Standardization efforts for PQC in OpenPGP in the Project PQC@Thunderbird

Stephan Ehlen\textsuperscript{BSI}, Andreas Hülsing\textsuperscript{TU/e}, Evangelos Karatsiolis\textsuperscript{MTG}, Stavros Kousidis\textsuperscript{BSI}, Johannes Roth\textsuperscript{MTG}, Falko Strenzke\textsuperscript{MTG}

BSI: German Federal Office for Information Security
MTG: MTG AG, Germany
TU/e: University of Eindhoven
Background of PQC@Thunderbird

- BSI-project: contractors MTG with TU/e
- timeline: 12/2021 until 12/2024
- standardization of PQC in OpenPGP (NIST-PQC selection)
- implementation of proof-of-concept
  - multi-algorithm KEM and signature (lattice-based)
  - in Thunderbird (via RNP and Botan)
  - in GnuPG / Libgcrypt
Motivation

- Store now / decrypt later
- long-term security for signatures is required
- PQC is entering the standardization phase
- demand for PQC is observed in the field
- integration in existing protocols has started
Completed and Ongoing PQC Standardization

Completed

- PQC scheme RFCs: XMSS (Informational), LMS (Informational), LMS in CMS and CBOR (both Proposed Standard)

Ongoing

- LAMPS IETF 113: numerous PQC-related drafts considered for adoption:
  - composite keys, encryption, signatures
  - binary data formats
- draft-vangeest-x509-hash-sigs: ASN.1 Encoding for hash-based schemes
- ETSI: TR on migration to PQC, etc.
- ISO: ongoing activities
<table>
<thead>
<tr>
<th>Year</th>
<th>2022</th>
<th>2023</th>
<th>2024</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Design**
- **PoC**
- **our initial OpenPGP-PQC I-D**
- **our standardization activities**
- **NIST-PQC stand. phase**

Today: NIST-PQC standards
Design Criteria

- use multi-algorithm (classic + PQC, a.k.a. hybrid)
  - public keys
  - KEM construction (use established proposals)
  - signatures
- orientation to existing proposals / standards
- backwards compatibility:
  - for multi-algorithm public key formats
  - multi-algorithm signatures
Cooperation with the WG

- We are open for any kind of input or contribution
- We plan to work on a draft for later adoption by the WG