JSON Web Proof Updates

draft-ietf-jose-json-web-proof-01,
draft-ietf-jose-json-proof-algorithms-01
draft-ietf-jose-json-proof-token-01

David Waite, Ping Identity
IETF 117, San Francisco
July 25, 2023

What's Changed between -00 and -01

- Editorial cleanups to markdown
- Changes to point to current BBS work in CFRG

Editorial feedback/comments from review seem to be increasing

JWS Multiple Signature Option work also proposed here

Ongoing Changes for -02

- Move fully to new BBS draft (*draft-irtf-cfrg-bbs-signatures-03*)
  - Current text uses library-based invocation
  - Instead use algorithmic definitions in the current-latest draft
- Resume draft generation from test fixtures
  - Examples generated where possible from implementations of algorithms

Some changes after -02

- Resolution of JWS Multi-Payload Option (or of alternate proposals)
  - Investigate restructuring presentation form as a serialization of JWS Multi-Payload (a a JWP of one or more credential payloads)
- Tracking BBS Bound Signatures work, possibly as separate algorithm
  - Issued proof bound to holder key pair rather than holder secret
- Coordination around COSE-equivalents