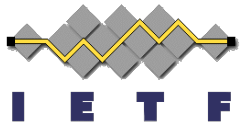
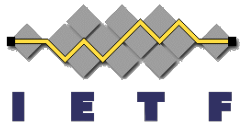
JSON Web Proofs Virtual BoF

Presenter Slides



Jeremie Miller and Michael B. Jones

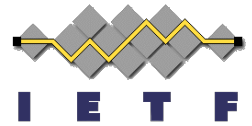
12 October 2022
1700 UTC



Presenters' Part One

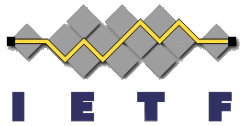
THE PROBLEM

Existing JOSE Cryptography Formats



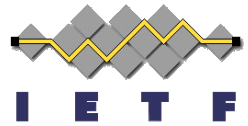
- JOSE is a widely adopted container format for Keys, Signatures, and Encryption
  - JSON and Web friendly
  - Cryptographic agility
  - Vetted underlying algorithms
- JOSE is unable to represent the growing category of Zero-Knowledge Proofs (ZKPs)
  - Most require an additional ***transform*** or ***finalize*** step
  - Many are designed to operate on ***sets*** and not single messages
  - Interface to ZKP algorithms has more inputs than conventional signing algorithms

Zero Knowledge Proofs (ZKPs)



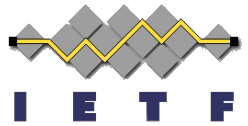
- ZKPs a result of decades of cryptographic research
  - Interest in deployment now due to increasing focus on privacy
- Different types of ZKPs
  - Proofs of Knowledge
  - Pairing Cryptography
  - Multi-party Computation
  - Ring and Threshold Signatures
  - Witness Protection
- ZKPs enable many capabilities
  - Selective Disclosure
  - Unlinkability
  - Predicate Proofs
  - Verifiable Computation
- Today, every application of a ZKP is forced to design its own custom container
  - Specific to the application – blockchain, Privacy Pass, anoncreds, etc.
  - Specific to the algorithm – greatly reduced agility

Popular ZKP Algorithms



- Small sample of popular ZKP Algorithms
  - BBS – https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/
  - CL Signatures – https://eprint.iacr.org/2012/562.pdf
  - Mercurial Signatures – https://eprint.iacr.org/2020/979
  - PS Signatures – https://eprint.iacr.org/2015/525.pdf
  - zkSNARKs – (numerous)
  - VOPRFs / DLEQ – https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/
  - Schnorr – https://www.rfc-editor.org/rfc/rfc8235
  - Algebraic MACs – https://eprint.iacr.org/2013/516
  - Pedersen Commitments – https://arxiv.org/abs/1705.05897

JWP in a Nutshell

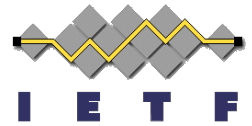


"JWE represents confidentiality protection, JWS represents authenticity/integrity protection, JWP represents ...? What is the single, clear cryptographic function that JWP would provide?"

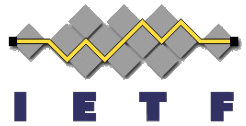
-- Richard Barnes during the initial JWP BoF

- JWS → Authenticity and Integrity Protection
- JWE → Confidentiality Protection
- JWP → Knowledge Protection

Interest in Solving the Problem

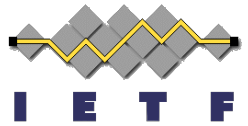


- W3C Verifiable Credentials 2.0 Working Group
  - Charter includes dependency on JWP
  - https://www.w3.org/2022/06/verifiable-credentials-wg-charter.html
- Decentralized Identity Foundation (DIF)
  - Incubated JWP specs in Applied Crypto WG
  - Then explicitly requested the IETF to take over the work
- IRTF CFRG
  - Standardizing BLS ZKP cryptography operations
  - Needs container formats, such as JWP
- Who else attending the BoF is interested?



Back to the Chairs

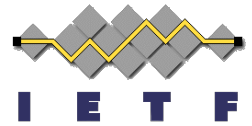
ATTENDEE DISCUSSION OF THE PROBLEM



Presenters' Part Two

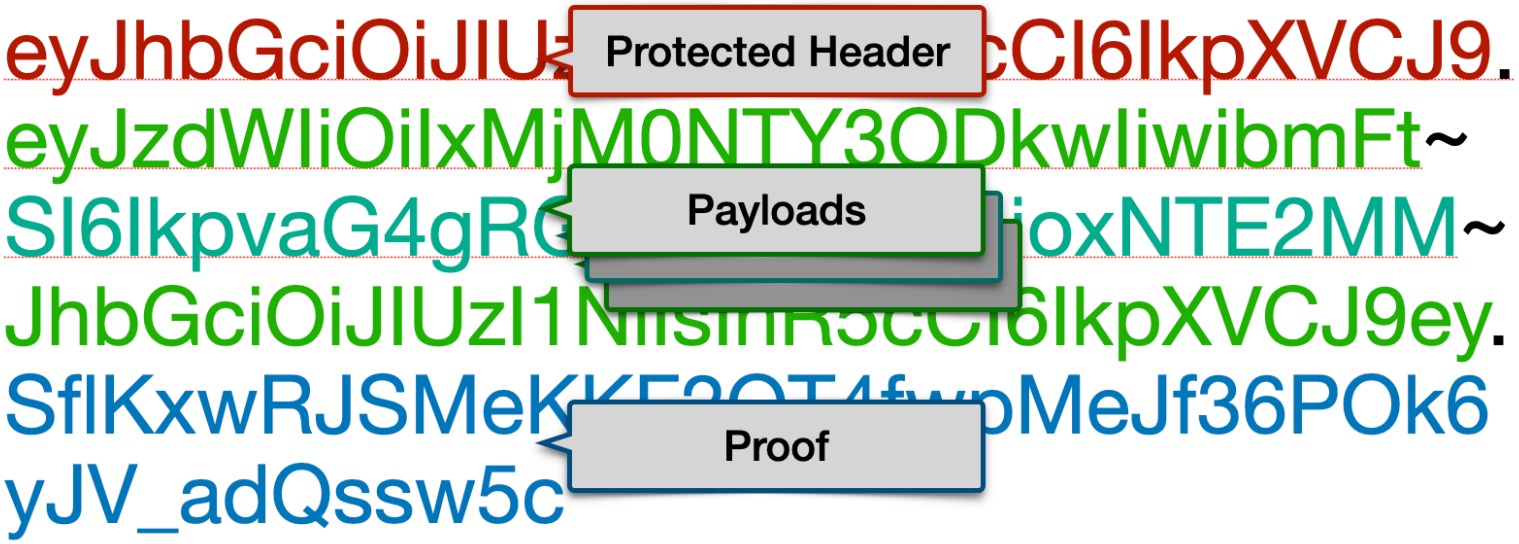
A POSSIBLE SOLUTION

JWP a Possible Solution



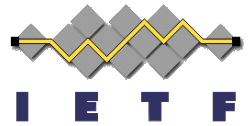
- JWP: A JSON-based Cryptographic Container Format for ZKPs
- Current JSON Web Proof drafts
  - https://www.ietf.org/archive/id/draft-jmiller-jose-json-web-proof-00.html
  - https://www.ietf.org/archive/id/draft-jmiller-jose-json-proof-algorithms-00.html
  - https://www.ietf.org/archive/id/draft-jmiller-jose-json-proof-token-00.html
- Demonstrate feasibility of solving the problem
- Could serve as a starting point for the WG (should one be chartered)
  - Supports multi-message algorithms
  - Supports unlinkability
  - Uniform algorithm interfaces supporting cryptographic agility
  - Strives to achieve JOSE-style simplicity and familiar patterns
  - Reuses parts of JOSE where appropriate

JWP Example

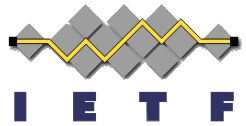


- Should look familiar if you who know the JWS Compact Serialization

We're not here to bikeshed solution

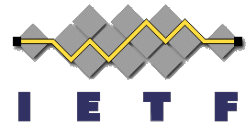


- That's the job of the working group (if chartered)
- We discussed JWP to demonstrate existence proof of solution
  - Not to imply that it's complete or immutable



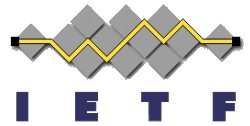
ANSWERING KEY QUESTIONS FROM THE LAST BOF

What about JWS and JWT?



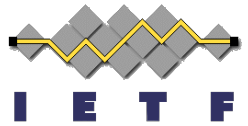
- Isn’t JWS and/or JWT enough?
- JOSE is unable to represent ZKP inputs and outputs
  - Most require an additional ***transform*** or ***finalize*** step
  - Many are designed to operate on ***sets*** and not single messages
  - Interface to ZKP algorithms has more inputs than conventional signing algorithms

What about SD-JWT?

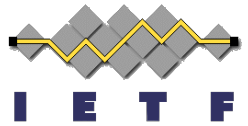


- OAuth WG is developing Selective Disclosure JWT (SD-JWT)
  - “specifies conventions for creating JSON Web Token (JWT) documents that support selective disclosure of JWT claim values”
  - https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/
- Isn’t SD-JWT enough?
  - SD-JWT doesn’t enable use of ZKP algorithms
    - And all the capabilities that come with them
  - JWP does

What about CBOR?



- The WG could choose to also create a CBOR-based container
  - CBOR representation included in the proposed charter
- As discussed in Philly, JSON has more restrictions than CBOR
  - So we're starting with the JSON-based container
  - CBOR should actually be easier



Back to the Chairs

ATTENDEE DISCUSSION OF SOLUTIONS