常见问题

（2013 年 8 月 23 日）

i) 什么是公钥簿（PKD）?

国际民航组织公钥簿是管理世界范围证书和证书撤销表互换的中央平台。这些证书和证书撤销表 用于验证电子护照和其他机读旅行证件的 RFID 芯片中包含的数据电子签名。公钥簿内容经过预 先验证，可免费下载。

ii) 公钥簿增加了哪些价值?

随着越来越多的国家引进电子护照，公钥簿保证了国家之间交换过程的简便快捷。公钥簿对于尽 可能减少所交换的证书和证书撤销十分重要，从而确保及时上传和下载，并管理遵守技术标准的 情况，确保实现和保持可互用性。

iii) 为什么国际民航组织为公钥簿提供支持很重要?

基于国际标准组织的标准，国际民航组织颁布了 Doc 9303 号文件，作为电子护照和其他机读旅行 证件的核心参考文件。国际民航组织现有的专门知识及其声誉，使支持公钥簿成为理所当然和不 言而喻的一种结果，它在其中的作用是无 可替代的。

iv) 公钥簿都有哪些参加方?

公钥簿的参加方均显示在公钥簿网站上。

 <http://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx>

（见“国际民航组织公钥簿 — 当前运营状态”）

v) 从哪里可以找到参加通知书?

参加通知书可从公钥簿网站上下载。

[http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU(includeslanguageversion(s))/NoticeofParticipation-Model.pdf](http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU%28includeslanguageversion%28s%29%29/NoticeofParticipation-Model.pdf)

（见“国际民航组织公钥簿的程序”）

vi) 在哪里可以找到登记通知书?

登记通知书可从公钥簿网站上下载。

[http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU(includeslanguageversion(s))/NoticeofRegistration-Model.pdf](http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU%28includeslanguageversion%28s%29%29/NoticeofRegistration-Model.pdf)

（见“国际民航组织公钥簿程序”）

vii) 参加公钥簿需支付哪些费用?

公钥簿收费表可从公钥簿网站上下载。

<http://www.icao.int/Security/FAL/PKD/Documents/PKDFinanceDocuments/B-Fin-123-PKD%20Fee%20Schedule%202016.pdf>

（见“公钥簿收费表”）

通过简单快速的网站接入(<https://pkddownloadsg.icao.int/>)，可免费下

载整个公钥簿内容。然而，未参加公钥簿的国家或非国家实体所运行的边检控制或类似的应用程 序可能会需要多种公钥簿接入。由于这种接入的安装和维护要求公钥簿运作人采取持续行动，谅 解备忘录允许用户费用定义中包含新出现的成本。具体内容见公钥簿收费表。

ix) 什么是有效参与?

在提交参加通知书并支付了登记费后，也即参加生效后，公钥簿参加方为连通其国家公钥簿与中 央公钥簿着手进行准备。在此期间，公钥簿运作人将提供支助。经过准备阶段后，公钥簿参加方 开始从公钥簿上传和下载预定内容，由此进入“有效”参与状态。

x) 公钥簿可提供哪些内容供免费下载？ 公钥簿提供文件签署人证书（DSC）和证书撤销表（CRL）以及国家签署证书当局（CSCA）证书

总列表，供免费下载。

xi) 如何能够通过公钥簿查验电子护照？ 查验电子护照须通过完整的信任链进行。这一信任链包括使用文件签署人证书及对 RFID 芯片数

据进行电子签名验证。它还包括对护照颁发国的 CSCA 以及文件签署人证书进行验证。必须证实 使用的所有证书材料不出现在当前的证书撤销表中。

xii) 能否使用公钥簿获取电子护照中的指纹？ 不能。尽管电子护照签名查验和获取电子护照中的指纹使用的是公钥簿基础设施（PKI）技术，但

无法通过公钥簿内容来获取指纹。

xiii) 什么是 15 个月的截止期限？

参加生效后，公钥簿参加方有 15 个月的时间开始有效参与。伴随着有效参与，年费被扩展至包括 活动费用（见公钥簿收费表）。

xiv) 通过互联网提供公钥簿有什么益处？ 证书和证书撤销表的互换必须做到可靠和及时。这种互换不能通过电子之外的其他方式来实现。

为保护公钥簿在互联网上免受攻击，采取了各种常用和适当的措施。

xv) 下载公钥簿时是否会带来病毒或其他恶意软件的风险？ 不会。公钥簿内容是案文文档，其中不包含任何脚本或可执行编码。

公钥簿网站为：<http://www.icao.int/Security/FAL/PKD/Pages/default.aspx>

,其中含有基本信息及大量可供下载的文件，可用来进行详细研究。可以与国际民航组织秘书处ICAO-PKD@ICAO.INT 或公钥簿委员会主席联络。另外，还有一个链接用来提交投诉或提供反 馈信息。

xvii) 公钥簿用来查验电子护照芯片上的数字签名。如何能够通过这种方式检测伪造欺诈？ 现代生物特征测定系统可在数秒中内将存储在电子护照中的人脸影像与现场拍摄的人脸影像进行

对比。这样，能够可靠地检测伪造欺诈中常有的微小差别，从而可以对相关人员进行二次检查。

基于公钥簿的电子护照芯片签名查验可确定芯片数据的完整性（包括生物特征测定在内）。如 果需要依靠存储在芯片中的人脸影像，对芯片进行验证至关重要，尤其是在边检站客流量很大 的情况下。

xviii) 公钥簿是否对指纹获取提供交换证书的简化手续？ 公钥簿谅解备忘录不涉及有关电子护照中辅助生物测量的文件验证人证书及相关信息的互换。

xix) 对于发行了电子护照但缺少自动化边检控制的国家，公钥簿有哪些额外价值？

对公钥簿的有效参与，意味着其他国家可通过公钥簿验证参与国家颁发的旅行证件。这意味着， 该国公民旅行时可享有更简便的过境手续，它给公民带来的益处显而易见。

xx) 为什么公钥簿中包含非标准的规范性内容？ 目前流通着一些有效的电子护照，这些护照是在公钥簿委员会为改进数据质量而采取的大量措

施生效之前颁发的。由于无法对这些护照进行简单的互换，因此，在芯片验证过程中，须明确 表明需要对哪些在电子护照制作期间使用的数据加以特别注意。

xxi) 公钥簿委员会为改进数据质量采取了哪些措施？ 如果公钥簿参加方试图上传非标准的规范性内容，这种做法只有在经公钥簿委员会适当审议之

后才能被接受。审议过程包括在最多六个月的过渡期内纠正非规范性的承诺。在过渡期过后， 再次显示同样的非规范性内容将被拒绝。在导入或上传以进行一致性测试前，公钥簿参加方可 相向公钥簿运作人发送CSCA证书或CSCA链接证书。

xxii) “严格的安全外交手段（带外分发）”是什么意思？ 此种分发可通过个人外交交换、外交邮袋或任何其他类似的程序或方式进行。也可通过电子邮

件、网站等进行，前提是接收人必须通过带外通信（例如，使用外交邮件寄送的印刷加密哈希 算法），以验证所收到的证书的完整性。

证书是公开信息，因此可以在网站上公布。这样做没有违反国际民航组织的准则。

xxiv) 从哪里可以找到将内容上传至公钥簿的技术信息？ 在参加公钥簿后，所有技术问题均可通过阅读国际民航组织公钥簿办公室和公钥簿运作人发送

给参加方的文件得到解答。您还可以在公钥簿网站上查看关于下载的公钥簿文件。请特别阅读 公钥簿规则和公钥簿程序的相关内容。同时，请下载 Doc 9303 号文件增补部分。该部分文件可 在机读旅行证件网站上找到，其中含有有关机读旅行证件技术规范的最新信息。

xxv) 如何区分中国、中国香港和中国澳门的 CSCA 证书、文件签署人证书（DSC）和证书撤销表

（CRL）？

中国有三个护照颁发地点：

i) 一个是中国大陆；

ii) 一个是中国香港；和

iii) 一个中国澳门。

在 CSCA 证书、文件签署人证书和证书撤销表中，它们拥有同一个国际标准组织的 3166 国家代码

（即：C = CN）。因此，在公钥簿中，这些证书和证书撤销表均存储在带有国家代码“CN”的部分中。 边检机关可使用国家代码（C）和组织（O）两者来区分条目，以便区别这三个颁发地点的证书和证书 撤销表。中国、中国香港和中国澳门证书特征的对比如下：

|  |  |  |
| --- | --- | --- |
| 中国 | 中国澳门 | 中国香港 |
| C C= CN | C C= CN | C C= CN |
| O O= 中国政府 | O O= 澳门特别行政区 | O O= 中国香港 |

xxvi) 为什么使用总列表时可以免费，而参加公钥簿却需要付费？

就 CSCA 证书而言，公钥簿中的总列表涵盖了世界电子护照颁发人的大部分。这些 CSCA 证书 允许对相关电子护照颁发人的证书链进行验证。然而，未参加公钥簿总列表的用户必须弄清以 下问题：

 国家自己的文件签署人证书（DSC）和证书撤销表（CRL）的分发对于总列表用户仍是一 个未解决的问题。

 如果唯一的信任锚是从公钥簿上下载的总列表，则总列表用户必须与一直作为公钥簿参加 方的总列表发行人生成信任关系。

 公钥簿参加方没有发行总列表或将 CSCA 证书纳入总列表的义务。公钥簿参加方亦没有义 务在颁发新的 CSCA 证书在某个时间期限内对总列表进行更新。因此，仅仅依赖总列表， 意味着接受在或短或长的一段时间内可能无法获得 CSCA 证书的这种情况。

 的确，非公钥簿参加方无须支付任何公钥簿费用。但非公钥簿参加方的下载通常是手工的 而不是自动的（见公钥簿收费表）。如此一来，就需要持续进行人工干预和下载后的处理， 这意味着参与或者不参与公钥簿在财务上的差别比预期要小。

 《芝加哥公约》附件 9 中的一项建议措施是，颁发或拟颁发电子护照和/或在边检实行电子 护照自动检查的国际民航组织缔约国，应参加公钥簿。此外，公钥簿还获得了来自欧洲安 全与合作组织、欧盟和八国集团的政治支持。

xxvii) 收费减少安排包括那些内容？ 随着参加方的增加，公钥簿的收费也会随之下降。 按照运作合同的预计，一旦公钥簿的参加方达到了 31 个，预期公钥簿运作人的费用就会下降。

因此，自 2014 年 1 月 1 日开始，公钥簿运作人的收费将会从 43000 美元下降至 34000 美元。运

行合同预计，一旦公钥簿参加方达到 65 个，收费还会进一步下降。

xxviii) 边检机关是否可以参加公钥簿？

是的，边检机关可以参加公钥簿。按照公钥簿谅解备忘录第 2.1 条，任何签发或拟签发电子机读 旅行证件的“国际民航组织缔约国”（即批准了《芝加哥公约》的国家）均可参加公钥簿。谅 解备忘录没有明确说明须由相关国家中的哪个实体启动参与。然而，须注意的是，每个国家只 能由一个实体来执行备忘录，并代表该国开展与之相关的工作。因此，指定由哪个实体来执行 备忘录是相关国家的一项主权决定。《芝加哥公约》附件 9－《简化手续》的标准和建议措施第

3.9.1 款明确表明，在边检机关使用自动化电子护照查验的情况下，则鼓励参加公钥簿。

**-----**