JSON Web Proofs
Initial Drafts

Jeremie Miller
Overview
JSON Web Proofs

What it is

- A new container format, in the family of JOSE containers (JWS, JWE, JWP)
- Aims to support newer algorithms and cryptographic techniques for new privacy-preserving applications such as "anonymous credentials" use cases
- Establish the role of a holder, which has limited capabilities to derive new restricted messages from an original issued message
- Enables messages that can still be cryptographically verified but not correlated when presented to different verifiers
JSON Web Proofs
What it is

Examples of capabilities an algorithm may support include:

- Selectively disclose a subset of information to the verifier
- Multiple uses of a proof without correlation from underlying cryptography
- Answer a predicate without disclosing the data used for evaluation
- Proof of possession
JSON Web Proofs

History

• Early 2021 - Initial ideas circulated in the OpenID Connect SIOP community by Jeremie Miller and David Waite

• Mid 2021 - Decided the effort needed incubation before any standards org, was adopted as a DIF work item in their Applied Crypto WG

• Late 2021 / Early 2022 - Regular meetings and many discussions resulting in the initial -00 drafts with much guidance and input from Mike Jones

• Mid 2022 - Recognition that the work constituted a notable advancement of the JOSE family to support Zero-Knowledge Proofs and related privacy structures
JSON Web Proof Specifications

- Single Use
- BBS
- zkSNARK

- draft-jmiller-jose-json-proof-algorithms
- draft-jmiller-jose-json-proof-token
- ...
JWP Design Factors
Adopt W3C Verifiable Credentials Terminology
Issuer, Holder, and Verifier

- Large community with a common understanding of the three roles
- Makes it easier to talk about the privacy primitives based on each role

**Issuer** - Signs the message

**Holder** - Holds and presents the message

**Verifier** - Verifies the message
Two Interrelated Privacy Features
Selective Disclosure & Unlinkability

• **Selective Disclosure** - capability for the holder of a message to reveal only a subset of that message while maintaining its verifiability
  - The issuer divides the message into disclosable subsets
  - The holder creates a presentation that is the selected subset

• **Unlinkability** - ensuring nothing inherently links one presented message with another
  - Easy - the issuer can generate single-use messages with different signatures
  - Hard - the holder can present a single message multiple times by generating a unique proof for each verifier
KISS
Advanced crypto is already hard enough

• Strove to adhere to the principle “What would JOSE do?”
• Core JWP draft is minimal container formatting only
• Support techniques adoptable today (Single-Use, Hashes)
• Support new signature types with necessary capabilities (BBS)
• Remain flexible to support more advanced crypto as it evolves (DL-PoK, ZKPs, Mercurial, predicates, verifiable compute, etc)
Comparison of JWP and JWS
Classic JSON Web Signature

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM...
SflKxwRJSMeKKF2QT4fwMeJf36POk6yJV_adQsssw5c
Classic JSON Web Signature

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM.
SflKxwRJSMeKKE2OT4fwMeJf36POk6yJV_adQssw5c

Protected Header
Payload
Signature
JSON Web Proof

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFt~Sl6lkpvaG4gRG9lIiwiaWF0IjoxNTE2M~JhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9ey.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
JSON Web Proof

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2M
ioxNTE2M~
JhbGciOiJIUzI1NisinR3cCI6IkpXVCJ9eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZ~yJV_adQssw5c
SflKxwRJSMMeKKE3OT4fwpMeJf36POk6
yJV_adQssw5c
JSON Web Proof

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZ
~~.SflKxwRJSMeKKF2QT4fwpMeJf36P
Ok6v.IV_adOssw5c

Two Omitted Payloads
Links

https://www.ietf.org/archive/id/draft-jmiller-jose-json-web-proof-00.html

https://www.ietf.org/archive/id/draft-jmiller-jose-json-proof-algorithms-00.html

https://www.ietf.org/archive/id/draft-jmiller-jose-json-proof-token-00.html