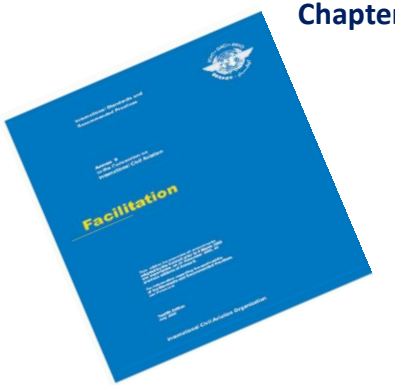
Public Key Directory: What is the PKD and How to Make Best Use of It

Christiane DerMarkar

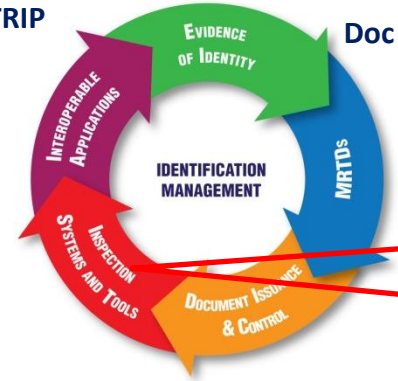
ICAO Programme Officer – Public Key Directory

ICAO PKD: one of the 3 interrelated pillars of Facilitation

Annex 9 → **ICAO TRIP Strategy** ← **ICAO PKD**



Chapter 3:main SARPs related to the TRIP



Doc 9303 Part 12: PKI specs

Mean to enhance security in cross-border movement.

Inspection Tool for ePassports verification, validation and authentication of the digital signatures and content of the chip

Amendment 25 to Annex 9:

RP 3.9.1: *"Contracting States issuing, or intending to **issue** eMRTDs **should join** the ICAO Public Key Directory (PKD) and **upload their information to the PKD**."*

RP 3.9.2: *"Contracting States implementing **checks** on eMRTDs at border controls **should join** the ICAO Public Key Directory (PKD) and **use** the information available from the **PKD** to **validate** eMRTDs at border controls."*

Connection between PKD and ePassports

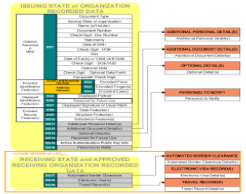
MRP

Machine Readable Passport (MRP)

ePASSPORT

CHIP RFID 14443

IMAGE FACE



Logical Data Structure (LDS)

0111001001010

PKI DIGITAL SIGNATURE Public Key Directory **(PKD)**

What is the PKD & What does it do?

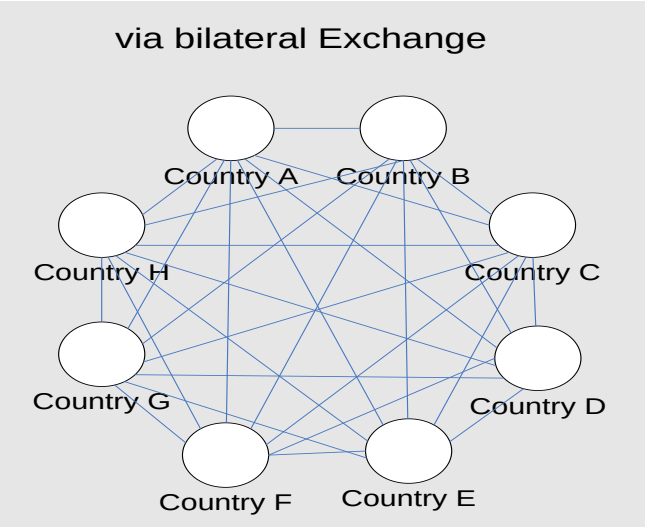
- A central storage location, highly secure where States and other entities can input and retrieve the security information to validate the electronic information on the passport.
- It allows Border control authorities to confirm that the ePassport:
  - Was issued by the right authority
  - Has not been altered
  - Is not a copy or cloned document

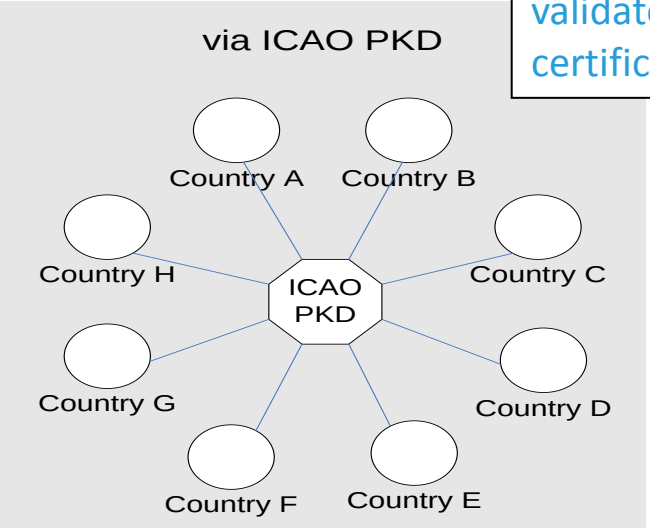
The Role of The PKD

- Minimizing the volume of certificate exchange:
  - Document Signer Certificates (DSCs)
  - Certificate Revocation Lists (CRLs)
  - Country Signing Certificate Authority (CSCA) Master List
- Ensuring timely uploads
- Managing adherence to technical standards
- Facilitating the validation process

Central Broker

Distribution of Certificates and CRLs



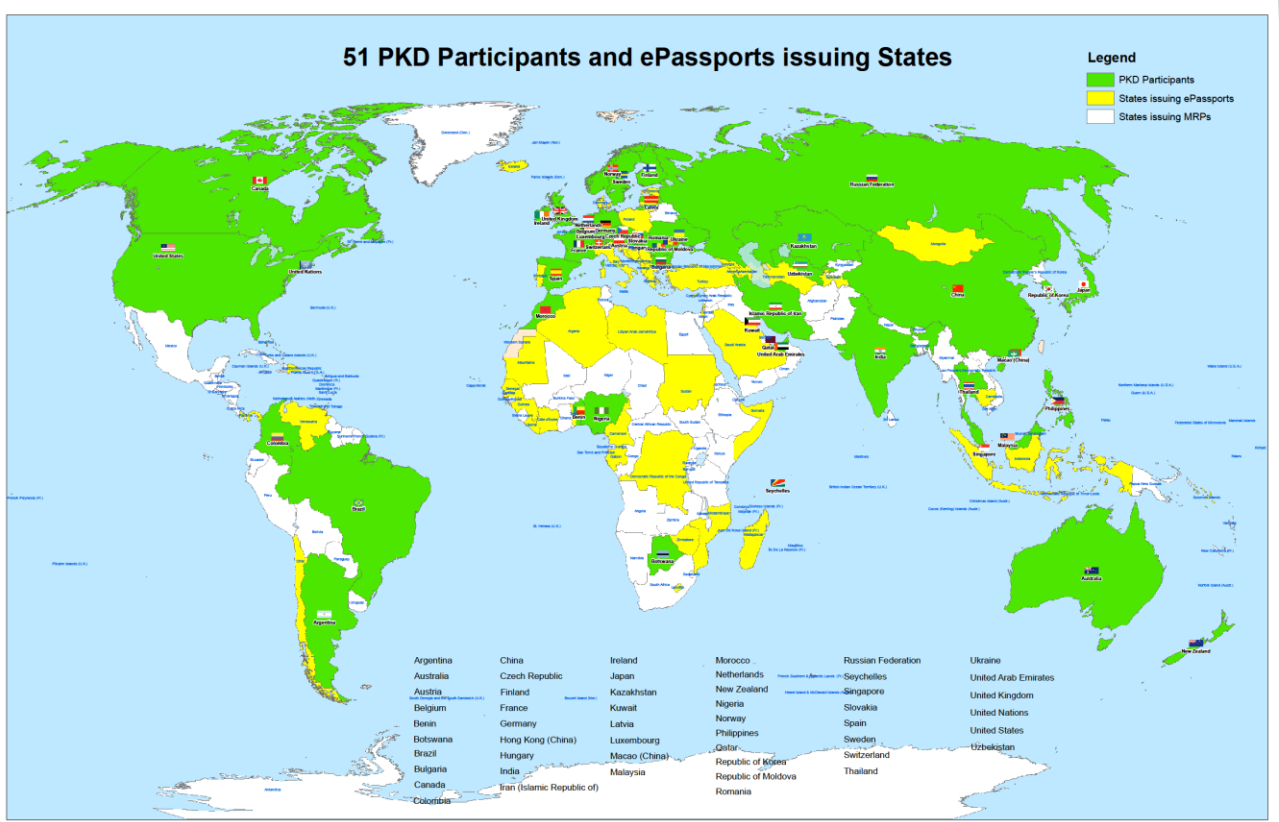


Conformity validated certificates

This example shows **8** States/non-States requiring **56** bilateral exchanges (left) or 2 exchanges with the PKD (right) to be up to date with DSCs and CRLs. In case of **191** ICAO States **36,290** bilateral exchanges would be necessary while there are still 2 exchanges with the PKD.

Current Services of the PKD

- Validated DSCs and CRLs of Participants
- CSCA Master List – List of CSCAs used by Participants
- Country Signing Certificate Authority (CSCA) Registry – Yellow Pages for the Passport Issuance Agency of the Participant
- A reference for compliance to Doc 9303 for DSCs and CRLs
- Contains lists on non-compliant certificates



51 Participants

New Participants:

- Romania
- Finland
- Benin
- Botswana
- Kuwait

ANNEX 9: Recommended Practice 3.9.1 & 3.9.2

The Standards and Recommended Practice of Annex 9 recommend the following:

3.9.1: "Contracting States issuing, or intending to issue eMRTDs should join the ICAO Public Key Directory (PKD) and upload their information to the PKD."

3.9.2: "Contracting States implementing checks on eMRTDs at border controls should join the ICAO Public Key Directory (PKD) and use the information available from the PKD to validate eMRTDs at border controls."

Some Arguments repeated over and over ….

✗	✓
It's too expensive	As of 01.01.2016 Fee reduction
Bilateral exchange works good enough	cumbersome, time consuming and possible security risk
It's not necessary – DSCs are (mostly) on the chip	A DSC on the ePassport but not on the PKD could mean a compromised private signing key. & CRLS are only distributed via PKD…
It's too complicated – we must first introduce ePassports	1. Participation in the PKD should go hand in hand with introduction of ePassports 2. PKD participation is key for setting up any successful ePassport based border control.

Reasons to Participate

- The need to exchange certificates is the logical step forward from the well known specimen exchange (you must know what you're looking for, when inspecting a travel document).

- Without the ability of validating the digital signature in a ePassport at the border, the travel document must be treated exactly as a simple MRP not an ePassport

- Using the PKD in ePassport validation is essential to capitalize on the investment made by States in developing ePassports to improve Border Security

Value of PKD for ePassports

- Use of the PKD enhances the security of the ePassport validation process
- Facilitates fast and secure cross-border movement by the ''frontline'' entities
- PKD can be used with Automated Border Controls (ABC)or with a manual e-reader
- Maintain compliance with ICAO specifications
- Assure smooth and continuous ePassport validation (less than 10 seconds per pax) at control points
- Fees for PKD membership are low compared to investment required for a multiple bilateral infrastructure
- Over 120 States claim that they are currently issuing ePassports (nearly half a billion of ePassports in circulation world wide)
- States still need to do significant work to ensure that the data chip in ePassports is fully compliant with ICAO Doc 9303 specifications
- ICAO and the International Organization for Standardization (ISO) have implemented a mechanism to make error codes available at each border to detect security issues when reading a non-compliant ePassport data chip

It's not complicated :
All you have to do is….

- Find out who is responsible
- Check legislation and budget
- Different organizations in different states (try to make it as simple as possible)
- Contact ICAO or any PKD Board Member or PKD Participant if you have questions

Formalities:
The steps to join the PKD

1. Deposit a Notice of Participation with the Secretary General of ICAO
2. Deposit a Notice of Registration with the Secretary General of ICAO
3. Effect payment of the Registration Fee and Annual Fee to ICAO
   a) **1.1.2016 Registration Fees : US $ 15,900**
   b) **Annual Fees: +/- US $40,000**
4. Securely submit to ICAO and all Participants, the CSCA certificate
5. Use the PKD : upload/Download certificates
6. http://www.icao.int/Security/mrtd/Pages/PKD-HowtoPartici.aspx

2016 a year that will bring changes

- New Fees ✓
- New Services

= ICAO Master List (new)

01.01.2016 : Fees reduction

A. For new Participants - Registration Fee: US $15,900

B. Annual Fees based on 49 Participants:

1. Operator: US $ 29,900
2. ICAO: US $ 9,262
3. Total: US $ 39,162

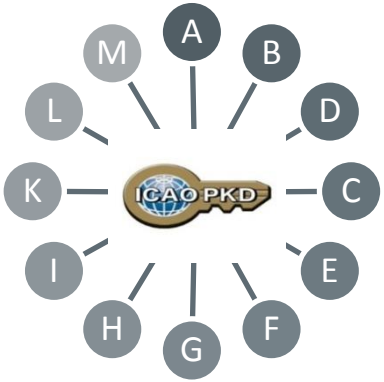
C. More Participants = reduction in Operators and ICAO Annual Fees

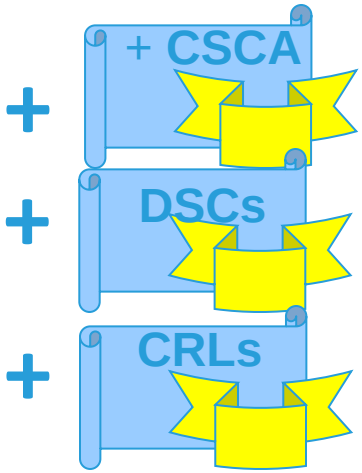
50 Participants	27,000.00 US$
55 Participants	24,500.00 US$
60 Participants	22,500.00 US$
65 Participants	20,900.00 US$

New Service
ICAO Global Master List

- A fact: e-MRTDs capabilities are not used at their full extend – Border Agencies need the tools (certificates) necessary, bilateral exchange doesn't meet the requirements

One-Stop Shop For ePassport Validation





= ICAO Master List (new)

= currently in the PKD

= currently in the PKD

Contact Details

Name: Christiane DerMarkar
Email: cdermarkar@icao.int

PKD website:

http://www.icao.int/Security/mrtd/Pages/icaoPKD.aspx