Federal Ministry
of the Interior

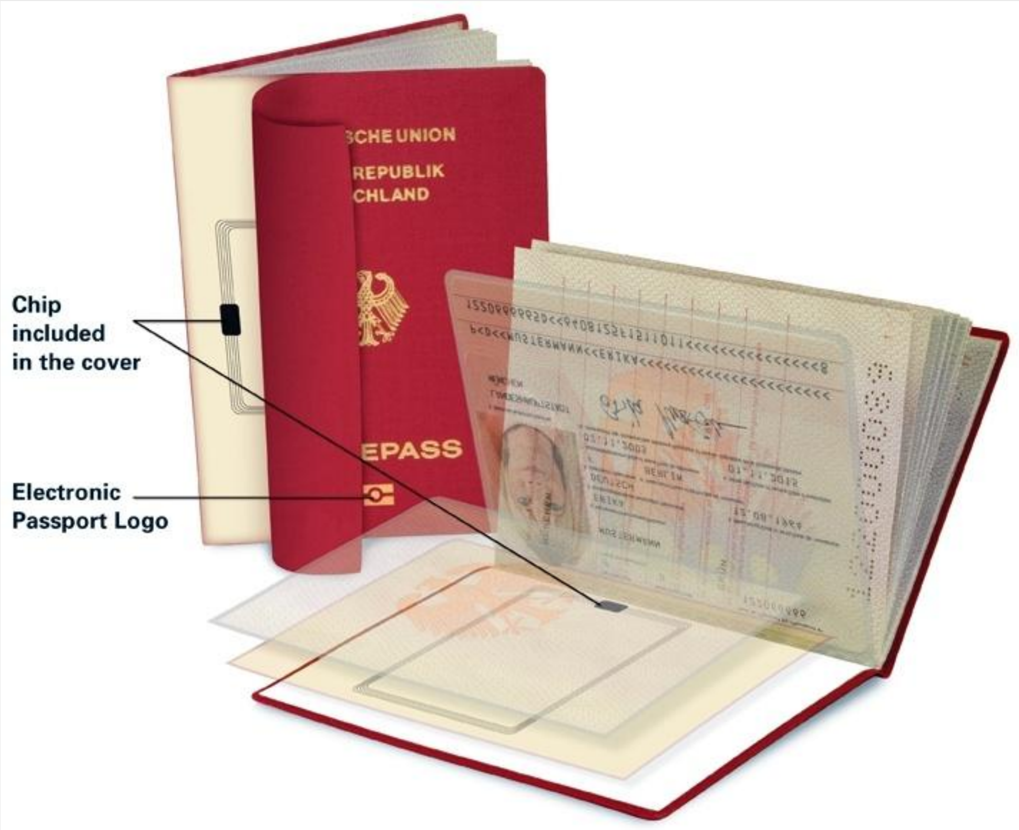
Recent Developments of the

ICAO Public Key Directory (PKD)

Dr. Eckart Brauer

ICAO Technical Advisory Group on Machine Readable Travel Documents (TAG MRTD)
Nineteenth Meeting
Montréal, 7 – 9 December 2009

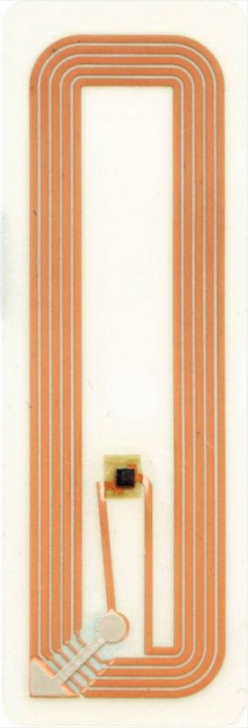
ePassport
Token for World Wide Travel



Chip:

- Given Name
- Last Name
- Date of Birth
- Photograph
- Fingerprints
- …
- Signature

ePassport
Chip Data Signature Check



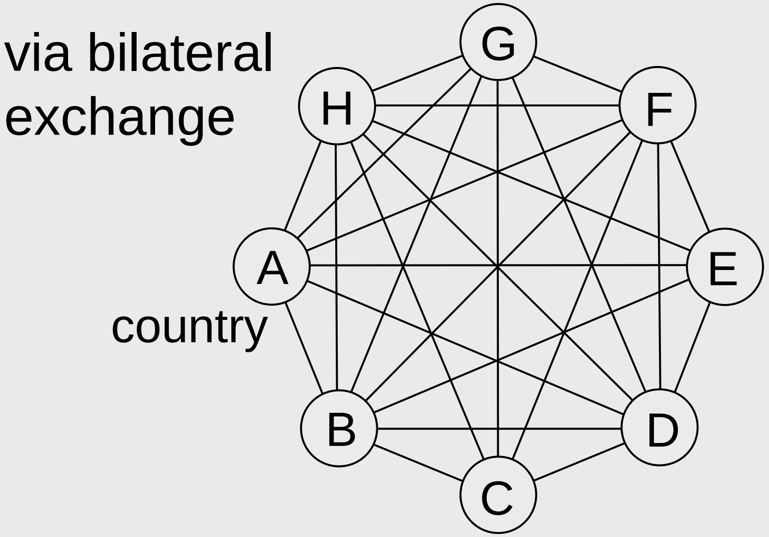
- **Security Chain**
  - Document Signer Certificate (DSC) / Certificate Revocation Lists (CRL) / CSCA Certificate
  - check signature: chip not compromised / chip and ePassport belong together
- **Valid Signature**
  - check before ANY subsequent use of ePassport
  - enables biometric comparison life vs. chip
  - enables …

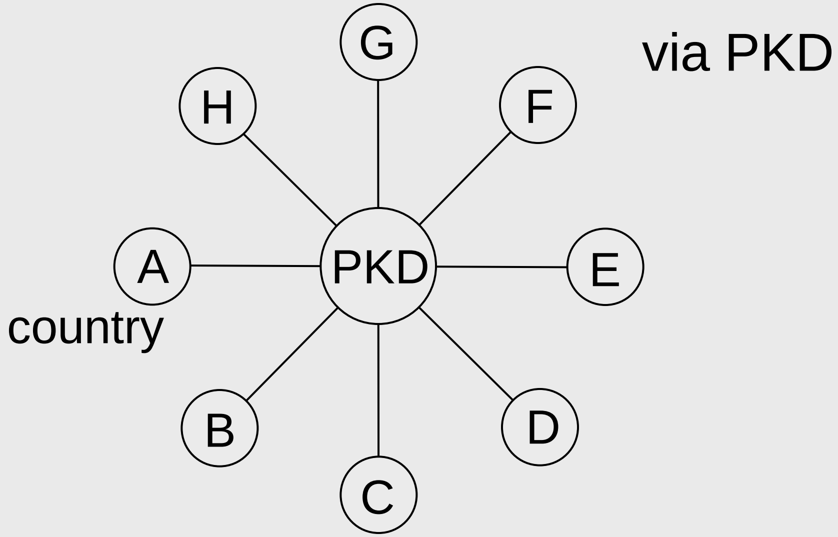
ICAO Public Key Directory (PKD) Basic Idea

- **Facilitate Distribution**
  - Document Signer Certificates (DSC) / Certificate Revocation Lists (CRL) / CSCA Link Certificates (LC) / CSCA Master Lists (ML)
- **World Wide Solution**
  - global travel is reality
  - the PKD is operational
- **Participation**
  - PKD Participants enjoy full service and upload possibilities

ICAO Public Key Directory (PKD) to put it in a nutshell …

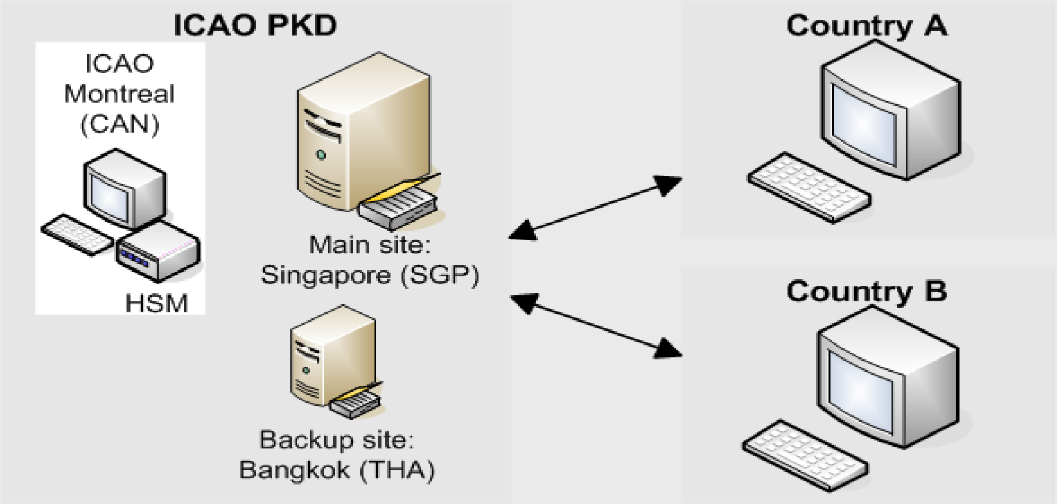
Distribution of Certificates and CRLs





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.

ICAO Public Key Directory (PKD) Operation



- **High Availability**
  - 24 / 7 Service + Backup
- **High Security**
  - HSM for CSCA Certificates
  - pre-validated PKD contents
  - Secure free download

main: **https://pkddownloadsg.icao.int/**

backup: **https://pkddownloadth.icao.int/**

NETRUST
YOU CAN BE SURE

ICAO Public Key Directory (PKD)
Recent Developments – MoU (1)

- **Memorandum of Understanding**
  - Master Lists (ML)
    - signed lists of CSCA Certificates (self-signed root cert.)
    - public ML: CSCA Certificates from PKD Participants
    - PKD internal ML: complete list of CSCA Certificates
  - CSCA Link Certificates (LC)
    - links CSCA Certificate with successor CSCA Certificate
    - facilitates import of new CSCA Certificates after first secure import at ICAO
  - ML and LC are essential facilitation enablers

ICAO Public Key Directory (PKD)
Recent Developments – MoU (2)

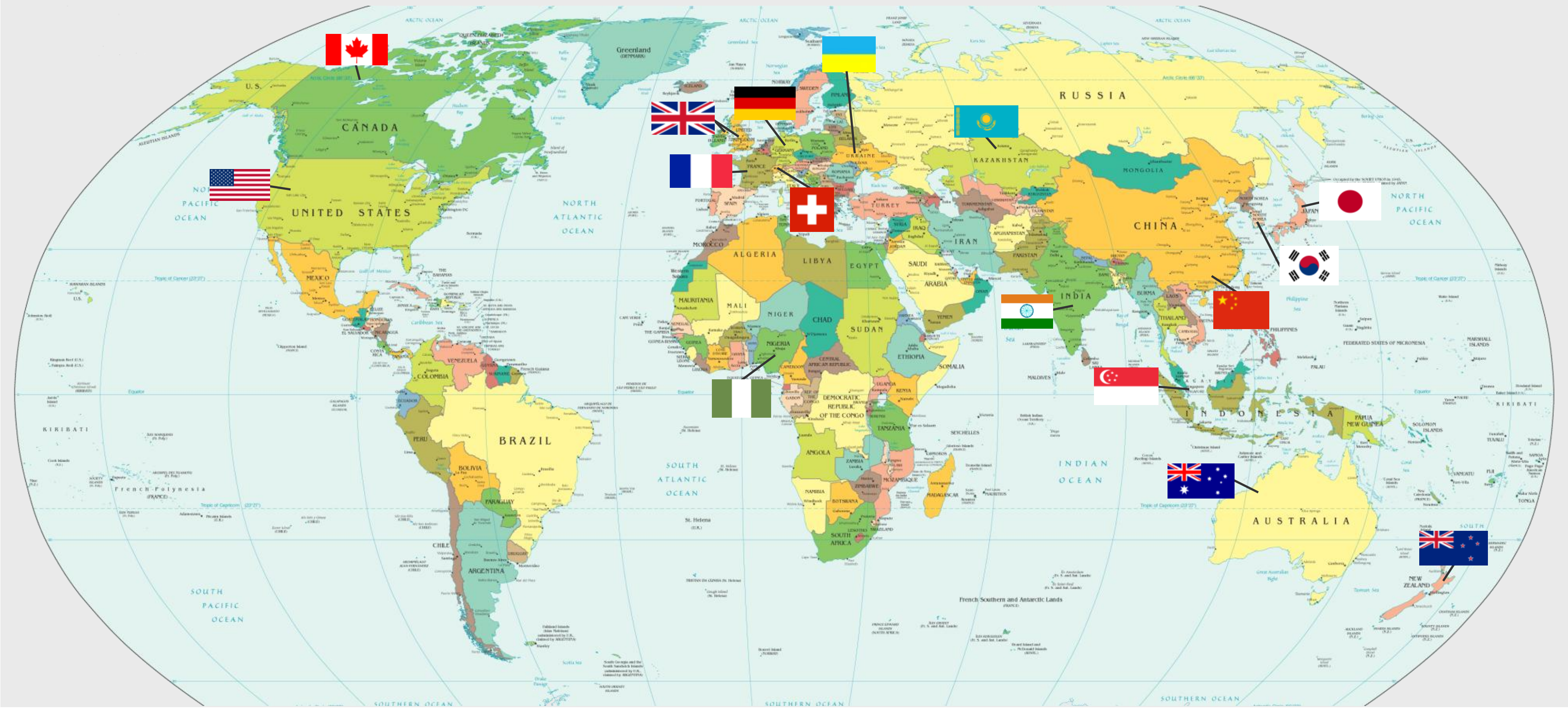
- **Memorandum of Understanding**
  - Fee Structure
    - Registration Fee: reduced to 56,000 US $
    - Annual Fee (ICAO): shared burden for PKD Participants
    - User Fees possible for qualified PKD access
  - Flexibility
    - PKD Board may set effective dates for MoU changes
  - Participation of non-State Entities
    - no rights or privileges under Chicago Convention

ICAO Public Key Directory (PKD)
Recent Developments - Contract

- **Operational Contract ICAO – PKD Operator**
  - valid 2009 – 2011 (main + backup site; ICAO site)
  - basic principles
    - PKD Participants active after 15 months
    - Annual Fee (Operator): flat fee for PKD activity
    - reduction of fees with 30+ PKD Participants
  - test bench for check of PKD / eMRTD applications
    - qualified PKD Operator support (one-time 9,600 US $)
    - independent from ICAO or PKD Participants

NETRUST
YOU CAN BE SURE

ICAO Public Key Directory (PKD)
Recent Developments - Participation



ICAO Public Key Directory (PKD)
Recent Developments - EU / Schengen

- **Common Approach**
  - all EU / Schengen States issue ePassports
  - signature check is precondition for ePassport use
  - distribution of certificates and revocation lists world wide
  - participation in the PKD proposed for 2010
- **Support**
  - European Borders Fund
  - Frontex

FRONTEX
LIBERTAS SECURITAS JUSTITIA

ICAO Public Key Directory (PKD)
Recent Developments - PKD Board

- **PKD Board**
  - 15 Members + other PKD Participant representatives
  - principle of rotation and equitable geographic distribution applied
  - 2009 chair: Germany

- **Work**
  - full administrative regime
  - all PKD Participants fully involved

Thank you very much for your attention!
Questions please

Dr. Eckart Brauer

2009 Chairman of the PKD Board

eckart.brauer@bmi.bund.de