EDHOC interop 4

LAKE WG virtual interim meeting, April 22nd, 2021

Report from Interop #4

- More bilateral tests in March after IETF 110
- Main interop event on the 14th of April, 2021
- Five implementations of v -05 tested against each other since IETF 110
  - Marco Tiloca (RISE), *Eclipse Californium*
  - Peter van der Stok, *C-based*
  - Stefan Hristozov (Fraunhofer), *C-based*
  - Timothy Claeys (INRIA), *C-based*
  - Christian Amsüss, *aiocoap*
    - Building on the *py-edhoc* from Timothy Claeys (INRIA)
- 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 ↔ Peter

- **Selected ciphersuite**
  - 2 (AES-CCM-16-64-128, SHA-256, P-256, ES256, P-256, AES-CCM-16-64-128, SHA-256)
  - 3 (AES-CCM-16-128-128, SHA-256, P-256, ES256, P-256, AES-CCM-16-64-128, SHA-256)
- **Authentication method**
  - 0 // Signature - Signature
  - 1 // Signature – Static DH
  - 2 // Static DH - Signature
  - 3 // Static DH – Static DH
- **Credential type x5chain**
  - x5chain, with real X509 certificates
- Ephemeral keys generated at runtime

1st time tested between 2 implementations

- Ciphersuite 3
- Methods 1 and 2
- Credential type “x5chain”
- Real x509 certificates

- The tests worked – Peter = Initiator and Marco = Responder

Report

Marco ↔ Stefan

- **Selected ciphersuite**
  - 0 (AES-CCM-16-64-128, SHA-256, X25519, EdDSA, Ed25519, AES-CCM-16-64-128, SHA-256)
- **Authentication method**
  - 0 // Signature - Signature
  - 3 // Static DH – Static DH
- **Credential type**
  - x5t
- Ephemeral keys generated at runtime

- The tests worked – Stefan = Initiator and Marco = Responder

Report

Timothy ↔ Christian

Marco ↔ Christian

- **Selected ciphersuite**
  - 0 (AES-CCM-16-64-128, SHA-256, X25519, EdDSA, Ed25519, AES-CCM-16-64-128, SHA-256)
- **Authentication method**
  - 3 // Static DH – Static DH
- **Credential type**
  - kid
- Ephemeral keys generated at runtime

- The tests worked
  - Timothy = Initiator and Christian = Responder, and vice versa
  - Marco = Initiator and Christian = Responder

Next steps

- More feedback for the next version of the draft

- Run more interop tests
  - More bilateral testing in the coming weeks
    - Especially Marco, Timothy and Christian
  - Planning a next interop meeting around mid-May

Thank you!