COSE and JOSE Registrations for Post Quantum Signatures

draft-ietf-cose-dilithium-04
draft-ietf-cose-sphincs-plus-05
draft-ietf-cose-falcon-XX

Mike Prorock
IETF 121, Dublin
November 2024

Draft Updates

`draft-ietf-cose-dilithium-04`

Updated, reviewed, tests, etc.

Pre-hash recommended as a separate draft

Authors believe ready for WG Last Call

Draft Updates

`draft-ietf-cose-sphincs-plus-04`

Aligned with FIPS 205 and ML-DSA drafts

PR Out with Updates based on reviews….

Once those are in… WGLC on the list?

Question for COSE WG

`draft-ietf-cose-falcon-01`

Waiting on a draft of FIPS 206 from NIST

Once 206 is in place, ready to move forward

Any steps requested before 206 is in place?

Question for COSE WG

Drafts for prehash versions?

Any other next steps from the group / chairs?

Resources

Work Item Repository (Issues, PRs, Details):
https://github.com/cose-wg/

Datatracker(s):
https://datatracker.ietf.org/doc/draft-ietf-cose-dilithium/
https://datatracker.ietf.org/doc/draft-ietf-cose-sphincs-plus/
https://datatracker.ietf.org/doc/draft-ietf-cose-falcon/

NIST PQC:
https://csrc.nist.gov/projects/post-quantum-cryptography/news
https://csrc.nist.gov/projects/post-quantum-cryptography

FIPS:
https://csrc.nist.gov/pubs/fips/204/ipd
https://csrc.nist.gov/pubs/fips/205/ipd