



**INTERNATIONAL
CIVIL AVIATION
ORGANIZATION**



ICAO Doc 9303 & Post Quantum Cryptography (PQC)

Christopher Hornek
ICAO Facilitation Subject Matter Expert

12 May 2026

Abidjan, Cote d'Ivoire

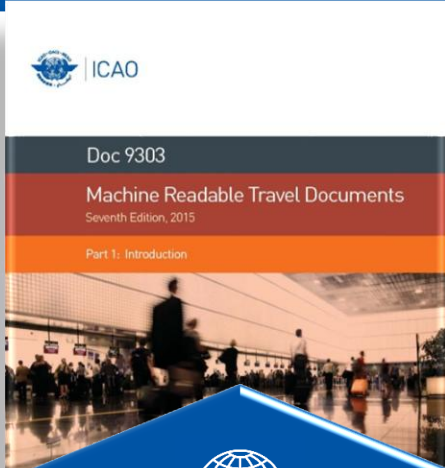
Background – eMRTD trust framework



Technical Advisory Group

New Technologies Working Group

Implementation & Capacity Building Working Group



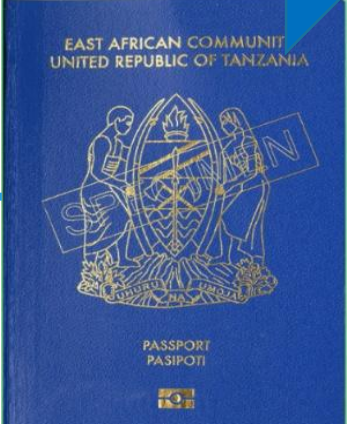
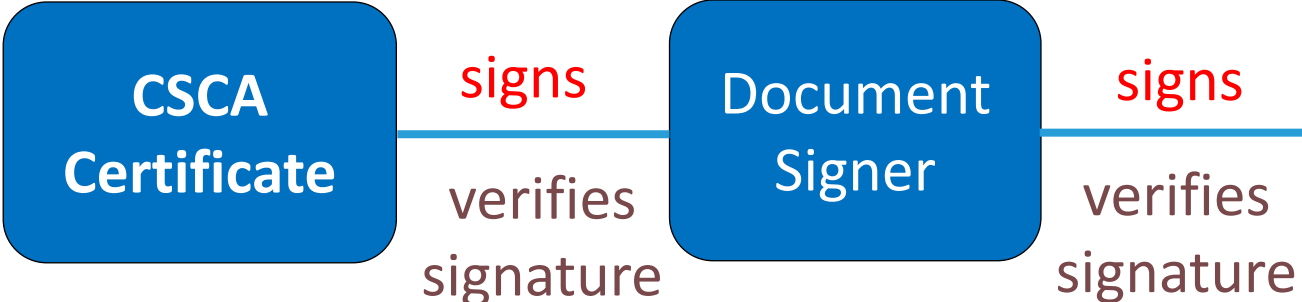
ISO
ISO/IEC JTC1 SC17/WG3



- ICAO Doc 9303 sets the specifications for electronic Machine Readable Travel Documents (eMRTD)
- Includes cryptographic mechanisms to strengthen the security of travel documents
- State managed (Sovereign) trust framework – no single root
- Distributed Public Key Infrastructure (PKI)
- Supported by the exchange of certificates, including via ICAO Public Key Directory (PKD)

Cryptography is at heart of ICAO eMRTDs

ePassport issuance using private keys



ePassport authentication using public keys

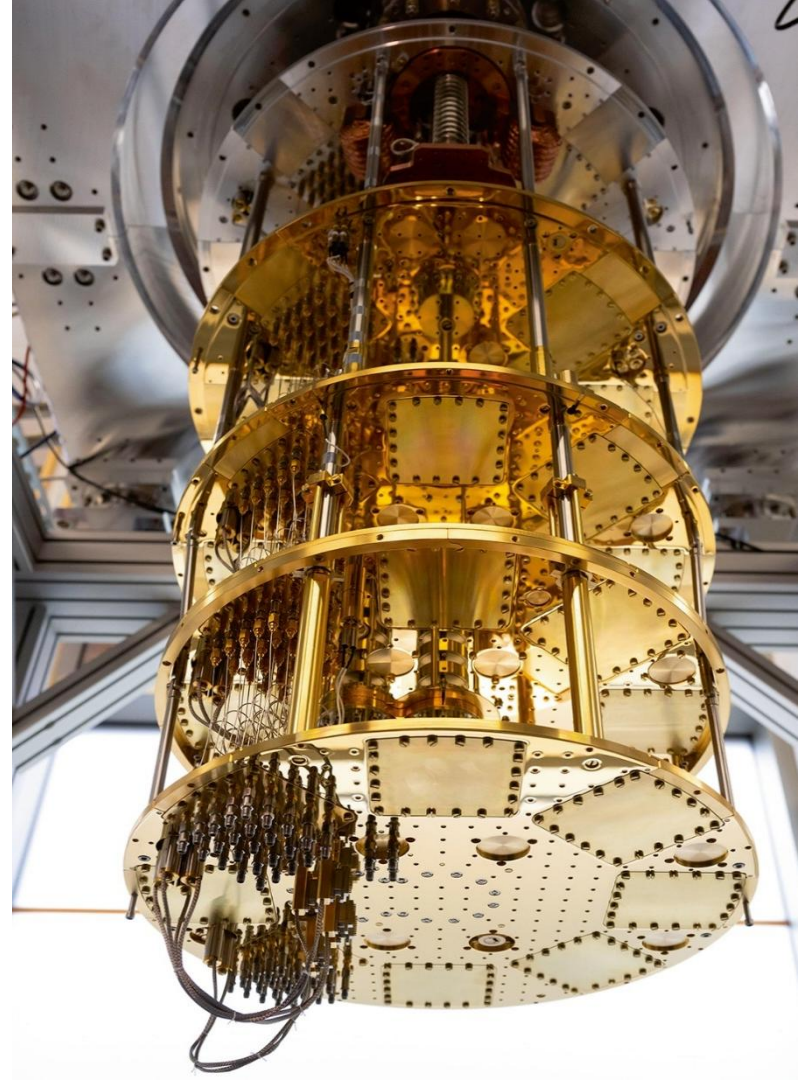
- Baseline security feature – Passive Authentication – ensures eMRTD data was signed by Issuing State and has not been tampered with
- More advanced security feature – Active or Chip Authentication – verifies the authenticity of the chip itself – prevents cloning or substitution of the chip

ICAO Trust Framework has stood the test of time

- Diffie-Hellman private/public key exchange published in 1976
- The security of private/public key cryptography lies in the high mathematical difficulty of solving algorithms
- ICAO PKI is impossible to compute (break) in a practical amount of time **even for modern supercomputers**
- The CSCA private key needs to remain exclusively in the ownership and control of the issuing State
- Private key compromise remains an issue, but this is not related to cryptography

Rise of Quantum Computing

- Although still under development – **Quantum Computing** is set to provide an exponential boost in computing power, including for cryptography
- **Unmatched Speed:** Recent developments suggest quantum processors can perform specific, complex tasks in minutes that would take classical supercomputers incalculable number of years
- Quantum Computing presents a definitive threat to classical cryptography as defined by ICAO Doc 9303



Threats posed by Quantum Computing

- We don't know when Q-Day will come, but its coming
- The threat to ICAO PKI is urgent, especially considering 10-year validity of eMRTDs being issued / signed now
- ICAO NTWG and ISO WG 3 have identified Passive Authentication as the security protocol most vulnerable to being broken by Quantum Computing
- The severity of the threat to Passive Authentication is also the highest and would affect a State's entire issuing system, thereby eroding trust in the global border management and travel ecosystem
- Anti-cloning measures (Active / Chip Authentication) and document access control mechanisms (PACE, Terminal Authentication) will also be impacted

Key Takeaways

- ICAO is in the process of specifying Post Quantum Cryptography (PQC) for inclusion into Doc 9303
- ICAO NTWG and ISO WG 3 have reviewed all quantum-safe signature algorithms that are currently standardized, including all algorithms currently standardized by ISO and those from NIST's PQC Standardization project
- **Possible Outcomes:**
 - Develop a feasible migration timeline for PKI and eMRTD security mechanisms to quantum-safe mechanisms
 - Two separate PKI (traditional and post quantum)
 - Two linked PKI (traditional and post quantum using hybrid certificates)
 - New Post-Quantum PKI only
 - Develop mitigation strategies against emerging threats posed by QC
 - Doubling key length
 - Reducing document validity period

Next Steps & Available Information

- ICAO will issue a State Letter asking countries to participate in a survey regarding their opinion on the next steps for standardizing quantum safe mechanisms for eMRTDs
- Information is being broadcasted through NTWG, ICBWG and the PKD Board to encourage broader engagement

Doc 9303 Guidance Material:

- Developments regarding Cryptographic Agility and Post-Quantum Cryptography for eMRTDs
- Quantum-safe mechanisms for the Document Issuing PKI and Passive Authentication
- Doc 9303 Cryptographic Key Length Review



2026
ICAO **TRIP**
SYMPOSIUM
22 - 24 SEPTEMBER | MONTRÉAL, CANADA



Thank you very much

And hope to see you in Montreal!