Lightweight Authorization using Ephemeral Diffie-Hellman Over COSE (ELA)

Göran Selander, John Mattsson, Mališa Vučinić, Geovane Fedrecheski, Michael Richardson

Workgroup: LAKE Working Group
Internet-Draft: draft-ietf-lake-authz-03
Published: 21 October 2024
Intended Status: Standards Track
Expires: 24 April 2025
Authors: G. Selander J. Preuß Mattsson M. Vučinić
Ericsson AB Ericsson AB INRIA
G. Fedrecheski M. Richardson
INRIA Sandelman Software Works

Lightweight Authorization using Ephemeral Diffie-Hellman Over COSE (ELA)

Abstract

Ephemeral Diffie-Hellman Over COSE (EDHOC) is a lightweight authenticated key exchange protocol intended for use in constrained scenarios. This document specifies Lightweight Authorization using EDHOC (ELA). The procedure allows authorizing enrollment of new devices using the extension point defined in EDHOC. ELA is applicable to zero-touch onboarding of new devices to a constrained network leveraging trust anchors installed at manufacture time.

About This Document

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

The latest revision of this draft can be found at https://lake-wg.github.io/authz/draft-ietf-lake-authz.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-lake-authz/.

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

Source for this draft and an issue tracker can be found at https://github.com/lake-wg/authz.

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 24 April 2025.

Copyright Notice

Table of Contents

1. Introduction

For constrained IoT deployments [RFC7228] the overhead and processing contributed by security protocols may be significant, which motivates the specification of lightweight protocols that are optimizing, in particular, message overhead (see [I-D.ietf-lake-reqs]). This document describes Lightweight Authorization using EDHOC (ELA), a procedure for augmenting the lightweight authenticated Diffie-Hellman key exchange EDHOC [RFC9528] with third party-assisted authorization.

ELA involves a device, a domain authenticator, and an enrollment server. The device and domain authenticator perform mutual authentication and authorization, assisted by the enrollment server that provides relevant authorization information to the device (a "voucher") and to the authenticator. The high-level model is similar to BRSKI [RFC8995].

In this document, we consider the target interaction for which authorization is needed to be "enrollment", for example joining a network for the first time (e.g., [RFC9031]), but it can be applied to authorize other target interactions.

The enrollment server may represent the manufacturer of the device, or some other party with information about the device from which a trust anchor has been pre-provisioned into the device. The (domain) authenticator may represent the service provider or some other party controlling access to the network in which the device is enrolling.

ELA assumes that authentication between device and authenticator is performed with EDHOC [RFC9528], and defines the integration of a lightweight authorization procedure using the External Authorization Data (EAD) fields defined in EDHOC.

ELA enables a low message count by performing authorization and enrollment in parallel with authentication, instead of in sequence, which is common for network access. It further reuses protocol elements from EDHOC, leading to reduced message sizes on constrained links.

This protocol is applicable to a wide variety of settings, and can be mapped to different authorization architectures.

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 have an understanding of CBOR [RFC8949], CDDL [RFC8610], and EDHOC [RFC9528]. Appendix C.1 of [RFC9528] contains some basic info about CBOR.

2. Protocol Outline

The goal of ELA is to enable a (potentially constrained) device (U) to enroll into a domain over a constrained link. The device authenticates and enforces authorization of the (non-constrained) domain authenticator (V) with the help of a voucher conveying authorization information. The voucher has a similar role as in [RFC8366] but should be considerably more compact. The domain authenticator, in turn, authenticates the device and authorizes its enrollment into the domain.

The procedure is assisted by a (non-constrained) enrollment server (W) located in a non-constrained network behind the domain authenticator, e.g., on the Internet, providing information to the device (conveyed in the voucher) and to the domain authenticator as part of the protocol.

The objective of this document is to specify such a protocol that is lightweight over the constrained link, by reusing elements of EDHOC [RFC9528] and by shifting message overhead to the non-constrained side of the network. See illustration in Figure 1.

Note the cardinality of the involved parties. It is expected that the domain authenticator needs to handle a large unspecified number of devices, but for a given device type or manufacturer it is expected that one or a few nodes host enrollment servers.

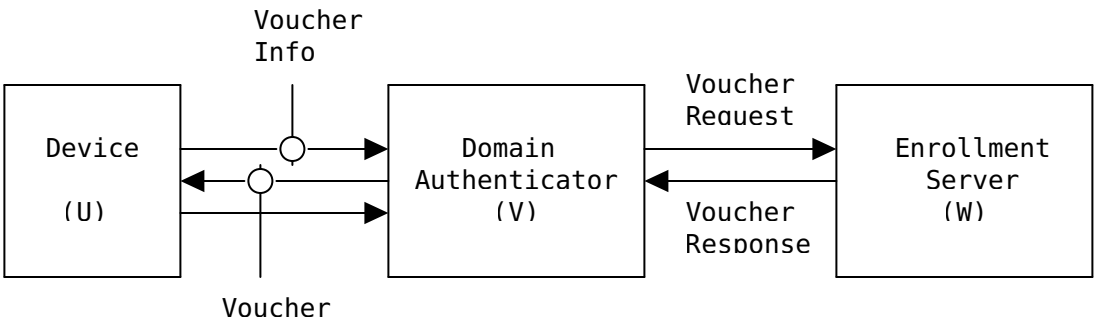

Figure 1: Overview of the message flow. EDHOC is used on the constrained link between U and V. Voucher Info and Voucher are sent in EDHOC External Authorization Data (EAD). The link between V and W is not constrained.

3. Assumptions

The protocol is based on the following pre-existing relations between the device (U), the domain authenticator (V) and the enrollment server (W), see Figure 2.

- U and W have an explicit relation: U is configured with a public key of W, see Section 3.1.
- V and W have an implicit relation, e.g., based on web PKI with trusted CA certificates, see Section 3.2.
- U and V need not have any previous relation. This protocol establishes a relation between U and V.

Each of the three parties can gain protected communication with the other two during the protocol.

V may be able to access credentials over non-constrained networks, but U may be limited to constrained networks. Implementations wishing to leverage the zero-touch capabilities of this protocol are expected to support transmission of credentials from V to U by value during the EDHOC exchange, which will impact the message size depending on the type of credential used.

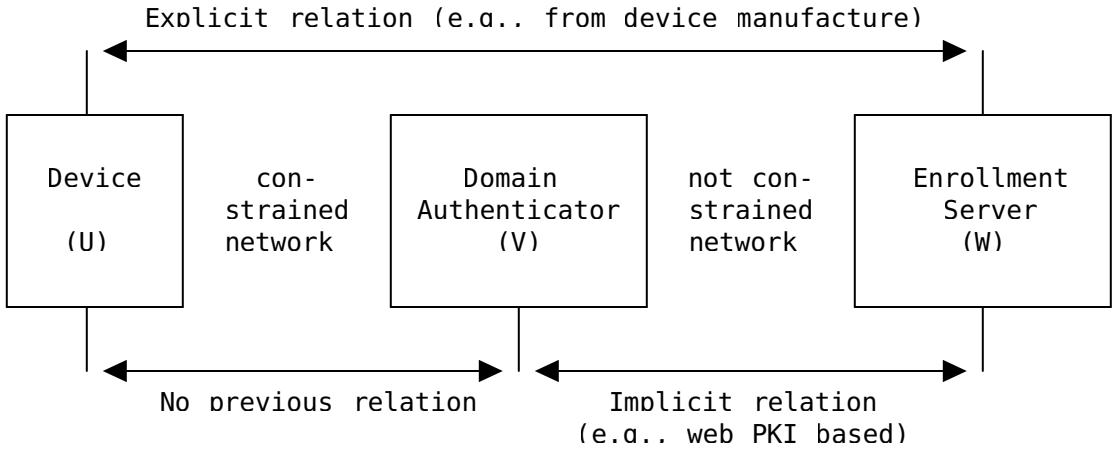

Figure 2: Overview of pre-existing relations.

3.1. Device (U)

To authenticate to V, the device (U) runs EDHOC in the role of Initiator with authentication credential CRED_U, for example, an X.509 certificate [RFC5280] or a CBOR Web Token (CWT, [RFC8392]). CRED_U may, for example, be carried by value in ID_CRED_I of EDHOC message_3 or be provisioned to V over a non-constrained network, leveraging a credential identifier in ID_CRED_I (see bottom of Figure 3).

U also needs to identify itself to W. The device identifier used for this is ID_U. The purpose of ID_U is for W to be able to determine if the device with this identifier is authorized to enroll with V. ID_U may be a reference to CRED_U, like ID_CRED_I in EDHOC (see Section 3.5.2 of [RFC9528]), or a device identifier from a different name space, such as EUI-64 identifiers.

U is also provisioned with information about W:

- A static public DH key of W (G_W) used to establish secure communication with the enrollment server (see Section 4.4).

- Location information about the enrollment server (LOC_W) that can be used by V to reach W. This is typically a URI but may alternatively be only the domain name.

3.2. Domain Authenticator (V)

To authenticate to U, the domain authenticator (V) runs EDHOC in the role of Responder with an authentication credential CRED_V containing a public key of V, see Section 4.5.2.1. This proves to U the possession of the private key corresponding to the public key of CRED_V. CRED_V typically needs to be transported to U in EDHOC (using ID_CRED_R = CRED_V, see Section 3.5.2 of [RFC9528]) since there is no previous relation between U and V.

V and W need to establish a secure (confidentiality and integrity protected) connection for the Voucher Request/Response protocol. Furthermore, W needs to access the same credential CRED_V that V uses with U (to compute the Voucher), and V needs to prove to W the possession of the private key corresponding to the public key of CRED_V. It is RECOMMENDED that V authenticates to W using the same credential CRED_V as with U.

Note that the choice of protocols may affect which type of credential and methods should be used by V. For example, in case V and W select TLS for the secure channel and PoP, then CRED_V is a X.509 certificate, and the EDHOC method used by V is signature-based. Some of the possible combinations of protocols to secure the connection between V and W are listed in Table 1 below.

Secure channel between V and W	Proof-of-Possession from V to W	Type of CRED_V	EDHOC method used by V
[D]TLS 1.3 with mutual authentication, where V is the client and W is the server.	Provided by [D]TLS.	Restricted to types that are supported by both [D]TLS and EDHOC, e.g., X.509 certificates.	V MUST authenticate using a signature.
[D]TLS 1.3, where V is the client and W is the server.	Run an EDHOC session on top of the TLS-protected channel.	Any type supported by EDHOC, e.g., X.509, C509, CWT, or CCS.	Any method may be used.
EDHOC and OSCORE, where V is the initiator and W is the responder.	Already provided by EDHOC during the setup of the secure channel.	Any type supported by EDHOC.	Any method may be used.

Table 1: Examples of how to secure the connection between V and W.

Note also that the secure connection between V and W may be long-lived and reused for multiple voucher requests/responses.

Other details of proof-of-possession related to CRED_V and transport of CRED_V are out of scope of this document.

3.3. Enrollment Server (W)

The enrollment server (W) is assumed to have the private DH key corresponding to G_W, which is used to establish secure communication with the device (see Section 4.4). W provides to U the authorization decision for enrollment with V in the form of a voucher (see Section 4.4.2). Authorization policies are out of scope for this document.

Authentication credentials and communication security with V is described in Section 3.2. To calculate the voucher, W needs access to message_1 and CRED_V as used in the EDHOC session between U and V, see Section 4.4.2.

- *W MUST verify that CRED_V is bound to the secure connection between W and V

- *W MUST verify that V is in possession of the private key corresponding to the public key of CRED_V

W needs to be available during the execution of the protocol between U and V.

4. The Protocol

4.1. Overview

The ELA protocol consist of three security sessions going on in parallel:

1. The EDHOC session between device (U) and (domain) authenticator (V)

2. Voucher Request/Response between authenticator (V) and enrollment server (W)

3. An exchange of voucher-related information, including the voucher itself, between device (U) and enrollment server (W), mediated by the authenticator (V).

Figure 3 provides an overview of the message flow detailed in this section. An outline of EDHOC is given in Section 2 of [RFC9528].

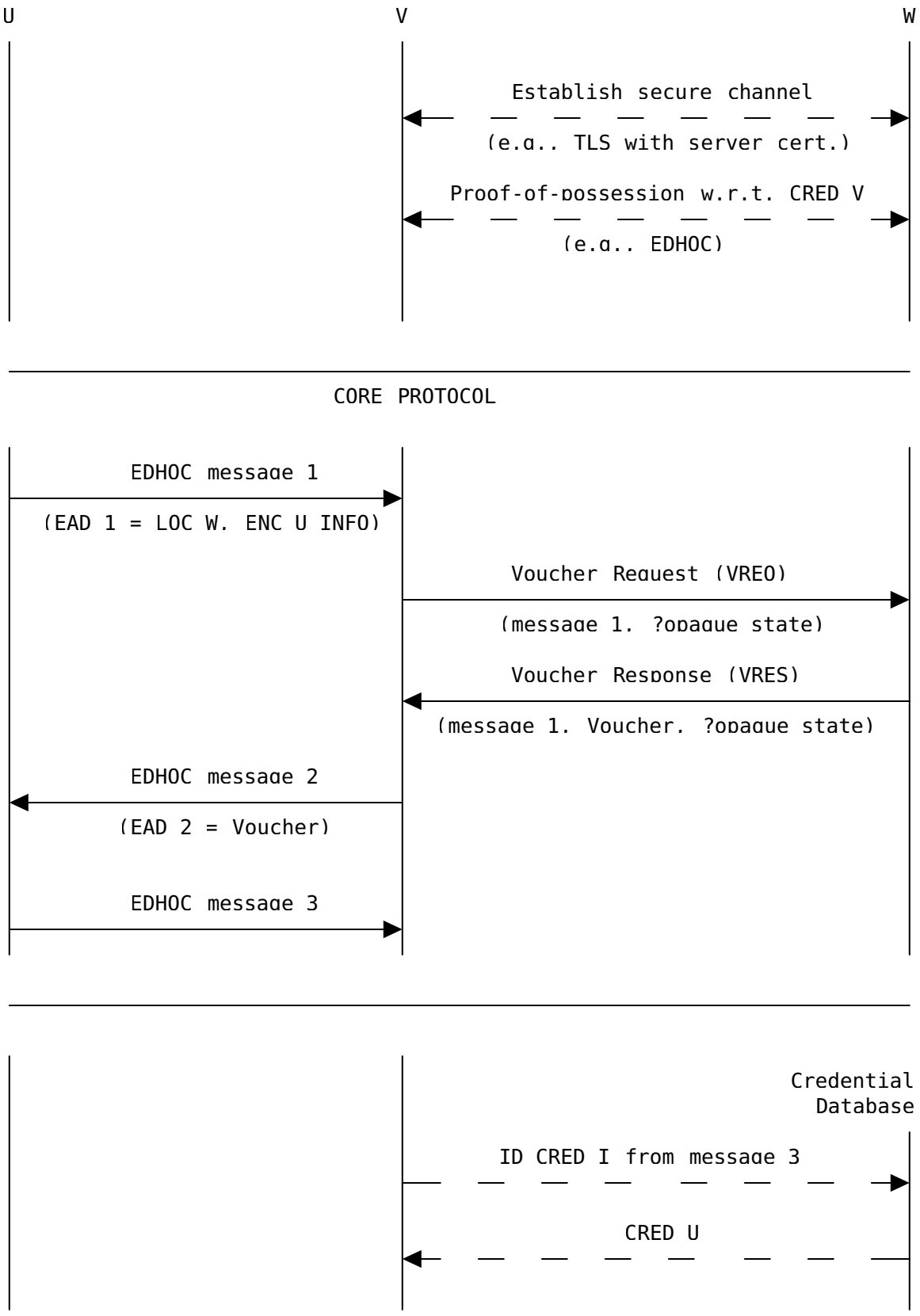
U
V
W
Establish secure channel
(e.g., TLS with server cert.)
Proof-of-possession w.r.t. CRED V
(e.g., EDHOC)
CORE PROTOCOL
EDHOC message 1
(EAD 1 = LOC W, ENC U INFO)
Voucher Request (VREQ)
(message 1, ?opaque state)
Voucher Response (VRES)
(message 1, Voucher, ?opaque state)
EDHOC message 2
(EAD 2 = Voucher)
EDHOC message 3
Credential
Database
ID CRED I from message 3
CRED U

Figure 3: Overview of ELA: W-assisted authorization of U and V to each other: EDHOC between U and V, and Voucher Request/Response between V and W. Before the protocol, V and W are assumed to have established a secure channel and performed proof-of-possession of relevant keys. Credential lookup of CRED_U may involve W or other credential database.

4.2. Reuse of EDHOC

The ELA protocol illustrated in Figure 3 reuses several components of EDHOC:

* G_X, the ephemeral public Diffie-Hellman key of U, is also used in the protocol between U and W.

* SUITES_I includes the cipher suite for EDHOC selected by U, and also defines the algorithms used between U and W (see Section 3.6 of [RFC9528]):

  - EDHOC AEAD algorithm: used to encrypt ID_U and to generate voucher

  - EDHOC hash algorithm: used for key derivation

  - EDHOC key exchange algorithm: used to calculate the shared secret between U and W

* EAD_1, EAD_2 are the External Authorization Data message fields of message_1 and message_2, respectively, see Section 3.8 of [RFC9528]. This document specifies the EAD items with ead_label = TBD1, see Section 8.1).

* ID_CRED_I and ID_CRED_R are used to identify the authentication credentials CRED_U and CRED_V, respectively. As shown at the bottom of Figure 3, V may use W to obtain CRED_U. CRED_V is transported in ID_CRED_R in message_2, see Section 4.5.2.1.

The protocol also reuses the EDHOC_Extract and EDHOC_Expand key derivation from EDHOC (see Section 4 of [RFC9528]).

* The intermediate pseudo-random key PRK is derived using EDHOC_Extract():

  - PRK = EDHOC_Extract(salt, IKM)

    owhere salt = 0x (the zero-length byte string)

    oIKM is computed as an ECDH cofactor Diffie-Hellman shared secret from the public key of W, G_W, and the private key corresponding to G_X (or v.v.), see Section 5.7.1.2 of [NIST-800-56A].

The output keying material OKM is derived from PRK using EDHOC_Expand(), which is defined in terms of the EDHOC hash algorithm of the selected cipher suite, see Section 4.1.2 of [RFC9528]:

```
  *OKM = EDHOC_Expand(PRK, info, length)

   where

info = (
   info_label : int,
   context : bstr,
   length : uint,
)
```

4.3. Stateless Operation of V

V may act statelessly with respect to U: the state of the EDHOC session started by U may be dropped at V until authorization from W is received. Once V has received EDHOC message_1 from U and extracted LOC_W from EAD_1, message_1 is forwarded unmodified to W in the form of a Voucher Request (see Section 4.6.1). V encapsulates the internal state that it needs to later respond to U, and sends that to W together with EDHOC message_1. This state typically contains addressing information of U (e.g., U's IP address and port number), together with any other implementation-specific parameter needed by V to respond to U. At this point, V can drop the EDHOC session that was initiated by U.

The encapsulated state MUST be protected using a uniformly-distributed (pseudo-)random key, known only to itself and specific for the current EDHOC session to prevent replay attacks of old encapsulated state.

How V serializes and encrypts its internal state is out of scope in this specification. For example, V may use CBOR and COSE.

Editor's note: Consider to include an example of serialized internal state.

W sends to V the voucher together with the echoed message_1, as received from U, and V's internal state, see Section 4.6.2. This allows V to act as a simple message relay until it has obtained the authorization from W to enroll U. The reception of a successful Voucher Response at V from W implies the authorization for V to enroll U. At this point, V can initialize a new EDHOC session with U, based on the message and the state retrieved from the Voucher Response from W.

4.4. Device <-> Enrollment Server (U <-> W)

The protocol between U and W is carried between U and V in message_1 and message_2 (Section 4.5), and between V and W in the Voucher Request/Response (Section 4.6). The data is protected between the

endpoints using secret keys derived from a Diffie-Hellman shared secret (see Section 4.2) as further detailed in this section.

4.4.1. Voucher Info

The external authorization data EAD_1 contains an EAD item with ead_label = TBD1 and ead_value = Voucher_Info, which is a CBOR byte string:

```
Voucher_Info = bstr .cborseq Voucher_Info_Seq

Voucher_Info_Seq = [ ; used as a CBOR sequence, not array
    LOC_W:      tstr,
    ENC_U_INFO:     bstr
]
```

where

- LOC_W is a text string used by V to locate W, e.g., a URI or a domain name.

- ENC_U_INFO is a byte string containing an encrypted identifier of U and, optionally, opaque application data prepared by U. It is calculated as follows:

ENC_U_INFO is encrypted using the EDHOC AEAD algorithm of the selected cipher suite specified in SUITE_I of EDHOC message_1. It consists of 'ciphertext' of COSE_Encrypt0 (Section 5.2 of [RFC9052]) computed from the following:

- The encryption key K_1 and nonce IV_1 are derived as specified below.

- 'protected' is a byte string of size 0

- 'plaintext' and 'external_aad' as below:

```
plaintext = (
    ID_U:           bstr,
)

external_aad = (
    SS:             int,
)
```

where

- ID_U is an identifier of the device, see Section 3.1.

- SS is the selected cipher suite in SUITES_I of EDHOC message_1, see Section 4.5.

The external_aad is wrapped in an enc_structure as defined in Section 5.3 of [RFC9052].

Editor's note: Add more context to external_aad.

The derivation of K_1 = EDHOC_Expand(PRK, info, length) uses the following input to the info struct (see OKM in Section 4.2):

- *info_label = 0

- *context = h'' (the empty CBOR string)

- *length is length of the key of the EDHOC AEAD algorithm in bytes (which is the length of K_1)

The derivation of IV_1 = EDHOC_Expand(PRK, info, length) uses the following input to the info struct (see OKM in Section 4.2):

- *info_label = 1

- *context = h'' (the empty CBOR string)

- *length is length of the nonce of the EDHOC AEAD algorithm in bytes (which is the length of IV_1)

4.4.2. Voucher

The voucher is an assertion to U that W has authorized V. It is encrypted using the EDHOC AEAD algorithm of the selected cipher suite specified in SUITE_I of EDHOC message_1. It consists of the 'ciphertext' field of a COSE_Encrypt0 object, which is a byte string, as defined below.

```
Voucher = bstr
```

Its corresponding plaintext value consists of an opaque field that can be used by W to convey information to U, such as a voucher scope. The authentication tag present in the ciphertext is also bound to message_1 and the credential of V as described below.

- *The encryption key K_2 and nonce IV_2 are derived as specified below.

- *'protected' is a byte string of size 0

- *'plaintext' and 'external_aad' as below:

```
plaintext = (
    ?OPAQUE_INFO: bstr
)
```

```
external_aad = (
    H_message_1:  bstr,
    CRED_V:        bstr,
)
```

where

- *OPAQUE_INFO is an opaque field provided by the application. If present, it will contain application data that W may want to convey to U, e.g., a voucher scope. Note that OPAQUE_INFO is opaque when viewed as an information element in EDHOC. It is opaque to V, while the application in U and W can read its contents.

- *H_message_1 is the hash of EDHOC message_1, calculated from the associated voucher request, see Section 4.6.1. The hash is computed by using the EDHOC hash algorithm of the selected cipher suite specified in SUITE_I of EDHOC message_1.

- *CRED_V is the credential used by V to authenticate to U and W, see Section 4.5.2.1 and Table 1.

The derivation of K_2 = EDHOC_Expand(PRK, info, length) uses the following input to the info struct (see Section 4.2):

- *info_label = 2

- *context = h'' (the empty CBOR string)

- *length is length of the key of the EDHOC AEAD algorithm in bytes

The derivation of IV_2 = EDHOC_Expand(PRK, info, length) uses the following input to the info struct (see Section 4.2):

- *info_label = 3

- *context = h'' (the empty CBOR string)

- *length is length of the nonce of the EDHOC AEAD algorithm in bytes

4.5. Device <-> Authenticator (U <-> V)

This section describes the processing in U and V, which includes the EDHOC protocol, see Figure 3. Normal EDHOC processing is omitted here.

4.5.1. Message 1

4.5.1.1. Processing in U

U composes EDHOC message_1 using authentication method, identifiers, etc. according to an agreed application profile, see Section 3.9 of [RFC9528]. The selected cipher suite, in this document denoted SS,

applies also to the interaction with W as detailed in Section 4.2, in particular, with respect to the Diffie-Hellman key agreement algorithm used between U and W. As part of the normal EDHOC processing, U generates the ephemeral public key G_X that is reused in the interaction with W, see Section 4.4.

The device sends EDHOC message_1 with EAD item (-TBD1, Voucher_Info) included in EAD_1, where Voucher_Info is specified in Section 4.4. The negative sign indicates that the EAD item is critical, see Section 3.8 of [RFC9528].

4.5.1.2. Processing in V

V receives EDHOC message_1 from U and processes it as specified in Section 5.2.3 of [RFC9528], with the additional step of processing the EAD item in EAD_1. Since the EAD item is critical, if V does not recognize it or it contains information that V cannot process, then V MUST abort the EDHOC session, see Section 3.8 of [RFC9528]. Otherwise, the ead_label = TBD1 triggers the voucher request to W as described in Section 4.6. The exchange between V and W needs to be completed successfully for the EDHOC session to be continued.

4.5.2. Message 2

4.5.2.1. Processing in V

V receives the voucher response from W as described in Section 4.6.

V sends EDHOC message_2 to U with the critical EAD item (-TBD1, Voucher) included in EAD_2, i.e., ead_label = TBD1 and ead_value = Voucher, as specified in Section 4.4.2.

The type of CRED_V may depend on the selected mechanism for the establishment of a secure channel between V and W, See Table 1.

In case the network between U and V is constrained, it is recommended that CRED_V be a CWT Claims Set (CCS) [RFC8392]. The CCS contains the public authentication key of V encoded as a COSE_Key in the 'cnf' claim, see Section 3.5.2 of [RFC9528]. ID_CRED_R contains the CWT Claims Set with 'kccs' as COSE header_map, see Section 10.6 of [RFC9528].

4.5.2.2. Processing in U

U receives EDHOC message_2 from V and processes it as specified in Section 5.3.3 of [RFC9528], with the additional step of processing the EAD item in EAD_2.

If U does not recognize the EAD item or the EAD item contains information that U cannot process, then U MUST abort the EDHOC session, see Section 3.8 of [RFC9528]. Otherwise, U MUST verify the Voucher using H_message_1, CRED_V, and the keys derived as in

Section 4.4.2. If the verification fails then U MUST abort the EDHOC session.

If OPAQUE_INFO is present, it is made available to the application.

4.5.3. Message 3

4.5.3.1. Processing in U

If all verifications are passed, then U sends EDHOC message_3.

EDHOC message_3 may be combined with an OSCORE-protected application request, see [I-D.ietf-core-oscore-edhoc].

4.5.3.2. Processing in V

V performs the normal EDHOC verifications of message_3. V may retrieve CRED_U from a Credential Database, after having learned ID_CRED_I from U.

4.6. Authenticator <-> Enrollment Server (V <-> W)

It is assumed that V and W have set up a secure connection, W has accessed the authentication credential CRED_V to be used in the EDHOC session between V and U, and that W has verified that V is in possession of the private key corresponding to CRED_V, see Section 3.2 and Section 3.3. V and W run the Voucher Request/Response protocol over the secure connection.

4.6.1. Voucher Request

4.6.1.1. Processing in V

V sends the voucher request to W. The Voucher Request SHALL be a CBOR array as defined below:

```
Voucher_Request = [
    message_1:      bstr,
    ? opaque_state: bstr
]
```

where

- *message_1 is a CBOR byte string whose value is the byte serialization of EDHOC message_1 as it was received from U.

- *opaque_state is OPTIONAL and represents the serialized and encrypted opaque state needed by V to statelessly respond to U after the reception of Voucher_Response.

4.6.1.2. Processing in W

W receives and parses the voucher request received over the secure connection with V. The voucher request essentially contains EDHOC message_1 as sent by U to V. W SHALL NOT process message_1 as if it was an EDHOC message intended for W.

W extracts from message_1:

- SS - the selected cipher suite, which is the (last) integer of SUITES_I.

- G_X - the ephemeral public key of U

- ENC_U_INFO - the encryption of the device identifier ID_U, contained in the Voucher_Info field of the EAD item with ead_label = TBD1 (with minus sign indicating criticality)

W verifies and decrypts ENC_U_INFO using the relevant algorithms of the selected cipher suite SS (see Section 4.2), and obtains ID_U.

W calculates the hash of message_1 H_message_1, and associates this session identifier to the device identifier ID_U. Note that message_1 contains a unique ephemeral key, therefore H_message_1 is expected to be unique.

If processing fails up until this point, the protocol SHALL be aborted with an error code signaling a generic issue with the request, see Section 6.4.1.

W uses ID_U to look up the associated authorization policies for U and enforces them. This is out of scope for the specification.

If ID_U is known by W, but authorization fails, the protocol SHALL be aborted with an error code signaling an access control issue, see Section 4.7 and Section 6.4.1.

4.6.2. Voucher Response

4.6.2.1. Processing in W

W retrieves CRED_V associated with the secure connection with V, and constructs the Voucher for the device with identifier ID_U (see Section 4.4.2).

W generates the voucher response and sends it to V over the secure connection. The Voucher_Response SHALL be a CBOR array as defined below:

```
Voucher_Response = [
    message_1:      bstr,
    Voucher:        bstr,
    ? opaque_state: bstr
]
```

where

- *message_1 is a CBOR byte string whose value is the byte serialization of EDHOC message_1 as it was received from V.

- *The Voucher is defined in Section 4.4.2.

- *opaque_state is the echoed byte string opaque_state from Voucher_Request, if present.

W signals the successful generation of the voucher via a status code in the REST interface, as defined in Section 6.4.1.

4.6.2.2. Processing in V

V receives the voucher response from W over the secure connection. If present, V decrypts and verifies opaque_state as received from W. If that verification fails, then the EDHOC session with U is aborted. If the voucher response is successfully received from W, then V responds to U with EDHOC message_2 as described in Section 4.5.2.1.

4.7. Error Handling

This section specifies a new EDHOC error code and how it is used in ELA.

4.7.1. EDHOC Error "Access denied"

This section specifies the new EDHOC error "Access denied", see Figure 4.

ERR CODE	ERR INFO Type	Description
TBD3	error content	Access denied

Figure 4: EDHOC error code and error information for ‘Access denied’.

Error code TBD3 is used to indicate to the receiver that access control has been applied and the sender has aborted the EDHOC session. The ERR_INFO field contains error_content which is a CBOR Sequence consisting of an integer and an optional byte string.

```
error_content = (
  REJECT_TYPE : int,
  ? REJECT_INFO : bstr,
)
```

The purpose of REJECT_INFO is for the sender to provide verifiable and actionable information to the receiver about the error, so that an automated action may be taken to enable access.

REJECT TYPE	REJECT INFO	Description
0	-	No REJECT INFO
1	bstr	REJECT INFO from trusted third party

Figure 5: REJECT_TYPE and REJECT_INFO for 'Access denied'.

4.7.2. Error handling in W, V, and U

ELA uses the EDHOC Error "Access denied" in the following way:

- W generates error_content and transfers it to V via the secure connection. If REJECT_TYPE is 1, then REJECT_INFO is encrypted from W to U using the EDHOC AEAD algorithm. W signals the error via an appropriate status code in the REST interface, as defined in Section 6.4.1.

- V receives error_content, prepares an EDHOC "Access denied" error, and sends it to U.

- U receives the error message and extracts the error_content. If REJECT_TYPE is 1, then U decrypts REJECT_INFO, based on which it may retry to gain access.

The encryption of REJECT_INFO follows a procedure analogous to the one defined in Section 4.4.2, with the following differences:

```
plaintext = (
    OPAQUE_INFO:     bstr,
 )

external_aad = (
    H_message_1:    bstr,
 )
```

where

*OPAQUE_INFO is an opaque field that contains actionable information about the error. It may contain, for example, a list of suggested Vs through which U should join instead.

*H_message_1 is the hash of EDHOC message_1, calculated from the associated voucher request, see Section 4.6.1.

5. Optimization Strategies

When ELA is used for zero-touch enrollment, U normally has little to no knowledge of the available V's. This may lead to situations where U has to retry several times at different V's until it finds one that works. This section presents two optimization strategies for such cases. They were developed to address scenarios where V's are radio gateways to which U wants to enroll, but may also be applicable to other use cases.

5.1. U anycasts message_1

This strategy consists in U disseminating EDHOC message_1 as anycast (a broadcast from which only one successful message_2 response is expected). When each of the V's in radio range of U receive message_1, one of the following can happen:

*V does not implement EDHOC, and drops the message

*V does not implement ELA, and since EAD_1 is critical, it either responds with an error or drops the message (Editor's note: dropping actually conflicts with the EAD field being critical)

*V forwards message_1 to W as VREQ, but W does not authorize it, and error handling is applied

*V forwards message_1 to W as VREQ, W authorizes it, and the protocol continues normally

U is expected to receive at most one message_2 as response, which contains the Voucher. In case U receives additional message_2's, they MUST be silently dropped.

This strategy may increase the number of messages that need to be processed by V and W, in exchange for reducing resource usage in U.

Security concerns related to this strategy, including potential reuse of G_X and double processing of message_2, are discussed in Section 7.

5.2. V advertises support for ELA

In this strategy, V shares some information (V_INFO) with a potential U, that can help it decide whether to try to enroll with that V.

The exact contents of the V_INFO structure, as well as the mechanism used to transport it, will depend on the underlying communication technology and also on application needs. For example, V_INFO may state that:

*V implements ELA -- similarly to how EAPOL [IEEE802.1X] frames state support for IEEE 802.1X.

*V is part of a certain domain -- similarly to how Eduroam [RFC7593] is used in the SSID field of IEEE 802.11 packets

V_INFO can be sent over a network beacon (see Appendix C.1), which may require technology specific profiling, e.g., the IEEE 802.15.4 enhanced beacon may be extended according to [RFC8137]. Alternatively, V_INFO can be sent as part of an EAD field, as shown in Appendix C.2.

As a guideline for implementers, we define the following field that can be included in a V_INFO structure:

DOMAIN_ID: bstr

The DOMAIN_ID field identifies the domain to which V belongs to, for example an URL or UUID.

Appendix C presents three examples of how the advertisement strategy may be applied according to different application needs.

6. REST Interface at W

The interaction between V and W is enabled through a RESTful interface exposed by W. This RESTful interface MAY be implemented using either HTTP or CoAP. V SHOULD access the resources exposed by W through the protocol indicated by the scheme in the LOC_W URI.

6.1. Scheme "https"

In case the scheme indicates "https", V MUST perform a TLS handshake with W and access the resources defined in Section 6.4 using HTTP. If the authentication credential CRED_V can be used in a TLS handshake, e.g., an X.509 certificate of a signature public key, then V SHOULD use it to authenticate to W as a client. If the authentication credential CRED_V cannot be used in a TLS handshake, e.g., if the public key is a static Diffie-Hellman key, then V SHOULD first perform a TLS handshake with W using available compatible keys. V MUST then perform an EDHOC session over the TLS connection proving to W the possession of the private key corresponding to CRED_V. Performing the EDHOC session is only necessary if V did not authenticate with CRED_V in the TLS handshake with W.

Editor's note: Clarify that performing TLS handshake is not necessary for each device request; if there already is a TLS connection between

V and W that should be reused. Similar considerations for 5.2 and 5.3.

6.2. Scheme "coaps"

In case the scheme indicates "coaps", V SHOULD perform a DTLS handshake with W and access the resources defined in Section 6.4 using CoAP. The normative requirements in Section 6.1 on performing the DTLS handshake and EDHOC session remain the same, except that TLS is replaced with DTLS.

6.3. Scheme "coap"

In case the scheme indicates "coap", V SHOULD perform an EDHOC session with W, as specified in Appendix A of [RFC9528] and access the resources defined in Section 6.4 using OSCORE and CoAP. The authentication credential in this EDHOC session MUST be CRED_V.

6.4. URIs

The URIs defined below are valid for both HTTP and CoAP. W MUST support the use of the path-prefix "/.well-known/", as defined in [RFC8615], and the registered name "lake-authz". A valid URI in case of HTTP thus begins with

* "https://www.example.com/.well-known/lake-authz"

In case of CoAP with DTLS:

* "coaps://example.com/.well-known/lake-authz"

In case of EDHOC and OSCORE:

* "coap://example.com/.well-known/lake-authz"

Each operation specified in the following is indicated by a path-suffix.

6.4.1. Voucher Request (/voucherrequest)

To request a voucher, V MUST issue a request such that:

* Method is POST

* Payload is the serialization of the Voucher Request object, as specified in Section 4.6.1.

* Content-Format (Content-Type) is set to "application/lake-authz-voucherrequest+cbor"

In case of successful processing at W, W MUST issue a response such that:

- *Status code is 200 OK if using HTTP, or 2.04 Changed if using CoAP

- *Payload is the serialized Voucher Response object, as specified in Section 4.6.2

- *Content-Format (Content-Type) is set to "application/lake-authz-voucherresponse+cbor"

In case of error, two cases should be considered:

- *U cannot be identified: this happens either if W fails to process the Voucher Request, or if it succeeds but ID_U is considered unknown to W. In this case, W MUST reply with 400 Bad Request if using HTTP, or 4.00 if using CoAP.

- *U is identified but unauthorized: this happens if W is able to process the Voucher Request, and W recognizes ID_U as a known device, but the access policies forbid enrollment. For example, the policy could enforce enrollment within a delimited time window, via a specific V, etc. In this case, W MUST reply with a 403 Forbidden code if using HTTP, or 4.03 if using CoAP; the payload is the serialized error_content object, with Content-Format (Content-Type) set to "application/lake-authz-vouchererror+cbor". The payload MAY be used by V to prepare an EDHOC error "Access Denied", see Section 4.7.

6.4.2. Certificate Request (/certrequest)

V requests the public key certificate of U from W through the "/certrequest" path-suffix. To request U's authentication credential, V MUST issue a request such that:

- *Method is POST

- *Payload is the serialization of the ID_CRED_I object, as received in EDHOC message_3.

- *Content-Format (Content-Type) is set to "application/lake-authz-certrequest+cbor"

In case of a successful lookup of the authentication credential at W, W MUST issue a response such that:

- *Status code is 200 OK if using HTTP, or 2.04 Changed if using CoAP

- *Payload is the serialized CRED_U

- *Content-Format (Content-Type) is set to "application/lake-authz-certresponse+cbor"

7. Security Considerations

This specification builds on and reuses many of the security constructions of EDHOC, e.g., shared secret calculation and key derivation. The security considerations of EDHOC [RFC9528] apply with modifications discussed here.

EDHOC provides identity protection of the Initiator, here the device. The encryption of the device identifier ID_U in the first message should consider potential information leaking from the length of ID_U, either by making all identifiers having the same length or the use of a padding scheme.

Although W learns about the identity of U after receiving VREQ, this information must not be disclosed to V, until U has revealed its identity to V with ID_CRED_I in message_3. W may be used for lookup of CRED_U from ID_CRED_I, or this credential lookup function may be separate from the authorization function of W, see Figure 3. The trust model used here is that U decides to which V it reveals its identity. In an alternative trust model where U trusts W to decide to which V it reveals U's identity, CRED_U could be sent in Voucher Response.

As noted in Section 9.2 of [RFC9528] an ephemeral key may be used to calculate several ECDH shared secrets. In this specification, the ephemeral key G_X is also used to calculate G_XW, the shared secret with the enrollment server.

The private ephemeral key is thus used in the device for calculations of key material relating to both the authenticator and the enrollment server. There are different options for where to implement these calculations. One option is as an addition to EDHOC, i.e., to extend the EDHOC API in the device, so that EDHOC can import the public key of W (G_W) and the device identifier of U (ID_U), and then produce the encryption of ID_U which is included in Voucher_Info in EAD_1.

8. IANA Considerations

8.1. EDHOC External Authorization Data Registry

IANA has registered the following entry in the "EDHOC External Authorization Data" registry under the group name "Ephemeral Diffie-Hellman Over COSE (EDHOC)". The ead_label = TBD1 corresponds to the ead_value Voucher_Info in EAD_1, and Voucher in EAD_2 with processing specified in Section 4.5.1 and Section 4.5.2, respectively, of this document.

Label	Value Type	Description
TBD1	bstr	Voucher related information

Table 2: Addition to the EDHOC EAD registry

8.2. The Well-Known URI Registry

IANA has registered the following entry in "The Well-Known URI Registry", using the template from [RFC8615]:

*URI suffix: lake-authz

*Change controller: IETF

*Specification document: [[this document]]

*Related information: None

8.3. Well-Known Name Under ".arpa" Name Space

This document allocates a well-known name under the .arpa name space according to the rules given in [RFC3172] and [RFC6761]. The name "lake-authz.arpa" is requested. No subdomains are expected, and addition of any such subdomains requires the publication of an IETF Standards Track RFC. No A, AAAA, or PTR record is requested.

8.4. Media Types Registry

IANA has added the media types "application/lake-authz-voucherrequest+cbor" to the "Media Types" registry.

8.4.1. application/lake-authz-voucherrequest+cbor Media Type Registration

*Type name: application

*Subtype name: lake-authz-voucherrequest+cbor

*Required parameters: N/A

*Optional parameters: N/A

*Encoding considerations: binary (CBOR)

*Security considerations: See Section 7 of this document.

*Interoperability considerations: N/A

*Published specification: [[this document]] (this document)

*Application that use this media type: To be identified

*Fragment identifier considerations: N/A

*Additional information:

-Magic number(s): N/A

-File extension(s): N/A

-Macintosh file type code(s): N/A

*Person & email address to contact for further information: IETF LAKE Working Group (lake@ietf.org)

*Intended usage: COMMON

*Restrictions on usage: N/A

*Author: LAKE WG

*Change Controller: IESG

8.5. CoAP Content-Formats Registry

IANA has added the following Content-Format number in the "CoAP Content-Formats" registry under the registry group "Constrained RESTful Environments (CoRE) Parameters".

Content Type	Content Encoding	ID	Reference
application/lake-authz-voucherrequest+cbor	-	TBD2	[[this document]]

Table 3: Addition to the CoAP Content-Formats registry

9. References

9.1. Normative References

[NIST-800-56A] Barker, E., Chen, L., Roginsky, A., Vassilev, A., and R. Davis, "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography - NIST Special Publication 800-56A, Revision 3", April 2018, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf>.

[RFC8366] Watsen, K., Richardson, M., Pritikin, M., and T. Eckert, "A Voucher Artifact for Bootstrapping Protocols", RFC 8366, DOI 10.17487/RFC8366, May 2018, <https://www.rfc-editor.org/info/rfc8366>.

[RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/info/rfc8392>.

[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/info/rfc8613>.

[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/info/rfc8949>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/info/rfc9052>.

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

9.2. Informative References

[I-D.amsuess-core-coap-over-gatt] Amsüss, C., "CoAP over GATT (Bluetooth Low Energy Generic Attributes)", Work in Progress, Internet-Draft, draft-amsuess-core-coap-over-gatt-07, 25 September 2024, <https://datatracker.ietf.org/doc/html/draft-amsuess-core-coap-over-gatt-07>.

[I-D.ietf-core-oscore-edhoc] Palombini, F., Tiloca, M., Höglund, R., Hristozov, S., and G. Selander, "Using Ephemeral Diffie-Hellman Over COSE (EDHOC) with the Constrained Application Protocol (CoAP) and Object Security for Constrained RESTful Environments (OSCORE)", Work in Progress, Internet-Draft, draft-ietf-core-oscore-edhoc-11, 9 April 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-core-oscore-edhoc-11>.

[I-D.ietf-lake-reqs] Vučinić, M., Selander, G., Mattsson, J. P., and D. Garcia-Carillo, "Requirements for a Lightweight AKE for OSCORE", Work in Progress, Internet-Draft, draft-ietf-lake-reqs-04, 8 June 2020, <https://datatracker.ietf.org/doc/html/draft-ietf-lake-reqs-04>.

[IEEE802.15.4] IEEE standard for Information Technology, "IEEE Std 802.15.4 Standard for Low-Rate Wireless Networks", n.d..

[IEEE802.1X] IEEE standard for Information Technology, "IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control", February 2010.

[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/info/rfc2119>.

[RFC3172] Huston, G., Ed., "Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa")", BCP 52, RFC 3172, DOI 10.17487/RFC3172, September 2001, <https://www.rfc-editor.org/info/rfc3172>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", RFC 6761, DOI 10.17487/RFC6761, February 2013, <https://www.rfc-editor.org/info/rfc6761>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/info/rfc7228>.

[RFC7593] Wierenga, K., Winter, S., and T. Wolniewicz, "The eduroam Architecture for Network Roaming", RFC 7593, DOI 10.17487/RFC7593, September 2015, <https://www.rfc-editor.org/info/rfc7593>.

[RFC8137] Kivinen, T. and P. Kinney, "IEEE 802.15.4 Information Element for the IETF", RFC 8137, DOI 10.17487/RFC8137, May 2017, <https://www.rfc-editor.org/info/rfc8137>.

[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/info/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[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/info/rfc8610>.

[RFC8615] Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, DOI 10.17487/RFC8615, May 2019, <https://www.rfc-editor.org/info/rfc8615>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key

Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/info/rfc8995>.

[RFC9031] Vučinić, M., Ed., Simon, J., Pister, K., and M. Richardson, "Constrained Join Protocol (CoJP) for 6TiSCH", RFC 9031, DOI 10.17487/RFC9031, May 2021, <https://www.rfc-editor.org/info/rfc9031>.

Appendix A. Use with EDHOC reverse flow

Editor's note: I am not sure if this should be an appendix or an actual section in the main document.

This appendix describes how the protocol can be used with the EDHOC reverse message flow defined in Appendix A.2.2 of [RFC9528], where the CoAP client is the Responder and the CoAP server is the initiator.

A.1. U is the Initiator

The reverse flow can be applied when U implements a CoAP server, but acts as an EDHOC Initiator. In this case, U awaits for a CoAP request to be sent from V, which will act as a trigger message to start the EDHOC handshake with ELA. Next, U replies with an EDHOC message_1, thus executing the protocol normally.

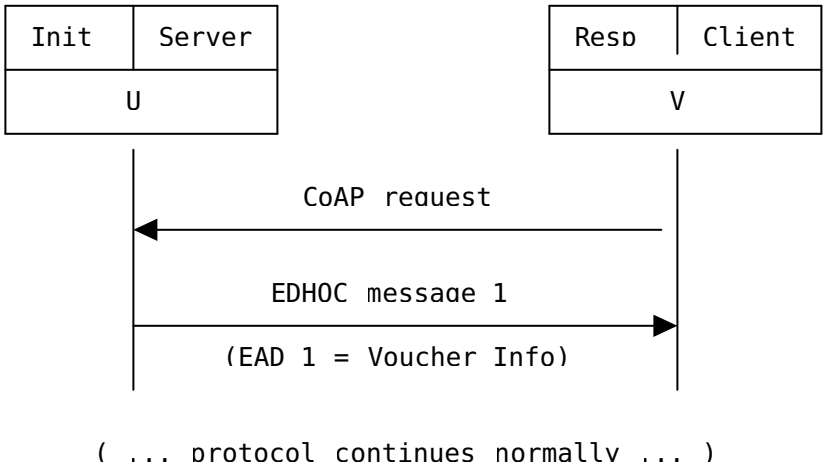

Figure 6: ELA with EDHOC reverse mesasge flow when U is initiator.

One use case is to perform ELA over Bluetooth Low Energy, as discussed in [I-D.amsuess-core-coap-over-gatt].

A.2. U is the Responder

The reverse flow can also be used when U implements a CoAP client, but acts as a Responder, as illustrated in Figure 7. The main changes in this case are:

- Instead of sending EDHOC message_1, U sends an initial trigger packet to V, e.g., a CoAP request, which then initiates the handshake by replying with an EDHOC message_1.

- The Voucher_Info and Voucher structs are sent over EAD_2 and EAD_3, respectively (instead of over EAD_1 and EAD_2).

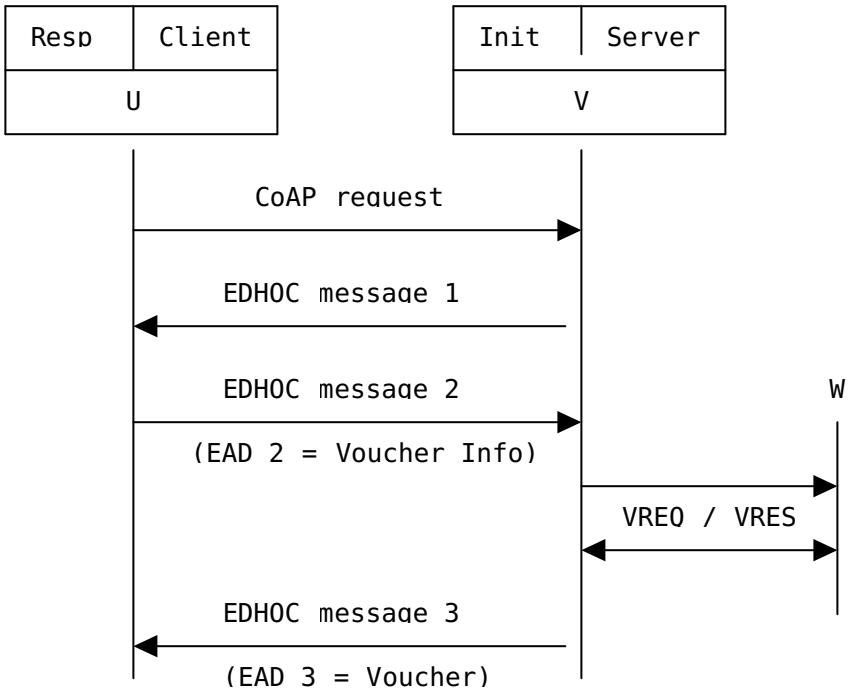

Figure 7: ELA with EDHOC reverse mesasge flow when U is responder.

Appendix B. Use with Constrained Join Protocol (CoJP)

This section outlines how ELA is used for network enrollment and parameter provisioning. An IEEE 802.15.4 network is used as an example of how a new device (U) can be enrolled into the domain managed by the domain authenticator (V).

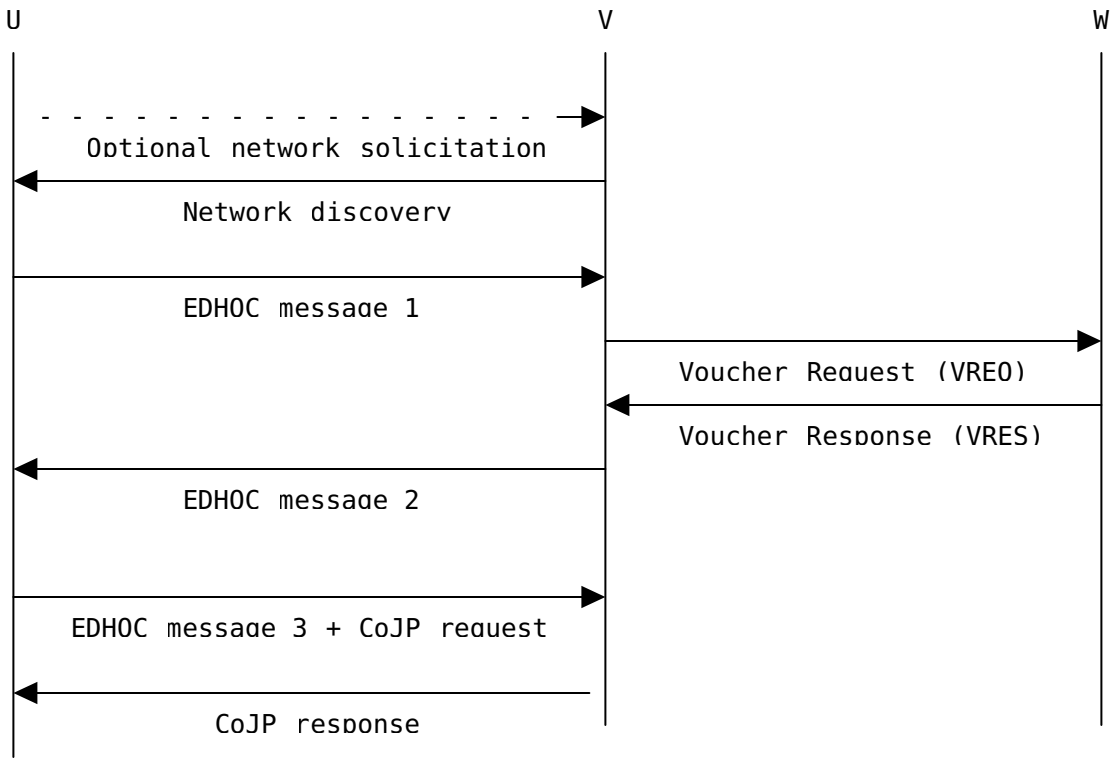

Figure 8: Use of draft-ietf-lake-authz with CoJP.

B.1. Network Discovery

When a device first boots, it needs to discover the network it attempts to join. The network discovery procedure is defined by the link-layer technology in use. In case of Time-slotted Channel Hopping (TSCH) networks, a mode of [IEEE802.15.4], the device scans the radio channels for Enhanced Beacon (EB) frames, a procedure known as passive scan. EBs carry the information about the network, and particularly the network identifier. Based on the EB, the network identifier, the information pre-configured into the device, the device makes the decision on whether it should join the network advertised by the received EB frame. This process is described in Section 4.1 of [RFC9031]. In case of other, non-TSCH modes of IEEE 802.15.4, it is possible to use the active scan procedure and send solicitation frames. These solicitation frames trigger the nearest network coordinator to respond by emitting a beacon frame. The network coordinator emitting beacons may be multiple link-layer hops away from the domain authenticator (V), in which case it plays the role of a Join Proxy (see [RFC9031]). The Join Proxy does not participate in the protocol and acts as a transparent router between the device and the domain authenticator. For simplicity, Figure 8 illustrates the case when the device and the domain authenticator are a single hop away and can communicate directly.

B.2. The Enrollment Protocol with Parameter Provisioning

B.2.1. Flight 1

Once the device has discovered the network it wants to join, it constructs EDHOC message_1, as described in Section 4.5. The device SHALL map the message to a CoAP request:

- The request method is POST.
- The type is Confirmable (CON).
- The Proxy-Scheme option is set to "coap".
- The Uri-Host option is set to "lake-authz.arpa". This is an anycast type of identifier of the domain authenticator (V) that is resolved to its IPv6 address by the Join Proxy.
- By means of Uri-Path options, the Uri-Path is set to ".well-known/edhoc".
- The payload is the (true, EDHOC message_1) CBOR sequence, where EDHOC message_1 is constructed as defined in Section 4.5.

B.2.2. Flight 2

The domain authenticator receives message_1 and processes it as described in Section 4.5. The message triggers the exchange with the enrollment server, as described in Section 4.6. If the exchange between V and W completes successfully, the domain authenticator prepares EDHOC message_2, as described in Section 4.5. The authenticator SHALL map the message to a CoAP response:

- The response code is 2.04 Changed.
- The payload is the EDHOC message_2, as defined in Section 4.5.

B.2.3. Flight 3

The device receives EDHOC message_2 and processes it as described in Section 4.5. Upon successful processing of message_2, the device prepares flight 3, which is an OSCORE-protected CoJP request containing an EDHOC message_3, as described in [I-D.ietf-core-oscore-edhoc]. EDHOC message_3 is prepared as described in Section 4.5. The OSCORE-protected payload is the CoJP Join Request object specified in Section 8.4.1 of [RFC9031]. OSCORE protection leverages the OSCORE Security Context derived from the EDHOC session, as specified in Appendix A of [RFC9528]. To that end, [I-D.ietf-core-oscore-edhoc] specifies that the Sender ID of the client (device) must be set to the connection identifier selected by the domain authenticator, C_R. OSCORE includes the Sender ID as the kid in the OSCORE option. The network identifier in the CoJP Join Request object is set to the network identifier obtained from the

network discovery phase. In case of IEEE 802.15.4 networks, this is the PAN ID.

The device SHALL map the message to a CoAP request:

- *The request method is POST.
- *The type is Confirmable (CON).
- *The Proxy-Scheme option is set to "coap".
- *The Uri-Host option is set to "lake-authz.arpa".
- *The Uri-Path option is set to ".well-known/edhoc".
- *The EDHOC option [I-D.ietf-core-oscore-edhoc] is set and is empty.
- *The payload is prepared as described in Section 3.2 of [I-D.ietf-core-oscore-edhoc], with EDHOC message_3 and the CoJP Join Request object as the OSCORE-protected payload.

Note that the OSCORE Sender IDs are derived from the connection identifiers of the EDHOC session. This is in contrast with [RFC9031] where ID Context of the OSCORE Security Context is set to the device identifier (pledge identifier). Since the device identity is exchanged during the EDHOC session, and the certificate of the device is communicated to the authenticator as part of the Voucher Response message, there is no need to transport the device identity in OSCORE messages. The authenticator playing the role of the [RFC9031] JRC obtains the device identity from the execution of the authorization protocol.

B.2.4. Flight 4

Flight 4 is the OSCORE response carrying CoJP response message. The message is processed as specified in Section 8.4.2 of [RFC9031].

Appendix C. Example Advertisement Strategies

This appendix presents three example strategies that can be used to advertise the presence of a V. It includes sending V_INFO in network beacons, as part of EAD_1 in reverse message flow, or as part of a periodic CoAP multicast packet. It also presents the advantages, costs, and security impacts of each strategy.

C.1. V_INFO in network beacons

PR editor's note: this is approach A1

This approach allows carrying V_INFO in beacons sent over the network layer, as shown in Figure 9. It requires that the network layer offers a mechanism to configure its beacon packets. Depending on the

network type, a solicitation packet may also be needed, as is the case of non-beaconed IEEE 802.15.4 and BLE with GATT.

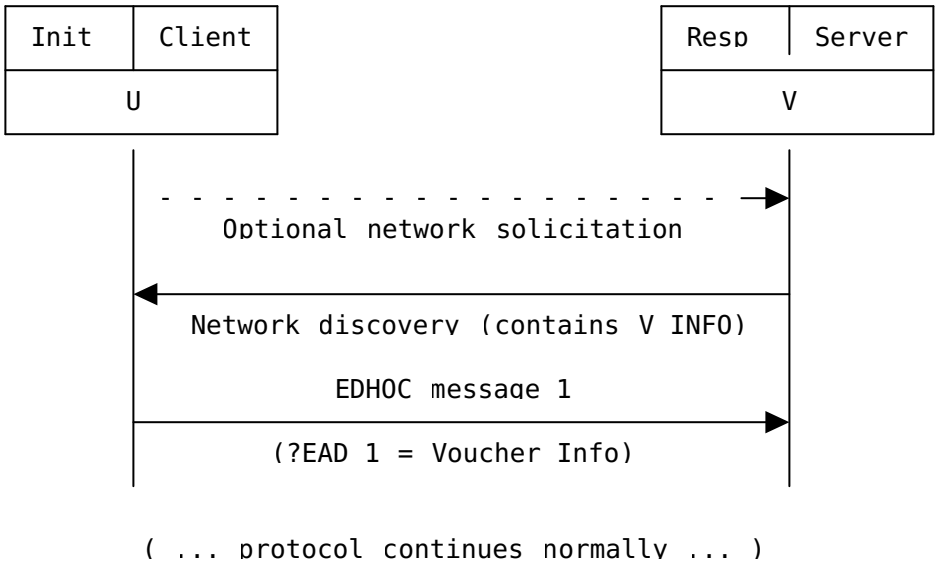

Figure 9: Advertising ELA using V_INFO in network-layer beacons.

This strategy can be used, for example, in IEEE 802.15.4, where an Enhanced Beacon [IEEE802.15.4] can be used to transmit V_INFO. Specifically, a new information element for carrying V_INFO can be defined according to [RFC8137].

This approach has the advantage of requiring minimal changes to the default protocol as presented in Section 4.1, i.e., no reverse flow. It requires, however, some profiling of the lower layer beacons.

C.2. V_INFO in EAD_1

PR editor's note: this is approach A2

ELA with EDHOC in the reverse flow allows implementing advertising where U first sends a trigger packet, in the format of a CoAP request that is broadcasted to the newtork. When a suitable V receives the solicitation, if it implements ELA, it should respond with an EDHOC message_1 whose EAD_1 has label TBD1 and value V_INFO (see Section Section 5).

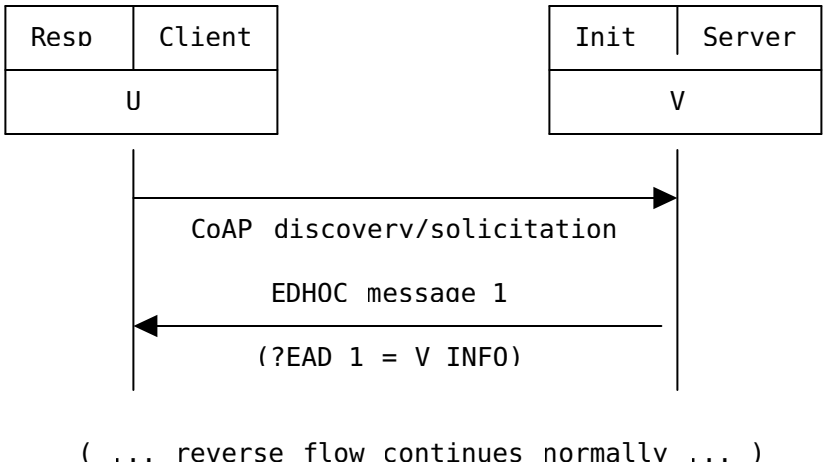

Figure 10: Advertising ELA using V_INFO in EAD_1, eploying the EDHOC reverse flow with U as responder.

Note that V will only reply if it supports ELA, therefore in this strategy there is no need to transport ELA_ID. V_INFO can then be structured to contain only the optional domain identifier:

```
V_INFO = (
  ?DOMAIN_ID: bstr,
)
```

This approach enables a simple filtering mechanism, where only V's that support ELA will reply. It also encrypts Voucher_Info (as part of EAD_2), wehereas it is sent in the clear in the original flow. In addition, it may not require layer-two profiling (in case the network allows transporting data before authorization). Finally, note that the reverse flow with U as Responder protects the identity of V (instead of U's as in the forward flow).

C.3. V_INFO in a CoAP Multicast Packet

PR editor's note: this is approach A3

In this approach, V periodically multicasts a CoAP packet containing V_INFO, see Figure 11. Upon receiving one or more CoAP messages and processing V_INFO, U can decide whether or not to initiate the ELA protocol with a given V. Next, the application can either keep U acting as a server, and thus employ the EDHOC reverse flow, or implement a CoAP client and use the forward flow.

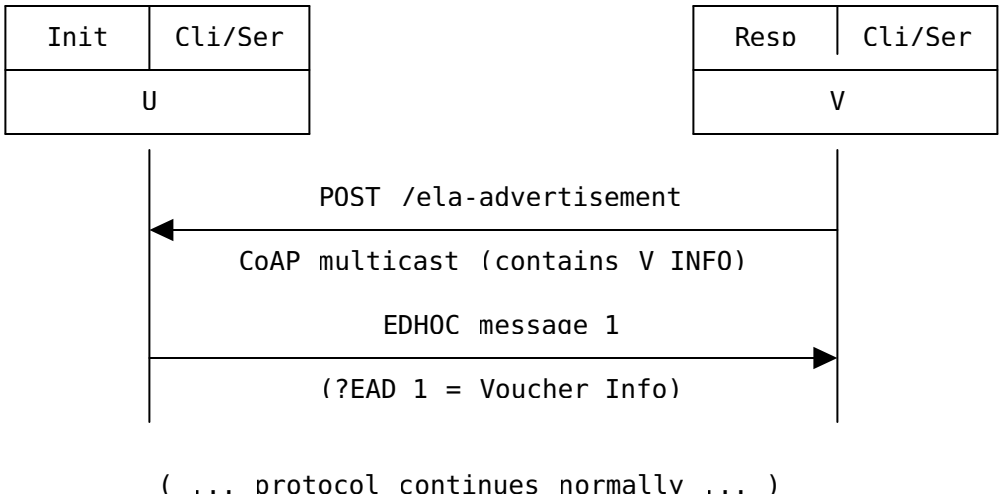

Figure 11: Advertising ELA using the network layer.

The V_INFO structure is sent as part of the CoAP payload. It is encoded as a CBOR sequence:

```
V_INFO = (
  ?DOMAIN_ID: bstr,
)
```

One advantage of this approach is that, since U is the initiator, it's identity is protected in the context of the EDHOC handshake. On the other hand, the periodic multicast may have resource usage impacts in the network.

Appendix D. Examples

This section presents high level examples of the protocol execution.

Note: the examples below include samples of access policies used by W. These are provided for the sake of completeness only, since the authorization mechanism used by W is out of scope in this document.

D.1. Minimal

This is a simple example that demonstrates a successful execution of ELA.

Premises:

*device u1 has ID_U = key id = 14

*the access policy in W specifies, via a list of ID_U, that device u1 can enroll via any domain authenticator, i.e., the list contains ID_U = 14. In this case, the policy only specifies a

restriction in terms of U, effectively allowing enrollment via any V.

Execution:

1. device u1 discovers a gateway (v1) and tries to enroll

2. gateway v1 identifies the zero-touch join attempt by checking that the label of EAD_1 = TBD1, and prepares a Voucher Request using the information contained in the value of EAD_1

3. upon receiving the request, W obtains ID_U = 14, authorizes the access, and replies with Voucher Response

D.2. Wrong gateway

In this example, a device u1 tries to enroll a domain via gateway v1, but W denies the request because the pairing (u1, v1) is not configured in its access policies.

This example also illustrates how the REJECT_INFO field of the EDHOC error Access Denied could be used, in this case to suggest that the device should select another gateway for the join procedure.

Premises:

* devices and gateways communicate via Bluetooth Low Energy (BLE), therefore their network identifiers are MAC addresses (EUI-48)

* device u1 has ID_U = key id = 14

* there are 3 gateways in the radio range of u1:

  - v1 with MAC address = A2-A1-88-EE-97-75

  - v2 with MAC address = 28-0F-70-84-51-E4

  - v3 with MAC address = 39-63-C9-D0-5C-62

* the access policy in W specifies, via a mapping of shape (ID_U; MAC1, MAC2, ...) that device u1 can only join via gateway v3, i.e., the mapping is: (14; 39-63-C9-D0-5C-62)

* W is able to map the PoP key of the gateways to their respective MAC addresses

Execution:

1. device u1 tries to join via gateway v1, which forwards the request to W

2. W determines that MAC address A2-A1-88-EE-97-75 is not in the access policy mapping, and replies with an error. The

error_content has REJECT_TYPE = 1, and the plaintext OPAQUE_INFO (used to compute the encrypted REJECT_INFO) specifies a list of suggested gateways = [h'3963C9D05C62']. The single element in the list is the 6-byte MAC address of v3, serialized as a bstr.

3. gateway v1 assembles an EDHOC error "Access Denied" with error_content, and sends it to u1

4. device u1 processes the error, decrypts REJECT_INFO, and retries the protocol via gateway v3

Acknowledgments

The authors sincerely thank Aurelio Schellenbaum for his contribution in the initial phase of this work, and Marco Tiloca for extensively reviewing the document.

Authors' Addresses

Göran Selander
Ericsson AB
Sweden

Email: goran.selander@ericsson.com

John Preuß Mattsson
Ericsson AB
Sweden

Email: john.mattsson@ericsson.com

Mališa Vučinić
INRIA
France

Email: malisa.vucinic@inria.fr

Geovane Fedrecheski
INRIA
France

Email: geovane.fedrecheski@inria.fr

Michael Richardson
Sandelman Software Works
Canada

Email: mcr+ietf@sandelman.ca