IETFとPKI関連標準化

セコム株式会社　IS研究所
伊藤 忠彦

2022/1/27

自己紹介

伊藤忠彦（セコム株式会社、IS研究所、暗号認証基盤グループ、主務研究員）

- 暗号プロトコル・暗号鍵管理に関する研究に従事
  - 低リソースデバイス（IoTデバイス等）
  - 長期的な鍵管理に関する検討
    - 量子コンピュータの影響なども

- ルート認証局関連業務（PKI分野）にも従事
  - ルート認証局構築
  - CA/BForumでの活動
  - IETFでの活動 (RFC8813)

他にも、暗号鍵管理についての仕組みやルール作りで活動しています

もくじ

- IETFとは

- 参加方法

- いくつかの壁

IETFとは

- RFCで有名
  - RFC（Request for Comments）は、インターネットで用いられるさまざまな技術の標準化や運用に関する事項など幅広い情報共有を行うために公開される文書シリーズです。(by JPNIC)

- 世界で最も普及しているフォーラム標準の1つ
  - tcp, ip, smtp, udp, quic, etc.

- ラフコンセンサスと実装を重視
  - 技術者によるボトムアップな提案・活動が多い

参加方法

- 公開プロセス
  - 基本はMLで議論（WGによってはgithubで）
    - 追うのは結構大変
  - 現地開催は年3回（最近はリモート開催）
    - 動画はYoutubeでも公開されている
    - チャット欄で興味深い議論が進行する事もあり、リアルタイムで参加する利点もある
  - 会員制度はなく個人で参加

いくつかの壁

- 参加の壁
  - 昔は旅費や参加費にそれなりの費用が発生した
    （今は大幅に安くなった）

- 議論をする場合の壁
  - 話を聞いてもらうには
  - 相手の価値観とゴールを想定する

- 標準化の壁
  - 味方を作る
  - 本当に必要なものを

参加の壁（低い）

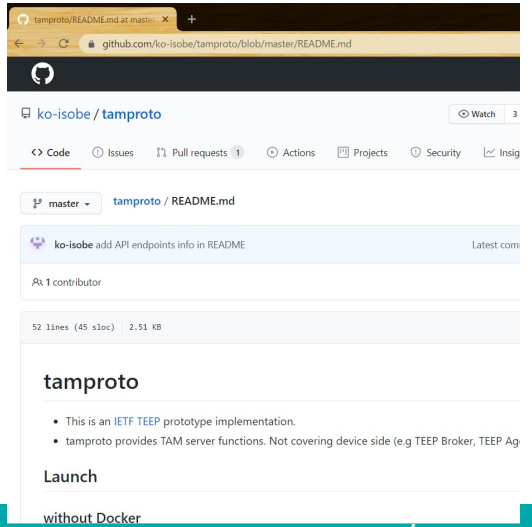
- 昔は旅費や参加費にそれなりの費用が発生した
  - 参加費10万円以上、旅費、宿泊費…

- 今は、オンライン参加費のみで参加可能
  - 3万円くらい
  - チャット欄が面白い
    - 例：Chromeの人がFlocについて発表
    - 例：NISTの人がPQCについて発表
    - 一流の技術者の反応が見れる（慣れは必要）

- YouTubeでも公開されている
  - 無料
  - 発表資料等は一般公開されている
  - チャット欄は見れない
  - 発言はできない

議論をする場合の壁

- 話を聞いてもらうには？
  - （おすすめ）ハッカソン等に参加してみる
    - 実装者は特に歓迎されます
    - 色々教えてもらえます
  - とりあえずI-D (Internet Draft)を書いてみる
    - 誰でも投稿できる
  - とりあえずMLや本人に聞いてみる
    （メールアドレスは公開されている）
    - ある程度予習はしておく
      - 関連しそうなI-Dを検索してみる
      - そのI-DについてのMLの反応を調べてみる

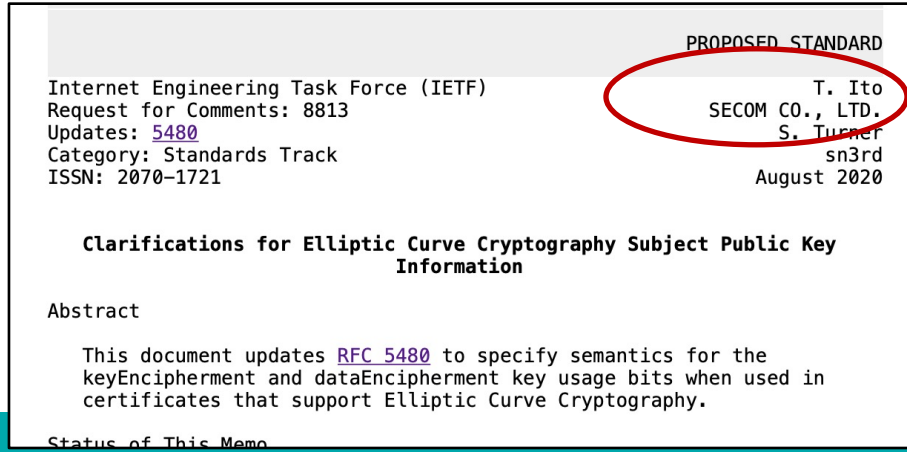


標準化の壁

- 必要なものを標準化したい
  - 使われない技術の標準化にリソースを割きたくない
  - 実際のユースケースを持っている人（困っている人）が特に歓迎される
  - 「運用で困っている事」は非常に重要

- 複雑性を上げるような標準化は嫌厭される
  - 上記目標を達成するための最低限の機能を
    - 最低限の機能を議論している最中に自分のユースケースを差し込むのも有効（自分のユースケースが標準でサポートされなくなるのを防ぐ）

- 賛成してくれる仲間を作る必要がある
  - 価値観の近い人を見つけて仲間になってもらう
    - 同じ業界の同じような事で困っている人
    - MLで自分の考えに近い発言をする人
  - 継続して参加していると、仲の良い人も増える



PROPOSED STANDARD

Internet Engineering Task Force (IETF) — T. Ito
Request for Comments: 8813 — SECOM CO., LTD.
Updates: 5480 — S. Turner
Category: Standards Track — sn3rd
ISSN: 2070-1721 — August 2020

Clarifications for Elliptic Curve Cryptography Subject Public Key Information

Abstract

This document updates RFC 5480 to specify semantics for the keyEncipherment and dataEncipherment key usage bits when used in certificates that support Elliptic Curve Cryptography.

Status of This Memo