PQ in X.509

IETF 124
1-2 Nov 2025
Montreal, Canada

IETF

PQC in X.509 interoperability Project

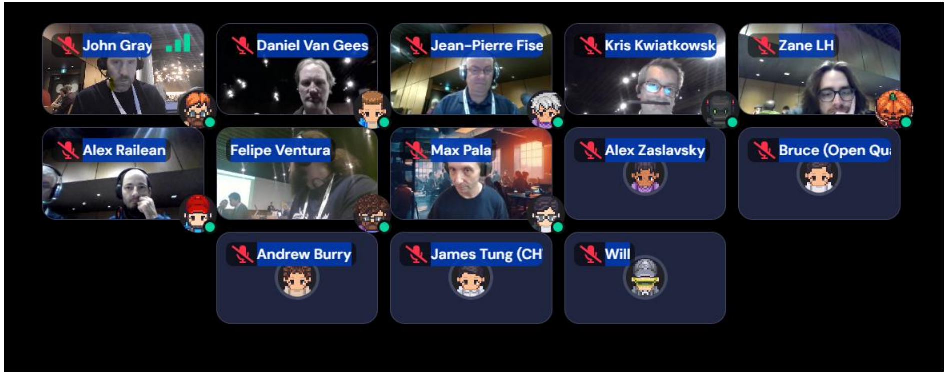
- Goals:
  - Adding PQ algorithm support into existing X.509 structures (keys, signatures, certificates and protocols)
  - Test interoperability between different algorithm implementations
  - Gain experience using PQ algorithms
  - Provide feedback to the standards groups about practical usage

- Drafts

- RFC 9881
- 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/
- RFC 9810
- draft-ounsworth-cfrg-kem-combiners
- draft-ietf-lamps-cms-kyber

What got done

- Lots of interoperability Testing on Composite Signatures (Official OID assignments)
  - Max/Felipe – collaborative OpenSSL implementation
  - Dan – cryptoNext
  - JP, Zane, Will and Andrew – Crypto4a
  - John - Entrust
  - James T – CHT
  - Alex Z - Safelogic
- Composite KEM Testings
  - Dan / Carl



What got done

- General Maintenance updates to the repository
  - Updated the OID list to align with the latest drafts
- CMP Test Suite augmentation
  - Alex R / John
- Statistical analysis of rejection sampling in ML-DSA
  - Kris – PQShield
- Automated CMS test suite (Signatures and KEMs)

What we learned

- Implementing the composite key formats in version -13 was found to be relatively easy, dealing with crypto library specific implementations was the most difficult.
- The composite KEM private key format is a "bit annoying" because it includes the public key.

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

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

Rows are producers. Columns are parsers.

-	bc	composite-ref-impl	openssl	ssai
bc	✅	✅	✅	✅
carl-redhound	✅	✅	✅	✅
cht	✅	✅	✅	✅
composite-kem-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-sigs-ref-impl	corey-digicert	crypto4a	cryptonext	entrust	ossl35	safelogic	seventhsense.ai
ML-KEM-512-both	✅ 1/1		○ 0/1				✅ 1/1	✅ 1/1		✅ 1/1		
ML-KEM-512-cert	✅ 2/2		✅ 1/1				✅ 1/1	✅ 2/2		✅ 2/2		✅ 1/1
ML-KEM-512-consistent	✅ 1/1		✅ 1/1				✅ 1/1	✅ 1/1		✅ 1/1		
ML-KEM-512-expandedkey	✅ 1/1		○ 0/1					✅ 1/1		✅ 1/1		
ML-KEM-512-seed	✅ 2/2		○ 0/1					✅ 2/2		✅ 2/2		
ML-KEM-768-both	✅ 1/1		○ 0/1				✅ 1/1	✅ 1/1		✅ 1/1		
ML-KEM-768-cert	✅ 2/2		✅ 1/1	✅ 2/2			✅ 1/1	✅ 2/2		✅ 2/2		✅ 1/1
ML-KEM-768-consistent	✅ 1/1		✅ 1/1				✅ 1/1	✅ 1/1		✅ 1/1		
ML-KEM-768-expandedkey	✅ 1/1		○ 0/1					✅ 1/1		✅ 1/1		
ML-KEM-768-seed	✅ 2/2		○ 0/1					✅ 2/2		✅ 2/2		
ML-KEM-1024-both	✅ 1/1		○ 0/1				✅ 1/1	✅ 1/1		✅ 1/1		
ML-KEM-1024-cert	✅ 2/2		✅ 1/1	✅ 2/2			✅ 1/1	✅ 2/2		✅ 2/2		✅ 1/1
ML-KEM-1024-consistent	✅ 1/1		✅ 1/1				✅ 1/1	✅ 1/1		✅ 1/1		
ML-KEM-1024-expandedkey	✅ 1/1		○ 0/1					✅ 1/1		✅ 1/1		
ML-KEM-1024-seed	✅ 2/2		○ 0/1					✅ 2/2		✅ 2/2		

Automated Results

-- Composite 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-sigs-ref-impl	corey-digicert	crypto4a	cryptonext	entrust	ossl35	safelogic	seventhsense.ai
id-MLKEM768-RSA2048-SHA3-256-cert				✅ 1/1				✅ 1/1				
id-MLKEM768-RSA3072-SHA3-256-cert				✅ 1/1				✅ 1/1				
id-MLKEM768-RSA4096-SHA3-256-cert				✅ 1/1				✅ 1/1				
id-MLKEM768-X25519-SHA3-256-cert				✅ 1/1				✅ 1/1				
id-MLKEM768-ECDH-P256-SHA3-256-cert				✅ 1/1				✅ 1/1				
id-MLKEM768-ECDH-P384-SHA3-256-cert				✅ 1/1				✅ 1/1				
id-MLKEM768-ECDH-brainpoolP256r1-SHA3-256-cert				✅ 1/1				✅ 1/1				
id-MLKEM1024-RSA3072-SHA3-256-cert				✅ 1/1				✅ 1/1				
id-MLKEM1024-ECDH-P384-SHA3-256-cert				✅ 1/1				✅ 1/1				
id-MLKEM1024-ECDH-brainpoolP384r1-SHA3-256-cert				✅ 1/1				✅ 1/1				
id-MLKEM1024-X448-SHA3-256-cert				✅ 1/1				✅ 1/1				
id-MLKEM1024-ECDH-P521-SHA3-256-cert				✅ 1/1				✅ 1/1				

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-kem-ref-impl	composite-sigs-ref-impl	corey-digicert	crypto4a	cryptonext	entrust	ossl35	safelogic	seventhsense.ai
id-MLDSA44-RSA2048-PSS-SHA256-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA44-RSA2048-PKCS15-SHA256-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA44-Ed25519-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA44-ECDSA-P256-SHA256-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA65-RSA3072-PSS-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA65-RSA3072-PKCS15-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA65-RSA4096-PSS-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA65-RSA4096-PKCS15-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA65-ECDSA-P256-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA65-ECDSA-P384-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA65-ECDSA-brainpoolP256r1-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA65-Ed25519-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3			◒ 2/4	
id-MLDSA87-ECDSA-P384-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA87-ECDSA-brainpoolP384r1-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA87-Ed448-SHAKE256-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA87-RSA3072-PSS-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA87-RSA4096-PSS-SHA512-cert			◒ 1/3		◒ 1/3			◒ 1/3				
id-MLDSA87-ECDSA-P521-SHA512-cert			◒ 1/3		◒ 1/3			◒ 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

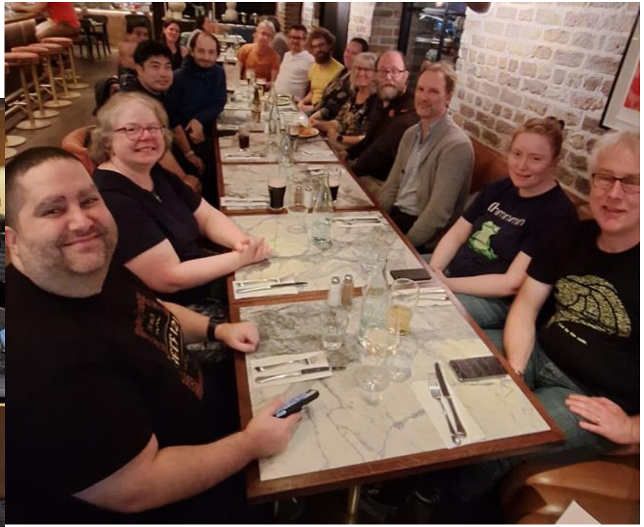
FIRST TIMERS

- **Yug Shah, Willoughby Peppler-mann**

NEXT STEPS

- Monthly meetings to continue progress – Next meeting is **Tuesday December 2nd**
- Github: https://github.com/IETF-Hackathon/pqc-certificates

JOIN US!



Contact John.gray@entrust.com to join!