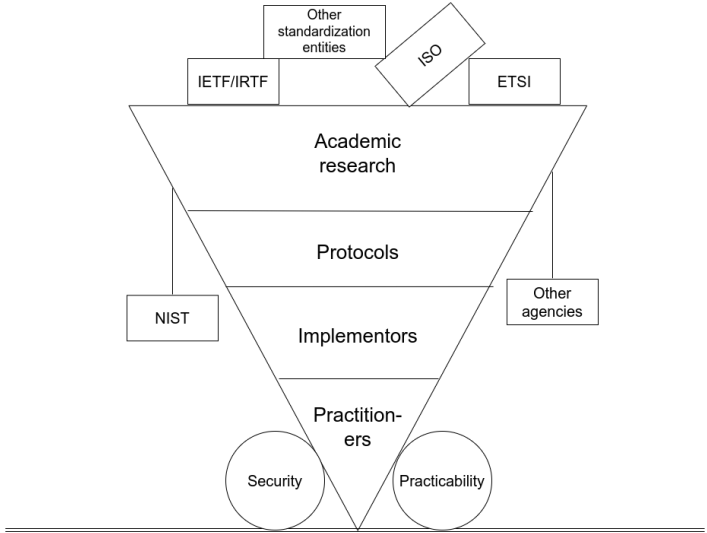
genua.

Post-Quanten-Kommunikation

Auf dem Weg der PQ-Migration

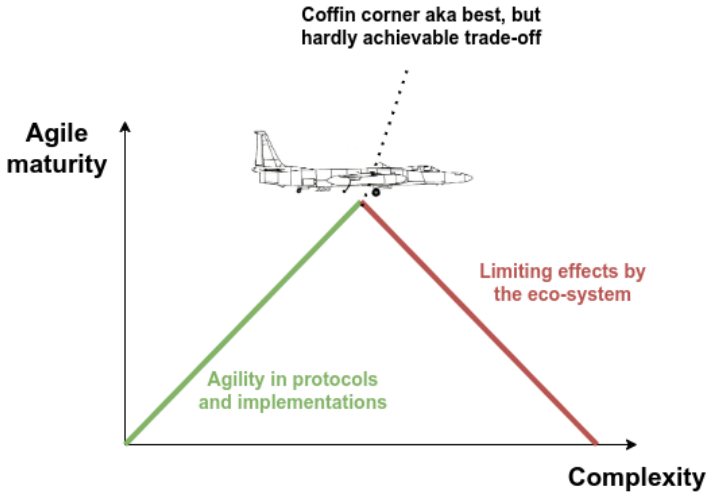
Stefan-Lukas_Gazdag@genua.de

20. Januar 2025


Other standardization entities
ISO
IETF/IRTF
ETSI
Academic research
Protocols
NIST
Other agencies
Implementors
Practition-ers
Security
Practicability

Reise zur Coffin Corner

Von United States Department of the Air Force - Defense Visual Information Center (1998). A DoD CD-Rom Image Collection: Best of the US Air Force. [1][2], Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=55114

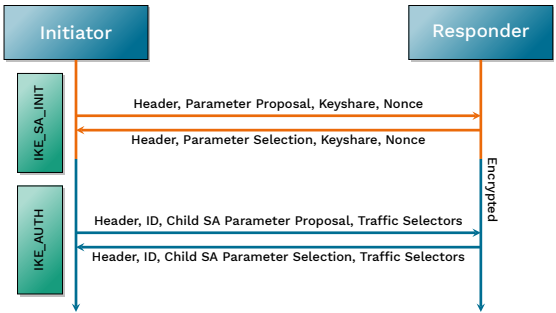


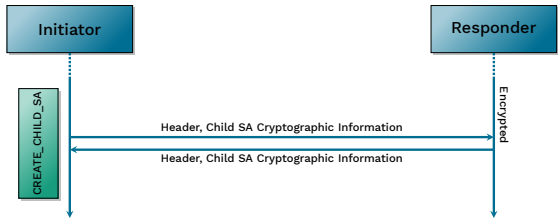
U-2 plane used as a part of work by Marcin Zieliński - Own work, CC BY 2.5,

https://commons.wikimedia.org/w/index.php?curid=1404361

Internet Key Exchange (IKEv2)

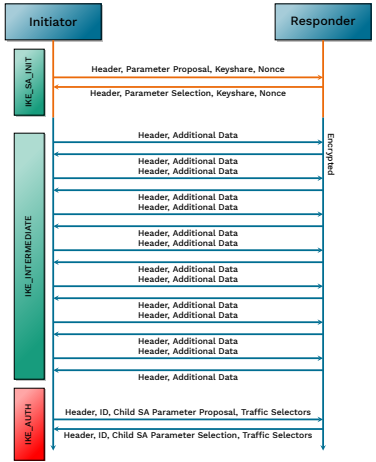
What used to be complex enough...

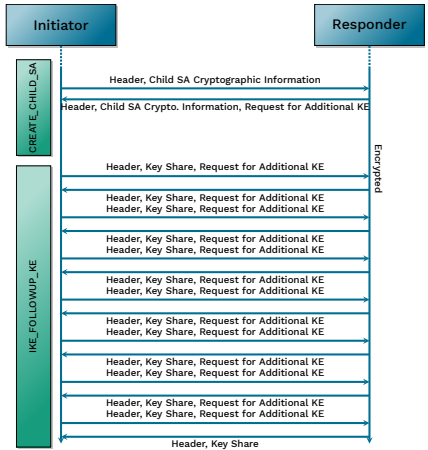




Internet Key Exchange (IKEv2)

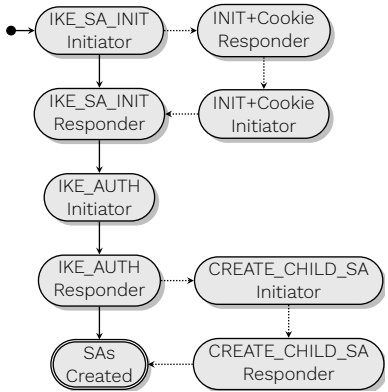
Full Post-Quantum Complexity

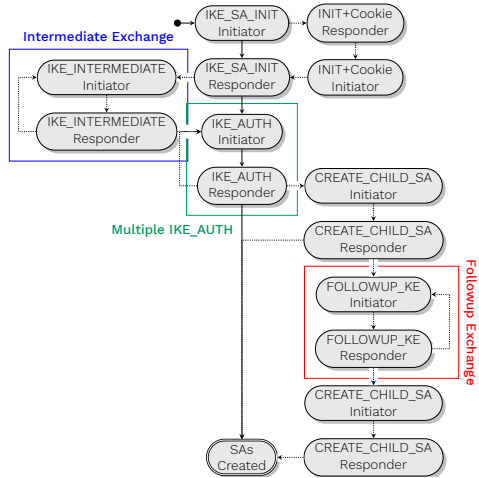




Internet Key Exchange (IKEv2)

State Machines





Unterschiedliche internationale Anforderungen

- Kryptoverfahren
  - ML-KEM/Kyber int. Standard
  - Auch andere Forderungen (Frodo, etc.)
  - Signaturen nach Anwendungsfall
  - Backup-Krypto für Vorfälle
- Hybrid oder direkte Migration?
  - Australien ab 2030 keine kl. Krypto
  - USA hybrid evtl. möglich, ab 2035 keine kl. Krypto
  - Deutschland vorerst hybrid

Vorschläge für KEX/KEM bei Standardisierung

- ML-KEM/Kyber allein
- hybrid mit ECDH:
  - mlkem768nistp256-sha256
  - mlkem1024nistp384-sha384
  - mlkem768x25519-sha256

  - mlkem768brainpool256 -> VPN bei genua (Zulassung 2024)
- teils unklar/uneinig: wie Secrets kombinieren?

Signaturen/Authentifizierung immer noch unklar

- Software-Updates/Root-Zertifikate:
  - LMS/HSS
  - XMSS/XMSS^{MT} -> Software-Updates bei genua (Zulassung 2017)
- ML-DSA/Dilithium everbody's darling
- Alternativen verfügbar / in der Mache

=> Key Management im nächsten Vortrag

Excellence in Digital Security

genua GmbH
Domagkstr. 7
85551 Kirchheim bei München
+49 89 991950-0
info@genua.de
www.genua.de