Lightweight Authorization using EDHOC

https://datatracker.ietf.org/doc/**draft-ietf-lake-authz** (diff)

Geovane Fedrecheski, Inria

editorial updates

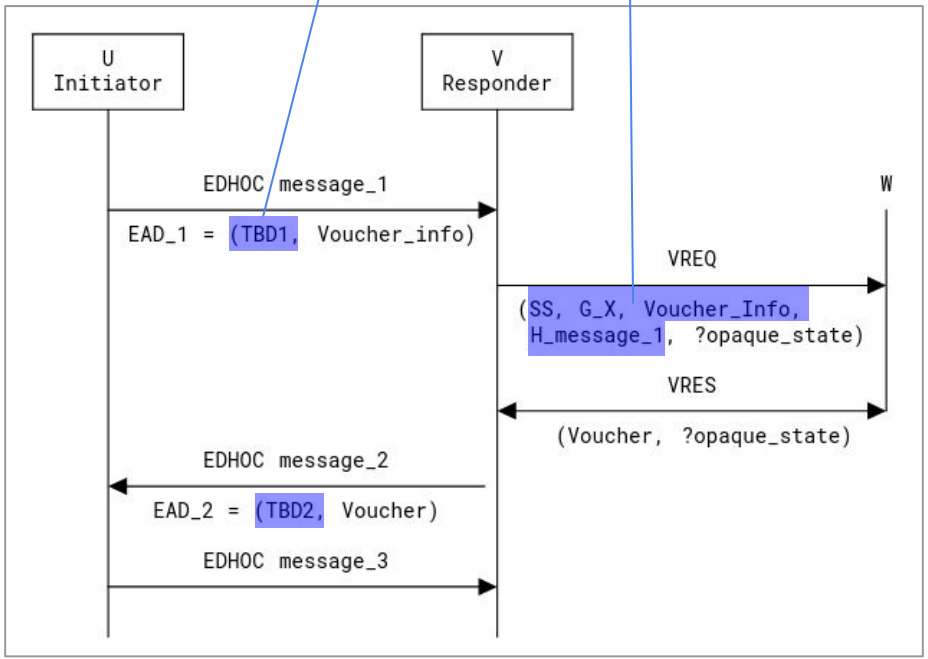
- Mention 'SS' as selected cipher suite in more places #47
- Fix typos and improve sentences #50
- Acknowledge partial funding from EU's OpenSwarm project #44
- Move optimization and advertisement sections to appendix #48

New Section: *4.8. ELA Reverse flow with U as Responder*

- issue #21: authz with U as R and V as I
- previous discussions included EDHOC reverse flow
  - not exactly what we need
  - we simply need “U as R”
  - EDHOC in reverse flow is orthogonal…
- so, new section for “U as R”, described as diff

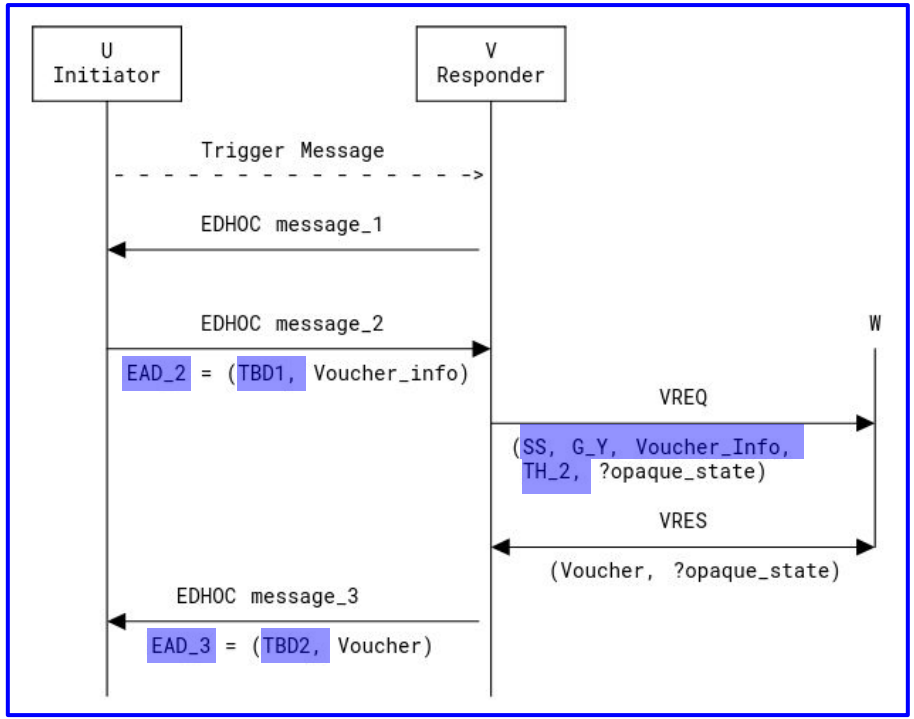
New Section: *4.8. ELA Reverse flow with U as Responder*

disambiguate / generalize



ELA default flow

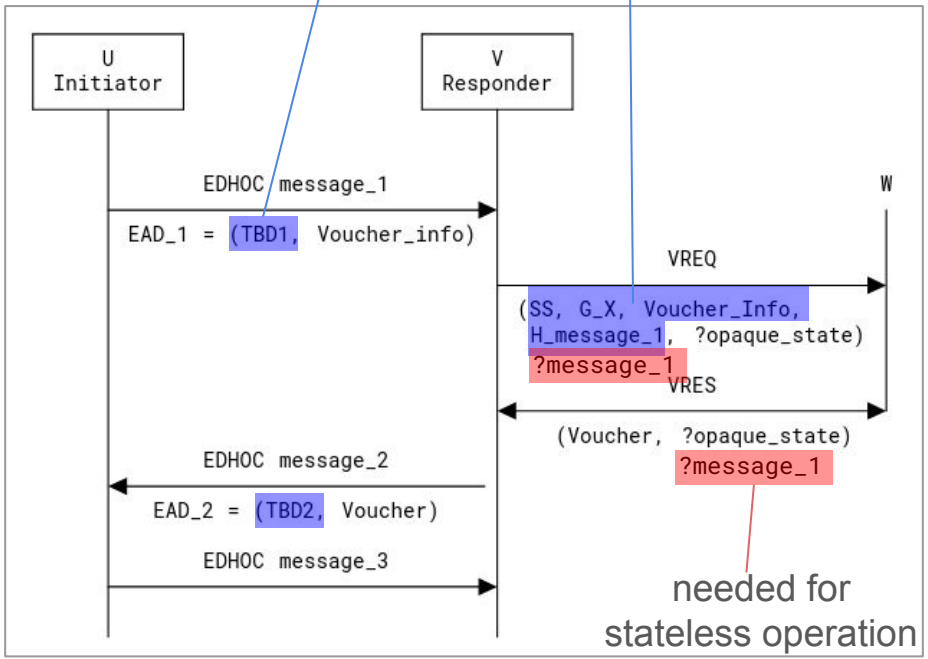
⬇️ new section, described as diff



ELA reverse flow

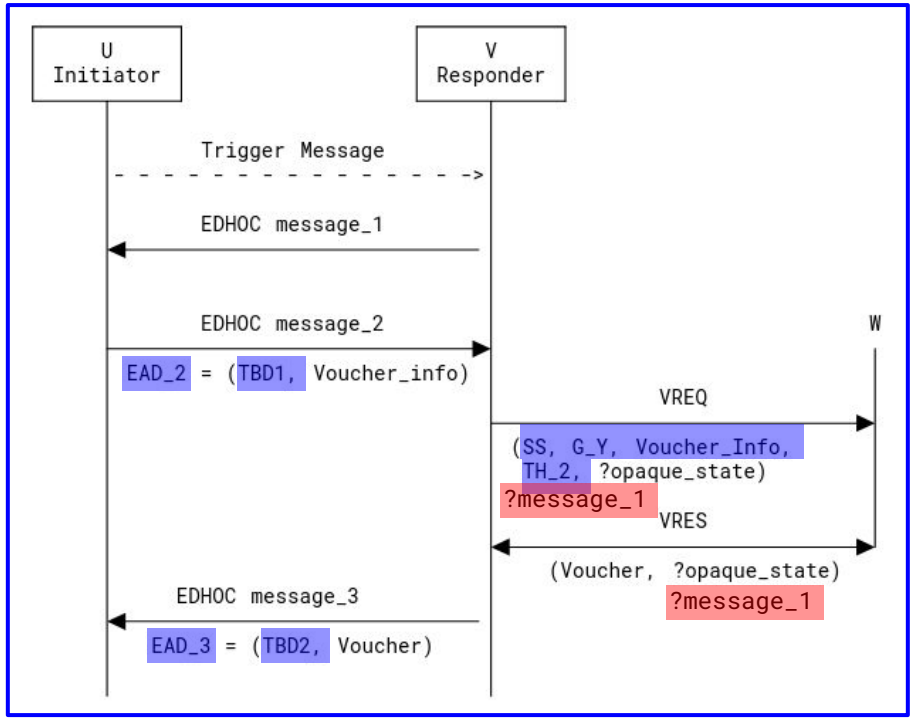
New Section: *4.8. ELA Reverse flow with U as Responder*

disambiguate / generalize



ELA default flow

⬇️ new section, described as diff



ELA reverse flow

New Section: *4.8. ELA Reverse flow with U as Responder*

- W is agnostic about default / reverse flow.
- W uses generic parameters G_U and H_handshake
  - regular flow: G_X, H_message_1
  - reverse flow: G_Y, TH_2

```
Voucher_Request = [
    SS:              int,
    G_U:             bstr,
    Voucher_Info:    bstr,
    H_handshake:     bstr,
    ? opaque_state: bstr
]
```

```
external_aad = (
    H_handshake:  bstr,
    CRED_V:        bstr,
)
```

(in Voucher)

New Section: *4.8. ELA Reverse flow with U as Responder*

- W is agnostic about default / reverse flow.
- W uses generic parameters G_U and H_handshake
  - regular flow: G_X, H_message_1
  - reverse flow: G_Y, TH_2

```
Voucher_Request = [
    SS:                int,
    G_U:               bstr,
    Voucher_Info:      bstr,
    H_handshake:       bstr,
    ? opaque_state:    bstr
]   ?message_1
```

```
external_aad = (
    H_handshake:  bstr,
    CRED_V:        bstr,
)   ?message_1
```

(in Voucher)

New Section: *4.8. ELA Reverse flow with U as Responder*

- Interoperability:
  - U: may support only 1 flow
  - V: must support both flows?
  - W: nothing changes
- Security of reverse flow
  - U has to share its identity first
  - Voucher_Info is confidential and Voucher is confidential / authenticated
    - fields are better protected than in default flow
  - Note: TH_2 is internal state
    - ➡️ discussed in Hackathon: fine since it’s all public information

issues about OPAQUE_INFO

#24 more concrete OPAQUE_INFO in Voucher

```
plaintext of Voucher = (
  role-of-v:        uint,
  directives-for-u: bstr,
)
```

#25 more concrete OPAQUE_INFO in Error message

```
plaintext of REJECT_INFO = (
  suggested-vs:              map,
  additional-recovery-info:  bstr,
)
```

Opinion: close both and leave it opaque, application handles it.

- when W is U's manufacturer, should be fine
- when not, will not lead to interoperability, only less optimized

issues

- authz with U as R and V as I #21
  - addressed with new Section 4.8
- identity protection service #26
  - stall issue, shall I close it?
- privacy of hints, ~~#27~~
  - no more hints, closed ✅
- IANA early review #51
- fix EAD labels TBD #52

next steps

- close remaining issues
- prepare for final version
  - do a detailed review
- if stable, update the implementation

thanks!
thoughts?

https://datatracker.ietf.org/doc/**draft-ietf-lake-authz**

geovane.fedrecheski@inria.fr