

Hybrid QSKE for IKEv2 Interoperability Testing Event

- Organized by **Secunet** on November 7, 2019
- Three active participants, few observers:
 - **strongSwan** <https://github.com/strongswan/strongswan/tree/ikev2-qske-draft>
 - **QuaSiModO** (based on OpenIKED from OpenBSD)
<https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/quasimodo>
 - **ELVIS-PLUS** (proprietary code)
- Features Tested:
 - all implementations support [draft-ietf-ipsecme-ikev2-intermediate-02](#)
 - one implementation fully supports [draft-tjhai-ipsecme-hybrid-qske-ikev2-04](#), two others support it partially (only initial IKE SA setup)
 - two implementations support PQKE methods, the other supports only classical KE methods

The Results

- Interoperability:
 - **strongSwan** & **ELVIS-PLUS** successfully established IKE SA with multiple (three) classical key exchanges
 - **QuaSiModO** & **strongSwan** performed hybrid PQKE (with newHope); KE itself was successful, IKE SA failed due to bug in computing AUTH payload
- Conclusions:
 - Hybrid QSKE works
 - Implementers badly need stable codepoints (at least for IKE_INTERMEDIATE)
 - Many of vendors who don't have implementations yet expressed an intent to implement QSKE once RFC is published