Traces of EDHOC
(Towards draft-ietf-lake-traces-06)

Göran Selander, Ericsson
John P. Mattsson, Ericsson
Marek Serafin, ASSA ABLOY
Marco Tiloca, RISE
Mališa Vučinić, Inria

IETF 117 Meeting – San Francisco – July 24th, 2023
Current status

› Publication requested
  – Received AD Review [1] – Thanks, Paul!

› Work is ongoing towards version -06

› Main required update
  – Implementations have to encrypt C_R in message_2, see draft-ietf-lake-edhoc-20
  – Updated values in the detailed traces (addressed in the Editor’s Copy)

› More required updates
  – Comments from Stephen (addressed in the Editor’s Copy)
  – Comments from the AD Review (addressed in the Editor’s Copy)

[1] https://mailarchive.ietf.org/arch/msg/lake/Jksn7IlQYQwbcCuzhPF6Hhh0H0Y/
Second trace

- Two implementations aligned with the EDHOC -20
  - Mališa Vučinić (INRIA): Rust/hacspec [2]
  - Marco Tiloca (RISE): Java (Eclipse Californium) [3]

- Same “final output” from [2] and [3]
  - Cipher suite 2 (curve P-256)
  - Method 3 (static-static)
  - CCS as authentication credentials
  - ‘kid’ as credential identifiers

- Trace detailed values successfully confirmed!

- The two implementations successfully interoped
  - Same configuration of the second trace (see above)

---

- PRK_out (32 bytes):
  0x6b2dae4032306571cfc2e4f94a255fb9f1f3fb29ca6f37
  9fec989d4fa90dca0

- OSCORE Master Secret (16 bytes):
  0x8c409a33223ad900e44f3434d2d2ce3

- OSCORE Master Salt (8 bytes):
  0x6163f44be862adfa

- PRK_out (after key update) (32 bytes):
  0x5e5efcaedda8d185bb7e261df191591c92049e70c
  23f6b434e36d6c1d1c

- OSCORE Master Secret (after key update) (16 bytes):
  0xc91b164c810b29a63fcb73e51bc455f3

- OSCORE Master Salt (after key update) (8 bytes):
  0x73ce792459403680

---

First trace

- One implementation aligned with EDHOC -20
  - Marco Tiloca (RISE): Java (Eclipse Californium) [3]

- “Final output” from [3] shown for the record
  - Cipher suite 0 (curve Ed25519)
  - Method 0 (sign-sign)
  - X.509 certificates as authentication credentials
  - x5t as credential identifiers

- Final output and trace detailed values to be confirmed by Marek
  - Any other implementor is welcome to confirm

Other pending updates to the draft

› WG Last Call comments from Stephen [4]
  – Addressed in the Editor’s Copy on Github [5]

› Comment #1 – Section 3.8.1
  – Missing field "notBefore" in the diagnostic notation of the Responder’s certificate for Trace 1
  – Fixed in the Editor’s Copy on Github [5]
  – No impact on the traces! The serialization of CRED_R did include “notBefore” already

› Comment #2 – Section 3.8
  – Certificates should include extensions, and especially "basic constraints"
  – Fixed in the Editor’s Copy on Github [6]
  – Added “basic constraints” and “key usage” extension, but only to the Common Root Certificate
  – That’s what RFC 5280 mandates. Instead, the end-entity certificates CRED_R and CRED_I are fine
  – Therefore, no impact on the traces!

Other pending updates to the draft

› AD Review from Paul [1]
  – Addressed in the Editor’s Copy, together with further editorial fixes [7]

› “I” for Initiator in plain sentences can be confusing – Spell the EDHOC roles out?
  – In plain sentences, replace “I” and “R” with “(the) Initiator” and “(the) Responder”

› Clarify the unit of key size (i.e., bytes)
  – 4 instances of "where the last value is the key length of EDHOC AEAD algorithm."
  – 2 instances of "where the last value is the key length of Application AEAD algorithm."

› Turn an external reference into a link
  – 2 instances of "see Appendix A.1 of [I-D.ietf-lake-edhoc]"

[1] https://mailarchive.ietf.org/arch/msg/lake/Jksn7IIQYQwbcCuzhPF6Hhh0H0Y/
[7] https://github.com/lake-wg/edhoc/commit/93292af679ea9552b86ce3ae5bde029c962ef0dd
Summary and next steps

› All the updates are in the Editor’s Copy

› Todo: confirm the first trace in detail, then submit version -06
Thank you!

https://github.com/lake-wg/edhoc