Implementation Considerations for Ephemeral Diffie-Hellman Over COSE (EDHOC)

draft-ietf-lake-edhoc-impl-cons-04

Marco Tiloca, RISE

IETF 123 Meeting – Madrid – July 22nd, 2025

Recap

- **Scope: considerations on side-topics related to the implementation of EDHOC [1]**
  - Those topics are out of scope for EDHOC itself

- **Topics that are currently covered**
  - Handling of EDHOC sessions and derived applications keys, if become invalid
  - Trust policies for learning peers' authentication credentials on-the-fly
  - Branched, side-processing of incoming EDHOC messages. This includes:
    - Fetching and validation of authentication credentials
    - Processing of EAD items, which may play a role in validating authentication credentials
  - Guidelines/advice on using EDHOC over CoAP with Block-wise transfers

- **Explored cases in point, in addition to plain EDHOC**
  - EDHOC and OSCORE profile of ACE --- *draft-ietf-ace-edhoc-oscore-profile*
  - Lightweight authorization using EDHOC (ELA) --- *draft-ietf-lake-authz*

[1] https://www.rfc-editor.org/rfc/rfc9528.html

Updates since version -03

- **Editorial improvements**

- **Generalized phrasing around "authentication credentials"**
  - OLD: "authentication credentials *of* the other peer"
  - NEW: "authentication credentials *associated with* the other peer"
  - Consistent with both RFC 9528 and *draft-ietf-lake-edhoc-psk*

- **NO-LEARNING trust policy for learning authentication credentials**
  - Generalized, clarified, and re-positioned exceptions
  - Section 3.2 – Exceptions typically based on a trusted third party vouching for the new credential
    - Vouching information provided through an EAD item, or out-of-band
    - The credential still needs to be validated by the learning peer
  - Two cases in point as illustrative example:
    - Section 3.3.1 – EDHOC and OSCORE profile of ACE --- *draft-ietf-ace-edhoc-oscore-profile*
    - Section 3.3.2 –Lightweight authorization using EDHOC (ELA) --- *draft-ietf-lake-authz*

Updates since version -03

- **Section 4.1 – Added short note on processing of incoming EDHOC message_1**
  - In the future, CRED_I might be somehow transported in an EAD item of EAD_1
  - ead_value will have to wrap CRED_I in a cryptographically protected "envelope"
  - Example: a variant of the EDHOC and OSCORE profile of ACE that supports EDHOC PSK
  - The processing of message_1 would become closer to that of message_2 and message_3

- **New Appendix A – "Foreseen Advanced Processing of Incoming EDHOC message_1"**
  - Step-based, generalized processing of a message_1 transporting CRED_I in EAD_1
  - A diagram shows the side processing at the side-processor object
  - Presentation style analogous to that in Section 4.3 for message_2 and message_3

Updates since version -03

- **Section 6 – "Security Considerations"**
  - Inherited considerations from RFC 9528 and RFC 9668 (EDHOC + OSCORE request)
  - Inherited implementation compliance requirements from RFC 9528

- **As they come, inherit considerations and compliance requirements from future:**
  - EDHOC extensions (e.g., new cipher suites, methods, types of authentication credentials, ...)
  - External security applications integrated through EDHOC EAD items

- **Section 6.1 – "Assessing the Correctness of Implementations"**
  - Mentioned tools relying on fuzz testing, e.g., EDHOC-Fuzzer [2]
  - Assist in finding implementation errors, e.g.:
    - Non-conformance with the protocol specification
    - Inappropriate states and state transitions
  - Help fix errors and reduce the memory footprint and code complexity
  - Help reduce the risks of bugs and related security vulnerabilities

[2] https://dl.acm.org/doi/10.1145/3597926.3604922

Next steps

- **This version -04 includes all that the author could think and write about :-)**

- **<u>Anything to add from other EDHOC implementors</u>? This can also include:**
  - More details about *draft-ietf-lake-authz* ? ➔ Extend Section 3.3.2 and/or Section 4
  - Considerations related to *draft-ietf-lake-ra* ? ➔ New Section 3.3.3 and/or extend Section 4
  - Considerations related to *draft-ietf-lake-edhoc-psk* ? ➔ Extend Section 4 (hardly needed)

- **If nothing else comes up to be added, this should be ready for WG Last Call**

Thank you!

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