概 述

充分利用新的技术

每个电子护照都含有一个内置电子芯片，存储持证人的照片和护照数据页所载的个人信息。电子护照使用公钥基础设施（PKI）技术，防止更改芯片内存储的信息。

除了持证人的信息以外，电子护照的芯片存储特定国家的数字保安特征，称为数字签名，这一数字签名源于该国的保安证书，即证件签名者证书（DSC）和国家签名证书（CSCA）。这些数字签名对于每个护照和每个国家都是独一无二的，可以使用护照颁发国的公钥证书予以核实。在扫描电子护照和读取芯片数据时，其经过认证的数字签名就告诉边境当局：芯片上的数据是真实无误的，该护照是由特定国家颁发和签署的，且护照未被篡改。

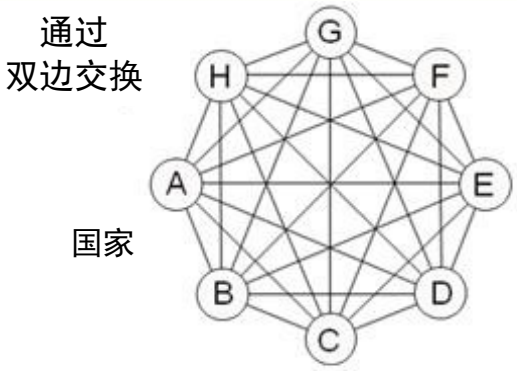
携手工作

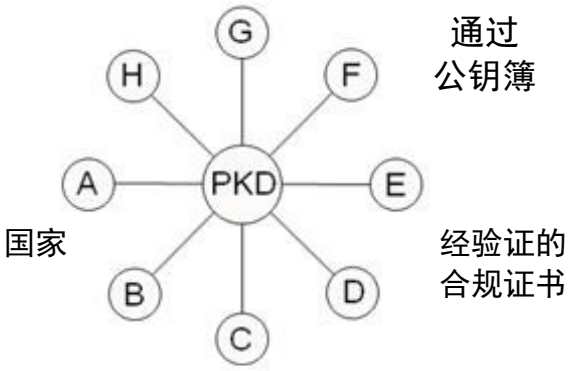
若要行之有效地使用该系统，边境当局和其他当局必须能够获得所有发布电子护照的国家的保安证书。出于这一原因，国际民用航空组织（ICAO）建立了一个系统，为各国之间分享公钥信息提供便利：国际民航组织公钥簿（PKD）。公钥簿是一个保存机构，使得公钥簿参加方[1]能够定期将其国家签名证书（CSCA）、证件签名者证书（DSC）、证书撤销表（CRL）和主表都输入公钥簿，同时允许已经完成公钥簿上载的所有公钥簿参加方获得经验证的保安证书。

公钥簿为分享最新的经验证信息提供了一种组织有序的、简单的、可靠的和具有成本效益的系统。如果没有公钥簿，每个国家必须彼此单独联系，以安全交换其证件签名者证书和证书撤销表。而通过公钥簿，本来需要数以百计的交易次数和工作小时才能完成的证书分享仅用两次交换即可完成 — 上载和下载经验证的信息。此外，含有经其他参加方验证的其他国家的国家签名证书主表也使您能够获得国家签名证书，即使您起初没有和所有国家交换国家签名证书。

[1] 截至 2013 年 6 月，国际民航组织公钥簿成员包括阿根廷、澳大利亚、奥地利、保加利亚、加拿大、中国、捷克共和国、法国、德国、香港特别行政区、匈牙利、印度、爱尔兰、日本、哈萨克斯坦、拉脱维亚、卢森堡、澳门特别行政区、马来西亚、摩尔多瓦、摩洛哥、荷兰、新西兰、尼日利亚、挪威、俄罗斯联邦、新加坡、斯洛伐克、大韩民国、西班牙、瑞典、瑞士、泰国、乌克兰、阿拉伯联合酋长国、联合王国、美国和联合国。

概 述





作为一项附加的宝贵益处，公钥簿为其参加方提供证书合规验证服务。通过在世界范围内确保证书的合规性和来源，为核实旅行证件和安然无虞地旅行提供了便利。

国际民航组织公钥簿并不含有任何护照持有人的个人信息，它也不提供关于护照芯片的辅助生物特征（例如指纹）的准入。

为旅行者开启大门

不仅仅是公钥簿参加方，每个国家都可以免费进入公钥簿[2]。这一信息共享公钥簿使得已经将其边境管制基础设施与公钥簿连接起来的所有国家的边境当局都能迅速验证电子护照，从而大大便利合法旅行者的入境。这一系统还帮助各国携手合作，打击护照欺骗，为国内和国际保安做出贡献。

关于进一步信息，请查阅公钥簿网站：
http://www.icao.int/Security/FAL/PKD/Pages/default.aspx

或联系：

国际民航组织公钥簿办公室

ICAO-PKD@ICAO.INT

[2] 免费准入的设计用于偶尔下载，不是为需要公钥簿运营人定期采取行动的边境管制用途所设计的，也不提供技术支持。