



| ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



ICAO PUBLIC KEY DIRECTORY (PKD) – Comment joindre le PKD de l'OACI

Christiane DerMarkar
ICAO PKD Officer

05/12/2018





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





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

NO COUNTRY LEFT BEHIND



Connection between PKD and ePassports

MRP



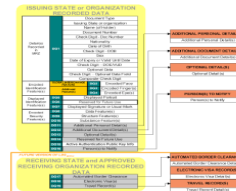
Machine Readable
Passport (MRP)



CHIP RFID
14443



IMAGE
FACE



Logical
Data
Structure
(LDS)



0111001001010

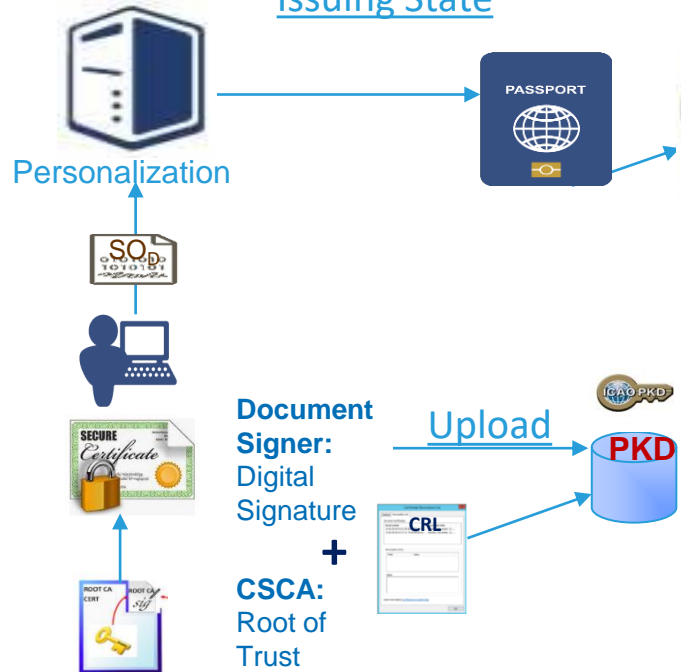
PKI
Certificate
from the
Public Key
Directory
(PKD)



Sharing the information

Operational View

ePassport Issuance Issuing State



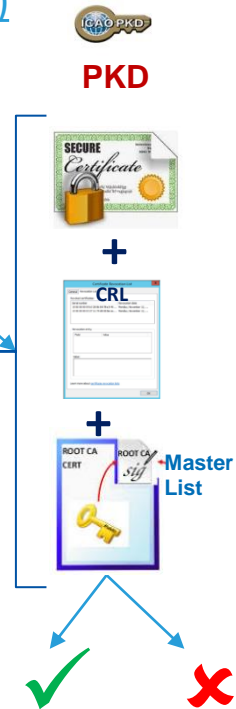
ePassport Inspection (Manual or Automated) Receiving State

Importance of being **compliant** with
Doc 9303 - Machine Readable Travel Document



Inspector / Inspection System

- Verify digital signature of State
- Validate data integrity and authenticity (Photo, etc...)
- Physical inspection





ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



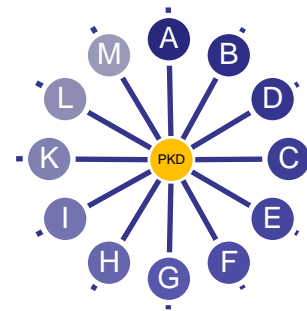
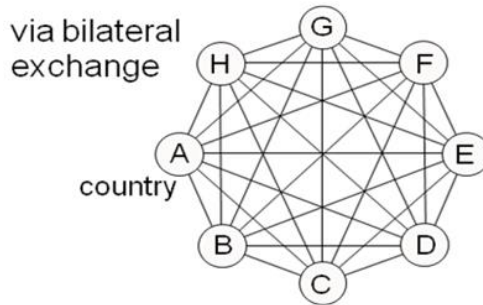
What is the PKD and what is its role

❖ 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





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.



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



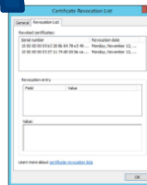
eMRTD



Document Signer (DSC)



CRL



+

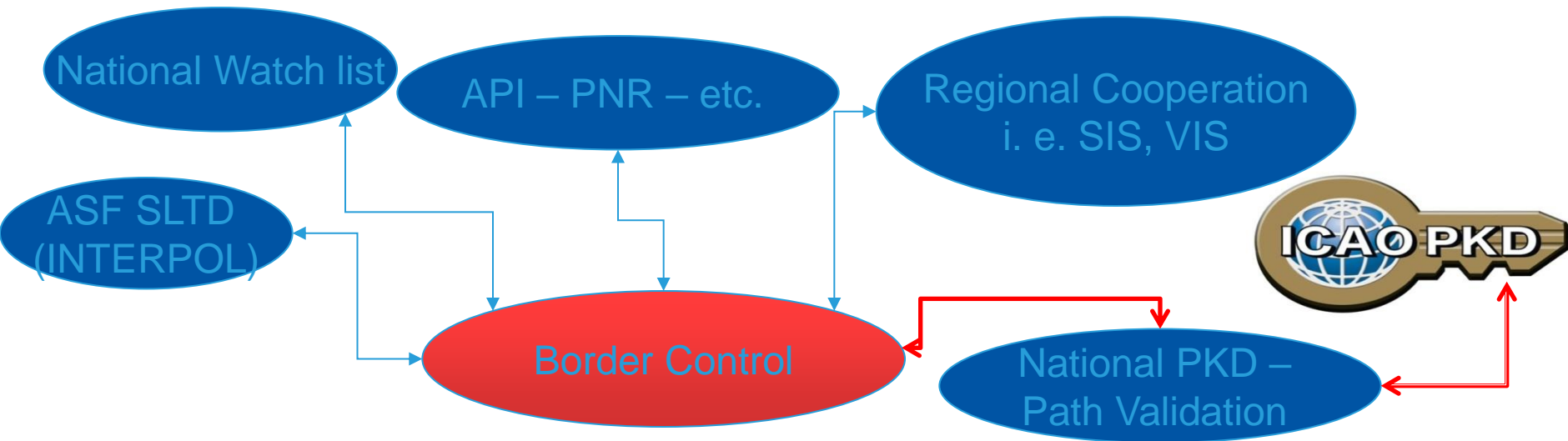
+

Validation Trust Chain





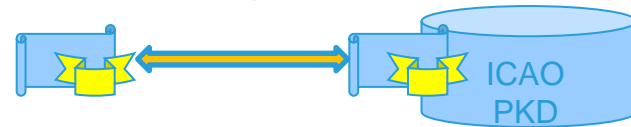
Border Control: the ideal setup includes ICAO PKD





Reasons to participate

- If not done at the same time, the participation at the ICAO PKD should be the immediate next goal of a country after introducing ePassports.
- 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).
- A reliable certificate exchange is a requirement for the use of automated border controls abroad by your citizens.





In the best national interest

- Issuing Authorities interests in the PKD

→ Sharing of the information necessary for the world wide recognition of a nation's ePassport, allowing it's citizens to cross borders as easily as possible (business, leisure, family relations etc.).

→ ePassports that cannot be validated must essentially be considered and treated as a non-electronic travel document and provides no added security.

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



ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



In the best national interest

- **Border Control Authorities interests in the PKD**

- ➔ Secure, reliable and fast border checks, living up to the citizens expectations for facilitation & security.
- ➔ Performing ePassport validation 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.
- ➔ PKD participation is not only the key for setting up successful Automated Border Controls, but any ePassport based border control.
- ➔ **By utilizing the ICAO PKD in the border control agencies a State proactively contributes to international border security and to aviation security.**



ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



In the best interest of your citizens

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.

 State participating in the ICAO PKD will facilitate international travelling for its citizens:

- Citizens from PKD Participant State will be more trusted at foreign borders
- Citizens with e-Passports can enjoy easier border crossings.



Facts and Figures

- We currently have 62 PKD Participants but over 120 States and non-State entities that issued about 850,000,000 ePassports (June 2017).
- 80% of ePassport in circulation are issued by PKD Participants and can be validated by using the PKD.
- Not or too late detected falsifications/misuses of eMRTDs lead to a massive loss of credibility in the ePassport and would impact on future developments.



ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



How to join?

- All the information and necessary forms can be found:
<https://www.icao.int/Security/FAL/PKD/Pages/How-to-Participate.aspx>



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?

Avoid inter agency disputes about competences, it's in everybody's interest

Question 2: Payment ?

- 1- Do you need to assign a paying entity
- 2- Do you have a budget that is set on a recurrent basis to ensure regular and annual membership payment ?

Question 3: Points of contact.

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



ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



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. Actively Use the PKD: Upload/Download to and from the PKD.



ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



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.
- An Operation agreement, NOT an International Treaty.
- The signatory should be from the Executive level.
- Notice of Participation: Attachment A to the PKD MoU
- <https://www.icao.int/Security/FAL/PKD/Pages/Publications.aspx>



ICAO

SECURITY & FACILITATION



Step 1: Deposit a Notice of Participation with the Secretary General of ICAO

Attachment A of the PKD MoU

<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 on 13 July 2010
(place) *(date)*
Republic of Utopia
On behalf of _____
Ministry of Interior
Name of Authority _____
Name, title Mr. Dolittle, Head of Division for Documents Law
Signature 



| ICAO

SECURITY & FACILITATION



Step 2:

Deposit a Notice of Registration with the Secretary General of ICAO

Attachment B of the PKD Rules and Regulations

<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



Step 3: Pay the Fees

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



Step 4: Active Participation

PKD Integration

1. Every new Participant is given two documents:
 - ☐ Interface Specifications document - the protocol for accessing the PKD.
 - ☐ PKD Pre-Production Environment Procedures
2. 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.
3. Participant are required to have completed the testing of the PKD interface and successfully imported the CSCA into the HSM in Montreal.
4. The PKI Infrastructure between National and ICAO PKD should be implemented.



ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



Becoming Active

1. Website for Conformance Checks: allows for checking the certificates before they are imported or uploaded to the PKD actual LDAP upload.
2. The website can be accessed via the following URL, using certificate-based authentication with an upload certificate: <https://reference.upload.pkd.icao.int>
6. 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/>)
7. 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




<https://reference.upload.pkd.icao.int>

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%



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 first 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 completed, 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

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

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


ICAO
Representative



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

NO COUNTRY LEFT BEHIND



25th PKD Board Meeting in ICAO Paris Office





ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



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

More Participants leads to reduced PKD fees

cumbersome, time consuming and possible security risk

DSC from the PKD ahead of the arrival & validate it against it's CSCA -----> **CHAIN OF TRUST**
CRL's from the PKD

-----> speed up operations at the border

-----> no need to go to the CRL Distribution Point in real time to get the certificate.

➡ Participation in the PKD should go hand in hand with introduction of ePassports

➡ PKD participation is key for setting up any **effective** ePassport based border control.



ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



Conclusion- ICAO 39th Assembly

- 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



ANY QUESTION???

- Christiane DerMarkar
- ICAO PKD Officer
- cdermarkar@icao.int



ICAO

SECURITY & FACILITATION

NO COUNTRY LEFT BEHIND



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