

LAKE Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 3 September 2026

M. Tiloca  
R. H<sub>U</sub>glund  
RISE AB  
2 March 2026

Coordinating the Use of Application Profiles for Ephemeral Diffie-  
Hellman Over COSE (EDHOC)  
draft-ietf-lake-app-profiles-04

## 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](mailto: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

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 3 September 2026.

## Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	3
1.1. Terminology . . . . .	6
2. EDHOC_Application_Profile . . . . .	6
3. Identifying EDHOC Application Profiles by Profile ID . . . . .	8
3.1. In Web Linking . . . . .	9
3.2. In the EDHOC_Information Object . . . . .	11
3.2.1. Use in the EDHOC and OSCORE Profile of the ACE Framework . . . . .	12
4. Additional Parameters for Web Linking . . . . .	13
5. Advertising Supported EDHOC Application Profiles during an EDHOC Session . . . . .	16
5.1. In EDHOC Message 1 and Message 2 . . . . .	16
5.1.1. Content Restrictions . . . . .	20
5.1.2. Agreeing on EDHOC_Exporter Output Lengths . . . . .	21
5.1.3. Examples of ead_value . . . . .	25
5.2. In the EDHOC Error Message . . . . .	27
5.2.1. Example of ERR_INFO . . . . .	28
6. Advertising Supported EDHOC Application Profiles using DNS SVCB Resource Records . . . . .	29
6.1. Examples of Wire-Format Values of the SvcParamKeys . . . . .	34
7. Well-known EDHOC Application Profiles . . . . .	36
7.1. Well-Known Application Profile MINIMAL-CS-2 . . . . .	37
7.2. Well-Known Application Profile MINIMAL-CS-0 . . . . .	37
7.3. Well-Known Application Profile BASIC-CS-2-X509 . . . . .	37
7.4. Well-Known Application Profile BASIC-CS-0-X509 . . . . .	38

7.5.	Well-Known Application Profile BASIC-CS-2-C509	38
7.6.	Well-Known Application Profile BASIC-CS-0-C509	38
7.7.	Well-Known Application Profile INTERMEDIATE-CS-2	38
7.8.	Well-Known Application Profile INTERMEDIATE-CS-0	39
7.9.	Well-Known Application Profile EXTENSIVE	39
8.	Identifiers of Well-known EDHOC Application Profiles	40
9.	Operational Considerations	41
9.1.	Relation with Network Operations	42
9.2.	Source of Data for Network Operators	42
9.3.	Logging and Reporting	43
10.	Security Considerations	43
11.	IANA Considerations	45
11.1.	Media Type Registrations	45
11.2.	CoAP Content-Formats Registry	46
11.3.	Target Attributes Registry	46
11.4.	EDHOC Information Registry	48
11.5.	EDHOC External Authorization Data Registry	49
11.6.	EDHOC Error Codes Registry	49
11.7.	DNS SVCB Service Parameter Keys (SvcParamKeys)	50
11.8.	EDHOC Application Profiles Registry	50
11.9.	Expert Review Instructions	51
12.	References	52
12.1.	Normative References	52
12.2.	Informative References	55
Appendix A.	CDDL Model	56
Appendix B.	Document Updates	57
B.1.	Version -03 to -04	57
B.2.	Version -02 to -03	58
B.3.	Version -01 to -02	58
B.4.	Version -00 to -01	59
Acknowledgments		60
Authors' Addresses		60

## 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 it 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., external security applications, or handling of authentication credentials), 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 11.8, 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 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 15 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 15 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 either required to support or not required 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 11.8.

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

- \* The parameter "ed-prof" for web linking [RFC8288] (see Section 3.1 of this document).
- \* The parameter "app\_prof" of the EDHOC\_Information object specified in [I-D.ietf-ace-edhoc-oscore-profile] (see Section 3.2 of this document).



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 11.8 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=0;ed-cred-t=1;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 it has label 23. The integer values are taken from the 'Profile ID' column of the "EDHOC Application Profiles" registry defined in Section 11.8 of this document.

The CDDL grammar describing the parameter "app\_prof" when included in the CBOR-encoded EDHOC\_Information object is:

```
app_prof_parameter = (
  ? 23 => int / [2* int]           ; app_prof
)
```

Figure 3: CDDL Definition of the Parameter "app\_prof" when Included in the CBOR-encoded EDHOC\_Information Object.

### 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 parameter "app\_prof", then the following applies.

- \* In addition to the parameter "app\_prof", 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". 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 parameter "app\_prof" 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-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.

The example in Figure 4 extends the earlier example in Figure 2, by additionally showing the use of the target attributes 'ed-ta-edcred-kid' and 'ed-ta-edcred-x5t'. Compared to the example in Figure 2, the following also applies.

- \* The link to the EDHOC resource at /.well-known/edhoc includes the target attribute 'ed-ta-edcred-kid'. The target attribute has value "AKw", i.e., the base64url-encoded text string of 0x00ac. The latter is the binary key identifier of a trust anchor supported by the server when running EDHOC through that resource.
- \* The link to the EDHOC resource at /edhoc-alt includes the target attribute 'ed-ta-edcred-kid'. The target attribute has value "\_wH\_", i.e., the base64url-encoded text string of 0xff01ff. The latter is the binary key identifier of a trust anchor supported by the server when running EDHOC through that resource.
- \* The link to the EDHOC resource at /edhoc-alt includes the target attribute 'ed-ta-edcred-x5t'. The target attribute has value "gi5IefKkG1EMH5s", i.e., the base64url-encoded text string of 0x822e4879f2a41b510c1f9b. The latter is the binary representation of the COSE\_CertHash [RFC9360] corresponding to an X.509 certificate [RFC5280] that the server supports as a trust anchor when running EDHOC through that resource. In CBOR diagnostic notation, the considered COSE\_CertHash is as follows: [-15, h'79f2a41b510c1f9b'].

```
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=0;ed-cred-t=1;ed-idcred-t=4;
        ed-i;ed-r;ed-comb-req;ed-ta-edcred-kid="AKw",
    </edhoc-alt>;rt=core.edhoc;ed-prof=500;ed-ead=333;
        ed-ta-edcred-kid="_wH_";ed-ta-edcred-x5t="gi5IefKkG1EMH5s"
```

Figure 4: The Web Link.

## 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 11.5 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 advertise\_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 advertise\_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 wish of the Initiator and accordingly advertise the EDHOC application profiles that it supports.

- o If advertise\_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 MUST be present and 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 11.8 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.

When sending EDHOC message\_1, the Initiator might want to include the EAD item "Supported EDHOC application profiles" and not advertise the EDHOC application profiles that it supports, but instead just take advantage of advertise\_flag and ask the Responder to advertise what is supported on its side. In order to do that, the Initiator can compose ead\_value such that, following advertise\_flag, the CBOR sequence APP\_PROF\_SEQ only consists of a single EDHOC\_Information object as an empty CBOR map.

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". 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 and throughout the session, 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 5.

```
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 = [?advertise_flag, APP_PROF_SEQ]

advertise_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 5: CDDL Definition of `ead_value` for the EAD Item "Supported EDHOC application profiles"

Examples of `ead_value` are shown in Section 5.1.3.

#### 5.1.1.1. 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 has received 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 one or more 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 a non-empty 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 a non-empty array, each element of which is an array including two unsigned integers. In CBOR, "exporter\_out\_len" is a non-empty array that has label 22, each element of which is an array including two unsigned integers.

The CDDL grammar describing the parameter "exporter\_out\_len" when included in the CBOR-encoded EDHOC\_Information object is:

```
exporter_out_len = (  
    ? 22 => [1* [uint, uint]]                ; app_prof  
)
```

Figure 6: CDDL Definition of the Parameter "exporter\_out\_len" when Included in the CBOR-encoded EDHOC\_Information Object.

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".

#### 5.1.3. Examples of ead\_value

Figure 7 shows an example in CBOR diagnostic notation of ead\_value for the EDHOC EAD item "Supported EDHOC application profiles", when used in EDHOC message\_1. With reference to the CDDL grammar in Figure 5, the following applies.

The CBOR data item advertise\_flag is present and encodes the CBOR simple value true (0xf5), hence asking the Responder to advertise the EDHOC application profiles that it supports, when replying to the present EDHOC message\_1.

The CBOR sequence APP\_PROF\_SEQ includes the following three elements:

- \* An element profile\_id, specifying the Profile ID of an EDHOC application profile supported by the Initiator. Specifically, that EDHOC application profile is the well-known application profile MINIMAL-CS-2 defined in Section 7.1.
- \* An element profile\_id, specifying the Profile ID of an EDHOC application profile supported by the Initiator. Specifically, that EDHOC application profile is the well-known application profile MINIMAL-CS-0 defined in Section 7.2.
- \* An element EDHOC\_Information, which in turn includes the following parameters:
  - "message\_4", encoded as the CBOR simple value true (0xf5), hence indicating that EDHOC message\_4 is expected in the current EDHOC session.
  - "eads", encoded as a CBOR array. The array includes two elements encoded as unsigned integers, i.e., the EAD labels 500 and 333 of the corresponding EAD items supported by the Initiator.

- "trust\_anchors", encoded as a CBOR map. The map includes a single element with value a CBOR array, which pertains to trust anchors whose purpose is the verification of authentication credentials of other EDHOC peers in an EDHOC session.

In turn, the array includes two CBOR maps. Within the first CBOR map, its entry's value is a CBOR byte string that encodes 0x00ac. Within the second CBOR map, its entry's value is a CBOR byte string that encodes 0xff01ff. Both 0x00ac and 0xff01ff are binary key identifiers of trust anchors supported by the Initiator in the current EDHOC session.

```
<<
true,                / advertise_flag /
e'APP-PROF-MINIMAL-CS-2', / profile_id /
e'APP-PROF-MINIMAL-CS-0', / profile_id /
{                    / EDHOC_Information /
  e'message_4' : true,
  e'eads' : [500, 333],
  e'trust_anchors' : {
    e'edhoc_cred' : [
      { e'kid_ta_type' : h'00ac' },
      { e'kid_ta_type' : h'ff01ff' }
    ]
  }
}
>>
```

Figure 7: Example of ead\_value for the EAD Item "Supported EDHOC application profiles" in EDHOC message\_1

Figure 8 shows an example in CBOR diagnostic notation of ead\_value for the EDHOC EAD item "Supported EDHOC application profiles", when used in EDHOC message\_2. With reference to the CDDL grammar in Figure 5, the following applies.

The CBOR sequence APP\_PROF\_SEQ includes the following two elements:

- \* An element profile\_id, specifying the Profile ID of an EDHOC application profile supported by the Responder. Specifically, that EDHOC application profile is the well-known application profile MINIMAL-CS-2 defined in Section 7.1.
- \* An element EDHOC\_Information, which in turn includes the following parameters:

- "comb\_req", encoded as the CBOR simple value true (0xf5), hence indicating that the Responder supports the EDHOC + OSCORE combined request defined in [RFC9668].
- "eads", encoded as a CBOR array. The array includes two elements encoded as unsigned integers, i.e., the EAD labels 500 and 999 of the corresponding EAD items supported by the Responder.
- "trust\_anchors", encoded as a CBOR map. The map includes a single element with value an inner CBOR map, which pertains to trust anchors whose purpose is the verification of authentication credentials of other EDHOC peers in an EDHOC session.

Within the inner map, its entry's value is a CBOR byte string that encodes 0x91ab, i.e., the binary key identifier of a trust anchor supported by the Responder in the current EDHOC session.

```
<<
e'APP-PROF-MINIMAL-CS-2', / profile_id /
{                               / EDHOC_Information /
  e'comb_req' : true,
  e'eads' : [500, 999],
  e'trust_anchors' : {
    e'edhoc_cred' : { e'kid_ta_type' : h'91ab' }
  }
}
>>
```

Figure 8: Example of ead\_value for the EAD Item "Supported EDHOC application profiles" in EDHOC message\_2

## 5.2. In the EDHOC Error Message

This section defines the error code TBD\_ERROR\_CODE, which is registered in Section 11.6 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 the 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.

#### 5.2.1. Example of ERR\_INFO

Figure 9 shows an example in CBOR diagnostic notation of ERR\_INFO for the EDHOC error message with Error Code TBD\_ERROR\_CODE. With reference to the CDDL grammar in Figure 5, the following applies.

The CBOR sequence APP\_PROF\_SEQ includes the following two elements:

- \* An element profile\_id, specifying the Profile ID of an EDHOC application profile supported by the Responder. Specifically, that EDHOC application profile is the well-known application profile MINIMAL-CS-0 defined in Section 7.2.
- \* An element EDHOC\_Information, which in turn includes the following parameters:

- "comb\_req", encoded as the CBOR simple value true (0xf5), hence indicating that the Responder supports the EDHOC + OSCORE combined request defined in [RFC9668].
- "eads", encoded as a CBOR array. The array includes two elements encoded as unsigned integers, i.e., the EAD labels 500 and 777 of the corresponding EAD items supported by the Responder.
- "trust\_anchors", encoded as a CBOR map. The map includes a single element with value an inner CBOR map, which pertains to trust anchors whose purpose is the verification of authentication credentials of other EDHOC peers in an EDHOC session.

Within the inner map, its entry's value is a COSE\_CertHash [RFC9360] corresponding to an X.509 certificate [RFC5280] that the Responder supports as a trust anchor when running EDHOC.

```
<<
e'APP-PROF-MINIMAL-CS-0', / profile_id /
{
  / EDHOC_Information /
  e'comb_req' : true,
  e'eads' : [500, 777],
  e'trust_anchors' : {
    e'edhoc_cred' : {
      e'x5t_ta_type' : [-15, h'79f2a41b510c1f9b']
    }
  }
}
>>
```

Figure 9: Example of ERR\_INFO for the EDHOC Error Message with Error Code TBD\_ERROR\_CODE

## 6. Advertising Supported EDHOC Application Profiles using DNS SVCB Resource Records

Given a server, its support for EDHOC and for EDHOC application profiles can be advertised using DNS 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 11.7.

- \* "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 10.

- 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 11, 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. The value of the CBOR byte string is the binary representation of the CBOR sequence SVCB\_EDHOC\_APP\_PROF, which is composed of one or two elements as specified below. The SVCB RR MUST be considered malformed if the SvcParamValue ends within edhoc-app-prof-value or if edhoc-app-prof-value is malformed.

- o The first element advertise\_flag is OPTIONAL. If present, it MUST encode the CBOR simple value true (0xf5). If advertise\_flag is present, a peer that runs EDHOC with the server is encouraged to advertise the EDHOC application profiles that it supports, when sending to the server its first EDHOC message in an EDHOC session.

In order to do that, the peer can rely as appropriate on the EDHOC EAD item "Supported EDHOC application profiles" (see Section 5.1) when sending an EDHOC message\_1 or message\_2, or on an EDHOC error message with error code TBD\_ERROR\_CODE (see Section 5.2).

If the peer supports the EDHOC EAD item "Supported EDHOC application profiles" or the error code TBD\_ERROR\_CODE, the peer MUST use those as appropriate to honor the wish of the server and accordingly advertise the EDHOC application profiles that it supports.

- o The second element server\_info is REQUIRED, and it 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 value of each CBOR byte string APP\_BSTR is the binary representation of the 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.

An SVCB RR might not be intended to advertise what EDHOC application profiles a server supports for a given EDHOC resource that it hosts. In such a case, server\_info can be composed such that the CBOR sequence APP\_PROF\_SEQ pertaining to that resource only consists of a single EDHOC\_Information object as an empty CBOR map.

The CDDL grammar describing the CBOR data item edhoc-app-prof-value is shown in Figure 12.

- 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, still specifies the URI paths of EDHOC resources at the server. However, no information is provided about what EDHOC application profiles the server supports.

If the SvcParamKey "edhoc-app-prof" is present in the SVCB RR, then the following applies to server\_info therein.

- \* If the SvcParamKey "edhocpath" is not present in the SVCB RR, then server\_info 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 server\_info 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 specified by the SvcParamKey "edhocpath".



- If the value of the SvcParamKey "edhocpath" is a CBOR array including N elements, then server\_info MUST be a CBOR array including N elements.

The information specified by the i-th element of server\_info 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 10: 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 11: ABNF Definition of path-absolute

```

edhoc-app-prof-value = bytes .cborseq SVCB_EDHOC_APP_PROF

; This defines an array, the elements of which
; are to be used in the CBOR Sequence SVCB_EDHOC_APP_PROF:
SVCB_EDHOC_APP_PROF = [?advertise_flag, server_info]

advertise_flag = bool

server_info = 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 12: CDDL Definition of the Value of the SvcParamKey  
"edhoc-app-prof"

### 6.1. Examples of Wire-Format Values of the SvcParamKeys

Using CBOR diagnostic notation, this section provides examples of wire-format values of the SvcParamKeys "edhocpath" and "edhoc-app-prof", within an SVCB RR corresponding to a given server.

Figure 13 shows an example of the SvcParamKey "edhocpath", with reference to the CDDL grammar in Figure 10.

In the example, two URI paths are specified, i.e., one for the EDHOC resource at `"/.well-known/edhoc"` and one for the EDHOC resource at `"/edhoc-alt"`.

```

[
    / edhocpath-value /
    <<
        ".well-known", / PATH_BSTR /
        "edhoc",       / path_segment /
    >>,
    <<
        "edhoc-alt"    / PATH_BSTR /
        / path_segment /
    >>
]

```

Figure 13: Example of Wire-Format Value of the SvcParamKey  
"edhocpath" within an SVCB RR

Figure 14 shows an example of the SvcParamKey "edhoc-app-prof", with reference to the CDDL grammar in Figure 12. In particular, the following applies.

The CBOR data item `advertise_flag` is present and encodes the CBOR simple value `true` (0xf5), hence indicating that a peer that runs EDHOC with the server is encouraged to advertise the EDHOC application profiles that it supports, when sending to the server its first EDHOC message in an EDHOC session.

The CBOR data item `server_info` is a CBOR array, which includes two CBOR byte strings `APP_BSTR`. In particular:

- \* The value of the first CBOR byte string is the binary representation of a CBOR sequence `APP_PROF_SEQ`, which advertises the EDHOC application profiles that the server supports when running EDHOC through the resource with URI path `"/.well-known/edhoc"`.
- \* The value of the second CBOR byte string is the binary representation of a CBOR sequence `APP_PROF_SEQ`, which advertises the EDHOC application profiles that the server supports when running EDHOC through the resource with URI path `"/edhoc-alt"`.

```

<<                                     / edhoc-app-prof-value /
true,                                / advertise_flag /
[                                     / server_info /
  <<                                 / APP_BSTR /
    e'APP-PROF-MINIMAL-CS-2',        / profile_id /
    e'APP-PROF-MINIMAL-CS-0',        / profile_id /
    {                                 / EDHOC_Information /
      e'message_4' : true,
      e'eads' : [500, 333],
      e'trust_anchors' : {
        e'edhoc_cred' : [
          { e'kid_ta_type' : h'00ac' },
          { e'kid_ta_type' : h'ff01ff' }
        ]
      }
    ]
  }
  >>,
  <<                                 / APP_BSTR /
    e'APP-PROF-MINIMAL-CS-2',        / profile_id /
    {                                 / EDHOC_Information /
      e'comb_req' : true,
      e'eads' : [500, 999],
      e'trust_anchors' : {
        e'edhoc_cred' : { e'kid_ta_type' : h'91ab' }
      }
    ]
  }
  >>
]
>>

```

Figure 14: Example of Wire-Format Value of the SvcParamKey  
"edhoc-app-prof" within an SVCB RR

## 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 11.8 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, Section 7.1]
1	MINIMAL-CS-0	Method 3; Cipher Suite 0; CCS; kid	[RFC-XXXX, Section 7.2]
2	BASIC-CS-2-X509	Methods (0, 3); Cipher Suite 2; (CCS, X.509 certificates); (kid, x5t)	[RFC-XXXX, Section 7.3]
3	BASIC-CS-0-X509	Methods (0, 3); Cipher Suite 0;	[RFC-XXXX, Section



		(CCS, X.509 certificates); (kid, x5t)	7.4]
4	BASIC-CS-2-C509	Methods (0, 3); Cipher Suite 2; (CCS, C509 certificates); (kid, c5t)	[RFC-XXXX, Section 7.5]
5	BASIC-CS-0-C509	Methods (0, 3); Cipher Suite 0; (CCS, C509 certificates); (kid, c5t)	[RFC-XXXX, Section 7.6]
6	INTERMEDIATE-CS-2	Methods (0, 3); Cipher Suite 2; (CCS, X.509/C509 certificates); (kid, kccs, x5t, x5chain, c5t, c5c)	[RFC-XXXX, Section 7.7]
7	INTERMEDIATE-CS-0	Methods (0, 3); Cipher Suite 0; (CCS, X.509/C509 certificates); (kid, kccs, x5t, x5chain, c5t, c5c)	[RFC-XXXX, Section 7.8]
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, Section 7.9]

Table 3: EDHOC Well-known Application Profiles

## 9. Operational Considerations

This section compiles the operational considerations that hold for this document.

### 9.1. Relation with Network Operations

The means defined in this document are largely about aiding peers in running the EDHOC protocol by achieving a common understanding of what they support, thereby facilitating interoperability between EDHOC implementations. Such coordination is expected to keep authenticate key exchange through EDHOC a smooth process in itself and with respect to network operation and management.

The use of these coordinating means in itself is not expected to have a notable impact on performance and network operations, and it is embedded within other relevant network protocols and components such as: the discovery of resources through web-linking [RFC8288] and CoRE Link Format [RFC6690] (see Section 3.1 and Section 4); the execution of the EDHOC protocol itself (see Section 5); and the discovery of server-related information via DNS SVCB RR [RFC9460][RFC9461] (see Section 6).

### 9.2. Source of Data for Network Operators

As further discussed in Section 10, information about what EDHOC application profiles a peer supports could be advertised in plain, depending on the approach specifically used. In such a case, a network operator can passively observe the plain exchange of such information, thereby gaining (a partial) knowledge of EDHOC application profiles that are supported and used in the network.

From the perspective of an individual network operator, this knowledge can be useful for (fine-)tuning the allocation of network resources.

Multiple, cooperating network operators could build an aggregated knowledge that indicates broad "trends" about EDHOC application profiles and their use. This raises awareness of what appears to be most supported and preferred by EDHOC peers, which can influence priority decisions about the development and use of EDHOC implementations, as well as the operations of infrastructures for provisioning and validating public authentication credentials.

As noted in Section 7, well-known EDHOC application profiles are not meant to be default profiles to use, and they are not meant to deviate from the EDHOC compliance requirements compiled in Section 8 of [RFC9528]. Instead, they are meant to reflect what is most common and expected to be supported by EDHOC peers. Hence, developing aggregated knowledge on typical uses of EDHOC can help identifying EDHOC application profiles that have become de facto well-known, thereby further accelerating their adoption.

### 9.3. Logging and Reporting

When using the means defined in this document, EDHOC peers are not expected to keep any particular log of such use, or to go beyond expectations already in place as to the logging of EDHOC sessions. However, when gaining knowledge about what EDHOC application profiles are supported by a given EDHOC peer, it is encouraged to locally preserve that knowledge for a non-negligible amount of time determined by the application. Especially under the assumption that what EDHOC peers support does not (often) change, this avoids the need to repeatedly re-gain the same knowledge at least in the short term.

If an EDHOC session fails due to an apparent mismatch with gained knowledge about commonly supported EDHOC application profiles, a peer can report such a failure to a network manager or infrastructure operator. This can help identify peers whose behavior deviates from what is advertised in terms of EDHOC application profiles that they allegedly support. In turn, this can be used to detect misbehaving peers, outdated information about what peers support, or ongoing tampering of such information if that is advertised in plain (see Section 10).

It is out of the scope of this document what specific semantics and data model are used for producing and processing such reports. Specific semantics and data models can be defined by applications and future specifications.

## 10. Security Considerations

The security considerations compiled in Section 9 of [RFC9528] hold for this document. The security considerations compiled in Section 7 of [RFC9668] also apply, when EDHOC is transported over CoAP [RFC7252] and specifically when using the EDHOC + OSCORE request defined in Section 3 of [RFC9668].

Instances of the EDHOC\_Application\_Profile objects (see Section 2) ought to be accepted only if provided by an identifiable, trusted party by using secure communication. When this is not the case, an EDHOC peer can be induced to: erroneously identify a given EDHOC application profile with a wrong Profile ID; erroneously believe a given EDHOC application profile to exist in the first place; develop a wrong understanding of what a given EDHOC application profile consists of.

Different security guarantees can be achieved about the acquired information on the EDHOC application profiles supported by a given peer, depending on the specific approach used. The potential consequences of acquiring such information in a non secured way are discussed later in this section.

- \* With respect to using web linking (see Section 3.1 and Section 4), the security considerations in Section 5 of [RFC8288] apply. When specifically relying on CoRE Link Format [RFC6690], the security considerations in Section 6 of [RFC6690] also apply.

Clearly, the discovery of EDHOC resources at a server is intended to happen before running EDHOC with the server. At that point in time, the peer attempting to discover EDHOC resources at the server is unlikely to already have a secure communication association with the server. Therefore, the discovery process is likely to use unsecured communication.

Alternatively, EDHOC resources at a server can be discovered by securely interacting with separate discovery services, e.g., by using the CoRE Resource Directory [RFC9176].

- \* With respect to using the EDHOC EAD item "Supported EDHOC application profiles" (see Section 5.1), the following applies.
  - When the EAD item is included in EDHOC message\_1, the information conveyed therein is not protected. However, changing EDHOC message\_1 in transit (e.g., by adding, removing, or modifying the EAD item) would result in the Initiator aborting the EDHOC session, after receiving and failing to verify EDHOC message\_2.
  - When the EAD item is included in EDHOC message\_2, the information conveyed therein is protected by EDHOC.
- \* With respect to using an EDHOC error message with error code TBD\_ERROR\_CODE, the information conveyed in ERR\_INFO is not protected, just like when any other error code is used.
- \* With respect to using the SvcParamKeys "edhocpath" and "edhoc-app-prof" within an SVCB RR (see Section 6), the security considerations from Section 12 of [RFC9460] and Section 8 of [RFC9461] apply.

It is encouraged that DNS is used with secure communication. Known threats for unprotected DNS are described in [RFC3833] and [RFC9076].

In case information about EDHOC application profiles supported by a peer is distributed in an unprotected way (e.g., through unsecured communication), a consumer should treat such information as a hint.

If the acquired information has been tampered with and does not reflect what a given peer supports and intends to advertise, this can set wrong expectations about what is effectively possible to do when running EDHOC with that peer. Although this can still result in successfully running EDHOC with a configuration that is commonly supported, such configuration would probably not have been selected, had reliable information been acquired. In the worst case, there might be the erroneous belief that there is not sufficient shared support with that peer.

What is discussed above does not have an impact on the security of the EDHOC protocol in itself. That is, even when the available information about supported EDHOC application profiles is not guaranteed to be reliable, the successful completion of an EDHOC session still provides the security guarantees that are expected as per the way the session was run (e.g., based on the selected cipher suite and EDHOC method used).

## 11. 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.

### 11.1. 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 10 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

#### 11.2. 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]

#### 11.3. 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-prof

- \* Brief Description: A supported EDHOC application profile
  - \* Change Controller: IETF
  - \* Reference: [RFC-XXXX, Section 3.1]
- 
- \* 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, Section 4]
- 
- \* 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, Section 4]
- 
- \* 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, Section 4]
- 
- \* 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, Section 4]
  
- \* 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, Section 4]
  
- \* 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, Section 4]

#### 11.4. 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]

#### 11.5. 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, Section 5.1]

#### 11.6. 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, Section 5.2]

#### 11.7. DNS SVCB Service Parameter Keys (SvcParamKeys)

IANA is asked to add the following entries to the "DNS SVCB 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, Section 6]
- 
- \* Number: 12 (suggested)
  - \* Name: edhoc-app-prof
  - \* Meaning: Supported EDHOC application profiles
  - \* Change Controller: IETF
  - \* Reference: [RFC-XXXX, Section 6]

#### 11.8. 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 11.9.

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.

#### 11.9. 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 objectives 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.

## 12. References

### 12.1. 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 $\ddot{u}$ 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-10, 1 March 2026, <<https://datatracker.ietf.org/doc/html/draft-ietf-ace-edhoc-oscore-profile-10>>.

[I-D.ietf-cose-cbor-encoded-cert]

Mattsson, J. P., Selander, G., Raza, S., Håglund, J., and M. Furuheid, "CBOR Encoded X.509 Certificates (C509 Certificates)", Work in Progress, Internet-Draft, draft-ietf-cose-cbor-encoded-cert-16, 25 January 2026, <<https://datatracker.ietf.org/doc/html/draft-ietf-cose-cbor-encoded-cert-16>>.

[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>>.

## 12.2. 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>>.
- [RFC3833] Atkins, D. and R. Austein, "Threat Analysis of the Domain Name System (DNS)", RFC 3833, DOI 10.17487/RFC3833, August 2004, <<https://www.rfc-editor.org/rfc/rfc3833>>.
- [RFC9076] Wicinski, T., Ed., "DNS Privacy Considerations", RFC 9076, DOI 10.17487/RFC9076, July 2021, <<https://www.rfc-editor.org/rfc/rfc9076>>.
- [RFC9176] Amss, C., Ed., Shelby, Z., Kostner, M., Bormann, C., and P. van der Stok, "Constrained RESTful Environments (CoRE) Resource Directory", RFC 9176, DOI 10.17487/RFC9176, April 2022, <<https://www.rfc-editor.org/rfc/rfc9176>>.
- [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
message_4 = 3
comb_req = 4
cred_types = 6
id_cred_types = 7
eads = 8
trust_anchors = 11
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 Trust Anchor Purposes
edhoc_cred = 0

; EDHOC Trust Anchor Types
kid_ta_type = 4
x5t_ta_type = 34

; EDHOC Authentication Credential Types
c509_cert = 3
```

Figure 15: CDDL model



## Appendix B. Document Updates

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

### B.1. Version -03 to -04

- \* Removed parameters that were removed from draft-ietf-ace-edhoc-oscore-profile.
- \* Renamed "reply\_flag" to "advertise\_flag".
- \* Defined use of "advertise\_flag" also in SVCB Resource Records.
- \* Added guidelines on using the EAD item "Supported EDHOC application profiles" only to take advantage of advertise\_flag.
- \* Added guidelines on having per-resource empty advertisements in an SVCB RR.
- \* Clarifications:
  - Deviations from prescriptive parameters are assessed throughout the whole EDHOC session.
- \* CDDL definitions:
  - Added CDDL definitions of the parameters "app\_prof" and "exporter\_out\_len" for the CBOR-encoded EDHOC\_Information object.
  - Fixed CDDL definition of ead\_value of the EAD item "Supported EDHOC application profiles".
- \* Added new examples:
  - Response in CoRE link-format using the target attributes 'ed-ta-edcred-\*'.
  - ead\_value for the EDHOC EAD item "Supported EDHOC application profiles".
  - Added examples of wire-format values of the SvcParamKeys "edhocpath" and "edhoc-app-prof".
  - ERR\_INFO for the EDHOC error message with Error Code TBD\_ERROR\_CODE.
- \* Added "Operational Considerations" section.

- \* Added security considerations.
- \* Editorial fixes and improvements.

#### B.2. 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.3. 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.4. 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 Amssss, 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