EDHOC Interop #5

LAKE WG Virtual Interim Meeting, June 1st, 2021

Report from Interop #5

- More bilateral tests after the April interim meeting
- Main interop event on the 18th of May, 2021
- Three implementations of v -06 tested against each other since the previous interop
  - Marco Tiloca (RISE), *Eclipse Californium*
  - Christian Amsüss, *aiocoap*
    - Building on the *py-edhoc* from Timothy Claeys (INRIA)
  - Lidia Pocero (ISI), *Contiki-NG*
    - Zoul device (CC2538 chipset), RPL over an IPv6 mesh network
- About 10 people attended throughout the test sessions
- Detailed cumulative notes and results at:
  - https://drive.google.com/drive/folders/1gYHR0DQt7--K3y4PWXWVJZ203pKl3_3k
  - Including report template and a spreadsheet with supported/tested features

Report

Marco / Christian

- **Selected ciphersuite: 0 (AES-CCM-16-64-128, SHA-256, X25519, EdDSA, AES-CCM-16-64-128, SHA-256)**
  - Authentication method: 0 (signature - signature); 3 (static DH - static DH)
  - Marco = initiator/responder; Christian = initiator/responder
- **Selected ciphersuite: 2 (AES-CCM-16-64-128, SHA-256, P-256, ES256, AES-CCM-16-64-128, SHA-256)**
  - Authentication method: 0; 1; 2; 3
  - Marco = initiator/responder; Christian = initiator/responder
- **Selected ciphersuite: 3 (AES-CCM-16-128-128, SHA-256, P-256, ES256, AES-CCM-16-64-128, SHA-256)**
  - Authentication method: 0; 1; 2; 3
  - Marco = initiator; Christian = initiator
- **Credential type ‘kid’**
- The tests were successful

Report

Christian / Lidia

- **Selected ciphersuite: 2 (AES-CCM-16-64-128, SHA-256, P-256, ES256, AES-CCM-16-64-128, SHA-256)**
  - Authentication method: 3 (static DH - static DH)
  - Christian = initiator ; Lidia = responder
- **Credential type ‘kid’**
- The test was successful

Next steps

- First align implementations to the upcoming v -08
- Then plan for a next interop

Thank you!