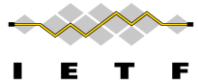
PQ in X.509

IETF 117
22-23 July 2023
San Francisco, California



Hackathon Plan

Goals:

- Adding PQ algorithm support into existing X.509 structures (keys, signatures, certificates and protocols)
- Test and interoperate with newer draft updated to support the migration to PQ
- provide an artifact repository for interoperability testing
- Provide a comprehensive compatibility matrix to show results
- 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-ietf-lamps-kyber-certificates/
draft-ounsworth-pq-composite-sigs/
draft-ounsworth-pq-composite-keys/
draft-ounsworth-pq-composite-kem/
draft-housley-lamps-cms-kemri-00.html
draft-becker-guthrie-cert-binding-for-multi-auth/
draft-bonnell-lamps-chameleon-certs/
draft-gazdag-x509-hash-sigs/

What got done

- Monthly meetings well attended (we can’t use gather anymore because we exceed the limit).
- Discussed a virtual interim hackathon meeting (probably September)
- New members: Alie Becker, Brendan Zember, Chris Rodine, Chris Brown, George Tasopoulos
- Binding for multi-auth draft implementation started
- Interest in developement of a light-weight ASN.1 parser, some initial work done.

What got done

- Working on updates to the compatibility matrix
- An Implementation of PQ using wolfSSL has been started
- Some interoperability testing of the Delta Certificates draft
- KEM certificates (Kyber) created and tested
  - Discussed CSR KEM POP issue (either sign by an alternate key, or an indirect POP where result is encrypted). Is a draft needed for this?
  - Some initial KEM work done as specified in the CMP updates draft (4210-bis)

What we learned

- Recent algorithm changes have caused OIDs to be versioned – algorithm support needs to be kept fresh
- Specification changes require nimble implementations
- Creation of a compatibility matrix that has a comprehensive view of the results is important to show progress.
- We like working together and are looking forward to a virtual interim hackathon
- For implementation work done on a draft, we can link the code repository to the draft.

Wrap Up

Team members: Team members:

IETF/Hackathon:

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

First timers @ IETF/Hackathon: Alie Becker, Brendan Zember, Chris Rodine, Chris Brown, George Tasopoulos

Next Steps:

- Monthly meetings to continue progress
- Virtual interim hackathon
- Compatiblity Matrix updates
- Github: https://github.com/IETF-Hackathon/pqc-certificates