The Need: Standards for Selective Disclosure and Zero-Knowledge Proofs

Michael B. Jones
Identity Standards Architect, Microsoft

JSON Web Proofs BoF
IETF 114, Philadelphia
July 25, 2022
The Success of JOSE and its Roles

- JOSE and JWT have been widely adopted for identity use cases
  - Including for OpenID Connect and STIR
- Its model has two roles:
  - Issuer and Recipient
  - Issuer typically knows who the intended Recipient (the audience) is
  - All claims are disclosed to the Recipient
New Developments and New Roles

- Newer solutions such as Verifiable Credentials have three roles:
  - Issuer, Holder, and Verifier
  - Designed to enhance privacy

- These separate credential issuance from credential presentation:
  - Issuer typically does not know who the verifier is or what subset of issued claims will be disclosed to it

- JOSE/JWT is an adopted representation for VCs:
  - However, JWS and JWT have limitations that make privacy protection challenging
JOSE/JWT Limitation: Selective Disclosure

- Clunky to use JOSE/JWTs for Selective Disclosure
- Requires issuing custom JWTs containing only the disclosed claims in real time
- Requires Issuer to be online
- Lets Issuer know who the Holder is and what claims it wants
- “Call-home” to issuer on every use not privacy preserving
JOSE/JWT Limitation: Unlinkability

- Desirable to perform identity-related interactions without identifying the participants and enabling correlation
- Again, clunky to do with JOSE/JWTs
- Workaround is to request a new token per Verifier from the Issuer each time
- Or pre-issuing batches of tokens to use a different one per Verifier
  - Such that they are single-use tokens
New Cryptography – New Formats

- Overcoming these limitations efficiently and securely a subject of much academic and applied-cryptography research
  - Often referred to as “Anonymous Credentials”
- Cryptographic techniques developed include pairing-friendly curves and zero-knowledge proofs

- Existing JOSE and JWT specs not capable of utilizing these new cryptographic techniques
The Need

- JSON representations for the new cryptographic techniques
- A working group to standardize these representations in

More will be said about applications and use cases shortly…
WHAT
WOULD
JOSE
DO?
Why re-form the JOSE WG?

- We’re defining a new JSON-based cryptographic format
  - JOSE defined the JWS and JWE (and JWK) formats
  - The JSON Web Proof (JWP) format parallels them, but for new cryptographic techniques, effectively expanding the JOSE family
- The JOSE working group participants are the right people
  - Existing expertise defining practical JSON-based cryptographic representations
- Why not the COSE working group?
  - COSE members specialize in compact binary representations
  - JSON has more limitations than CBOR, making JOSE a better fit
Proposed New Charter for JOSE

- Proposed charter text included in BoF proposal

- Structure of the charter text is:
  - Review of JOSE’s past deliverables
  - Motivation for new work
    - (Previous section of this presentation covers the same content)
  - Chartered Deliverables
Chartered Deliverables (1 of 2)

• An Informational document detailing **Use Cases and Requirements** for the new JSON Object Signing and Encryption (JOSE) specifications enabling selective disclosure and zero-knowledge proofs.

• Standards Track document(s) specifying **representation(s) of independently-disclosable integrity-protected sets of data and/or proofs** using JSON-based data structures, which also aims to prevent the ability to correlate by different verifiers.

• Standards Track document(s) specifying **representation(s) of JSON-based claims and/or proofs** enabling selective disclosure of these claims and/or proofs, and that also aims to prevent the ability to correlate by different verifiers.
Chartered Deliverables (2 of 2)

- Standards Track document(s) specifying new algorithms and algorithm identifiers.
- Standards Track document(s) specifying how to represent keys for these new algorithms as JSON Web Keys (JWKs).
- An Informational document defining test vectors for these new JOSE specifications.
- Standards Track document(s) defining CBOR-based representations corresponding to all the above, building upon the COSE and CWT specifications in the same way that the above build on JOSE and JWT.