PQC in X509

IETF 120

20-21 July 2024

Vancouver, Canada

PQC in X.509 interoperability Project

- At the IETF 115 Hackathon a group of people got together to start work on testing the interoperability of the new PQ algorithms in keys, signatures and certificates....
- This plan continues as we get closer to the final PQ Standards
- This project is referenced by the NCCoE

  Interoperability and performance work

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-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

- Built New Github action to automatically unzip uploaded artifacts and run them against the libOQS docker image.
  - Gives instant feedback as to the sanity of the artifacts posted.
- Automation scripts built for building KEMRecipientInfo artifacts
- Petr created a JSON format for the OID list so that it can be used in a more crypto agile manner. Providers are starting to make use of this to ensure their created artifacts use supported OIDs.
- First implementation of Composite KEM! - Thanks Carl
  - Still need to update the KDF function to SHA3 KDF
- Increased scope to include TLS/PQC and Hybrids (Mermaid TLS) to compare performances. No results yet, but we are looking for contributors.

What GOT DONE

- A number of new members joined the group
  - CHT – National Telecom of Taiwan (Abel and Auston) Posted new artifacts and tested interoperability between all existing providers. Found some issues with a few and are sending feedback
  - Joseph Lukefahr – Generated a new ACVP provider using the NIST ACVP implementation and submitted artifacts. Some interoperable testing with other providers done.
  - Lucas prabel – created artifacts for libOQS in preparation for eventual interoperability testing of new algorithm .
  - Conner Ybarra, Sean authelet, Nic Freeman – Joined project, generating artifacts

INTEROPERABLE OID Mapping Table

Signature Algorithm Name	Signature OID	Specification
ML-DSA-44-ipd	1.3.6.1.4.1.2.267.12.4.4	FIPS 204 (Initial Public Draft)
ML-DSA-65-ipd	1.3.6.1.4.1.2.267.12.6.5	FIPS 204 (Initial Public Draft)
ML-DSA-87-ipd	1.3.6.1.4.1.2.267.12.8.7	FIPS 204 (Initial Public Draft)
Falcon-512	1.3.9999.3.6*	NIST Round 3 -- OQS
Falcon-1024	1.3.9999.3.9*	NIST Round 3 -- OQS
SLH-DSA-SHA2-128s-ipd	1.3.9999.6.4.16	FIPS 205 (Initial Public Draft)
SLH-DSA-SHAKE-128s-ipd	1.3.9999.6.7.16	FIPS 205 (Initial Public Draft)
SLH-DSA-SHA2-128f-ipd	1.3.9999.6.4.13	FIPS 205 (Initial Public Draft)
SLH-DSA-SHAKE-128f-ipd	1.3.9999.6.7.13	FIPS 205 (Initial Public Draft)
SLH-DSA-SHA2-192s-ipd	1.3.9999.6.5.12	FIPS 205 (Initial Public Draft)
SLH-DSA-SHAKE-192s-ipd	1.3.9999.6.8.12	FIPS 205 (Initial Public Draft)
SLH-DSA-SHA2-192f-ipd	1.3.9999.6.5.10	FIPS 205 (Initial Public Draft)
SLH-DSA-SHAKE-192f-ipd	1.3.9999.6.8.10	FIPS 205 (Initial Public Draft)
SLH-DSA-SHA2-256s-ipd	1.3.9999.6.6.12	FIPS 205 (Initial Public Draft)
SLH-DSA-SHAKE-256s-ipd	1.3.9999.6.9.12	FIPS 205 (Initial Public Draft)
SLH-DSA-SHA2-256f-ipd	1.3.9999.6.6.10	FIPS 205 (Initial Public Draft)
SLH-DSA-SHAKE-256f-ipd	1.3.9999.6.9.10	FIPS 205 (Initial Public Draft)

KEM Algorithm Name	OID	Specification
ML-KEM-512-ipd	1.3.6.1.4.1.22554.5.6.1	FIPS 203 (Initial Public Draft)
ML-KEM-768-ipd	1.3.6.1.4.1.22554.5.6.2	FIPS 203 (Initial Public Draft)
ML-KEM-1024-ipd	1.3.6.1.4.1.22554.5.6.3	FIPS 203 (Initial Public Draft)

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 Table

Composite Algorithm Name	OID	Specification
MLDSA44-RSA2048-PSS-SHA256	2.16.840.1.114027.80.8.1.1	draft-ounsworth-pq-composite-sigs-13
MLDSA44-RSA2048-PKCS15-SHA256	2.16.840.1.114027.80.8.1.2	draft-ounsworth-pq-composite-sigs-13
MLDSA44-Ed25519-SHA512	2.16.840.1.114027.80.8.1.3	draft-ounsworth-pq-composite-sigs-13
MLDSA44-ECDSA-P256-SHA256	2.16.840.1.114027.80.8.1.4	draft-ounsworth-pq-composite-sigs-13
MLDSA44-ECDSA-brainpoolP256r1-SHA256	2.16.840.1.114027.80.8.1.5	draft-ounsworth-pq-composite-sigs-13
MLDSA65-RSA3072-PSS-SHA512	2.16.840.1.114027.80.8.1.6	draft-ounsworth-pq-composite-sigs-13
MLDSA65-RSA3072-PKCS15-SHA512	2.16.840.1.114027.80.8.1.7	draft-ounsworth-pq-composite-sigs-13
MLDSA65-ECDSA-P256-SHA512	2.16.840.1.114027.80.8.1.8	draft-ounsworth-pq-composite-sigs-13
MLDSA65-ECDSA-brainpoolP256r1-SHA512	2.16.840.1.114027.80.8.1.9	draft-ounsworth-pq-composite-sigs-13
MLDSA65-Ed25519-SHA512	2.16.840.1.114027.80.8.1.10	draft-ounsworth-pq-composite-sigs-13
MLDSA87-ECDSA-P384-SHA512	2.16.840.1.114027.80.8.1.11	draft-ounsworth-pq-composite-sigs-13
MLDSA87-ECDSA-brainpoolP384r1-SHA512	2.16.840.1.114027.80.8.1.12	draft-ounsworth-pq-composite-sigs-13
MLDSA87-Ed448-SHA512	2.16.840.1.114027.80.8.1.13	draft-ounsworth-pq-composite-sigs-13

KEM Algorithm Name	OID	Specification
NTRUHPS2048677	1.3.6.1.4.1.22554.5.5.2	NIST Round 3 -- BouncyCastle
NTRUHPS4096821	1.3.6.1.4.1.22554.5.5.3	NIST Round 3 -- BouncyCastle

Composite Algorithm Name	OID	Specification
MLKEM512-ECDH-P256-KMAC128	2.16.840.1.114027.80.5.2.1	draft-ietf-lamps-pq-composite-kem-03
MLKEM512-ECDH-brainpoolP256r1-KMAC128	2.16.840.1.114027.80.5.2.2	draft-ietf-lamps-pq-composite-kem-03
MLKEM512-X25519-KMAC128	2.16.840.1.114027.80.5.2.3	draft-ietf-lamps-pq-composite-kem-03
MLKEM512-RSA2048-KMAC128	2.16.840.1.114027.80.5.2.13	draft-ietf-lamps-pq-composite-kem-03
MLKEM512-RSA3072-KMAC128	2.16.840.1.114027.80.5.2.4	draft-ietf-lamps-pq-composite-kem-03
MLKEM768-ECDH-P256-KMAC256	2.16.840.1.114027.80.5.2.5	draft-ietf-lamps-pq-composite-kem-03
MLKEM768-ECDH-brainpoolP256r1-KMAC256	2.16.840.1.114027.80.5.2.6	draft-ietf-lamps-pq-composite-kem-03
MLKEM768-X25519-KMAC256	2.16.840.1.114027.80.5.2.7	draft-ietf-lamps-pq-composite-kem-03
MLKEM1024-ECDH-P384-KMAC256	2.16.840.1.114027.80.5.2.8	draft-ietf-lamps-pq-composite-kem-03
MLKEM1024-ECDH-brainpoolP384r1-KMAC256	2.16.840.1.114027.80.5.2.9	draft-ietf-lamps-pq-composite-kem-03
MLKEM1024-X448-KMAC256	2.16.840.1.114027.80.5.2.10	draft-ounsworth-pq-composite-sigs-13

Compatibility matrix Sample

-	bc	bc_old	botan	carl-redhound	corey-digicert	cryptonext	cryptonext-cnsprovider	entrust	isi-wolfssl	kris	openca	oqs-gnutls	oqs-openssl111	oqs-provider
ecPublicKey						✅	✅							
rsaEncryption						✅	✅							
ED448							✅							✅
ML-DSA-44-ipd	✅			✅	✅	✅	✅			✅				
ML-DSA-65-ipd	✅			✅	✅	✅	✅			✅				
ML-DSA-87-ipd	✅			✅	✅	✅	✅			✅				
~~Dilithium2~~	✅		✅	✅	✅	✅	✅	✅		✅	✅		✅	✅
~~Dilithium3~~	✅		✅	✅	✅	✅	✅	✅		✅	✅	✅	✅	✅
~~Dilithium5~~	✅		✅	✅	✅	✅	✅	✅		✅	✅		✅	✅
NTRUHPS2048677	✅													
NTRUHPS4096821	✅													
1.3.6.1.4.1.22554.5.5.4	✅													
ML-KEM-512-ipd	✅				✅	✅	✅							
ML-KEM-768-ipd	✅				✅	✅	✅							
ML-KEM-1024-ipd	✅				✅	✅	✅							
~~kyber512_shake~~						✅	✅							
~~kyber768_shake~~						✅	✅							
~~kyber1024_shake~~						✅	✅							
1.3.6.1.4.1.59634.9999.2.2.1						✅								
1.3.6.1.4.1.59634.9999.2.2.2						✅								
1.3.6.1.4.1.59634.9999.2.2.3						✅								
1.3.9999.2.7.2						✅								
1.3.9999.2.7.4						✅								
~~Falcon-512~~	✅			✅	✅	✅	✅	✅		✅	✅		✅	✅
~~Falcon-1024~~	✅			✅	✅	✅	✅	✅		✅	✅		✅	✅
Falcon-512	✅			✅	✅			✅		✅				✅
Falcon-1024	✅			✅	✅			✅		✅				✅
SLH-DSA-SHA2-128f-ipd	✅			✅	✅		✅	✅						✅
SLH-DSA-SHA2-128s-ipd	✅			✅	✅		✅	✅						✅

..

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 others

FIRST TIMERS

- Lucas prabel, Joseph LukeFahr, Ab
  C.H. Chen, Austin CHT, Roy Basmatir, Conner Ybarra, Nic Freeman, Sean Authlet

NEXT STEPS

- Monthly meetings to continue progress – Next meeting is **Tuesda**
  August 6th
- Virtual Interim Hackathon (September?)
- Final NIST Algorithms coming!

JOIN US!

Contact John.gray@entrust.com to join!