Quantum Resistant IKEv2

draft-ietf-ipsecme-qr-ikev2-02

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

IETF 101
Changes from -00 version

- The way PPK is stirred into calculation of $SK_{pi}$, $SK_{pr}$ and $SK_d$ is changed from using $prf$ to $prf+$
- Using PPK in case of EAP authentication is clarified - it is only used in the last IKE_AUTH flight
- Clarification is added that PPK is used only in initial IKE SA setup and MUST NOT be used in case of IKE SA rekey or resumption
- Added note that the initiator MUST ignore the content of $PPK_{IDENTITY}$ if for some reason it is not empty
- $PPK_{SUPPORT}$ notification is renamed to $USE_{PPK}$
- Official code points allocated by IANA are added to the draft
- Minor editorial nits
Status Update

• At least four vendors implemented the latest draft
  • some implementations were tested for interoperability against each other

• We believe the document is ready for WGLC