PQ in X.509

IETF 122
15–16 March 2025
Bangkok, Thailand

PQC in X.509 interoperability Project

- 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

- Drafts

  - draft-ietf-lamps-dilithium-certificates
  - draft-ietf-lamps-kyber-certificates
  - draft-bonnell-lamps-chameleon-certs/
  - draft-ietf-lamps-cms-kemri/
  - draft-ietf-lamps-pq-composite-sigs/
  - draft-ietf-lamps-pq-composite-kem/
  - draft-ietf-lamps-cert-binding-for-multi-auth
  - draft-lamps-okubo-certdiscovery
  - draft-ounsworth-lamps-pq-external-pubkeys/
  - draft-ietf-lamps-rfc4210bis
  - draft-ounsworth-cfrg-kem-combiners
  - draft-ietf-lamps-cms-kyber

What got done

- Updated to v5 zip artifact format file:
  - Adds artifacts for testing the 3 ML-DSA and ML-KEM private key formats.
  - Added artifacts for the SLH-DSA private key format
- Updated CMS KEM formats to v3
  - Added support for testing CMS signatures (added a signed attribute artifacts)
- 6 different implementations of the ML-DSA private key format tested!
- Composite Signatures draft -04 implemented and posted, need others for interoperability testing
- Much discussion on composite key format (ASN.1 SEQUENCE vs byte encoding). The serialization description should be updated to use ASN.1 byte encodings!

What got done

- Pure RUST implementations of ML-DSA, ML-KEM and SLH-DSA submitted as artifacts
- Implementation of RFC 9629 (KEMRecipientInfo) being added into OpenSSL
- OpenSSL implementations of ML-DSA, ML-KEM, SLH-DSA artifacts are being tested.
- Working on adding more granularity to the compatibility matrix regarding the testing of the private keys
- OpenSSL team is working on adding the newer RFC 5958 private key format

What we learned

- Usings SLH-DSA in CMS with SHAKE XOF is “difficult to implement” as there isn’t an OID that directly specifies the bits of output. The application context needs to be known. RFC 8702 introduced CMS specificity.
- RFC 9629 didn’t specify a default Mandatory to Implement (MTI) KDF which can make implementing it more difficult.
- Recommend that new algorithms in CMS MUST use signed attributes.
  - signing large messages creates usability issues.
- CMS RFC are often not consistent with digest algorithm recommendations. Some are very constraining, others are not.
- Working remotely with 12-hour time zone changes is difficult!

PQ in X.509 – Summary

TEAM MEMBERS

- Michael Baentsch, Alie Becker, Cory Bonnell, Chris Brown, John Gray, Britta Halle, David Hook, Pat Kelsey , Kris Kwiatkowski, Jake Massimo, Tomofumi Okubo, Markku-Juhani O.Saarinen, Mike Ounsworth, Max Pala, Julien Prat, Alexander Railean, Chris Rodine , Goutam Tamvada, George Tasopoulos , Daiki Ueno, Felipe Ventura, Carl Wallace, Brendan Zember, Ned Smith, Akira Nagai, Kan Yasuda, Yuta Fukagawa, Joe Mandel, Lucas prabel, Joseph LukeFahr, Abel C.H. Chen, Austin CHT, Roy Basmatir, Conner Ybarra, Nic Freeman, Sean Authlet, Jethro, Varun, Mike Tsai, Peiduo, others

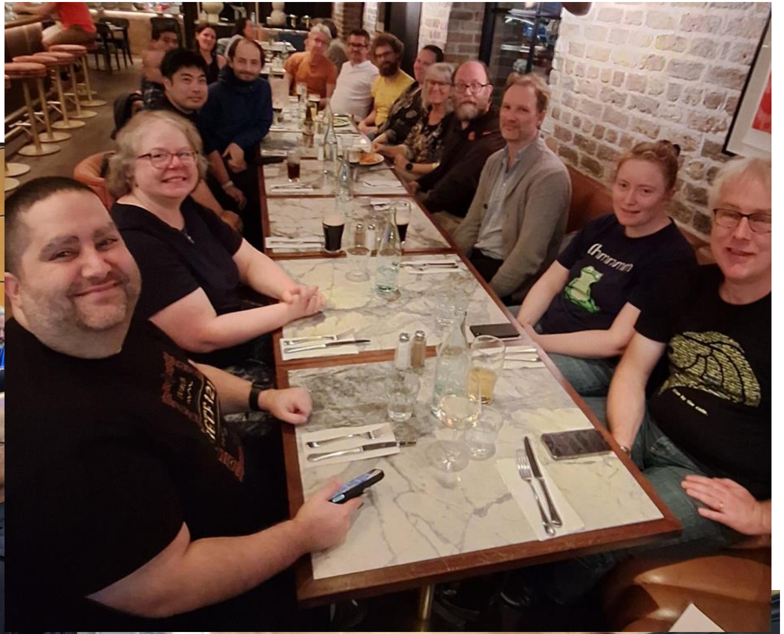
FIRST TIMERS

- Jean-Pierre Fiset, Viktor Dukhovni, Tim Hudson

NEXT STEPS

- Monthly meetings to continue progress – Next meeting is **Tuesday April 1st**
- Github: https://github.com/IETF-Hackathon/pqc-certificates

JOIN US!



Contact John.gray@entrust.com to join!