# Traces of EDHOC
## *draft-ietf-lake-traces-03*

Göran Selander, Ericsson
John P. Mattsson, Ericsson
Marek Serafin, ASSA ABLOY
**Marco Tiloca, RISE**

## … and overview of EDHOC testing

IETF 115 Meeting – London – November 8th, 2022

# Status of draft-ietf-lake-traces

- **Submitted version -03 before the cut-off**
  - Both traces are aligned with the latest EDHOC, i.e., version -17
  - Output based on the RISE Java implementation (*Eclipse Californium)* [1]

- **What has remained the same, in both traces**
  - CRED_I, CRED_R, ID_CRED_I, ID_CRED_R
  - Diffie-Hellman ephemeral keys
  - EDHOC Connection Identifiers and OSCORE Sender/Recipient IDs
  - EDHOC message_1 and the intermediate steps before it
  - Until and including TH_2 and G_XY, when preparing EDHOC message_2

- **Anything else did change in both traces, due to:**
  - PRK_2e = HMAC-SHA-256( salt, G_XY ), with **salt = TH_2**
  - TH_3 = H(TH_2, PLAINTEXT_2, **CRED_R**)
  - TH_4 = H(TH_3, PLAINTEXT_3, **CRED_I**)



[1] https://github.com/rikard-sics/californium/tree/edhoc-dev/cf-edhoc

# Status of draft-ietf-lake-traces

- **The second trace has been confirmed to be correct**
  - Cipher suite 2 (curve P-256) ; Method 3 (static-static)
  - CCS as authentication credentials ; ‘kid’ as credential identifiers
  - Validated by Mališa Vučinić with his Rust implementation [2][3]

- **Additional test vectors from Marek Serafin**
  - Also aligned with the latest EDHOC version -17
  - Cipher suite 2 (curve P-256); Method 0 (sign-sign) or 3 (static-static)
  - Test vectors available at [4]

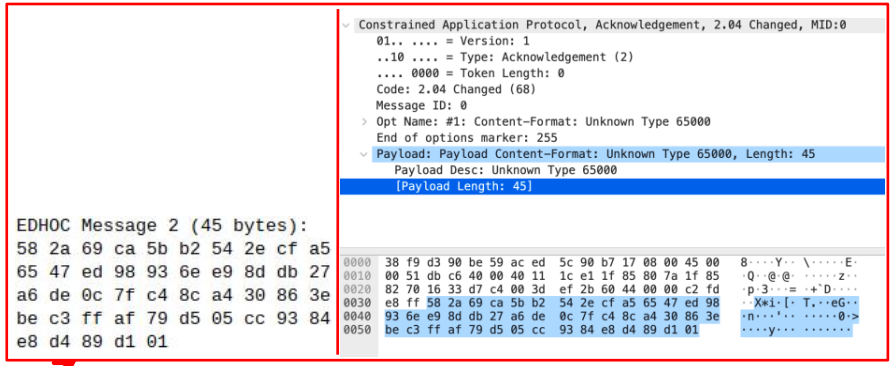
[2] Denis Merigoux, Franziskus Kiefer, Karthikeyan Bhargavan. *Hacspec: succinct, executable, verifiable specification for high-assurance cryptography embedded in Rust*, https://hal.inria.fr/hal-03176482/document

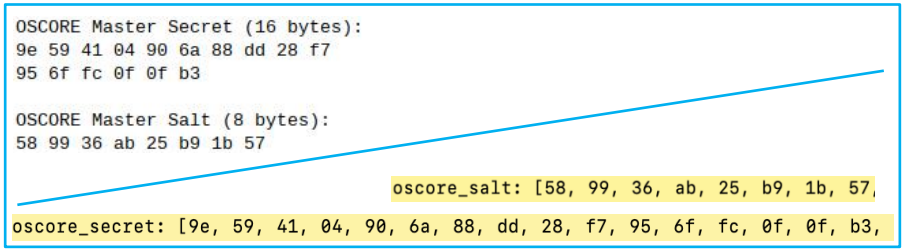
[3] https://github.com/hacspec/hacspec

[4] https://github.com/stoprocent/edhoc/tree/master/test-vectors-16

# Testing before/during IETF 115

- **Two implementations aligned with the latest version -17 of EDHOC**
  - Mališa Vučinić (INRIA): Rust/hacspec
  - 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



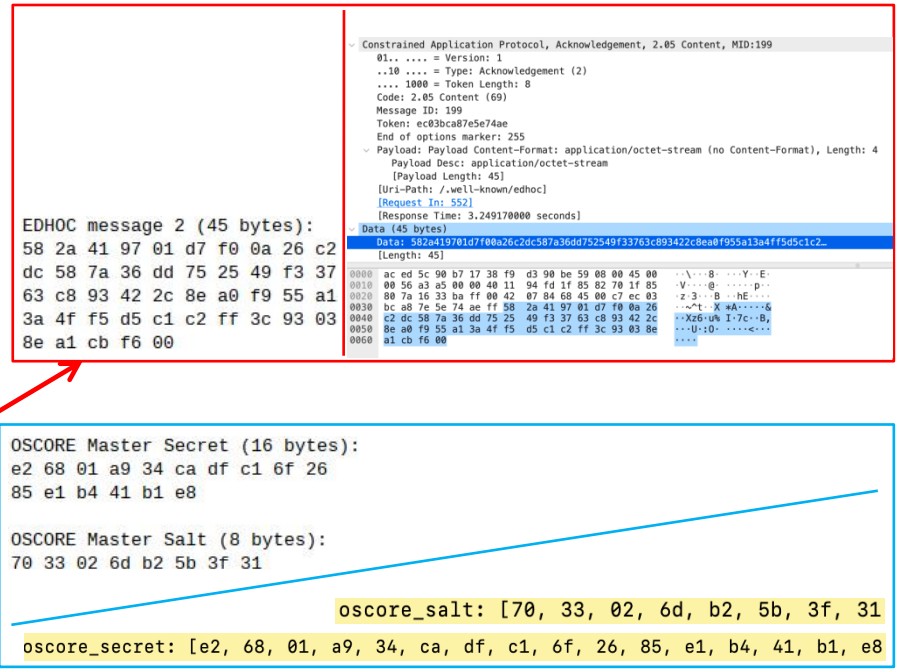

[2] Denis Merigoux, Franziskus Kiefer, Karthikeyan Bhargavan. *Hacspec: succinct, executable, verifiable specification for high-assurance cryptography embedded in Rust*, https://hal.inria.fr/hal-03176482/document

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

# Testing before/during IETF 115

- **Two implementations aligned with the latest version -17 of EDHOC**
  - Mališa Vučinić (INRIA): Rust/hacspec
  - Marco Tiloca (RISE): Java (*Eclipse Californium*)

- **Mališa: Responder (NEW); Marco: Initiator**
  - 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





[2] 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

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

# Next steps

- **More implementations are under ongoing updates**
  - Further tests will happen soon

- **On *draft-ietf-lake-traces***
  - Wait for the WGLC comments of *draft-ietf-lake-edhoc* to be processed
  - If anything changes for EDHOC on the wire, prepare a new draft-ietf-lake-traces-04
  - Otherwise and hopefully, draft-ietf-lake-traces-03 should be ready for WGLC

Thank you!