EDHOC + Traces

draft-ietf-lake-edhoc-22
draft-ietf-lake-traces-08
https://github.com/lake-wg/edhoc

IETF 118, LAKE WG, November 6, 2023

Since IETF 117

- —edhoc-21
  - —IESG review updates
- —edhoc-22
  - —Minor update, approved by IESG, sent to RFC Editor
  - —Temporarily stalled due to IANA discussion, now back to RFC Editor

- —traces-06
  - —IESG review updates
- —traces-07
  - — Added invalid traces
- — traces-08
  - —Minor update, approved by IESG, sent to RFC Editor

edhoc-20 → edhoc-21

- Recommendation to use chain rather than bag
- Changed the use of English in error message from requirement to recommendation
- Clarified transport requirements
- Updated security considerations
  - additional post-quantum considerations
  - clarified recommendation about threat model considerations
  - clarified limitation of denial-of-service mitigations
  - some text moved between sections

edhoc-21 → edhoc-22

— Recommendation about transport

Recent IANA discussion

— Overlapping IANA registrations detected:
  1. EDHOC defines two new COSE header maps
     — ”kcwt”: a CBOR Web Token (CWT) containing a ’cnf’ claim with a COSE_Key
     — ”kccs”: a CWT Claims Set (CCS) containing a ’cnf’ claim with a COSE_Key
  2. draft-ietf-cose-cwt-claims-in-headers defines a generic COSE header map for a CCS
     — overlaps with ”kccs”
— According to guidelines to experts about these registers, overlap should be avoided

— First expert: Consider register generic CCS in EDHOC (minor change)
  — EDHOC taken out of RFC Editor’s queue pending this
— Second expert: Further specification of the use of CCS needed in draft 2
— Resolution from EDHOC point of view: No change, back to RFC Editor

traces-05 → traces-06

- Traces aligne with edhoc-22
- Verified by two independent implementations
  - Mališa added as co-author
- Clarifications and editorials

traces-06 → traces-07

—New section with invalid traces
—Merged sections 1 & 2
—Clarified normative text
—Additional references

traces-07 → traces-08

—One case of invalid trace removed

—Clarifications and editorials