Hybrid IKEv2 Interoperability Testing

July 1st, 2021
“Hybrid IKEv2” = draft-ietf-ipsecme-ikev2-intermediate + draft-ietf-ipsecme-ikev2-multiple-ke

strongSwan
• Andreas Steffen
• Tobias Brunner

Genua – based on OpenBSD
• Stefan-Lukas Gazdag
• Tobias Heider
• Daniel Herzinger

ELVIS-PLUS
• Valery Smyslov

ORGANISATION
• Leonie Bruckert (secunet)
Results

**strongSwan → ELVIS-PLUS**

Successfully tested:
- Negotiation of algorithms
- Single intermediate exchange
- Up to four intermediate exchanges
- IKE SA rekeying
- Child SA rekeying
- PQC KEMs: Kyber, Saber, FrodoKEM, SIKE

Issues:
- Same algorithm selected for all three additional key exchange rounds

**Genua → ELVIS-PLUS**

Successfully tested:
- Negotiation of algorithms

Issues:
- (Genua) Crashing probably related to liboqs usage

**Genua → strongSwan**

Successfully tested:
- Negotiation of algorithms

Issues:
- (Genua) Crashing probably related to liboqs usage
Results (cont.)

- It would be useful to agree on algorithm IDs in private range until final NIST Standards are available → strongSwan IDs
- Further discussions in small group of interested people
- Genua and ELVIS-PLUS interested in testing beyond 64KB limit (Classic McEliece)