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

  - [Botan](#)
  - [LibGcrypt](#)
  - [LibreSSL](#)
  - [libtomcrypt](#)
  - [Mbed-TLS](#)
  - [Nettle](#)
  - [Network Security Services](#)
  - [noble-ed25519](#)
  - [WolfSSL](#)

- New code

  - Implement tests for [Monocypher](#) and [TweetNaCl](#), 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

Wrap up

Team members:

- Benson Muite

First timers @ IETF/Hackathon:

-

Other links:

-

Notes and contacts:

- benson_muite at emailplus dot org