ICAO PUBLIC KEY DIRECTORY (PKD)

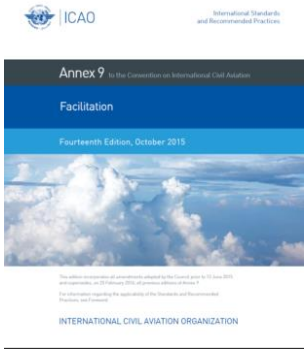
Christiane DerMarkar
ICAO PKD Officer

09/07/2018

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

ANNEX 9: Recommended Practice 3.9.1, 3.9.2 and 3.35.5

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."

3.35.5: "Contracting States utilizing ABC systems should, pursuant to 3.9.2 and 3.10.1, use the information available from the PKD to validate eMRTDs…."

WHAT is an eMRTD

Electronic Machine Readable Travel Document (**eMRTD**):
is a passport, card, Laissez Passer or other Travel Document that has a contactless integrated circuit embedded in it and the capability of being used for biometric identification of the MRTD holder in accordance with the standards specified in the relevant Part of Doc 9303 — Machine Readable Travel Documents.

Connection between PKD and ePassports

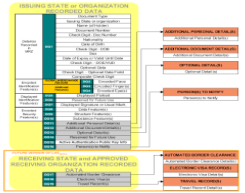
MRP

Machine Readable Passport (MRP)

ePASSPORT

CHIP RFID 14443

IMAGE FACE



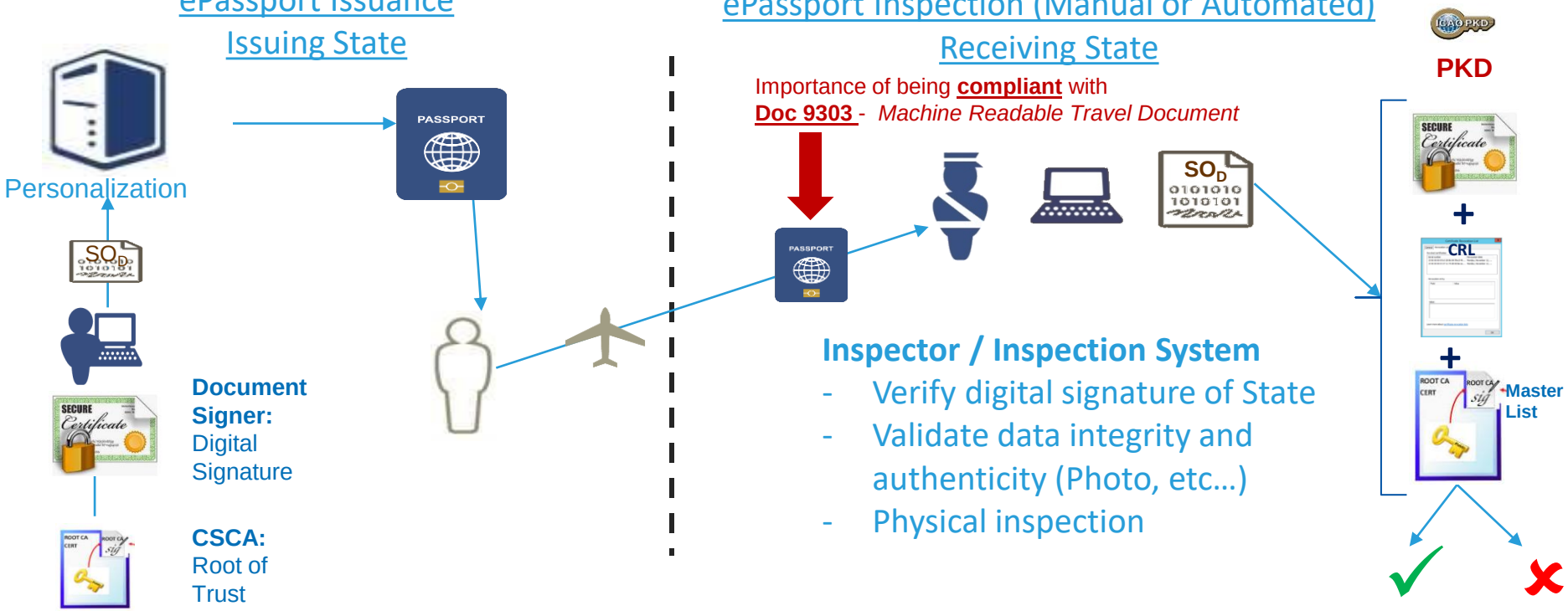
Logical Data Structure (LDS)

0111001001010

PKI Certificate from the Public Key Directory (PKD)

Public Key Infrastructure (PKI): major role in eMRTD security

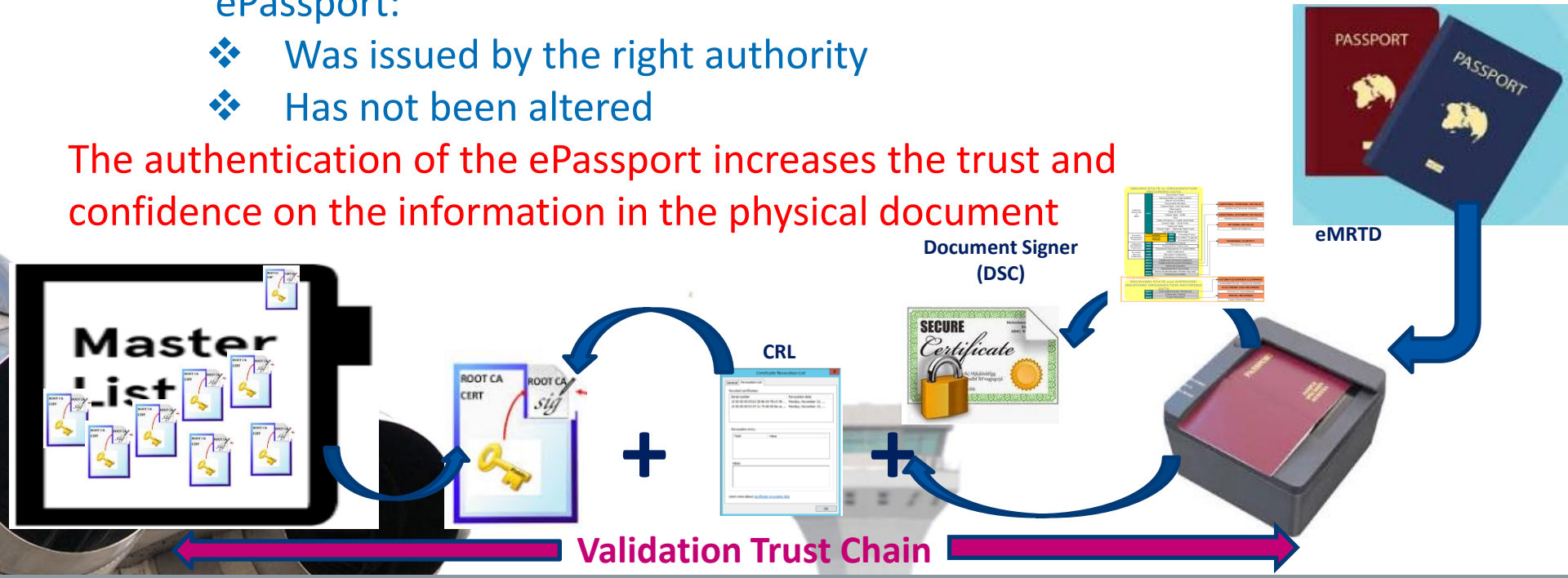
Operational View



ePassport Validation And PKD

- It allows Border Control authorities to confirm that the ePassport:
  - Was issued by the right authority
  - Has not been altered

The authentication of the ePassport increases the trust and confidence on the information in the physical document

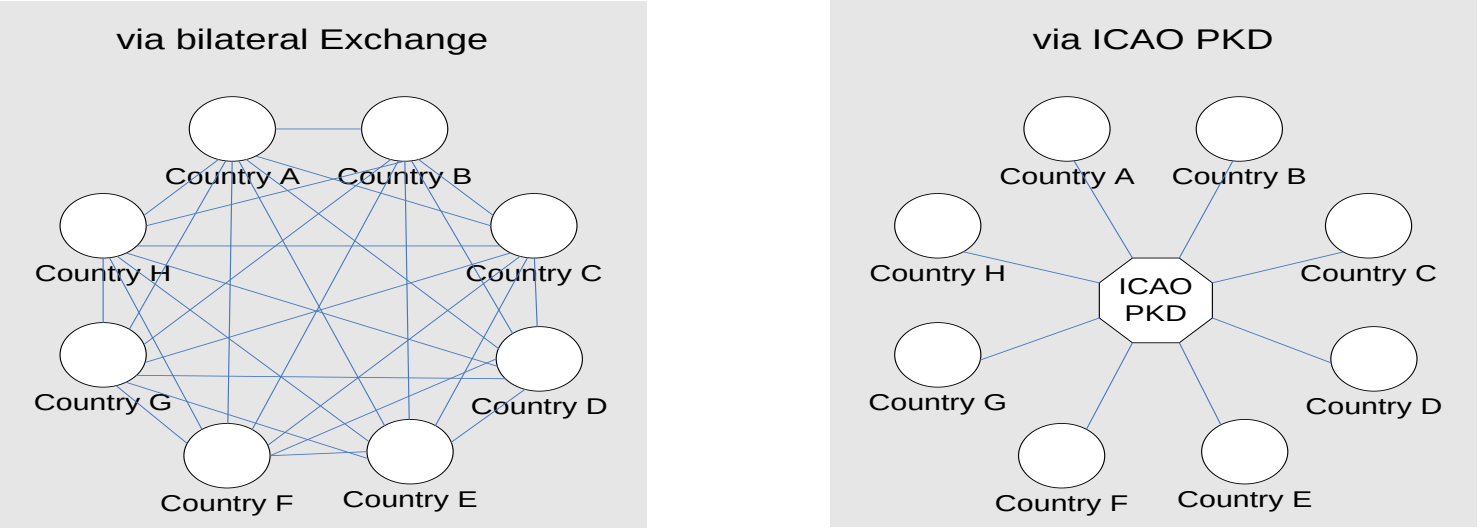


What is the PKD and what is its role

- A central Repository that simplify and facilitates the sharing of PKI certificates required to authenticate ePassport.
- Minimizing the volume of certificate exchange:
  - Document Signer Certificates (DSCs)
  - Certificate Revocation Lists (CRLs)
  - Country Signing Certificate Authority (CSCA) Master List
  - Deviation List
- Ensuring timely uploads

Central Broker

Distribution of Certificates and CRLs



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.

Why Join the PKD

Issuer Perspective:

Border authorities around the world can validate the ePassports that you issue.

ePassports that cannot be validated must essentially be considered and treated as a non-electronic travel document.

And you are not capitalizing and the investment made to implement ePassports

→ The ICAO PKD provides a means of distributing your information to other States that is efficient, reliable, and always accessible.

Border Authority Perspective:

performing ePassport validation (according to Doc 9303 7th Edition, Part 12) and accessing the information necessary to perform it, provides confidence that the travel document under inspection has been issued by the proper authorities and that the information recorded on the document has not been tampered with.

→ The ICAO PKD provides a means of accessing the necessary information published by other States in a cost efficient way that is always available.

Traveler Perspective:

Validation through the ICAO PKD, confirms the authenticity and integrity of the data on the chip, and in turn facilitates the fast and secure cross-border movement of citizens by the ‘’frontline’’ entities.

→ The ICAO PKD is the most efficient and reliable means of both providing and accessing the information required for ePassport validation.

Pre- Joining the PKD

Question 1 : Organizational Structure

1- Who is the responsible Travel Document Issuance Authority (TDIA)?

2- What is the legal basis for issuing e-passport and running an e-passport PKI?

Question 2:Country Signing Certificate Authority / Document Signer

1- Ensure there is a Certificate Policy (CP) in place

2- Stick to ICAO recommendations (Doc 9303 Part 12- PKI)

Question 3: Operations of the Travel Document PKI

1- Who operates the e-passport PKI and how is this done?

The steps to join the PKD

For a state or non-state entity:

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.
4. When ready, securely submit to ICAO, the Country Signing CA Certificate (CSCA).
5. Upload/Download to and from the PKD.

https://www.icao.int/Security/FAL/PKD/Pages/How-to-Participate.aspx

ICAO PKD MoU: Legal Framework

- Multilateral agreement to be signed by all States Participating in the PKD.
- Legally support formal arrangements between ICAO and each PKD Participating State in regards to the PKD System.
- Notice of Participation: Attachment A to the PKD MoU

- https://www.icao.int/Security/FAL/PKD/Pages/Publications.aspx

https://www.icao.int/Security/FAL/PKD/Pages/How-to-Participate.aspx

1. Select PKD MoU
2. Select Notice of Participation (model)

MEMORANDUM OF UNDERSTANDING (MoU)
REGARDING PARTICIPATION AND COST SHARING IN THE
ELECTRONIC MACHINE READABLE TRAVEL DOCUMENTS
ICAO PUBLIC KEY DIRECTORY (PKD)

NOTICE OF PARTICIPATION

The Ministry of Interior
(*name of the Authority designated by the Participant concerned as its authorized organ*)

of Republic of Utopia
(*name of Participant*)

hereby gives the Secretary General of the International Civil Aviation Organization (ICAO)

notice of participation of

Identity and Passport Service Authority
Moon Street no. 123, 54321 Utopia City, Republic of Utopia
(*name and address of the Participant*)

in the *Memorandum of Understanding (MoU) Regarding Participation and Cost Sharing in the Electronic Machine Readable Travel Documents ICAO Public Key Directory (ICAO PKD)*.

NOTE: Participation by a non-State entity in the ICAO PKD (the functions of which are technical and operational) will not afford such non-State entities the rights or privileges accorded to ICAO Contracting States under the Chicago Convention.

Signed at Utopia City (place) on 13 July 2010 (date)

On behalf of Republic of Utopia

Name of Authority Ministry of Interior

Name, title Mr. Dolittle, Head of Division for Documents Law

Signature

https://www.icao.int/Security/FAL/PKD/Pages/How-to-Participate.aspx

1. **Select Notice of Registration (model)**

MODEL
NOTICE OF REGISTRATION

REGISTRATION FOR PARTICIPATION IN ICAO PKD	
PASSPORT DATA	
Estimated number of Document Signer Certificates that will be issued each year:	12
Estimated number of Certificate Revocation Lists that will be issued each year:	8
Number of expired and valid Country Signing CA Certificates:	3
Number of expired and valid Country Signing CA Link Certificates:	2
Average validity period for Country Signing CA (Link) Certificates:	10 years
Estimated number of Master Lists issued each year:	12
Estimated number of entries per Master List:	50
eMRTD AUTHORITY (EMA) DETAILS	
Name:	Mr. Dolittle, Ministry of Interior
Title:	Head of Division for Documents Law
Address:	Moon Street no. 111, 55555 Utopia City, Republic of Utopia
Telephone:	+333-222-1111 9999
Fax:	+333-222-1111 8888
E-Mail:	Doc@MoI.gov.uto
Designation (eMRTD System):	chief ePassports and ID-cards adviser
Senior Officer (eMRTD System):	Mr. Domuch, Ministry of Interior, CIO
eMRTD COUNTRY SIGNING CERTIFICATE AUTHORITY (CSCA)	
Name:	Mr. Dosomething, Identity and Passport Service Authority
Title:	Senior PKI Officer
Address:	Moon Street no. 123, 54321 Utopia City, Republic of Utopia
Telephone:	+333-222-2222 9999
Fax:	+333-222-2222 7777
E-Mail:	CSCA@ema.gov.uto
Designation (eMRTD System):	Head of N-PKD

Participation fee

A. ICAO Registration Fee: **US $15,900**

B. Estimated Annual Fee 2018 based on 55+ Active Participants: **US $ 31,755** (Operator Fee US $ 24,500 + ICAO Operator fee US $ 7,255)

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

*ICAO prepares an annual operation budget every year which is divided over the total number of PKD participants. For 2018 the ICAO Operation Fees have been established at US $7,255.00.

Active Participants	Operator Fees (US $)	ICAO * Fees (US $)
50 Participants	27,000.00	7,351.00
55 Participants	24,500.00	7,351.00
60 Participants	22,500.00	7,351.00
65 Participants	20,900.00	7,351.00

Active Participation

PKD Integration

1. A PKD Participant should start active Participation (CSCA Import and PKD Upload) at the latest 15 months after paying The Registration Fee and becoming Effective participants.
2. Participant are required to have completed the testing of the PKD interface and successfully imported the CSCA into the HSM in Montreal.
3. The PKI Infrastructure between National and ICAO PKD should be implemented.

CSCA KEY CEREMONY

- the CSCA Certificate plays the main role as the anchor of trust in the validation process of the ePassports
- Each state participating in the ICAO PKD is required to securely submit its CSCA certificate to ICAO.
- The CSCA certificate, must be hand delivered by a State Representative to ICAO headquarter in Montreal where it is imported securely to the ICAO PKD (High Security Module, HSM) under the observation of the state's representatives and the ICAO security officials
- After the Key ceremony is complete, the DSCs and CRLs can be uploaded to the ICAO PKD. The authenticity of the DSCs and CRLs can now be verified using the public keys stored inside the CSCA certificates that are stored within the ICAO PKD.

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

- Review national legislation:
  - Essential before introducing ePassport and joining the PKD
- Find out who is responsible:
  - Define roles and responsibilities of all those involved with the PKD (PKI, NPKD, etc…)
- Establish a budget line:
  - streamline the annual payment
- Address Technical Specifications:
  - ensure that the National PKD is technically compatible with the ICAO PKD
- Integrate the National PKD with the ICAO PKD:
  - This includes National PKDs uploading and downloading certificates (DSCs and MLs) and revocation lists to and from the ICAO PKD

Conclusion

- ICAO urges all ICAO Member States to join and actively use the certificates distributed by the ICAO PKD as a means to validate and authenticate ePassports at Border Controls.

ICAO SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND

ICAO

THANK YOU