
ICAO
TRIP
2017
Passport
Passeport Pasaporte
护照 Паспорт جواز سفر
ICAO
ICAO

#icaoTRIP

ICAO PKD, N-PKD and Masterlist

Florian Holeczek
Responsible Service Manager of the ICAO PKD

ICAO TRIP: Making Air Travel more Secure and Efficient

TOWARD BETTER TRAVELLER IDENTIFICATION MANAGEMENT

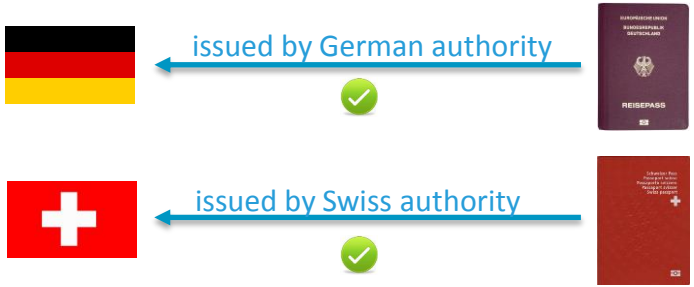
FOR ENHANCED BORDER CONTROL INTEGRITY

Topics

- ICAO PKD and N-PKD
  - Context and Big Picture
  - How does the PKD work?
  - PKD and N-PKD
- Further increasing eMRTD's conformity to Doc 9303
  - The PKD's conformance checks
  - Using the ICAO PKD Conformance Website
- Focus on Master Lists
  - What is a Master List?
  - Why to use a Master List?
  - How does the PKD make use of them?
  - How to use Master Lists as a State?
  - ICAO Master List

Context: Border Control with ePassports

Verification devices at border control use **certificates** in order to ensure **authenticity** and **integrity** of **ePassports**.

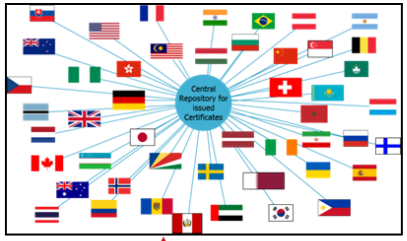


The prerequisite is a **trust anchor** (CSCA root certificate) **per each country**
and further ICAO PKI related objects

Problem: Bilateral Exchange of the Trust Anchors

Solution: ICAO PKD as the central exchange repository

Big Picture



ICAO PKD

Secure upload and download via TLS and certificate-based access

Check conformance of all uploaded objects against ICAO's Doc 9303 standard

Internet

National PKD

Production

Passport PKI

- CSCAs
- Document Signer Cert.
- CRLs

Consumption

Border Control System

- CSCAs
- Document Signer Cert.
- CRLs

ICAO PKD – What is it?

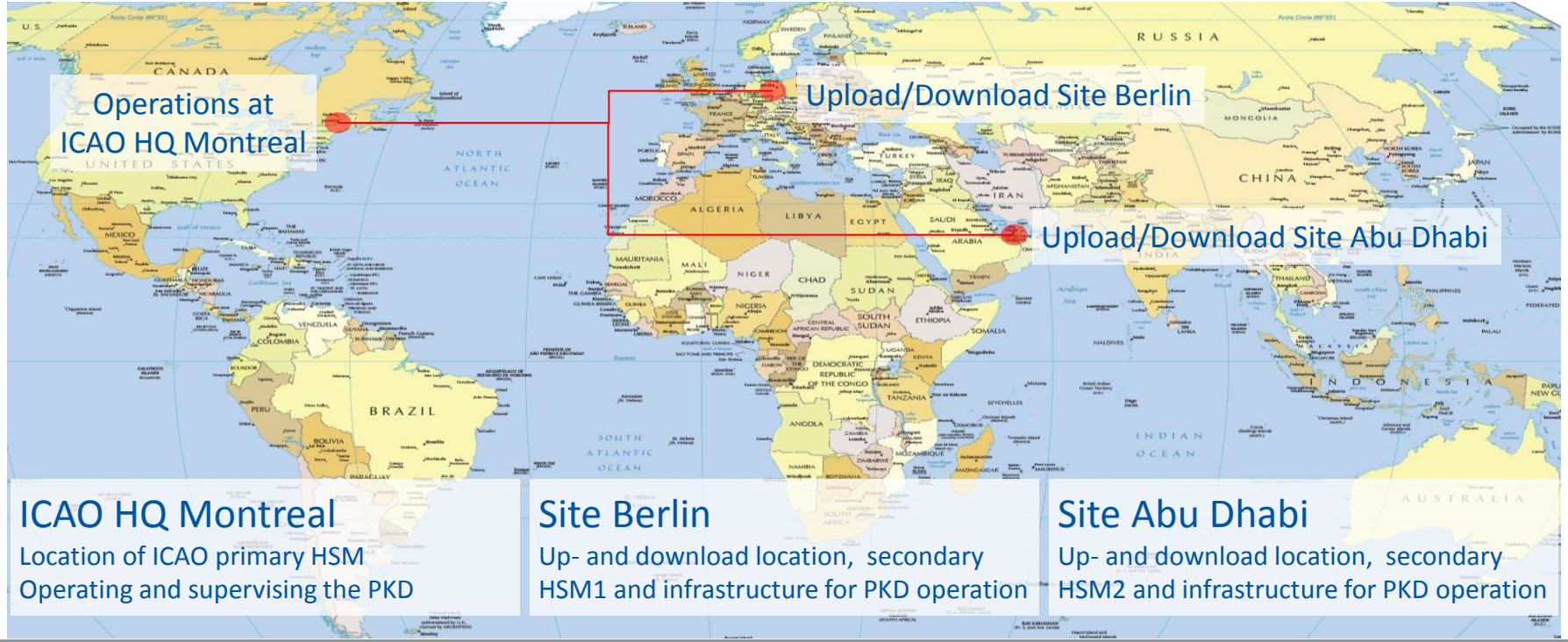
Primarily:

- **Exchange platform** for PKI objects needed for doing Passive Authentication
  - The more States are participating, the more useful it gets for every single participant!

But also:

- **Community** of States interested in smoothening the handling of electronic travel documents,
- therefore aiming to increase standard conformity of the involved documents and systems
  - ***"educate and advise"***
- Funded on a cost share/recovery basis
  - the more join, the cheaper it becomes!

Solution Overview ICAO PKD Service



ICAO HQ Montreal

Location of ICAO primary HSM
Operating and supervising the PKD

Site Berlin

Up- and download location, secondary HSM1 and infrastructure for PKD operation

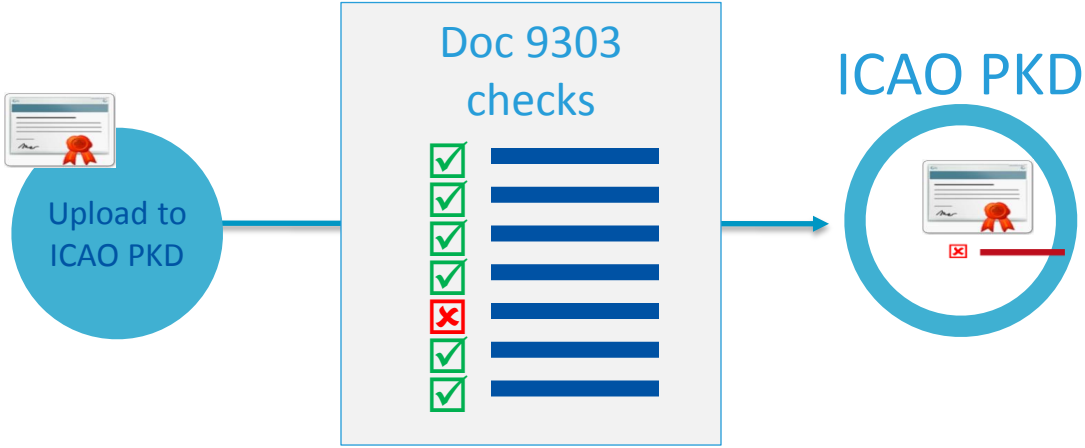
Site Abu Dhabi

Up- and download location, secondary HSM2 and infrastructure for PKD operation

How does the PKD work? – An Example

The PKD's Conformance Checks

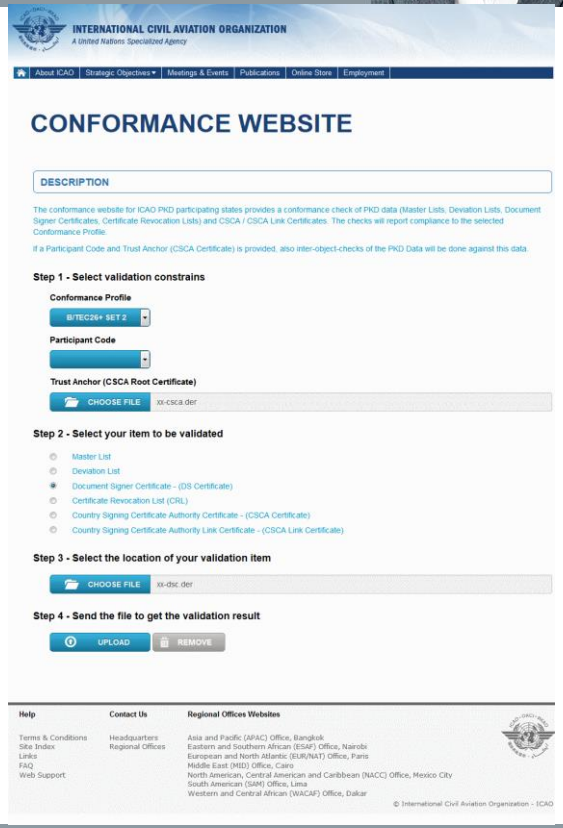
- Self-service on conformance website
- During upload of new PKD content (Document Signer Certificates, CRLs, Master Lists, Deviation Lists)
- During key ceremony at ICAO HQ (CSCA certificates, CSCA Link certificates)



Monitoring and quality assurance of PKD data to be distributed
Transparency for consumers of PKD Data
Facilitation of long-term improvement to involved PKIs

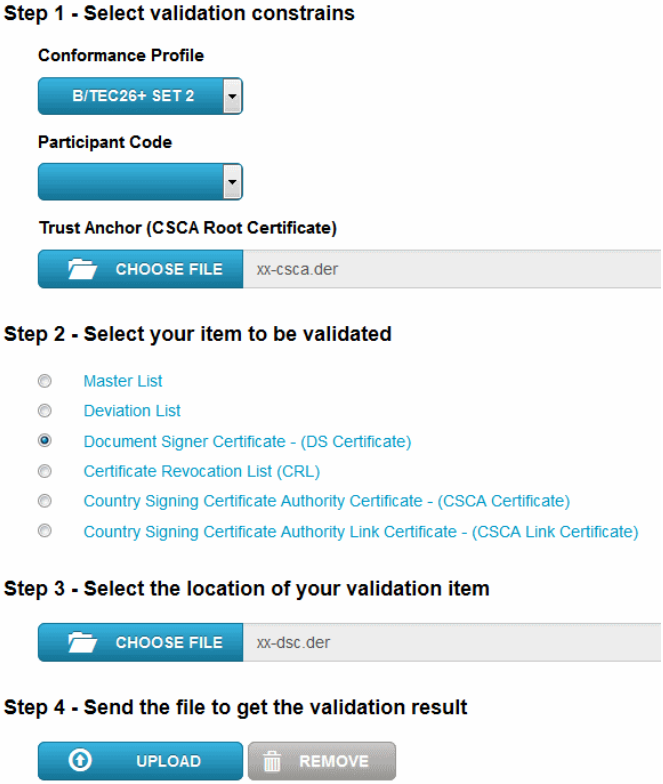
Further Increasing conformity to Doc 9303 – Using the ICAO PKD Conformance Website

- The Conformance Website provides performing the PKD's Doc 9303 related conformance checks, without the need of uploading them to the PKD.
- Use it to quick check your CSCA's PKI objects, ideally already before going into production.



- Select Conformance Profile (Set 1 for pre 2015 CSCAs, Set 2 for newer ones)
- Select Participant Code (two letter country code)
- Choose Trust Anchor (your CSCA certificate)
- Select the kind of object you want to check
- Choose the object you want to check
- Click on “UPLOAD”

- You will be presented with the results immediately



CONFORMANCE CHECK RESULTS

Errors and Warnings related to the CSCA itself

xx-dsc.der

Errors and Warnings related to the object to be checked (here: DSC)

Errors and Warnings

Deviation	TypeID	ElementID	NonConformanceID	Description
ERR	CSCA	CDP	14	Error: CSCA Certificate field CRL Distribution Point Field_Not_Present
ERR	CSCA	IAN	14	Error: CSCA Certificate field Issuer Alternative Name Field_Not_Present
ERR	CSCA	SAN	14	Error: CSCA Certificate field Subject Alternative Name Field_Not_Present
ERR	DSC	SAN	14	Error: Document Signer Certificate field Subject Alternative Name Field_Not_Present
ERR	DSC	IAN	14	Error: Document Signer Certificate field Issuer Alternative Name Field_Not_Present
ERR	DSC	CDP	14	Error: Document Signer Certificate field CRL Distribution Point Field_Not_Present

Focus on Conformance Checks

- Both the PKD's Conformance Website and the PKD itself do perform a non-comprehensive list of documented conformance checks.

- The currently implemented profiles are:
  - “B-Tec/26+ Set 1” classifies check results acc. to older versions of Doc 9303
  - “B-Tec/26+ Set 2” classifies check results acc. to Doc 9303 Edition 7

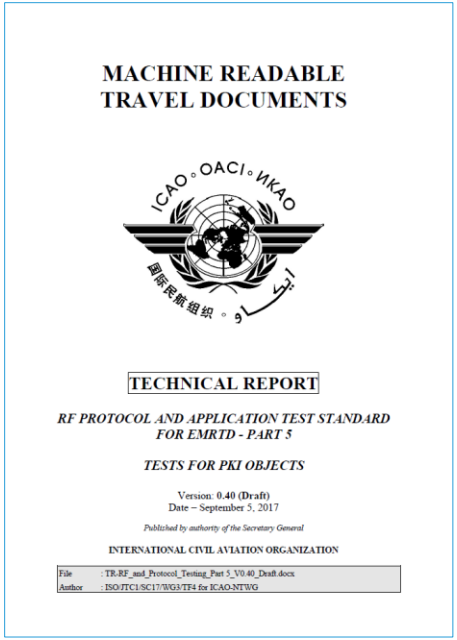
- It's important to note that the PKD historically never aimed to do a comprehensive checking, but only checks the most important aspects.
- So, if the Conformance Website tells you "No errors or warnings", this doesn't necessarily mean that the checked object is conformant in every aspect of Doc 9303.
- However, …

Focus on Conformance Checks (cont.)

- The community's expectation is actually a different one, i.e. the PKD should check more and give more guidance in order to reach the goal of creating fully conformant objects.

- Effort to contribute a test specification for the PKI part of Doc 9303:
  Veridos is the editor of the draft TR
  RF Protocol and Application Test Standard for eMRTD –
  Part 5: "Tests for PKI Objects"

- We assume that once this is finally published as an ICAO Technical Report, it's a good idea to extend the PKD by the additional checks.



MACHINE READABLE TRAVEL DOCUMENTS

TECHNICAL REPORT

RF PROTOCOL AND APPLICATION TEST STANDARD FOR EMRTD - PART 5

TESTS FOR PKI OBJECTS

Version: 0.40 (Draft)
Date – September 5, 2017

Published by authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION

File	: TR-RF_and_Protocol_Testing_Part 5_V0.40_Draft.docx
Author	: ISO/JTC1/SC17/WG3/TF4 for ICAO-NTWG

Focus on Master Lists – What is a Master List?

A CSCA Master List is

- is a collection of (domestic and foreign) CSCA certificates (including CSCA Link certificates), that
- is signed by the issuing State's Master List Signer.

Structure of a Master List (simplified):

Focus on Master Lists – Why to use a Master List?

- Note that anybody can technically create a root certificate that looks like a CSCA certificate of any specific State!
- The CSCA certificates are the trust anchor for passively authenticating ePassports
- Therefore, it is essential for every State not to simply accept any assumed CSCA certificate received, but follow a verification policy.
- By including foreign CSCA certificates in its Master List, the issuing State signs that it trusts in these certificates' authenticity according to its verification policy.
- Other States can then use this fact as one pillar of their own trust in a specific CSCA certificate.

Focus on Master Lists – How does the PKD make use of them?

- The ICAO PKD internally uses CSCA certificates as trust anchors for verifying uploaded content.
- It makes use of CSCA Master Lists (one per each State) to offer adequate downloads of CSCA certificates – direct downloads of CSCA certificates are not possible for security reasons!
- In order to further increase the PKD's value for its participating States, ICAO plans to issue an ICAO Master List in the near future.

Focus on Master Lists – How to use Master Lists as a State?

- Receive Master List (e.g. download from the PKD)
- Verify its signature – In case of downloading it from the PKD, this has been done by the PKD already before publishing the ML
- Extract the payload (i.e. the contained CSCA certificates)
- Use the extracted data according to your national policy

ICAO Master List – Current status

- Technically, the (Bundesdruckerei) PKD supports Master List creation from the beginning on
- The plan is:
  - to have the UN CSCA sign an ICAO Master List Signer (since ICAO is a UN organization)
  - To have ICAO use that MLS in order to issue the ICAO MasterList with it
- Current workpackages include:
  - UN is working on updating their CSCA in order to
    - Re-key to an Edition 7 conformant certificate
    - Be able to issue MLS
    - Change the Alpha2 country code from ZZ to UN

ICAO Master List – Current status (cont.)

- UN and ICAO are both working on creating policies (CP/CPS) taking the ML topic into account
  These policies need to include amongst other things:
  - Validity and Private Key Usage Period of the MLS
  - Rules on which certificates should be included
  - Rules on how often a ML will be generated

ICAO PKD – Conclusion and Outlook

- The ICAO PKD is the worldwide exchange platform for exchanging certificates for efficient border control
- Highly secure and highly available infrastructure
- Established and reliable processes supervised by ICAO
- Conformance checks help to increase standard-compliance of eMRTD PKIs on the long run
- Commercial use of the PKD for e.g. banks, telecoms, etc. – passive authentication also in the private sector
- Further contents can easily be added, like:
  - Masterlists of institutions or regions –
    ICAO Masterlist
    EU's Schengen Masterlist
  - Use of the PKD for signer certificates
    for non-electronic documents ("Visible Digital Seals")

Contact Details

Name: Florian Holeczek
Email: florian.holeczek@veridos.com