Using EDHOC with CoAP and OSCORE

draft-ietf-core-oscore-edhoc-07

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

IETF 116 meeting – Yokohama – March 28th, 2023

Since IETF 115

- **Completed Working Group Last Call**

- **Received reviews from Christian Amsüss and John P. Mattsson – Thanks a lot!**
  - https://mailarchive.ietf.org/arch/msg/core/Rs9EMsszA-QzRue7QJDIZN280WU/
  - https://mailarchive.ietf.org/arch/msg/core/n6Kmomt6znH8y52C1-v3ufz7yPI/
  - https://mailarchive.ietf.org/arch/msg/core/8Cxad5Byb1qK07B00qQksPEJeiI/

- **Selected comments were discussed at the 2023-03-01 CoRE interim meeting**
  - https://datatracker.ietf.org/doc/minutes-interim-2023-core-04-202303011500/

- **Version -07 submitted before the cut-off**
  - All the comments should have been addressed

Update summary

- **Changed document title**
  - "Using EDHOC with CoAP and OSCORE"

- **Main change – Payload format in the EDHOC + OSCORE request**
  - Not a CBOR sequence anymore
  - EDHOC message_3 is still a CBOR data item (byte string), followed by ...
  - … the OSCORE ciphertext not wrapped in a CBOR byte string

- **More on message processing**
  - Precisely, the client first creates EDHOC message_3, then derives the OSCORE Sec Ctx
  - After EDHOC message_3, EDHOC error messages are explicitly not protected with OSCORE
  - Error handling on the server for the EDHOC option is now more general and future-proof

Update summary

- **Web Linking – Lot of comments on this part!**
  - All target attributes prefixed by “ed-”
  - All target attributes registered in the “Target Attributes” IANA Registry
  - New target attributes “ed-i” and “ed-r” (EDHOC roles and flows supported by the server)
  - Reverted Web Linking example to use /.well-known/edhoc
  - Defined new “EDHOC Authentication Credential Types” IANA Registry
    - Source of values for the target attribute “ed-cred-t”
  - Single target attribute “ed-ead” (server support of a specific EAD item), with simpler semantics

- **Left out to consider for the EDHOC specification or follow-up works**
  - Definition of a new IANA Registry for EDHOC application profiles
    - Source of values for a possible, new target attribute “ed-prof”
  - Definition of a well-known EDHOC application profile

Update summary

- **More security considerations**
  - The optimized workflow yields a minimum of 128-bit security against online attacks
- **Removed the Appendix on performance considerations with Block-wise**
  - Just added a short sentence when defining the client processing (Section 3.2.1)
- **Clarifications**
  - Use of "forward message flow" and "reverse message flow"
  - Clearer and more precise use of CoAP and CBOR terminology
  - Much simpler description of the selection of EDHOC/OSCORE Identifiers
  - Revised and improved examples
  - Various editorial improvements

Summary and next steps

- **Version -07 addresses all the WG Last Call comments**
- **No further issues are known**
- **Ready for Shepherd review and write-up**

Thank you!

Comments/questions?

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

EDHOC + OSCORE request