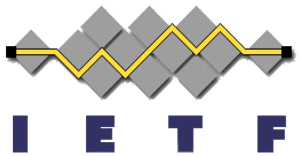
*

Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)



draft-jones-ace-cwt-proof-of-possession

Michael B. Jones
IETF 99, Prague
July 2017

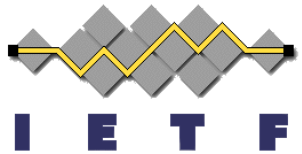
Background

- RFC 7800 – Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs) – defines a representation for proof-of-possession keys in JWTs, for example:

```
"cnf":{
  "jwk":{
    "kty": "EC",
    "use": "sig",
    "crv": "P-256",
    "x": "18wHLeIgW9wVN6VD1Txgpqy2LszYkMf6J8njVAibvhM",
    "y": "-V4dS4UaLMgP_4fY4j8ir7cl1TXlFdAgcx55o7TkcSA"
  }
}
```

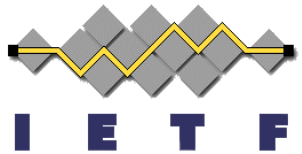
- Equivalent functionality desirable for CBOR Web Tokens (CWTs)

Similar CWT PoP representation in two drafts



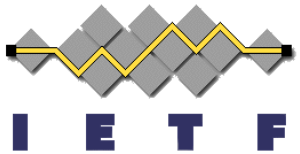
- draft-ietf-ace-oauth-authz and draft-jones-ace-cwt-proof-of-possession independently made essentially the same choices
- draft-jones-ace-cwt-proof-of-possession contains only the port of RFC 7800 from JSON/JWT to CBOR/CWT
- draft-ietf-ace-oauth-authz also contains the ACE OAuth functionality

Similar CWT PoP representation in two drafts



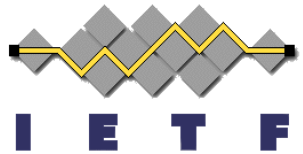
- draft-ietf-ace-oauth-authz and draft-jones-ace-cwt-proof-of-possession independently made essentially the same choices
- draft-jones-ace-cwt-proof-of-possession contains only the port of RFC 7800 from JSON/JWT to CBOR/CWT
- draft-ietf-ace-oauth-authz also contains the ACE OAuth functionality

Why have CWT PoP be in it's own draft?



- Like CWT, PoP for CWT will be used in many application contexts, both for ACE and non-ACE use cases
  - Hannes surveyed several working groups and a number of individuals responded saying that they have non-ACE use cases
- The CWT PoP functionality is simple, directly based on RFC 7800, and needs no further work
- If adopted by the WG, it could quickly go to WGLC
  - IETF and IESG reviews should go smoothly since it invents no functionality not already in RFC 7800
- ***draft-jones-ace-cwt-proof-of-possession could become an RFC within a few months***

Credit Where Credit Is Due



- Several people contributed to the CWT PoP functionality in draft-ietf-ace-oauth-authz – especially Ludwig Seitz
- All the ACE OAuth draft authors are also authors on the standalone draft

Next Steps

- Question to the working group:
  - Should draft-jones-ace-cwt-proof-of-possession be adopted as a WG document?
- Question to the chairs:
  - If adopted, do you believe that we should then start WGLC?