



ICAO

SECURITY & FACILITATION



NO COUNTRY LEFT BEHIND



# ICAO Public Key Directory (PKD) How to join

**Christiane DerMarkar**

*ICAO PKD Officer*

Antigua & Barbuda ICAO TRIP Regional Seminar

31 January – 2 February 2017

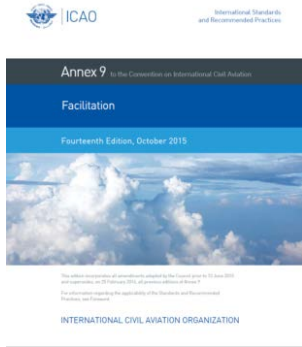


# ICAO PKD: one of the 3 interrelated pillars of Facilitation




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



NO COUNTRY LEFT BEHIND



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



## 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



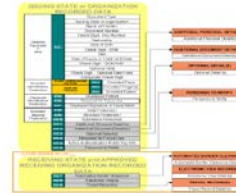
Machine Readable  
Passport (MRP)



CHIP RFID  
14443



IMAGE  
FACE



Logical  
Data  
Structure  
(LDS)



0111001001010

PKI DIGITAL  
SIGNATURE  
Public Key  
Directory  
(PKD)



# ePassport Issuance and Validation

- **CSCA - Country Signing Certificate Authority Certificate:** It is the national trust point for ePassport. It is the anchor of the trust chain.
- **DSC - Document Signer Certificate:** Contain 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



# ePassport Issuance and Validation

## The chain of trust:





# What is the PKD & Why you Should Join?

- ❖ A central Repository for exchanging the information required to authenticate ePassport and facilitates fast and secure cross-border movement of citizens by the “frontline” entities
  
- ❖ 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

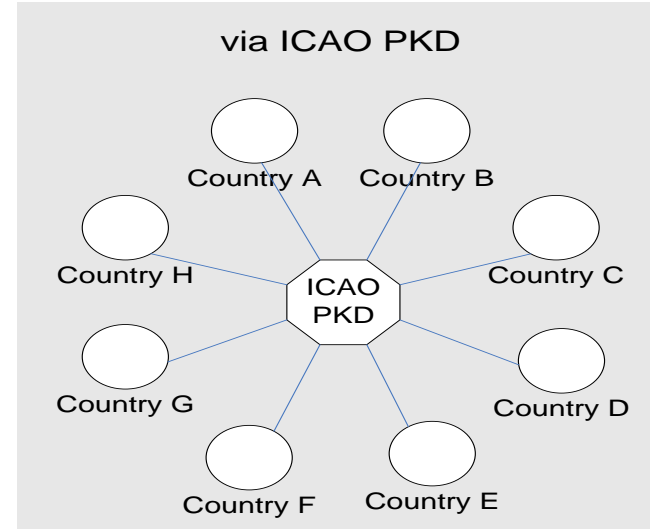
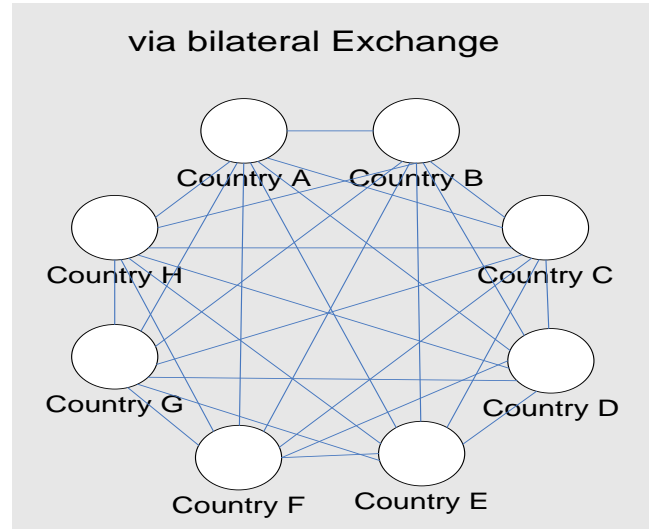
- Minimizing the volume of certificate exchange:
  - Document Signer Certificates (DSCs)
  - Certificate Revocation Lists (CRLs)
  - Country Signing Certificate Authority (CSCA) Master List
- Ensuring timely uploads
- Managing adherence to technical standards
- Facilitating the validation process





# Central Broker

## Distribution of Certificates and CRLs



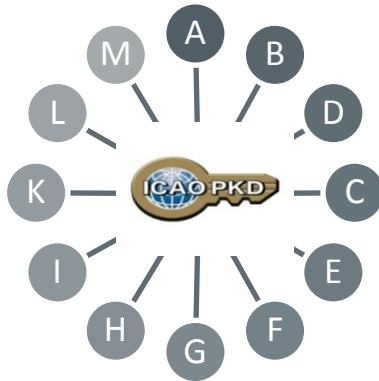
This example shows **8** States/non-States requiring **56** bilateral exchanges (left ) or 2 exchanges with the PKD (right) to be up to date with DSCs and CRLs. In case of **191** ICAO States **36,290** bilateral exchanges would be necessary while there are still 2 exchanges with the PKD.



## 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

+

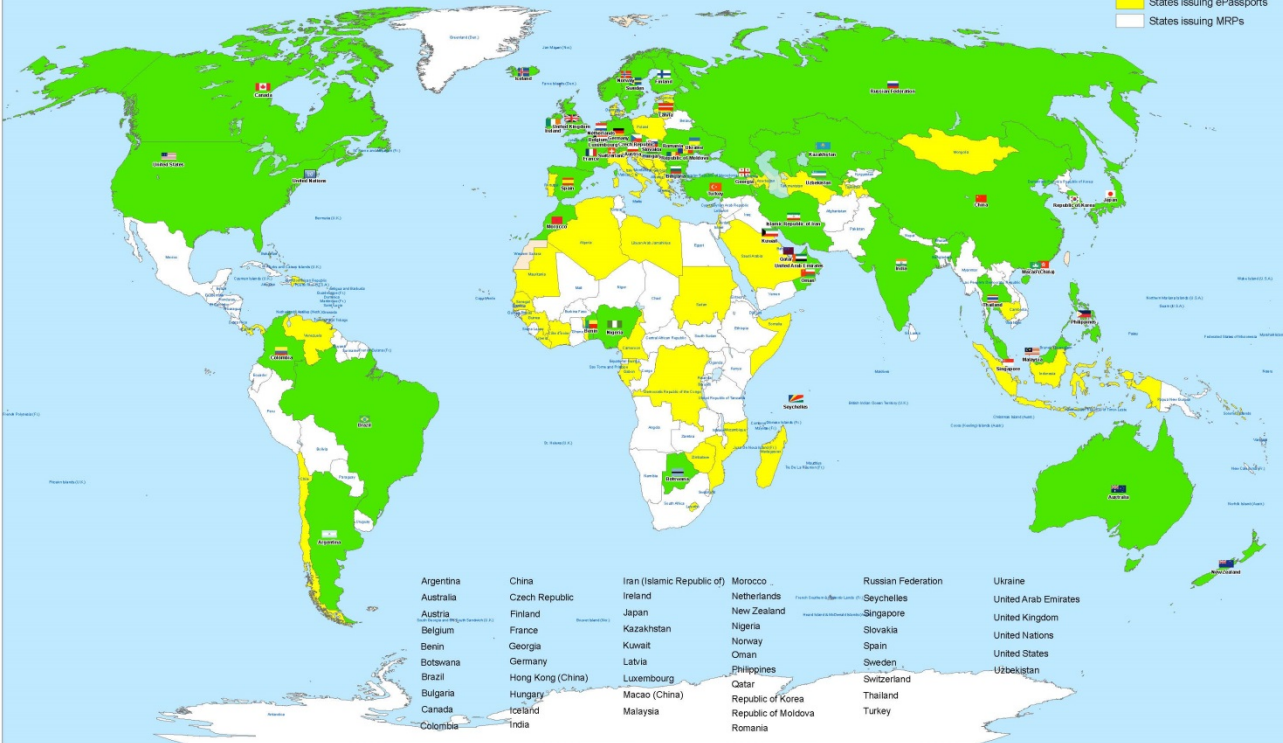


= currently in the PKD



### 55 PKD Participants and ePassports issuing States

**Legend**  
 ■ PKD Participants  
 ■ States issuing ePassports  
 ■ States issuing MRPs



# 55 Participants

## New 2016 Participants:

- Romania
- Finland
- Benin
- Botswana
- Kuwait
- Georgia
- Turkey
- Iceland
- Oman

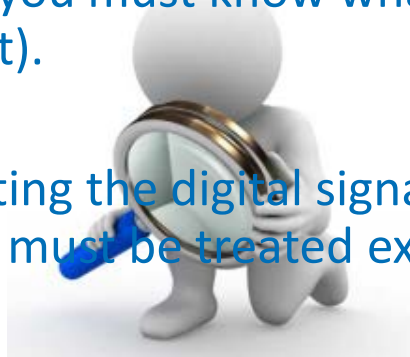


## Reasons to Participate

- 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 and facilitate the movement of citizens.





| ICAO

SECURITY & FACILITATION



NO COUNTRY LEFT BEHIND



## 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



ICAO

SECURITY & FACILITATION



NO COUNTRY LEFT BEHIND



## Steps to join the PKD

1. Deposit a Notice of Participation and Notice of Registration with the Secretary General of ICAO
2. Once the signed Notice of Participation is received by ICAO, the officer designated by the State will receive a Registration Fee invoice of **US \$15,900.00**



ICAO

SECURITY & FACILITATION



NO COUNTRY LEFT BEHIND



## Steps to join the PKD

4. **The payment of the Registration Fee to ICAO is necessary in order to become a PKD participant.**
5. Securely submit to ICAO and all Participants, the CSCA certificate
6. **Use the PKD : upload/Download certificates**
7. <http://www.icao.int/Security/FAL/PKD/Pages/How-to-Participate.aspx>



ICAO

SECURITY & FACILITATION



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 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 [Handwritten Signature]

http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU(includeslanguageversion(s))/NoticeofParticipation-Model.pdf

1. Select PKD documents





ICAO

SECURITY & FACILITATION



[http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU\(includeslanguageversion\(s\)\)/NoticeofRegistration-Model.pdf](http://www.icao.int/Security/FAL/PKD/Documents/PKDMoU(includeslanguageversion(s))/NoticeofRegistration-Model.pdf)

## 1. Select PKD documents

### 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@Mol.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



## Fees reduction

- A. Registration Fee: **US \$15,900**
- B. 2017 Annual Fees based on 55 Participants: **US \$ 34,400**
- C. More Participants = reduction in Operators and ICAO Annual Fees



Active Participants	Operator and ICAO Fees
50 Participants	37,000.00 US\$
55 Participants	34,400.00 US\$
60 Participants	32,500.00 US\$
65 Participants	30,900.00 US\$



ICAO

SECURITY & FACILITATION



NO COUNTRY LEFT BEHIND



## 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. Full conformity to Doc 9303 is required.



ICAO

SECURITY & FACILITATION



NO COUNTRY LEFT BEHIND



## Becoming Active

1. Every new Participant is given two documents:
  - Interface Specifications document - the protocol for accessing the PKD.
  - PKD Pre-Production Environment Procedures
2. The Participant is required to be familiar with both documents before starting the PKD testing and integration.
3. The pre-production system is available for all participants in order to:
  - Test the interface between their national infrastructure and the ICAO PKD System
  - Test their PKD Data prior to the upload to the ICAO PKD Production System
  - Check conformance of the PKD Data against the PKD Upload Conformance Checks



| ICAO

SECURITY & FACILITATION



NO COUNTRY LEFT BEHIND



## Becoming Active

4. Website for Conformance Checks: allows for checking the certificates before they are imported or uploaded to the PKD actual LDAP upload.
5. The website can be accessed via the following URL, using certificate-based authentication with an upload certificate: <https://reference.upload.pkd.icao.int>



ICAO

SECURITY & FACILITATION




NO COUNTRY LEFT BEHIND



Conformance Website - Windows Internet Explorer

https://reference.upload.pkd.icao.int/pkdvalidation#top

Conformance Website



# CONFORMANCE WEBSITE

## DESCRIPTION

The conformance website for ICAO PKD participating states provides a conformance check of PKD data (Master Lists, Document Signer Certificates, Certificate Revocation Lists) and CSCA certificates. The checks will report compliance to B-Tec/26 and B-Tec/48.

### Step 1 - Select your item to be validated

- Masterlist
- Document Signer Certificate - (DS Certificate)
- Certificate Revocation List (CRL)
- Country Signing Certificate Authority Certificate - (CSCA Certificate)
- Country Signing Certificate Authority Link Certificate - (CSCA Link Certificate)

### Step 2 - Select the corresponding file on your PC

### Step 3 - Send the file to get the validation result

Done Internet | Protected Mode: Off 100%



ICAO

SECURITY & FACILITATION



NO COUNTRY LEFT BEHIND



## CSCA IMPORT

1. The Participant should check the CSCA certificate to be imported by the means of the ICAO PKD conformance website (<https://reference.upload.pkd.icao.int/>)
2. In case of issues with the certificate the participant should contact the PKD support of Veridos ([pkdsupport@verdios.com](mailto:pkdsupport@verdios.com)) for assistance.
3. If conformance is confirmed, the PKD Participant will submit its CSCA certificate along with the electronic thumbprint to ICAO by electronic means for registering the key ceremony.



ICAO

SECURITY & FACILITATION



NO COUNTRY LEFT BEHIND



## CSCA IMPORT

1. The credentials of the PKD Participant representative will need to be submitted: Passport # and Identity Details
2. A date will for the import will be fixed
3. On the date of the import: In the presence of the State Representative and ICAO Security Officers, the CSCA is imported in the High Secure Module (HSM):  
**the anchor of trust for the PKD.**
4. A protocol of the Import will be signed by both the PKD participant Representative and ICAO confirming that the Anchor of Trust has been imported into the PKD HSM





ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



# CSCA IMPORT Protocol

## Protocol for Key Ceremony with Representative

Participant	CO
Key Ceremony ID	351
Created by	Helen Manentis
Created at	Oct 26, 2016 2:00:10 PM

### Representative

Sex	MALE
Title	Representative of Colombia on the Council of ICAO
Full Name	Alberto Munoz Gomez
Date of Birth	04/11/1959
E-Mail	
ID Type	Passport
ID Number	DP046143
ID Expiration Date	Jun 15, 2020

### CSCA Certificate

Fingerprint	3D:47:9E:80:BE:C0:54:BF:13:19:C9:18:49:A4:7B:AA:D4:7C:E6:80
Certificate ID	CN=Government of Colombia CSCA,OU=Certification Authorities,O=Colombia,C=CO / 55770B5A

### PKD Operator

Imported at	Helen Manentis Oct 27, 2016 8:55:03 PM
-------------	---

### PKD Officer

Imported at	Christiane DerMarkar Oct 27, 2016 8:57:18 PM
-------------	---



ICAO



Representative



## Some Arguments repeated over and over ....



**It's too expensive**

**Bilateral exchange works good enough**

**It's not necessary – DSCs are (mostly) on the chip**

**It's too complicated – we must first introduce ePassports**



**As of 01.01.2016 Fee reduction**

**cumbersome, time consuming and possible security risk**

**A DSC on the ePassport but not on the PKD could mean a compromised private signing key. & CRLS are only distributed via PKD...**

**-----> CHAIN OF TRUST**

**➔ Participation in the PKD should go hand in hand with introduction of ePassports**

**➔ PKD participation is key for setting up any successful ePassport based border control.**



| ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



# Conclusion

- ICAO urges all ICAO Member States to join and actively use the ICAO PKD to validate and authenticate ePassports at Border Controls.



| ICAO

SECURITY & FACILITATION



NO COUNTRY LEFT BEHIND



THANK YOU

Contact Details

Name: Christiane DerMarkar  
Email: [cdermarkar@icao.int](mailto:cdermarkar@icao.int)