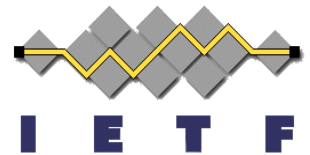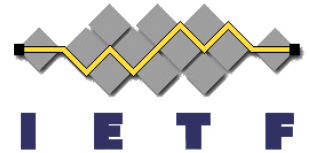# Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs)

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

Michael B. Jones
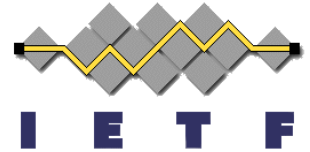IETF 103, Bangkok
November 2018

Status

- CWT PoP is a simple spec that intentionally parallels RFC 7800 in structure and content

- CWT became RFC 8392 in May

  - CWT PoP is also required for many ACE specs

- We conducted WGLC after IETF 101

  - Draft -03 addressed most review comments

  - Draft -04 addressed the remainder of them

Changes in -04

- Very few changes:
  - Removed two unnecessary and confusing sentences
  - Corrected type descriptions in IANA registrations
- See thread "RE: Summarizing WGLC discussion of draft-ietf-ace-cwt-proof-of-possession" for detailed responses to all outstanding comments
  - Thanks to Roman Danyliw for compiling list

Next Steps
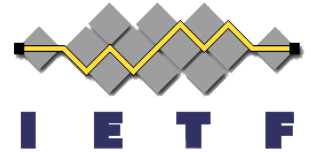
- Time for shepherd review
- Then address shepherd comments and request publication