EDHOC

draft-ietf-lake-edhoc-06

LAKE interim, April 2021

Göran Selander

Main Changes -05 → -06

- New section 5.2 "Message Processing Outline"

- Optional initial byte in message 1 = (
  ? C_1 : null,
  . . .
- Presence of C1 included in applicability statement

- Errors messages
  - New format as agreed IETF 110
  - Table of error codes
  - IANA registry
- Change of recommendation for CoAP
  - "SHOULD be sent as successful request and response (e.g. POST and 2.04 (Changed)"
    →
    "does not restrict how error message are transported”

- Test vectors
  - Added assumption C1 (= null) not present to test vectors
  - Same test vectors as in -05

Main Changes -05 → -06

- Applicability statement
  - Overlapping content in 3.7 and appendix C
  - Merge content into 3.7
  - Change title of 3.7 to "Applicability Statement"

- Deterministic CBOR
  - Always used
  - In case of CRED_x:
    “COSE_key parameters SHALL be encoded in bytewise lexicographic order of their deterministic encoding”

- New section on message deduplication
- New appendix containing all CDDL definitions
- New appendix with change log

- Removed section "Other documents referencing EDHOC”
  - References analysing security included in security cons
- Updated text of the use of TEEs
-

- Clarifications (reviews from Peter van der Stok, Marco Tiloca)
- Updated references, RFC 8152 → (-struct, -algs)