Improvements for Post-Quantum IKEv2
Intermediate Exchanges

- Often fragmented, especially when used for PQKEs
- Signing fragmented intermediate messages is complex
- Large PQKEs in intermediate messages lead to vulnerabilities against DOS attacks ⇒ Move them to FOLLOWUP_KE
Status Quo
First Step: No IKE_INTERMEDIATE
Second Step: New Authentication Exchange
Benefits

- Independent of complex IKE_INTERMEDIATE exchanges
- DoS protected introduction of large PQKEs
- Clean state machine
- New place for exchanging handshake data after establishing an authenticated channel