NTP WG @ IETF 115
Chair Slides
Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF’s patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- **BCP 9** (Internet Standards Process)
- **BCP 25** (Working Group processes)
- **BCP 25** (Anti-Harassment Procedures)
- **BCP 54** (Code of Conduct)
- **BCP 78** (Copyright)
- **BCP 79** (Patents, Participation)
Draft Agenda

1. Admin and Agenda Bash (Chairs - 5 minutes)

2. Charter review (Chairs - 10 minutes)

3. JSON Web Proof Drafts (Mike Jones - 30 minutes)
   -- JSON Web Proofs
   -- JSON Proof Algorithms
   -- JSON Proof Token

4. X.509 Certificate Extended Key Usage (EKU) (Migault - 10 minutes)

5. Way Ahead and AOB (Chairs - 5 minutes)
Charter (Rationale)

The original [JSON Object Signing and Encryption (JOSE) working group][1] standardized JSON-based representations for: Integrity-protected objects (JSON Web Signatures/JWS, RFC 7515), Encrypted objects (JSON Web Encryption/JWE, RFC7516), Key representations (JSON Web Key/JWK, RFC 7517), Algorithm definitions (JSON Web Algorithms/JWA, RFC 7518), and Test vectors for the above (Examples of Protecting Content Using JSON Object Signing and Encryption, RFC 7520).

These were used to define the JSON Web Token (JWT) (RFC 7519), which in turn, has seen widespread deployment in areas as diverse as [digital identity][2] and [secure telephony][3].

As adoption of these standards to express and communicate sensitive data has grown, so too has an increasing societal focus on privacy. User consent, minimal disclosure, and unlinkability are common privacy themes in identity solutions.

A multi-decade research activity for a sizeable academic and applied cryptography community has focused on these privacy and knowledge mechanisms (often referred to as anonymous credentials). Certain cryptographic techniques developed in this space involve pairing-friendly curves and zero-knowledge proofs (ZKPs) (to name just a few). Some of the benefits of ZKP algorithms include unlinkability, selective disclosure, and the ability to use predicate proofs.

The current container formats defined by JOSE and JWT are not able to represent data using ZKP algorithms. Among the reasons are that most require an additional transform or finalize step, many are designed to operate on sets and not single messages, and the interface to ZKP algorithms has more inputs than conventional signing algorithms. The reconstituted JOSE working group will address these new needs, while reusing aspects of JOSE and JWT, where applicable.
Charter (Goals & Milestones)

This group is chartered to work on the following goals:

- An Informational document detailing Use Cases and Requirements for new specifications enabling JSON-based 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.
- Standards Track document(s) specifying how to use existing cryptographic algorithms and defining their algorithm identifiers. The working group will not invent new cryptographic algorithms.
- 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 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.

One or more of these goals may be combined into a single document, in which case the concrete milestones for these goals will be satisfied by the consolidated document(s).
An informal goal of the working group is close coordination with the [rechartered W3C Verifiable Credentials WG][4], which has taken a dependency on this work for the second version of its Verifiable Credentials specification. The working group will also coordinate with the [Selective Disclosure JWT][5] work in the [OAuth][6] working group, the [Privacy Pass][7] working group, the [CBOR][8] working group, and the [CFRG][8].
Way Ahead and AOB

- AOB
- Define Milestones
- Virtual Interims?