Hackathon report

IETF 114, LAKE WG, July 27th, 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

```
EDHOC Message 2 (45 bytes):
58 2a 28 b5 40 93 b8 e3 c3 87
4b 4a 39 41 35 38 64 91 6a 41
3e 1a f8 b5 fe a0 48 74 b3 6a
80 2f 5e 48 a5 5f 0d b1 32 d1
c7 f6 95 13 01
```

```
OSCORE Master Secret (16 bytes):
cf 19 53 da d3 fd 25 e4 a0 c5
03 53 2e 3b d0 8b

OSCORE Master Salt (8 bytes):
3a 35 2c 9e ef 76 91 8f
```

- **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

[2] https://github.com/hacspec/hacspec

Thank you!