IETF Hackathon: One Tax API

IETF 115

5-6 November 2022

London

Hackathon Plan

- What problem were you working on?
  - RFC 8032
- Specific problems to solve
  - Determine good set of test vectors
- How you planned to solve it?
  - Try test vectors from Chalkias, Garillot and Nikolaenko on a variety of libraries

What got done

- What you achieved? (key results)
  - Add tests for
  - LibreSSL
  - WolfSSL
  - LibGcrypt
  - New code
    - Tmplement test for NaCl

What we learned

Lessons learned from this hackathon

- NaCl and NaCl.js pass and fail the same tests from [Chalkias, Garillot and Nikolaenko](https://eprint.iacr.org/2020/1244

Wrap up

Team members:

- Benson Muite

First timers @ IETF/Hackathon:

-

Other links:

- noble-ed25519

Notes and contacts:

- benson_muite at emailplus dot org