LAKE Working Group
Internet-Draft
Intended status: Standards Track
Expires: 21 October 2026

G. Selander
J. Preu Mattsson
Ericsson
M. Vuini
Inria

19 April 2026

# Hashing Authentication Credentials in EDHOC
## draft-selander-lake-cred-hash-01

## Abstract

This document defines a COSE header parameter which signals that an authentication credential is replaced by the hash of the authentication credential in the protocol message computations. This further relaxes the need for transporting authentication credentials in EDHOC, which reduces protocol message sizes and improves performance in constrained networks.

## 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/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 21 October 2026.

## Copyright Notice

Table of Contents



## 1. Introduction

The lightweight authenticated key exchange protocol Ephemeral Diffie-Hellman over COSE (EDHOC, [RFC9528]) supports a variety of authentication credentials and different options for identifying credentials during the protocol execution. The latter allows the protocol messages to carry, for example, references or unique identifiers instead of the authentication credentials, thereby reducing message size and improving performance in constrained networks.

In this document we describe a new mode of processing authentication credentials in EDHOC which further relaxes the need for transporting them. This new mode is signalled with a new COSE header parameter using an existing protocol mechanism and does not require any changes to the message format.

### 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 EDHOC [RFC9528].

## 2. Background

### 2.1. Authentication Credentials in EDHOC

Public key authentication credentials in EDHOC are described in Section 3.5 of [RFC9528]. (Pre-shared keys are out of scope.)

The authentication credentials for the Initiator (I) and the Responder (R) are denoted CRED_I and CRED_R, respectively. To allow more flexibility in identifying and obtaining the credential, the EDHOC protocol does not have dedicated message fields for CRED_I and CRED_R. Instead the fields ID_CRED_I and ID_CRED_R are intended to facilitate the retrieval of the authentication credentials and the authentication keys. ID_CRED_I and ID_CRED_R are of type COSE header_map and contain one or more COSE header parameters, see corresponding IANA register. Some examples below for the case when the authentication credential (here CRED_R, similar applies to CRED_I) is an X.509 certificate:

1. CRED_R may be referenced by including the COSE header parameter x5u in the ID_CRED_R field of EDHOC message 2. x5u contains a URI to the Responder’s certificate, for example, at some certificate repository.

2. If the certificate is already available to the Initiator, then it can be identified using the COSE header parameter x5t in ID_CRED_R. x5t contains the certificate hash.

3. ID_CRED_R can contain both x5u and x5t, allowing retrival and/or verification of the X.509 certificate.

(Note that in case the certificate do need to be transported it can be included with the COSE header parameter x5chain in ID_CRED_R or ID_CRED_I.)

### 2.2. Lightweight Certificate Enrolment with EST-OSCORE

EST-OSCORE [I-D.ietf-ace-coap-est-oscore] specifies a lightweight certificate enrolment protocol protecting EST payloads over CoAP with OSCORE [RFC8613].

In the same spirit as in Section 2.1, the EST-OSCORE enrolment request from the EST client may result in a response from the Certification Authority (CA) containing a reference to and/or hash of the issued certificate, rather than the certificate itself. In this case the certificate is not available to the client (= the subject of the certificate) but of course the public/private key pair is. Hence, the client should be able to authenticate using EDHOC to a peer by providing a reference and/or hash of the certificate as described Section 2.1. This could be favorable if the client is on a constrained network and the peer and CA is on a non-constrained network, since the certificate is only transported over the non-constrained network compared to twice over the constrained network.

However, this doesn’t work directly with the current message processing in [RFC9528] as we explain in Section 3, followed by a straightforward fix that makes it work in Section 4.

## 3. Authentication Credentials in EDHOC Message Processing

When the EDHOC protocol was designed it was assumed that each endpoint has access to its own credential, and that it obtained the other endpoint’s credential at least the first time it was used. Hence it was feasible to include the authentication credentials in the protocol message computations:

* CRED_R is used in the computation of the message field Signature_or_MAC_2 (see Section 5.3.2 of [RFC9528]):
  - MAC_2 is computed with context_2 = << C_R, ID_CRED_R, TH_2, CRED_R, ? EAD_2 >>.
  - The ’signature’ field of the COSE_Sign1 object is computed with external_aad = << TH_2, CRED_R, ? EAD_2 >>.
* CRED_R is included in the transcript hash TH_3 which is used to calculate, e.g., keys for message 3:
  - TH_3 = H(TH_2, PLAINTEXT_2, CRED_R), where H() is the EDHOC hash algorithm of the selected cipher suite.
* CRED_I is used in the computation of the message field Signature_or_MAC_3 (see Section 5.4.2 of [RFC9528]):

- MAC_3 is computed with context_3 = << ID_CRED_I, TH_3, CRED_I, ? EAD_3 >>.

- The 'signature' field of the COSE_Sign1 object is computed with external_aad = << TH_3, CRED_I, ? EAD_3 >>.

* CRED_I is included in the transcript hash TH_4 which is used to calculate, e.g., keys for message 4 and the session key PRK_out:

  - TH_4 = H(TH_3, PLAINTEXT_3, CRED_I), where H() is the EDHOC hash algorithm of the selected cipher suite.

Since [RFC9528] requires the peers to use the authentication credentials to perform the protocol computations, and a client enrolling a certificate as described in the example in Section 2.2 only obtains a reference and/or a hash, it would not be able to use that certificate when authenticating to other peers.

# 4. Replacing Authentication Credential with Hash

To ensure the integrity of the authentication credentials it is sufficient to include in the computation a digest of the relevant authentication credentials using a secure hash function.

With this in mind we define a new mode of processing credentials in EDHOC where an authentication credential is replaced by a secure hash of that credential. The hash function used is the EDHOC hash function of the selected cipher suite, see Section 3.6 of [RFC9528].

## 4.1. New COSE Header Parameter

The new processing mode is indicated with the COSE header parameter 'Hashed Credential', see Section 7.1. The parameter has no value.

## 4.2. New Processing

The presence of the COSE header parameter 'Hashed Credential' in an ID_CRED_R indicates that CRED_R SHALL be replaced with H(CRED_R) in all EDHOC protocol computations, where H() is the EDHOC hash algorithm of the selected cipher suite. Analogously, the presence of the 'Hashed Credential' in an ID_CRED_I indicates that CRED_I SHALL be replaced with H(CRED_I) in all EDHOC protocol computations.

Note that this parameter may be (typically is) present together with other COSE header parameters identifying the credential.

The EDHOC processing described in Section 3 is thus replaced by the following:

* H(CRED_R) is used in the computation of the message field Signature_or_MAC_2:
  - MAC_2 is computed with context_2 = << C_R, ID_CRED_R, TH_2, H(CRED_R), ? EAD_2 >>.
  - The 'signature' field of the COSE_Sign1 object is computed with external_aad = << TH_2, H(CRED_R), ? EAD_2 >>.
* H(CRED_R) is included in the transcript hash TH_3:
  - TH_3 = H(TH_2, PLAINTEXT_2, H(CRED_R)).
* H(CRED_I) is used in the computation of the message field Signature_or_MAC_3:
  - MAC_3 is computed with context_3 = << ID_CRED_I, TH_3, H(CRED_I), ? EAD_3 >>.
  - The 'signature' field of the COSE_Sign1 object is computed with external_aad = << TH_3, H(CRED_I), ? EAD_3 >>.
* H(CRED_I) is included in the transcript hash TH_4:
  - TH_4 = H(TH_3, PLAINTEXT_3, H(CRED_I)).

## 5. Security Considerations

Replacing the credential with the hash value from a secure hash function does not impact the integrity properties. But it must be the correct hash and computed over the correct credential.

In case the Initiator's own credential is hashed without it having access to the credential, like the client in the example of Section 2.2, then the Initiator needs to obtain the hash of the credential from a trusted source. Similar for the Responder.

In case the Responder's credential is hashed, the then Initiator MUST verify that the credential hash is correct, and vice versa. Each peer typically needs access to the other peer's credential anyway, to be able to authenticate, verify credential and/or meta-data, etc.

## 6. Privacy Considerations

There are no privacy considerations.

## 7. IANA Considerations

### 7.1. COSE Header Parameters Registry

IANA is requested to register the entry 'Hashed Credential' in the "COSE Header Parameters" registry under the registry group "CBOR Object Signing and Encryption (COSE)" (see Figure 1). The parameter has no value. The Value Registry for this item is empty and omitted from the table below.

| Name | Label | Value Type | Description |
|---|---|---|---|
| Hashed Credential | TBD | - | The credential shall be replaced with the hash of the credential in protocol computations. |

Figure 1: COSE Header Parameter.

## 8. References

### 8.1. Normative References

[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>.

[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>.

### 8.2. Informative References

[I-D.ietf-ace-coap-est-oscore] Selander, G., Raza, S., Furuhed, M., Vuini, M., and T. Claeys, "Protecting EST Payloads with OSCORE", Work in Progress, Internet-Draft, draft-ietf-ace-coap-est-oscore-10, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-ace-coap-est-oscore-10>.

[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

## Authors' Addresses

Gran Selander
Ericsson
Email: goran.selander@ericsson.com

John Preu Mattsson
Ericsson
Email: john.mattsson@ericsson.com

Malia Vuini
Inria
Email: malisa.vucinic@inria.fr