PQ in X.509

IETF 116
25 March 2023
Yokohama, Japan

I E T F

PQ in X.509 Hackathon

Goals:

- Adding PQ algorithm support into existing X.509 structures (keys, signatures, certificates and protocols)
- Test interoperability between different algorithm implementations
- Gain experience using PQ algorithms
- Provide feedback to the standards groups about practical usage

RFC Drafts:

RFC 5280, 5208, 5958, 2986 (Public and Private key formats, Certificate Request, others

draft-ietf-lamps-dilithium-certificates

draft-ounsworth-pq-composite-sigs/

draft-ounsworth-pq-composite-kem/

draft-becker-guthrie-cert-binding-for-multi-auth/

draft-ietf-lamps-kyber-certificates/

draft-ounsworth-pq-composite-keys/

draft-housley-lamps-cms-kemri-00.html

What got done… since 115

- Monthly meetings well attended (we hit the gather limit of 10 in meeting earlier this month and some people could not join). We will need to switch to another platform due to this limit unless it is changed (we prefer gather).
- Expanded our Github artifact repository https://github.com/IETF-Hackathon/pqc-certificates
    - Testing automated tooling to create more granular compatibility matrix outputs
    - Added CMP message structures into artifact repository and tested interoperability
    - CMS messages with KEM have been produced (need more people to interop test)
    - Hybrid Catalyst certificates (using V3Extensions for PQ material)
    - Generic /Explicit composite and hash-then-sign composite artifacts
    - Experimental new SIA access method for multi-certificate chains implemented
  - 9 different vendor submissions (Java, C, Python, Rust).
    - Open Source (OpenSSL, Bouncy Castle, Python, LibPKI)
    - 6 Vendor implementations

What we have learned

- Lots of Discussion – What is the future of LibOQS (prototyping library). What does production ready PQ look like?
- Our project is useful beyond the scope of our project (for example the NCCoE - The National Cybersecurity Center of Excellence often references our project).
  - OID interoperability table :

    https://github.com/IETF-Hackathon/pqc-certificates/blob/master/docs/oid_mapping.md
- There is a lot of interest in hybrid certificate formats (composite, catalyst, multi-cert) for migration or future upgrade scenarios. Tools in the tool box

What we have learned

- Adding PQ signatures into existing protocols like CMP is straight forward and works as expected
- KEM will take longer to implement as the basic operations are not yet implemented in most languages
- Implemented an alternate mechanism to https://datatracker.ietf.org/doc/draft-becker-guthrie-cert-binding-for-multi-auth/ using an SIA extension to carry the Access Location of alternate certificate paths. It was easy to implement and very flexible. Will give feedback to the authors later this week.

Wrap Up

Team members:

IETF/Hackathon:

First Time: Goutam Tamvada, Daiki Ueno, Julien Prat

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

Next Steps:

- Monthly meetings to continue progress
- **May 1st 12:00 UTC**
- More granular reporting