Lightweight Authorization using EDHOC

version -06 updates

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

Geovane Fedrecheski

(closed) Issue #26 -- Use case: Identity protection service

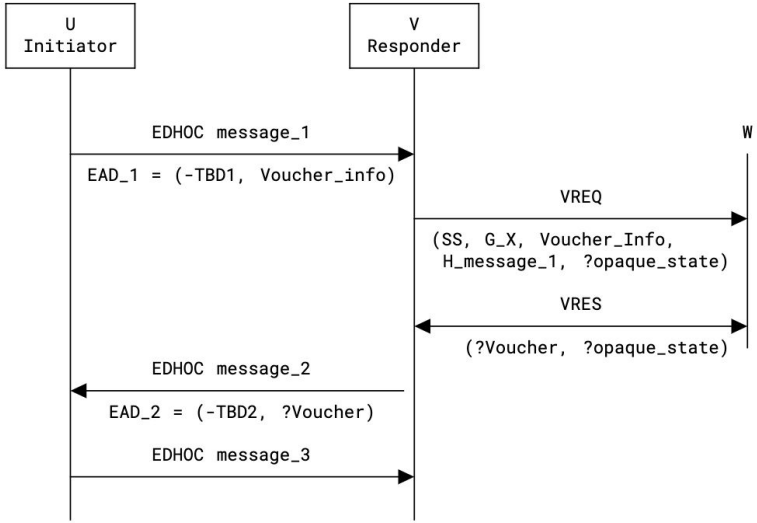
-> Use cases where the 3-party flow of ELA is useful, but a Voucher is not needed

- e.g. W simply helps U and V establish trust

-> **Proposal**: make the Voucher optional

✅ Done

```
Voucher_Response = [
    ? Voucher:          bstr,
    ? opaque_state: bstr
]
```



Open Issue #71 -- Support EDHOC with PQS cipher suites

- Upcoming cipher suites for EDHOC use KEM instead of DH
- Goal is to make ELA compatible with those suites (turns out it's simple)

Proposal:

TO-DO

- add a mandatory crypto element to EAD_1 and EAD_2
  - DH_EPH_Key_or_KEM_CT
- G_W / G_Y can either be a DH public key or a KEM encapsulation key
  - reference to PQ Suites draft

Open Issue #53 -- Allow keys for V and W be the same

-> Use cases where V and W are co-located, or you want to allow an “encrypted client hello” -like use case

- issue: re-use of salt in EDHOC_Extract(salt, IKM)

-> document does not necessarily encourages such use cases, the main point is to make it hard to misuse

PAUSED

-> **Proposal**: still TBD, e.g., ensure salt is not empty / not re-used

⬅️ First make the Changes of #26 and #71, then re-check

Implementation status

- Implemented [1] and evaluated on constrained devices
  - version -01 (now at version -05)
- Plan is to update it once the draft stabilizes

-> Looking forward to more implementations so we can interop test!

[1] https://github.com/lake-rs/lakers/tree/main/ead/lakers-ead-authz

Next steps

- Solve open issues #71, #53
- End-to-end document reviews
- Call for implementations and interop tests
- Looking forward to WG last call for ~~IETF 124~~ IETF 125

thanks!

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

geovane.fedrecheski@inria.fr