LAKE Working Group
Internet-Draft
Intended status: Standards Track
Expires: 23 April 2026

M. Tiloca
R. H旦glund
RISE AB

20 October 2025

Coordinating the Use of Application Profiles for Ephemeral Diffie-Hellman Over COSE (EDHOC) draft-ietf-lake-app-profiles-03

Abstract

The lightweight authenticated key exchange protocol Ephemeral Diffie-Hellman Over COSE (EDHOC) requires certain parameters to be agreed out-of-band, in order to ensure its successful completion. To this end, application profiles specify the intended use of EDHOC to allow for the relevant processing and verifications to be made. In order to ensure the applicability of such parameters and information beyond transport- or setup-specific scenarios, this document defines a canonical, CBOR-based representation that can be used to describe, distribute, and store EDHOC application profiles. Furthermore, In order to facilitate interoperability between EDHOC implementations and support EDHOC extensibility for additional integrations, this document defines a number of means to coordinate the use of EDHOC application profiles. Finally, this document defines a set of well-known EDHOC application profiles.

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://github.com/lake-wg/app-profiles.

Status of This Memo

Table of Contents

1. Introduction

Ephemeral Diffie-Hellman Over COSE (EDHOC) [RFC9528] is a lightweight authenticated key exchange protocol, especially intended for use in constrained scenarios. A main use case for EDHOC is the establishment of a Security Context for Object Security for Constrained RESTful Environments (OSCORE) [RFC8613].

In order to successfully run EDHOC, the two peers acting as Initiator and Responder have to agree on certain parameters. Some of those are in-band and communicated through the protocol execution, during which a few of them may even be negotiated. However, other parameters have to be known out-of-band, before running the EDHOC protocol.

As discussed in Section 3.9 of [RFC9528], applications can use EDHOC application profiles, which specify the intended usage of EDHOC to allow for the relevant processing and verifications to be made. In particular, an EDHOC application profile may include both in-band and out-of-band parameters.

In order to ensure the applicability of such parameters and information beyond transport- or setup-specific scenarios, this document also defines the EDHOC_Application_Profile object, i.e., a

canonical, CBOR-based representation that can be used to describe, distribute, and store EDHOC application profiles as CBOR data items (see Section 2). The defined representation is transport- and setup-independent, and avoids the need to reinvent an encoding for the available options to run the EDHOC protocol or the selection logic to apply on those.

The CBOR-based representation of an EDHOC application profile can be, for example: retrieved as a result of a discovery process; or retrieved/provided during the retrieval/provisioning of an EDHOC peer's public authentication credential; or obtained during the execution of a device on-boarding/registration workflow.

Furthermore, in order to facilitate interoperability between EDHOC implementations and to support EDHOC extensibility for additional integrations (e.g., of external security applications, handling of authentication credentials, and message transports), this document defines a number of means to coordinate the use of EDHOC application profiles, that is:

* The new IANA registry "EDHOC Application Profiles" defined in Section 10.8, where to register integer identifiers of EDHOC application profiles to use as corresponding Profile IDs.

* The new parameter "ed-prof" defined in Section 3.1. This parameter is employed to specify an EDHOC application profile identified by its Profile ID and can be used as target attribute in a web link [RFC8288] to an EDHOC resource, or as filter criterion in a discovery request to discover EDHOC resources.

  For instance, the target attribute can be used in a CoRE link-format document [RFC6690] describing EDHOC resources at a server, when EDHOC is transferred over the Constrained Application Protocol (CoAP) [RFC7252] (see Appendix A.2 of [RFC9528] as well as [RFC9668]).

* The new parameter "app_prof" defined in Section 3.2 for the EDHOC_Information object specified in [I-D.ietf-ace-edhoc-oscore-profile]. This parameter is employed to specify a set of EDHOC application profiles, each identified by its Profile ID.

  For instance, the parameter can be used in the EDHOC and OSCORE profile [I-D.ietf-ace-edhoc-oscore-profile] of the ACE framework for authentication and authorization in constrained environments (ACE) [RFC9200], in order to indicate the EDHOC application profiles supported by an ACE resource server.

This parameter is also used in the EDHOC_Application_Profile object defined in this document, in order to encode the Profile ID of the EDHOC application profile described by an instance of that object.

* Additional parameters that provide information about an EDHOC application profile. These parameters correspond to elements of the EDHOC_Information object and are to be used as target attributes in a web link to an EDHOC resource, or as filter criteria in a discovery request to discover EDHOC resources (see Section 4).

* A new EDHOC External Authorization Data (EAD) item (see Section 5.1) and a new error code for the EDHOC error message (see Section 5.2). When running EDHOC, a peer can use those in order to advertise the EDHOC application profiles that it supports to the other peer.

* The use of SVCB Resource Records (RR) [RFC9460][RFC9461] to advertise the support for EDHOC and for EDHOC application profiles of a given server (see Section 6).

Finally, this document defines a set of well-known EDHOC application profiles (see Section 7). These application profiles are meant to reflect what is most common and expected to be supported by EDHOC peers, while they are not to be intended as "default" application profiles or as a deviation from what is mandatory to support for EDHOC peers (see Section 8 of [RFC9528]). On the other hand, they provide implementers and users with a quick overview of the several available options to run the EDHOC protocol and of their most expected combinations.

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.

The reader is expected to be familiar with terms and concepts defined in EDHOC [RFC9528] and with the use of EDHOC with CoAP [RFC7252] and OSCORE [RFC8613] defined in [RFC9668].

Concise Binary Object Representation (CBOR) [RFC8949] and Concise Data Definition Language (CDDL) [RFC8610] are used in this document. CDDL predefined type names, especially bstr for CBOR byte strings and tstr for CBOR text strings, are used extensively in this document.

CBOR data items are represented using the CBOR extended diagnostic notation as defined in Section 8 of [RFC8949] and Appendix G of [RFC8610] ("diagnostic notation"). Diagnostic notation comments are used to provide a textual representation of the parameters' keys and values.

In the CBOR diagnostic notation used in this document, constructs of the form e'SOME_NAME' are replaced by the value assigned to SOME_NAME in the CDDL model shown in Figure 7 of Appendix A. For example, {e'methods' : [0, 1, 2, 3], e'cipher_suites': 3} stands for {1 : [0, 1, 2, 3], 2 : 3}.

Note to RFC Editor: Please delete the paragraph immediately preceding this note. Also, in the CBOR diagnostic notation used in this document, please replace the constructs of the form e'SOME_NAME' with the value assigned to SOME_NAME in the CDDL model shown in Figure 7 of Appendix A. Finally, please delete this note.

2. EDHOC_Application_Profile

This section defines the EDHOC_Application_Profile object, which can be used as a canonical representation of EDHOC application profiles for their description, distribution, and storage.

An EDHOC_Application_Profile object is encoded as a CBOR map [RFC8949]. All elements that can be included in the EDHOC_Application_Profile object are elements that can be included in the CBOR-encoded EDHOC_Information object specified in Section 3.4 of [I-D.ietf-ace-edhoc-oscore-profile]. In particular, they use the same CBOR abbreviations from the 'CBOR label' column of the IANA registry "EDHOC Information" defined in [I-D.ietf-ace-edhoc-oscore-profile].

The CBOR map encoding an EDHOC_Application_Profile object MUST include the element "app_prof" defined in Section 3.2 of this document, as well as the elements "methods" and "cred_types" defined in Section 3.4 of [I-D.ietf-ace-edhoc-oscore-profile].

The value of the element "app_prof" is the unique identifier of the EDHOC application profile described by the instance of the EDHOC_Application_Profile object in question. The identifier is taken from the 'Profile ID' column of the "EDHOC Application Profiles" registry defined in this document and encoded as a CBOR integer.

The CBOR map MUST NOT include the following elements: "session_id", "uri_path", "initiator", "responder", and "trust_anchors". Also, the CBOR map MUST NOT include the element "exporter_out_len" defined in

Section 5.1.2 of this document. A consumer MUST ignore those elements if they are included in the EDHOC_Application_Profile object.

The CBOR map MAY include other elements.

Furthermore, consistent with Sections 8 and A.1 of [RFC9528] and with Section 5.4 of [RFC8613], the following applies:

* If the element "cipher_suites" is not present in the CBOR map, this indicates that the EDHOC application profile uses the EDHOC cipher suites 2 and 3, and possibly other cipher suites.

* If the element "id_cred_types" is not present in the CBOR map, this indicates that the EDHOC application profile uses "kid" as type of authentication credential identifiers for EDHOC, and possibly other types of authentication credential identifiers.

* The absence of any other elements in the CBOR map MUST NOT result in assuming any value.

If an element is present in the CBOR map and the corresponding entry in the IANA registry "EDHOC Information" specifies "NP" (non-prescriptive) in the 'Type' column and "True or False" in the 'CBOR type' column, then the following applies. An EDHOC peer that adheres to the EDHOC application profile in question is required or not to support the property or feature of EDHOC associated with the element in the CBOR map, if that element encodes the CBOR simple value true (0xf5) or false (0xf4), respectively. For example, the presence of the parameter "comb_req" denotes whether EDHOC peers adhering to the EDHOC application profile have to support the EDHOC + OSCORE combined request defined in [RFC9668], or instead do not have to but might if they are willing to.

If an element present in the CBOR map specifies an information that is intrinsically a set of one or more co-existing alternatives, then all the specified alternatives apply for the EDHOC application profile in question. For example, the element "cipher_suites" with value the CBOR array [0, 2] means that, in order to adhere to the EDHOC application profile in question, an EDHOC peer has to implement both the EDHOC cipher suites 0 and 2, because either of them can be used by another EDHOC peer also adhering to the same EDHOC application profile.

The CDDL grammar describing the EDHOC_Application_Profile object is:

```
EDHOC_Application_Profile = {
      1 => int / array,    ; methods
      6 => int / array,    ; cred_types
     23 => int,            ; app_prof
   * int / tstr => any
}
```

Figure 1: CDDL Definition of the EDHOC_Application_Profile object

3. Identifying EDHOC Application Profiles by Profile ID

This document introduces the concept of Profile IDs, i.e., integer values that uniquely identify EDHOC application profiles, for which an IANA registry is defined in Section 10.8.

This section defines two parameters to convey such Profile IDs, i.e.:

* The parameter "ed-prof" for web linking [RFC8288] (see Section 3.1).

* The parameter "app_prof" of the EDHOC_Information object specified in [I-D.ietf-ace-edhoc-oscore-profile] (see Section 3.2).

  As defined in Section 2, Profile IDs are also conveyed by the parameter "app_prof" in the EDHOC_Application_Profile object, in order to identify the EDHOC application profile described by a given instance of that object.

As defined later in this document, Profile IDs can be used to identify EDHOC application profiles also:

* Within certain EDHOC messages sent during an EDHOC session by a peer that supports such EDHOC application profiles (see Section 5).

* When using SVCB Resource Records (RR) [RFC9460][RFC9461] to advertise the support for EDHOC and for EDHOC application profiles of a given server (see Section 6).

3.1. In Web Linking

Section 6 of [RFC9668] defines a number of target attributes that can be used in a web link [RFC8288] with resource type "core.edhoc" (see Section 10.10 of [RFC9528]). This is the case, e.g., when using a CoRE link-format document [RFC6690] describing EDHOC resources at a server, when EDHOC is transferred over CoAP [RFC7252] as defined in Appendix A.2 of [RFC9528]. This allows a client to obtain relevant information about the EDHOC application profile(s) to be used with a

certain EDHOC resource.

In the same spirit, this section defines the following additional parameter, which can be optionally specified as a target attribute with the same name in the link to the respective EDHOC resource, or among the filter criteria in a discovery request from a client.

* 'ed-prof', specifying an EDHOC application profile supported by the server. This parameter MUST specify a single value, which is taken from the 'Profile ID' column of the "EDHOC Application Profiles" registry defined in Section 10.8 of this document. This parameter MAY occur multiple times, with each occurrence specifying an EDHOC application profile.

When specifying the parameter 'ed-prof' in a link to an EDHOC resource, the target attribute rt="core.edhoc" MUST be included.

If a link to an EDHOC resource includes occurrences of the target attribute 'ed-prof', then the following applies.

* The link MUST NOT include other target attributes that provide information about an EDHOC application profile (see, e.g., Section 6 of [RFC9668] and Section 4 of this document), with the exception of the target attribute 'ed-ead' that MAY be included.

  The recipient MUST ignore other target attributes that provide information about an EDHOC application profile, with the exception of the target attribute 'ed-ead'.

* If the link includes occurrences of the target attribute 'ed-ead', the link provides the following information: when using the target EDHOC resource as per the EDHOC application profile indicated by any occurrence of the target attribute 'ed-prof', the server supports the External Authorization Data (EAD) items that are specified in the definition of that EDHOC application profile, as well as the EAD items indicated by the occurrences of the target attribute 'ed-ead'.

The example in Figure 2 shows how a CoAP client discovers two EDHOC resources at a CoAP server, and obtains information about the application profile corresponding to each of those resources. The CoRE Link Format notation from Section 5 of [RFC6690] is used.

The example assumes the existence of an EDHOC application profile identified by the integer Profile ID 500, which is supported by the EDHOC resource at /edhoc-alt and whose definition includes the support for the EAD items with EAD label 111 and 222.

Therefore, the link to the EDHOC resource at /edhoc-alt indicates that, when using that EDHOC resource as per the EDHOC application profile with Profile ID 500, the server supports the EAD items with EAD label 111, 222, and 333.

```
REQ: GET /.well-known/core

RES: 2.05 Content
    </sensors/temp>;osc,
    </sensors/light>;if=sensor,
    </.well-known/edhoc>;rt=core.edhoc;ed-csuite=0;ed-csuite=2;
        ed-method=0;ed-cred-t=1;ed-cred-t=3;ed-idcred-t=4;
        ed-i;ed-r;ed-comb-req,
    </edhoc-alt>;rt=core.edhoc;ed-prof=500;ed-ead=333
```

Figure 2: The Web Link.

3.2. In the EDHOC_Information Object

Section 3.4 of [I-D.ietf-ace-edhoc-oscore-profile] defines the EDHOC_Information object and an initial set of its parameters. The object can be used to convey information that guides two peers about executing the EDHOC protocol.

This document defines the new parameter "app_prof" of the EDHOC_Information object. The parameter is of type non-prescriptive (NP) and is summarized in Table 1. The parameter is specified further below.

Name	CBOR label	CBOR type	Registry	Description	Type
app_prof	23	int or array	EDHOC Application Profiles Registry	Set of supported EDHOC Application Profiles	NP

Table 1: EDHOC_Information Parameter "app_prof"

* app_prof: This parameter specifies a set of supported EDHOC application profiles, identified by their Profile ID. If the set is composed of a single EDHOC application profile, its Profile ID is encoded as an integer. Otherwise, the set is encoded as an array of integers, where each array element encodes one Profile ID. In JSON, the "app_prof" value is an integer or an array of integers. In CBOR, "app_prof" is an integer or an array of

integers, and has label 23. The integer values are taken from the 'Profile ID' column of the "EDHOC Application Profiles" registry defined in Section 10.8 of this document.

3.2.1. Use in the EDHOC and OSCORE Profile of the ACE Framework

Section 3 of [I-D.ietf-ace-edhoc-oscore-profile] defines how the EDHOC_Information object can be used within the workflow of the EDHOC and OSCORE transport profile of the ACE framework for authentication and authorization in constrained environments (ACE) [RFC9200].

In particular, the AS-to-C Access Token Response includes the parameter "edhoc_info", with value an EDHOC_Information object. This allows the ACE authorization server (AS) to provide the ACE client (C) with information about how to run the EDHOC protocol with the ACE resource server (RS) for which the access token is issued.

Similarly, the access token includes the corresponding claim "edhoc_info", with value an EDHOC_Information object. This allows the AS to provide the ACE RS with information about how to run the EDHOC protocol with the ACE client, according to the issued access token.

In turn, the EDHOC_Information object can include the parameter "app_prof" defined in this document. This parameter indicates a set of EDHOC application profiles associated with the EDHOC resource to use at the RS, which is either implied or specified by the parameter "uri_path" within the same EDHOC_Information object.

If the EDHOC_Information object specified as the value of the parameter/claim "edhoc_info" includes the "app_prof" parameter, then the following applies.

* In addition to the "app_prof" parameter, the object MUST NOT include other parameters, with the exception of the following parameters that MAY be included:

  - The parameter "eads".

  - Any parameter that is not allowed in the EDHOC_Application_Profile object defined in Section 2, unless its inclusion in the EDHOC_Information object is explicitly forbidden by the parameter's definition.

For example, the parameter "session_id" is not allowed in the EDHOC_Application_Profile object (see Section 2) and thus can be included in the EDHOC_Information object, where in fact it has to be present (see Sections 3.3 and 3.3.1 of [I-D.ietf-ace-edhoc-oscore-profile]).

C and RS MUST ignore other parameters that are not admitted if they are present in the EDHOC_Information object.

* The object might provide an information that corresponds to an EDHOC_Information prescriptive parameter (see Section 3.4 of [I-D.ietf-ace-edhoc-oscore-profile]), e.g., "message_4" or "max_msgsize". The type of a parameter is indicated in the 'Type' column of the corresponding entry in the IANA registry "EDHOC Information" (see [I-D.ietf-ace-edhoc-oscore-profile]).

  If the object specifies such an information multiple times, then each occurrence of that information MUST convey exactly the same content. This MUST take into account prescriptive parameters that are included: i) as elements of the EDHOC_Information object; or ii) as elements of an EDHOC_Application_Profile object (see Section 2) encoding an EDHOC application profile, which is identified by its Profile ID specified in the "app_prof" parameter of the EDHOC_Information object.

  A consumer MUST treat as malformed an EDHOC_Information object that does not comply with the restriction above.

* If the EDHOC_Information object specified in the parameter "edhoc_info" of the AS-to-C Access Token Response includes the parameter "eads", then the following applies.

  When using the target EDHOC resource as per any EDHOC application profile indicated by the parameter "app_prof", the ACE RS for which the access token is issued supports the EAD items that are specified in the definition of that EDHOC application profile, as well as the EAD items indicated by the parameter "eads".

* If the EDHOC_Information object specified in the claim "edhoc_info" of the access token includes the parameter "eads", then the following applies.

  When using the target EDHOC resource as per any EDHOC application profile indicated by the parameter "app_prof", the ACE client to which the access token is issued supports the EAD items that are specified in the definition of that EDHOC application profile, as well as the EAD items indicated by the parameter "eads".

4. Additional Parameters for Web Linking

Building on what is defined and prescribed in Section 6 of [RFC9668], this section defines additional parameters for web linking [RFC8288], which can be used to obtain relevant pieces of information from the EDHOC application profile associated with an EDHOC resource.

These parameters can be optionally specified as target attributes with the same name in a link with resource type "core.edhoc" (see Section 10.10 of [RFC9528]) targeting an EDHOC resource, or as filter criteria in a discovery request from a client.

When specifying any of the parameters defined below in a link to an EDHOC resource, the target attribute rt="core.edhoc" MUST be included.

* ’ed-max-msgsize’, specifying the admitted maximum size of EDHOC messages in bytes. This parameter MUST specify a single unsigned integer value.

* ’ed-coap-ct’, specifying that CoAP messages have to include the CoAP Content-Format Option with value 64 (application/edhoc+cbor-seq) or 65 (application/cid-edhoc+cbor-seq) as appropriate, when the message payload includes exclusively an EDHOC message possibly prepended by an EDHOC connection identifier (see Sections 3.4.1 and A.2 of [RFC9528]). A value MUST NOT be given to this parameter and any present value MUST be ignored by the recipient.

* ’ed-epid-t’, specifying a type of endpoint identity for EDHOC supported by the server. This parameter MUST specify a single value, which is taken from the ’CBOR Label’ column of the "EDHOC Endpoint Identity Types" registry defined in [I-D.ietf-ace-edhoc-oscore-profile]. This parameter MAY occur multiple times, with each occurrence specifying a type of endpoint identity for EDHOC.

* ’ed-tp’, specifying a means for transporting EDHOC messages supported by the server. This parameter MUST specify a single value, which is taken from the ’Transport ID’ column of the "EDHOC Transports" registry defined in [I-D.ietf-ace-edhoc-oscore-profile]. This parameter MAY occur multiple times, with each occurrence specifying a means for transporting EDHOC messages.

* ’ed-ta-edcred-uuid’, specifying the identifier of a trust anchor supported by the server for verifying authentication credentials of other EDHOC peers, as a UUID [RFC9562]. This parameter MUST specify a single value, which is the UUID in its string format

(see Section 4 of [RFC9562]). This parameter MAY occur multiple times, with each occurrence specifying one trust anchor identifier.

* 'ed-ta-edcred-kid', specifying the identifier of a trust anchor supported by the server for verifying authentication credentials of other EDHOC peers, as a binary key identifier. This parameter MUST specify a single value, which is the base64url-encoded text string of the binary representation of the key identifier. This parameter MAY occur multiple times, with each occurrence specifying one trust anchor identifier.

* 'ed-ta-edcred-c5t', specifying the identifier of a trust anchor supported by the server for verifying authentication credentials of other EDHOC peers, as a hash of a C509 certificate [I-D.ietf-cose-cbor-encoded-cert]. This parameter MUST specify a single value, which is the base64url-encoded text string of the binary representation of the certificate hash encoded as a COSE_CertHash [RFC9360]. This parameter MAY occur multiple times, with each occurrence specifying one trust anchor identifier.

* 'ed-ta-edcred-c5u', specifying the identifier of a trust anchor supported by the server for verifying authentication credentials of other EDHOC peers, as a URI [RFC3986] pointing to a C509 certificate [I-D.ietf-cose-cbor-encoded-cert]. This parameter MUST specify a single value, which is the URI pointing to the certificate. This parameter MAY occur multiple times, with each occurrence specifying one trust anchor identifier.

* 'ed-ta-edcred-x5t', specifying the identifier of a trust anchor supported by the server for verifying authentication credentials of other EDHOC peers, as a hash of an X.509 certificate [RFC5280]. This parameter MUST specify a single value, which is the base64url-encoded text string of the binary representation of the certificate hash encoded as a COSE_CertHash [RFC9360]. This parameter MAY occur multiple times, with each occurrence specifying one trust anchor identifier.

* 'ed-ta-edcred-x5u', specifying the identifier of a trust anchor supported by the server for verifying authentication credentials of other EDHOC peers, as a URI [RFC3986] pointing to an X.509 certificate [RFC5280]. This parameter MUST specify a single value, which is the URI pointing to the certificate. This parameter MAY occur multiple times, with each occurrence specifying one trust anchor identifier.

5. Advertising Supported EDHOC Application Profiles during an EDHOC Session

The rest of this section defines means that an EDHOC peer can use in order to advertise the EDHOC application profiles that it supports to another EDHOC peer, when running EDHOC with that other peer.

Such means are an EDHOC EAD item (see Section 5.1) and an error code for the EDHOC error message (see Section 5.2).

5.1. In EDHOC Message 1 and Message 2

This section defines the EDHOC EAD item "Supported EDHOC application profiles", which is registered in Section 10.5 of this document.

The EAD item MAY be included:

* In the EAD_1 field of EDHOC message_1, in order to specify EDHOC application profiles supported by the Initiator.

* In the EAD_2 field of EDHOC message_2, in order to specify EDHOC application profiles supported by the Responder.

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 NOT occur more than once in the EAD fields of EDHOC message_1 or message_2. The recipient peer MUST abort the EDHOC session and MUST reply with an EDHOC error message with error code (ERR_CODE) 1, if the EAD item occurs multiple times in the EAD fields of EDHOC message_1 or message_2.

The EAD item MUST NOT be included in the EAD fields of EDHOC message_3 or message_4. In case the recipient peer supports the EAD item, the recipient peer MUST silently ignore the EAD item if this is included in the EAD fields of EDHOC message_3 or message_4.

The EAD item MUST specify an ead_value, as a CBOR byte string with value the binary representation of a CBOR sequence [RFC8742]. In particular:

* When the EAD item is included in the EAD_1 field, the value of the CBOR byte string is the binary representation of the CBOR sequence OUTER_SEQ. In turn, OUTER_SEQ is composed of the following elements:

- The CBOR data item reply_flag, which MAY be present. If present, it MUST encode the CBOR simple value true (0xf5) or false (0xf4). The semantics of this element is as follows.

  o If reply_flag is present and encodes the CBOR simple value true (0xf5), the Initiator is asking the Responder to advertise the EDHOC application profiles that it supports, within the EDHOC message sent in reply to EDHOC message_1.

    If such a message is EDHOC message_2, the Responder relies on the EAD item "Supported EDHOC application profiles" included in the EAD_2 field. If such a message is an EDHOC error message with error code TBD_ERROR_CODE (see Section 5.2), the Responder relies on ERR_INFO.

    If the Responder sends either of those messages in reply to such an EDHOC message_1, the Responder MUST honor the request from the Initiator and accordingly advertise the EDHOC application profiles that it supports.

  o If reply_flag is present and encodes the CBOR simple value false (0xf4), the Initiator is suggesting the Responder to not advertise the EDHOC application profiles that it supports, within the EDHOC message sent in reply to EDHOC message_1. This is relevant when the Initiator already knows what EDHOC application profiles are supported by the Responder, e.g., based on previous interactions with that Responder or on the outcome of a discovery process.

    In spite of the suggestion from the Initiator, the Responder MAY still advertise the EDHOC application profiles that it supports, when replying to EDHOC message_1 with EDHOC message_2 or with an EDHOC error message with error code TBD_ERROR_CODE (see Section 5.2). For example, when sending EDHOC message_2, the Responder might wish to steer the rest of the EDHOC session in a specific way, by including the EAD item "Supported EDHOC application profiles" that specifies information corresponding to EDHOC_Information prescriptive parameters (see Section 3.4 of [I-D.ietf-ace-edhoc-oscore-profile]).

- The CBOR sequence APP_PROF_SEQ, which is specified further below.

* When the EAD item is included in the EAD_2 field, the value of the CBOR byte string is the binary representation of the CBOR sequence APP_PROF_SEQ.

The CBOR sequence APP_PROF_SEQ is composed of one or more elements, whose order has no meaning. Each element of the CBOR sequence MUST be either of the following:

* A CBOR integer, specifying the Profile ID of an EDHOC application profile. The integer value is taken from the 'Profile ID' column of the "EDHOC Application Profiles" registry defined in Section 10.8 of this document.

  This element of the CBOR sequence indicates that the message sender supports the EDHOC application profile identified by the Profile ID.

* A CBOR array including at least two elements. In particular:

  - The first element MUST be a CBOR integer, specifying the Profile ID of an EDHOC application profile. The integer value is taken from the 'Profile ID' column of the "EDHOC Application Profiles" registry.

  - Each of the elements following the first one MUST be a CBOR unsigned integer, specifying the ead_label of an EAD item.

  This element of the CBOR sequence indicates that the message sender supports:

  - The EDHOC application profile PROFILE identified by the Profile ID in the first element of the array; and

  - The EAD items identified by the ead_label in the elements following the first one, in addition to the EAD items that are specified in the definition of the EDHOC application profile PROFILE.

* An EDHOC_Information object encoded in CBOR, i.e., as a CBOR map (see Section 3.4 of [I-D.ietf-ace-edhoc-oscore-profile]).

  The EDHOC_Information object MUST NOT include the element "app_prof". Also, it MUST NOT include elements that are not allowed within the EDHOC_Application_Profile object defined in Section 2, with the exception of the following elements that MAY be included:

  - "trust_anchors".

  - "exporter_out_len" (see Section 5.1.2).

This element of the CBOR sequence indicates that the message sender supports an EDHOC application profile consistent with the pieces of information specified by the EDHOC_Information object.

The recipient peer MUST abort the EDHOC session and MUST reply with an EDHOC error message with error code (ERR_CODE) 1, if ead_value is malformed or does not conform with the format defined above.

It is possible that ead_value provides information corresponding to EDHOC_Information prescriptive parameters (see Section 3.4 of [I-D.ietf-ace-edhoc-oscore-profile]), e.g., "message_4" or "max_msgsize". The type of such parameters is indicated in the 'Type' column of the corresponding entry in the IANA registry "EDHOC Information" (see [I-D.ietf-ace-edhoc-oscore-profile]).

If the EAD item "Supported EDHOC application profiles" is included in EDHOC message_1 and/or message_2 during an EDHOC session, the peers participating in that session MUST NOT act in violation of what is indicated by prescriptive parameters that are specified in those EAD items. Upon receiving an EDHOC message, a peer MUST check whether the other peer has violated such indications. If any violation is found, the peer MUST abort the EDHOC session and MUST reply with an EDHOC error message with error code (ERR_CODE) 1.

When composing ead_value, the sender peer MUST comply with the content restrictions specified in Section 5.1.1.

The CDDL grammar describing ead_value for the EAD item "Supported EDHOC application profiles" is shown in Figure 3.

```
ead_value = ead_1_value / ead_2_value

ead_1_value = bytes .cborseq OUTER_SEQ

ead_2_value = bytes .cborseq APP_PROF_SEQ

; This defines an array, the elements of which
; are to be used in the CBOR Sequence OUTER_SEQ:
OUTER_SEQ = [?reply_flag, APP_PROF_SEQ]

reply_flag = bool

; This defines an array, the elements of which
; are to be used in the CBOR Sequence APP_PROF_SEQ:
APP_PROF_SEQ = [1* element]

element = profile_id / profile_id_with_eads / EDHOC_Information

profile_id = int

profile_id_with_eads = [profile_id, 1* uint]

; The full definition is provided in
; draft-ietf-ace-edhoc-oscore-profile
EDHOC_Information : map
```

Figure 3: CDDL Definition of ead_value for the EAD Item "Supported EDHOC application profiles"

5.1.1. Content Restrictions

When the sender peer composes ead_value of the EDHOC EAD item "Supported EDHOC application profiles", the following applies.

It is possible that ead_value provides an information corresponding to an EDHOC_Information prescriptive parameter (see Section 3.4 of [I-D.ietf-ace-edhoc-oscore-profile]).

If ead_value specifies such an information multiple times, then each occurrence of that information MUST convey exactly the same content. With reference to the CBOR sequence APP_PROF_SEQ defined in Section 5.1, the enforcement of these content restrictions MUST take into account prescriptive parameters that are included:

* As elements of an EDHOC_Information object specified within APP_PROF_SEQ; or

* As elements of an EDHOC_Application_Profile object encoding an EDHOC application profile, which is identified by its Profile ID specified within APP_PROF_SEQ.

If the Responder receives the EAD item in the EAD_1 field of EDHOC message_1 and intends to include the EAD item in the EAD_2 field of EDHOC message_2, then the Responder MUST further take into account the presence of such information in the received EAD item when composing ead_value.

A consumer MUST treat as malformed an EDHOC_Information object that does not comply with the restrictions above.

5.1.2. Agreeing on EDHOC_Exporter Output Lengths

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.

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. As described below, this can be achieved in-band, by using the EDHOC EAD item "Supported EDHOC application profiles" defined in Section 5.1.

This document defines the new parameter "exporter_out_len" of the EDHOC_Information object (see Section 3.4 of [I-D.ietf-ace-edhoc-oscore-profile]). The parameter is of type prescriptive (P) and is summarized in Table 2. The parameter is specified further below.

Name	CBOR label	CBOR type	Registry	Description	Type
exporter_out_len	22	array	EDHOC Exporter Labels	Set of output lengths to use with the EDHOC_Exporter interface	P

Table 2: EDHOC_Information Parameter "exporter_out_len"

* exporter_out_len: This parameter specifies a set of pairs (X, Y), where:

  - The first element X specifies a value to use as first argument "exporter_label" when invoking the EDHOC_Exporter interface (see Section 4.2.1 of [RFC9528]).

    The value of X 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 specifies 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.

  The set is encoded as an array, each element of which MUST be an array of exactly two elements, hence encoding one pair (X, Y). That is, each inner array includes X encoded as an unsigned integer and Y encoded as an unsigned integer, in this order.

  Within the set of pairs (X, Y), the order of the inner arrays encoding the pairs is not relevant. The set MUST NOT specify multiple pairs that have the same unsigned integer value as their first element X.

In JSON, the "exporter_out_len" value is an array, each element of which is an array including two unsigned integers. In CBOR, "exporter_out_len" is an array, each element of which is an array including two unsigned integers, and has label 22.

Within ead_value of the EAD item "Supported EDHOC application profiles", the parameter "exporter_out_len" can be included within instances of the EDHOC_Information object that are specified within the CBOR sequence APP_PROF_SEQ (see Section 5.1).

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 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".

* 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 "Supported EDHOC application profiles" and specifying the parameter "exporter_out_len", then the following applies if the Responder includes the EAD item "Supported EDHOC application profiles" in EDHOC message_2, with ead_value specifying the parameter "exporter_out_len". 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 within the EAD item included in the received EDHOC message_1.

If the Initiator receives an EDHOC message_2 including the EAD item "Supported EDHOC application profiles" and specifying the parameter "exporter_out_len", then the following applies if the Initiator included the EAD item "Supported EDHOC application profiles" in EDHOC message_1, with ead_value specifying the parameter "exporter_out_len". 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.

Since the parameter "exporter_out_len" is of type prescriptive, the restrictions compiled in Section 5.1.1 apply. In particular, the "information" corresponding to the prescriptive parameter "exporter_out_len" is the "length" Y to use when invoking the EDHOC_Exporter interface using the paired "exporter_label" X.

That is, if ead_value provides the length of the EDHOC_Exporter output for a given "exporter_label" multiple times, then each of such occurrences MUST specify the same "length" value. Within this constraint, it remains possible for ead_value to specify multiple instances of the EDHOC_Information object within APP_PROF_SEQ and for each of such instances to include the parameter "exporter_out_len", which can overall encode a value different from that of the same parameter in another instance of the EDHOC_Information object.

The recipient peer MUST abort the EDHOC session and MUST reply with an EDHOC error message with error code (ERR_CODE) 1, if the parameter "exporter_out_len" is malformed or does not conform with the format and constraints defined above.

In an EDHOC session during which the EAD item "Supported EDHOC application profiles" has been included in EDHOC message_1 and/or message_2 as specifying the parameter "exporter_out_len", 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.

When using the EDHOC and OSCORE transport profile of the ACE framework [I-D.ietf-ace-edhoc-oscore-profile], the parameter "exporter_out_len" MUST NOT be included within the EDHOC_Information object specified as the value of the parameter/claim "edhoc_info".

5.2. In the EDHOC Error Message

This section defines the error code TBD_ERROR_CODE, which is registered in Section 10.6 of this document.

Error code TBD_ERROR_CODE MUST only be used when replying to EDHOC message_1. If an EDHOC error message with error code TBD_ERROR_CODE is received as reply to an EDHOC message different from EDHOC message_1, then the recipient of the error message MUST ignore what is specified in ERR_INFO.

The Responder MUST NOT abort an EDHOC session exclusively due to the wish of sending an error message with error code TBD_ERROR_CODE. Instead, the Responder can advertise the EDHOC application profiles that it supports to the Initiator by means of the EAD item "Supported EDHOC application profiles" defined in Section 5.1, specifying it in the EAD_2 field of the EDHOC message_2 to send in the EDHOC session.

When replying to an EDHOC message_1 with an error message, the Responder has to consider the reason for which it is aborting the EDHOC session and MUST NOT specify error code TBD_ERROR_CODE if a different, more appropriate error code can be specified instead. For example, if the negotiation of the selected cipher suite fails (see Section 6.3 of [RFC9528]), the error message MUST NOT specify error code TBD_ERROR_CODE, since the error message intended to be used in that case specifies error code 2 (Wrong selected cipher suite) and conveys SUITES_R as ERR_INFO.

When using error code TBD_ERROR_CODE, the error information specified in ERR_INFO MUST be a CBOR byte string with value the binary representation of a CBOR sequence APP_PROF_SEQ.

In particular, APP_PROF_SEQ has the same format and semantics specified in Section 5.1, except for the following difference: for each element of the CBOR sequence that is an EDHOC_Information object, such an object MUST NOT include the element "exporter_out_len" defined in Section 5.1.2.

The recipient peer MUST silently ignore elements of the CBOR sequence APP_PROF_SEQ that are malformed or do not conform with the intended format of APP_PROF_SEQ.

6. Advertising Supported EDHOC Application Profiles using SVCB Resource Records

Given a server, its support for EDHOC and for EDHOC application profiles can be advertised using SVCB Resource Records (RR) [RFC9460][RFC9461].

To this end, this document specifies the SvcParamKeys "edhocpath" and "edhoc-app-prof", which are defined below and are registered in Section 10.7.

* "edhocpath" - The SvcParamKey "edhocpath" is single-valued and specifies a list of one or more absolute paths to EDHOC resources at the server.

  - The wire-format value of "edhocpath" is the binary representation of the CBOR data item edhocpath-value, which MUST exactly fill the SvcParamValue.

    In particular, edhocpath-value MUST be a CBOR byte string PATH_BSTR or a CBOR array. In the latter case, the array MUST include at least two elements, each of which MUST be a CBOR byte string PATH_BSTR. The SVCB RR MUST be considered malformed if the SvcParamValue ends within edhocpath-value or if edhocpath-value is malformed.

    The value of each CBOR byte string PATH_BSTR is the binary representation of a CBOR sequence PATH_SEQ composed of zero or more CBOR text strings. In particular, each PATH_SEQ specifies the URI path of an EDHOC resource at the server, with each CBOR text string within that PATH_SEQ specifying a URI path segment.

    If edhocpath-value is a CBOR array, it MUST NOT include any two elements that specify the same URI path.

    The CDDL grammar describing the CBOR data item edhocpath-value is shown in Figure 4.

  - The presentation format value of "edhocpath" SHALL be a comma-separated list (see Appendix A.1 of [RFC9460]) of one or more absolute paths to EDHOC resources at the server. The same considerations for the "," and "\" characters in paths for zone-file implementations as for the alpn-ids in an "alpn" SvcParam apply (see Section 7.1.1 of [RFC9460]).

The i-th path in the presentation format value is the textual representation of the path specified by the i-th CBOR sequence PATH_SEQ in the wire-format value (see above).

The textual representation of each path follows the semantics of path-absolute shown in the ABNF definition in Figure 5, which is provided by the ABNF for path-absolute in Section 3.3 of [RFC3986]. In particular, given the path specified by a CBOR sequence PATH_SEQ, segment-nz is the value of the first CBOR text string in PATH_SEQ (if any), while each segment is the value of a CBOR text string following the first one in PATH_SEQ (if any).

* "edhoc-app-prof" - The SvcParamKey "edhoc-app-prof" is single-valued and specifies a set of EDHOC application profiles that the server supports.

  - The wire-format value of "edhoc-app-prof" is the binary representation of the CBOR data item edhoc-app-prof-value, which MUST exactly fill the SvcParamValue.

    In particular, edhoc-app-prof-value MUST be a CBOR byte string APP_BSTR or a CBOR array. In the latter case, the array MUST include at least two elements, each of which MUST be a CBOR byte string APP_BSTR. The SVCB RR MUST be considered malformed if the SvcParamValue ends within edhoc-app-prof-value or if edhoc-app-prof-value is malformed.

    The value of each CBOR byte string APP_BSTR is the binary representation of a CBOR sequence APP_PROF_SEQ. In particular, APP_PROF_SEQ has the same format and semantics specified in Section 5.1, except for the following difference: for each element of the CBOR sequence that is an EDHOC_Information object, such an object MUST NOT include the element "exporter_out_len" defined in Section 5.1.2.

    The SVCB RR MUST be considered malformed if APP_PROF_SEQ is malformed or does not conform with the intended format.

    The CDDL grammar describing the CBOR data item edhoc-app-prof-value is shown in Figure 6.

- The presentation format value of "edhoc-app-prof" SHALL be the CBOR extended diagnostic notation (see Section 8 of [RFC8949] and Appendix G of [RFC8610]) of edhoc-app-prof-value in the wire-format value (see above). When producing the presentation format value, care ought to be taken in representing Unicode with the limited ASCII character subset (e.g., by means of Punycode [RFC3492]) and in removing unnecessary common blank spaces within the CBOR extended diagnostic notation.

If the SvcParamKey "edhoc-app-prof" is not present in the SVCB RR, then the SvcParamKey "edhocpath", if present, specifies the URI paths of EDHOC resources at the server.

If the SvcParamKey "edhoc-app-prof" is present in the SVCB RR, then the following applies.

* If the SvcParamKey "edhocpath" is not present in the SVCB RR, then the value of the SvcParamKey "edhoc-app-prof" MUST be a CBOR byte string.

  The information specified by the SvcParamKey "edhoc-app-prof" pertains to the EDHOC resource at the server with URI path "/.well-known/edhoc".

* If the SvcParamKey "edhocpath" is present in the SVCB RR, then the following applies.

  - If the value of the SvcParamKey "edhocpath" is a CBOR byte string, then the value of the SvcParamKey "edhoc-app-prof" MUST also be a CBOR byte string.

    The information specified by the SvcParamKey "edhoc-app-prof" pertains to the EDHOC resource at the server with URI path specified by the SvcParamKey "edhocpath".

  - If the value of the SvcParamKey "edhocpath" is a CBOR array including N elements, then the value of the SvcParamKey "edhoc-app-prof" MUST also be a CBOR array including N elements.

    The information specified by the i-th element of the CBOR array within the SvcParamKey "edhoc-app-prof" pertains to the EDHOC resource at the server with URI path specified by the i-th element of the CBOR array within the SvcParamKey "edhocpath".

A consumer MUST treat as malformed an SVCB RR, in case the SvcParamKeys "edhocpath" and "edhoc-app-prof", if present, do not comply with the format and restrictions defined above.

```
edhocpath-value = PATH_BSTR / [2* PATH_BSTR]

PATH_BSTR = bytes .cborseq PATH_SEQ

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

path_segment = tstr
```

Figure 4: CDDL Definition of the value of the SvcParamKey "edhocpath"

```
path-absolute = "/" [ segment-nz *( "/" segment ) ]

segment       = *pchar
segment-nz    = 1*pchar

pchar = unreserved / pct-encoded / sub-delims / ":" / "@"

unreserved    = ALPHA / DIGIT / "-" / "." / "_" / "~"
pct-encoded   = "%" HEXDIG HEXDIG
sub-delims    = "!" / "$" / "&" / "'" / "(" / ")"
              / "*" / "+" / "," / ";" / "="
```

Figure 5: ABNF Definition of path-absolute

```
edhoc-app-prof-value = APP_BSTR / [2* APP_BSTR]

; The full definition of APP_PROF_SEQ
; is provided in Section 5.1
APP_BSTR = bytes .cborseq APP_PROF_SEQ
```

Figure 6: CDDL Definition of the value of the SvcParamKey "edhoc-app-prof"

7. Well-known EDHOC Application Profiles

This section defines a set of well-known EDHOC application profiles that are meant to reflect what is most common and expected to be supported by EDHOC peers.

The well-known application profiles are _not_ to be intended as "default" profiles to use, in case no other indication is provided to EDHOC peers.

In particular, an EDHOC peer MUST NOT assume that, unless otherwise indicated, any of such profiles is used when running EDHOC through a well-known EDHOC resource, such as the resource at /.well-known/edhoc when EDHOC messages are transported as payload of CoAP messages (see Appendix A.2 of [RFC9528]).

Building on the above, the well-known application profiles are _not_ intended to deviate from what is mandatory to support for EDHOC peers, which is defined by the compliance requirements in Section 8 of [RFC9528].

The rest of this section defines the well-known application profiles, each of which is represented by means of an EDHOC_Application_Profile object (see Section 2) using the CBOR extended diagnostic notation.

An entry for each well-known application profile is also registered at the "EDHOC Application Profiles" registry defined in Section 10.8 of this document.

7.1. Well-Known Application Profile MINIMAL_CS_2

```
{
        e'methods' : 3, / EDHOC Method Type 3 /
  e'cipher_suites' : 2, / EDHOC Cipher Suite 2 /
     e'cred_types' : 1, / CWT Claims Set (CCS) /
  e'id_cred_types' : 4, / kid /
       e'app_prof' : e'APP-PROF-MINIMAL-CS-2'
}
```

This application profile is aligned with the example trace of EDHOC compiled in Section 3 of [RFC9529].

7.2. Well-Known Application Profile MINIMAL_CS_0

```
{
        e'methods' : 3, / EDHOC Method Type 3 /
  e'cipher_suites' : 0, / EDHOC Cipher Suite 0 /
     e'cred_types' : 1, / CWT Claims Set (CCS) /
  e'id_cred_types' : 4, / kid /
       e'app_prof' : e'APP-PROF-MINIMAL-CS-0'
}
```

7.3. Well-Known Application Profile BASIC_CS_2_X509

```
{
        e'methods' : [0, 3], / EDHOC Method Types 0 and 3 /
  e'cipher_suites' : 2, / EDHOC Cipher Suite 2 /
     e'cred_types' : [1, 2], / CWT Claims Set (CCS)
                               and X.509 certificate /
  e'id_cred_types' : [4, 34], / kid and x5t /
       e'app_prof' : e'APP-PROF-BASIC-CS-2-X509'
}
```

This application profile is aligned with the example trace of EDHOC compiled in Section 3 of [RFC9529].

7.4. Well-Known Application Profile BASIC_CS_0_X509

```
{
        e'methods' : [0, 3], / EDHOC Method Types 0 and 3 /
  e'cipher_suites' : 0, / EDHOC Cipher Suite 0 /
     e'cred_types' : [1, 2], / CWT Claims Set (CCS)
                               and X.509 certificate /
  e'id_cred_types' : [4, 34], / kid and x5t /
       e'app_prof' : e'APP-PROF-BASIC-CS-0-X509'
}
```

This application profile is aligned with the example trace of EDHOC compiled in Section 2 of [RFC9529].

7.5. Well-Known Application Profile BASIC_CS_2_C509

```
{
        e'methods' : [0, 3], / EDHOC Method Types 0 and 3 /
  e'cipher_suites' : 2, / EDHOC Cipher Suite 2 /
     e'cred_types' : [1, e'c509_cert'], / CWT Claims Set (CCS)
                                          and C509 certificate /
  e'id_cred_types' : [4, e'c5t'], / kid and c5t /
       e'app_prof' : e'APP-PROF-BASIC-CS-2-C509'
}
```

7.6. Well-Known Application Profile BASIC_CS_0_C509

```
{
        e'methods' : [0, 3], / EDHOC Method Types 0 and 3 /
  e'cipher_suites' : 0, / EDHOC Cipher Suite 0 /
     e'cred_types' : [1, e'c509_cert'], / CWT Claims Set (CCS)
                                          and C509 certificate /
  e'id_cred_types' : [4, e'c5t'], / kid and c5t /
       e'app_prof' : e'APP-PROF-BASIC-CS-0-C509'
}
```

7.7. Well-Known Application Profile INTERMEDIATE_CS_2

```
{
        e'methods' : [0, 3], / EDHOC Method Types 0 and 3 /
  e'cipher_suites' : 2, / EDHOC Cipher Suite 2 /
     e'cred_types' : [1, 2, e'c509_cert'], / CWT Claims Set (CCS),
                                             X.509 certificate,
                                             and C509 certificate /
  e'id_cred_types' : [4, 14, 34, 33, e'c5t', e'c5c'], / kid, kccs,
                                                        x5t, x5chain,
                                                        c5t, and c5c /
       e'app_prof' : e'APP-PROF-INTERMEDIATE-CS-2'
}
```

This application profile is aligned with the example trace of EDHOC compiled in Section 3 of [RFC9529].

7.8. Well-Known Application Profile INTERMEDIATE_CS_0

```
{
        e'methods' : [0, 3], / EDHOC Method Types 0 and 3 /
  e'cipher_suites' : 0, / EDHOC Cipher Suite 0 /
     e'cred_types' : [1, 2, e'c509_cert'], / CWT Claims Set (CCS),
                                             X.509 certificate,
                                             and C509 certificate /
  e'id_cred_types' : [4, 14, 34, 33, e'c5t', e'c5c'], / kid, kccs,
                                                        x5t, x5chain,
                                                        c5t, and c5c /
       e'app_prof' : e'APP-PROF-INTERMEDIATE-CS-0'
}
```

This application profile is aligned with the example trace of EDHOC compiled in Section 2 of [RFC9529].

7.9. Well-Known Application Profile EXTENSIVE

```
{
        e'methods' : [0, 1, 2, 3], / EDHOC Method Types
                                     0, 1, 2, and 3 /
  e'cipher_suites' : [0, 1, 2, 3], / EDHOC Cipher Suites
                                     0, 1, 2, and 3 /
     e'cred_types' : [1, 0, 2, e'c509_cert'], / CWT Claims Set (CCS),
                                                CWT, X.509 certificate,
                                                and C509 certificate /
  e'id_cred_types' : [4, 14, 13, 34, 33, e'c5t', e'c5c'], / kid,
                                                            kccs, kcwt,
                                                            x5t,
                                                            x5chain,
                                                            c5t, and
                                                            c5c /
       e'app_prof' : e'APP-PROF-EXTENSIVE'
}
```

This application profile is aligned with the example traces of EDHOC compiled in Sections 2 and 3 of [RFC9529].

8. Identifiers of Well-known EDHOC Application Profiles

This document defines the following identifiers of well-known EDHOC application profiles.

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

Profile ID	Name	Description	Reference
0	MINIMAL-CS-2	Method 3; Cipher Suite 2; CCS; kid	[RFC-XXXX]
1	MINIMAL-CS-0	Method 3; Cipher Suite 0; CCS; kid	[RFC-XXXX]
2	BASIC-CS-2-X509	Methods (0, 3); Cipher Suite 2; (CCS, X.509 certificates); (kid, x5t)	[RFC-XXXX]
3	BASIC-CS-0-X509	Methods (0, 3); Cipher Suite 0; (CCS, X.509 certificates); (kid,	[RFC-XXXX]

		x5t)	
4	BASIC-CS-2-C509	Methods (0, 3); Cipher Suite 2; (CCS, C509 certificates); (kid, c5t)	[RFC-XXXX]
5	BASIC-CS_0-C509	Methods (0, 3); Cipher Suite 0; (CCS, C509 certificates); (kid, c5t)	[RFC-XXXX]
6	INTERMEDIATE-CS-2	Methods (0, 3); Cipher Suite 2; (CCS, X.509/C509 certificates); (kid, kccs, x5t, x5chain, c5t, c5c)	[RFC-XXXX]
7	INTERMEDIATE-CS-0	Methods (0, 3); Cipher Suite 0; (CCS, X.509/C509 certificates); (kid, kccs, x5t, x5chain, c5t, c5c)	[RFC-XXXX]
8	EXTENSIVE	Methods (0, 1, 2, 3); Cipher Suites (0, 1, 2, 3); (CCS, CWT, X.509/C509 certificates); (kid, kccs, kcwt, x5t, x5chain, c5t, c5c)	[RFC-XXXX]

Table 3: EDHOC Well-known Application Profiles

9. Security Considerations

TBD

10. 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.

10.1. Media Type Registrations

IANA is asked to register the media type "application/edhoc-app-profile+cbor-seq". This registration follows the procedures specified in [RFC6838].

Type name: application

Subtype name: edhoc-app-profile+cbor-seq

Required parameters: N/A

Optional parameters: N/A

Encoding considerations: Must be encoded as a CBOR sequence [RFC8742] of CBOR maps [RFC8949]. Each element of each CBOR map is also defined as an element of the CBOR-encoded EDHOC_Information object from Section 3.4 of [I-D.ietf-ace-edhoc-oscore-profile].

Security considerations: See Section 9 of [RFC-XXXX].

Interoperability considerations: N/A

Published specification: [RFC-XXXX]

Applications that use this media type: Applications that need to describe, distribute, and store a representation of an EDHOC application profile (see [RFC-XXXX] and Section 3.9 of [RFC9528]).

Fragment identifier considerations: N/A

Additional information: N/A

Person & email address to contact for further information: LAKE WG mailing list (lake@ietf.org) or IETF Applications and Real-Time Area (art@ietf.org)

Intended usage: COMMON

Restrictions on usage: None

Author/Change controller: IETF

Provisional registration: No

10.2. CoAP Content-Formats Registry

IANA is asked to add the following entry to the "CoAP Content-Formats" registry within the "Constrained RESTful Environments (CoRE) Parameters" registry group.

Content Type: application/edhoc-app-profile+cbor-seq

Content Coding: -

ID: TBD (range 0-255)

Reference: [RFC-XXXX]

10.3. Target Attributes Registry

IANA is asked to register the following entries in the "Target Attributes" registry within the "Constrained RESTful Environments (CoRE) Parameters", as per [RFC9423].

* Attribute Name: ed-max-msgsize

* Brief Description: The admitted maximum size of EDHOC messages in bytes

* Change Controller: IETF

* Reference: [RFC-XXXX]

* Attribute Name: ed-coap-ct

* Brief Description: Requested use of the CoAP Content-Format Option in CoAP messages whose payload includes exclusively an EDHOC message, possibly prepended by an EDHOC connection identifier

* Change Controller: IETF

* Reference: [RFC-XXXX]

* Attribute Name: ed-epid-t

* Brief Description: A supported type of endpoint identity for EDHOC

* Change Controller: IETF

* Reference: [RFC-XXXX]

* Attribute Name: ed-tp

* Brief Description: A supported means for transporting EDHOC messages

* Change Controller: IETF

* Reference: [RFC-XXXX]

* Attribute Name: ed-prof

* Brief Description: A supported EDHOC application profile

* Change Controller: IETF

* Reference: [RFC-XXXX]

* Attribute Name: ed-ta-edcred-uuid

* Brief Description: Identifier of a supported trust anchor for verifying authentication credentials of other EDHOC peers, as a UUID

* Change Controller: IETF

* Reference: [RFC-XXXX]

* Attribute Name: ed-ta-edcred-kid

* Brief Description: Identifier of a supported trust anchor for verifying authentication credentials of other EDHOC peers, as a binary key identifier

* Change Controller: IETF

* Reference: [RFC-XXXX]

* Attribute Name: ed-ta-edcred-c5t

* Brief Description: Identifier of a supported trust anchor for verifying authentication credentials of other EDHOC peers, as a hash of a C509 certificate

* Change Controller: IETF

* Reference: [RFC-XXXX]

* Attribute Name: ed-ta-edcred-c5u

* Brief Description: Identifier of a supported trust anchor for verifying authentication credentials of other EDHOC peers, as a URI pointing to a C509 certificate

* Change Controller: IETF

* Reference: [RFC-XXXX]

* Attribute Name: ed-ta-edcred-x5t

* Brief Description: Identifier of a supported trust anchor for verifying authentication credentials of other EDHOC peers, as a hash of an X.509 certificate

* Change Controller: IETF

* Reference: [RFC-XXXX]

* Attribute Name: ed-ta-edcred-x5u

* Brief Description: Identifier of a supported trust anchor for verifying authentication credentials of other EDHOC peers, as a URI pointing to an X.509 certificate

* Change Controller: IETF

* Reference: [RFC-XXXX]

10.4. EDHOC Information Registry

IANA is asked to register the following entries in the "EDHOC Information" registry defined in [I-D.ietf-ace-edhoc-oscore-profile].

* Name: exporter_out_len
* CBOR label: 22 (suggested)
* CBOR type: array
* Registry: EDHOC Exporter Labels
* Description: Set of output lengths to use with the EDHOC_Exporter interface
* Type: P
* Specification: [RFC-XXXX][RFC9528]

* Name: app_prof
* CBOR label: 23 (suggested)
* CBOR type: int or array
* Registry: EDHOC Application Profiles registry
* Description: Set of supported EDHOC application profiles
* Type: NP
* Specification: [RFC-XXXX][RFC9528]

10.5. 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: Supported EDHOC application profiles
* Label: TBD_EAD_LABEL (range 0-23)
* Description: Set of supported EDHOC application profiles

* Reference: [RFC-XXXX]

10.6. EDHOC Error Codes Registry

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

* ERR_CODE: TBD_ERROR_CODE (range -24 to 23)

* ERR_INFO Type: app_profiles

* Description: Supported EDHOC application profiles

* Change Controller: IETF

* Reference: [RFC-XXXX]

10.7. DNS SVCB Service Parameter Keys (SvcParamKeys)

IANA is asked to add the following entries to the "Service Parameter Keys (SvcParamKeys)" registry within the "DNS Service Bindings (SVCB)" registry group. The definition of these parameters can be found in Section 6.

* Number: 11 (suggested)

* Name: edhocpath

* Meaning: EDHOC resource path

* Change Controller: IETF

* Reference: [RFC-XXXX]

* Number: 12 (suggested)

* Name: edhoc-app-prof

* Meaning: Supported EDHOC application profiles

* Change Controller: IETF

* Reference: [RFC-XXXX]

10.8. EDHOC Application Profiles Registry

IANA is requested to create a new "EDHOC Application Profiles" registry within the "Ephemeral Diffie-Hellman Over COSE (EDHOC)" registry group defined in [RFC9528].

The registration policy is either "Private Use", "Standards Action with Expert Review", or "Specification Required" per Section 4.6 of [RFC8126]. "Expert Review" guidelines are provided in Section 10.9.

All assignments according to "Standards Action with Expert Review" are made on a "Standards Action" basis per Section 4.9 of [RFC8126], with Expert Review additionally required per Section 4.5 of [RFC8126]. The procedure for early IANA allocation of Standards Track code points defined in [RFC7120] also applies. When such a procedure is used, IANA will ask the designated expert(s) to approve the early allocation before registration. In addition, WG chairs are encouraged to consult the expert(s) early during the process outlined in Section 3.1 of [RFC7120].

The columns of this registry are:

* Profile ID: This field contains the value used to identify the EDHOC application profile. These values MUST be unique. The value can be a positive integer or a negative integer. Different ranges of values use different registration policies [RFC8126]. Integer values from -24 to 23 are designated as "Standards Action With Expert Review". Integer values from -65536 to -25 and from 24 to 65535 are designated as "Specification Required". Integer values smaller than -65536 and greater than 65535 are marked as "Private Use".

* Name: This field contains the name of the EDHOC application profile.

* Description: This field contains a short description of the EDHOC application profile.

* Reference: This field contains a pointer to the public specification for the EDHOC application profile.

This registry has been initially populated with the values in Table 3.

10.9. Expert Review Instructions

"Standards Action with Expert Review" and "Specification Required" are two of the registration policies defined for the IANA registry established in this document. This section gives some general guidelines for what the experts should be looking for, but they are being designated as experts for a reason so they should be given substantial latitude.

Expert reviewers should take into consideration the following points:

* Clarity and correctness of registrations. Experts are expected to check the clarity of purpose and use of the requested entries. Experts need to make sure that the object of registration is clearly defined in the corresponding specification. Entries that do not meet these objective of clarity and completeness must not be registered.

* Point squatting should be discouraged. Reviewers are encouraged to get sufficient information for registration requests to ensure that the usage is not going to duplicate one that is already registered and that the point is likely to be used in deployments. The zones tagged as "Private Use" are intended for testing purposes and closed environments. Code points in other ranges should not be assigned for testing.

* Specifications are required for the "Standards Action With Expert Review" range of point assignment. Specifications should exist for "Specification Required" ranges, but early assignment before a specification is available is considered to be permissible. When specifications are not provided, the description provided needs to have sufficient information to identify what the point is being used for.

* Experts should take into account the expected usage of fields when approving point assignment. Documents published via Standards Action can also register points outside the Standards Action range. The length of the encoded value should be weighed against how many code points of that length are left, the size of device it will be used on, and the number of code points left that encode to that size.

11. References

11.1. Normative References

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

[I-D.ietf-ace-edhoc-oscore-profile]
Selander, G., Mattsson, J. P., Tiloca, M., and R. H旦glund, "Ephemeral Diffie-Hellman Over COSE (EDHOC) and Object Security for Constrained Environments (OSCORE) Profile for Authentication and Authorization for Constrained Environments (ACE)", Work in Progress, Internet-Draft, draft-ietf-ace-edhoc-oscore-profile-08, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ace-edhoc-oscore-profile-08>.

[I-D.ietf-cose-cbor-encoded-cert]
Mattsson, J. P., Selander, G., Raza, S., H旦glund, J., and M. Furuhed, "CBOR Encoded X.509 Certificates (C509 Certificates)", Work in Progress, Internet-Draft, draft-ietf-cose-cbor-encoded-cert-15, 18 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-cbor-encoded-cert-15>.

[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>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/rfc/rfc3986>.

[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/rfc/rfc5280>.

[RFC6690] Shelby, Z., "Constrained RESTful Environments (CoRE) Link Format", RFC 6690, DOI 10.17487/RFC6690, August 2012, <https://www.rfc-editor.org/rfc/rfc6690>.

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013, <https://www.rfc-editor.org/rfc/rfc6838>.

[RFC7120] Cotton, M., "Early IANA Allocation of Standards Track Code Points", BCP 100, RFC 7120, DOI 10.17487/RFC7120, January 2014, <https://www.rfc-editor.org/rfc/rfc7120>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/rfc/rfc7252>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/rfc/rfc8126>.

[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>.

[RFC8288] Nottingham, M., "Web Linking", RFC 8288, DOI 10.17487/RFC8288, October 2017, <https://www.rfc-editor.org/rfc/rfc8288>.

[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>.

[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>.

[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>.

[RFC9200] Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments Using the OAuth 2.0 Framework (ACE-OAuth)", RFC 9200, DOI 10.17487/RFC9200, August 2022, <https://www.rfc-editor.org/rfc/rfc9200>.

[RFC9360] Schaad, J., "CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates", RFC 9360, DOI 10.17487/RFC9360, February 2023, <https://www.rfc-editor.org/rfc/rfc9360>.

[RFC9460] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", RFC 9460, DOI 10.17487/RFC9460, November 2023, <https://www.rfc-editor.org/rfc/rfc9460>.

[RFC9461] Schwartz, B., "Service Binding Mapping for DNS Servers", RFC 9461, DOI 10.17487/RFC9461, November 2023, <https://www.rfc-editor.org/rfc/rfc9461>.

[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>.

[RFC9562] Davis, K., Peabody, B., and P. Leach, "Universally Unique IDentifiers (UUIDs)", RFC 9562, DOI 10.17487/RFC9562, May 2024, <https://www.rfc-editor.org/rfc/rfc9562>.

[RFC9668] Palombini, F., Tiloca, M., Hglund, 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)", RFC 9668, DOI 10.17487/RFC9668, November 2024, <https://www.rfc-editor.org/rfc/rfc9668>.

11.2. Informative References

[I-D.serafin-lake-ta-hint] Serafin, M. and G. Selander, "Trust Anchor Hints in Ephemeral Diffie-Hellman Over COSE (EDHOC)", Work in Progress, Internet-Draft, draft-serafin-lake-ta-hint-00, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-serafin-lake-ta-hint-00>.

[RFC3492] Costello, A., "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)", RFC 3492, DOI 10.17487/RFC3492, March 2003, <https://www.rfc-editor.org/rfc/rfc3492>.

[RFC9423] Bormann, C., "Constrained RESTful Environments (CoRE) Target Attributes Registry", RFC 9423, DOI 10.17487/RFC9423, April 2024, <https://www.rfc-editor.org/rfc/rfc9423>.

[RFC9529] Selander, G., Preu Mattsson, J., Serafin, M., Tiloca, M., and M. Vuini, "Traces of Ephemeral Diffie-Hellman Over COSE (EDHOC)", RFC 9529, DOI 10.17487/RFC9529, March 2024, <https://www.rfc-editor.org/rfc/rfc9529>.

Appendix A. CDDL Model

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

```
; EDHOC Information
methods = 1
cipher_suites = 2
cred_types = 6
id_cred_types = 7
app_prof = 23

; EDHOC Application Profiles
APP-PROF-MINIMAL-CS-2 = 0
APP-PROF-MINIMAL-CS-0 = 1
APP-PROF-BASIC-CS-2-X509 = 2
APP-PROF-BASIC-CS-0-X509 = 3
APP-PROF-BASIC-CS-2-C509 = 4
APP-PROF-BASIC-CS-0-C509 = 5
APP-PROF-INTERMEDIATE-CS-2 = 6
APP-PROF-INTERMEDIATE-CS-0 = 7
APP-PROF-EXTENSIVE = 8

; COSE Header Parameters
c5t = 22
c5c = 25

; EDHOC Authentication Credential Types
c509_cert = 3
```

Figure 7: CDDL model

Appendix B. Document Updates

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

B.1. Version -02 to -03

* Removed restrictions on the scope of the EDHOC_Application_Profile object.

* Forbidden violations of prescriptive indications in the EAD item. The EDHOC session fails if such a violation is detected.

* Extended semantics of ead_value: optional boolean flag when the EAD item is used in EDHOC message_1.

* Defined parameter "exporter_out_len", for in-band negotiation of EDHOC_Exporter output lengths through the EAD item "Supported EDHOC application profiles".

* Specified wire-format and presentation format for the SvcParamKeys.

* Fixed errors in CDDL notations.

* Specified type of "app_prof" in the IANA registration request.

* Clarifications and editorial improvements.

B.2. Version -01 to -02

* Revised order of sections.

* Use of parameters aligned with corresponding updates in draft-ietf-ace-edhoc-oscore-profile.

* EAD item "Supported EDHOC application profiles":

  - It can be used only in a critical way.

  - Improved semantics of ead_value.

  - Content restrictions to avoid inconsistent information.

* Use of the parameter "app_prof" in draft-ietf-ace-edhoc-oscore-profile:

  - Improved co-existence with other parameters.

  - Content restrictions to avoid inconsistent information.

* Error handling:

  - EAD item "Supported EDHOC application profiles" occurring multiple times in EDHOC message_1 or message_2.

  - EAD item "Supported EDHOC application profiles" in EDHOC message_3 or message_4.

  - Invalid ead_value in EAD item "Supported EDHOC application profiles".

  - Invalid information in EDHOC error message with new error code.

* Fixed encoding of ERR_INFO for the EDHOC error message with the new error code.

* EDHOC_Application_Profile object

  - Clarified scope.

  - Clarified meaning of boolean parameters that are non-prescriptive.

  - Forbid the presence of the element "trust_anchors".

* Advertisement of Supported EDHOC Application Profiles using SVCB Resource Records.

* Updated integer abbreviations for the EDHOC_Information parameters.

* Editorial improvements.

B.3. Version -00 to -01

* Clarified motivation in the abstract and introduction.

* Moved definition of EDHOC_Information parameters to draft-ietf-ace-edhoc-oscore-profile.

* Renamed ed-idep-t x as ed-epid-t.

* Content-Format abbreviated as "ct" (not "cf").

* CBOR abbreviation of "app_prof" changed to 23.

* Added preamble on identifying application profiles by Profile ID.

* Defined target attributes "ed-ta-*" for specifying supported trust anchors.

* Defined new EAD item and error code to advertise supported EDHOC application profiles.

* Defined how to handle non admitted parameters.

* Renamed well-known EDHOC application profiles.

* Updated IANA considerations:

- Suggested range 0-255 for CoAP Content-Format ID.

- Requested registration for target attributes "ed-ta-*".

- Removed requests for registration of removed parameters.

* Updated references.

* Editorial improvements.

Acknowledgments

The authors sincerely thank Christian Amsss, Carsten Bormann, Geovane Fedrecheski, Martine Lenders, Elsa Lopez-Perez, Michael Richardson, Gran Selander, Brian Sipos, and Malia Vuini for their feedback and comments.

The target attributes "ed-ta-*" for specifying supported trust anchors build on a proposal originally described in [I-D.serafin-lake-ta-hint].

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-16440 Stockholm Kista
Sweden
Email: marco.tiloca@ri.se

Rikard Hglund
RISE AB
Isafjordsgatan 22
SE-16440 Stockholm Kista
Sweden
Email: rikard.hoglund@ri.se