EDHOC implementations

LAKE, IETF 109, November 2020

Test Vectors

- Test vectors in -02
  - Detailed step-by-step description of message creation
  - 2 methods:
    - Method 0: EDHOC Authenticated with Signature Keys and X.509 certificates
      - hash value 'x5t' is used to identify the certificate
    - Method 3: EDHOC Authenticated with Static Diffie- Hellman Keys and COSE_Key
      - Kid is used to identify the credential, encoded as COSE_Key

- Extensive set of test vectors on Github
  - https://github.com/lake-wg/edhoc/blob/master/test-vectors/vectors.txt
  - Test vector for Error message in progress

Interop Plans

- Interest: Fraunhofer AISEC, INRIA, RISE …
  - December timeframe if suitable for implementers
  - Test suite in progress (based on test vectors)

More participants are welcome!

- More info to come on the LAKE mailing list