



| ICAO

SECURITY & FACILITATION



# ICAO PUBLIC KEY DIRECTORY

Christiane DerMarkar

*ICAO TRIP Officer*

Windhoek, Namibia – 24/07/19





ICAO

SECURITY & FACILITATION

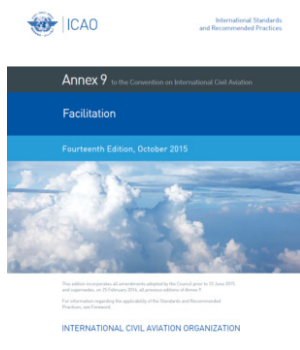


## ICAO PKD: one of the 3 interrelated pillars of Facilitation

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





| ICAO

SECURITY & FACILITATION



## **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....”*



ICAO

SECURITY & FACILITATION

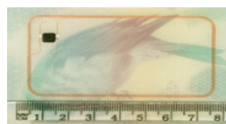


# Connection between PKD and ePassports

## MRP



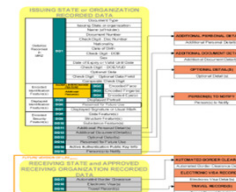
Machine Readable  
Passport (MRP)



CHIP RFID  
14443



IMAGE  
FACE



Logical  
Data  
Structure  
(LDS)



0111001001010

PKI  
Certificate  
from the  
Public Key  
Directory  
(PKD)



| ICAO

SECURITY & FACILITATION



## Useful Definitions

- **CSCA – Country Signing Certificate Authority Certificate** : It's the national trust point for ePassport. It is the anchor of the trust chain
- **DSC – Document Signer Certificate** Contains the information required to verify the digital signature on ePassport
- **CRL – Certificate Revocation List**: List issued by States to revoke any certificate that was compromised
- **Master Lists**: List of CSCAs that has been assembled and signed by an issuing authority



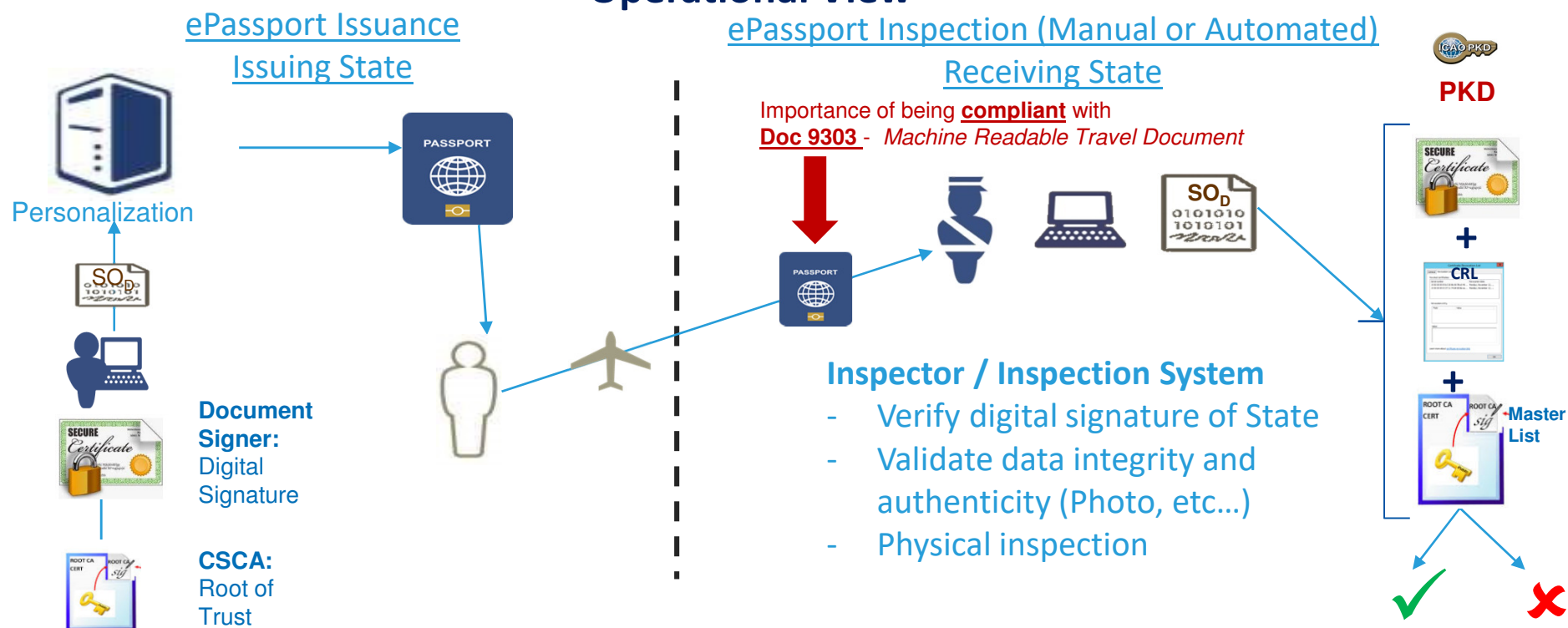
ICAO

SECURITY & FACILITATION



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

### Operational View





| ICAO

SECURITY & FACILITATION



# What do Border Control Authorities need to check?

- Some may require only CSCAs (**minimum requirement**, trust chain)
- Some require CSCA and CRL
- Some require CSCA, DSC and CRL

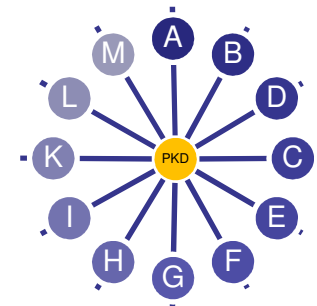
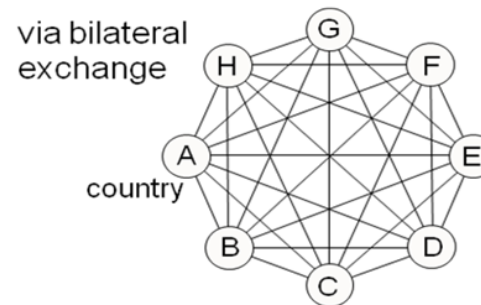


Publish all three in the PKD and let the responsible authorities use what they want.



## 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





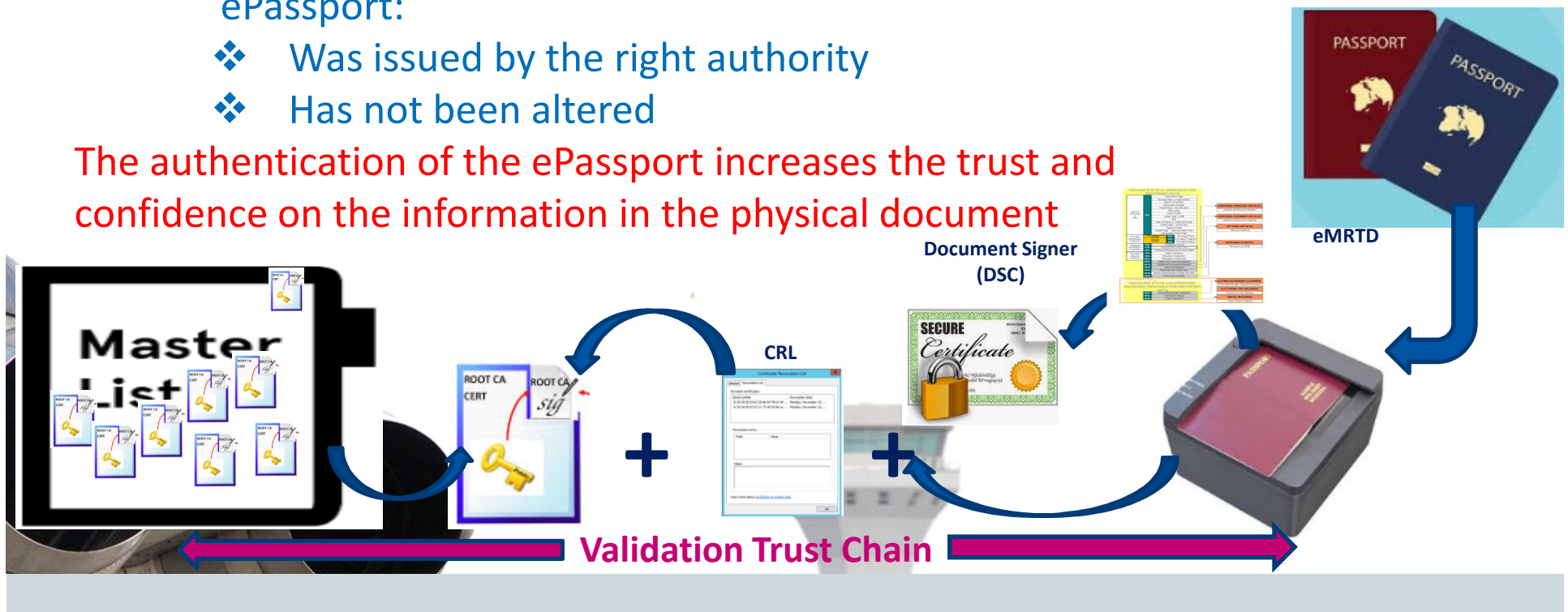
ICAO

SECURITY & FACILITATION

## 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



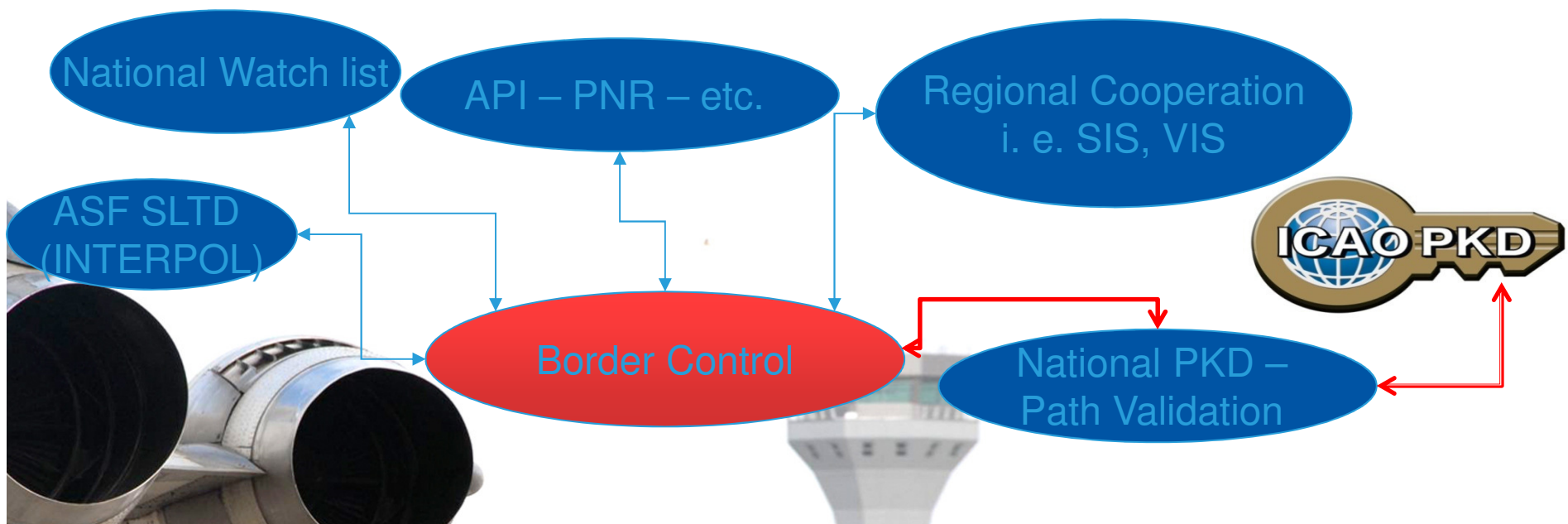


ICAO

SECURITY & FACILITATION



## Border Control: the ideal setup includes ICAO PKD

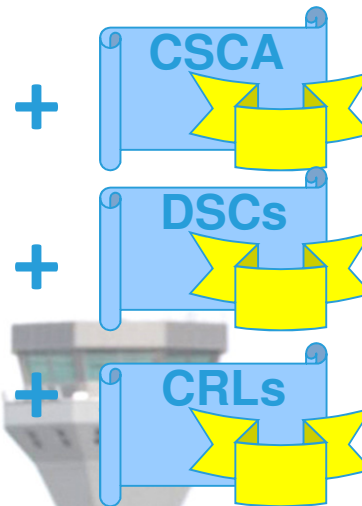
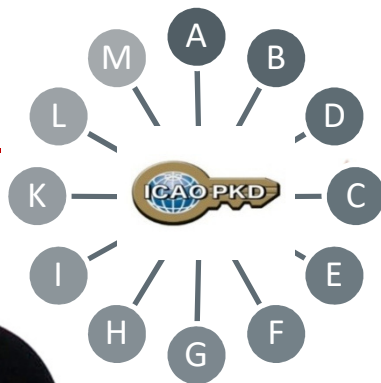




## New Service: ICAO Global Master List

- A fact: e-MRTDs capabilities are not used to their full extent – 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**



## 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 7<sup>th</sup> 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.



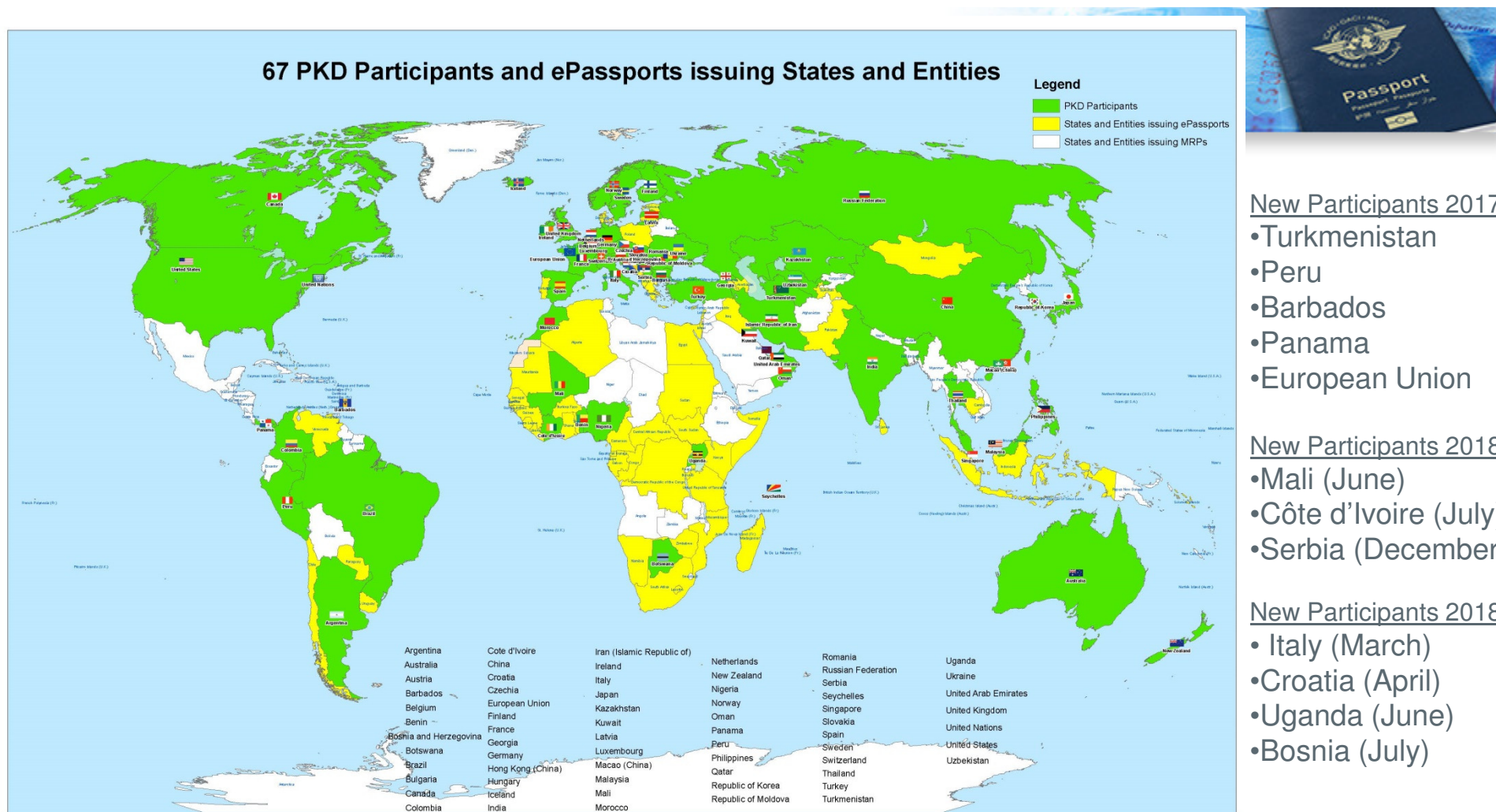
### Traveler Perspective:

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.





#### New Participants 2017

- Turkmenistan
- Peru
- Barbados
- Panama
- European Union

#### New Participants 2018

- Mali (June)
- Côte d'Ivoire (July)
- Serbia (December)

#### New Participants 2018

- Italy (March)
- Croatia (April)
- Uganda (June)
- Bosnia (July)



| ICAO

SECURITY & FACILITATION



## 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

SECURITY & FACILITATION



## 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)


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 on 13 July 2010  
(place) (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	
<b>PASSPORT DATA</b>	
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
<b>eMRTD AUTHORITY (EMA) DETAILS</b>	
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
<b>eMRTD COUNTRY SIGNING CERTIFICATE AUTHORITY (CSCA)</b>	
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 2019 based on 60+ Active Participants:  
**US \$ 29,853** (Operator Fee US \$ 22,500 + ICAO Operator fee US \$ 7,353)

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 2019 the ICAO Operation Fees have been established at US \$7,353.00.



Active Participants	Operator Fees (US \$)	ICAO * Fees (US \$)
50 Participants	27,000.00	9,118.00
55 Participants	24,500.00	8,289.00
60 Participants	22,500.00	7,353.00
65 Participants	20,900.00	7,013.00



| ICAO

SECURITY & FACILITATION



## 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.



| ICAO

SECURITY & FACILITATION



## 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.



| ICAO

SECURITY & FACILITATION



## 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



| ICAO

SECURITY & FACILITATION



## 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



## 25<sup>e</sup> PKD Board Meeting in ICAO Paris Office





ICAO

## SECURITY & FACILITATION



ICAO

North American  
Central American  
and Caribbean  
(NACC) Office  
Mexico City

South American  
(SAM) Office  
Lima

ICAO  
Headquarters  
Montréal

Western and  
Central African  
(WACAF) Office  
Dakar

European and  
North Atlantic  
(EUR/NAT) Office  
Paris

Middle East  
(MID) Office  
Cairo

Eastern and  
Southern African  
(ESAF) Office  
Nairobi

Asia and Pacific  
(APAC) Sub-office  
Beijing

Asia and Pacific  
(APAC) Office  
Bangkok



THANK YOU