OVERVIEW

ICAO PUBLIC KEY DIRECTORY (PKD)

Taking full advantage of new technologies

Every ePassport contains an embedded electronic chip that stores the holder's photo and personal information found in the passport data page. ePassports use Public Key Infrastructure (PKI) technology that prevents the information stored on the chip from being altered.

In addition to the holder's information, the ePassport chip stores a country specific digital security feature, known as a digital signature, which is derived from the country's security certificates i.e. Document Signer Certificates (DSC) and Country Signing Certificate (CSCA). These digital signatures are unique to each passport and country and can be verified using the public key certificates of the issuing country. When the ePassport is scanned and the chip data is read, its authenticated digital signature tells border authorities that the data on the chip is authentic, that it was issued and signed by the given country and that it has not been tampered with.

Working together

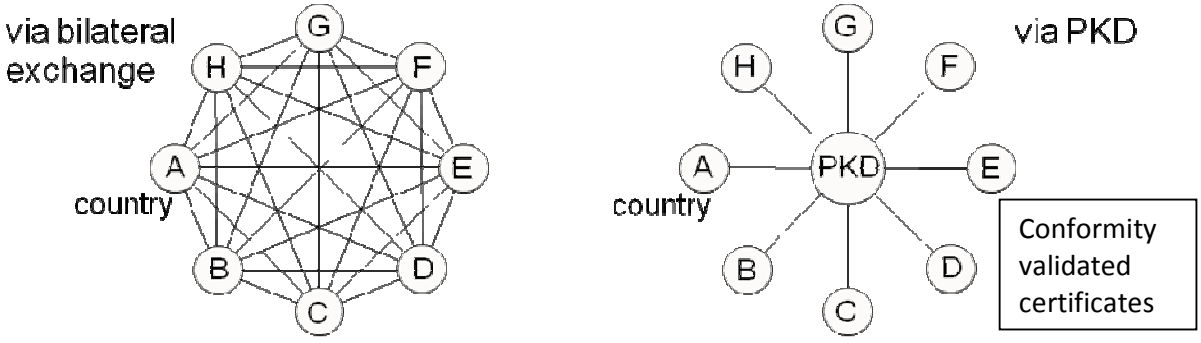
To be used effectively, border and other authorities must have access to the security certificates of all the countries that issue ePassports. For this reason, the International Civil Aviation Organization (ICAO) has created a system to facilitate the sharing of public key information between countries: the ICAO Public Key Directory (PKD). The PKD is a repository that enables PKD Participants to input routinely their CSCA, DSC, Certificate Revocation Lists (CRL) and Master Lists into the directory while also allowing access to the validated security certificates of all PKD Participants that have completed their upload to the directory.

The PKD provides an organized, simple, secure and cost effective system for sharing validated up-to date information. Without the PKD, each country must go to one another individually to securely exchange their DSC and CRL. With the PKD, certificate sharing that would require hundreds of transactions and work hours can be accomplished in just two exchanges — the upload and the download of validated information. Furthermore the available Master Lists, containing validated CSCAs of other countries by other participants, give you access to CSCAs even if initial CSCA exchange has not been done with all countries.

INTERNATIONAL CIVIL AVIATION ORGANIZATION

OVERVIEW

ICAO PUBLIC KEY DIRECTORY (PKD)



As an additional valuable benefit the PKD offers its participants a certificate conformity validation service. By assuring the conformity and origin of the certificate worldwide, verification of the travel document and trouble free travels are facilitated.

The ICAO PKD does not contain any personal information about any passport holder, nor does it provide access to passport chip secondary biometrics, like fingerprints.

Opening doors for travellers

Every country, not just PKD Participants, can access the PKD for free[1]. This information-sharing directory enables border authorities in all countries that have connected their border control infrastructure to the PKD to quickly validate ePassports, greatly facilitating the entry of legitimate travellers. This system also helps all nations to work together in combating passport fraud and contributing to domestic and international security.

For more information, please consult the PKD Web site:
http://www.icao.int/Security/FAL/PKD/Pages/default.aspx

Or contact:

ICAO-PKD@ICAO.INT

[1] The free access is designed for occasional downloads, it's not designed for border control use that requires regular PKD operator action and offers no technical support.