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

はじめに

この資料は、「JavaScript による End-to-End セキュリティ」の補足資料である。
標準規格や鍵フォーマットなどについて解説を与えている。
また、鍵フォーマットなどは、JavaScript でハンドリングするためのサンプルコードも記述している。

暗号周りの標準規格

PKCS (Public Key Cryptography Standards)

NIST FIPS PUB

RFC (Request for Comments) とは

その他

CRYPTOREC, NESSIE, ISO...

基本的には、「アルゴリズム」「プロトコル」のどれを標準として採用します、という「推奨技術リスト」。

「ここで採用されたアルゴリズム・プロトコルを使ってるから安全です」と言える以上の意味はない。
仕様の詳細は PKCS, RFC, NIST FIPS PUB を参考にする。

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。