One Tax API

IETF 114

23-24 July 2022

Philadelphia, Pennsylvania

Hackathon Plan

- What drafts/RFC's were involved?
  - Hare issues
    - HKDF RFC 5869
    - AES-GCM RFC 8452?
    - EdDSA RFC 7748 and RFC 8032
- Specific Problems
  - Implement encryption protocols in Hare

What got done

- Ideas:
  - Implement Ristretto in Hare, currently in last call
  - Implement AES-GCM-SIV, RFC-8452 in Hare
- New code:
  - Start adding Ed25519 conformance tests to Hare

Conformance Test Results

Library	0	1	2	3	4	5	6	7	8	9	10	11
ed25519-hare	X	V	V	V	X	X	V	V	X	X	X	V
BoringSSL	V	V	V	V	X	X	X	X	X	X	X	V
BouncyCastle	V	V	V	V	X	X	X	X	X	X	X	X
CryptoKit	V	V	V	V	X	X	X	X	X	X	X	V
Dalek	V	V	V	V	X	X	X	X	X	X	X	V
Dalek strict	X	X	X	V	X	X	X	X	X	X	X	X
ed25519-donna	V	V	V	V	X	X	V	X	X	X	X	V
ed25519-java	V	V	V	V	X	X	V	V	X	X	V	X
Go	V	V	V	V	X	X	X	X	X	X	X	V
libra-crypto	X	X	X	V	X	X	X	X	X	X	X	X
LibSodium	X	X	X	V	X	X	X	X	X	X	X	X
npm	V	V	V	V	X	X	X	X	X	X	X	V
OpenSSL-3.0	V	V	V	V	X	X	X	X	X	X	X	V
PyCA	V	V	V	V	X	X	X	X	X	X	X	V
python-ed25519	V	V	V	V	X	X	V	V	X	X	X	V
ref10	V	V	V	V	X	X	V	X	X	X	X	V
TweetNaCl-js	V	V	V	V	X	X	V	V	X	X	X	V
Zebra	V	V	V	V	V	V	X	X	X	V	V	V

What we learned

- Implemented in Hare
  - HKDF
  - Ed25519
  - Curve 25519
- Several AES-GCM ciphers
  - AES-GCM implemented
  - AES-GCM-SIV not yet implemented in Hare, example implementations
    - Rust
    - C
  - Soatak summarizes that AES-GCM is faster than AES-GCM-SIV but less secure
- Issues with existing drafts/RFCs
  - Chalkias, Garillot and Nikolaenko suggest improvements to RFC 8032 to enable use in contract sigining, electronic voting and transactions
  - Henry De Valence suggests standardizing signature validity rules for Ed25519
  - Chalkias, Garillo and Nikolaenko's test vectors should be added to those specified in RFC 8032

Wrap up

Team members:

- Benson Muite

First timers @ IETF/Hackathon:

-

Other links:

- noble-ed25519

Notes and contacts:

- benson_muite at emailplus dot org