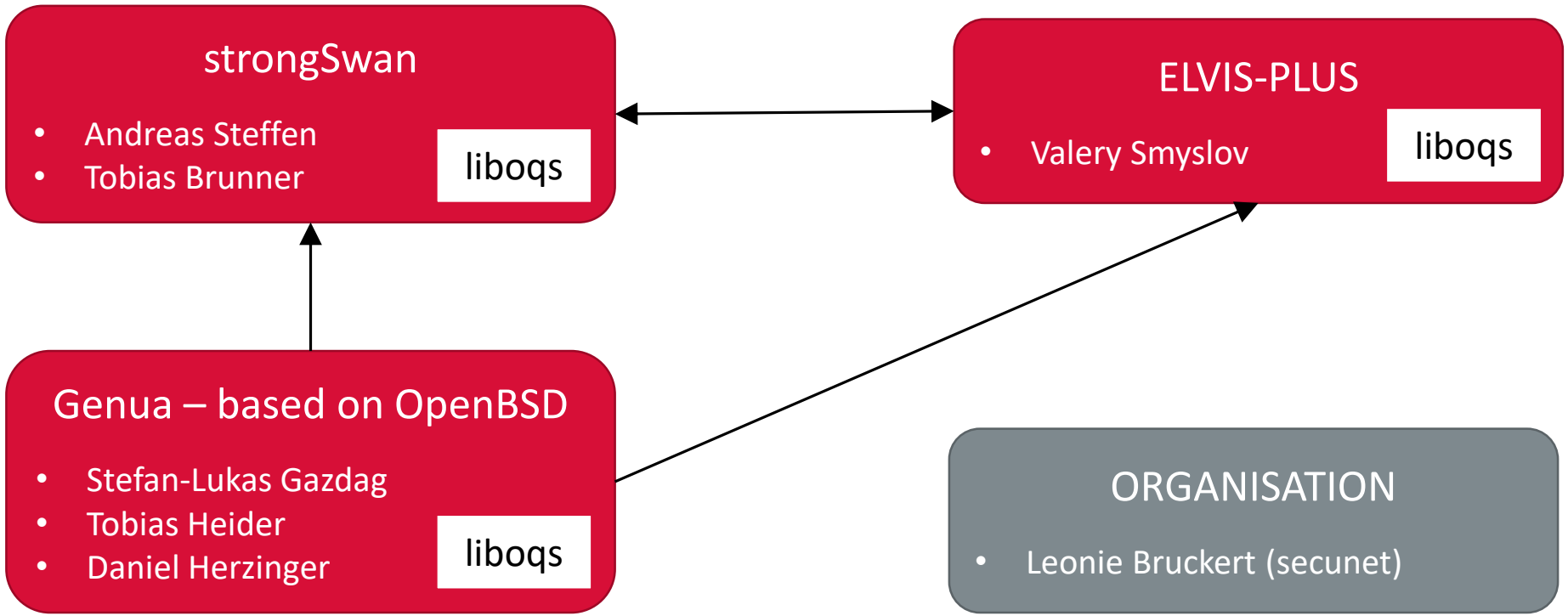
Hybrid IKEv2 Interoperability Testing

July 1st, 2021

Setting

"Hybrid IKEv2" = draft-ietf-ipsecme-ikev2-intermediate + draft-ietf-ipsecme-ikev2-multiple-ke



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)

```
/** NIST round 3 KEM candidates, in PRIVATE USE */
KE_KYBER_L1         = 1050,
KE_KYBER_L3         = 1051,
KE_KYBER_L5         = 1052,
KE_NTRU_HPS_L1      = 1053,
KE_NTRU_HPS_L3      = 1054,
KE_NTRU_HPS_L5      = 1055,
KE_NTRU_HRSS_L3     = 1056,
KE_SABER_L1         = 1057,
KE_SABER_L3         = 1058,
KE_SABER_L5         = 1059,
/** NIST alternative KEM candidates, in PRIVATE USE */
KE_BIKE_L1          = 1060,
KE_BIKE_L3          = 1061,
KE_BIKE_L5          = 1062,
KE_FRODO_AES_L1     = 1063,
KE_FRODO_AES_L3     = 1064,
KE_FRODO_AES_L5     = 1065,
KE_FRODO_SHAKE_L1   = 1066,
KE_FRODO_SHAKE_L3   = 1067,
KE_FRODO_SHAKE_L5   = 1068,
KE_HQC_L1           = 1069,
KE_HQC_L3           = 1070,
KE_HQC_L5           = 1071,
KE_SIKE_L1          = 1072,
KE_SIKE_L2          = 1073,
KE_SIKE_L3          = 1074,
KE_SIKE_L5          = 1075,
```