

Status of draft-selander-lake-traces

(to be submitted as draft-ietf-lake-traces)

Status

- Adoption call triggered on 18 Oct 2021
- Feedback from
 - Marco Tiloca
 - Stefan Hristozov
 - Sean Turner
 - John Mattsson (co-author)
- Support adoption, support (informational) RFC publication
- Ensure correctness by verifying with multiple implementations
- Scope...

Current scope:

- Methods 0 and 3
- Cipher suite 0 (CCM 64-bit tags, SHA-256, X25519)

Interest for:

- P-256 –based suites (2 and 3)
- Which method – cipher suite combinations to support ?
 - Exhaustive
 - Selective
 - Method 3 with cipher suite 0
 - Method 0 with cipher suite 2