



International Civil Aviation Organization

Sixth Symposium and Exhibition
on ICAO MRTDs, Biometrics
and Security Standards

ICAO Headquarters, Montréal, Canada
1 - 4 November 2010



Participation in the ICAO Public Key Directory (PKD) - Policy and Administrative Framework -

Dr. Eckart Brauer

PKD Board Chairman

Senior Officer

Federal Ministry of the Interior - Germany



ePassport at Borders (1)

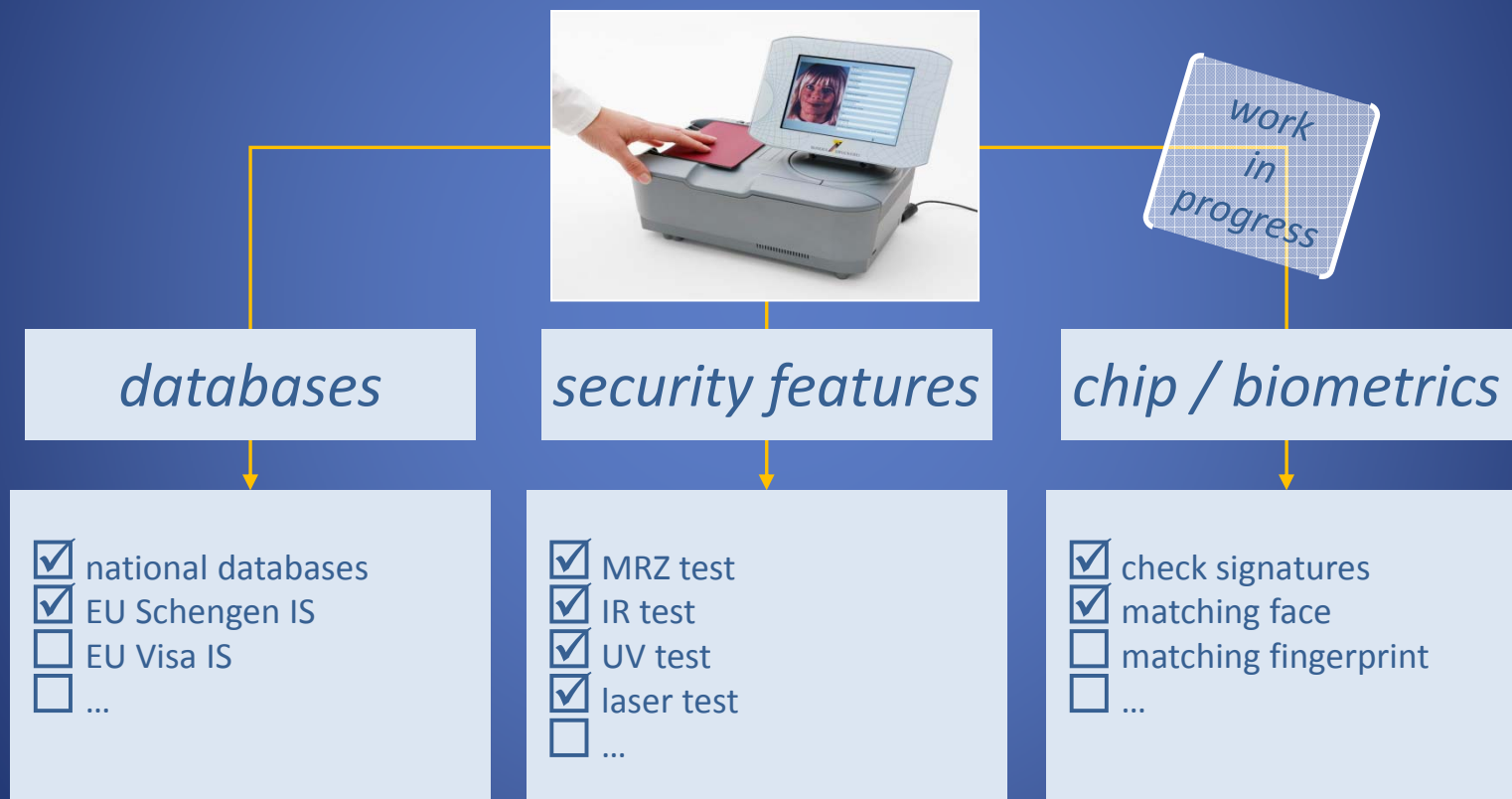


Frankfurt/M. Airport 2008

- about 30 Mio. non-Schengen passengers
- about 23 Mio. passengers checked
- March 2009, 1 lane
- all Passports: 9.980 (100%)
- ePassports: 1.305 (13%)
- numbers are growing



ePassport at Borders (2)







ePassport – Counterfeits (1)

United Kingdom of Great Britain and Northern Ireland - Dokumententyp: P

Datei Einstellungen Sprachen Hilfe



Einzelergebnisse		MLZ	
✓ B-900-Test (IR)		Name	KAPAJ
✓ MLZ-Test		Vornamen	KRESHNIK
✓ Wertpapier-Test		Nationalität	GBR
☐ Laser-Test		Geburtsdatum	02.01.1982
✓ Muster-Test		Geschlecht	männlich
		Gültig bis	08.09.2018
		Dokumenten-Nr.	761258971
		Dokumententyp	P
		Ausstell. Staat	GBR
		Zusatz 1	


Prüfung OK

Status: user_L0
Prüfung OK

Start Posteingang - Microsoft ... BSI ePass C

BSI ePass Client

MRZ-Eingabe... Erneut lesen Details... MRZ-Vergleich... Systemtest



DE 13:39

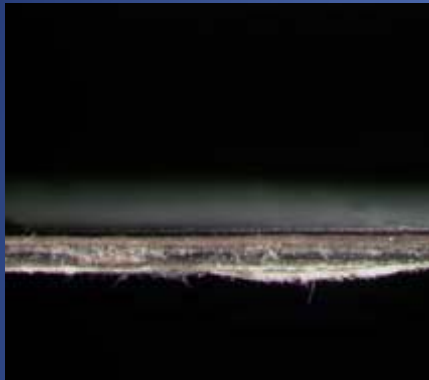
Example 2010

- 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





ePassport – Counterfeits (3)

Attacker **know-how** ...

- personalize data page
- calculate MRZ incl. check digits
- deactivate genuine chip
- glue in fake chip
- personalize fake chip
- understand BAC

The Attacker did not know ...

- Germany: active PKD Participant
- full signature chain check with PKD immediately reveals fake



ePassport – Counterfeits (4)



Attackers know-how will get better

You should be prepared



Security Chain

Document Signer Certificate (ICAO mandatory)
authorized producer / issuer; contents unchanged

Certificate Revocation List

valid certificates in use (related: expired certificates)

CSCA Certificate Master List

list of certificates in use; reduction of diplomatic exchange possible

CSCA Link Certificate

diplomatic first exchange follow-up; impossible to fake



Business Case

exchange ?



home

Role of Signature Check

- precondition for use of biometrics

Role ePassport

- secured identity with biometrics
- document and person firmly linked together

Certificate Distribution

- world wide travel
- national / regional exchange ?

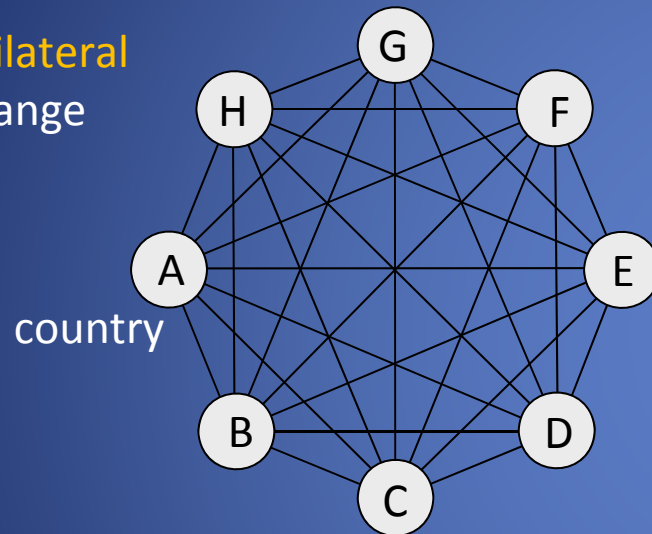
World Wide Solution !

- ICAO Public Key Directory (**PKD**)

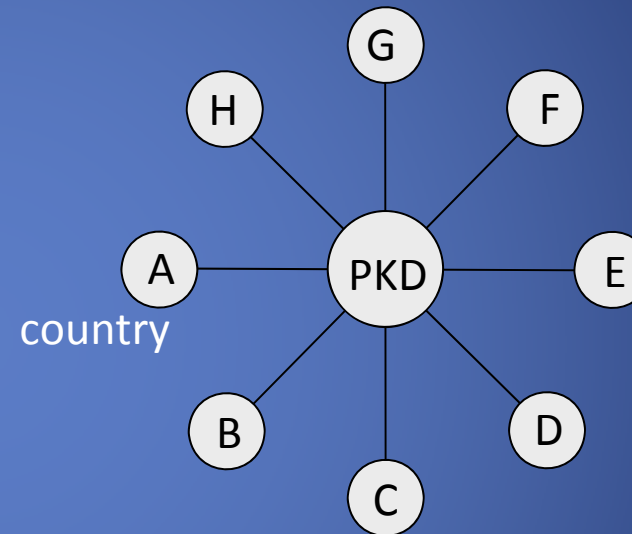


Exchange Model

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.



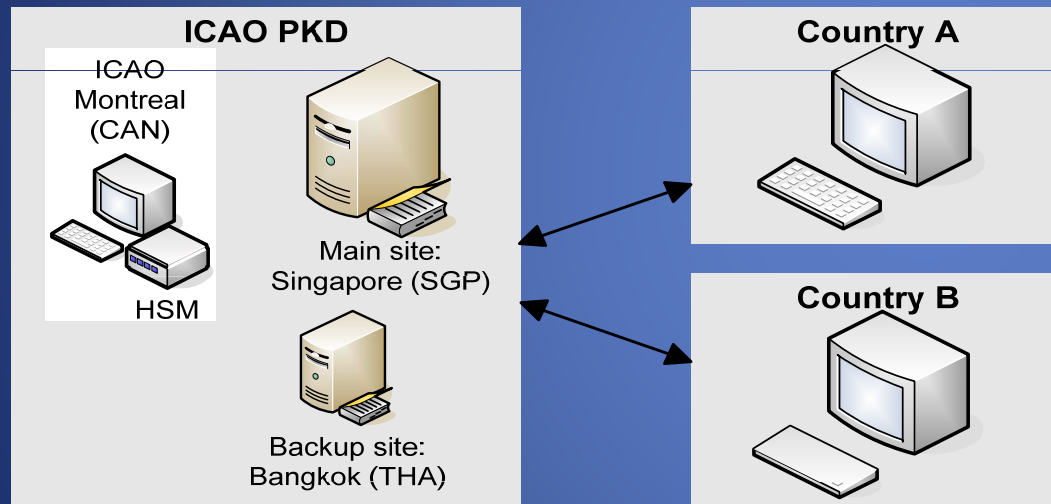
PKD Infrastructure

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/>

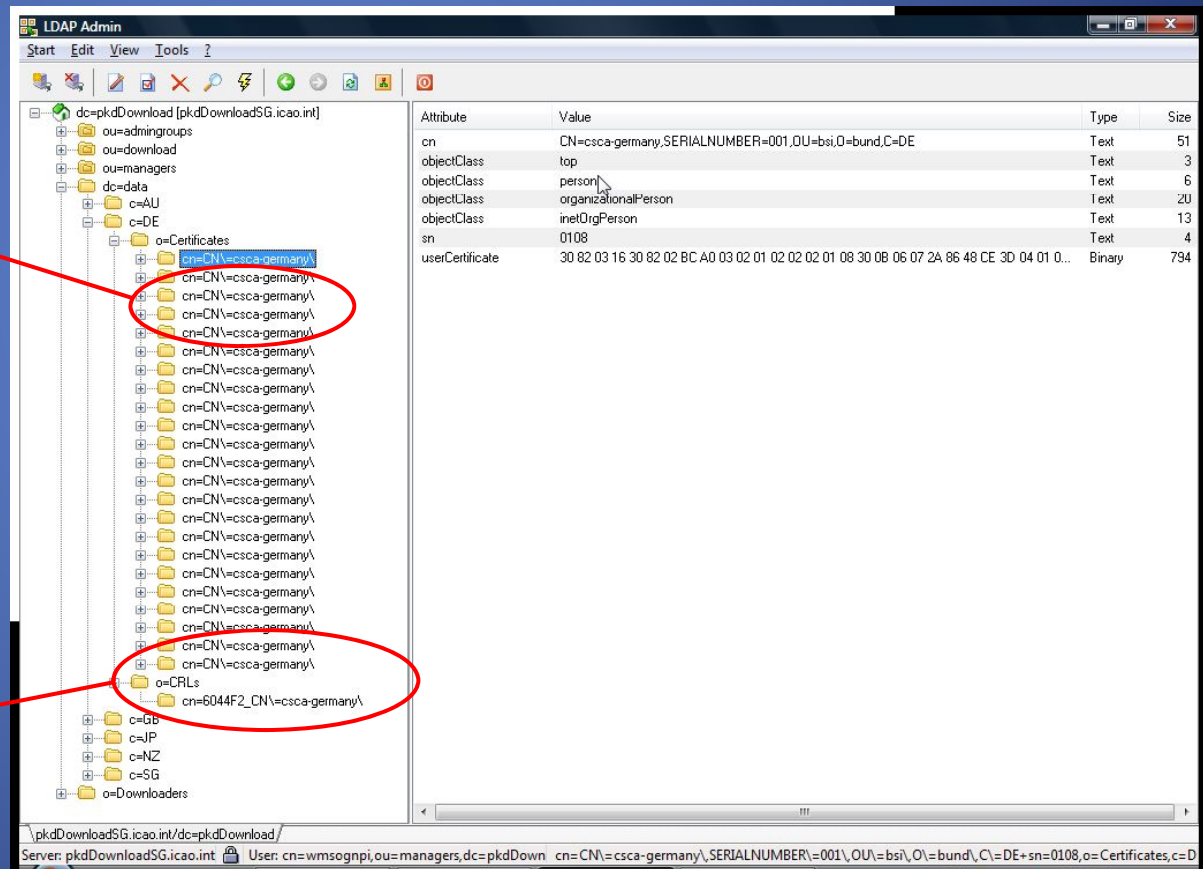


PKD Contents

- complete **security chain**
- pre-validated contents

DSC

CRL



Attribute	Value	Type	Size
cn	CN=ecscs-germany.SERIALNUMBER=001,OU=bsi,O=bund,C=DE	Text	51
objectClass	top	Text	3
objectClass	person	Text	6
objectClass	organizationalPerson	Text	20
objectClass	inetOrgPerson	Text	13
sn	0108	Text	4
userCertificate	30 82 03 16 30 82 02 BC A0 03 02 01 02 02 02 01 08 30 0B 06 07 2A 86 48 CE 3D 04 01 0...	Binary	794



PKD Access

Access for **everybody**

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



Access for eMRTD **Vendors**

- test bench for check of PKD / eMRTD applications and qualified PKD Operator support offered
- one-time charge is 9,600 US\$
- see PKD Fee Schedule 2010



Start of PKD Participation

Preparation

- ask PKD Participants and ICAO for support
- PKD part of ePassport implementation

Notice of Participation

- fill in PKD MoU Attachment A and send it to ICAO

Registration Fee

- one time fee to prepare participation

Annual Fee

- recurring fee to cover running costs

(<http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx>)



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 14,700 US\$ each at 21 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

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



PKD Added Value

Consider

- 
- complete check of certificate chain enabled by only one world wide infrastructure
 - 1st hand up-to-date information / meet the right people
 - government surveillance / well defined procedures / standard technology
 - ePassport automated border control with no security compromise (full signature check !)

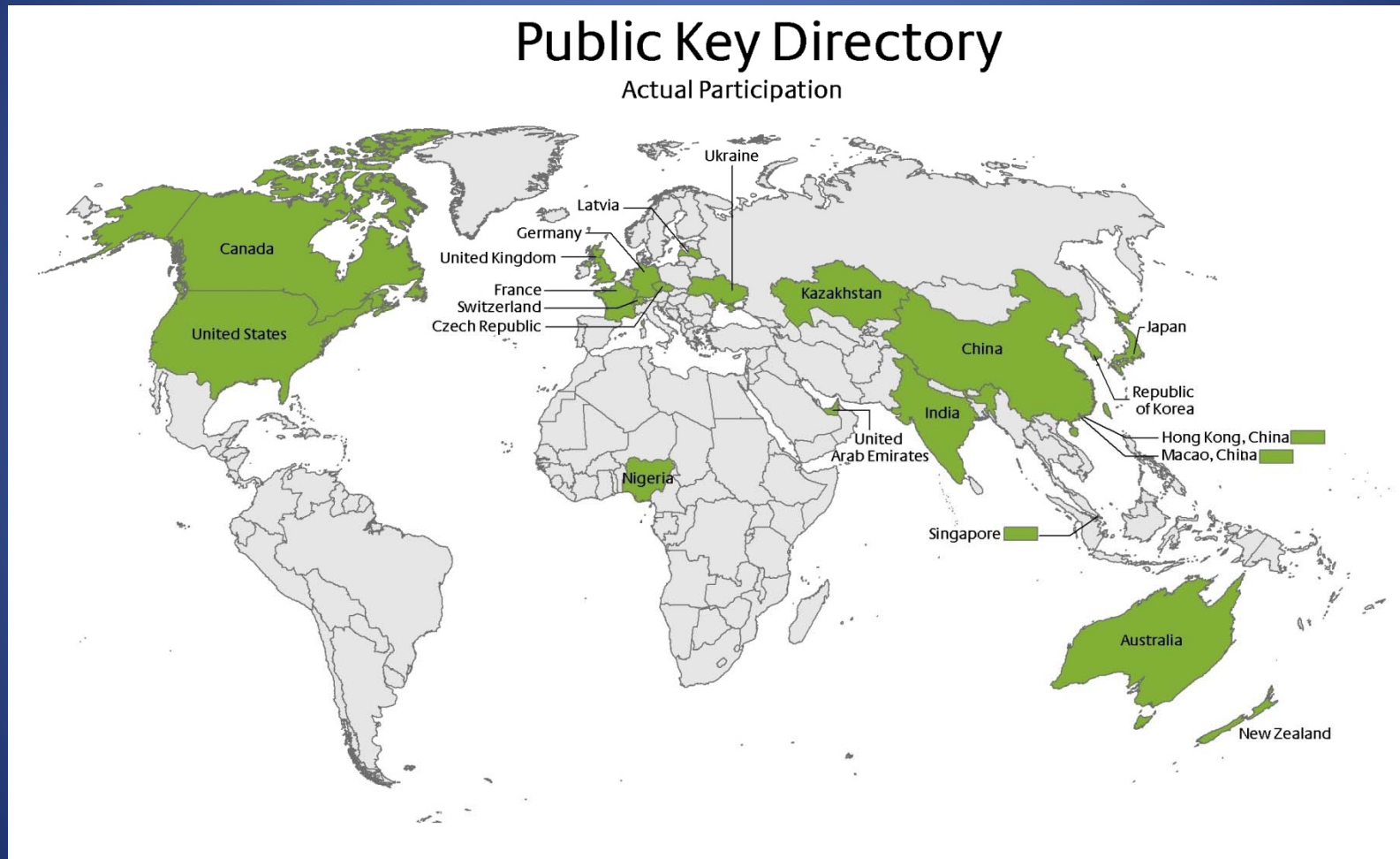
Result

- PKD becomes a **tangible** added value



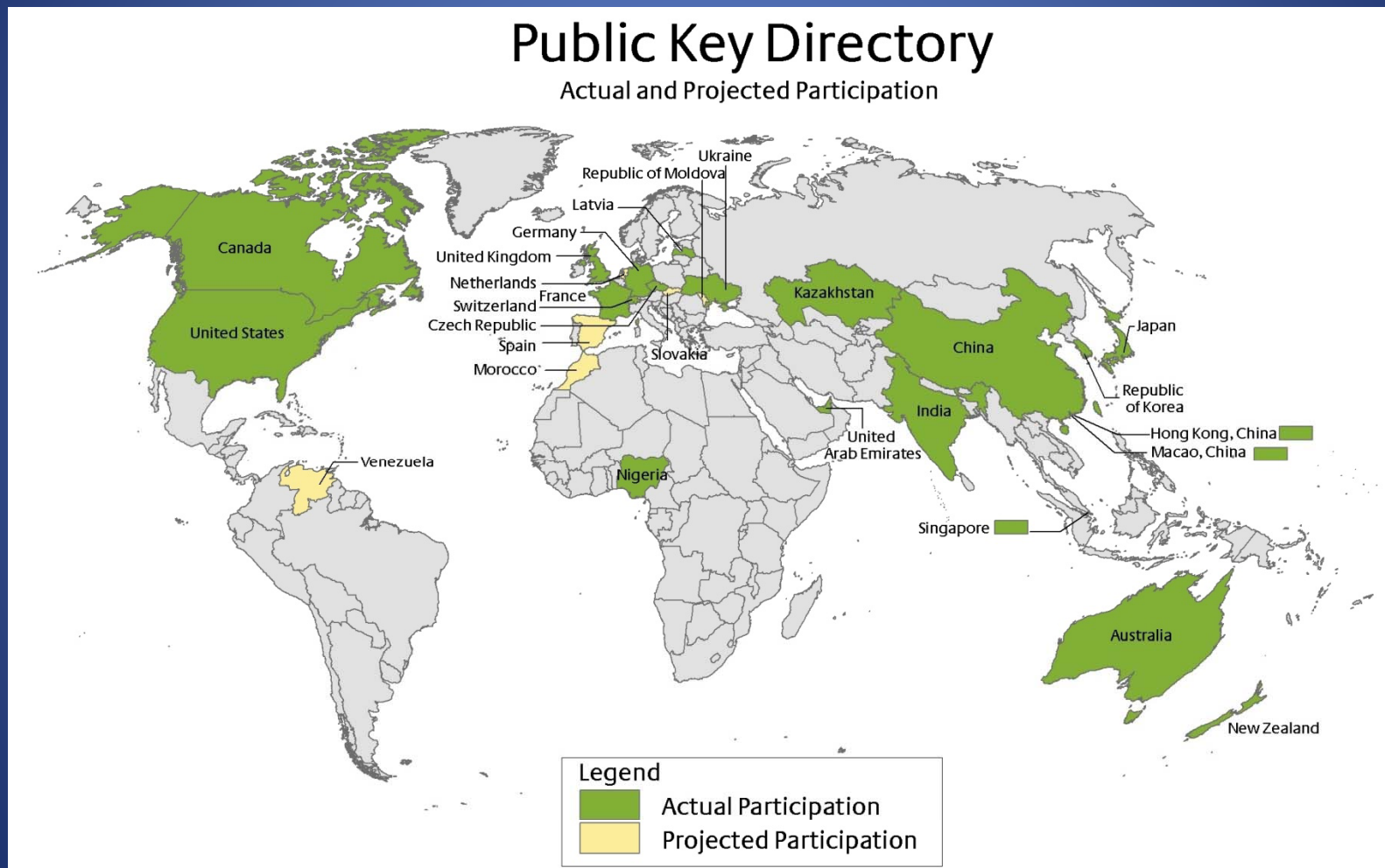


PKD Participants 2010 (1)

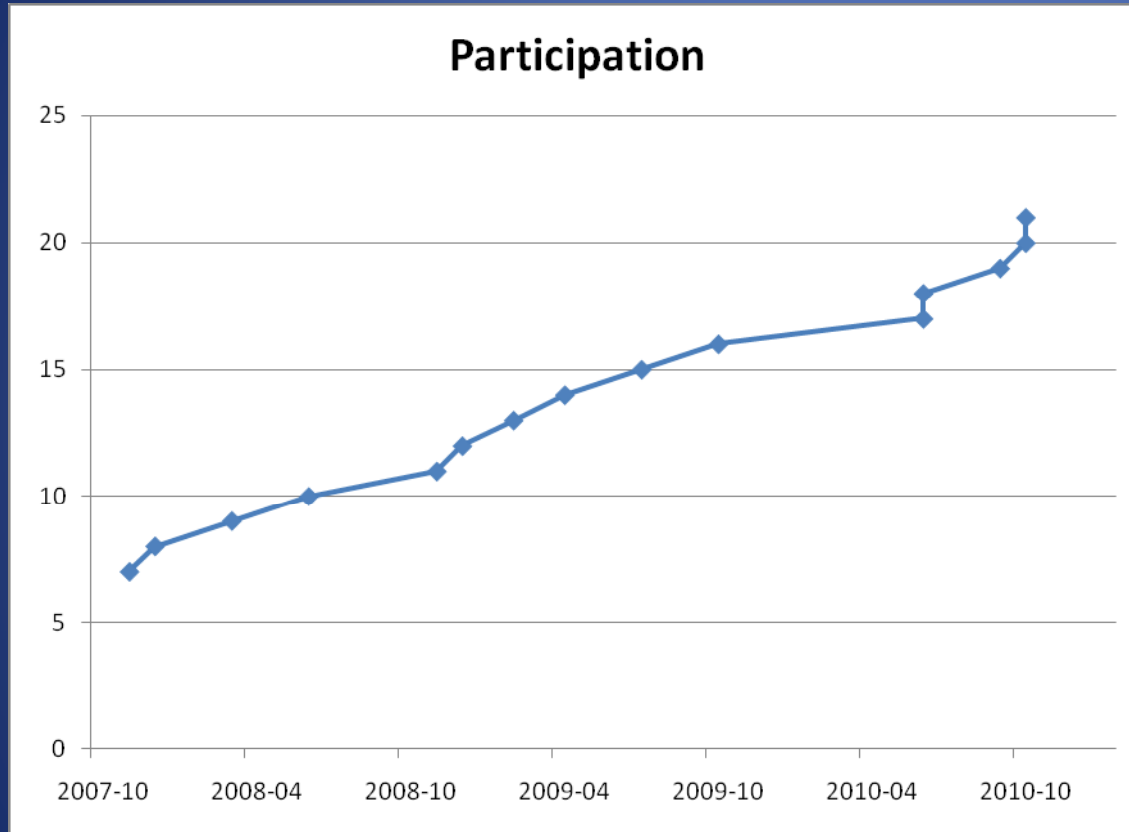




PKD Participants 2010 (2)



PKD Participation Growth



Sixth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards, 1 to 4 November 2010, Montréal





Thank You for Your Attention. Questions Please.

Dr. Eckart Brauer

PKD Board Chairman

Senior Officer

Federal Ministry of the Interior - Germany

