Post-quantum cryptography migration use cases

draft-vaira-pquip-pqc-use-cases
PQUIP – IETF 120 – July 23rd 2024

Hendrik Brockhaus
Siemens

John Gray
Entrust

Mike Ounsworth
Entrust

Alex Railean
Siemens
What is it?

Systematize migration strategies for digital signature use cases

Aims

• Help choose fitting algorithms and parameters
• Start a discussion
What changed since IETF 119?

• Incorporate feedback

• Wording around hybrids
  • Better supporting argumentation, bias for action
  • Acknowledge potential downsides

• Revised decision tree
  • removed subjective component
What next? Explore “pessimistic migration”

• Assumption: CRQC-attacks start sooner than standardization or migration is complete. How about tomorrow?

• What can one do today to
  • not be an easy target tomorrow
  • and buy time on Q-day

• Some techniques
  • Wrap legacy communications (e.g., SSH tunnels with NTRU/x25519)
  • Symmetric ciphers with pre-shared keys without handshakes (e.g., shadowsocks)
What next?

• Find me and let’s talk
  • Challenges
  • Questions

• Feedback
  • IETF channels
  • https://github.com/avaira77/pq-ietf-usecase