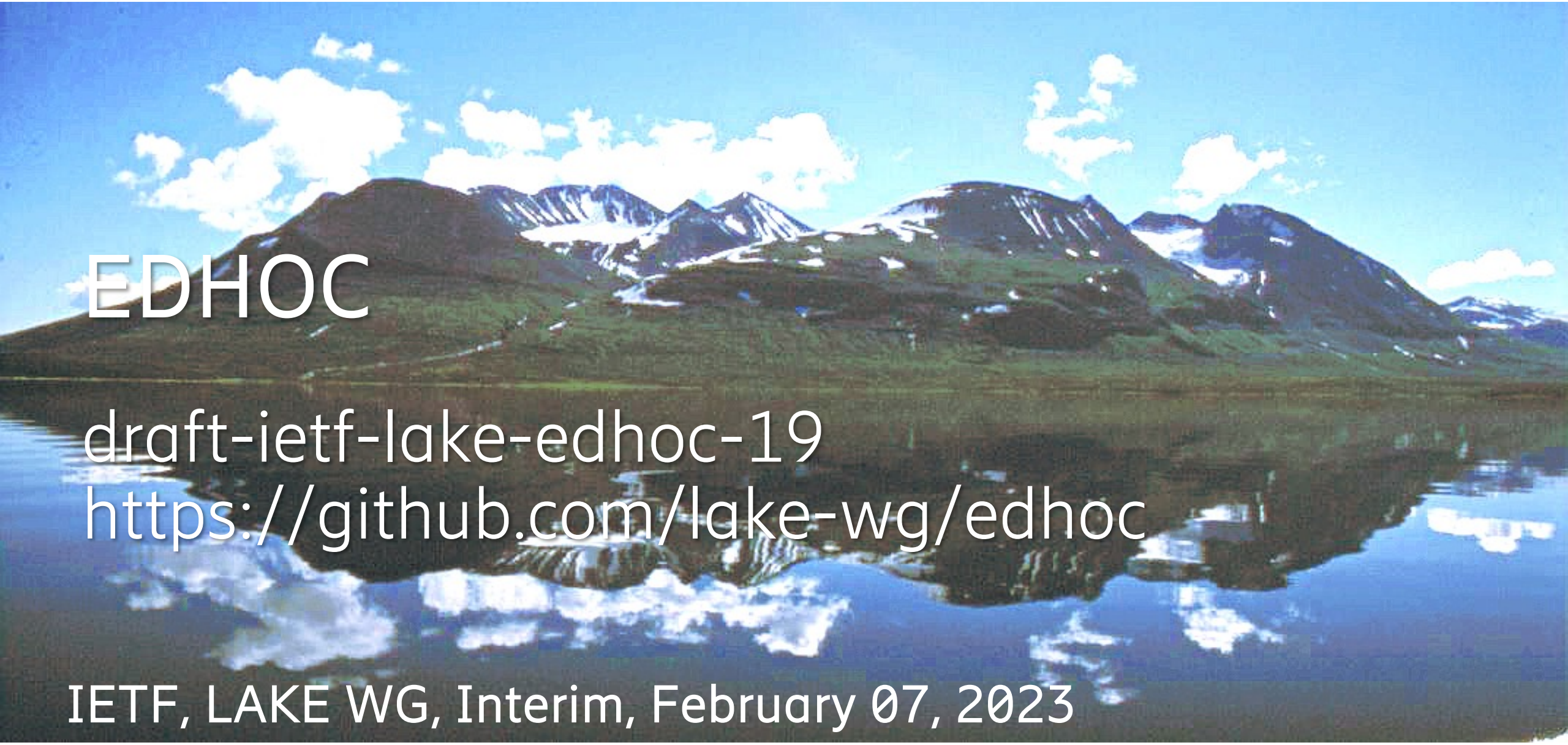


EDHOC

draft-ietf-lake-edhoc-19
https://github.com/lake-wg/edhoc

IETF, LAKE WG, Interim, February 07, 2023

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

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

EDHOC \ OSCORE	Sender ID	Recipient ID
Initiator	C_R	C_I
Responder	C_I	C_R

Summary: edhoc-18 → edhoc-19

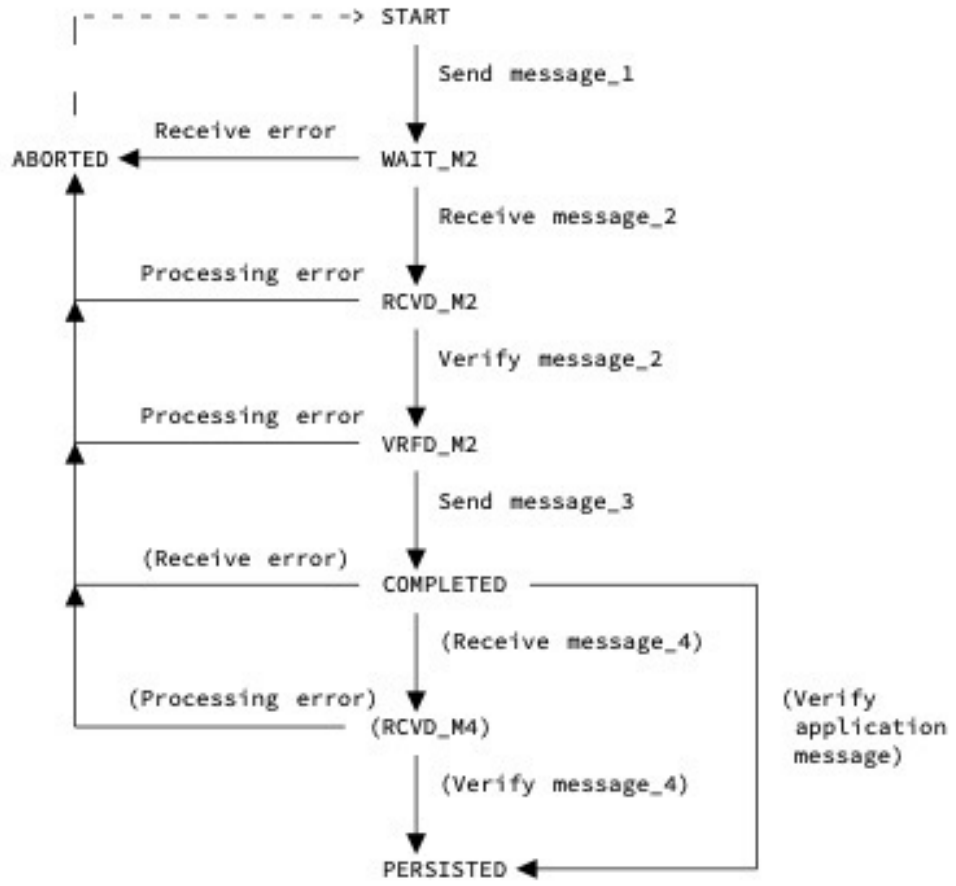
- No impact on wire format
- Clarifications:
  - Relation to SIGMA, role of Static DH, Initiator and Responder roles, construction of SUITES_I, cipher suite negotiation example, message processing, padding, ead processing, long PLAINTEXT_2 processing
  - Message correlation in new subsection, appendix 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

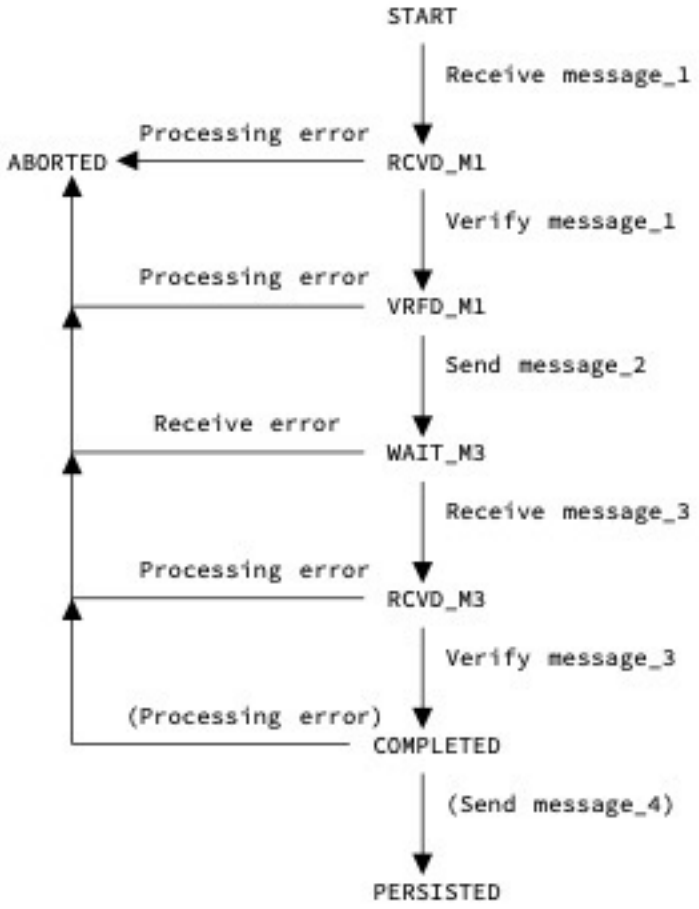
- Updated list of security analysis papers
- New appendix with example state machine
- New and updated references

New Appendix: State Machine Example

Initiator State Machine



Responder State Machine



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."

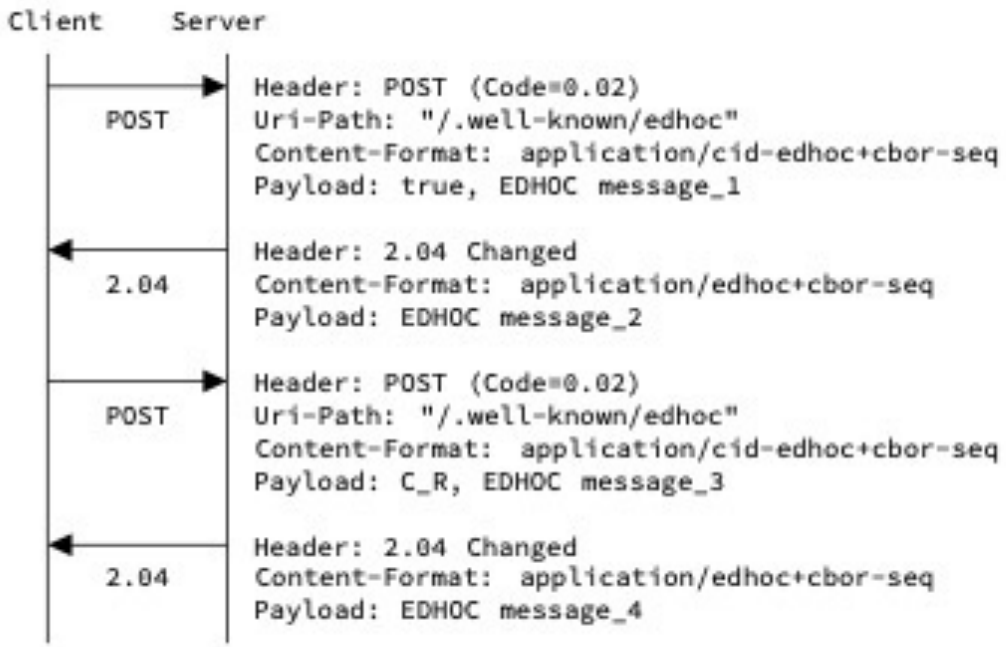


Figure 18: Example of the forward message flow.

Figure 19: Example of the reverse message flow.

IANA considerations

Range	Registration Procedures
-65536 to -25	Specification Required
-24 to 23	Standards Action with Expert Review
24 to 65535	Specification Required

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

EDHOC_Exporter label registration

Label	Description	Reference
0	Derived OSCORE Master Secret	[[this document]]
1	Derived OSCORE Master Salt	[[this document]]
2-22	Unassigned	
23	Reserved	[[this document]]
24-32767	Unassigned	
32768-65535	Private Use	

Figure 13: EDHOC Exporter Label

Range	Registration Procedures
0-23	Standards Action
24-32767	Expert Review

Next steps

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