Post-quantum cryptography use cases

`draft-vaira-pquip-pqc-use-cases`

A. Vaira, H. Brockhaus, A. Railean, J. Gray, M. Ounsworth

Antonio Vaira

IETF 118 – PQUIP Working Group

Introduction

- "`draft-vaira-pquip-pqc-use-cases`" is primarily meant to be a collection of PQC migration use cases.

- It additionally aims at listing PQC migration strategies and mapping them with PQC migration use cases.

- It is still in its infancy…

PQC: post-quantum cryptography

Document Objectives and Scope

- Make order among use cases and identify PQC migration strategies.

- Evaluate PROS and CONS of use cases x migration strategies.

- The current scope is “challenging migration scenarios”:
  - Long lived assertion,
  - Non-trivial update mechanisms,
  - Compliance with upcoming regulations.*

*BSI-hybrid: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4

Why should PQUIP be interested?

- Anchoring into tangible use case the evaluation of PQC migration strategies, like:
  - multiple certificates,
  - hybrid-composite vs. hybrid-non-composite,
  - LMS/XMSS vs. SPHINCS+, etc.

- Accompanying https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/

- It does not need to become a RFC, but rather a living document..

Next Steps…

- Continue working on it:
  - join as contributor and tells us about your use cases, OR
  - join as co-author and add your use cases yourself…

- Keep discussing it in the WG mailing list or at https://github.com/avaira77/pq-ietf-usecase

- Use its content to discuss migration strategy on a common ground…

BACKUP

Use Case Examples

- BACnet/SC stands for Building Automation and Control Networks / Secure Connect' (BACnet/SC)

- BACnet/SC's implementation adheres to established industry standards defined in IETF RFCs
  - RFC7468 - Textual Encodings of PKIX, PKCS, and CMS Structures
  - RFC8446 - The Transport Layer Security (TLS) Protocol Version 1.3
  - etc.

- In this specific use case using hybrid-composite can help fulfil upcoming requirements for supporting hybrid cryptography*.

*BSI-hybrid states: […] quantum computer-resistant methods should not be used alone - at least in a transitional period - but only in hybrid mode, i.e. in combination with a classical method.