JSON Web Proof

Mike Jones, David Waite

IETF 125, Shenzhen
Mar 17, 2025

Document Updates Since Montreal

*-13 drafts

- Use “proof_alg” rather than “alg” in JWKs and COSE_Keys
  - JWP algorithms are in a different registry than JOSE and COSE algorithms
- Make all cryptographic operations in examples deterministic
  - Examples now are consistent across spec rebuilds
  - Has already helped catch an issue for upcoming draft 14

What Comes Next?

Open Question: JPT Subclaim Support

- JSON Proof Tokens (JPT) constrain payloads to a set of claims
- Targets the same domains as SD-JWT/SD-CWT with newer algs
- SD-JWT/SD-CWT however, can selectively disclose parts of claims
- Registering all desired subsets (e.g. `address-city`, `address-zip`) would be untenable
- Two separate implementers proposed extremely similar solutions/syntax
  - Syntax also aligns with SD-JWT VC metadata for describing claims
- Also would like to align with `draft-mahy-cbor-pointer` if possible

Named Claims/Subclaims and Presented Form

Claims

`"given_name"`	`"John"`
`"family_name"`	`"Doe"`
`"email"`	`"johndoe@example.com"`
`"address"`	`{ "street_address": "123 Main St", "locality": "Anytown", "region": "Anystate", "country": "US" }`

Subclaim Proposal

`["address","country"]`	`"US"`

BBS Extensions

- Now have infrastructure to start experimenting with the drafts
- Not as mature as BBS Signatures. Intent is to:
  - describe using the BBS extensions in a separate document
  - capture learnings in core JWP documents

So far:

- Extensions currently require verifier support even if not used
- Will require a fair bit of setup exchange outside the JWP response

BBS Blind Signatures Support

- Allow for messages known only to the holder, not the issuer
- Primary interest is around secret keys to confirm holder

- Holder can disclose values to verifiers, however
- Need to determine if we want to support that in JWP
  - Some proposals would extend the current shape

BBS Per-Verifier Identifiers Support

- Use long-held secrets to generate pseudonyms per verifier
- Still a bit early, some use case usability issues

Your Feedback

- What would you like the working group to know or consider?