Quantum-safe ePassports: Migrating Electronic Travel Documents to Post-Quantum Security

Federal Office
for Information Security

Agenda

- Life cycle of an ePassport
- Electronic Security Mechanisms for travel documents
- Threat Analysis
- Challenges specific to travel documents
- Way forward

Life cycle of an electronic travel document

Enrolment Authority (e.g. municipality)

Application

Document Manufacturer

Issuance

Citizen

Usage

Document Inspection (e.g. border control)

- Country specific procedures
- Involves secure exchange of applicants biographic and -metric data

- Document must be handed out to the rightful holder

- Doc 9303 specifications

Life cycle of an electronic travel document

Enrolment Authority (e.g. municipality)

Application

Document Manufacturer

Issuance

Citizen

Usage

Document Inspection (e.g. border control)

- Country specific procedures
- Involves secure exchange of applicants biographic and -metric data

- Document must be handed out to the rightful holder

- Doc 9303 specifications

All life-cycle phases involve cryptographic mechanisms

Threat Analysis

of threats imposed by cryptographic relevant quantum computer

- **Threats to cryptographic mechanisms in electronic travel documents (eMRTDs)**

Cryptographic Protocol	Impact of a cryptographically relevant quantum computer on current protocol implementation.	Current Algorithms	Threat Severity
Passive Authentication	Cryptographic protection of an electronic travel document would be entirely compromised. Both the document issuing PKI (CSCA) as well as the authenticity of the data stored by an eMRTD would be affected.	RSA, ECDSA	High
Chip/Active Authentication	Protection against cloning or substitution of the eMRTD's chip would be no longer available.	RSA,ECDSA, DH,ECDH	Medium
PACE	The inspection procedure of an eMRTD's chip would no longer be protected from sniffing and/or eavesdropping.	DH,ECDH	Medium
Terminal Authentication	Protection of highly sensitive biometric data on a chip (fingerprints or iris) would no longer be available.	RSA,ECDSA	Medium
Secure Messaging	None (if a sufficient key-length is used)	3DES,AES	None

Threat Analysis

Cryptographic Protocol	Impact of a cryptographically relevant quantum computer on current protocol implementation.	Threat Severity
Passive Authentication	Cryptographic protection of an electronic travel document would be entirely compromised. Both the document issuing PKI (CSCA) as well as the authenticity of the data stored by an eMRTD would be affected.	High
Chip/Active Authentication	Protection against cloning or substitution of the eMRTD's chip would be no longer available.	Medium
PACE	The inspection procedure of an eMRTD's chip would no longer be protected from sniffing and/or eavesdropping.	Medium
Terminal Authentication	Protection of highly sensitive biometric data on a chip (fingerprints or iris) would no longer be available.	Medium
Secure Messaging	None (if a sufficient key-length is used)	None

- **Severity addresses impact on travel document ecosystem**
  - E.g.: If Passive Authentication breaks, also mechanism providing protection against cloning are not available anymore.
- **All mechanisms must be migrated to quantum-safe mechanisms**
  - The severity level only provides guidance for prioritising the migration of individual mechanisms.
  - Standardisation efforts currently focus of Passive Authentication and the Document Issuing PKI

Challenges specific to travel documents

for the transition to quantum-safe mechanisms

- **Very long life-span**
- **Complex ecosystem**
  - Each country operate at least one Issuer and typically multiple receiving entities (border control, police, regulated use-cases, etc.)
- **Security mechanisms rely on secure hardware implementations**
  - Smartcards and HSMs
- **Automated border control demands for fast document inspection**

Migration to quantum-safe mechanisms

(while product life-cycles are very long)

- **Travel documents typically have a validity period of up to 10 years.**
  - Document verifying infrastructure must be able to process travel documents implementing classic cryptography until these are out of circulation.
  - Issuer can only issue quantum-safe travel documents when any receiving state is able to process them.
    - States must reach consensus on transition period

- **Cryptographic agility required**
  - A standard for verifying electronic travel documents should offer:
    - Backwards compatibility: Allows for the timely issuance of quantum-safe travel documents before all receiving entities have migrated their infrastructure
    - Forwards compatibility: Provide flexibility to introduce new algorithms in the future without the need to introduce a new interface specification.

Cryptographic Agility

Which eMRTD security mechanisms already support this?

- **Passive Authentication** ?
  - Doc 9303 allows multiple signatures on chip (but does not recommend it)
  - No definition of how inspection systems should react in the case of unknown algorithms (accept document if only one signature could be validated, reject document, ….)
- **Active Authentication** ✗
  - eMRTD may implement only one Active Authentication mechanism
- **Chip Authentication** ✓
  - eMRTD may implement multiple cipher suites and offer them to the Inspection System
  - Inspection Systems chooses suitable suite
- **Terminal Authentication** ?
  - Protocol allows to change cryptographic algorithms for already issued documents.
  - Handling of environment with mixed documents (classic and quantum-safe) non-trivial.
- **PACE** ✓
  - Same as Chip Authentication

Backwards compatible migration strategies

for Passive Authentication

Possible options for the operation of the Document Issuing PKI (CSCA)

- **Parallel operation of two PKI branches (classic & quantum-safe)**
  - Each eMRTD gets signed twice, one signature from each branched respectively.
  - Classic inspection systems (without PQC support) may ignore quantum-safe certificate and signature.
  - Operation of two branches could result in additional expenses for issuing authorities.

- **Hybrid solution: PKI implements hybrid certificates and signatures**
  - Only backwards compatible if inspection systems are able to ignore the quantum-safe part.

- **Quantum-safe only**
  - More straight-forward implementation: Existing classic signature on eMRTD would be replaced by quantum-safe one.
  - Obviously not backwards compatible

Ongoing survey among states concerning preferred option

Implementing quantum-safe mechanisms

(on devices with constrained resources)

- **eMRTDs heavily rely on smartcard based contactless ICs**

➢ **Storage capacity and computing power is limited**

- Cryptographic certificates and keys must be stored on the travel document‘s IC
- Data must be transferred via a NFC-like interface (ISO/IEC 14443) with limited transmission rates
  - ➢ Key sizes must be kept small
- Cryptographic operations must be executed within the constraints of an IC
- Hardware is in the field for a long time
  - ➢ Assurances must be uphold throughout that validity period of a travel document
  - ➢ Rigid security certification required (e.g. Common Criteria) of hardware, algorithms and protocols

Implementing quantum-safe mechanisms

with limited storage capacity

- **Quantum safe digital signature algorithms comparison**

	ML-DSA	Falcon	SLH-DSA	LMS	XMSS
Security	Lattice	Lattice	Hash	Hash (stateful)	Hash (stateful)
Size of 2 Signatures & 1 Public Key [byte]	8.570 / 11.846	N.A. / 4.353	32.496 / 59.648	- / 5.720	3.516 / 5.708
Fraction of DG2 (á 15 kB)	0.56 / 0.77	N.A. / 0.28	2.11 / 3.88	- / 0.37	0.22 / 0.37
Standard	FIPS 204	TBS	FIPS 205	IETF RFC 8554, NIST SP 800-208	

Estimated readout time for certificates compared to the time required to read the facial image from the chip (from DG2)

- **Ongoing survey among states concerning suitability of algorithms**

Way forward

- **ICAO has endorsed a work item to create a technical specification on the implementation of quantum-safe mechanisms in the Document Issuing PKI and Passive Authentication**
- **States must reach consensus on**
  - Suitable cryptographic algorithms (Digital Signature algorithms and Key-Exchange algorithms)
  - Allowed PKI operation methods and certificate formats (parallel, hybrid, pure-PQC, …)
- **On-going prototypes serve as input for future specification to implement anti-cloning and access control mechanism on eMRTD chips**

Thank you for your attention!

Michael Hoppe
Senior Expert eID Components and Official Documents

michael.hoppe@bsi.bund.de

Federal Office for Information Security (BSI)
Godesberger Allee 87, 53175 Bonn

www.bsi.bund.de

Federal Office
for Information Security

Follow us: