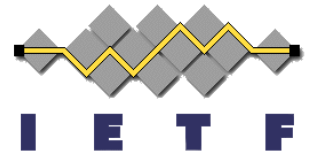


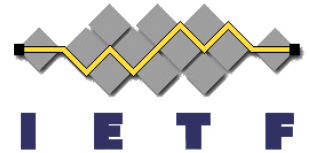
# Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)

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

Michael B. Jones  
IETF 100, Singapore  
November 2017

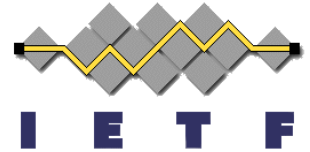


# Status



- draft-jones-ace-cwt-proof-of-possession-01 adopted as draft-ietf-ace-cwt-proof-of-possession-00 after IETF 99
- New in WG -01 draft:
  - Now uses CBOR diagnostic notation for the examples (*thanks to Ludwig Seitz*)
  - Added table summarizing “cnf” values
  - Addressed some of Jim Schaad’s comments on -00

# Next Steps



- At IETF 99 we decided to try to do this fast
- Thorough reviews now requested – providing necessary data to keep this moving
  - Thanks to Jim Schaad for already doing this
    - Authors will finish addressing Jim’s comments shortly
  - Can we get additional volunteers to review?