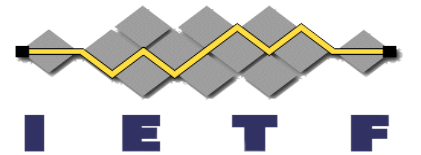


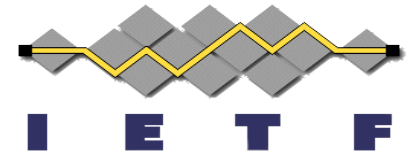
JSON Web Proofs Update

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

David Waite, Mike Jones
IETF 121, Dublin
November 4th, 2024



Progress Since IETF 120 (1 of 2)



Substantial normative and editorial updates to all 3 drafts

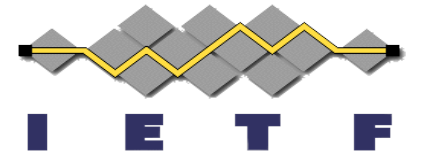
Moved to WG Github

- <https://github.com/ietf-wg-jose/json-web-proof>

-06 Drafts: September 2024

- Described ability to encrypt JWPs
 - by wrapping JWP in JWE
- Reworked descriptions of Compact and JSON Serializations
- Described detached payloads
 - Payloads can be separated from their proof

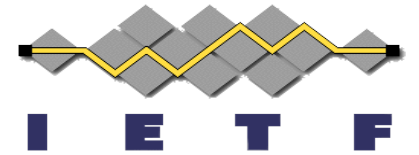
Progress Since IETF 120 (2 of 2)



-07 Drafts: October 2024

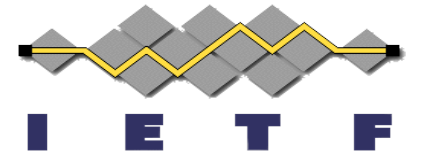
- Added CBOR Representation
 - CBOR-based encoding for headers and parameters
 - (Partially) aligned headers based on their two sources (JOSE and COSE, JWT and CWT)
 - CBOR serialization for issued and presented forms
- Registry Additions for CBOR
 - Integer names/labels for header parameters and algorithms

BBS Update



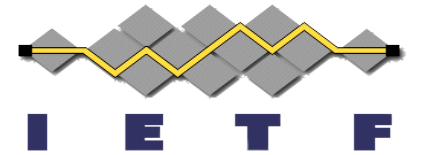
- CFRG cryptographic reviews happened in October 2024
 - Julia Hesse
 - Michele Orrù
 - Response by editor Vasilis Kalos
- New proposals discussed in cryptographic reviews
 - Blinded Values
 - Embedding payloads unknown to the Issuer
 - Pseudonymous Identifiers
 - Deriving verifier-specific identifiers from a payload

Next Steps



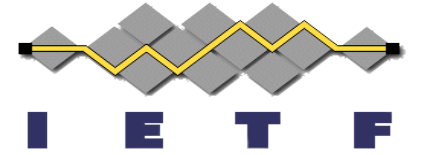
- Make decision on removal of JSON Serialization
- Evaluate possible future use of BBS extensions within JWP
 - Blinded values
 - Pseudonymous identifiers
 - But this functionality only in individual drafts
- Evaluate optionally disclosed header parameters
- Create CBOR representation for Proof Tokens

Participation Opportunities



- Seeking implementer feedback
 - Including on new CBOR representation
- Adding more cryptographic algorithms to increase diversity
 - Particularly post-quantum safe
 - Your suggestions?
- Interop testing

Your Turn



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