EDHOC interop 3

IETF 110, LAKE WG, March 9th, 2021

Report from Interop #3

- During the IETF 110 Hackathon – March 01-05, 2021

- Three implementations tested against each other
  - Marco Tiloca (RISE), *Eclipse Californium*
  - Lidia Pocero (ISI), *Contiki-NG*
  - Christian Amsüss, *aiocoap*
    - Building on the *py-edhoc* from Timothy Claeys (INRIA)

- Roughly 10 people attended throughout the week

- Detailed 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 ↔ Lidia
- Lidia setup
  - Zoul device (CC2538 chipset)
  - RPL over an IPv6 mesh network
- Tested configurations
  - Fixed **selected ciphersuite = 2** // ECDSA with P-256
    (AES-CCM-16-64-128, SHA-256, P-256, ES256, P-256, AES-CCM-16-64-128, SHA-256)
  - Fixed **authentication method = 3** // Static-static DH keys
  - Credential type: tested both **kid** and **x5t**
  - Ephemeral keys generated at runtime
- Both configurations worked, with (Marco=Initiator, Lidia=Responder) and vice versa

Report

- Marco ↔ Christian
- Tested configurations
  - Fixed **selected ciphersuite = 0** // EdDSA with Ed25519
    (AES-CCM-16-64-128, SHA-256, X25519, EdDSA, Ed25519, AES-CCM-16-64-128, SHA-256)
  - Fixed **authentication method = 0** // Signature from both sides
  - Credential type: **x5t**
    - Same identity keys and (non-real) certificates from Appendix B.1
  - Ephemeral keys generated at runtime
- The test worked, with (Marco=Initiator, Christian=Responder) and vice versa

Next steps

- More feedback for the next version of the draft

- Run more interop tests
  - Spontaneous pairwise testing in the coming weeks
  - Setting up a next interop meeting in April
    - One day in week 12-16, at 13:00 – 15:00 UTC
    - https://doodle.com/poll/k97hfiqvupr8b22q

Thank you!