Hackathon report

IETF 114, LAKE WG, July 27\textsuperscript{th}, 2022
Testing

› Two implementations aligned with the latest version -15 of EDHOC
  – Mališa Vučinić (INRIA): Rust/hacspec [1][2]
  – Marco Tiloca (RISE): Java (Eclipse Californium)

› Mališa: Initiator ; Marco: Responder
  – Cipher suite: 2 (curve P-256)
  – Method 3: Static-Static
  – Credential Type: CCS for both peers
  – ID_CRED Type: ‘kid’ for both peers (int on the wire)
  – Minimum possible size for message_2 (45 bytes)
  – Correctly completed EDHOC execution

› More implementations are under ongoing update
  – More tests are expected in the near future

[1] Denis Merigoux, Franziskus Kiefer, Karthikeyan Bhargavan. Hacspec: succinct, executable, verifiable specification for high-assurance cryptography embedded in Rust, https://hal.inria.fr/hal-03176482/document
Thank you!