JSON Web Proof Update

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

David Waite, Mike Jones
IETF 123, Madrid
July 24, 2025

Updates Since IETF 122

Single Use (SU) and MAC algorithm changes

- The presentation now provides integrity over data derived from the issued form
  - Previously only covered the presentation protected header
- Removes caveats that come up for applications where keys and the issued form are allowed to be reused

Updates Since IETF 122 (SU/MAC)

- Needed equivalent of JWS Signing Input / COSE Sig_structure
- Needed to be generatable by JSON/CBOR-only implementations

- Settled on a common binary construction that matches well-formed CBOR, using 64-bit length/count values
- This value is generated as an internal binary value to feed to algorithms for signing/verification

- MAC has a similar internal form, which was changed to align

Updates Since IETF 122 (SU/MAC)

- Now allow the holder to use a different signing algorithms from the issuer
  - For example, to support differing hardware capabilities
- Public key/algorithm are both embedded within the issued form
- Issuer decides which algorithms holder can use
  - Specs may profile this capability away
- Now provides step-by-step guidance for implementers doing generation/verification with the algorithms

Updates Since IETF 122 (Misc)

- Implementer feedback led to cleanup of CDDL and some text
- "+cwp" structured suffix registration for COSE usage
- Shortened "proof_key" to "iek" (Issuer Ephemeral Key) and "presentation_key" to "hpk" (Holder Presentation Key).

- JSON Serialization dropped
  - Note that it had no capabilities beyond those already provided by Compact Serialization
  - If you have specific use cases that need to leverage additional unsigned data, let’s talk

Resolution: Parameter Unification

- JOSE and COSE header parameters are spiritually similar but not always interoperable
  - E.g., COSE ref to a JWK or JOSE ref to a COSE_Key by "kid"
  - Also, JOSE “kid” a string, COSE “kid” a byte array
- Many JWT and CWT claims registered in one place but not the other
  - And sometimes registered with differing definitions
- During IETF 122, we did not see interest in a unified namespace for JWP
- JSON and CBOR parameters will remain distinct but parallel, barring new feedback
  - JSON and CBOR serializations express distinct information
- JSON and CBOR serializations maintain the same structure/algorithms

Treatment of Parameters and Claims

JWP Protected Header Parameter registry

- JOSE/COSE header parameters are not used
- Strongly encourage both JSON and CBOR definitions for all parameters

JSON Proof Token

- References JWT Claims registry
- May require new claims corresponding JWP header parameters

CBOR Proof Token

- References CWT Claims registry
- Parallel to JPT

Open Issue: New BBS Extensions

- Evaluate possible use of new BBS extensions within JWP
  - draft-irtf-cfrg-bbs-blind-signatures
  - draft-irtf-cfrg-bbs-per-verifier-linkability
  - Drafts were adopted by the CFRG
- Can these be used with JWP with no updates to JWP?
  - We suspect so
- Are these useful for JWP use cases as specified?

Represented in issue #181

Open Issue: ZKP Using ECDSA

- “Anonymous Credentials from ECDSA” developed by Google
  - draft-google-cfrg-libzk and https://eprint.iacr.org/2024/2010
  - Abhi Shelat, "libZK: a zero-knowledge proof library" in CFRG session
- One opportunity (speaking with the authors) is to simplify/optimize the arithmetic circuits needed
- Should we add a JWP algorithm based on this approach?
- What additional capabilities would this give us?

Represented in issue #148

Open Issue: Sigma Protocols

- Cathie Yun, "Sigma Protocols and Fiat-Shamir" presented this week in CFRG
  - Sigma Protocols describe a three-round proof-of-knowledge, such as an algebraic relationship
  - Not enough to adopt in its current form
  - Interest in what problems it will solve within the IETF

Represented in issue #182

Participation Opportunities

- Always seeking feedback from implementers
  - Including on CBOR representation
- Adding more cryptographic algorithms to increase diversity
  - ECDSA-based ZKP
  - Post-quantum safe algorithms
  - Your suggestions?
- Interop testing

Your Turn

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