Since IETF 115

— edhoc-18
  — Final wrap up from WGLC
— edhoc-19
  — Directorate reviews (secdir, intdir, tsvart, genart)
  — Shepherd review and Stephen’s pre-last call review

As always, details in https://github.com/lake-wg/edhoc
Summary: edhoc-17 → edhoc-18

— Padding realised as EAD, with ead_label=0, PAD field removed
— EAD syntax revised, ead_value is now optional
— Clarifications:
  — Identifier representation, authentication credential, RPL, encoding of ID_CRED with key, representation of public keys,
  — y-coordination of ephemeral key and validation
  — Processing after completed protocol
  — Making verifications available to the application
  — Relation between EDHOC and OSCORE identifiers
— Terminology alignment: session / protocol; discontinue / terminate
— Updated CDDL
— Additional unicode encodings in the document
— Large number of nits from WGLC

```python
ead = (
    ead_label : int,
    ? ead_value : bstr,
)
```

<table>
<thead>
<tr>
<th>EDHOC  \ OSCORE</th>
<th>Sender ID</th>
<th>Recipient ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiator</td>
<td>C_R</td>
<td>C_I</td>
</tr>
<tr>
<td>Responder</td>
<td>C_I</td>
<td>C_R</td>
</tr>
</tbody>
</table>
Summary: edhoc-18 ➔ edhoc-19

- No impact on wire format
- Clarifications:
  - Relation to SIGMA, role of Static DH, Initiator and Responder roles, construction of SUITES_I, cipher suite negotiation example, message processing, padding, ead processing, long PLAINTEXT_2 processing
  - Message correlation in new subsection, appendix H removed
  - Transport properties
  - Terminology, notation, captions, language, acknowledgements, etc.
  - Updated IANA section with registration procedures

- Clarifying normative text in Appendix A
  - Normative text in OSCORE processing
  - Naming the two EDHOC over CoAP cases as “forward”/“reverse” message flow

- Updated list of security analysis papers
- New appendix with example state machine
- New and updated references
New Appendix: State Machine Example

**Initiator State Machine**

- **START**
  - Send message_1
  - Receive error → **WAIT_M2**
    - Processing error → **RCVD_M2**
      - Verify message_2
      - Send message_3
      - (Receive error) → **COMPLETED**
        - (Receive message_4)
        - (Processing error) → **RCVD_M4**
          - (Verify application message)
          - **PERSISTED**

**Responder State Machine**

- **START**
  - Receive message_1
  - Processing error → **RCVD_M1**
    - Verify message_1
    - Processing error → **VRFD_M1**
      - Send message_2
      - Receive error → **WAIT_M3**
        - Receive message_3
        - Processing error → **RCVD_M3**
          - Verify message_3
          - (Processing error) → **COMPLETED**
            - (Send message_4)
            - **PERSISTED**
Appendix A.2 EDHOC over CoAP

“The use of CoAP or OSCORE with EDHOC is optional, but if you are using CoAP or OSCORE, then certain normative requirements apply as detailed in the subsections.”

Figure 18: Example of the forward message flow.

Figure 19: Example of the reverse message flow.
IANA considerations

<table>
<thead>
<tr>
<th>Range</th>
<th>Registration Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>-65536 to -25</td>
<td>Specification Required</td>
</tr>
<tr>
<td>-24 to 23</td>
<td>Standards Action with Expert Review</td>
</tr>
<tr>
<td>24 to 65535</td>
<td>Specification Required</td>
</tr>
</tbody>
</table>

These registration procedures apply for:
- Methods
- Error Codes
- EAD (should be only non-negative integers)
- Cipher suites (-21, -22, -23, -24 for private use)

23 is reserved in all registers
Next steps

— AD review
— IETF Last Call
— Submit updated version of -traces