JSON Web Proofs Specifications

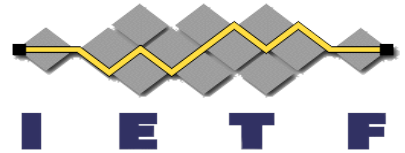
draft-ietf-jose-json-web-proof
draft-ietf-jose-json-proof-algorithms
draft-ietf-jose-json-proof-token

Mike Jones, David Waite, Jeremie Miller
IETF 119, Brisbane
March 18, 2024

Progress Since IETF 118

- Substantial normative and editorial additions to all 3 drafts, e.g.:
  - Normatively defined header parameters used
  - Populated IANA Considerations sections
  - Allowed proof representations to contain multiple base64url-encoded parts
  - Specified representation of zero-length disclosed payloads
  - Added Terminology sections
  - Updated to use draft-irtf-cfrg-bbs-signatures-05
  - Updated to use draft-ietf-cose-bls-key-representations-04
  - More and better examples
  - Improvements resulting from a full proofreading
- Addressed majority of outstanding GitHub issues and PRs

Landscape of Related Specifications

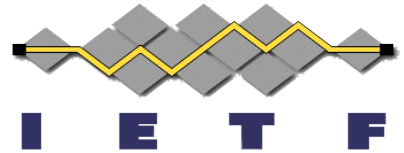


- The BBS Signatures draft continues to evolve
  - The JWP -03 drafts use BBS -05 from December 2023
    - BBS -05 updated proof generation & verification
- BLS Key Representations draft recently updated
  - Now uses "kty": “EC” for uncompressed representation
  - Now spells identifiers “BLS” rather than “Bls” (since are people’s initials)
- Come to COSE tomorrow for a relevant discussion
  - Tobias Looker will discuss whether to add a compressed representation
  - Teaser: draft-irtf-cfrg-pairing-friendly-curves defines a bespoke compressed representation. To use or not to use?

Next Steps

- Continue working through issues
  - https://github.com/json-web-proofs/json-web-proofs/issues
- Continue tracking specs we're dependent upon
  - BBS Signatures
  - BLS Key Representations
- Consider additional zero-knowledge-proof algorithms
- Interop testing among implementations
  - Iterate using what we learn from testing to improve the specifications

Your Turn



- What are your use cases for JSON Web Proofs?
- What would you like to see us do next?