RubyishなQUIC実装の進捗について

うなすけ

RubyKaigi 2023 follow up

2023-08-19

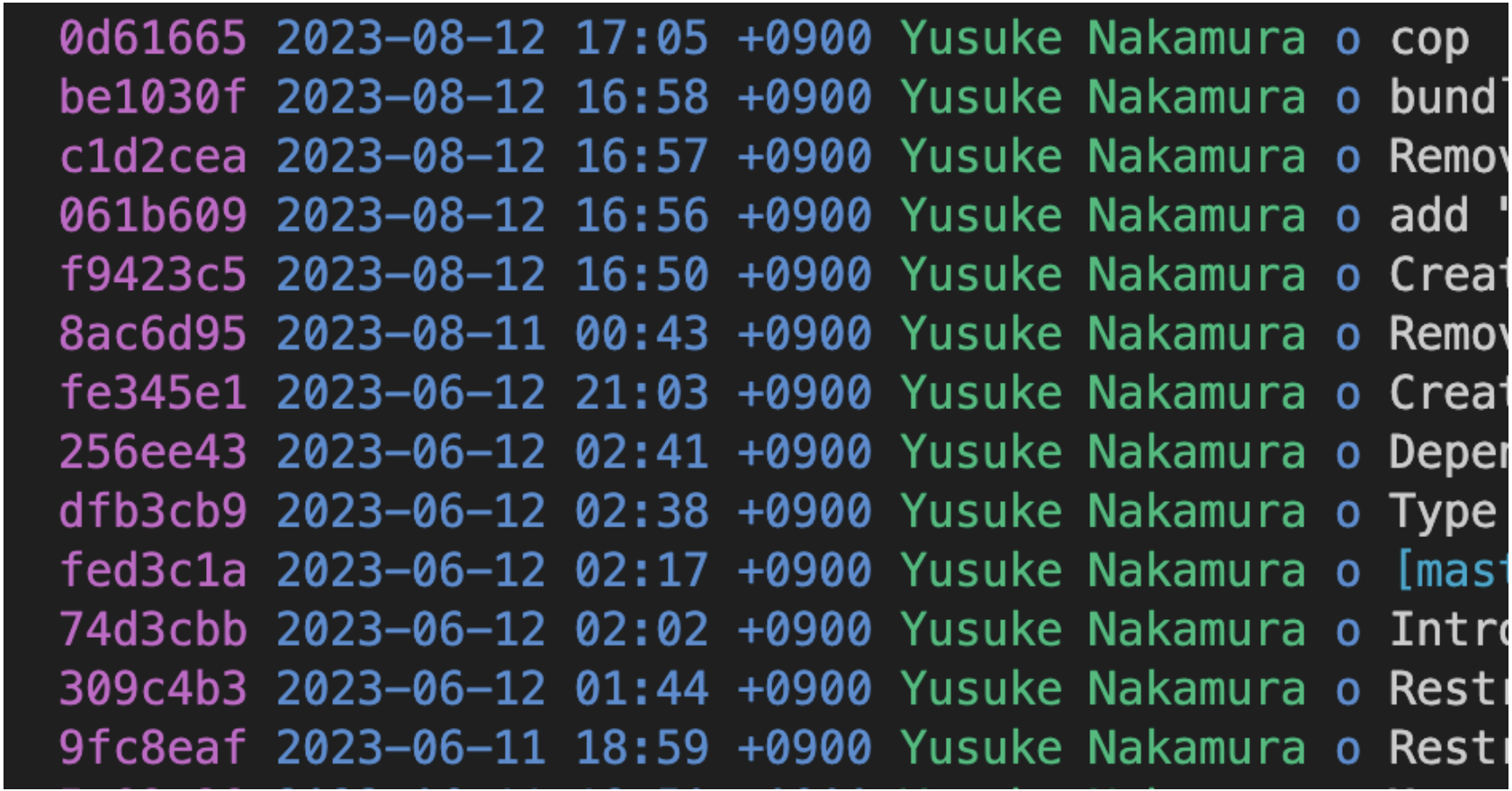
自己紹介

- Name: うなすけ
- Work: フリーランス
- Kaigi on Rails オーガナイザー（10/27-28 開催）
- GitHub https://github.com/unasuke
- ActivityPub https://mstdn.unasuke.com/@unasuke
- X (Twitter) https://twitter.com/yu_suke1994
- https://unasuke.com

RubyKaigi 2023の復習

- QUICとは何か、という話はすっ飛ばします
- PythonのQUIC実装aioquicをRubyに移植した
  - 移植元 → https://github.com/aiortc/aioquic
  - 移植先 → https://github.com/unasuke/raioquic
    - “Ruby” の “aioquic” で “raioquic”

commit log


0d61665 2023-08-12 17:05 +0900 Yusuke Nakamura o cop
be1030f 2023-08-12 16:58 +0900 Yusuke Nakamura o bund
c1d2cea 2023-08-12 16:57 +0900 Yusuke Nakamura o Remo
061b609 2023-08-12 16:56 +0900 Yusuke Nakamura o add
f9423c5 2023-08-12 16:50 +0900 Yusuke Nakamura o Creat
8ac6d95 2023-08-11 00:43 +0900 Yusuke Nakamura o Remo
fe345e1 2023-06-12 21:03 +0900 Yusuke Nakamura o Creat
256ee43 2023-06-12 02:41 +0900 Yusuke Nakamura o Deper
dfb3cb9 2023-06-12 02:38 +0900 Yusuke Nakamura o Type
fed3c1a 2023-06-12 02:17 +0900 Yusuke Nakamura o [mast
74d3cbb 2023-06-12 02:02 +0900 Yusuke Nakamura o Intro
309c4b3 2023-06-12 01:44 +0900 Yusuke Nakamura o Restr
9fc8eaf 2023-06-11 18:59 +0900 Yusuke Nakamura o Restr

言い訳タイム

- IETF 117 San Francisco
  - 参加記がまだ書けていない……
- CloudNative Days Fukuoka 2023
  - 発表した
  - https://event.cloudnativedays.jp/cndf2023/talks/1890
- Kaigi on Rails 2023
  - 絶賛準備中！
- RFC 8446を読んでた（後述）
- 例のアレ

コードでやったこと

- HKDF (RFC 5869)
  - https://www.rfc-editor.org/rfc/rfc5869.html
- AEAD (RFC 5116, RFC 9001)
  - https://www.rfc-editor.org/rfc/rfc5116.html
  - https://www.rfc-editor.org/rfc/rfc9001.html#name-aead-usage
- YARDを書いている
- エディタで見せたほうが早い

コード外でやったこと

- RFC 8446 (TLS 1.3)をイチから読み直した
  - https://www.rfc-editor.org/rfc/rfc8446.html
  - https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8446bis/

悩んでいること

- API
  - “Rubyish” ってなんだ……？
  - 例 `raioquic/lib/raioquic/tls.rb`