*

Using secp256k1 with JOSE and COSE

draft-jones-webauthn-secp256k1

Michael B. Jones
IETF 102, Montreal
July 2018

draft-jones-webauthn-secp256k1

- Registers JOSE and COSE identifiers for the SECG secp256k1 elliptic curve
  - Described by Dan Brown and Certicom in “SEC 2: Recommended Elliptic Curve Domain Parameters” http://www.secg.org/sec2-v2.pdf
- Used by FIDO UAF, W3C Verifiable Claims interest group, several blockchain projects
- Goal to get identifiers registered so IETF crypto standards can be used w/ secp256k1
  - Rather than ad-hoc crypto representations

Reason to become an RFC

- COSE Algorithms assignment for integer values between -256 and 255 designated as “Standards Action”
  - Section 16.4 of RFC 8152
- Draft needs to become RFC if identifiers are to be small integers
- Ekr pointed out alternative
  - Create RFC relaxing COSE assignment rules so RFC not required for assigning small integers
  - Precedent: draft-ietf-tls-iana-registry-updates

Actions To Date

- Asked Ben Kaduk about AD sponsorship
  - Ben suggested asking SecDispatch
- Discussion on SecDispatch list
  - Michael Richardson volunteered to be Shepherd
  - Phillip Hallam-Baker suggested adding table cross-referencing identifiers, including OIDs
- Asked CFRG for feedback on the curve
  - At Ekr’s suggestion
  - Dan Brown replied in detail with pros and cons
  - No practical attacks against the curve are known

This won’t be the last such draft registering identifiers

- For instance, some communities interested in using these currently unregistered algs:
  - ChaCha20Poly1305, XChaCha20Poly1305, Salsa20Poly1305, XSalsa20Poly1305
- https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-ecdaa-algorithm-v2.0-id-20180227.html defines and registers several attestation algorithms
- Surely more of these drafts to come

Possible Next Steps

- AD sponsorship
  - Straightforward & addresses the immediate need
- Ask Michael Richardson to shepherd
  - Since he already volunteered
- Or write draft-ietf-cose-iana-registry-updates
  - Would enable COSE registrations from non-RFC (probably from a W3C WebAuthn specification)
  - With AD sponsorship?
- Other possibilities?