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

draft-ietf-lake-app-profiles-01

Marco Tiloca, RISE
Rikard Höglund, RISE

IETF 122 Meeting – Bangkok – March 18th, 2025

Recap

- **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 <u>EDHOC application profile</u>, specifying:**
  - The intended use of EDHOC, also as to relevant processing and verification
  - Parameters for the EDHOC execution, both in-band and out-of-band ones

- **Scope: facilitate the definition and discovery of EDHOC application profiles to use**
  - Numeric identifiers of application profiles, and related new IANA registry
    - Value of the new target attribute “ed-prof” for web links
    - Value of the new parameter “app_prof” in the EDHOC_Information object [1]
  - Target attributes for web links, one per supported “feature” of an application profile
  - An EAD item and an EDHOC error code, for advertisement in EDHOC messages ***NEW***
  - EDHOC_Application_Profile object, as a CBOR-based canonical representation
  - Set of well-known application profiles to be registered

[1] *draft-ietf-ace-edhoc-oscore-profile*

Updates since IETF 121

- **Internet Draft adopted as WG Document**

- **Editorial fixes**
  - Updated references, clearer phrasing, ...
  - s/ed-<u>idep</u>-t/ed-<u>epid</u>-t (EDHOC-Endpoint-ID-Type)
  - Content-Format abbreviated as “ct” (not as “cf”)

- **Comments from Michael Richardson during WG Adoption – Thanks!**
  - Make the motivation clearer in the abstract and introduction
    - Facilitate interoperability between EDHOC implementations
    - Support EDHOC extensibility for additional integrations
      - External security applications, handling of authentication credentials, …
  - Don’t use “WK-” when naming the well-known application profiles
    - Fixed in Section 6 – E.g., changed WK-MINIMAL-CS-2 to MINIMAL-CS-2

Updates since IETF 121

- **Section 2.0 – Early overview of <u>where</u> a profile identifier can appear**
  - Value of the new “ed-prof” target attribute (see Section 2.1)
  - Value of the new “app_prof” parameter of the EDHOC_Information object (see Section 2.2)
  - In certain EDHOC message fields (see Section 4) ***NEW***
  - In the EDHOC_Application_Profile object (see Section 5)

- **Section 2.2 – CBOR integer abbreviation of “app_prof”**
  - Multiple updates in the past, due to more abbreviations added in the same namespace
  - Now set to <u>23</u> – Last value in the short-size range of unsigned integers

- **Section 5 – Ignore unexpected parameters in the EDHOC_Application_Profile object**
  - Some parameters must not be present, as they are meaningless
  - Now defined that the recipient must ignore them if present anyway

Updates since IETF 121

- **Positioning of parameters for the EDHOC_Information object [1]**
  - "max_msgsize"
  - "coap_ct"
  - "ep_id_types"
  - "transports"

  Definition and IANA considerations have been moved to [1]

  - "app_prof" .... Definition and IANA considerations are kept in this document

- **Corresponding link target attributes**
  - "ed-max-msgsize"
  - "ed-coap-ct"
  - "ed-epid-t"
  - "ed-tp"
  - "ed-prof"

  Definition and IANA considerations are kept in this document

[1] *draft-ietf-ace-edhoc-oscore-profile*

Updates since IETF 121

- **A new parameter for the EDHOC_Information object has been defined in [1]**
  - “trust_anchors”, enforcing a feature originally proposed in [2]
    - Identifiers of supported Trust Anchors (e.g., certificates of CAs)
      - Different possible purposes, e.g., verifying EDHOC peers’ authentication credentials
    - Set of type-value pairs. Current types can be: UUID, kid, c5t, c5u, x5t, x5u
    - Definition and IANA considerations are in [1]

- **Corresponding link target attributes**
  - “ed-ta-edcred-uuid”
  - “ed-ta-edcred-kid”
  - “ed-ta-edcred-c5t”
  - “ed-ta-edcred-c5u”
  - “ed-ta-edcred-x5t”
  - “ed-ta-edcred-x5u”

Definition and IANA considerations are in this document

[1] *draft-ietf-ace-edhoc-oscore-profile*
[2] *draft-serafin-lake-ta-hint*

Updates since IETF 121

- **<u>Means for advertising</u> EDHOC capabilities and application profiles**
  a) EDHOC_Application_Profile object
     - CBOR abbreviations from the same namespace of the EDHOC_Information object [1]
  b) EDHOC_Information object [1]
  c) Target attributes for Web Linking

  Specify either:
  - Supported individual EDHOC features;
  OR
  - Supported application profiles identified by ID, possibly with additional supported EAD items

  … … … … … …

- **New means: EDHOC messages!**
  – EDHOC message_1 and message_2, through a new EAD item
  – EDHOC error message, when replying to EDHOC message_1
  – Same information used in (b), with abbreviations from the same namespace
  – The EDHOC peer sending the message describes what it supports

[1] *draft-ietf-ace-edhoc-oscore-profile*

Updates since IETF 121

- **EAD item, in EDHOC message_1 or message_2**
  - ead_label > 0 → Used only in the non-critical way
  - ead_value : CBOR byte string wrapping a CBOR sequence

- **In the EAD item value, each element of the sequence can be:**
  - A CBOR integer identifying an EDHOC application profile
  - A CBOR array of at least two integers:
    - First one: identifier of an EDHOC application profile
    - Following ones: EAD labels of supported EAD items
  - A CBOR EDHOC_Information object [1]
    - Not including "session_id" or "app_prof"

```
ead_value = << APP_PROF_SEQ >>

; 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
```

- **EDHOC error message, in reply to EDHOC message_1**
  - ERR_CODE: new registered value
  - ERR_INFO: same semantics of the ead_value above
  - Appropriate only if EDHOC fails in the first place and no other ERR_CODE is more pertinent

[1] *draft-ietf-ace-edhoc-oscore-profile*

Open points

- **How should the recipient handle misplaced information?**

1. **New EAD item included in EDHOC message_3 or message_4 (now forbidden)**
   - That’s too late to be useful in the present EDHOC session
   - Should the recipient silently ignore the EAD item?

2. **New EAD item included multiple times in the EDHOC field (now forbidden)**
   - Should the recipient silently ignore the EAD item after the first instance?

3. **In the EAD item or error message, an element of the CBOR sequence if malformed**
   - Should the recipient silently ignore that element and continue?

- **The EDHOC_Application_Profile object is defined in CBOR only**
  - Do we need to define it also in JSON?

Next steps

- **Add examples**
  - In link format, e.g., when using the ed-ta-edcred-* target attributes
  - In CBOR diagnostic notation, e.g., when using the new EAD item and EDHOC error message
- **Update the list of well-known application profiles?**
  - The current set is just an initial proposal; we need feedback
- **Any information that application profiles cannot effectively specify?**
- **Additional “advertisement venues” where EDHOC-related information can be placed?**
- **Security considerations**
  - E.g., one point from Michael Richardson: “… need to be very clear about when communications/tampering of the application profile could result in an attack.”
- **Comments and feedback are welcome!**

Thank you!

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