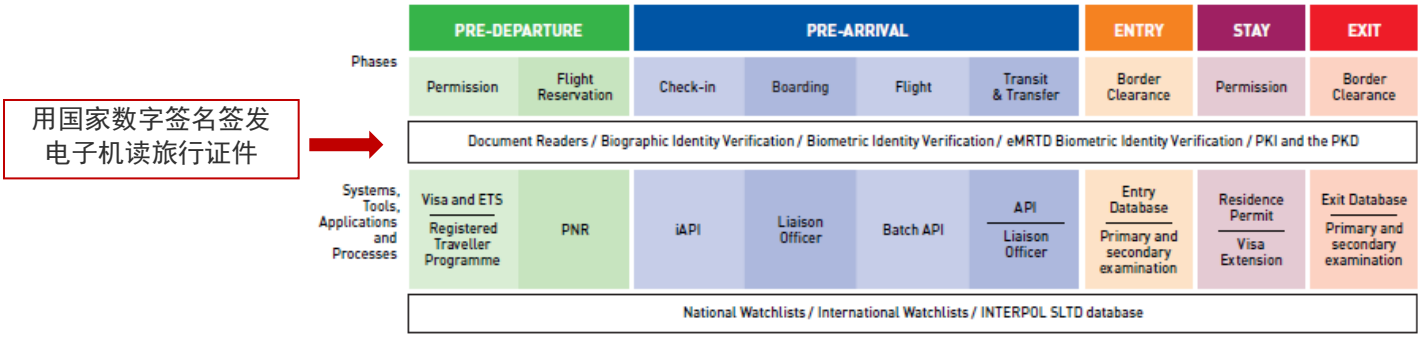


国际民航组织旅行者身份识别方案战略第四项和第五项要素不同项目的突出样例见下表

检查系统和工具	可互用的应用
签证和电子旅行系统(ETS)	预报旅客资料(API)和互动式预报旅客资料(iAPI)
证件阅读器	旅客姓名记录(PNR)数据
公钥基础设施(PKI)	公钥基础设施(PKI)
国际民航组织公钥簿(PKD)	国际民航组织公钥簿(PKD)
个人身份核证	电子机读旅行证件(eMRTD)生物特征身份核证
生物特征身份核证	国际刑警组织(INTERPOL)被盗和遗失旅行证件(SLTD)数据库
国家监控名单	国际监控名单
出入境数据库	自动边境管制(ABCs)
自动边境管制(ABCs)	

旅行者旅程的不同阶段

对于使用国际民航组织公钥簿工具的准备，应始于出发前这一阶段，即签发电子机读旅行证件(eMRTD)(国际民航组织旅行者身份识别方案第二要素)之时。在入境阶段，国际民航组织公钥簿工具(国际民航组织旅行者身份识别方案第四要素)将用于认证电子机读旅行证件，而其可互用性(国际民航组织旅行者身份识别方案第五要素)将促成电子机读旅行证件与其他可互用的应用相连。



在旅程的所有阶段:使用证件阅读器以可靠和高效地采集旅行者的详细身份资料。使用从旅行证件中读取的数据进行个人身份核证检查。通过使用公钥簿工具，生物特征身份核证和公钥基础设施认证(如有)有助于确保对旅行者的身份识别。在以充分的置信度确定了旅行者的身份后，国家可核对国际刑警组织(INTERPOL)被盗和遗失旅行证件(SLTD)数据库以及国家和国际监控名单，提供信息以进行旅行者风险评估。

— — — — — — — —

附录 E

加入国际民航组织公钥簿的实用步骤

1) 审查国家立法: 在推出电子护照并参加国际民航组织公钥簿之前，必需对国家立法框架进行一次透彻审查 。

2) 界定作用和职责并实施国家公钥簿: 国家有责任确保通过国际民航组织公钥簿分享的材料的质量。这要求清楚地界定国家各利害攸关方的作用和职责，并遵守和维护各项技术标准。这一点尤其适用于与国际民航组织公钥簿相互上载和下载各类证书的国家公钥簿(NPKDs)，和国家签名认证机构(CSCA)。

3) 加入国际民航组织公钥簿: 国家要迈出的第一步，是与国际民航组织签署公钥簿谅解备忘录(MoU)；然后有 15 个月的时间，将国家公钥簿与国际民航组织公钥簿连接并启动上载和下载。愿意成为国际民航组织公钥簿参加方的国家，应与秘书处就登记流程细节进行协商。.

4) 将国家公钥簿整合到国际民航组织公钥簿之中: 最后一步，是将该国的国家公钥簿完全整合到国际民航组织公钥簿之中，这包括国家公钥簿与国际民航组织公钥簿相互上载和下载各类证书和撤销清单。

— 完 —