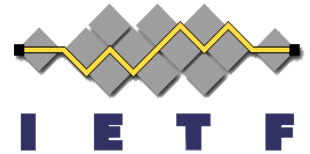


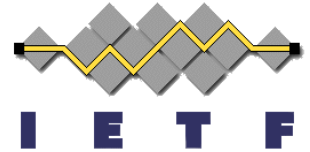
# Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)

**draft-ietf-ace-cwt-proof-of-possession**

Michael B. Jones  
IETF 101, London  
March 2018

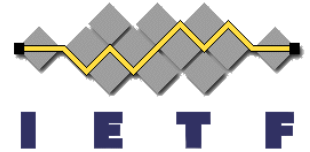


# Status



- draft-ietf-ace-cwt-proof-of-possession-02 addressed existing review comments
  - Including some of Jim Schaad's comments on -00 that we didn't get to in -01
  - I believe that Jim owes us suggested text on a few of his outstanding comments on -00
  - The editors did not accept comments that suggested significant divergence from RFC 7800

# Next Steps



- At IETF 99 we decided to try to do this fast
- It's a simple draft that intentionally parallels RFC 7800 in structure and content
- Note that CWT has gone to the RFC Editor
  - CWT PoP also required for many ACE specs
- I believe that this now ready for WGLC