LAKE Working Group
Internet-Draft
Intended status: Standards Track
Expires: 8 January 2026

M. Tiloca
R. Höglund
RISE AB
E. Lopez-Perez
Inria

7 July 2025

In-band Agreement of Output Lengths for the EDHOC_Exporter Interface of Ephemeral Diffie-Hellman Over COSE (EDHOC)
draft-tiloca-lake-exporter-output-length-00

Abstract

The lightweight authenticated key exchange protocol Ephemeral Diffie-Hellman Over COSE (EDHOC) allows two peers to compute a shared secret session key. Once the session key is available, the two peers can use the EDHOC_Exporter interface, e.g., to derive keying material for an application protocol. This document defines an in-band approach that can be used by the two peers to agree about the lengths of the outputs produced with the EDHOC_Exporter interface. The defined approach relies on an EDHOC External Authorization Data (EAD) item that can be exchanged in the first two EDHOC messages of an EDHOC session.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the Lightweight Authenticated Key Exchange Working Group mailing list (lake@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/lake/.

Source for this draft and an issue tracker can be found at https://gitlab.com/crimson84/draft-tiloca-lake-exporter-output-length.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Terminology 3
2. EAD Item "EDHOC_Exporter Output Lengths" 4
3. Processing at the Recipient Side 6
4. Security Considerations 7
5. IANA Considerations 7
5.1. EDHOC External Authorization Data Registry 8
6. References 8
6.1. Normative References 8
6.2. Informative References 9
Acknowledgments 9
Authors' Addresses 9

1. Introduction

Ephemeral Diffie-Hellman Over COSE (EDHOC) [RFC9528] is a lightweight authenticated key exchange protocol, especially intended for use in constrained scenarios.

Two peers participate in the EDHOC protocol, i.e., a peer acts as EDHOC Initiator and starts an EDHOC session with another peer acting as EDHOC Responder. The main output of a successfully completed EDHOC session is the shared secret session key PRK_out (see Section 4.1.3 of [RFC9528]).

After having established PRK_out, the two peers can use the EDHOC_Exporter interface defined in Section 4.2.1 of [RFC9528], e.g., to derive keying material for an application protocol. Among its inputs, the EDHOC_Exporter interface includes "exporter_label" as a registered numeric identifier of the intended output and "length" as the length in bytes of the intended output.

At the time of writing, notable uses of the EDHOC_Exporter interface include the derivation of:

* The Master Secret and Master Salt to use for establishing a Security Context for the security protocol Object Security for Constrained RESTful Environments (OSCORE) [RFC8613]. These derivations are specified in Appendix A.1 of [RFC9528].

* A symmetric Pre-Shared Key rPSK to use for session resumption in EDHOC and the corresponding credential identifier rID_CRED_PSK [I-D.ietf-lake-edhoc-psk]. These derivations are specified in Section 6 of [I-D.ietf-lake-edhoc-psk].

When using the EDHOC_Exporter interface, it is crucial that the two peers agree about the length in bytes of each intended output, in order to ensure the correctness of their operations. To this end, the two peers can rely on pre-defined default lengths, or agree out-of-band on alternative lengths. However, the two peers might need or prefer to explicitly agree about specific output lengths to use on a per-session basis.

This document defines an in-band approach that the two peers can use to agree about the lengths of the outputs produced with the EDHOC_Exporter interface. The defined approach relies on an EDHOC External Authorization Data (EAD) item (see Section 3.8 of [RFC9528]), which the two peers can exchange in the first two EDHOC messages of an EDHOC session.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Readers are expected to be familiar with the terms and concepts related to EDHOC [RFC9528], Concise Data Definition Language (CDDL) [RFC8610], and Concise Binary Object Representation (CBOR) [RFC8949].

Examples throughout this document are expressed in CBOR diagnostic notation as defined in Section 8 of [RFC8949] and Appendix G of [RFC8610]. Diagnostic notation comments are often used to provide a textual representation of the numeric parameter names and values.

2. EAD Item "EDHOC_Exporter Output Lengths"

This section defines the EDHOC EAD item "EDHOC_Exporter Output Lengths", which is registered in Section 5.1 of this document.

The EAD item MAY be included:

* In the EAD_1 field of EDHOC message_1, in order to specify the output lengths that the Initiator wishes to use with the EDHOC_Exporter interface in the present EDHOC session.

* In the EAD_2 field of EDHOC message_2, in order to specify the output lengths that the Responder wishes to use with the EDHOC_Exporter interface in the present EDHOC session.

Within an EAD_1 field or EAD_2 field, the EAD item MUST NOT occur more than once. The EAD item MUST NOT be included in the EAD fields of EDHOC message_3 or message_4.

When the EAD item is present, its ead_label TBD_EAD_LABEL MUST be used only with negative sign, i.e., the use of the EAD item is always critical (see Section 3.8 of [RFC9528]).

The EAD item MUST specify an ead_value, as a CBOR byte string with value the binary representation of a CBOR sequence [RFC8742], namely EXP_LEN_SEQ. As specified below, the CBOR sequence is composed of pairs of items, with the order of pairs having no meaning.

Each pair (X, Y) of the CBOR sequence MUST be as follows.

* The first element X is a CBOR unsigned integer, specifying the value to use as first argument "exporter_label" when invoking the EDHOC_Exporter interface (see Section 4.2.1 of [RFC9528]).

  The unsigned integer value is taken from the ’Label’ column of the "EDHOC Exporter Labels" registry within the "Ephemeral Diffie-Hellman Over COSE (EDHOC)" registry group [EDHOC.Exporter.Labels].

* The second element Y is a CBOR unsigned integer, specifying the value to use as third argument "length" when invoking the EDHOC_Exporter interface using the value specified by X as first argument "exporter_label" (see Section 4.2.1 of [RFC9528]).

The value specified by Y MUST be a valid value to use as "length" when using the value specified by X as "exporter_label". For example, when X specifies 0 as the "exporter_label" to derive an OSCORE Master Secret [RFC8613], Y is required to be not less than the "length" default value defined in Appendix A.1 of [RFC9528], i.e., the key length (in bytes) of the application AEAD Algorithm of the selected cipher suite for the EDHOC session.

In the EAD item, ead_value MUST NOT specify multiple pairs that encode the same unsigned integer value in their first element X.

The CDDL grammar [RFC8610] describing the ead_value for the EAD item "EDHOC_Exporter Output Lengths" is provided in Figure 1.

```
ead_value = << EXP_LEN_SEQ >>

; This defines an array, the elements of which
; are to be used in the CBOR Sequence EXP_LEN_SEQ:
EXP_LEN_SEQ = [* pair]

pair = (
  exporter_label: uint,
  length: uint
)
```

Figure 1: CDDL Definition of ead_value for the EAD Item "EDHOC_Exporter Output Lengths"

An example of ead_value in CBOR diagnostic notation is provided in Figure 2. In the example, ead_value indicates the wish to use the EDHOC_Exporter interface to derive an OSCORE Master Secret and an OSCORE Master Salt [RFC8613] as per Appendix A.1 of [RFC9528], such that:

* the OSCORE Master Secret (exporter_label: 0) has a length of 32 bytes; and

* the OSCORE Master Salt (exporter_label: 1) has a length of 16 bytes.

```
<< 0, 32, 1, 16 >>
```

Figure 2: Example of ead_value for the EAD Item "EDHOC_Exporter Output Lengths" in CBOR Diagnostic Notation

That is, assuming the second argument "context" of the EDHOC_Exporter interface to be the empty CBOR byte string (i.e., h'' in CBOR diagnostic notation), the example above is consistent with performing the following two invocations of the EDHOC_Exporter interface:

```
EDHOC_Exporter(0, h'', 32)
EDHOC_Exporter(1, h'', 16)
```

3. Processing at the Recipient Side

In case the recipient peer supports the EAD item, the recipient peer MUST silently ignore the EAD item "EDHOC_Exporter Output Lengths" if this is specified in the EAD_3 field of EDHOC message_3 or in the EAD_4 field of EDHOC message_4.

Upon receiving an EDHOC message_1 or EDHOC message_2 whose EAD field includes the EAD item "EDHOC_Exporter Output Lengths", the recipient peer MUST abort the EDHOC session and MUST reply with an EDHOC error message with error code (ERR_CODE) 1, if any of the following occurs:

* the EAD field includes multiple occurrences of the EAD item "EDHOC_Exporter Output Lengths";

* ead_value is malformed or does not conform with what is defined in Section 2;

* the recipient peer does not recognize the value encoded by the first element X of a pair (X, Y) as a valid "exporter_label" to be used when invoking the EDHOC_Exporter interface;

* in a pair (X, Y), the value encoded by the second element Y is not valid to be used as "length" when invoking the EDHOC_Exporter interface using the value encoded by the first element X as "exporter_label"; or

* for a pair (X, Y), the recipient peer is not going to be able to invoke the EDHOC_Exporter interface using the values encoded by X and Y as the first argument "exporter_label" and the third argument "length", respectively.

If the Responder has received an EDHOC message_1 including the EAD item "EDHOC_Exporter Output Lengths" and the Responder includes the EAD item "EDHOC_Exporter Output Lengths" in EDHOC message_2, then the following applies. Within ead_value of the EAD item included in EDHOC message_2, the Responder MUST NOT specify any pair (X, Y) such that the unsigned integer value encoded by X was encoded by the first element of a pair of the EAD item included in the received EDHOC message_1.

If the Initiator receives an EDHOC message_2 including the EAD item "EDHOC_Exporter Output Lengths" after having sent an EDHOC message_1 including the EAD item "EDHOC_Exporter Output Lengths", then the following applies. The Initiator MUST abort the EDHOC session and MUST reply with an EDHOC error message with error code (ERR_CODE) 1, if ead_value of the EAD item included in EDHOC message_2 specifies any pair (X, Y) such that the unsigned integer value encoded by X was encoded by the first element of a pair of the EAD item included in the sent EDHOC message_1.

In an EDHOC session during which the EAD item "EDHOC_Exporter Output Lengths" has been included in EDHOC message_1 and/or message_2, the following applies.

* The Initiator (Responder) considers the successful verification of EDHOC message_2 (message_3) as a confirmed agreement with the other peer about how to invoke the EDHOC_Exporter interface, once the session key PRK_out for the present EDHOC session is available.

  That is, for each pair (X, Y) specified by the exchanged EAD items, the two peers MUST use the unsigned integer values encoded by X and Y as the first argument "exporter_label" and the third argument "length", respectively.

* If a particular "exporter_label" value is not specified by the exchanged EAD items, then a possible invocation of the EDHOC_Exporter interface using that value as its first argument takes as value for its third argument "length" a pre-defined default value, or an alternative value agreed out-of-band.

4. Security Considerations

The same security considerations for EDHOC from [RFC9528] hold for this document. Furthermore, the following considerations apply.

TBD

5. IANA Considerations

This document has the following actions for IANA.

Note to RFC Editor: Please replace all occurrences of "[RFC-XXXX]" with the RFC number of this specification and delete this paragraph.

5.1. EDHOC External Authorization Data Registry

IANA is asked to register the following entry in the "EDHOC External Authorization Data" registry within the "Ephemeral Diffie-Hellman Over COSE (EDHOC)" registry group defined in [RFC9528].

* Name: EDHOC_Exporter Output Lengths
* Label: TBD_EAD_LABEL (range 0-23)
* Description: Set of output lengths to use with the EDHOC_Exporter interface
* Reference: [RFC-XXXX]

6. References

6.1. Normative References

[EDHOC.Exporter.Labels] IANA, "EDHOC Exporter Labels", <https://www.iana.org/assignments/edhoc/edhoc.xhtml#edhoc-exporter-labels>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/rfc/rfc8610>.

[RFC8742] Bormann, C., "Concise Binary Object Representation (CBOR) Sequences", RFC 8742, DOI 10.17487/RFC8742, February 2020, <https://www.rfc-editor.org/rfc/rfc8742>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

[RFC9528] Selander, G., Preu Mattsson, J., and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)", RFC 9528, DOI 10.17487/RFC9528, March 2024, <https://www.rfc-editor.org/rfc/rfc9528>.

6.2. Informative References

[I-D.ietf-lake-edhoc-psk] Lopez-Perez, Selander, G., Mattsson, J. P., and R. Marin-Lopez, "EDHOC Authenticated with Pre-Shared Keys (PSK)", Work in Progress, Internet-Draft, draft-ietf-lake-edhoc-psk-04, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lake-edhoc-psk-04>.

[RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, DOI 10.17487/RFC8613, July 2019, <https://www.rfc-editor.org/rfc/rfc8613>.

Acknowledgments

The authors sincerely thank Gran Selander for his comments and feedback.

This work was supported by the Sweden’s Innovation Agency VINNOVA within the EUREKA CELTIC-NEXT project CYPRESS.

Authors’ Addresses

Marco Tiloca
RISE AB
Isafjordsgatan 22
SE-164 40 Kista
Sweden
Email: marco.tiloca@ri.se

Rikard Hglund
RISE AB
Isafjordsgatan 22
SE-164 40 Kista
Sweden
Email: rikard.hoglund@ri.se

Elsa Lopez-Perez
Inria

Email: elsa.lopez-perez@inria.fr