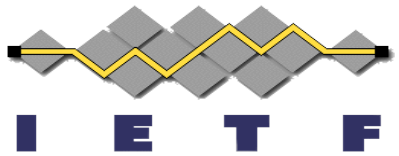
*

JSON Web Proofs Specifications



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

David Waite, Mike Jones, Jeremie Miller
IETF 120, Vancouver
July 22, 2024

Progress Since IETF 119 (1 of 2)

Substantial normative and editorial additions to all 3 drafts

Draft 4

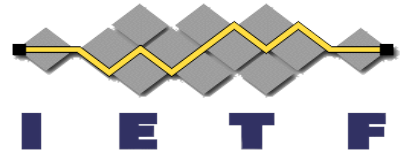
- Refactoring centered around examples
  - Combine examples throughout documents to be based on a common set of documents
  - Consolidated example algorithm text to the appendix of JPA
  - Programmatically generated by build process (MAC deferred to -05)
- Moved to BBS draft 06 – dropped `-DRAFT-5` alg qualifier
- Moved to latest BLS key representation

Progress Since IETF 119 (2 of 2)

Draft 5

- Move to multi-part proofs
  - Array of octet strings instead of requiring proof to be a single octet string
  - Single Use and MAC algorithms refactored to this from binary concatenation
  - Remove algorithm-specific buffer arithmetic for dynamically sized messages
- Remove base64url encoding from algorithms
  - Algorithms are meant to be binary-safe but some required base64url internally
  - Now only used for serializations
- Use raw JWA rather than composed JWS for SU / MAC
  - Previously defined in terms of synthesized headers and extract signatures
  - Simplifies construction and removes dependency
- `+jwp` structured syntax suffix registration

Landscape of Related Specifications



- The BBS Signatures draft continues to evolve
  - BBS draft 06 tweaked input ordering
  - Focus starting to shift on extensions (blinded signatures, pseudonyms)
- BLS Key Representations draft updated before IETF 119
  - Now uses "kty": “EC” for uncompressed representation
  - Now spells identifiers “BLS” rather than “Bls” (since are people’s initials)

Next Steps

- Evaluate use of BBS extensions within JWP
  - Blinded values
  - Pseudonymous identifiers
- Define holder confirmation as something algorithms support intrinsically or extrinsically
- Move to JWS for extrinsic holder confirmation
- Begin creating CBOR/COSE representations
- Continue to scout for help with additional algorithms

Your Turn

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