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 32byte 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.
    - drafts should be updated to give guidance, for example:
      - draft-ietf-lamps-cms-kyber
- 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
- Added OIDs for Hash ML-DSA and SLH-DSA to test those algorithms
- ASN.1 Querying tool for RFC structures in pyasn1-modules

INTEROPERABLE OID Mapping Table

Signature Algorithm Name	OID	Specification
ML-DSA-44	2.16.840.1.101.3.4.3.17	FIPS 204
ML-DSA-65	2.16.840.1.101.3.4.3.18	FIPS 204
ML-DSA-87	2.16.840.1.101.3.4.3.19	FIPS 204
SLH-DSA-SHA2-128s	2.16.840.1.101.3.4.3.20	FIPS 205
SLH-DSA-SHA2-128f	2.16.840.1.101.3.4.3.21	FIPS 205
SLH-DSA-SHA2-192s	2.16.840.1.101.3.4.3.22	FIPS 205
SLH-DSA-SHA2-192f	2.16.840.1.101.3.4.3.23	FIPS 205
SLH-DSA-SHA2-256s	2.16.840.1.101.3.4.3.24	FIPS 205
SLH-DSA-SHA2-256f	2.16.840.1.101.3.4.3.25	FIPS 205
SLH-DSA-SHAKE-128s	2.16.840.1.101.3.4.3.26	FIPS 205
SLH-DSA-SHAKE-128f	2.16.840.1.101.3.4.3.27	FIPS 205
SLH-DSA-SHAKE-192s	2.16.840.1.101.3.4.3.28	FIPS 205
SLH-DSA-SHAKE-192f	2.16.840.1.101.3.4.3.29	FIPS 205
SLH-DSA-SHAKE-256s	2.16.840.1.101.3.4.3.30	FIPS 205
SLH-DSA-SHAKE-256f	2.16.840.1.101.3.4.3.31	FIPS 205

KEM Algorithm Name	OID	Specification
ML-KEM-512	2.16.840.1.101.3.4.4.1	FIPS 203
ML-KEM-768	2.16.840.1.101.3.4.4.2	FIPS 203
ML-KEM-1024	2.16.840.1.101.3.4.4.3	FIPS 203

KEM Algorithm Name	OID	Specification
bike128	1.3.6.1.4.1.22554.5.8.1	NIST Round 4 -- BouncyCastle
bike192	1.3.6.1.4.1.22554.5.8.2	NIST Round 4 -- BouncyCastle
bike256	1.3.6.1.4.1.22554.5.8.3	NIST Round 4 -- BouncyCastle
hqc128	1.3.6.1.4.1.22554.5.9.1	NIST Round 4 -- BouncyCastle
hqc192	1.3.6.1.4.1.22554.5.9.2	NIST Round 4 -- BouncyCastle
hqc256	1.3.6.1.4.1.22554.5.9.3	NIST Round 4 -- BouncyCastle
mceliece348864	1.3.6.1.4.1.22554.5.1.1	NIST Round 4 -- BouncyCastle
mceliece460896	1.3.6.1.4.1.22554.5.1.3	NIST Round 4 -- BouncyCastle
mceliece6688128	1.3.6.1.4.1.22554.5.1.5	NIST Round 4 -- BouncyCastle
mceliece6960119	1.3.6.1.4.1.22554.5.1.7	NIST Round 4 -- BouncyCastle
mceliece8192128	1.3.6.1.4.1.22554.5.1.9	NIST Round 4 -- BouncyCastle

INTEROPERABLE OID Mapping Tableb- composites

#	Composite Signature AlgorithmID	ObjectID	First Algorithm	Second Algorithm
1	id-MLDSA44-RSA2048-PSS	<CompSig>.21	id-ML-DSA-44	id-RSASA-PSS with id-sha256
2	id-MLDSA44-RSA2048-PKCS15	<CompSig>.22	id-ML-DSA-44	sha256WithRSAEncryption
3	id-MLDSA44-Ed25519	<CompSig>.23	id-ML-DSA-44	id-Ed25519
4	id-MLDSA44-ECDSA-P256	<CompSig>.24	id-ML-DSA-44	ecdsa-with-SHA256 with secp256r1
5	id-MLDSA65-RSA3072-PSS	<CompSig>.26	id-MLDSA65	id-RSASA-PSS with id-sha256
6	id-MLDSA65-RSA3072-PKCS15	<CompSig>.27	id-MLDSA65	sha256WithRSAEncryption
7	id-MLDSA65-RSA4096-PSS	<CompSig>.34	id-MLDSA65	id-RSASA-PSS with id-sha384
8	id-MLDSA65-RSA4096-PKCS15	<CompSig>.35	id-MLDSA65	sha384WithRSAEncryption
9	id-MLDSA65-ECDSA-P384	<CompSig>.28	id-MLDSA65	ecdsa-with-SHA384 with secp384r1
10	id-MLDSA65-ECDSA-brainpoolP256r1	<CompSig>.29	id-MLDSA65	ecdsa-with-SHA256 with brainpoolP256r1
11	id-MLDSA65-Ed25519	<CompSig>.30	id-MLDSA65	id-Ed25519
12	id-MLDSA87-ECDSA-P384	<CompSig>.31	id-MLDSA87	ecdsa-with-SHA384 with secp384r1
13	id-MLDSA87-ECDSA-brainpoolP384r1	<CompSig>.32	id-MLDSA87	ecdsa-with-SHA384 with brainpoolP384r1
14	id-MLDSA87-Ed448	<CompSig>.33	id-MLDSA87	id-Ed448

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	◒			◒		

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!