JSON Web Proofs - JWTs with Superpowers

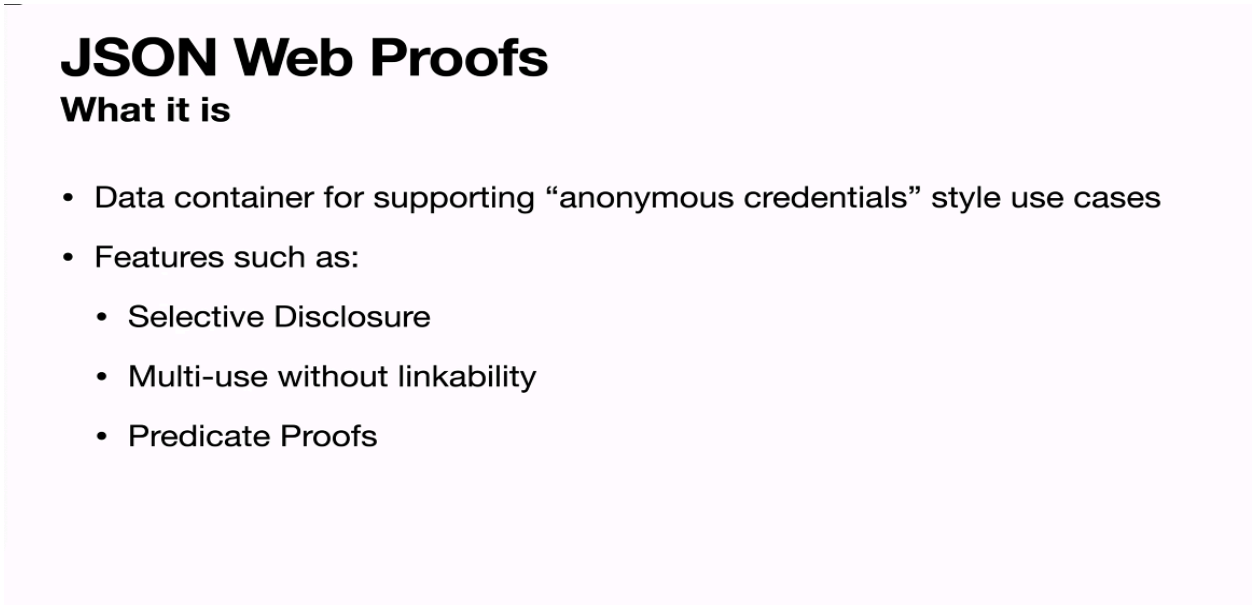
Thursday 20A
Convener: David Waite
Notes-taker(s): Andrew Hughes

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

Github: https://github.com/json-web-proofs/json-web-proofs
Slides: https://github.com/json-web-proofs/documentation/blob/main/JSON%20Web%20Proofs%20IIW%20XXXIII.pdf
DIF Applied Crypto Slack: https://difdn.slack.com/archives/C021JUSRXC0

Notes:

- 40+ attendees
- Work happening at DIF
- Screen shots of slides follow - go to the github link above to get updated versions



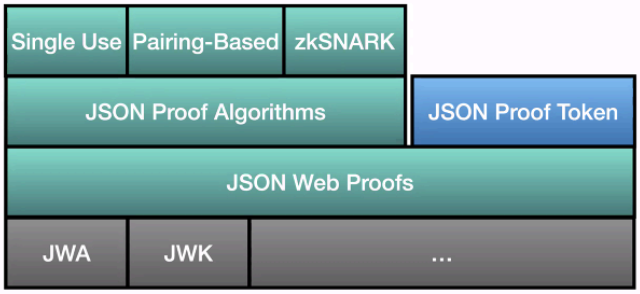
- Supports a wide array of algos

JSON Web Proofs
Standards Relations

- Incubated within Decentralized Identity Foundation Advanced Crypto WG
- Very Early!
- JOSE (JSON Object Signing and Encryption) inspired
  - Various JWA, JWK, JWT dependencies
- Would like to see it moved to IETF following incubation
- Also motivated to define an equivalent CBOR-format container

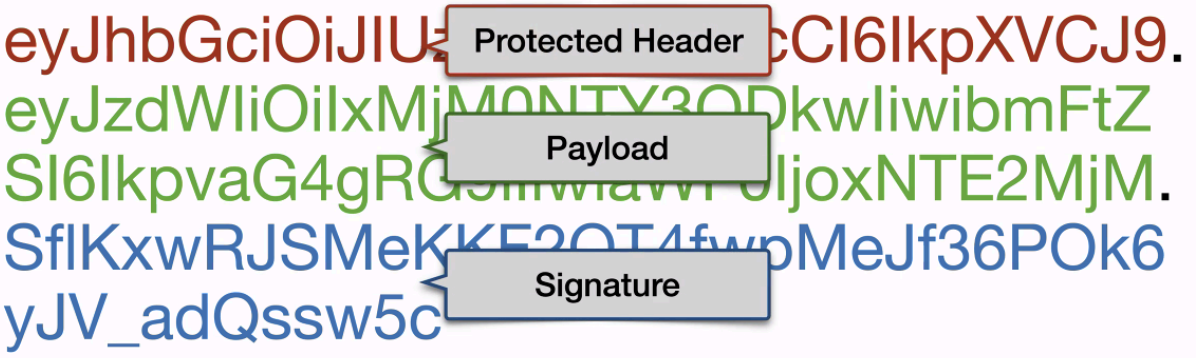
- DIF group = Applied Crypto WG
- IETF has their own crypto tech research group

JSON Web Proof Structure
(As envisioned)

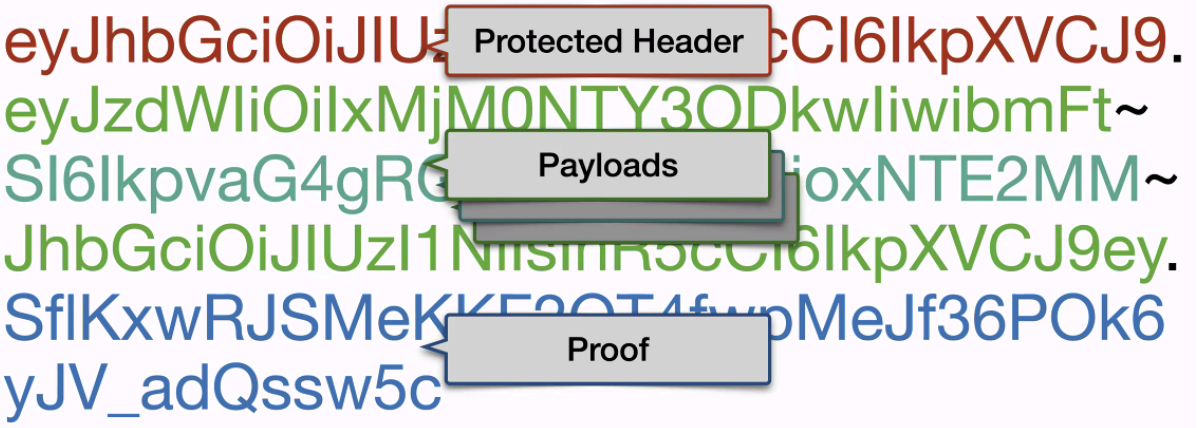


- JSON Proof algorithms - defines the primitives needed for the algos
- Top layer - a realization of how to use the system

Classic JSON Web Signature



JSON Web Proof



- Similar to JWS - but has multiple payloads
- Can omit payloads

JSON Web Proof

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZ
~~.SflKxwRJSMeKKF2QT4fwpMeJf36P
Ok6yJV_adQssw5c

Two Omitted Payloads

JSON Proof Token

For Token/Credential-style Use-cases

«Protected Header»

```
{
  "alg": "ES256",
  "typ": "JWT"
}
```

«Payload»

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

JWT Example

«Protected Header»

```
{
  "alg": "ES256+SU",
  "typ": "JPT",
  "kid": "12345"
}
```

«Payloads»

```
"1234567890"

"John Doe"

1516239022
```

JPT Example

JSON Proof Token

For Token/Credential-style Use-cases

```
{
   "jwks": [
      {
         "kid": "12345",
         …,
         "token-payloads": [
            { "claim": "sub" },
            { "claim": "name" },
            { "claim": "iat" }
         ]
      }
   ]
}
```

Issuer Metadata

```
«Protected Header»
{
  "alg": "ES256+SU",
  "typ": "JPT",
  "kid": "12345"
}
«Payloads»

"1234567890"

"John Doe"

1516239022
```

JPT Example

- The issuer metadata defines how the right side should be interpreted
- Q: is the jwks normative? Wonders about the presence of the token-payloads
  - A: not finalized yet - need some level of metadata in there
- Q: is the token-payload an ordered list? A: yes
- Q: The threat model makes sense (of not wanting to leak # of claims etc), but doesn't the token-payloads property do that?
  - A: yes - to the same degree that a particular kid at a particular issuer does

Single Use Scheme

- Proof is simply a concatenation of signatures, e.g.
  Sig(*header* || *Sig(payload$_1$)* || … || *Sig(payload$_n$)*) || Sig(payload$_1$) || … || Sig(payload$_n$)
- One could imagine a variety of other approaches (seeded Merkel tree, etc)
  - Multiple signatures is just easier to specify and implement
- Allows for use of NIST approved algorithms, out-of-box crypto support (including secure element usage)
- Does not expose some primitives needed for a subset of predicate algorithms
  - Other approaches available for selective disclosure, such as hash chains

- When doing selective disclosure & reveal some and hide others - the proof value itself will include randomized proofs of each value whether or not it’s revealed

- Q: What's the strategy for preventing a holder generating a JWP and handing it to another person who presents it on their behalf?
    - A: a bit out of scope. But it comes down to the binding at issuance. The JWP is created by the Issuer - to it's their level of assurance/binding - hardware bound? Software bound? If the issuer gets a hardware attestation, then there' stronger prevention for private key sharing. If private key in software there's not much to prevent.
    - A: could emit several VCs, some of which are strongly bound
- Q: most zkSnarks require a trusted third party - who is that in this case?
    - A: it will be part of the algo - e.g. if you use this algo, you need a 'trusted setup' - might be the trust framework.
- Q: if have zkSnarks, why support selective disclosure? SD just slows down the rate at which people find out your data. All the privacy attacks boil down to a verifier being able to arbitrarily choose the challenge. Sees no projects that define what a challenge is - and force a verifer to commit to what kind of challenge must be. Verifier could ue a "20 questions" attack. Selective disclosure allows fingerprinting holders so they can be tracked between presentations. Humans won't be able to monitor the challenge-responses fingerprinting. Need a commitment by a verifier in the form of a verifiable computation. So holder can check their verifiable computation in advance. Arbitrary challenges formed by the verifier is a chosen text attack on privacy.
    - A: Presentation exchange is the problem, not selective disclosure. However JWP is the container - not the policy of how the interaction works.
      @David Huseby: I 100% agree, and it's not been addressed anywhere yet:
      https://github.com/decentralized-identity/presentation-exchange/issues/204
- Q; interesting - if i codify my privacy policy about my need for specific data - is there a legal binding at the protocol level? Verifiers need to define their data requirement and and the data use policy - should we push this into the protocol? No. But verifiers should have to codify it into machine readable.
    - A:
- Q: Could I think JSON + JWP as a kind of simpler alternative of JSON-LD + LD-Proof?
  For me it looks like: JSON + JWP === JSON-LD + LD-Proof - LD*
  (*: data linking feature with complex RDF things...)
    - A: Dan: yes, that is a goal, both a simpler alternative but also one that supports a wider range of capabilities
- Q: Responding to statement that people are not aware of algo properties and consequences. Please all educate each other - we need to increase 'known' stuff.
    - In the work - we are working out the proper layering. There will be more situations that will need more knowledge about the choices implications/consequences to avoid problems.
- Q: strongly don't disagree ;-)
    - Highly encourage joining the Applied Crypto slack and mailing lists - good discussions
- Q; about binding, its an open research question - no final answers yet. Can use verifiable computations to do deciding functions to avoid having to share private data _ever_
    - Want's to hear about the research
    - There's a tacit assumption that for humans a biometric will be sent along with the selected disclosure - e.g. a photo along with covid certificate
    - We will need to tie the hands of the verifiers so that they must reveal their business logic
    - Huesby wrote an essay in the Applied Crypto chat :-)
    - **DIF Applied Crypto Slack: https://difdn.slack.com/archives/C021JUSRXC0**

- Q: isn't this the point of Presentation Exchange? RP telling Holders what they want to receive in the presentation? It's hard to get down to a single set of expressions due to the broad range of requirements. Eventually PE will include the ability to state that a presentation must conform to a specific trust framework or specification.
    - A: Yes - that's exactly the thing.
    - A: envision that a credential request could be the equivalent of a Swagger/OpenAPI document
- Q: Where is the use case for using the signature scheme- what's the added value to the existing schemes?
    - A: The approach combines the selective disclosure and the unlinkability - to ensure that nothing in the container makes it easy to introduce linkability. Also to easily drop in different signature algos. So they can all use the same container format - just like JOSE patterns do - same approach.
- Q: Was in the UProve TAG - experience with integrating it for application layer. Didn't need new specs/formats. What's the pitch/justification/need for a new format?
    - A: One objective is to support multi-use credentials. This allows the Holder to present multiple time to multiple audiences - without causing linkability by default.
    - Current view is that thi can't be achieved by existing JOSE specs.