The Importance of the Public Key Directory (PKD) in Ensuring eMRTD Security

David Philp

Chair – ICAO Implementation and Capacity Building Working Group (ICBWG)

Manager, New Zealand Passports

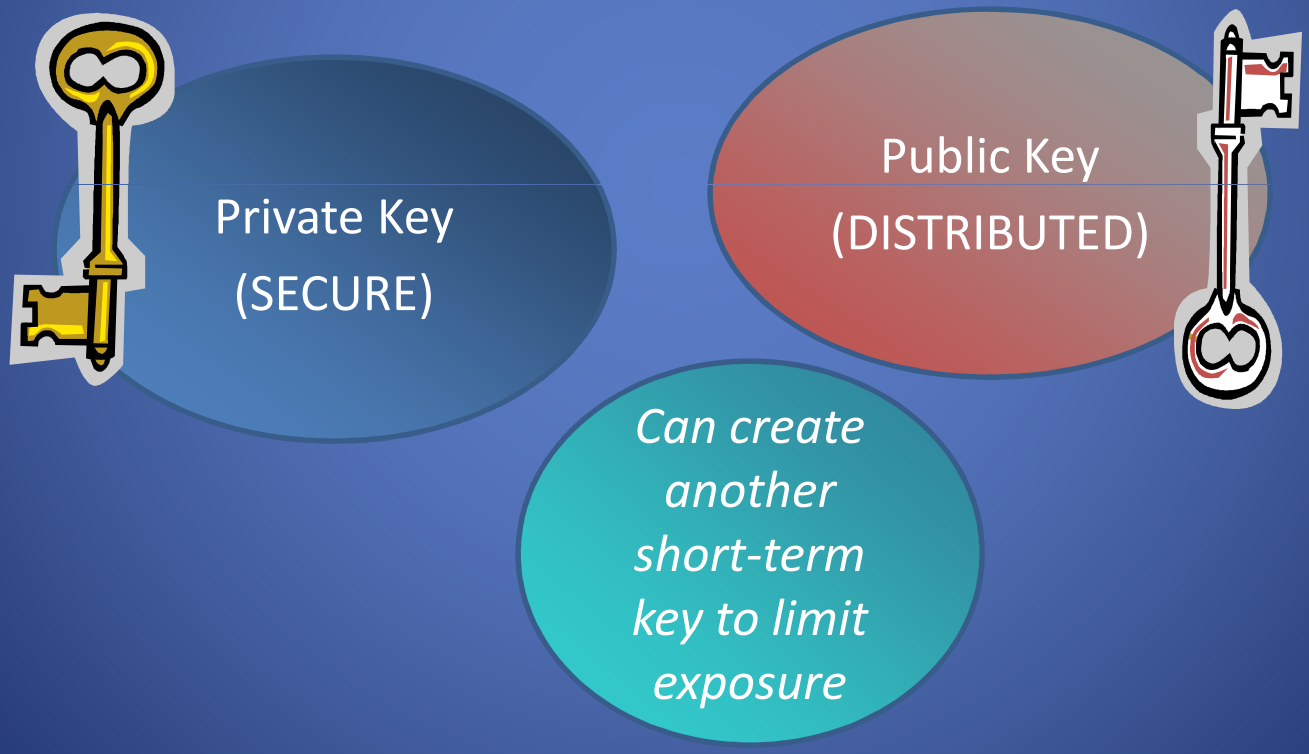
Introduction

- Potential benefits of the ePassport:
  - Facilitate cross-border facilitation
  - Enhance border security

- If the document is not electronically validated at the border using Public Key Infrastructure (PKI), the main benefits of the ePassport are lost

Public Key Infrastructure (PKI)

- Facilitates a trusted exchange between parties using two sets of keys



PKI for Passports

- Country Signing Certificate Authority (CSCA) securely generates two sets of keys
  - private country signing certificate with matching public key
  - private document signing certificate (DSC) with matching public key
- Private keys are not shared with anybody
- Public keys are distributed, and in the case of the DSC are written to the ePassport chip

PKI: Encryption

Passport data consists of MRZ data, facial image, and data groups 3-14 available for other biometrics and security information

Passport Data

Hash Algorithm

Hash Result 7EA3DA9540D

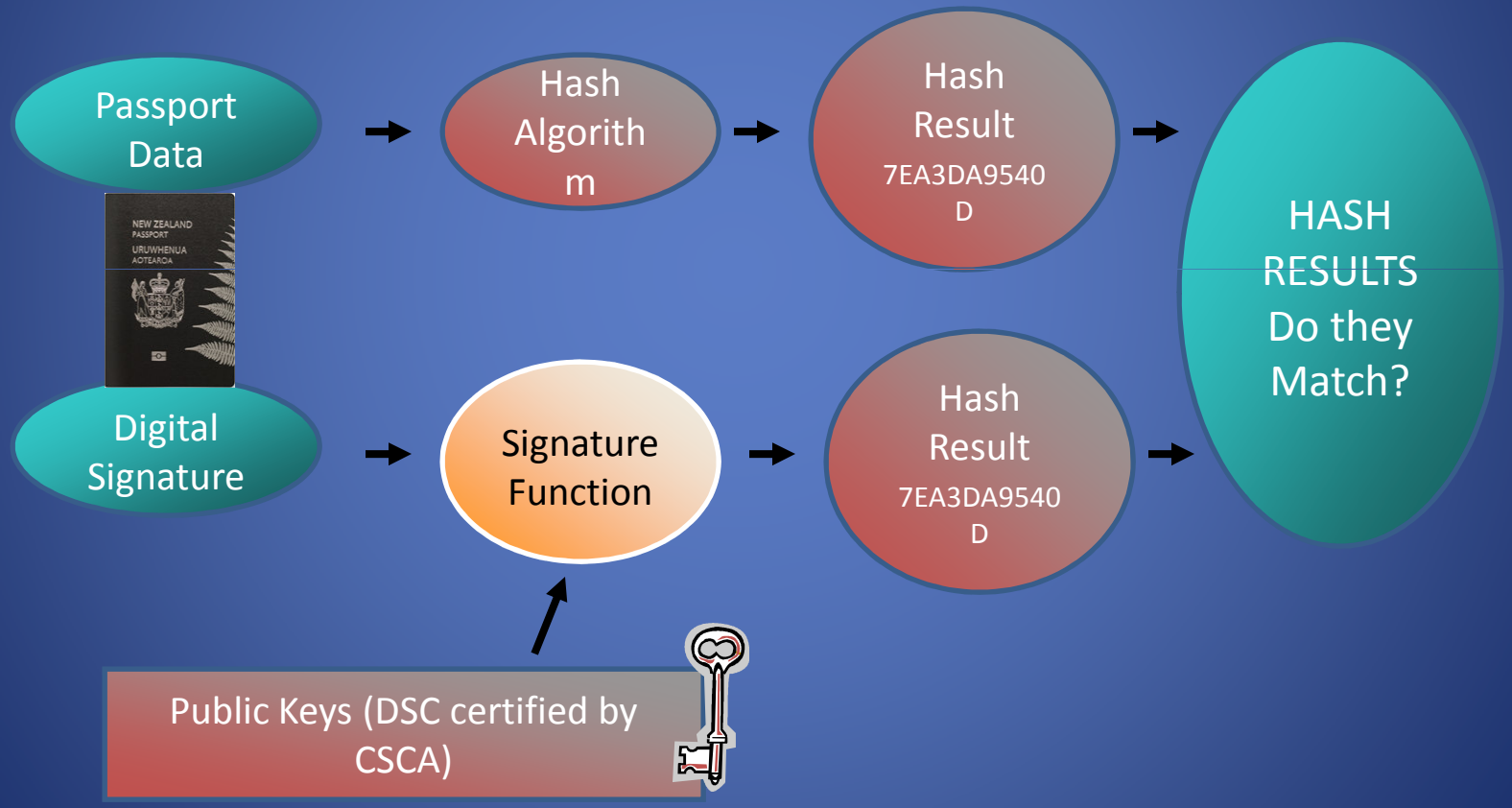
Signature Function

Chip Encoding
- Passport Data
- Digital Signature

Private Keys (DSC certified by CSCA)

PKI: Certificate Verification

- To ensure an ePassport is valid the data held on the chip must be authenticated each time it is read



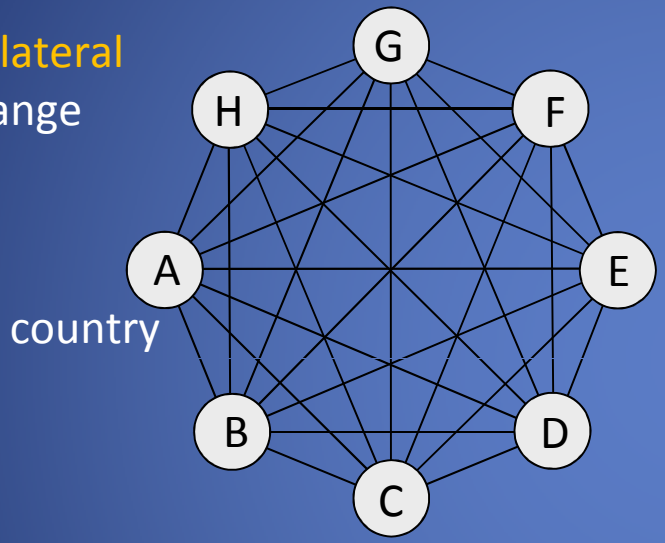
Public Key Directory (PKD)

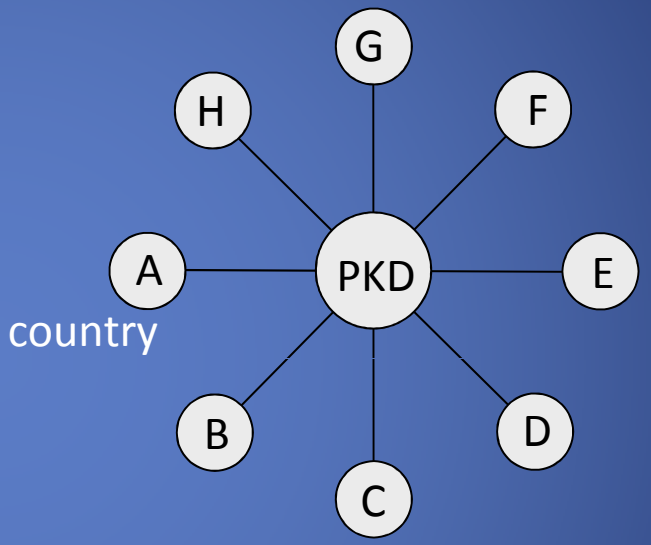
ICAO PKD:

- is a global distribution point for public signing key certificates from issuers of ePassports
- holds Document Signer Certificates and Certificate Revocation Lists that have been validated against respective Country Signing CA certificates
- holds Master Lists of certificates to further simplify the global PKI process
- can be accessed by border control authorities and other users 24/7

PKD Exchange Model

via bilateral exchange

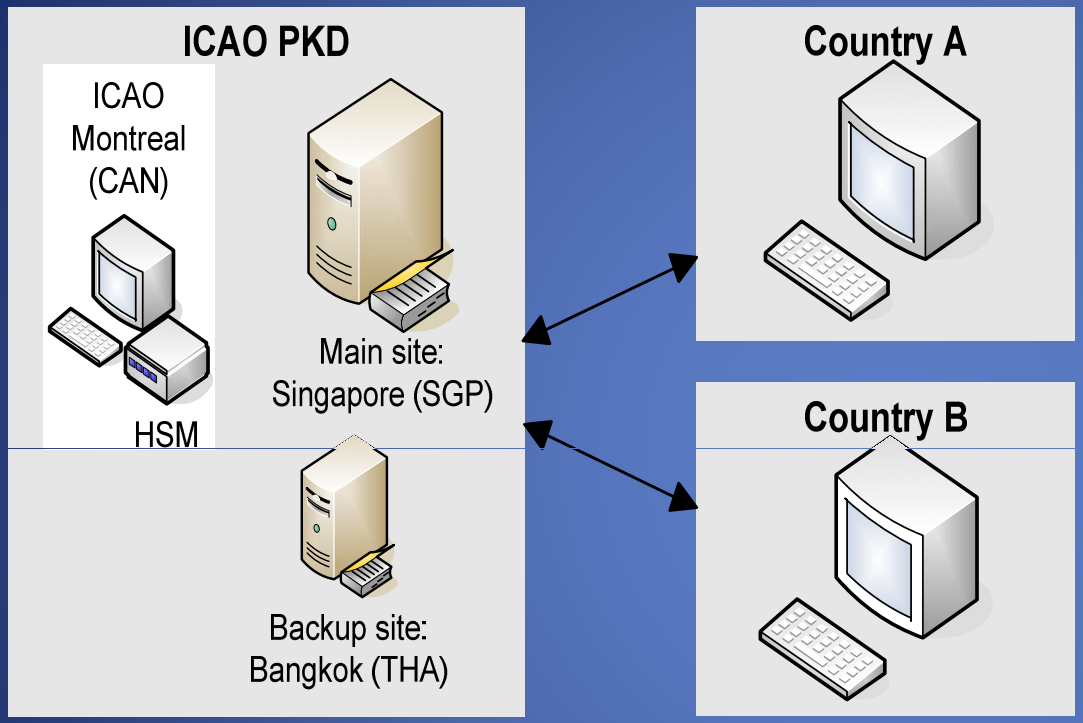




via PKD

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 revocation lists. In case of 190 ICAO States 35,910 bilateral exchanges would be necessary while there are still 2 exchanges necessary with the PKD.

PKD Infrastructure



High Availability

- 24/7 service, site backup

High Security

- HSM for CSCA Certificates
- pre-validated contents
- free registered download

main: https://pkddownloadsg.icao.int/
backup: https://pkddownloadth.icao.int/

Security Chain

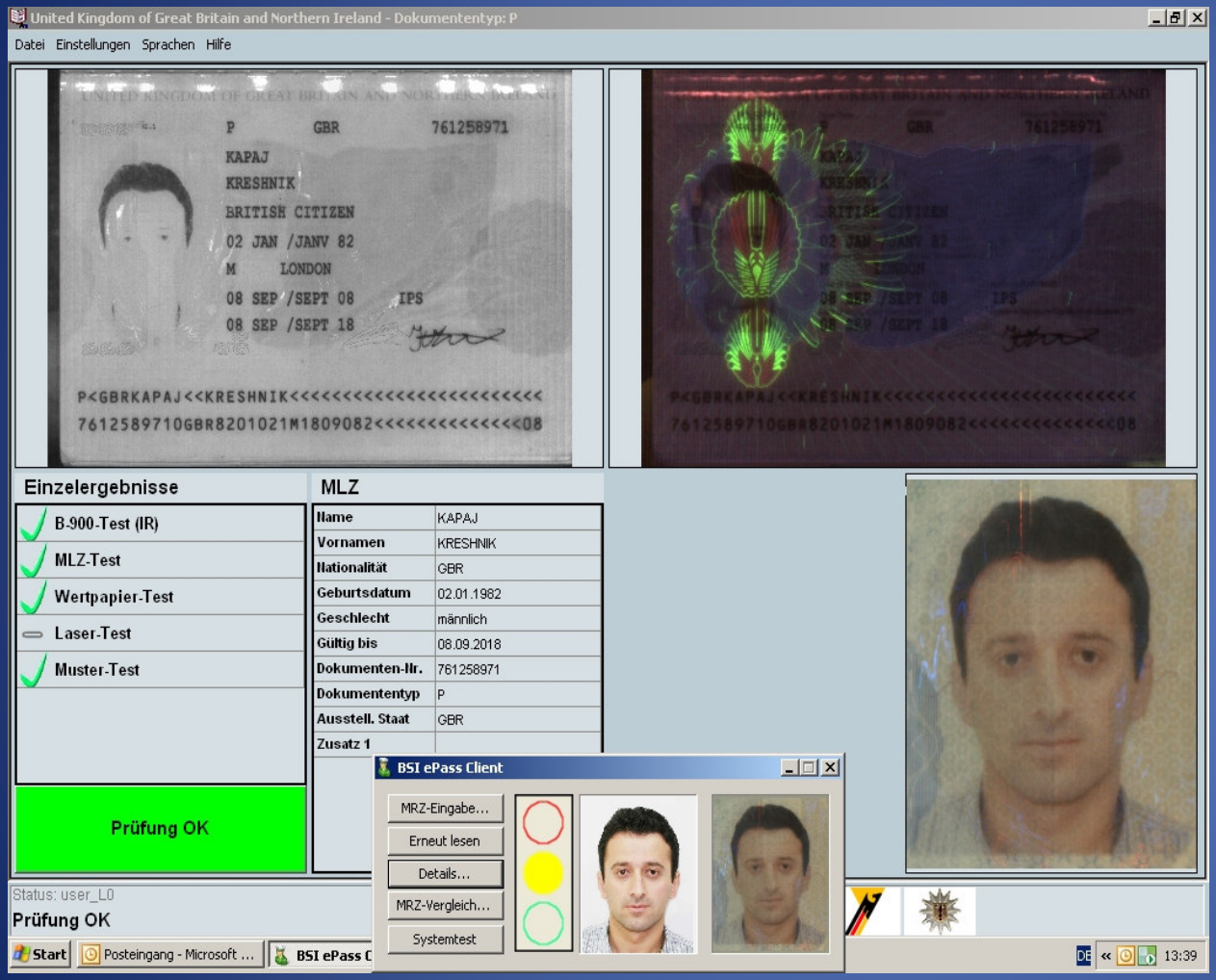
- Validation of ePassports through the exchange of PKI certificates is essential to realise the benefits of ePassports
- Validation of the chip signature using PKI certificates enables border control to determine whether:
  - a document held by a traveller has been genuinely issued by the responsible authority
  - biographic and biometric information on the chip has been altered after issuance
  - the certificate necessary to validate the document has been revoked

PKD Added Value

The ICAO PKD:

- Completes the authentication process of ePassports at border control
- Facilitates fast and secure cross border movement
- Is a resource for enhancing trust in ePassports
- Is a cost effective and efficient way of exchanging certificates

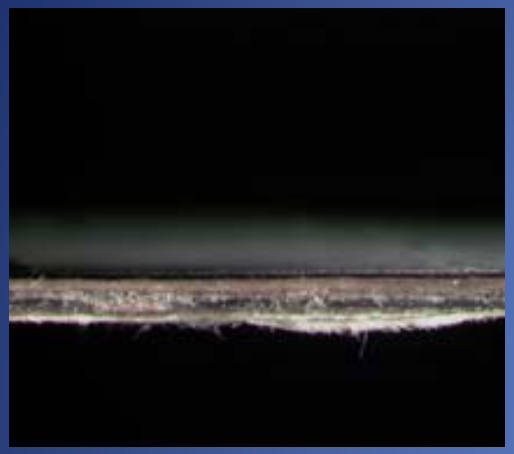
ePassport – Counterfeits (1)



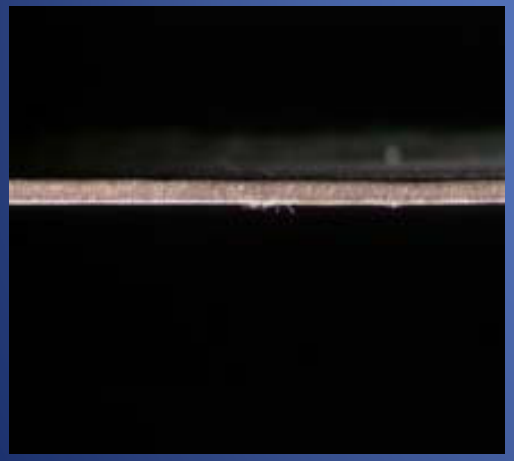
Example 2010

- traditional features verified
- electronic features: “yellow” traffic light

ePassport – Counterfeits (2)



fake

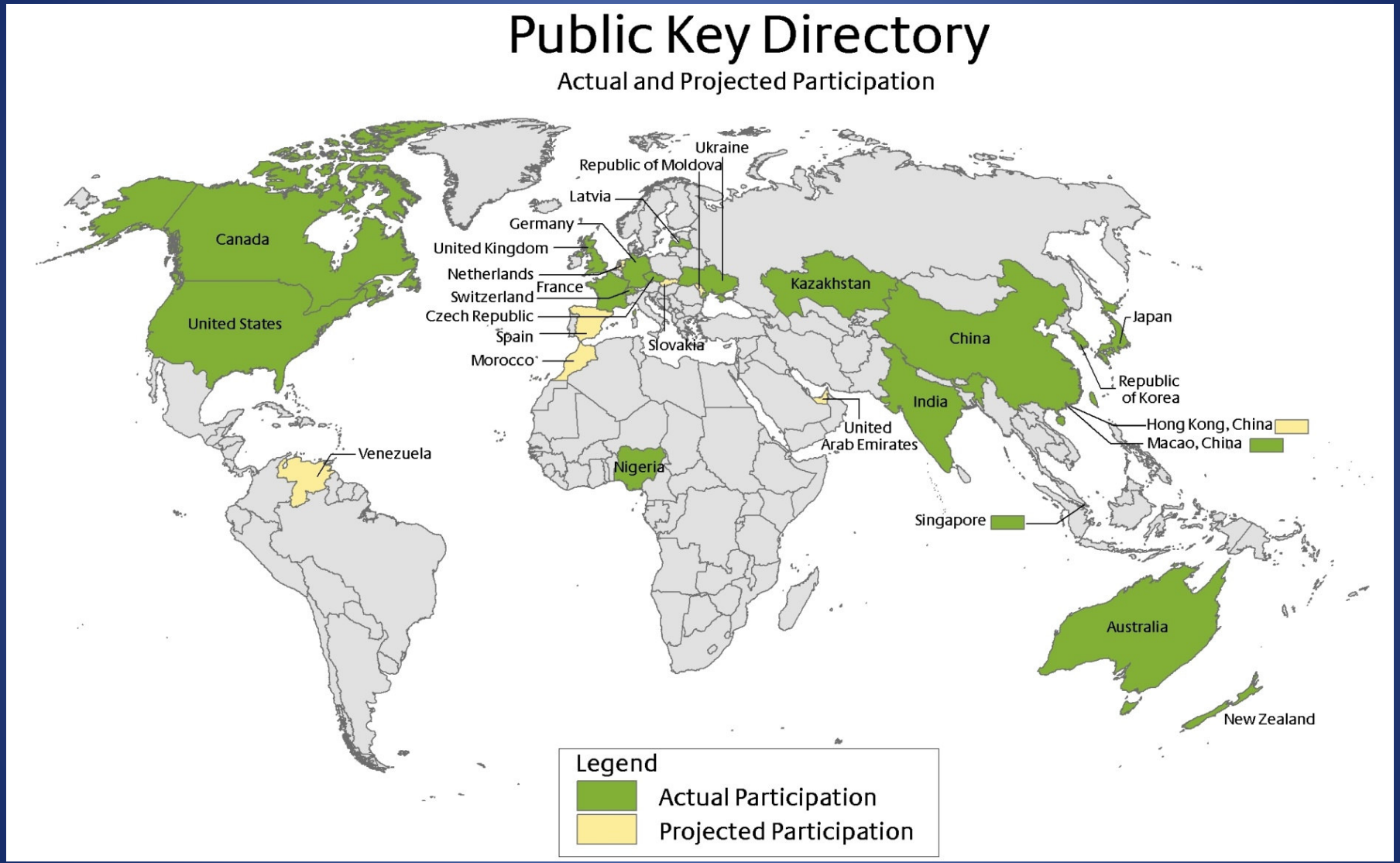


genuine

2nd / 3rd Line Inspection

- data page manipulation traces
- data page illegal personalisation
- genuine chip deactivated
- new chip mounted at back cover
- new chip personalized like data page
- Document Signer Certificate does not fit a valid CSCA Certificate

PKD Participants 2010

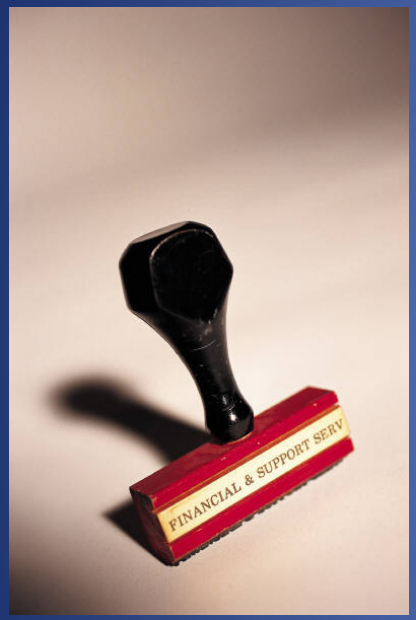


PKD Access

Access for everybody

- manual download of PKD contents free of charge
- Border Control Authorities / Travel Industry / …

PKD Fees (1)



1x Registration Fee

- one time fee to prepare activity in the PKD (all PKD Participants)
- ICAO Council decision: 56,000 US$ covers:
  - technical integration of a new PKD Participant
  - depreciation of ICAO Headquarter PKD assets
  - ICAO administrative registration costs

due after Notice of Participation

- to be paid in full (no pro rata arrangement)

PKD Fees (2)

recurring Annual Fee

1st: covers ICAO costs (all PKD Participants)

- administrative support from ICAO Secretariat
- e.g. 2011: 308,700 US$ - shared burden (around 16,250 US$ each at 19 PKD Participants)

2nd: covers Netrust costs (active PKD Participants)

- full year 43,000 US$ (after 15 month)
- contract: reduced fee with 30+ PKD Participants

small in comparison to ePassport costs

- technical setup and enrolment costs Millions

PKD Board

- oversight and supervision of the PKD
- 15 PKD Board Members appointed
- Member rotation among all PKD Participants possible
- active work / 2 - 3 meetings per year
- 2010 Chair: Germany

Observers

- possibility to observe on invitation

Thank You for Your Attention. Questions?

David Philp

Chair of the ICAO Implementation and Capacity Building Working Group (ICBWG)
Manager, New Zealand Passports
david.philp.@dia.govt.nz