JavaScript による End-to-End セキュリティ

付録 RFC とか鍵フォーマットとか

栗原 淳

2019 年 10 月 31 日

はじめに

PKCS (Public Key Cryptography Specification) とは

RFC (Request for Comments) とは

公開鍵・秘密鍵のフォーマット・エンコーディング

- PEM
- DER
- JWK
- [ECC 鍵のみ] RAW (Octet form)

JS の基本は JWK。OpenSSL や SSH などで馴染みがあるのは PEM。

ECDH, ECDSA の鍵選択 (曲線の選択)

どの曲線を使えばいいのか？

- P-256,
- P-256K, (Bitcoin で利用)
- P-384,
- P-521

あたりが無難なところ。