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

- Ideas, add tests for
  - LibGcrypt
  - LibreSSL
  - libtomcrypt
  - Mbed-TLS
  - Nettle
  - Network Security Services
  - noble-ed25519
- New code
  - Implement tests for Botan, Monocypher TweetNaCl, and WolfSSL,
  - Pull request to project repository

What we learned

Lessons learned from this hackathon

- NaCl and NaCl.js pass and fail the same tests from Chalkias, Garillot and Nikolaenko
- Monocypher passes and fails the same tests as OpenSSL 3
- wolfSSL passes the same tests as OpenSSL 3, but indicates a failure in the verification process for other tests, not a failed verification
- Botan passes ed25519-donna and Supercop on which it is derived from

Wrap up

Team members:

- Benson Muite

First timers @ IETF/Hackathon:

-

Other links:

-

Notes and contacts:

- benson_muite at emailplus dot org