ICAO SECURITY & FACILITATION NO COUNTRY LEFT BEHIND

ICAO Public Key Directory (PKD)

Christiane DerMarkar

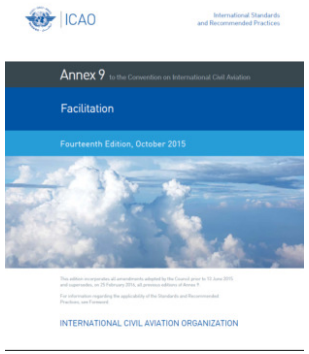
Programme Officer, PKD

Hong Kong ICAO TRIP Regional Seminar

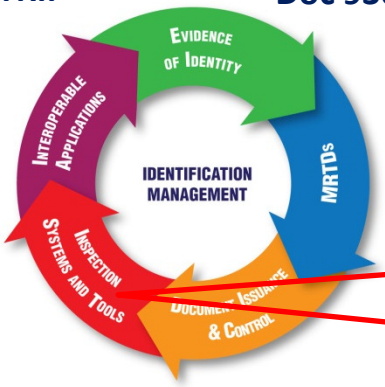
ICAO PKD: one of the 3 interrelated pillars of Facilitation

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

Connection between PKD and ePassports

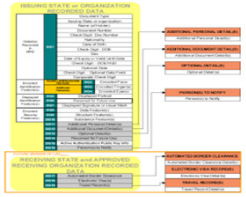
MRP

Machine Readable Passport (MRP)

ePASSPORT

CHIP RFID 14443

IMAGE FACE



Logical Data Structure (LDS)

0111001001010

PKI Certificate from the Public Key Directory (PKD)

ePassport Issuance and Validation

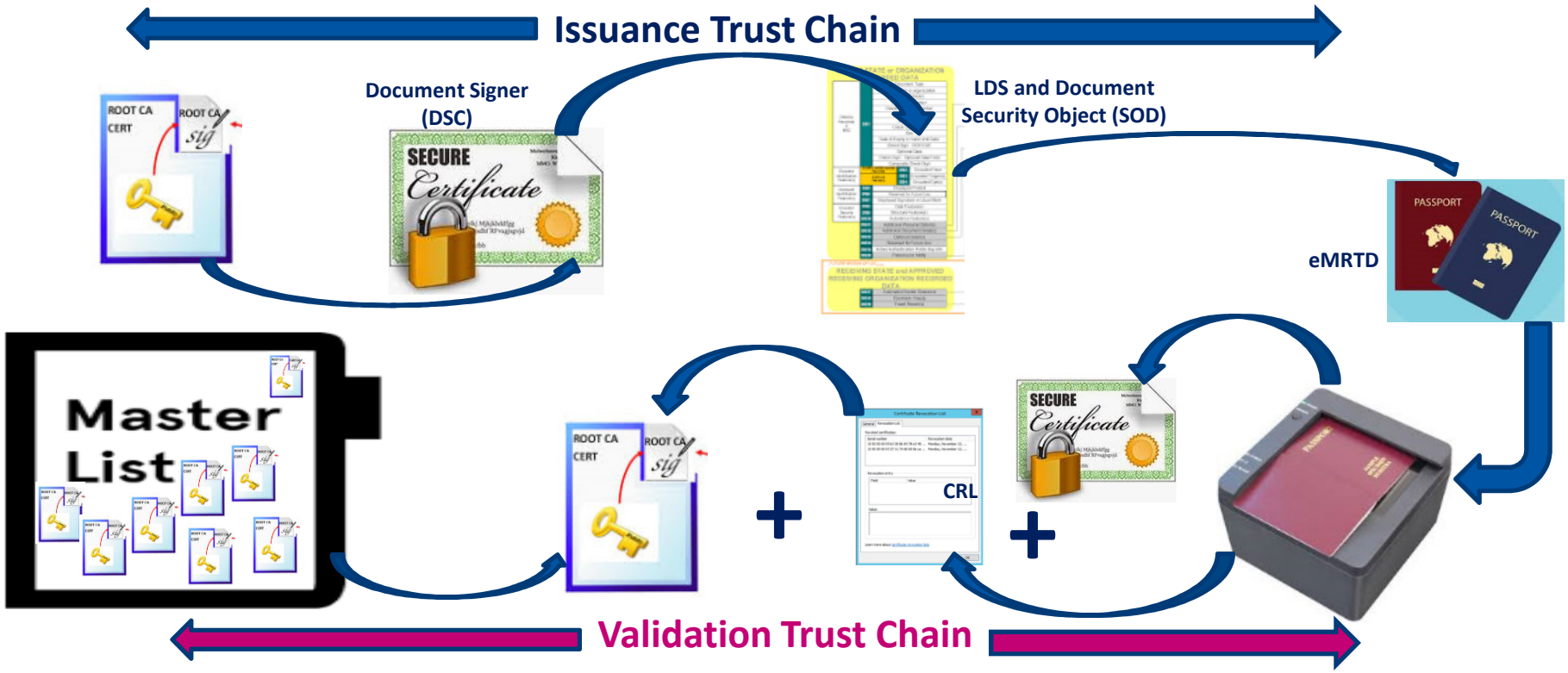
- **CSCA - Country Signing Certificate Authority Certificate**: It is the national trust point for ePassport. It is the anchor of the trust chain.

- **DSC - Document Signer Certificate**: 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

ePassport Issuance and Validation



Basic eMRTD Validation passive authentication

Authentication of Personal Data + Face

National PKD with Country Signing Certificate Authorities (CSCAs), Document Signer (DSC), Certificate Revocation lists(CRLS) and Master Lists (ML)

Inspection System

ICAO PKD

Up and download of:
- DSCs
- CRLs
- Master Lists

- Signed personal data
- Document Signer Certificates

What is the PKD & Why you Should Join?

- A central Repository for facilitating the exchange of information required to authenticate ePassport
- and in turn facilitates the fast and secure cross-border movement of citizens by the ‘’frontline’’ entities

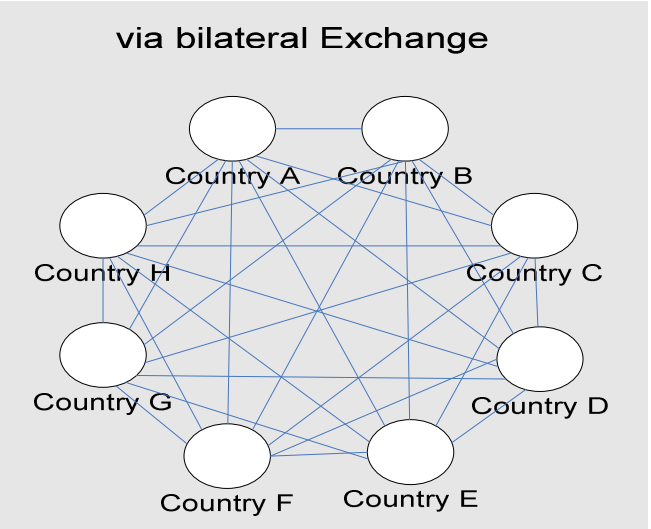
- It allows Border Control authorities to confirm that the ePassport:
  - Was issued by the right authority for the country
  - Has not been altered
  - Is not a copy or cloned document

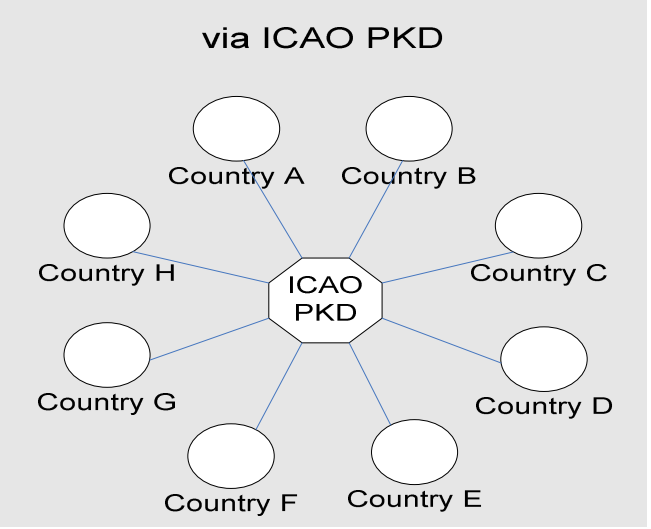
The Role of The PKD

- Minimizing the volume of certificate exchange:
  - Document Signer Certificates (DSCs)
  - Certificate Revocation Lists (CRLs)
  - Country Signing Certificate Authority (CSCA) Master List
  - Deviation List
- Ensuring timely uploads

Central Broker

Distribution of Certificates and CRLs



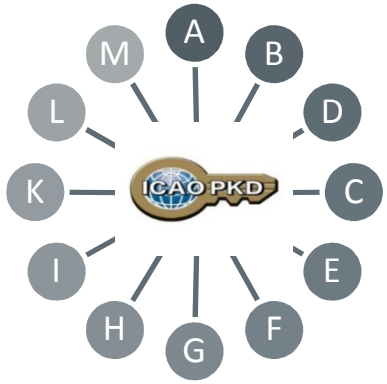


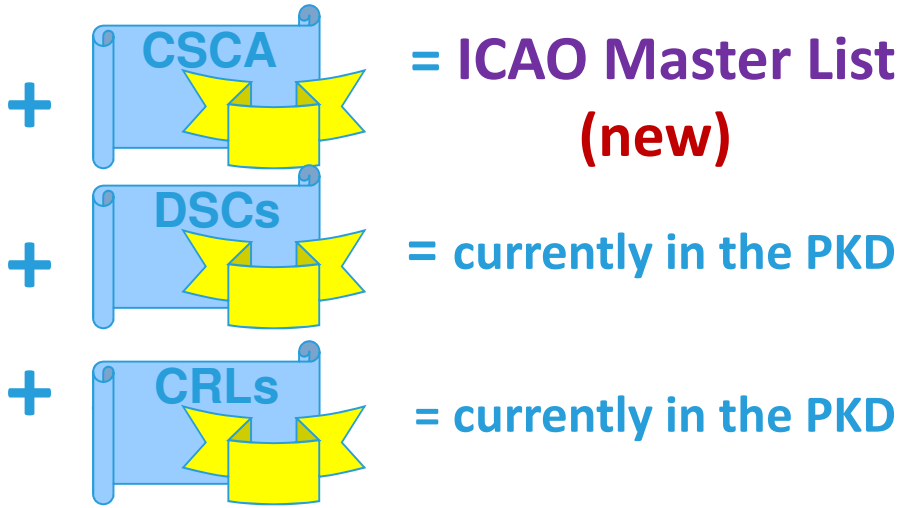
This example shows **8** States/non-States requiring **56** bilateral exchanges (left) or 2 exchanges with the PKD (right) to be up to date with DSCs and CRLs. In case of **191** ICAO States **36,290** bilateral exchanges would be necessary while there are still 2 exchanges with the PKD.

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





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.

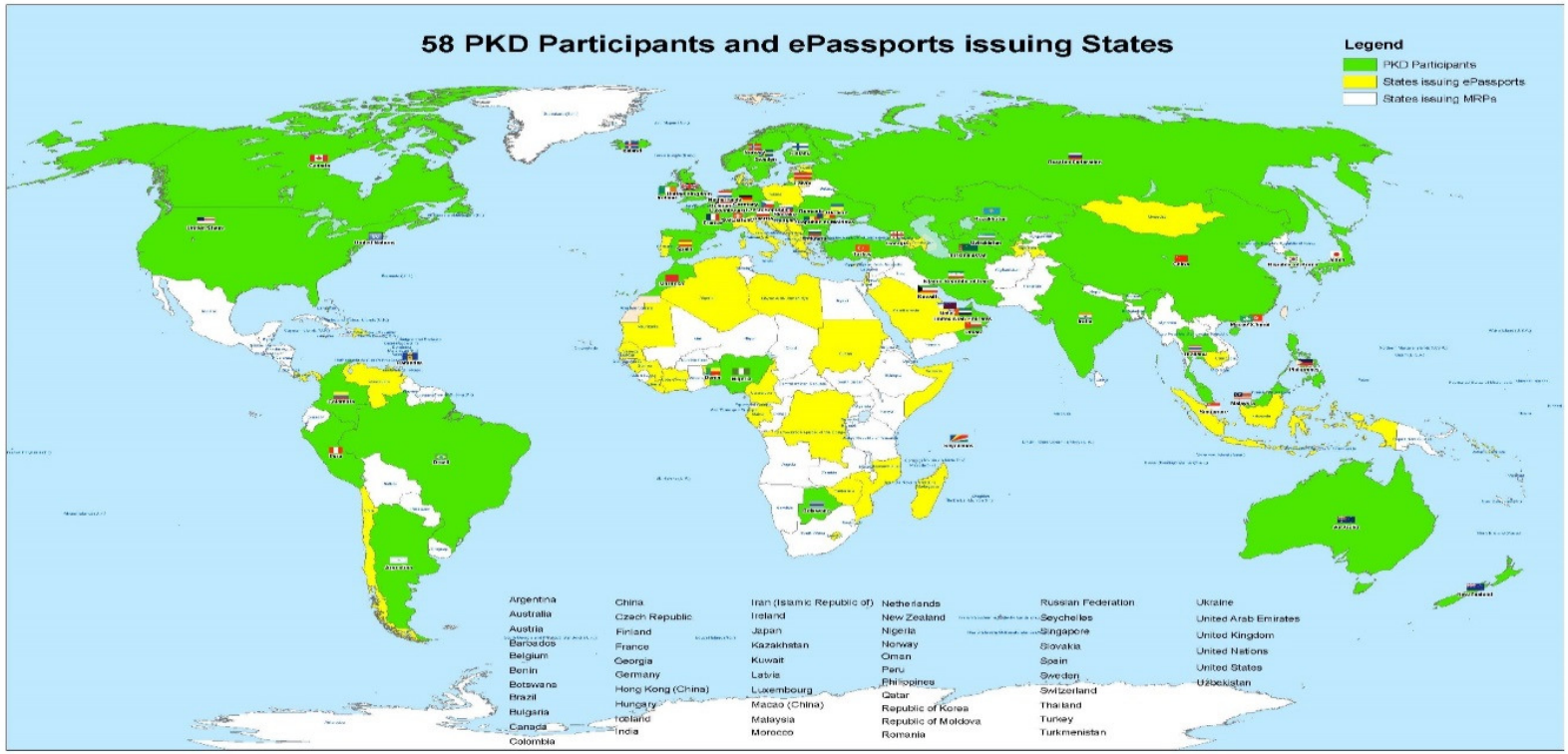
The ICAO PKD provides a means of accessing the necessary information published by other States in a cost efficient way that is always available.

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.

58 PKD Participants



New Participants 2016

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

New Participants 2017

- Turkmenistan
- Peru
- Barbados

ANNEX 9: Recommended Practice 3.9.1 & 3.9.2

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."

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 if you have questions

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

3. 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**

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

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

1. Select Notice of Participation

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/Publications.aspx

1. Select PKD MoU
2. 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 2017 based on 50+ Participants: US $ 34,351 (Operator Fee US $ 27,000, ICAO Operator fee US $ 7,351)

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 2017 the ICAO Operation Fees have been established at US $7,351.00.

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.

Becoming Active

1. Every new Participant is given two documents:
   - ❑ Interface Specifications document - the protocol for accessing the PKD.
   - ❑ PKD Pre-Production Environment Procedures

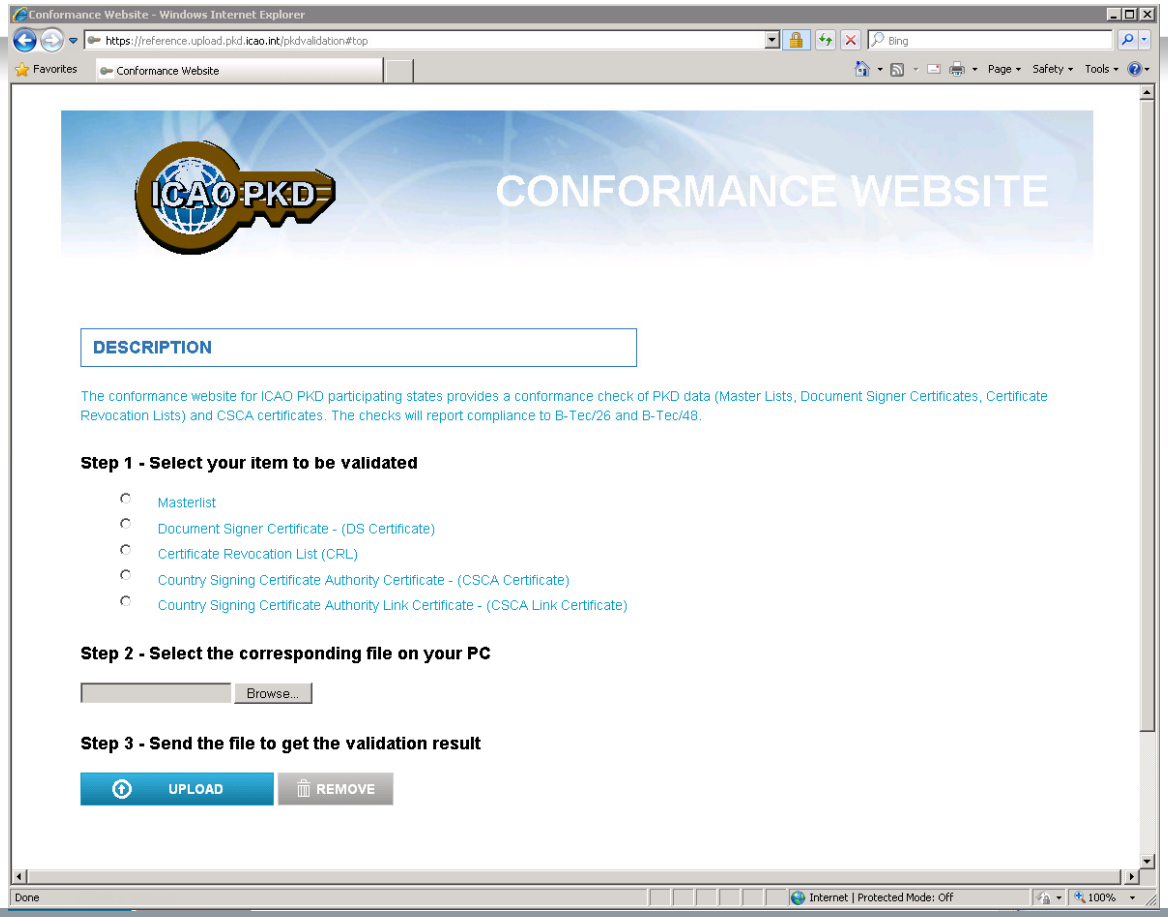
2. The Participant is required to be familiar with both documents before starting the PKD testing and integration.

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

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


Conformance Website - Windows Internet Explorer
https://reference.upload.pkd.icao.int/pkdvalidation#top
Favorites
Conformance Website
Page
Safety
Tools
ICAO PKD
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
Browse...
Step 3 - Send the file to get the validation result
UPLOAD
REMOVE
Done
Internet | Protected Mode: Off
100%

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) 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.

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

CSCA IMPORT Protocol

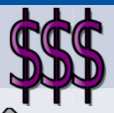
Protocol for
Key Ceremony with Representative

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

Some Arguments repeated over and over ….

It's too expensive 	As of 01.01.2016 Fee reduction
Bilateral exchange works good enough 	cumbersome, time consuming and possible security risk
It's not necessary – DSCs are (mostly) on the chip 	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.
It's too complicated – we must first introduce ePassports	➡ 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.

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.

THANK YOU

Contact Details

Name: Christiane DerMarkar
Email: cdermarkar@icao.int