Mario Wiesen / Ciaran Carolan

Chair of the ICAO PKD Board / ICAO PKD Officer

TRIP2022

ICAO

The ICAO PKD
In a nutshell

Electronic Verification of eMRTDs assures:
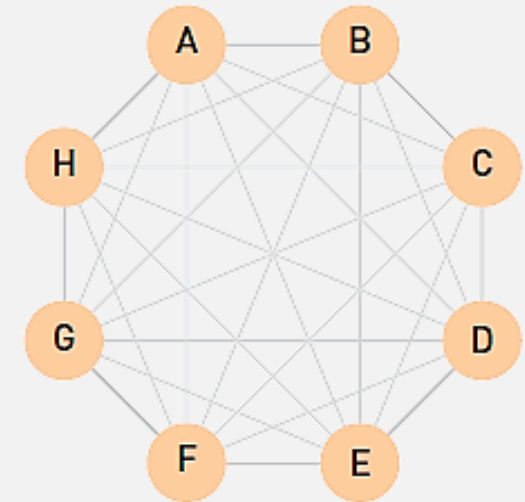
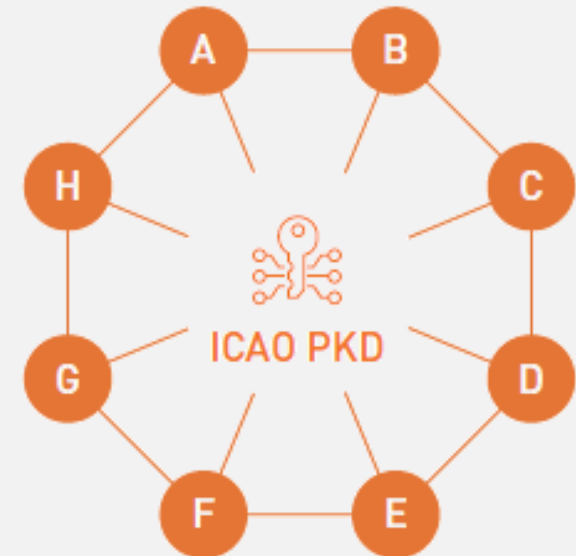## Authenticity

- Issuance by genuine authority

Integrity

- Data hasn't been changed since issuance (including the facial image)

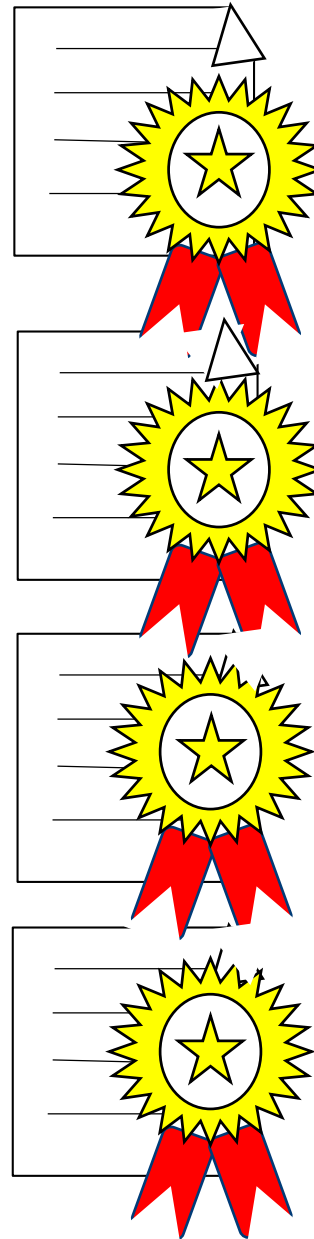**Electronic Verification needs availability of public keys**

Without the PKD

With the PKD

Public key Information in the ICAO PKD

Everything needed to validate the full ePassport certificate chain

= > A One-Stop Shop for ePassport Validation

TRIP2022

ICAO

☑ **CSCA certificates** — **Encoded in the ICAO Master List (ML) and national Master Lists**

☑ **DS certificates**

☑ **CRLs**

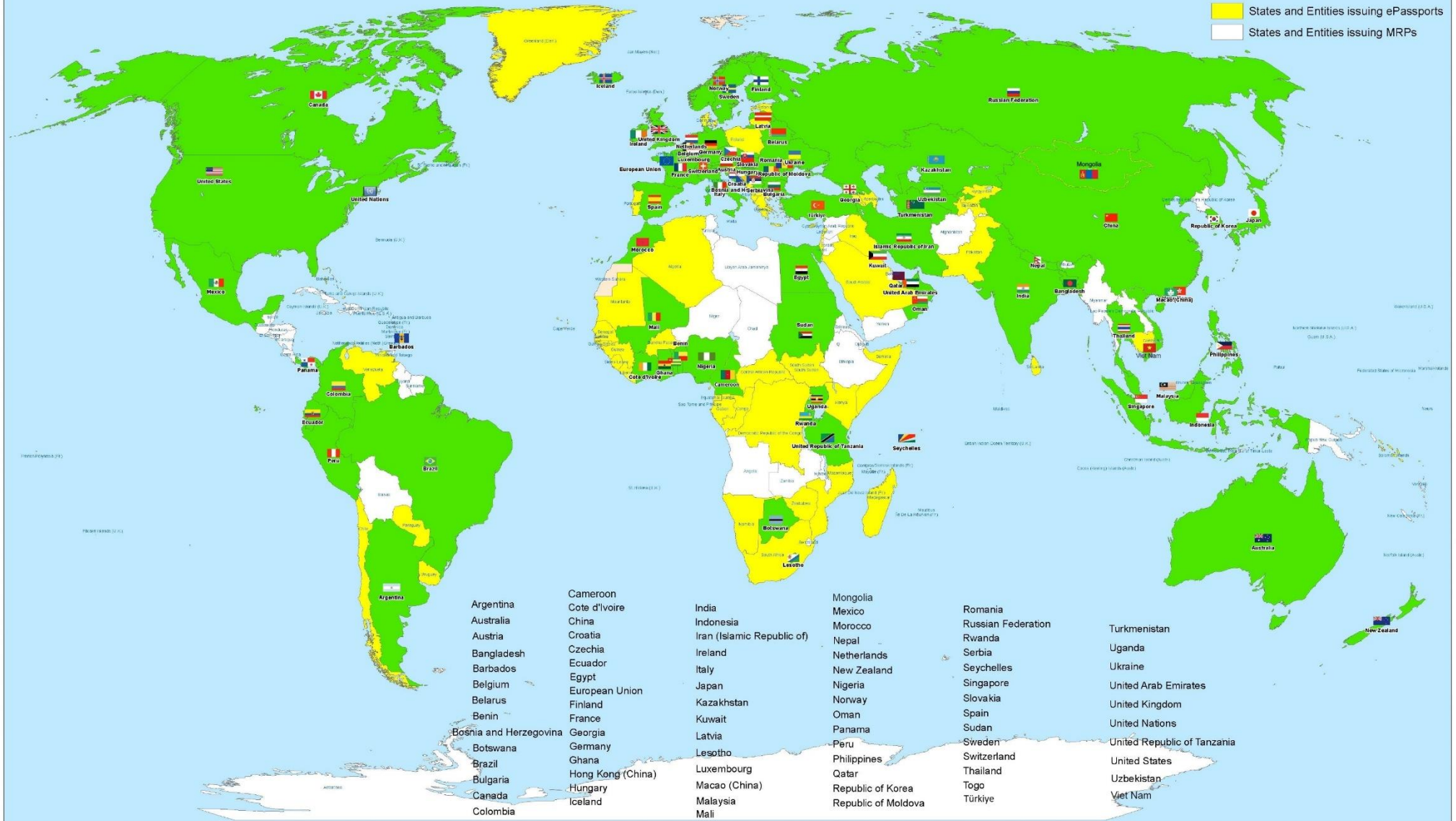☑ **DLs**

Included in the main PKD repository

Voluntary participation in the ICAO PKD

83 PKD Participants and ePassports issuing States and Entities

Legend
- PKD Participants
- States and Entities issuing ePassports
- States and Entities issuing MRPs

Advancing the PKD to meet current and future needs

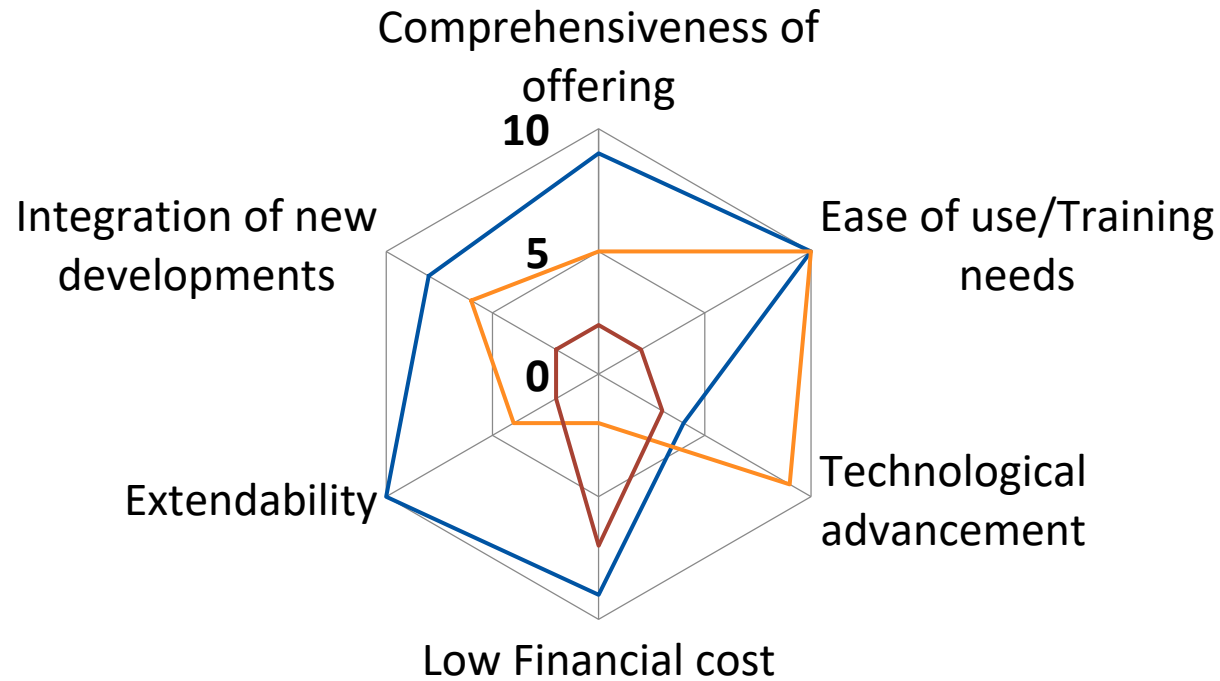## PKD Board priorities

Value for participants

Costs for participants

The ICAO PKD – complete, flexible, low cost and easy to use

—**ICAO PKD**   —**Bilateral ID schemes**   —**Manual Passport checks**

Value

- Increase participation and use
- Intensify capacity building
- Include additional eMRTD certificates
- Build new partnerships
- Enhance flexibility to new developments

Costs

- Increase number of participants
- Retain technological simplicity

ICAO   TRIP2022

The ICAO PKD Data Quality Coach initiative

⬆ Value

Virtual calls to provide concrete support

On-site visit to assess implementation and provide advice

Follow-up support based on established relationships

The ICAO PKD Data Quality Coach initiative

2021-22- *Mongolia is the first recipient of the PKD DQ coaching program, supported by experts from Luxembourg*

2022 – *Further countries standing to benefit, beginning with Barbados, Cameroon and Uganda*

The program is open to all PKD participants, new and old, with selection of recipients based on submitted requests for support and geographic prioritization of the PKD Board year-to-year.

TRIP2022

ICAO

ICAO PKD Workshop

Availing of all benefits of ICAO PKD participation: Considerations from operational and implementation points of view

Speke Resort Munyonyo, Kampala, Uganda

15 November 2022

- For existing PKD participants and representatives of States interested in possible future participation (separate tracks offered)

- Dedicated sessions for decision makers, operational staff and technical senior officers

- Objectives include:

  o Enhancing understanding and awareness of ePassport PKI and the relevance of the PKD

  o Supporting national implementations are optimal and ensure that all benefits are realized

  o Facilitating exchange of information and perspectives

The ICAO PKD Private Sector Use Pilot

Value
Cost

Grow participation amongst all who can benefit from the PKD in line with ICAO objectives	• Development of solutions by the private sector based on PKD data can enhance global capabilities to properly authenticate electronic travel documents • Airlines/airports are asked to verify documents – we need to give them capabilities to do so!
Ensure that the PKD can support future development of globally interoperable solutions	• Standalone solutions from industry could help States more rapidly incorporate capabilities for authenticating new electronic documents (e.g. VDS-NC) • Private sector usage can motivate improved usage of the PKD by States

TRIP2022

ICAO

Main principles

- Six month pilot period with collection of information and perspectives towards the end to direct next steps
- Usage of the existing public download capabilities to eliminate any need for capability development
- Authorization given based on derogation from defined Terms and Conditions on the PKD public download site
- Administration by the Secretariat, oversight by the PKD Board through Secretariat reporting
- Full alignment with the MoU approved by Council

TRIP2022

ICAO

Status of the pilot

15 Companies enrolled, more candidates expressing interest

May 2021 First Participant survey

23 Dec 2021 Pilot kick-off

31 March 2023 Pilot end date

TRIP2022

ICAO

ICAO TRIP Program

Raising awareness of new initiatives

ICAO PKD Program

Facilitating implementation of new initiatives

TRIP2022
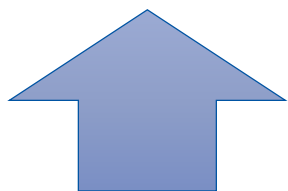
ICAO

State Experts
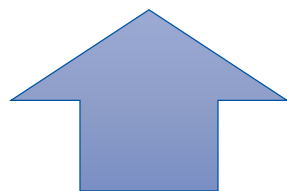
ICAO Secretariat
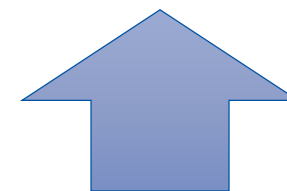
ISO Experts

*Supporting validation of ~~ePassports~~*

eMRTDs

The ICAO Health Master List

Supporting use of the ICAO VDS-NC

- Public Key Infrastructure approach generally follows that of ePassports

- Trust anchor can be an existing CSCA or a different CA used for health proof purposes

- Encoding of the barcode signer certificate in the barcode is optional

  - International distribution mechanism needed for sharing of the health-oriented CA certificates and (preferably) the barcode signer certificates
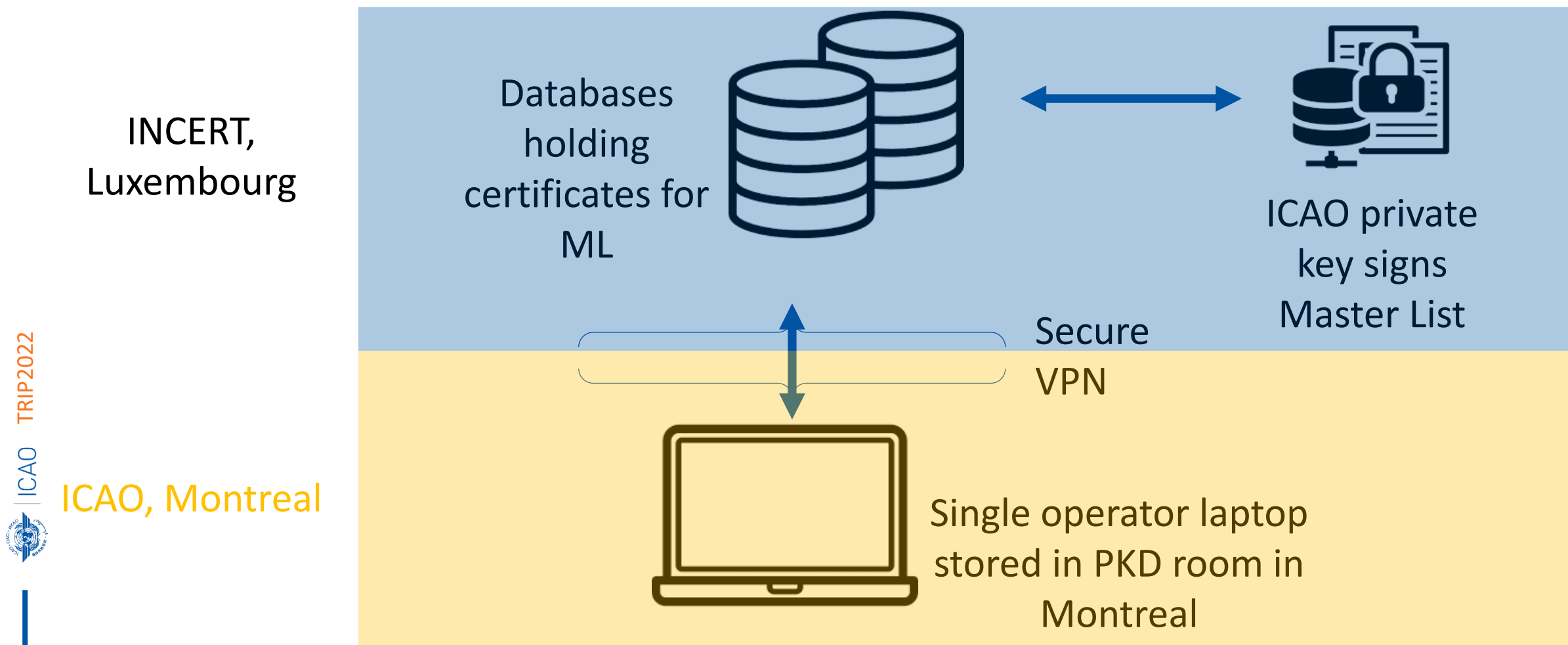
-> The ICAO Health Master List
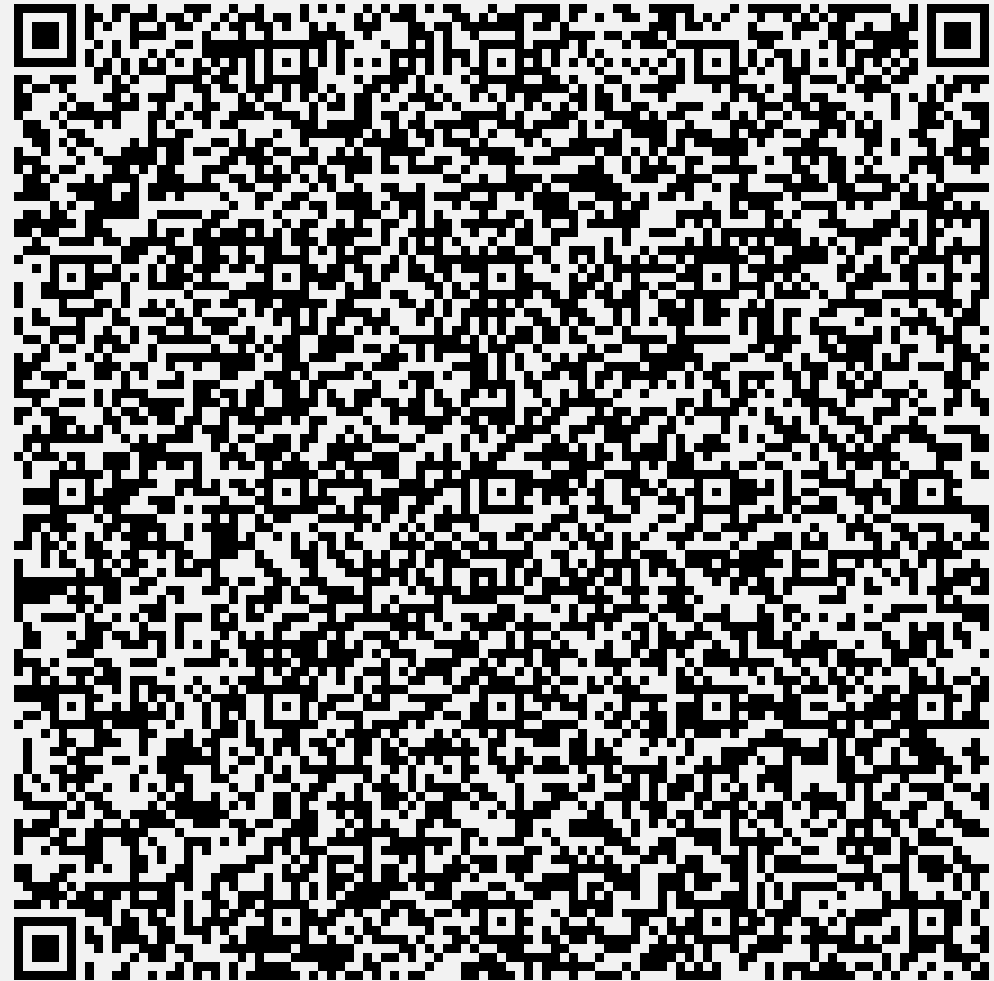
Global PKI in support of international health proofs for travel

The ICAO Health Master List

- All that is required to assure authenticity and integrity of VDS-NC
- Sharing trust anchors for international health proofs

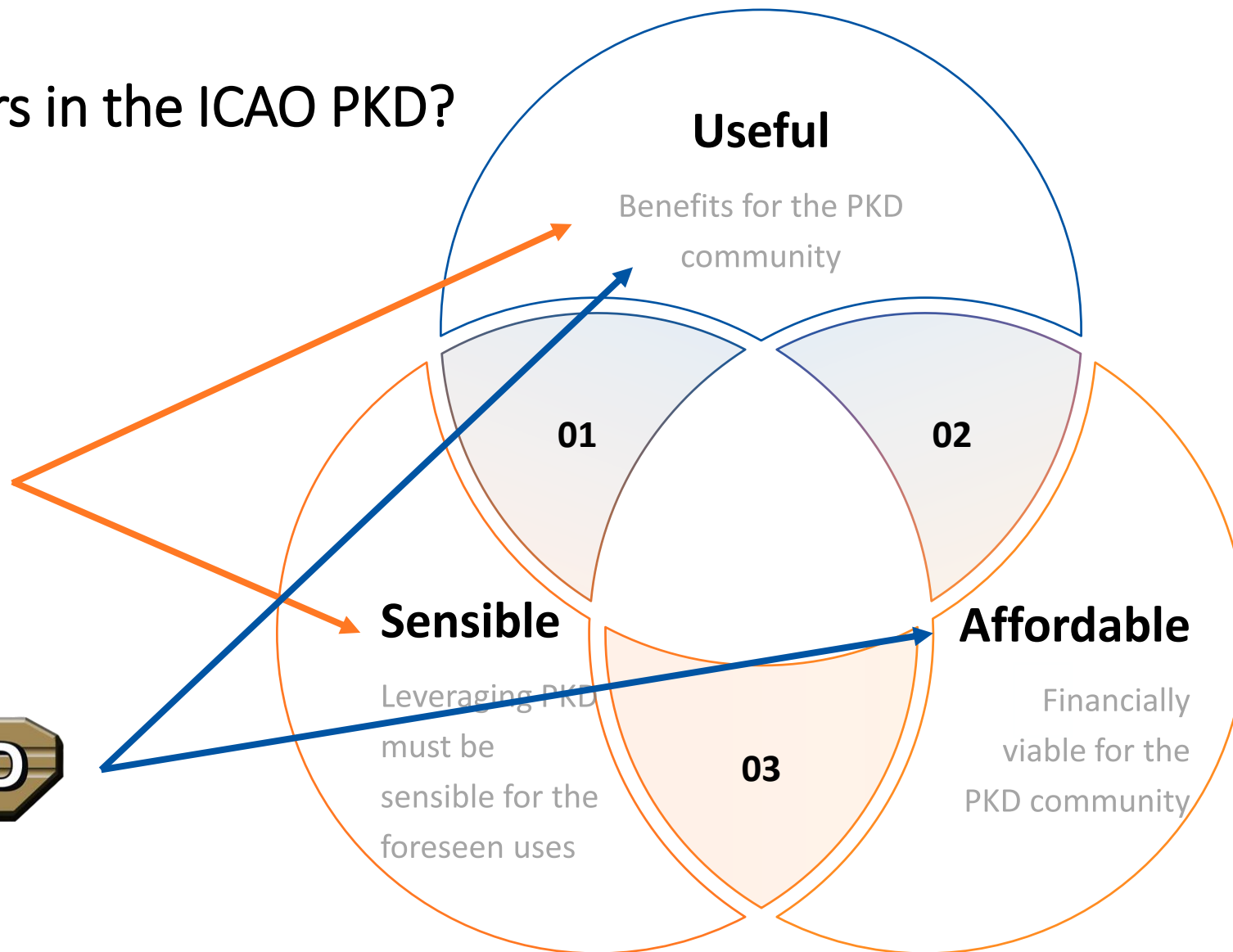# Collaboration with INCERT LU -> free of charge for ICAO and for participants

INCERT, Luxembourg

Databases holding certificates for ML

ICAO private key signs Master List

Secure VPN

TRIP2022

ICAO

ICAO, Montreal

Single operator laptop stored in PKD room in Montreal

Visible Digital Seals (VDS) for Non-Electronic Documents –Part 13, 9303, 8th Edition

TRIP2022

ICAO

VDS Barcode Signers in the ICAO PKD?
Discussion continues

Useful

Benefits for the PKD community

01

02

Sensible

Leveraging PKD must be sensible for the foreseen uses

03

Affordable

Financially viable for the PKD community

ICAO   TRIP2022

TRIP-PKD Cooperation is essential

- Vital that specification development goes hand-in-hand with PKD implementation planning to the greatest extent possible

- Common awareness of interrelations critical within WGs and governance structures

- Mutual interest in capacity building and implementation support implies cooperation in this area

ICAO

Implementation

Usefulness

Demand for supporting infrastructure