

IETF Hackathon

One Tax API

IETF 113

19-20 March 2022

Online

Hackathon Plan

One Tax API

- No RFC's yet, but is related to previous RFC's for forward secrecy
- Relevant to web monetization
- Try out and understand McTiny
 - a sync flood resistant forward secrecy preserving protocol
 - Public domain code <https://mctiny.org/software.html>
 - USENIX 2020 presentation
 - <https://www.usenix.org/conference/usenixsecurity20/presentation/bernstein>

Deploy the code, review the paper, take measurements

What got done

What you achieved? (key results)

- Deployed on and ran the code on the cloud using Ubuntu 20.04 and Rocky Linux 8
- Started on simplified examples of McEliece encryption
- <https://github.com/OneTaxApi/McEliece>

What we learned

Lessons learned from this hackathon

- Implementation seems to work, but needs further examination
- Needs real world testing for sync flood resistance
- Needs real world testing for forward secrecy

Wrap up

Team members:

- Benson Muite

Other links:

- <https://mctiny.org>
- <https://github.com/OneTaxApi/McEliece>

First timers @ IETF/Hackathon:

-

Notes and contacts:

- benson dot muite at emailplus dot org