COSE and JOSE Registrations for Post Quantum Signatures

draft-ietf-cose-dilithium-03

draft-ietf-cose-sphincs-plus-04

Mike Prorock

IETF 120, Vancouver

July 2024

Draft Updates

`draft-ietf-cose-dilithium-03`

IANA Sections All Updated
Security Considerations Updated
Aligned with FIPS 204

WG Last Call?

Draft Updates

`draft-ietf-cose-sphincs-plus-03`

IANA Sections All Updated
Security Considerations Updated
Aligned with FIPS 205

WG Last Call?

Question for COSE WG

`draft-ietf-cose-falcon-01`

Anyone *need* falcon?

Happy to do the work if requested.

Question for COSE WG

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