IETF Hackathon

IETF 115
5-6 Nov 2022
London, England

I E T F

PQ Keys and Signatures Hackathon

Goals:

- Production and validation of X.509 keys, certificates, PKCS10, CRLs and other X.509 structures with the new NIST algorithms (Dilithium, Falcon, SPHINCS+, Kyber) alone and in composite combinations with traditional crypto
- Solving ASN.1 encoding issues to help clarify specifications in the new drafts
- Obtain experience with practical use of the new NIST algorithms in X.509
- Provide an artifact repository for interoperability testing

RFC Drafts:

- https://datatracker.ietf.org/doc/html/draft-uni-qsckeys-00.html
- https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/
- https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-keys/
- https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/
- RFC 5280, 5208, 5958, 2986 (Public and Private key formats, Certificate Request, others)
- https://www.secg.org/sec1-v2.pdf - section section 2.3.1/2.3.2

What got done

- Formed new Hackathon team with about 16 participants!
  - Created Github artifact repository https://github.com/IETF-Hackathon/pqc-certificates
  - Defined a .zip file structure for X.509 artifacts to make interoperability testing easier. These include pure PQ artifacts as well as composites.
  - Agreed on public and private key ASN.1 encodings (See what we learned).
  - 7 different implementations (Java, C, Python, Rust).
    - Open Source (OpenSSL, Bouncy Castle, Python)
    - 4 Vendor implementations

What we learned

- Public Keys – OCTET STRING can be mapped to BIT STRING from RFC 5208
  - https://www.secg.org/sec1-v2.pdf section section 2.3.1/2.3.2
  - “**treat BIT STRING and OCTET STRING identically** (doing sensible 0-bit-padding if BIT STRING is no multiple of 8)“
  - Thus no need for wrapping/adding another TLV layer for implementations that internally operate on octet strings (and tag BIT STRINGS only where the standard mandates it)”

What we learned

- Private Keys - No need to have an OCTET_STRING wrapping another OCTET_STRING. We will use a Single OCTET_STRING representation as per 5958.
- OIDS – Object Ids need to be flexible at this point, and we are suggesting they be version controlled as there are still tweaks being made to the NIST competition winners (Dilithium, SPHINCS+, Falcon, Kyber)
- Suggest <Arc>.Version.SecurityLevel
- Most issues found are not related to PQ algorithms

Wrap Up

Team members:

First timers @ IETF/Hackathon:

Mike Ounsworth, John Gray, Felipe Ventura, Jake Massimo, Cory Bonnell, Michael Baentsch, Kris Kwiatkowski, Alexander Railean, Pat Kelsey, Britta Hale, Tomofumi Okubo, Carl Wallace, Max Pala, Markku-Juhani O.Saarinen, David Hook, @bblfish

Next Steps:

- Monthly meetings to continue progress
- Monday Dec 5 12:00 UTC
- Expand artifacts and add X.509 based protocols