PQ in X.509

IETF 123
18–19 July 2025
Madrid, Spain

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/
  - RFC 9629
  - draft-ietf-lamps-pq-composite-sigs/
  - draft-ietf-lamps-pq-composite-kem/
  - RFC 9763
  - draft-ietf-lamps-certdiscovery
  - draft-ounsworth-lamps-pq-external-pubkeys/
  - draft-ietf-lamps-rfc4210bis
  - draft-ounsworth-cfrg-kem-combiners
  - draft-ietf-lamps-cms-kyber

What got done

- General Maintenance updates to the repository
  - Updated the OID list to align with the latest drafts
  - Clarified wording on artifact formats
  - Remove Open Quantum Safe as an automated verifier
    - it is a research library
- Much MORE discussion on composite key format (ASN.1 SEQUENCE vs byte encoding).
  - Multiple implementations of latest composite key formats completed.

What got done

- Added or updated test artifacts and verified others artifacts:
  - Seventh Sense AI added new artifacts into the repository (Zhao Peiduo)
  - SafeLogic added brand new artifacts to the repository (Alex Zaslavsky)
  - Crypto4a added new artifacts to the repository (JP Fiset)
  - CHT Added Composite Signatures artifacts into the repository (James Tung)
  - Redhound added new Composite Signatures artifacts into repository (Carl Wallace)
  - CryptoNext updated artifacts tests (Dan Van Geest)
  - Composite reference implementation added _priv der files (Mike Ounsworth)
  - Composite KEM reference implementation artifact files added (Stepan Yakimovich)

What we learned

- Implementing the composite key formats in version -07 was found to be straight forward, and easier for people who had implemented earlier versions
- Many crypto libraries still do not yet support the seed format

Manual Compatibility Matrix Results

-- PQ Signatures

✅ = 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	composite-ref-impl	composite-sigs-ref-impl	corey-digicert	crypto4a	cryptonext	entrust	ossl35	safelogic	seventhsense.ai
Falcon-1024-cert	✅ 1/1							✅ 1/1	✅ 1/1			
Falcon-1024-consistent	○ 0/1							✅ 1/1	○ 0/1			
Falcon-1024-priv	○ 0/1							✅ 1/1	○ 0/1			
ML-DSA-44-both	✅ 4/4	✅ 5/5	✅ 2/2			✅ 5/5	✅ 5/5	✅ 5/5		✅ 5/5	✅ 1/1	○ 0/1
ML-DSA-44-cert	✅ 4/4	✅ 4/4	✅ 1/1	✅ 1/1		✅ 4/4	✅ 4/4	✅ 4/4	✅ 4/4	✅ 4/4	✅ 1/1	
ML-DSA-44-consistent	✅ 3/3	✅ 3/3				✅ 3/3	✅ 3/3	✅ 3/3	◒ 1/2	✅ 3/3	✅ 1/1	
ML-DSA-44-expandedkey	✅ 5/5	✅ 5/5	✅ 2/2			✅ 5/5		✅ 5/5	◒ 2/5	✅ 5/5	✅ 2/2	○ 0/1
ML-DSA-44-priv					✅ 1/1							
ML-DSA-44-seed	✅ 4/4	✅ 4/4	✅ 2/2			✅ 4/4		✅ 4/4		✅ 4/4	✅ 1/1	○ 0/1
ML-DSA-65-both	✅ 4/4	✅ 5/5	✅ 2/2			✅ 5/5	✅ 5/5	✅ 5/5		✅ 5/5	✅ 1/1	○ 0/1
ML-DSA-65-cert	✅ 4/4	✅ 4/4	✅ 1/1			✅ 4/4	✅ 4/4	✅ 4/4	✅ 4/4	✅ 4/4	✅ 1/1	
ML-DSA-65-consistent	✅ 3/3	✅ 3/3				✅ 3/3	✅ 3/3	✅ 3/3	◒ 1/2	✅ 3/3	✅ 1/1	
ML-DSA-65-expandedkey	✅ 5/5	✅ 5/5	✅ 2/2			✅ 5/5		✅ 5/5	◒ 2/5	✅ 5/5	✅ 2/2	○ 0/1
ML-DSA-65-priv					✅ 1/1							
ML-DSA-65-seed	✅ 4/4	✅ 4/4	✅ 2/2			✅ 4/4		✅ 4/4		✅ 4/4	✅ 1/1	○ 0/1
ML-DSA-87-both	✅ 4/4	✅ 5/5	✅ 2/2			✅ 5/5	✅ 5/5	✅ 5/5		✅ 5/5	✅ 1/1	○ 0/1
ML-DSA-87-cert	✅ 4/4	✅ 4/4	✅ 1/1			✅ 4/4	✅ 4/4	✅ 4/4	✅ 4/4	✅ 4/4	✅ 1/1	
ML-DSA-87-consistent	✅ 3/3	✅ 3/3				✅ 3/3	✅ 3/3	✅ 3/3	◒ 1/2	✅ 3/3	✅ 1/1	
ML-DSA-87-expandedkey	✅ 5/5	✅ 5/5	✅ 2/2			✅ 5/5		✅ 5/5	✅ 1/1	✅ 5/5	✅ 2/2	○ 0/1
ML-DSA-87-priv					✅ 1/1				◒ 1/3			
ML-DSA-87-seed	✅ 4/4	✅ 4/4	✅ 2/2			✅ 4/4		✅ 4/4		✅ 4/4	✅ 1/1	○ 0/1
SLH-DSA-SHA2-128s-both												✅ 1/1
SLH-DSA-SHA2-128s-cert	✅ 4/4	✅ 4/4	✅ 1/1					✅ 4/4		✅ 4/4		
SLH-DSA-SHA2-128s-consistent	✅ 3/3	✅ 3/3						✅ 3/3		✅ 3/3		
SLH-DSA-SHA2-128s-expandedkey												✅ 1/1
SLH-DSA-SHA2-128s-priv	✅ 5/5	✅ 5/5	✅ 2/2				✅ 1/1	✅ 5/5		✅ 5/5		
SLH-DSA-SHA2-128s-seed												✅ 1/1
SLH-DSA-SHA2-128f-both												✅ 1/1
SLH-DSA-SHA2-128f-cert	✅ 4/4	✅ 4/4	✅ 1/1					✅ 4/4		✅ 4/4		
SLH-DSA-SHA2-128f-consistent	✅ 3/3	✅ 3/3						✅ 3/3		✅ 3/3		
SLH-DSA-SHA2-128f-expandedkey												✅ 1/1
SLH-DSA-SHA2-128f-priv	✅ 5/5	✅ 5/5	✅ 2/2				✅ 1/1	✅ 5/5		✅ 5/5		
SLH-DSA-SHA2-128f-seed												✅ 1/1
SLH-DSA-SHA2-192s-both												✅ 1/1

Manual Compatibility Matrix Results

-- PQ Signatures

✅ = 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.

Click On Link

-	bc	carl-redhound	cht	composite-ref-impl	composite-sigs-ref-impl	corey-digicert	crypto4a	cryptonext	entrust	ossl35	safelogic	seventhsense.ai
Falcon-1024-cert	✅ 1/1							✅ 1/1	✅ 1/1			
Falcon-1024-consistent	○ 0/1							✅ 1/1	○ 0/1			
Falcon-1024-priv								✅ 1/1	○ 0/1			
ML-DSA-44-both							5/5	✅ 5/5		✅ 5/5	✅ 1/1	○ 0/1
ML-DSA-44-cert							4/4	✅ 4/4	✅ 4/4	✅ 4/4	✅ 1/1	
ML-DSA-44-consistent							3/3	✅ 3/3	◒ 1/2	✅ 3/3	✅ 1/1	
ML-DSA-44-expandedkey								✅ 5/5	◒ 2/5	✅ 5/5	✅ 2/2	○ 0/1
ML-DSA-44-priv												
ML-DSA-44-seed								✅ 4/4		✅ 4/4	✅ 1/1	○ 0/1
ML-DSA-65-both							5/5	✅ 5/5		✅ 5/5	✅ 1/1	○ 0/1
ML-DSA-65-cert							4/4	✅ 4/4	✅ 4/4	✅ 4/4	✅ 1/1	
ML-DSA-65-consistent							3/3	✅ 3/3	◒ 1/2	✅ 3/3	✅ 1/1	
ML-DSA-65-expandedkey								✅ 5/5	◒ 2/5	✅ 5/5	✅ 2/2	○ 0/1
ML-DSA-65-priv												
ML-DSA-65-seed								✅ 4/4		✅ 4/4	✅ 1/1	○ 0/1
ML-DSA-87-both							5/5	✅ 5/5		✅ 5/5	✅ 1/1	○ 0/1
ML-DSA-87-cert							4/4	✅ 4/4	✅ 4/4	✅ 4/4	✅ 1/1	
ML-DSA-87-consistent							3/3	✅ 3/3	◒ 1/2	✅ 3/3	✅ 1/1	
ML-DSA-87-expandedkey								✅ 5/5	✅ 1/1	✅ 5/5	✅ 2/2	○ 0/1
ML-DSA-87-priv									◒ 1/3			
ML-DSA-87-seed								✅ 4/4		✅ 4/4	✅ 1/1	○ 0/1
SLH-DSA-SHA2-128s-both												✅ 1/1
SLH-DSA-SHA2-128s-cert	✅ 4/4	✅ 4/4	✅ 1/1					✅ 4/4		✅ 4/4		
SLH-DSA-SHA2-128s-consistent	✅ 3/3	✅ 3/3						✅ 3/3		✅ 3/3		
SLH-DSA-SHA2-128s-expandedkey												✅ 1/1
SLH-DSA-SHA2-128s-priv	✅ 5/5	✅ 5/5	✅ 2/2				✅ 1/1	✅ 5/5		✅ 5/5		
SLH-DSA-SHA2-128s-seed												✅ 1/1
SLH-DSA-SHA2-128f-both												✅ 1/1
SLH-DSA-SHA2-128f-cert	✅ 4/4	✅ 4/4	✅ 1/1					✅ 4/4		✅ 4/4		
SLH-DSA-SHA2-128f-consistent	✅ 3/3	✅ 3/3						✅ 3/3		✅ 3/3		
SLH-DSA-SHA2-128f-expandedkey												✅ 1/1
SLH-DSA-SHA2-128f-priv	✅ 5/5	✅ 5/5	✅ 2/2				✅ 1/1	✅ 5/5		✅ 5/5		
SLH-DSA-SHA2-128f-seed												✅ 1/1
SLH-DSA-SHA2-192s-both												✅ 1/1

ML-DSA-44-cert (2.16.840.1.101.3.4.3.17-cert)

Rows are producers. Columns are parsers.

-	carl-redhound	cht	crypto4a	cryptonext	ossl35	safelogic
bc	✅	✅		✅	✅	✅
carl-redhound	✅	✅		✅	✅	✅
cht		✅		✅		
composite-kem-ref-impl						
composite-ref-impl		✅				
composite-sigs-ref-impl				✅		
corey-digicert	✅	✅		✅	✅	✅
crypto4a	✅	✅		✅	✅	✅
cryptonext	✅	✅		✅	✅	❌
entrust	✅	✅		✅	✅	❌
ossl35	✅	✅		✅	✅	✅
safelogic	✅			✅		
seventhsense.ai				✅		

Manual Compatibility Matrix Results

-- ML KEM

✅ = 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	composite-kem-ref-impl	composite-ref-impl	composite-sigs-ref-impl	corey-digicert	crypto4a	cryptonext	entrust	ossl35	safelogic	seventhsense.ai
ML-KEM-512-both	✅ 3/3		◒ 1/2						✅ 4/4		✅ 4/4		
ML-KEM-512-cert	✅ 4/4		✅ 2/2						✅ 4/4		✅ 4/4		✅ 1/1
ML-KEM-512-consistent	✅ 3/3		✅ 1/1						✅ 3/3		✅ 3/3		✅ 1/1
ML-KEM-512-expandedkey	✅ 4/4		◒ 1/2						✅ 4/4		✅ 4/4		
ML-KEM-512-priv													○ 0/1
ML-KEM-512-seed	✅ 4/4		◒ 1/2						✅ 4/4		✅ 4/4		
ML-KEM-768-both	✅ 3/3		◒ 1/2						✅ 4/4		✅ 4/4		
ML-KEM-768-cert	✅ 4/4		✅ 2/2	✅ 1/1					✅ 4/4		✅ 4/4		✅ 1/1
ML-KEM-768-consistent	✅ 3/3		✅ 1/1	✅ 1/1					✅ 3/3		✅ 3/3		✅ 1/1
ML-KEM-768-expandedkey	✅ 4/4		◒ 1/2						✅ 4/4		✅ 4/4		
ML-KEM-768-priv				✅ 1/1									○ 0/1
ML-KEM-768-seed	✅ 4/4		◒ 1/2						✅ 4/4		✅ 4/4		
ML-KEM-1024-both	✅ 3/3		◒ 1/2						✅ 4/4		✅ 4/4		
ML-KEM-1024-cert	✅ 4/4		✅ 2/2	✅ 1/1					✅ 4/4		✅ 4/4		✅ 1/1
ML-KEM-1024-consistent	✅ 3/3		✅ 1/1	✅ 1/1					✅ 3/3		✅ 3/3		✅ 1/1
ML-KEM-1024-expandedkey	✅ 4/4		◒ 1/2						✅ 4/4		✅ 4/4		
ML-KEM-1024-priv				✅ 1/1									○ 0/1
ML-KEM-1024-seed	✅ 4/4		◒ 1/2						✅ 4/4		✅ 4/4		

Manual Compatibility Matrix Results

✅ = 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.

-- Composite KEM

-	bc	carl-redhound	cht	composite-kem-ref-impl	composite-ref-impl	composite-sigs-ref-impl	corey-digicert	crypto4a	cryptonext	entrust	ossl35	safelogic	seventhsense.ai
id-MLKEM768-RSA2048-HMAC-SHA256-cert				✅ 1/1					✅ 1/1				
id-MLKEM768-RSA2048-HMAC-SHA256-consistent				✅ 1/1					✅ 1/1				
id-MLKEM768-RSA2048-HMAC-SHA256-priv				✅ 1/1					✅ 1/1				
id-MLKEM768-RSA3072-HMAC-SHA256-cert				✅ 1/1					✅ 1/1				
id-MLKEM768-RSA3072-HMAC-SHA256-consistent				✅ 1/1					✅ 1/1				
id-MLKEM768-RSA3072-HMAC-SHA256-priv				✅ 1/1					✅ 1/1				
id-MLKEM768-RSA4096-HMAC-SHA256-cert				✅ 1/1					✅ 1/1				
id-MLKEM768-RSA4096-HMAC-SHA256-consistent				✅ 1/1					✅ 1/1				
id-MLKEM768-RSA4096-HMAC-SHA256-priv				✅ 1/1					✅ 1/1				
id-MLKEM768-X25519-SHA3-256-cert				✅ 1/1					✅ 1/1				
id-MLKEM768-X25519-SHA3-256-consistent				✅ 1/1					✅ 1/1				
id-MLKEM768-X25519-SHA3-256-priv				✅ 1/1					✅ 1/1				
id-MLKEM768-ECDH-P256-HMAC-SHA256-cert				✅ 1/1					✅ 1/1				
id-MLKEM768-ECDH-P256-HMAC-SHA256-consistent				✅ 1/1					✅ 1/1				
id-MLKEM768-ECDH-P256-HMAC-SHA256-priv				✅ 1/1					✅ 1/1				
id-MLKEM768-ECDH-P384-HMAC-SHA256-cert				✅ 1/1					✅ 1/1				
id-MLKEM768-ECDH-P384-HMAC-SHA256-consistent				✅ 1/1					✅ 1/1				
id-MLKEM768-ECDH-P384-HMAC-SHA256-priv				✅ 1/1					✅ 1/1				
id-MLKEM768-ECDH-brainpoolP256r1-HMAC-SHA256-cert				✅ 1/1					✅ 1/1				
id-MLKEM768-ECDH-brainpoolP256r1-HMAC-SHA256-consistent				✅ 1/1					✅ 1/1				
id-MLKEM768-ECDH-brainpoolP256r1-HMAC-SHA256-priv				✅ 1/1					✅ 1/1				
id-MLKEM1024-ECDH-P384-HMAC-SHA512-cert				✅ 1/1					✅ 1/1				
id-MLKEM1024-ECDH-P384-HMAC-SHA512-consistent				✅ 1/1					✅ 1/1				
id-MLKEM1024-ECDH-P384-HMAC-SHA512-priv				✅ 1/1					✅ 1/1				
id-MLKEM1024-ECDH-brainpoolP384r1-HMAC-SHA512-cert				✅ 1/1					✅ 1/1				
id-MLKEM1024-ECDH-brainpoolP384r1-HMAC-SHA512-consistent				✅ 1/1					✅ 1/1				
id-MLKEM1024-ECDH-brainpoolP384r1-HMAC-SHA512-priv				✅ 1/1					✅ 1/1				
id-MLKEM1024-X448-SHA3-256-cert				✅ 1/1					✅ 1/1				
id-MLKEM1024-X448-SHA3-256-consistent				✅ 1/1					✅ 1/1				
id-MLKEM1024-X448-SHA3-256-priv				✅ 1/1					✅ 1/1				
id-MLKEM1024-ECDH-P521-HMAC-SHA512-cert				✅ 1/1					✅ 1/1				
id-MLKEM1024-ECDH-P521-HMAC-SHA512-consistent				✅ 1/1					✅ 1/1				
id-MLKEM1024-ECDH-P521-HMAC-SHA512-priv				✅ 1/1					✅ 1/1				
id-MLKEM1024-RSA3072-HMAC-SHA512-cert				✅ 1/1					✅ 1/1				
id-MLKEM1024-RSA3072-HMAC-SHA512-consistent				✅ 1/1					✅ 1/1				
id-MLKEM1024-RSA3072-HMAC-SHA512-priv				✅ 1/1					✅ 1/1				

Automated Results

-- Signatures

✅ = 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	composite-sigs-ref-impl	corey-digicert	crypto4a	cryptonext	entrust	ossl35	safelogic	seventhsense.ai
Falcon-1024-cert	◒ 1/2						○ 0/2	◒ 1/2			
ML-DSA-44-cert	✅ 3/3	✅ 3/3	✅ 3/3	✅ 3/3	✅ 3/3	✅ 3/3	✅ 3/3	◒ 2/3	✅ 3/3	✅ 3/3	✅ 3/3
ML-DSA-65-cert	✅ 3/3	✅ 3/3	✅ 3/3	✅ 3/3	✅ 3/3	✅ 3/3	✅ 3/3	◒ 2/3	✅ 3/3	✅ 3/3	✅ 3/3
ML-DSA-87-cert	✅ 3/3	✅ 3/3	✅ 3/3	✅ 3/3	✅ 3/3	✅ 3/3	✅ 3/3	◒ 2/3	✅ 3/3	✅ 3/3	✅ 3/3
SLH-DSA-SHA2-128s-cert	✅ 2/2	✅ 2/2	✅ 2/2			✅ 2/2	✅ 2/2		✅ 2/2		✅ 2/2
SLH-DSA-SHA2-128f-cert	✅ 2/2	✅ 2/2	✅ 2/2			✅ 2/2	✅ 2/2		✅ 2/2		✅ 2/2
SLH-DSA-SHA2-192s-cert	✅ 2/2	✅ 2/2	✅ 2/2			✅ 2/2	✅ 2/2		✅ 2/2		✅ 2/2
SLH-DSA-SHA2-192f-cert	✅ 2/2	✅ 2/2	✅ 2/2			✅ 2/2	✅ 2/2		✅ 2/2		✅ 2/2
SLH-DSA-SHA2-256s-cert	✅ 2/2	✅ 2/2	✅ 2/2			✅ 2/2	✅ 2/2		✅ 2/2		✅ 2/2
SLH-DSA-SHA2-256f-cert	✅ 2/2	✅ 2/2	✅ 2/2			✅ 2/2	✅ 2/2		✅ 2/2		✅ 2/2
SLH-DSA-SHAKE-128s-cert	✅ 2/2	✅ 2/2	✅ 2/2			✅ 2/2	✅ 2/2		✅ 2/2		✅ 2/2
SLH-DSA-SHAKE-128f-cert	✅ 2/2	✅ 2/2	✅ 2/2			✅ 2/2	✅ 2/2		✅ 2/2		✅ 2/2
SLH-DSA-SHAKE-192s-cert	✅ 2/2	✅ 2/2	✅ 2/2			✅ 2/2	✅ 2/2		✅ 2/2		✅ 2/2
SLH-DSA-SHAKE-192f-cert	✅ 2/2	✅ 2/2	✅ 2/2			✅ 2/2	✅ 2/2		✅ 2/2		✅ 2/2
SLH-DSA-SHAKE-256s-cert	✅ 2/2	✅ 2/2	✅ 2/2			✅ 2/2	✅ 2/2		✅ 2/2		✅ 2/2
SLH-DSA-SHAKE-256f-cert	✅ 2/2	✅ 2/2	✅ 2/2			✅ 2/2	✅ 2/2		✅ 2/2		✅ 2/2
HASH-ML-DSA-44-cert	✅ 2/2		✅ 2/2		✅ 2/2	✅ 2/2	✅ 2/2				✅ 2/2
HASH-ML-DSA-65-cert	✅ 2/2		✅ 2/2		✅ 2/2	✅ 2/2	✅ 2/2				✅ 2/2
HASH-ML-DSA-87-cert	✅ 2/2		✅ 2/2		✅ 2/2	✅ 2/2	✅ 2/2				✅ 2/2
HASH-SLH-DSA-SHA2-128s-cert	✅ 2/2		✅ 2/2			✅ 2/2	✅ 2/2				✅ 2/2
HASH-SLH-DSA-SHA2-128f-cert	✅ 2/2		✅ 2/2			✅ 2/2	✅ 2/2				✅ 2/2
HASH-SLH-DSA-SHA2-192s-cert	✅ 2/2		✅ 2/2			✅ 2/2	✅ 2/2				✅ 2/2
HASH-SLH-DSA-SHA2-192f-cert	✅ 2/2		✅ 2/2			✅ 2/2	✅ 2/2				✅ 2/2
HASH-SLH-DSA-SHA2-256s-cert	✅ 2/2		✅ 2/2			✅ 2/2	✅ 2/2				✅ 2/2
HASH-SLH-DSA-SHA2-256f-cert	✅ 2/2		✅ 2/2			✅ 2/2	✅ 2/2				✅ 2/2
HASH-SLH-DSA-SHAKE-128s-cert	✅ 2/2		✅ 2/2			✅ 2/2	✅ 2/2				✅ 2/2
HASH-SLH-DSA-SHAKE-128f-cert	✅ 2/2		✅ 2/2			✅ 2/2	✅ 2/2				✅ 2/2
HASH-SLH-DSA-SHAKE-192s-cert	✅ 2/2		✅ 2/2			✅ 2/2	✅ 2/2				✅ 2/2
HASH-SLH-DSA-SHAKE-192f-cert	✅ 2/2		✅ 2/2			✅ 2/2	✅ 2/2				✅ 2/2
HASH-SLH-DSA-SHAKE-256s-cert	✅ 2/2		✅ 2/2			✅ 2/2	✅ 2/2				✅ 2/2
HASH-SLH-DSA-SHAKE-256f-cert	✅ 2/2		✅ 2/2			✅ 2/2	✅ 2/2				✅ 2/2
id-MLDSA44-RSA2048-PSS-SHA256-cert		○ 0/3		◒ 1/3							
id-MLDSA44-RSA2048-PKCS15-SHA256-cert		○ 0/3		◒ 1/3							

Automated Results

-- Composite Signatures

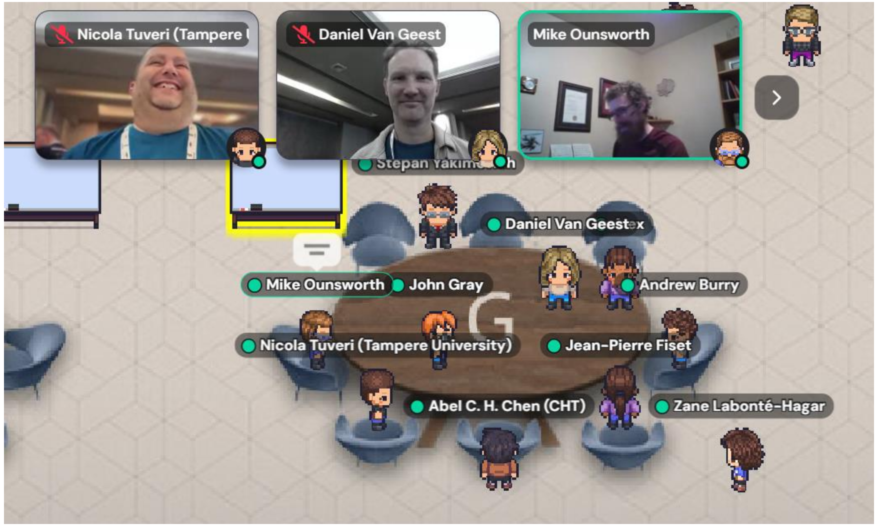
✅ = passing all verifiers
◒ = passing some verifiers
○ = not passing any verifiers
Columns represent producers who submitted artifacts. Verifiers are not listed in this table, but are listed in the broken-out tables below.

-	bc	carl-redhound	cht	composite-sigs-ref-impl	corey-digicert	crypto4a	cryptonext	entrust	ossl35	safelogic	seventhsense.ai
id-MLDSA44-RSA2048-PSS-SHA256-cert		○ 0/3		◒ 1/3							
id-MLDSA44-RSA2048-PKCS15-SHA256-cert		○ 0/3		◒ 1/3							
id-MLDSA65-ECDSA-brainpoolP256r1-SHA512-cert				◒ 1/3							
id-MLDSA65-Ed25519-SHA512-cert		○ 0/3		◒ 1/3							
id-MLDSA87-ECDSA-P384-SHA512-cert		○ 0/3		◒ 1/3							
id-MLDSA87-ECDSA-brainpoolP384r1-SHA512-cert				◒ 1/3							
id-MLDSA87-Ed448-SHAKE256-cert				◒ 1/3							
id-MLDSA87-RSA3072-PSS-SHA512-cert		○ 0/3		◒ 1/3							
id-MLDSA87-RSA4096-PSS-SHA512-cert		○ 0/3		◒ 1/3							
id-MLDSA87-ECDSA-P521-SHA512-cert		○ 0/3		◒ 1/3							
id-MLDSA44-Ed25519-SHA512-cert		○ 0/3		◒ 1/3							
id-MLDSA44-ECDSA-P256-SHA256-cert		○ 0/3		◒ 1/3							
id-MLDSA65-RSA3072-PSS-SHA512-cert		○ 0/3		◒ 1/3							
id-MLDSA65-RSA3072-PKCS15-SHA512-cert				◒ 1/3							
id-MLDSA65-RSA4096-PSS-SHA512-cert		○ 0/3		◒ 1/3							
id-MLDSA65-RSA4096-PKCS15-SHA512-cert		○ 0/3		◒ 1/3							
id-MLDSA65-ECDSA-P256-SHA512-cert		○ 0/3		◒ 1/3							
id-MLDSA65-ECDSA-P384-SHA512-cert		○ 0/3		◒ 1/3							

PQ in X.509 – Summary

TEAM MEMBERS

- Michael Baentsch, Alie Becker, Corey 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, Zhao Peiduo, Nicola Tuveri, Dan Van Geest, Jean-Pierre Fiset, Viktor Dukhovni, Tim Hudson, others



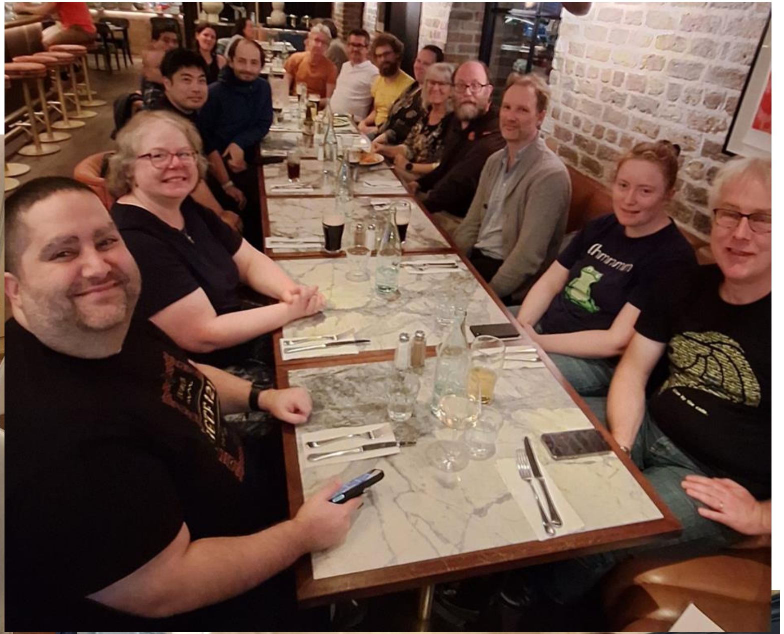
FIRST TIMERS

- Alex Zaslavsky, Stepan Yakimovich, Andrew Burry, Zane Labonte-hagar

NEXT STEPS

- Monthly meetings to continue progress – Next meeting is **Tuesday September 9th**
- Github: https://github.com/IETF-Hackathon/pqc-certificates

JOIN US!



Contact John.gray@entrust.com to join!