

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

draft-ietf-lake-edhoc-impl-cons-06

Marco Tiloca, RISE

IETF 125 Meeting – Shenzhen – March 16th, 2026

Recap

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

Updates since version -04

- › **Editorial fixes and improvements**
- › **Most updates are related to ELA (*draft-ietf-lake-authz*) and to its recent changes**
- › **Generalized trust assessment of authentication credentials**
 - In some cases, a valid credential learnt on-the-fly might be only provisionally trusted
 - A confirmation is expected later during the EDHOC session, e.g., a Voucher in ELA
 - If that expected confirmation comes, the credential is kept and marked as ultimately trusted
 - Otherwise, the credential is discarded and the EDHOC session is aborted
 - See updates in:
 - › Section 3 – Concept in general
 - › Section 3.3.2 – ELA and its Voucher as a case in point
 - › Section 4.3.1.1 – Pre-verifications side message processing (also reflected in Figure 5)

Updates since version -04

- › **Focused alignment with the latest ELA procedure**
 - Mostly in the related Section 3.3.2
- › **Positioning of the Voucher in the protocol workflow**
 - EDHOC forward message flow
 - › CRED_V is CRED_R in EDHOC message_2
 - › The Voucher is in EDHOC message_4 **NEW**
 - EDHOC reverse message flow
 - › CRED_V is CRED_I in EDHOC message_3
 - › The Voucher is in EDHOC message_3
- › **If U's trust policy is NO_LEARNING, what's the overriding exception to consider CRED_V?**
 - EDHOC forward message flow → U wants to run ELA, including Voucher_Info in message_3
 - EDHOC reverse message flow → U retrieves an expected, valid Voucher from message_3

Updates since version -04

- › **Closed Github issue #1 raised by Christian – Thanks!**

- ELA procedure as a case in point

- › v -06: If W does not produce the Voucher → V includes the EAD item without ead_value

- › **v -07: If W does not produce the Voucher → V does not include the EAD item**

- A recipient EDHOC peer has to be able to detect the absence of an (expected) EAD item



- › **Additions in Section 4 “Side Processing of Incoming EDHOC Messages”**

- The application instructs the side-processor object (SPO) also about expected EAD items

- › E.g., due to planned external security applications like the ELA procedure

- Throughout an EDHOC session, the SPO keeps the list of such EAD items up-to-date

- › E.g., based on planned/unplanned security applications occurring in the EDHOC session

- If an incoming message does not include an EAD item that was strictly expected ...

- › The SPO can determine whether to continue or abort the EDHOC session

Updates since version -04

› Added new Section 6 “Operational Considerations”

- Increasingly expected, see <https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-rfc5706bis>
- Nothing special to say in this document → Appropriate boilerplate + explanation

There are no new operations or manageability requirements introduced by this document.

Explanation: this document provides considerations for implementers of the EDHOC protocol, without updating the protocol or introducing extensions thereof.

Next steps

- › **This version -06 includes all that the author could think and write about :-)**
- › **Recently addressed:**
 - Alignment to *draft-ietf-lake-authz*, as to which EDHOC message includes the Voucher
 - Generalization on (provisionally) trusted authentication credentials learnt on-the-fly
 - Ability to detect the absence of (expected) EAD items in incoming EDHOC messages
- › **This version should be ready for WG Last Call**

Thank you!

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