# Coordinating the Use of Application Profiles for Ephemeral Diffie-Hellman Over COSE (EDHOC)

*draft-tiloca-lake-app-profiles-00*

**Marco Tiloca, RISE**
Rikard Höglund, RISE

IETF 118 Meeting – Prague – November 6th, 2023

# Motivation

- **Peers have to agree about how to run EDHOC and on certain parameters**
  - Some are exchanged during the protocol execution, when a few can be negotiated

- **In general, two peers have to rely on an EDHOC application profile, specifying:**
  - The intended use of EDHOC, including relevant processing and verification
  - Parameters for the EDHOC execution, both in-band and out-of-band ones

- **How to facilitate the definition, discovery, and use of EDHOC application profiles?**
  - Related points first raised during the WG Last Call of *draft-ietf-core-oscore-edhoc*
  - Agreed that it was better to address this topic in the LAKE WG

- **Also in the latest WG Charter:** *The working group will also work on a Standard Track means for coordinating the use and discovery of EDHOC application profiles, the definition of a well-known application profile …*

# Contribution

- **Definition of integer identifiers of EDHOC application profiles**
  - Supported by a new, dedicated IANA registry for profile identifiers
- **Identification of EDHOC application profiles by their integer ID**
  - In a Web Link, e.g., in Link-Format through a target attribute when CoAP is used
  - In a descriptive object, e.g., in the EDHOC_Information object defined in [1]
- **Canonical description of EDHOC application profiles at specification time**
  - As a CBOR-item; applicable to definition, distribution, and storage of application profiles
- **Definition of one or more "well-known" EDHOC application profiles**
  - Reflecting the most common, expected way(s) to use EDHOC



[1] https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/

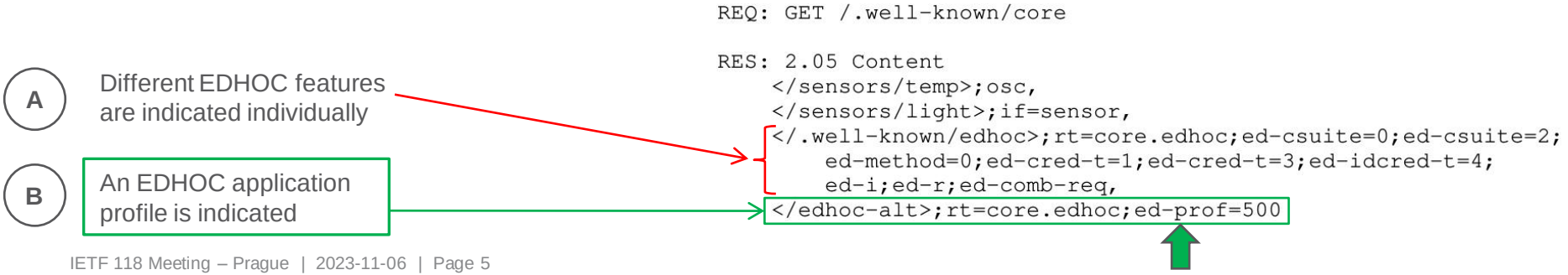
# 1. Profile identifiers

- **New IANA registry "EDHOC Application Profiles"**
  - Profile ID: unique integer value
    - Different ranges with different registration policies
    - [-24..23] are "Standards Action with Expert Review"
    - [-65536..-25] and [24..65535] are "Specification Required"
    - Smaller than -65536 and greater than 65535 are "Private Use"
  - Name: profile name
  - Description: profile short description
  - Reference: document specifying the profile

# 2. Identification of profiles #1

- **Discovery through Web Linking**
  - When using CoAP, a link-format document (RFC 6690) can have links to EDHOC resources
    - *draft-ietf-lake-edhoc* already defines the resource type rt="core.edhoc"

- **Defined a new target attribute 'ed-prof' for such links**
  - To be registered in the "Target Attributes Registry", see *draft-ietf-core-target-attr*
  - Value taken from the 'Profile ID' column of the new "EDHOC Application Profiles" registry
  - It can occur multiple times in the same link → Multiple application profiles are supported



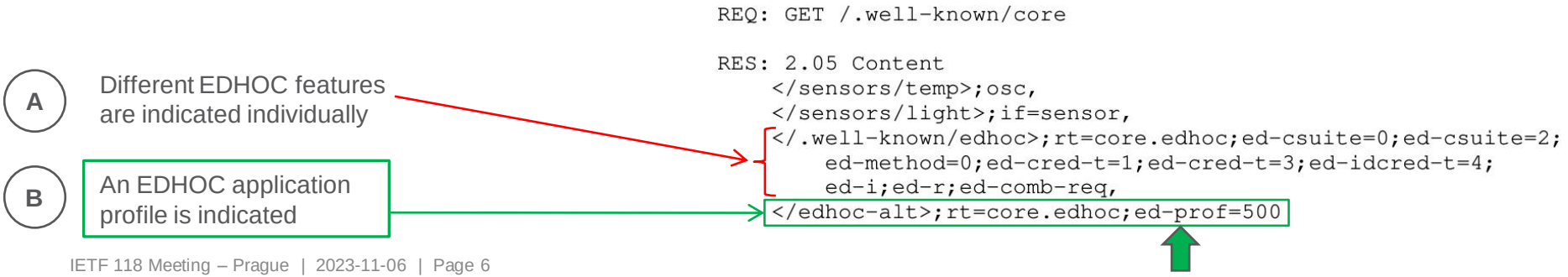
# 2. Identification of profiles #1

- **At the moment, the draft says:**

  *If a link to an EDHOC resource includes occurrences of the target attribute 'ed-prof', the link MUST NOT include other target attributes that provide information pertaining to an EDHOC application profile (see, e.g., Section 6 of [I-D.ietf-core-oscore-edhoc]), which, if present, MUST be ignored by the recipient.*

- **That is, do NOT mix approach A and approach B in the same link!**

- **Open point: admit both 'ed-prof' AND 'ed-ead' indicating supported EAD items?**
  - If not, possible many registration requests for similar profiles, differing only in the supported EAD items



# 2. Identification of profiles #2

- **[1] defines the EDHOC_Information object and the "EDHOC Information" IANA registry**
  - In general, the object informs two peers about how to run EDHOC with one another
  - In particular, it is also used in the ACE workflow considered in [1]
  - Initial set of parameters also defined in [1]

- **This document defines new parameters for the EDHOC_Information object**
  - 'cred_types', 'id_cred_types', 'eads', 'initiator', 'responder', 'app_prof'
  - 'app_prof' is an integer or an array of integers; it corresponds to the target attribute 'ed-prof'
    - Values: identifiers taken from the new "EDHOC Application Profiles" registry

- **Section 3.1 defines how to use the 'app_prof' specifically in [1]**
  - Text temporarily included here, to avoid inconsistencies with [1] around the cut-off
  - This text belongs to [1]; plan to move it to [1] for the next iteration of both documents
  - It is worth moving to [1] also the newly defined parameters, except for 'app_prof'



[1] https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/

# 3. Canonical description

- **EDHOC_Application_Profile object, as a CBOR map**
  - Defined also a Media Type – Encoding: CBOR Sequence of CBOR maps
- **Possible entries (i.e., considered namespace)**
  - Same of the EDHOC_Information_Object defined in [1]
  - Reuse CBOR abbreviations of map keys from the same “EDHOC Information” registry
- **The following entries MUST be present**
  - ‘app_prof’, identifying the profile in question
  - ‘methods’ and ‘cred_types’
- **The following entries MUST NOT be present**
  - ‘session_id’ and ‘uri_path’
- **Other entries can be present**

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

*(The draft wrongly says “9 => int“ ; to be fixed in v -01)*



[1] https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/

# 3. Canonical description

- **Other information is expected from an EDHOC application profile**

- **Type(s) of endpoint identifiers (e.g., EUI-64)**
  - New parameter for this? New registry for the type of endpoint identifiers?

- **Transport(s) to use for EDHOC**
  - How to indicate this?
  - Different transports may require to indicate additional, specific information
  - Indicate a “transport suite”? New registry for suite identifiers and transport-specific detail?

- **More in general, what should/may application profiles specify?**

# 4. Well-known application profile

- **This section has just Editor's notes at the moment**

- **What "well-known profile" does NOT mean**
  - It is a "default profile" to use if nothing else is said
    - That is, it overrides the EDHOC specification on what is mandatory to implement
  - It is necessarily supported by the /.well-known/edhoc resource if nothing else is said

- **What does "well-known profile" mean?**
  - Authors' understanding: reflecting what is most common and expected to use

- **In general, what should a well-known EDHOC application profile specify?**

# Summary and next steps

- **Means to assist the discovery and use of EDHOC application profiles**
  - Definition of integer identifiers of EDHOC application profiles
  - Identification of EDHOC application profiles by their integer ID
  - Canonical description of EDHOC application profiles
  - Definition of one or more “well-known” EDHOC application profiles

- **Plan for the next version**
  - Move Section 3.1 into [1], as specific to that document
  - Definition of EDHOC application profiles
    - Clarify what they may and should specify
    - Clarify how some of its parts are specified (e.g,. peer identifier type; transport to use)
  - Understand what a well-known profile should specify

- **Reviews and input are welcome!**



[1] https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/

# Thank you!

https://gitlab.com/crimson84/draft-tiloca-lake-app-profiles