The ICAO PKI

Security and Simplicity
Basic Objectives

- Add digital signatures to ID data stored on passport ICCs.
- Permit easy chip data authentication at borders.
- Provide procedures and specs for global “confidence” in each country’s use.
- Provide an effective means of key and certificate sharing.
Application Profile

- Peer group of signing entities (countries).
- De facto cross-certification/trust.
- Two key levels; document signing and country CA certificate signing.
- Only countries have certificates; none for passport holders.
- Very infrequent revocations.
Certificates

- Country CA signing key certificates shared between countries by diplomatic means. Relatively stable (3-5 years?)
- Document signing key certificates shared via an ICAO certificate directory (certs may also appear on the MRTD). Used ≤ 3 months?
- ICAO does not act as global CA.
The ICAO Directory

- Central access to all certificates and CRLs:
  - Border inspection systems
  - Airlines
  - Others
- ICAO provides due diligence and some comfort that countries are following standard practices;
- Directory is downloadable, not for real-time access;
- Open Internet availability
Difficulties?

- KISS – how to keep it simple.
  - Revocations only for compromised keys; hopefully infrequent if ever
  - Limited numbers of keys and certs
  - A private application

- Limitations of COTS solutions?
  - Chain of trust validation
  - Cross-certification
  - Frequent revocations/CRL updates
  - Key lengths and hashing algorithms
Needed?

- Understanding that PKI can be used for “non-typical” applications.
- More modular OTS solutions – pick and choose?
- Flexibility regarding hard-and-fast rules
- Accent on the generic technology