ICAO Regional FAL Seminar
Bangkok, Thailand
23-26 March 2015

What is the PKD &
how to become a PKD Participant:
A Guided Tour

25 March 2015

ePassports and Public Key Infrastructure

- ePassports : new security feature, the digital signature
- The digital signature validates the content of the chip
- The distribution of public keys is necessary for validating the digital signature

What is the PKD?

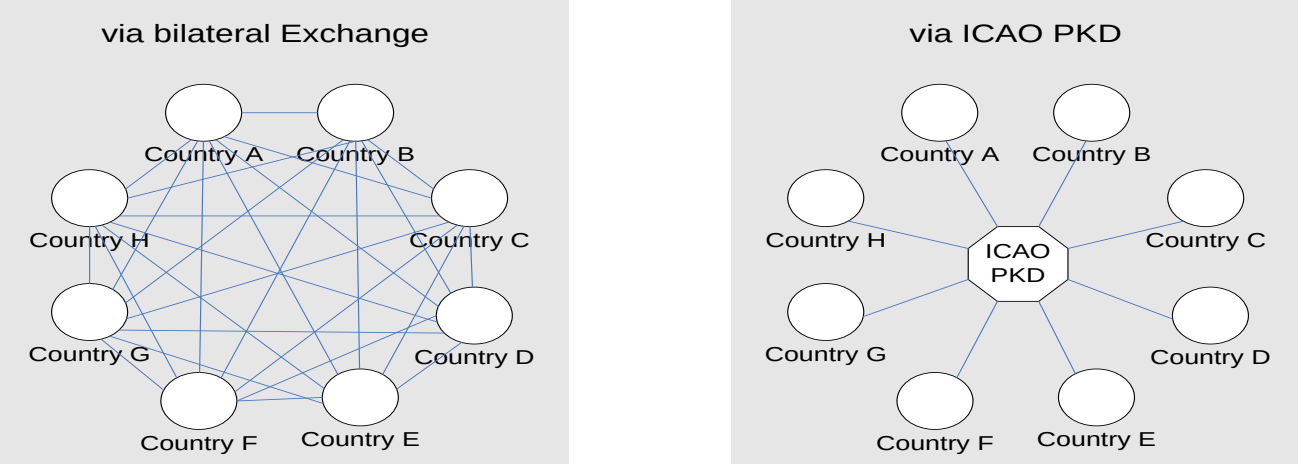
- An inspection tool available to border control, airlines, and other entities using ePassports
- A directory of all country public keys needed to validate data stored on ePassports
- The primary means by which ePassport countries distribute their public keys
- A highly secure facility and service

The Role of The PKD

- The ICAO PKD is the central Platform to manage the world wide exchange of certificates. Those certificates are used to validate the electronic signature of data contained in the ePassports.
- The most effective means by which the electronic passport issuing countries distribute their public.
- And everything in:
  - Facilitating the validation process
  - Minimizing the volume of certificate exchange
  - Ensuring timely uploads
  - Managing adherence to technical standards

Central Broker

Distribution of Certificates and CRLs



This example shows 8 states requiring 56 bilateral exchanges (left) or 2 exchanges with the PKD (right) to be up to date with certificates and CRLs. In case of 188 ICAO States 35,156 bilateral exchanges would be necessary while there are still 2 exchanges necessary with the PKD.

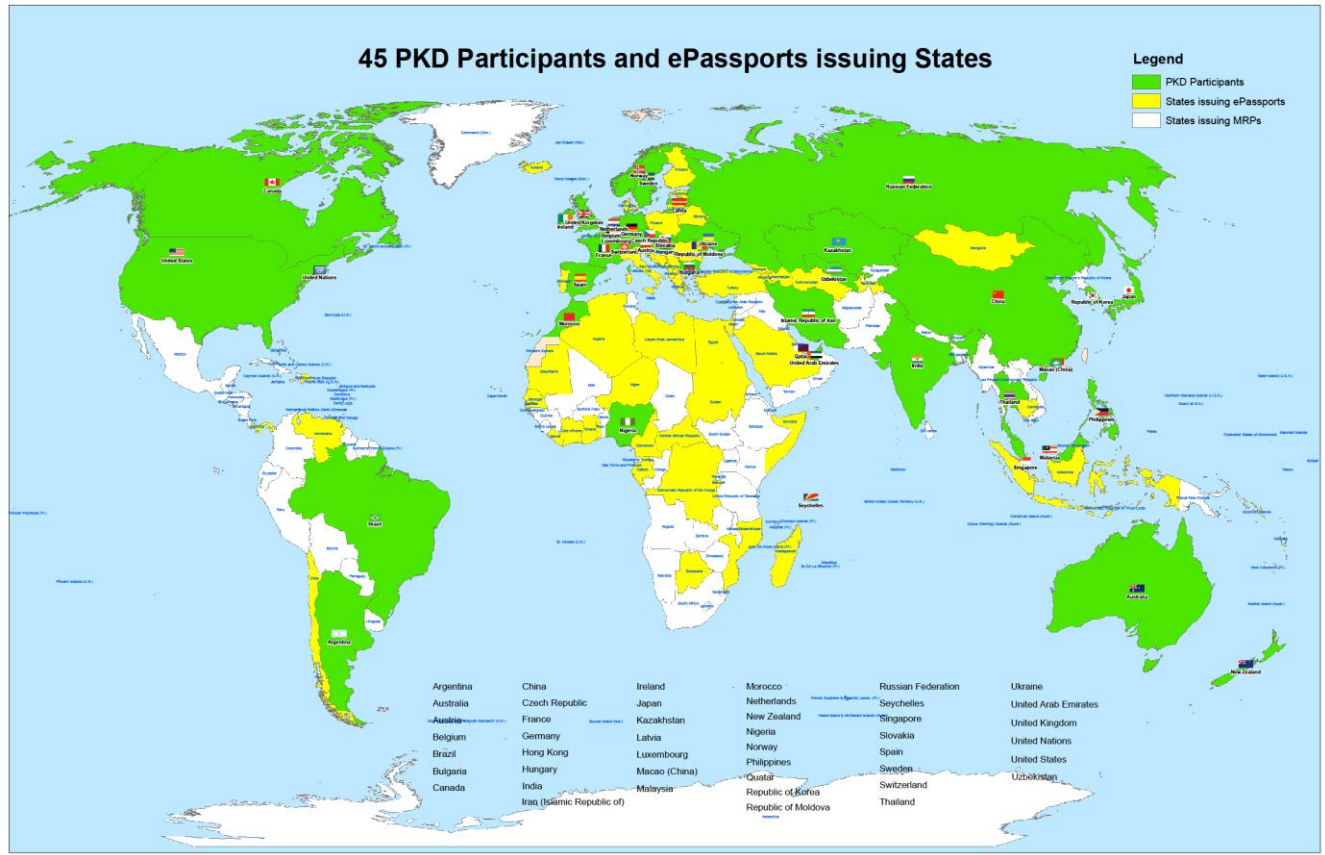
Other Services

- Authoritative source of validated public keys
- Authoritative source of country CSCAs through CSCA master list
- PKD Registry: Yellow pages for contacting the Passport Issuing agency of each Participant
- A reference for compliance to Doc 9303 for Certificates and CRLs
- Contains lists on non-compliant certificates

Why?

- ICAO PKD provides a fast and secure way for the electronic validation of ePassports
- Compromised or false certificates or keys are immediately detected through the ICAO PKD
- A State participating in the ICAO PKD will facilitate international travelling for its citizens
- By using the ICAO PKD in the border control agencies a State proactively contributes to international border security and to aviation security

45Participants



And You?????

SHOULD YOU JOIN THE PKD

ANNEX 9:
Recommended Practice 3.9.1

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

"ICAO Contracting States issuing, or intending to issue ePassports and/or; implementing at border control automated checks on ePassports; should join the ICAO Public Key Directory (PKD)."

The steps to join the PKD

In order to become a Participant in the ICAO PKD, it is required to do the following:

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 and all Participants, the Country Signing CA Certificate (CCSCA).
5. Upload/Download to and from the PKD.

STEP 1: Fill the Notice of Participation

Complete and send to the ICAO Secretary General the Notice of Participation to the PKD Memorandum of Understanding (MoU) with ICAO

1. The official start of the Process of joining the PKD.
2. The Notice of Participation can be found in: Attachment A of the PKD MoU.
3. A Model of the Notice of Participation is available for download at the MRTD Web site.
   http://www.icao.int/Security/mrtd/PKD%20MoU/Forms/AllItems.aspx
4. The Notice of Participation should be filled by the authority in charge of ePassport or identity documents.

http://www.icao.int/Security/mrtd/PKD%20MoU/Notice%20of%20Participation%20-%20Model.pdf

1. Select PKD documents

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

STEP 2: Fill the Notice of Registration

Complete and send to the ICAO Secretary General the Notice of Registration

1. The Notice of Registration can be found in: Attachment B of the Procedures of the ICAO PKD.
2. A Model of the Notice of Registration is available for download at the MRTD Website: http://www.icao.int/Security/mrtd/PKD%20MoU/Forms/AllItems.aspx
3. The Notice of Registration is important to establish the State Representative contact details: the eMRTD Authority (EMA).
4. The Notice of Registration permits the State to register with the Operator.

http://www.icao.int/Security/mrtd/PKD%20MoU/Notice%20of%20Registration%20-%20Model.pdf

1. **Select PKD documents**

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

STEP 3: Payment of Fees: Registration Fee

1. A Onetime fee : US $56,000.
2. To prepare activity in the PKD and the technical integration of a new PKD Participant.
3. Is payable to ICAO upon filing of the Notice of Participation.
4. Full payment is mandatory for participation in the PKD to become effective.
5. Once Registration Fee is paid and the participation is effective, the Participant receives 2 documents:
   - the Interface Specifications: detailing the protocol for accessing the PKD
   - the Test Bench procedures: detailing the testing procedure for the access to the PKD

STEP 3: Payment of Fees: Annual Fee

1. On the first year of participation calculated on a pro-rata basis from the day when PKD participation becomes effective.
2. Recurring Fee to cover running costs of participation.
3. For an active Participant the Annual Fee is around US $43,642 in 2015:
   a) ICAO Fees: US $9,642/year (2015 based upon 45 participants).
   b) The Operator Fees: US $34,000/year.
4. Not paying the Annual Fee: withdrawal of services.

Active Participation
PKD Integration / Upload

1. A PKD Participant should start active Participation (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 Central PKD should be implemented.
4. Full conformity to Doc 9303 is required.

Summary

1. Establish who will be the authority responsible for PKD.
2. Establish a permanent budgetary line.
3. Conformance with Doc 9303 is essential.
4. Follow the steps described and become active within 15 months.
5. Contact ICAO, the PKD Board Chairman or any PKD Board member for additional questions.

ICAO UNITING AVIATION

Come and Join!!!

THANK YOU

QUESTIONS????

Christiane DerMarkar,
Programme Officer – PKD
Secretary of the PKD Board
cdermarkar@icao.int

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