# Combining EDHOC and OSCORE

draft-ietf-core-oscore-edhoc-01

Francesca Palombini, Ericsson
Marco Tiloca, RISE
**Rikard Höglund**, RISE
Stefan Hristozov, Fraunhofer AISEC
Göran Selander, Ericsson

IETF 111, CoRE WG, July 28th, 2021

# Recap

- EDHOC is a lightweight authenticated key exchange developed in LAKE WG
  - Main use case: keying OSCORE for establishing a Security Context
  - Normal workflow: two round-trips

- This draft combines EDHOC (run over CoAP) with OSCORE
  - EDHOC message_3 combined with the first OSCORE-protected request
    - A single EDHOC + OSCORE request, transporting both
  - Achieve a minimum number of round trips required
    - To set up the OSCORE Security Context
    - To complete the first OSCORE transaction with that Context

- More details that are too detailed for EDHOC? (To be discussed)

# Plain way: EDHOC then OSCORE

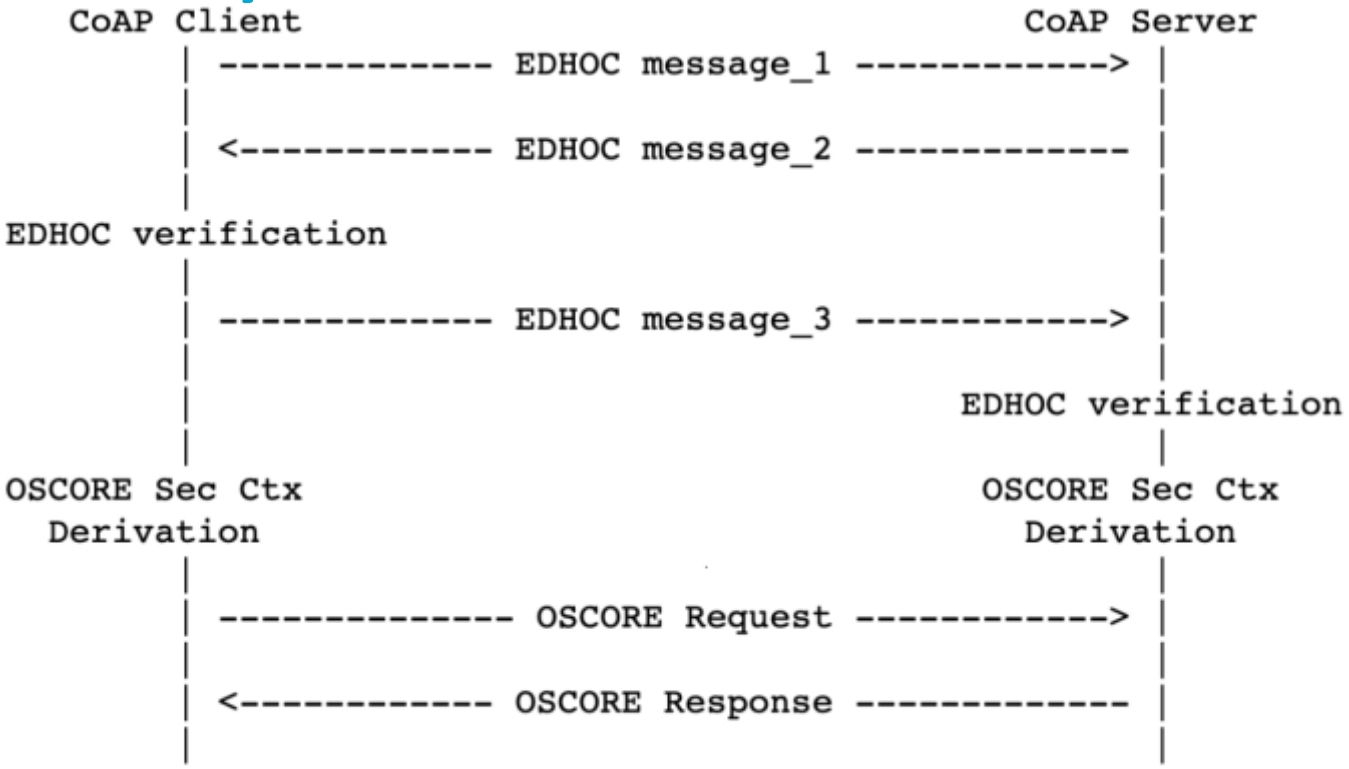



Figure 1: EDHOC and OSCORE run sequentially

# New way: EDHOC + OSCORE Request

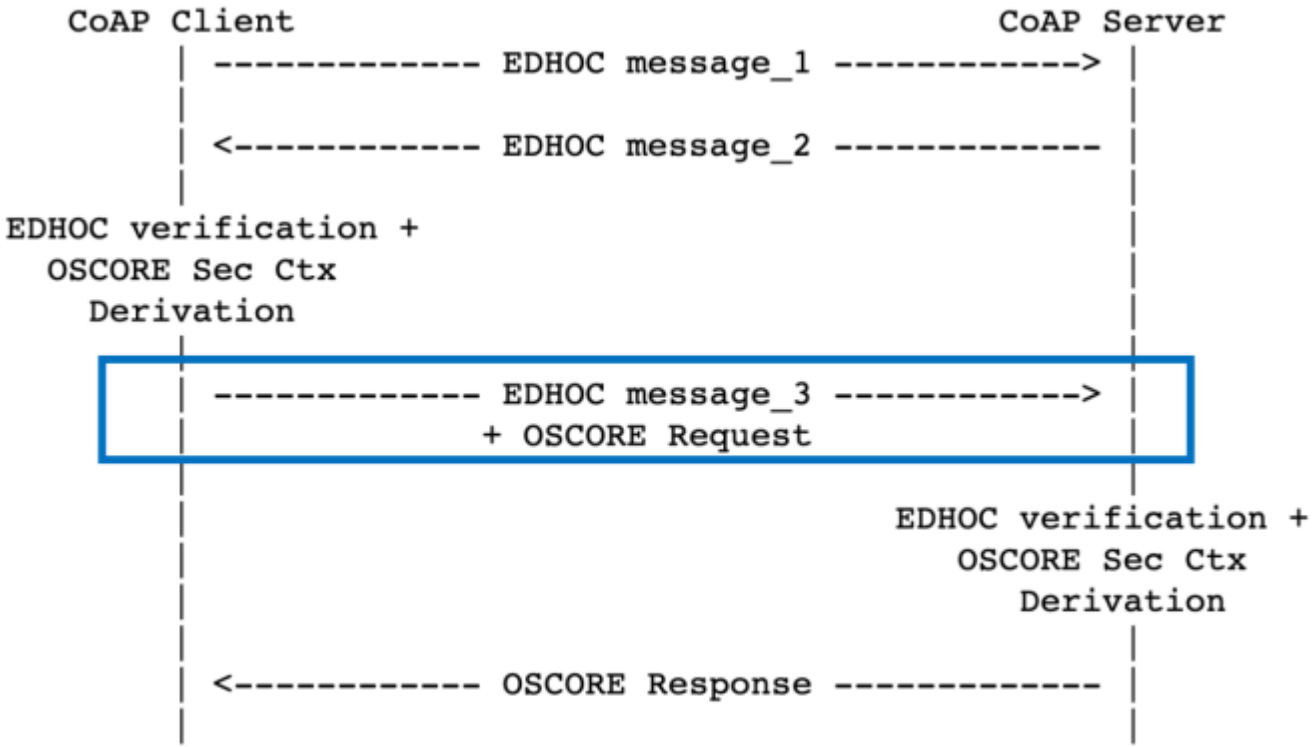
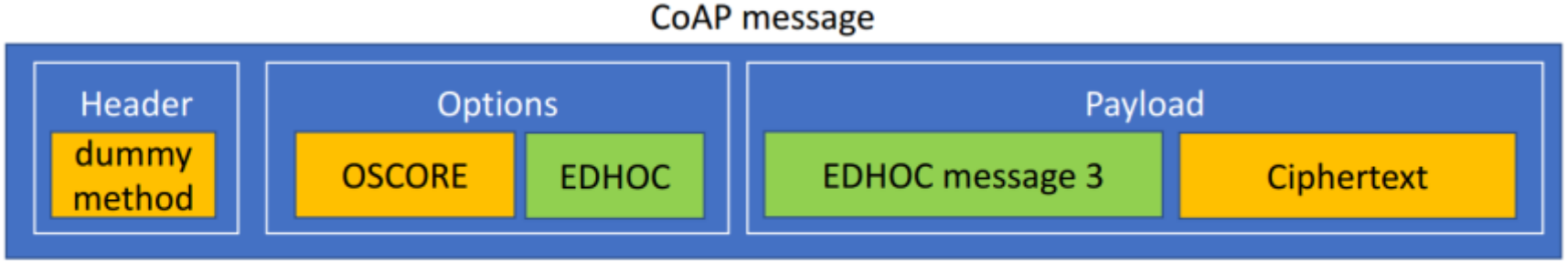
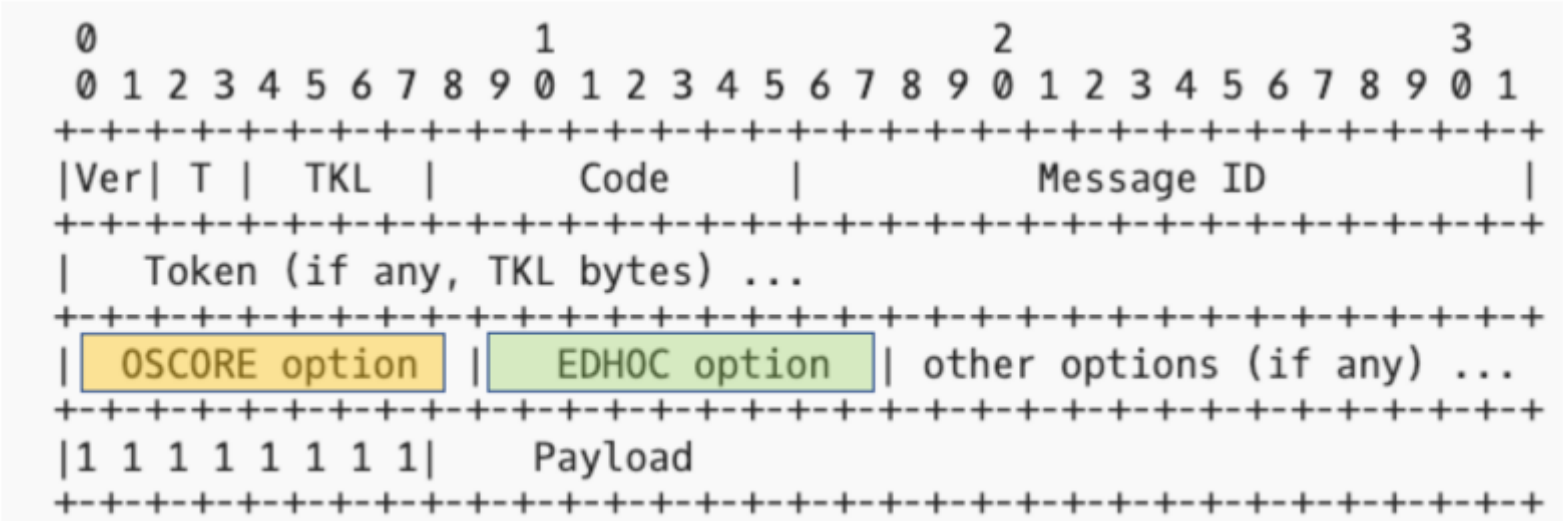



Figure 2: EDHOC and OSCORE combined

# EDHOC + OSCORE request



# Updates from IETF 110

- Settled on EDHOC Option number 21
  - Instead of 13 in the previous version
  - Better since 21 works just as well, and other use cases may need 13 more
  - Request for early IANA allocation in the CoAP Option Numbers registry
- Extended and improved background about EDHOC
  - Based on feedback from the IETF 110 meeting
- Align with updates to EDHOC draft
  - Especially encoding of connection identifiers (can now be both CBOR bstr/int)
- Improvements and updating examples

# Updates from IETF 110

- As triggered by the EDHOC changes on connection identifiers

- Defined a conversion method from EDHOC IDs to OSCORE Sender/Recipient IDs
  - Initially defined here, from Christian's proposal
  - After discussions, this was moved to the EDHOC document in LAKE

- Defined a conversion method from OSCORE Sender/Recipient IDs to EDHOC IDs
  - Note: there are 2 "equivalent" EDHOC IDs for each OSCORE ID, i.e., CBOR *int* or *bstr*
  - This method deterministically picks either the *int* or the *bstr* EDHOC identifier
    - Required for the EDHOC+OSCORE request, as including an OSCORE Sender ID
    - Performance advantage: the selected identifier is the smallest of the two
  - Now in Appendix A. Move to the document body?

# Open point

- Previous attempts were made to have CoRE-specific content here
  - Derivation of OSCORE Security Context: EDHOC ==> Here ==> EDHOC
  - Conversion from EDHOC ID to OSCORE ID: Here ==> EDHOC

- Consider scope expansion: "Profiling the Use of EDHOC for CoAP and OSCORE"
  - Already have content about conversion from OSCORE ID to EDHOC ID (previous slide)
  - Use of a potential URI compression option (Christian's separate proposal)
  - Web linking
    - *rt=edhoc* might be already registered in the EDHOC draft
    - More target attributes aligned with the applicability statement can be added here
  - Any further things judged to be too detailed for the EDHOC draft

Opinions? More input?

# Next Steps

- Request for early IANA allocation: Option number 21 for the "EDHOC" CoAP option
- Planned updates to the draft
  - Make text/figures consistent with the use of content-format in the EDHOC draft
  - Notes on the EDHOC applicability statement
    - Support for EDHOC+OSCORE request and ID conversion method
- Update the implementation
  - We have running code, only based on EDHOC v –07
  - First need to update the EDHOC implementation to its v –08 (ongoing :-)
- Need for reviews

# Thank you!

# Comments/questions?

https://github.com/core-wg/oscore-edhoc/