EDHOC interop 2

LAKE, Interim, January 2021

Report from Interop #2

- 22th of January 2021
- 3 implementations tested against each other:
  - Timothy Claeys INRIA,
  - Stefan Hristozov Fraunhofer AISEC,
  - Marco Tiloca RISE
- 13 attendees

- Detailed notes: https://hackmd.io/@fpalombini/EDHOC-Interop-2-220120

Report

- Based on test vector on appendix B.1 + self generated ephemeral keys:
  - signature authentication and X.509 certificates
  - method = 0
  - selected cipher suite = 0
    (AES-CCM-16-64-128, SHA-256, X25519, EdDSA, Ed25519, AES-CCM-16-64-128, SHA-256)

Init \ Resp	**Stefan**	**Marco**	**Timothy**
Stefan	–	Passed	Passed
Marco	Passed	–	Passed
Timothy	Passed	Passed	–

Report

- Started testing on test vector from appendix B.2
  - EDHOC Authenticated with Static Diffie-Hellman keys
  - method = 3
  - selected cipher suite = 0
    (AES-CCM-16-64-128, SHA-256, X25519, EdDSA, Ed25519, AES-CCM-16-64-128, SHA-256)

Init \ Resp	**Stefan**	**Marco**	**Timothy**
Stefan	–	Fail**	TODO
Marco	Fail	–	TODO
Timothy	TODO	TODO	–

Next Steps

- More good feedback to be incorporated in the draft
- Michel Veillette from Trilliant provided additional traces for method 0, cipher suite 5: https://drive.google.com/file/d/12ejAoMVrTDHfzDbQzSyffm_Y1zXe2E4y/view

- More interop planned to continue testing (Appendix B.2 + other methods/cipher suite)