Post-quantum cryptography migration use cases

draft-vaira-pquip-pqc-use-cases

PQUIP – IETF 119 – March 19th 2024

Antonio Vaira
Siemens

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 118?

- Incorporate feedback
- Simplify document structure
- Categorize use-cases in terms of
  - Lifetime
  - Protocol type
  - Backward-compatibility
- Add flowchart

What next?

- Find me and let’s talk
  - Challenges
  - Stories
  - Questions

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