*

Additional Algorithm Registrations for COSE and JOSE

draft-jones-cose-additional-algorithms

Mike Jones

IETF 104, Prague

March 26, 2019

Spec Overview

- Registers algorithm identifiers for additional algorithms used by W3C Web Authentication (WebAuthn) standard
  - 4 RSA signing algorithms – already provisionally registered
  - Signing with secp256k1 curve – not yet registered
- Draft fulfills this charter deliverable
  - “4. Define the algorithms needed for W3C Web Authentication for COSE using draft-jones-webauthn-cose-algorithms and draft-jones-webauthn-secp256k1 as a starting point (Informational).”
- WebAuthn standard
  - https://www.w3.org/TR/2019/REC-webauthn-1-20190304/

Call for Adoption Pending

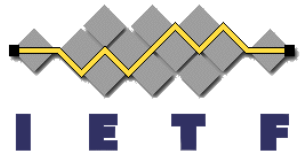
- The chairs issued a call for working group adoption on March 13 to run until about March 26 (today)
- I saw a number of “adopt” responses and no objections

Reviews Received

- Detailed reviews sent by:
  - Jim Schaad
  - John Mattsson

- Thanks for the useful reviews!
- Discussion points to follow result from those reviews

Two WebAuthn Algorithms Not in Current Draft



- Elliptic Curve Direct Anonymous Attestation (ECDAA) algorithms “ED256” and “ED512”
- Algorithms defined in FIDO ECDAA Algorithms spec
  - https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-ecdaa-algorithm-v2.0-id-20180227.html
- WebAuthn IANA Considerations section proposes COSE registrations for them
  - https://www.w3.org/TR/2019/REC-webauthn-1-20190304/#sctn-cose-alg-reg
- Should we just ask Designated Experts for approval of these registrations or does WG want to work on them?
- Observation: More complicated than other algs in draft

Document Title

- Title currently
  - Additional Algorithm Registrations for COSE and JOSE
- Jim Schaad suggested adding WebAuthn to title
- John Mattsson suggested possibly also adding FIDO or CTAP to title

- If adopted, do people want a title change, and if so, to what?

secp256k1 Curve Name

- Draft currently registers JOSE curve identifier “P-256K”
- Multiple reviewers have suggested simply registering “secp256k1” instead
  - Makes sense to me

Compressed vs. Non-compressed Points

- Jim asked whether there's a recommendation for using compressed versus non-compressed points for secp256k1
  - Currently no recommendation in the draft
  - Uncompressed will clearly work
  - It would be good to have data on whether people are using uncompressed and/or compressed points with this curve

Next Steps

- Working Group Adoption?
- Address feedback from reviews and discussions today