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。

セキュリティ関連の標準規格

PKCS (Public Key Cryptography Standards)

NIST FIPS PUB

RFC (Request for Comments)

その他; 各国の推奨技術リストとしての標準規格

- CRYPTOREC[1]
  電子政府推奨暗号リストを作り、その実装や運用方法も含めて安全性を調査・評価・監視・検討するプロジェクト (2000 年〜)
- NESSIE[2]
  EU の制定した暗号標準リストを策定するプロジェクト (2000 年〜)

基本的には、「評価検討した結果、既存の暗号アルゴリズム・プロトコルのどれそれを標準として採用する」という「推奨技術リスト」の策定プロジェクトだと思って差し支えない。

[1] Cryptography Research and Evaluation Committee

[2] New European Schemes for Signature, Integrity, and Encryption

「各国独自」という意味

推奨技術リストへ採用されたアルゴリズム・プロトコルは、「その国において正しく評価された比較的安全なもの」というお墨付きを得る。セキュリティ技術は国防上重要な意味を持つため、このお墨付きは、その技術を自国で利用して良いものかどうかを判定するもの、と言える。

例外はもちろん存在するが、仕様の詳細は PKCS, NIST 公募 (NIST FIPS PUB), あるいは IETF (RFC) など国際的に比較的オープンな場でまず採用・策定される。
そしてそれを各国が独自に調査検討して推奨技術リストとして採用する、というケースが多い。

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。