

PQ interoperability

IETF 125
14-15 March 2026
Shenzhen, China



PQC 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

► Some drafts and RFCs we have been testing:

- [RFC 9881 \(ML-DSA\)](#)
- [RFC 9882 \(CMS ML-DSA\)](#)
- [draft-ietf-lamps-kyber-certificates](#)
- [RFC 9629 \(CMS KEM\)](#)
- [draft-ietf-lamps-pq-composite-sigs/](#)
- [draft-ietf-lamps-pq-composite-kem/](#)
- [draft-ietf-lamps-cms-composite-sigs](#)
- [draft-ietf-lamps-cms-composite-kem](#)
- [RFC 9763](#)
- [draft-ietf-lamps-certdiscovery](#)
- [RFC 9810 \(CMPv3\)](#)
- [RFC 9936 \(CMS Kyber\)](#)

What got done (January 24 Hackathon)

- Interim Hackathon on January 24th
 - Composite Signature and KEM testing (numerous implementations in progress – OpenSSL, BC, proprietary)
 - Composite ML-DSA private key format uses an optional parameter in the key format which caused some interop issues
 - Bouncy Castle automated verifier updated to support IANA assigned composite signature OIDS.
 - Certificate Discovery (basic working implementation)
 - TLS composite Signature authentication demonstration (Nicola)

What got done (Since January)

- PQ artifacts created for the NIST PKITS test suite (Carl)
 - See: <https://github.com/IETF-Hackathon/pqc-certificates/pull/267>
- Discovered some ML-KEM verifiers are failing due to missing artifacts or bugs (JP)
- Creation of JOSE artifacts for Composites signatures and interest for PQC algorithm artifacts (Lucas / James / Abel / Hannes)
- Certificate Discovery implementations being worked (Corey / John)
- Automated verifiers and manual testing updated (everyone)

What we learned

- Still dealing with nits in algorithm implementations which cause some interop test failures.
- We need to clean out the “old stuff” in the repo to clarify the results.

Sample Compatibility Matrix Results

https://ietf-hackathon.github.io/pqc-certificates/pqc_hackathon_results_certs_r5_automated_tests.html

- ✓ = 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	entrust-pkihub	leancrypto	openjdk	ossl35	safelogic	seventhsense.ai
id-MLDSA44-RSA2048-PSS-SHA256-cert	✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
id-MLDSA44-RSA2048-PKCS15-SHA256-cert	✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
id-MLDSA44-Ed25519-SHA512-cert	✓ 2/2		✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2				
id-MLDSA44-ECDSA-P256-SHA256-cert	✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
id-MLDSA65-RSA3072-PSS-SHA512-cert	✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
id-MLDSA65-RSA3072-PKCS15-SHA512-cert	✓ 2/2		✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
id-MLDSA65-RSA4096-PSS-SHA512-cert	✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
id-MLDSA65-RSA4096-PKCS15-SHA512-cert	✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
id-MLDSA65-ECDSA-P256-SHA512-cert	✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
id-MLDSA65-ECDSA-P384-SHA512-cert	✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
id-MLDSA65-ECDSA-brainpoolP256r1-SHA512-cert	✓ 2/2		✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2						
id-MLDSA65-Ed25519-SHA512-cert	✓ 2/2		✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2			✓ 4/4	
id-MLDSA87-ECDSA-P384-SHA512-cert	✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
id-MLDSA87-ECDSA-brainpoolP384r1-SHA512-cert	✓ 2/2		✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2						
id-MLDSA87-Ed448-SHAKE256-cert	✓ 2/2		✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2				
id-MLDSA87-RSA3072-PSS-SHA512-cert	✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
id-MLDSA87-RSA4096-PSS-SHA512-cert	✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
id-MLDSA87-ECDSA-P521-SHA512-cert	✓ 2/2	✓ 2/2	✓ 2/2		✓ 2/2		✓ 2/2	✓ 2/2	✓ 2/2	✓ 2/2					
ML-DSA-44-both	✓ 1/1	✓ 1/1	✓ 1/1			✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1			✓ 1/1	✓ 1/1	✓ 1/1	○ 0/1
ML-DSA-44-cert	✓ 3/3	✓ 3/3	✓ 3/3		✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3
ML-DSA-44-consistent	✓ 1/1	✓ 1/1	✓ 1/1			✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	○ 0/1
ML-DSA-44-expandedkey	✓ 1/1	✓ 1/1	✓ 1/1			✓ 1/1		✓ 1/1			✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	○ 0/1
ML-DSA-44-seed	✓ 1/1	✓ 1/1	✓ 1/1			✓ 1/1		✓ 1/1		✓ 1/1		✓ 1/1	✓ 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	✓ 1/1	✓ 1/1	○ 0/1
ML-DSA-65-cert	✓ 3/3	✓ 3/3	✓ 3/3		✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3
ML-DSA-65-consistent	✓ 1/1	✓ 1/1	✓ 1/1			✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	○ 0/1
ML-DSA-65-expandedkey	✓ 1/1	✓ 1/1	✓ 1/1			✓ 1/1		✓ 1/1			✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	○ 0/1
ML-DSA-65-seed	✓ 1/1	✓ 1/1	✓ 1/1			✓ 1/1		✓ 1/1		✓ 1/1		✓ 1/1	✓ 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	✓ 1/1	✓ 1/1	○ 0/1
ML-DSA-87-cert	✓ 3/3	✓ 3/3	✓ 3/3		✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3	✓ 3/3
ML-DSA-87-consistent	✓ 1/1	✓ 1/1	✓ 1/1			✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	○ 0/1
ML-DSA-87-expandedkey	✓ 1/1	✓ 1/1	✓ 1/1			✓ 1/1		✓ 1/1			✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	○ 0/1
ML-DSA-87-seed	✓ 1/1	✓ 1/1	✓ 1/1			✓ 1/1		✓ 1/1		✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	✓ 1/1	○ 0/1

PQ interoperability – 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, Yug Shah, Willoughby Peppler-mann

FIRST TIMERS

- Jens-Rene Giesen, Gefei Li

NEXT STEPS

- Monthly meetings to continue progress –
Next meeting is **Tuesday April 14th**
- Github: <https://github.com/IETF-Hackathon/pqc-certificates>



JOIN US!



Contact John.gray@entrust.com to join!

IETF Hackathon – PQ in X509