# PQ IN X.509

IETF 118

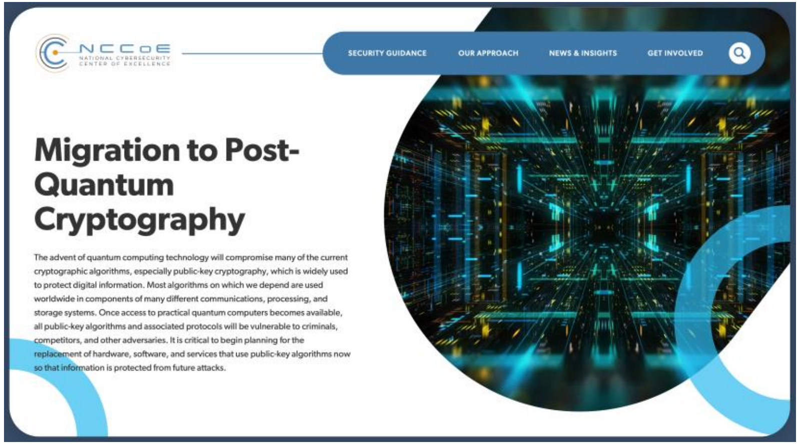
4–5 November 2023

Prague, Czech Republic

# PQ 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….

- The project grew and was soon noticed by the NIST NCCOE Interoperability working group.



## Migration to Post-Quantum Cryptography

The advent of quantum computing technology will compromise many of the current cryptographic algorithms, especially public-key cryptography, which is widely used to protect digital information. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to criminals, competitors, and other adversaries. It is critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

# WHAT GOT DONE

- Updated testing to support the NIST draft ML-DSA, ML-SLH and ML-KEM specifications
  - New certificate “R3” .zip file format defined to simplify testing algorithms.
  - Updated the OID mapping table to align with the NIST draft release
  - Added a table describing source of PQ algorithms.
    - See [https://github.com/IETF-Hackathon/pqc-certificates/tree/master/providers](https://github.com/IETF-Hackathon/pqc-certificates/tree/master/providers)
  - We now have 4 unique algorithm implementations for MLDSA defined

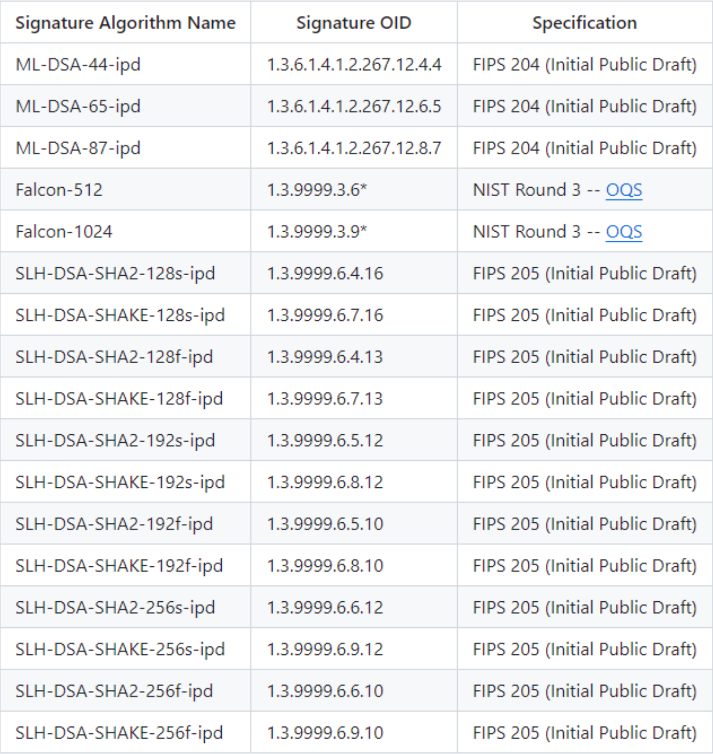
# WHAT GOT DONE

- Interoperability testing artifact format being defined for CMP.  The goal is to develop a CMP interoperability test suite
- The first composite KEM implementation is being developed
- Multi-auth for certificate binding implementation being worked on
  - Discussions about how the multi-auth binding and discovery drafts can be complimentary
- 6 updated R3 artifact .zip formats plus additional verifications of artifacts by new members

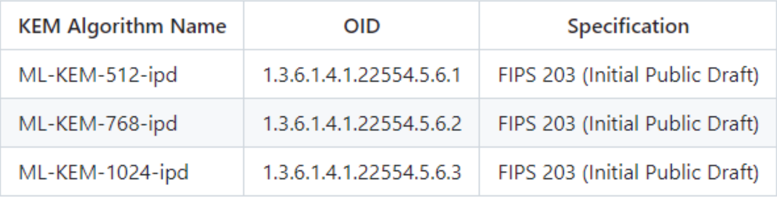
# WHAT GOT DONE

- Newly updated compatibility matrix
- Chameleon certificate discussion
- Composite signature implementations being updated to the updated version -10 standard
  - New compact signature format is a bit challenging to implement
  - Further discussion on the non-separability strengthening of the composite draft.

# INTEROPERABLE OID MAPPING TABLE

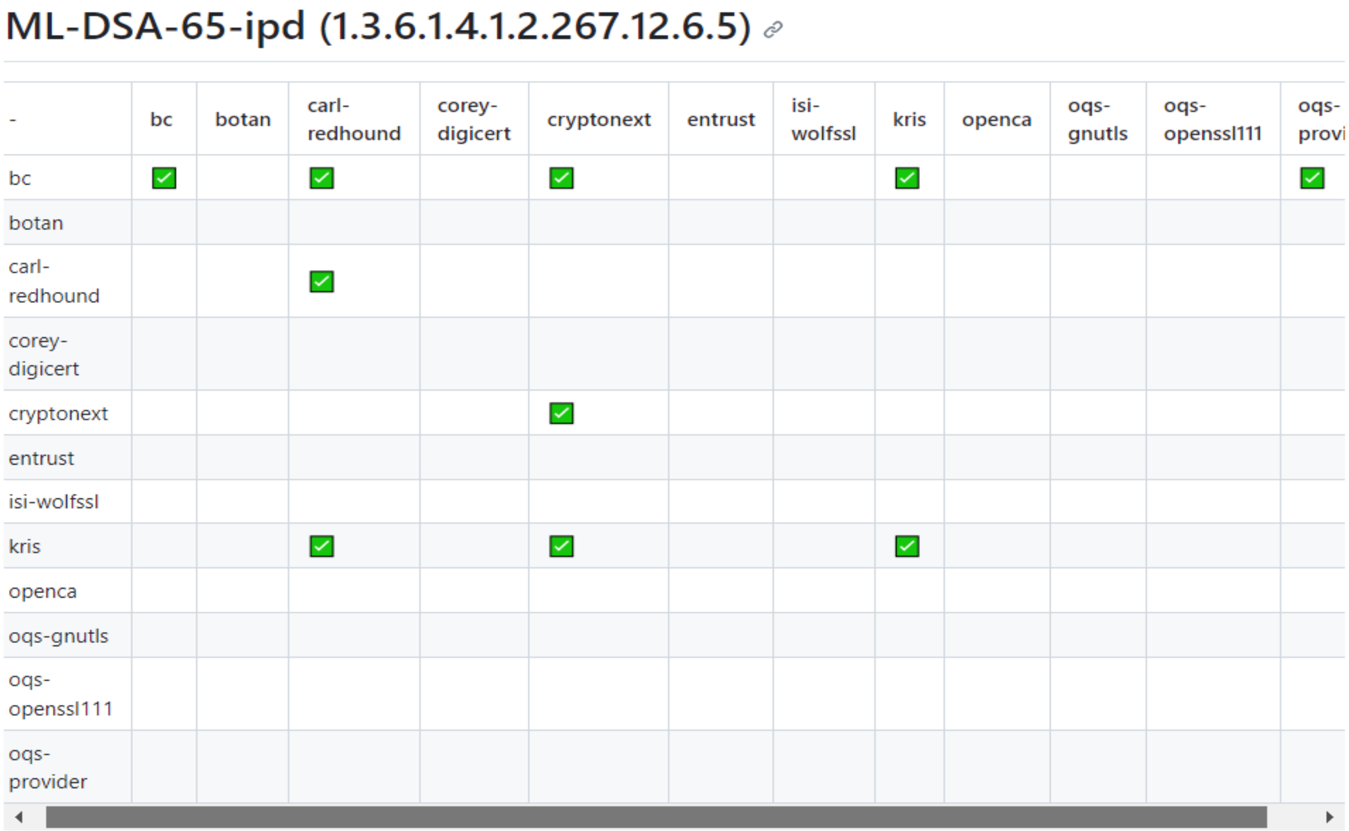


| Signature Algorithm Name | Signature OID | Specification |
|---|---|---|
| ML-DSA-44-ipd | 1.3.6.1.4.1.2.267.12.4.4 | FIPS 204 (Initial Public Draft) |
| ML-DSA-65-ipd | 1.3.6.1.4.1.2.267.12.6.5 | FIPS 204 (Initial Public Draft) |
| ML-DSA-87-ipd | 1.3.6.1.4.1.2.267.12.8.7 | FIPS 204 (Initial Public 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) |

# COMPATIBILITY MATRIX SAMPLE



## ML-DSA-65-ipd (1.3.6.1.4.1.2.267.12.6.5)

| - | bc | botan | carl-redhound | corey-digicert | cryptonext | entrust | isi-wolfssl | kris | openca | oqs-gnutls | oqs-openssl111 | oqs-provi |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| bc | ✅ |  | ✅ |  | ✅ |  |  | ✅ |  |  |  | ✅ |
| botan |  |  |  |  |  |  |  |  |  |  |  |  |
| carl-redhound |  |  | ✅ |  |  |  |  |  |  |  |  |  |
| corey-digicert |  |  |  |  |  |  |  |  |  |  |  |  |
| cryptonext |  |  |  |  | ✅ |  |  |  |  |  |  |  |
| entrust |  |  |  |  |  |  |  |  |  |  |  |  |
| isi-wolfssl |  |  |  |  |  |  |  |  |  |  |  |  |
| kris |  |  | ✅ |  | ✅ |  |  | ✅ |  |  |  |  |
| openca |  |  |  |  |  |  |  |  |  |  |  |  |
| oqs-gnutls |  |  |  |  |  |  |  |  |  |  |  |  |
| oqs-openssl111 |  |  |  |  |  |  |  |  |  |  |  |  |
| oqs-provider |  |  |  |  |  |  |  |  |  |  |  |  |

....

# PQ IN X.509 INTEROPERABILITY – SUMMARY

## TEAM MEMBERS

- Mike Ounsworth, John Gray, Cory Bonnell, Michael Baentsch, Kris Kwiatkowski, Alexander Railean, Pat Kelsey, Tomofumi Okubo, Max Pala, Markku-Juhani O.Saarinen, David Hook, Felipe Ventura, Jake Massimo, Carl Wallace, Goutam Tamvada, Daiki Ueno, Julien Prat, Alie Becker, Brendan Zember, Chris Rodine, Chris Brown, George Tasopoulos, Britta Halle

## FIRST TIMERS

- Dimity BelYavskiy, Pravek Sharma

## NEXT STEPS

- Monthly meetings to continue progress – Next one is Tuesday December 5th
- Compatibility Matrix updates
- Github: https://github.com/IETF-Hackathon/pqc-certificates
- JOIN US!