Lightweight Authorization using EDHOC

version -05 updates + open discussions

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

Geovane Fedrecheski

IETF 123 | Madrid, Spain | Jul 22, 2025

editorial updates

Editor’s notes -- **merged PRs**:

- #65: Interoperability of V: enforce regular flow and have reverse be optional
- #66: Add example opaque state for stateless V
- #67: Clarification about reuse of TLS in V<->W
- #68: Solve editor note about dropping msg_1
- #69: Add more context to external_aad in Voucher_Info
    - -> looking for co-author’s reviews
- #56: update acknowledgements

IANA review

Merged PRs:

- #54: preferred EAD value range is 0-23
- #63: considerations for .arpa domain
- #55: more few tiny changes

Open 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

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

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

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:

- add an optional KEM ciphertext element to EAD_1 and EAD_2
- G_W / G_Y can either be a DH public key or a KEM encapsulation key

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 #26, #53, #71 (all have a plan)
- End-to-end document reviews
- Call for implementations and interop tests
- Looking forward to WG last call for IETF 124

thanks!
thoughts?

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

geovane.fedrecheski@inria.fr