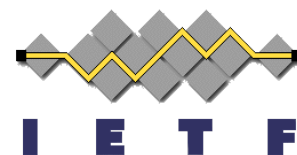


*

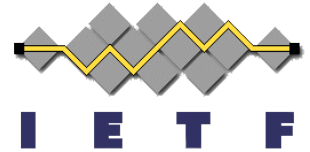
COSE and JOSE Registrations for WebAuthn Algorithms

**draft-ietf-cose-
webauthn-algorithms**



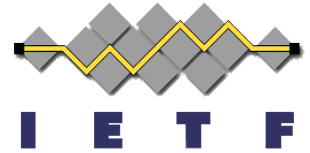
Mike Jones
IETF 105, Montreal
July 26, 2019

Spec Overview



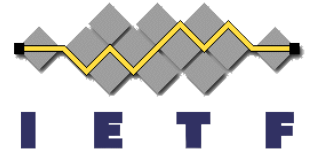
- Registers algorithm identifiers for additional algorithms used by W3C Web Authentication (WebAuthn) standard
 - 4 RSA signing algorithms – already provisionally registered
 - Signing with secp256k1 curve – not yet registered
- Draft fulfills this charter deliverable
 - “4. Define the algorithms needed 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/>

What's Happened Since Prague?



- Working group adoption
- Title change to
 - COSE and JOSE Registrations for WebAuthn Algorithms
- Addressed review comments received
 - From John Mattsson, Matt Palmer, Jim Schaad
- Normative changes
 - Changed the JOSE curve identifier from “P-256K” to “secp256k1”
 - Specified that secp256k1 signing is done using the SHA-256 hash function

Next Steps



- Time for Working Group Last Call?