Quantum Resistant IKEv2

draft-ietf-ipsecme-qr-ikev2-04

Scott Fluhrer, David McGrew, Panos Kampanakis
Cisco Systems
Valery Smyslov
ELVIS-PLUS

IETF 102

Changes from -02 version

- No changes of bits on the wire, only few clarifications:
  - Using NO_PPK_AUTH was clarified (text provided by Tommy Pauly)
  - Using Group PPK was more explicitly discouraged (feedback from Quynh Dang)
  - Minor editorial nits

Status Update

- At least four vendors implemented the -02 draft
  - implementations were tested for interoperability against each other
- We believe the document is stable and ready for WGLC