*

# JSON Web Proofs Specifications

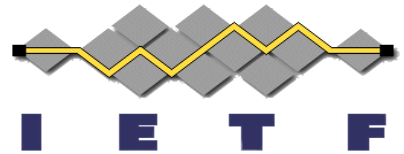
***draft-ietf-jose-json-web-proof***
***draft-ietf-jose-json-proof-algorithms***
***draft-ietf-jose-json-proof-token***

Mike Jones, David Waite, Jeremie Miller
IETF 118, Prague
November 10, 2023

# Progress Since IETF 117

- Primary change in -02 drafts was to align with draft-irtf-cfrg-bbs-signatures-03
  - Examples are now generated using Pairing Cryptography library
    - https://github.com/mattrglobal/pairing_crypto
- Addressed GitHub comments and PRs from several contributors
  - Brent Zundel
  - Alberto Solavagione (who has an implementation)

# Landscape of Related Specifications



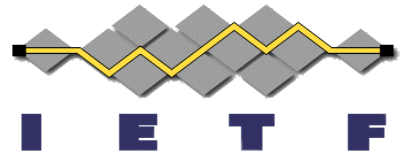

- The BBS Signatures draft continues to evolve
  - The JWP -02 drafts use BBS -03 from July 2023
  - BBS -04 published October 2023, updating proof generation & verification
  - BBS -05 publication expected shortly
  - ***JOSE WG members encouraged to review -05, when published!***

- Dependency on BLS Key Representations draft
  - draft-ietf-cose-bls-key-representations-03 the current version

# 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
- Populate the IANA Considerations sections
  - Define JWP Algorithms registry and its initial registrations
  - Define and register Content Type identifiers
- Consider additional algorithms

# Your Turn




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