PQC in X509

IETF 121
Nov 2–3 2024
Dublin, Ireland

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

- Crypto Providers updated to the new V4 Certificates format file and adding support for ML-KEM, ML-DSA and SLH-DSA Standards
- Automated github action updated to trigger on the new artifacts_certs_v4.zip file
- Quantcrypt validator being adding into the guthub automation. https://hub.docker.com/r/jethrolow/quantcrypt_validator

What GOT DONE

- CMS KEM artifacts tested– updating to latest ML-KEM and V2 format artifacts
  - Found ML-KEM private Key format incompatibilities
    - Some people use 32 byte seed, some use long form of key
    - Some use ASN.1 wrapping inside the OCTET_STRING to determine which form of ML-KEM key was used, some did not use ASN.1 wrapping. For historical perspective, EdDSA did use internal ASN.1 wrapping.
    - Draft consensus and discussions at LAMPS indicating only the seed format should be used.
- Automated github action for CMS artifacts being worked on.

What GOT DONE

- Interop testing of latest Composite KEM draft started
- Successful Interop testing of Composite Signatures -03
- Added testing of Hash ML-DSA (OIDS listed in tables)
- ASN.1 Querying tool for RFC structures in pyasn1-modules

Automated Compatibility matrix Sample

✅ = passing all verifiers
◒ = passing some verifiers
○ = not passing any verifiers

....

-	bc	cht	corey-digicert	cryptonext	cryptonext-cnsprovider	kris
ML-DSA-44	◒	◒	◒	◒	◒	◒
ML-DSA-65	◒	◒	◒	◒	◒	◒
ML-DSA-87	◒	◒	◒	◒	◒	◒
SLH-DSA-SHA2-128s	◒	◒		◒	◒	
SLH-DSA-SHA2-128f	◒	◒		◒	◒	
SLH-DSA-SHA2-192s	◒	◒		◒	◒	
SLH-DSA-SHA2-192f	◒	◒		◒	◒	
SLH-DSA-SHA2-256s	◒	◒		◒	◒	
SLH-DSA-SHA2-256f	◒	◒		◒	◒	
SLH-DSA-SHAKE-128s	◒	◒		◒	◒	
SLH-DSA-SHAKE-128f	◒	◒		◒	◒	
SLH-DSA-SHAKE-192s	◒	◒		◒	◒	
SLH-DSA-SHAKE-192f	◒	◒		◒	◒	
SLH-DSA-SHAKE-256s	◒	◒		◒	◒	
SLH-DSA-SHAKE-256f	◒	◒		◒	◒	
HASH-ML-DSA-44	◒		◒	○		
HASH-ML-DSA-65	◒		◒	○		
HASH-ML-DSA-87	◒		◒	○		
HASH-SLH-DSA-SHA2-128s	◒			◒		
HASH-SLH-DSA-SHA2-128f	◒			◒		
HASH-SLH-DSA-SHA2-192s	◒			◒		

ML-DSA-65 (2.16.

Rows are producers. Columns are parse

-	bc	oqs
bc	✅	❌
carl-redhound	✅	❌
cht	✅	❌
corey-digicert	✅	❌
cryptonext	✅	❌
cryptonext-cnsprovider	✅	❌
kris	✅	❌

Manual Compatibility matrix Sample

✅ = passing all verifiers
◒ = passing some verifiers
○ = not passing any verifiers
Columns represent producers who submitted artifacts. Verifiers are not listed in this table, but are listed in the broken-out tables below.

-	bc	carl-redhound	cht	cnsprovider	corey-digicert	cryptonext	cryptonext-cnsprovider	kris	seventhsense.ai
ML-DSA-44	✅	✅	✅	✅	✅	✅	✅	✅	✅
ML-DSA-65	✅	✅	✅	✅	✅	✅	✅	✅	✅
ML-DSA-87	✅	✅	✅	✅	✅	✅	✅	✅	✅
SLH-DSA-SHA2-128s	✅	✅	✅	✅		✅	✅		✅
SLH-DSA-SHA2-128f	✅	✅	✅	✅		✅	✅		✅
SLH-DSA-SHA2-192s	✅	✅	✅	✅		✅	✅		✅
SLH-DSA-SHA2-192f	✅	✅	✅	✅		✅	✅		✅
SLH-DSA-SHA2-256s	✅	✅	✅	✅		✅	✅		✅
SLH-DSA-SHA2-256f	✅	✅	✅	✅		✅	✅		✅
SLH-DSA-SHAKE-128s	✅	✅	✅	✅		✅	✅		✅
SLH-DSA-SHAKE-128f	✅	✅	✅	✅		✅	✅		✅
SLH-DSA-SHAKE-192s	✅	✅	✅	✅		✅	✅		✅
SLH-DSA-SHAKE-192f	✅	✅	✅	✅		✅	✅		✅
SLH-DSA-SHAKE-256s	✅	✅	✅	✅		✅	✅		✅
SLH-DSA-SHAKE-256f	✅	✅	✅	✅		✅	✅		✅
HASH-ML-DSA-44	◒	✅			✅	◒			✅

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 others

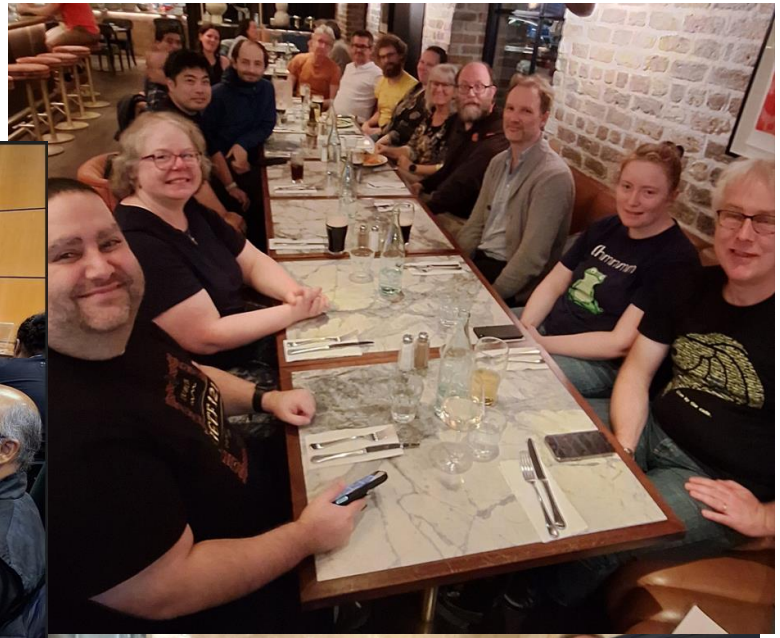
FIRST TIMERS

- Jethro, Varun, Mike Tsai, Peiduo

NEXT STEPS

- Monthly meetings to continue progress – Next meeting is **Tuesday Dec 3rd**
- Virtual Interim Hackathon (January?)
- Github: https://github.com/IETF-Hackathon/pqc-certificates

JOIN US!



Contact John.gray@entrust.com to join!