Lightweight Authorization using EDHOC

version -07 updates

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

Geovane Fedrecheski

Issue #74 -- Spoofing ID_U vulnerability

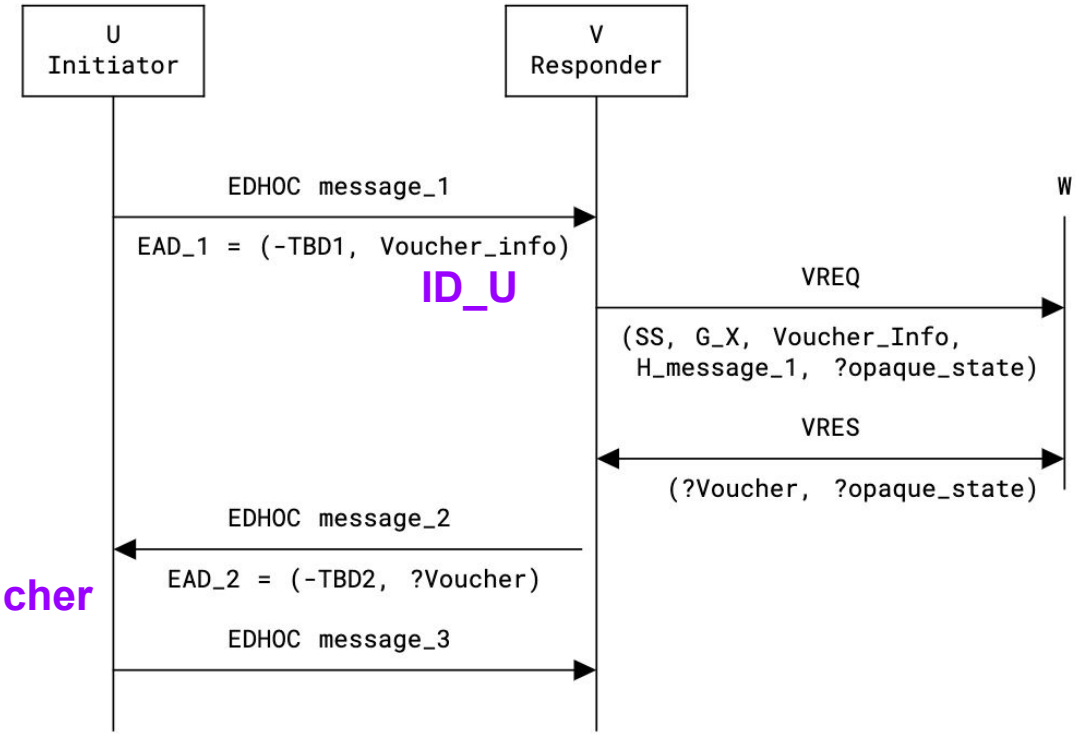
lake-authz-06

Context: U sends **ID_U** to W, which will evaluate authorization policies and reply with a **Voucher**

Note: authorization happens before authentication

```
plaintext = (
    ?OPAQUE_INFO: bstr
)
```

Voucher

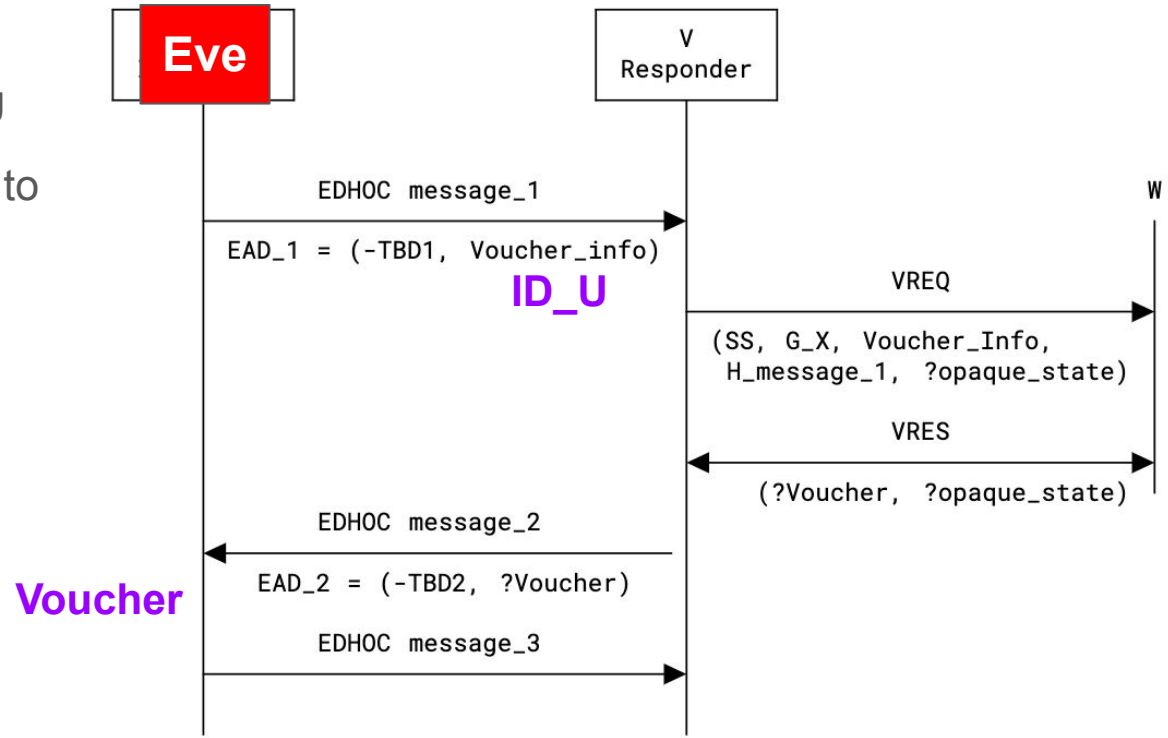


Issue #74 -- Spoofing ID_U vulnerability

lake-authz-06

Attack: Eve impersonates U to W, who issues a valid Voucher for U

Assumption: Eve learns the ID_U from a legitimate U, and uses that to build a valid Voucher_Info and execute the ELA protocol



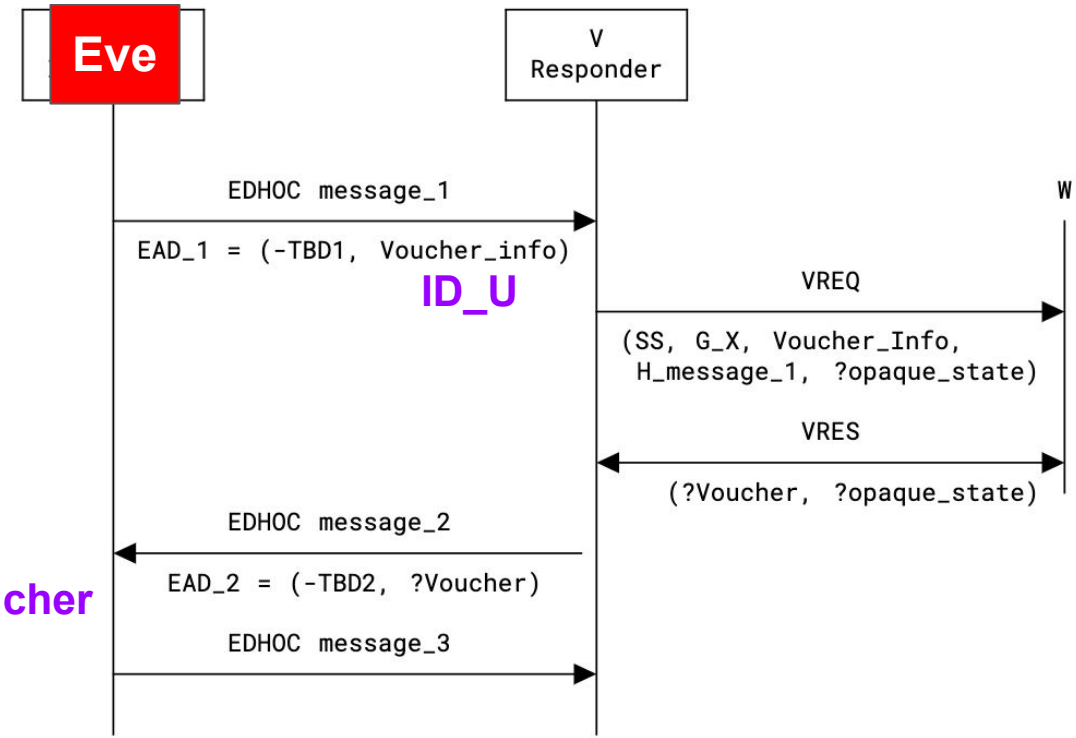
Issue #74 -- Spoofing ID_U vulnerability

lake-authz-06

Consequence: Eve learns what U is authorized to do in the system

- W will think this ID_U is valid and authorize it, and Eve will get a valid Voucher
- Information leak about authorization policies managed by W

plaintext = (
  ?OPAQUE_INFO: bstr ——— **Voucher**
)



Issue #74 -- Spoofing ID_U vulnerability

lake-authz-06

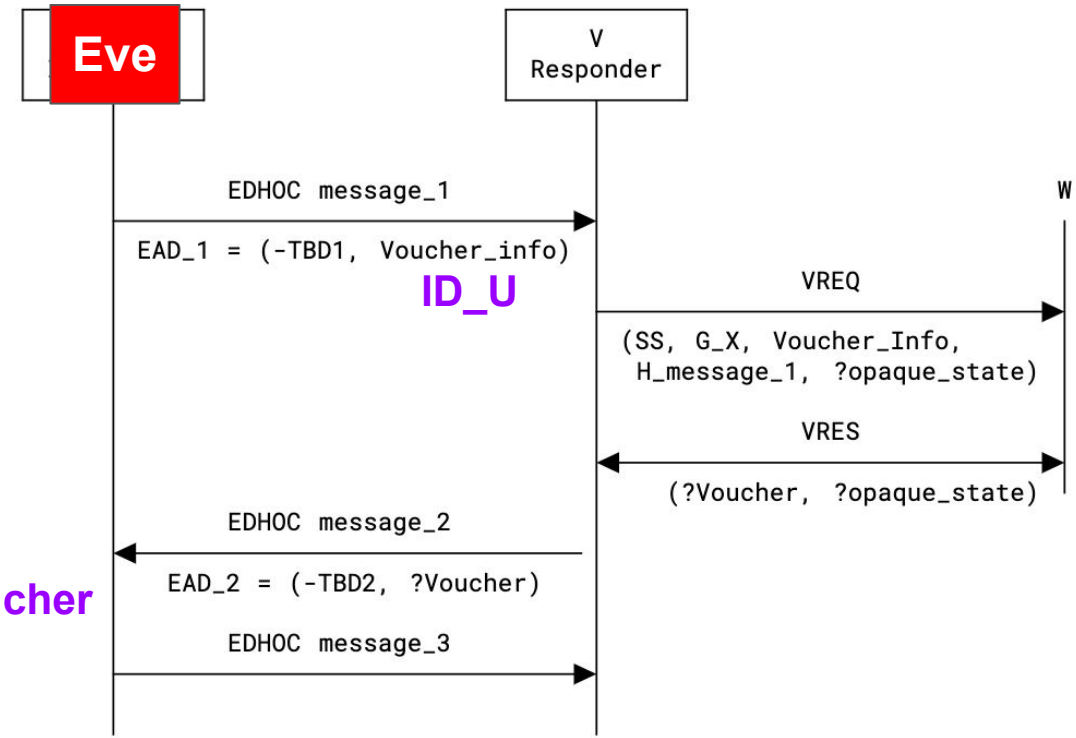
If there is no OPAQUE_INFO:

- Voucher means a binary Yes/No

If OPAQUE_INFO is present:

- Voucher can contain arbitrary information about how U is expected to interact with V

plaintext = (
  ?OPAQUE_INFO: bstr ——— **Voucher**
)

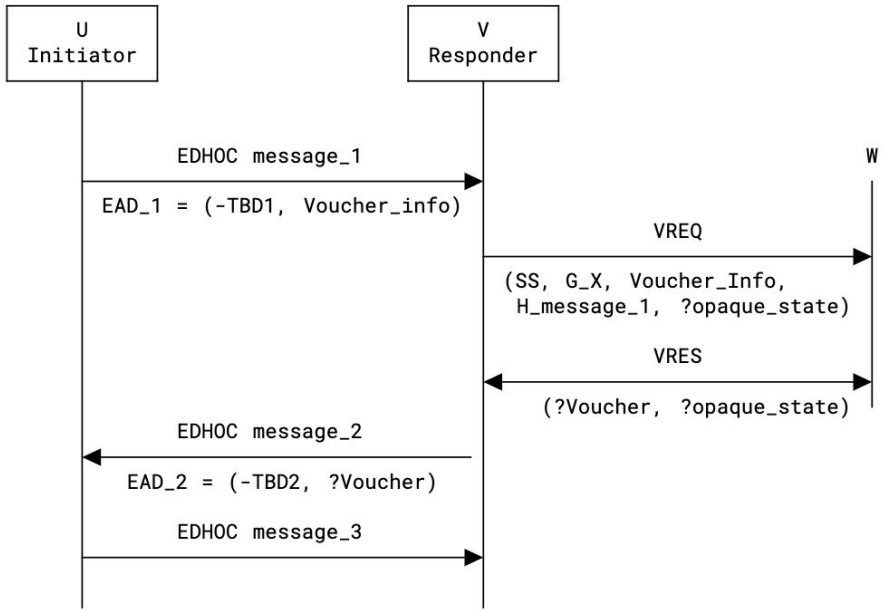


Issue #74 -- Spoofing ID_U vulnerability

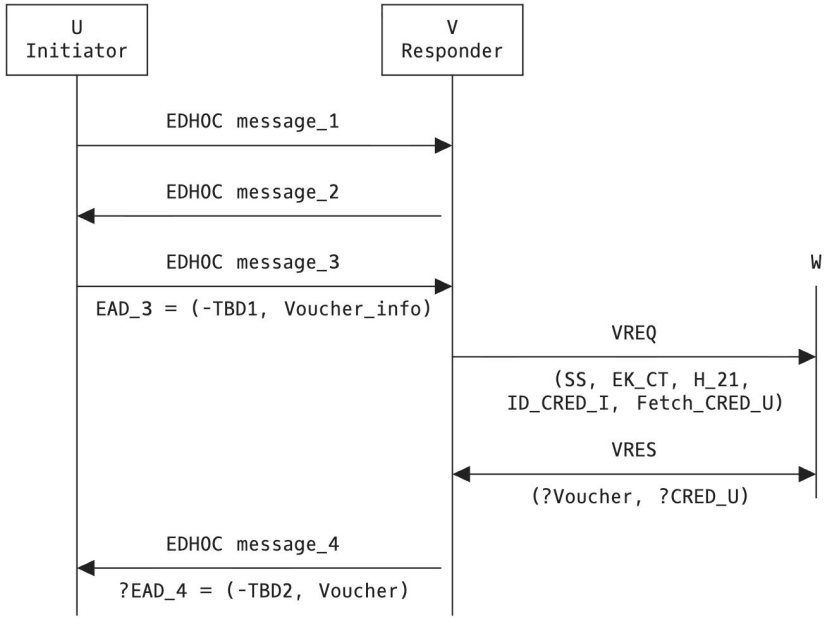
Major protocol update!

+284 -418

Proposal: modify protocol to use message_3 / message_4 (so that V can check U's identity)



lake-authz-06



lake-authz-07

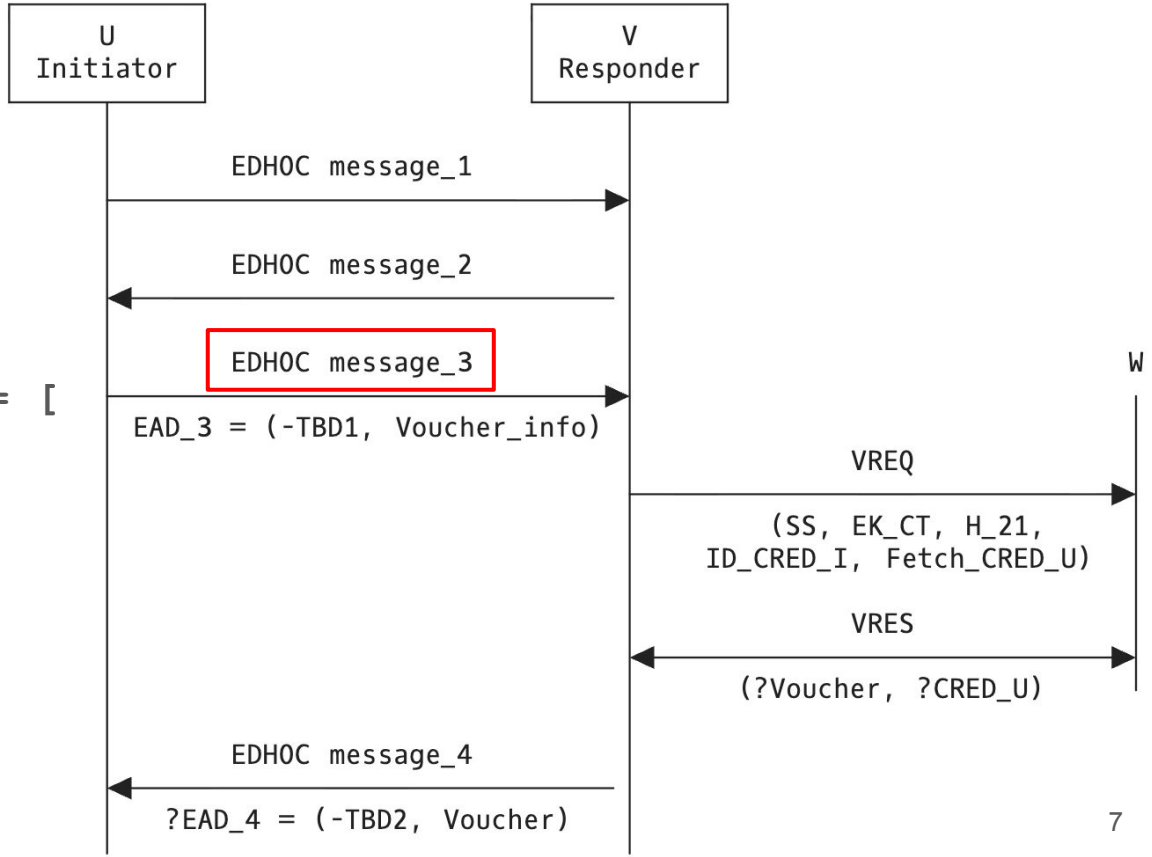
Issue #74 -- Spoofing ID_U vulnerability

lake-authz-07

Remove ID_U: favor

reuse ID_CRED_I

```
Voucher_Info_Seq = [
    LOC_W: tstr,
    EK_CT: bstr,
]
```

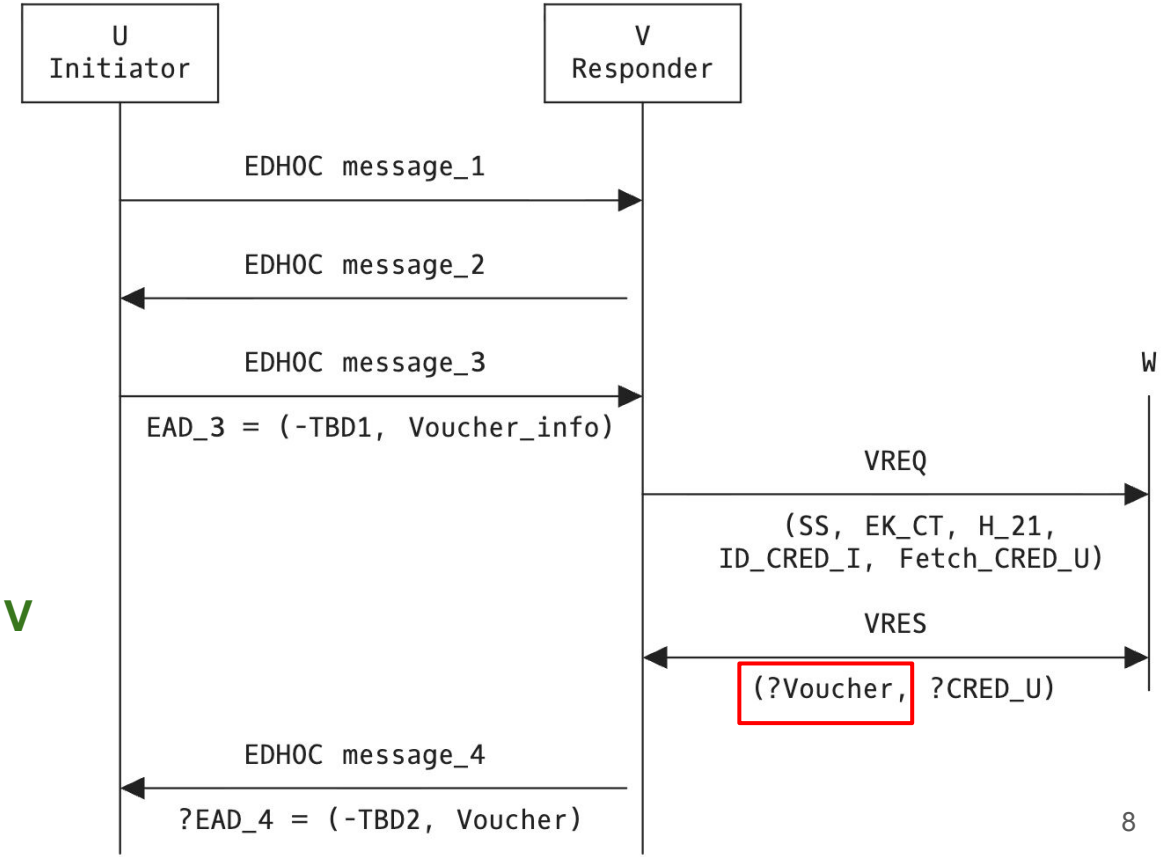


Issue #74 -- Spoofing ID_U vulnerability

lake-authz-07

```
Voucher's external_aad = (
    H_21:          bstr,
    ID_CRED_I:     bstr,
    CRED_V:        bstr,
)
```

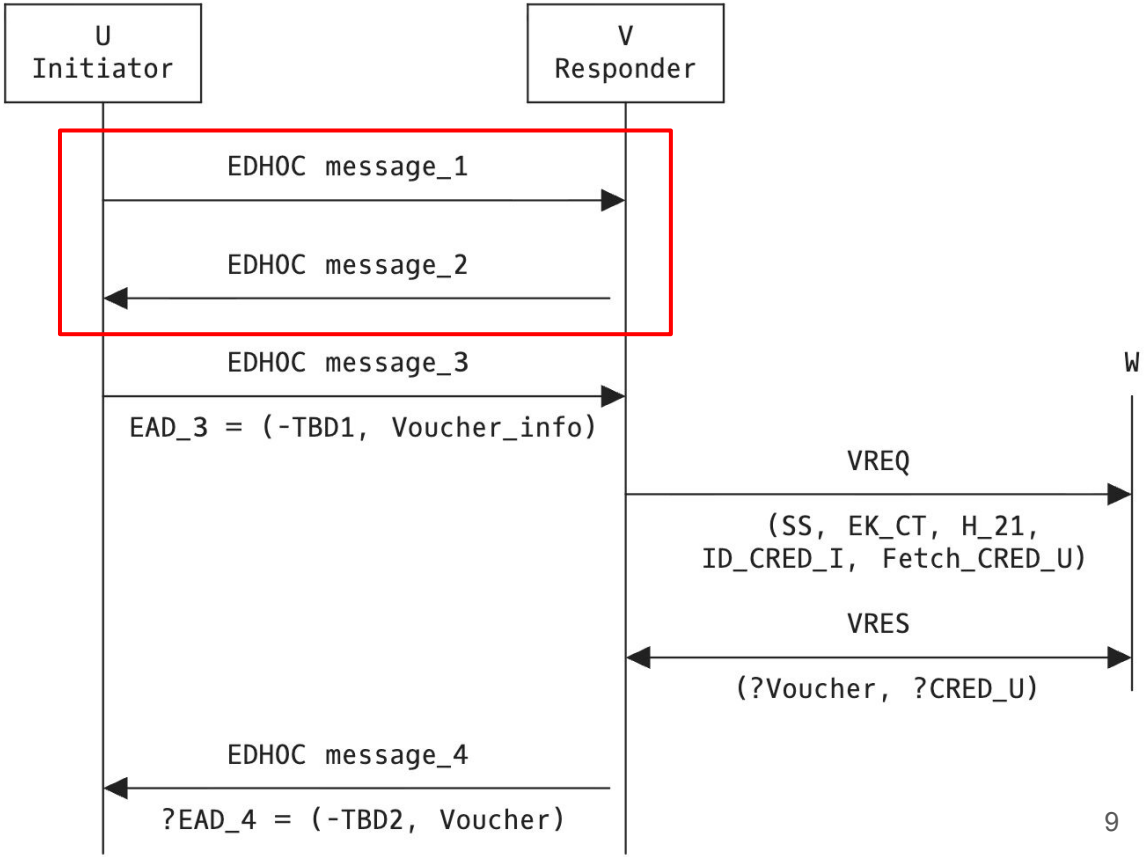
- **bind EDHOC session, U, and V**
- **H_21 = H(m2, H(m1))**



Issue #74 -- Spoofing ID_U vulnerability

lake-authz-07

2-RT join with CoJP no longer possible, Appendix was removed



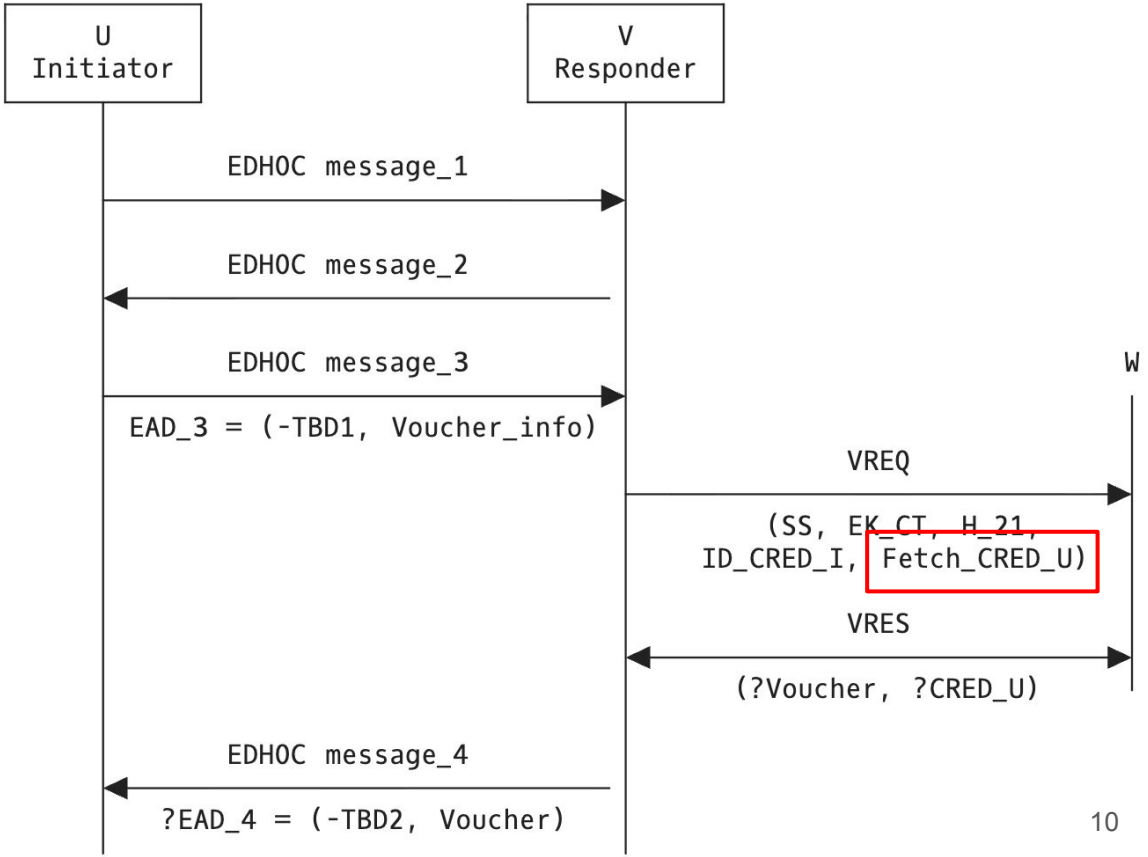
Other changes

lake-authz-07

V can try different forms of obtaining CRED_U

Fetch_CRED_U field

- indicates whether W should try to fetch and send CRED_U
- *optional*: W is concerned with Authorization, and MAY act as credential provider



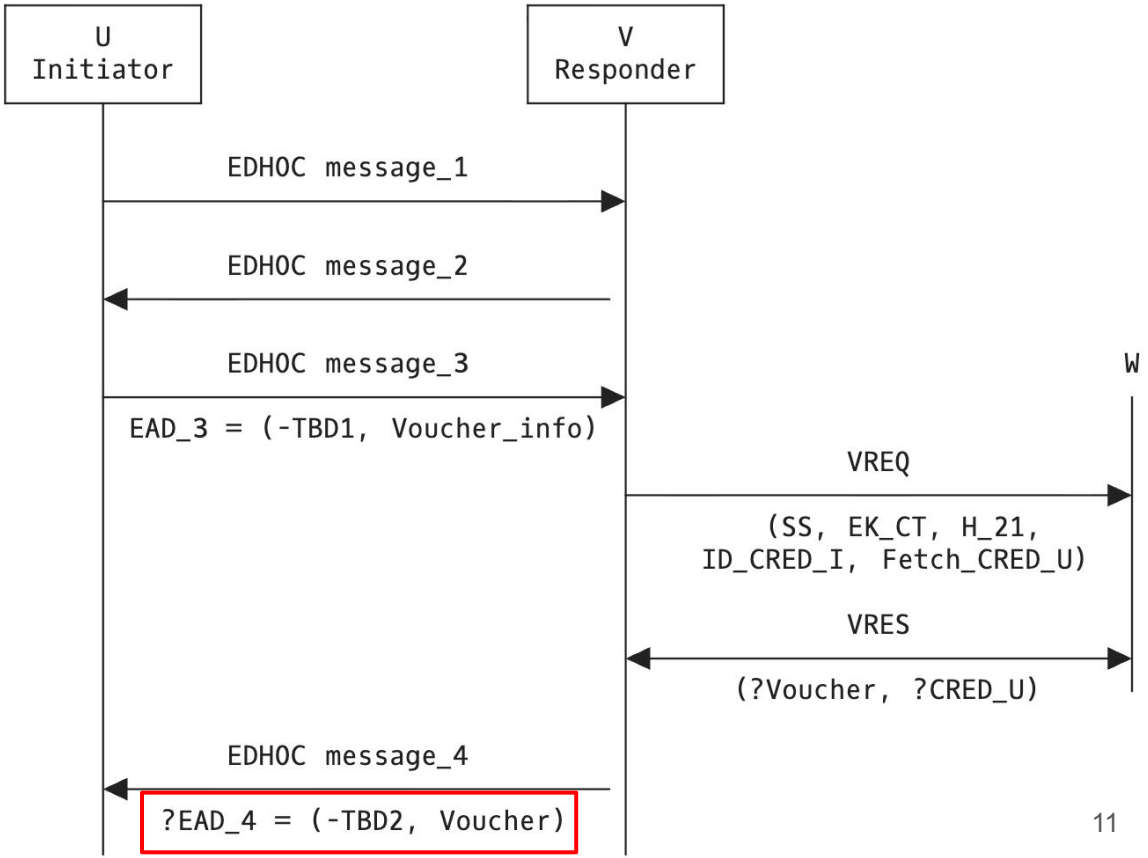
Other changes

lake-authz-07

Make whole EAD_4 optional

- for the case when W sends no Voucher to V

Address comment by chrysn in a previous PR

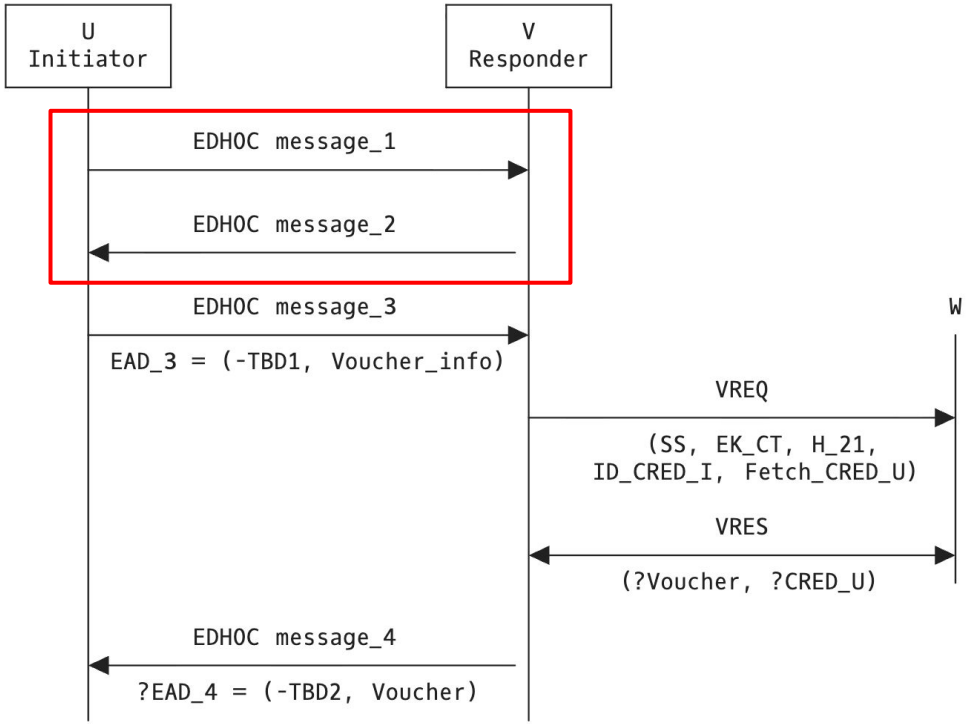


Other changes

lake-authz-07

Use with lake-app-profiles

- advertise ELA support in message_1 and _2
- Example in Appendix A.1




```
[e'APP-PROF-MINIMAL-CS-2', TBD1, TBD2]  / profile_id_with_eads /
```

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)

✅ Done

Also avoids reuse of ephemeral key G_X!

Proposal:

- add a mandatory crypto element to EAD_2 / EAD_3
  - EK_CT - Ephemeral Key or Ciphertext
- G_W / G_Y can either be a DH public key or a KEM encapsulation key
  - reference to PQ Suites draft

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)

✅ Closed

Closed: “encrypted client hello” use case not applicable anymore

PR #78 Clarify that Fetch_CRED_U is best-effort

- Also clarify that if V fails to obtain CRED_U, the session is aborted

PR #80 Review by Marco Tiloca

- Clarify
  - use with lake-app-profiles
  - non-reuse of G_X: ephemeral keys should only be used once
- Determine that V uses same CRED_V with U and W
- Interoperability: V must support both flows
- Adjust REST error codes (remove special case for when ID_CRED_I is unknown)
- Editorial fixes

PR #79 Sync with lake-ra

Adjust and rename H_21 -> H_12

```
* H_21 is H(message_2, H(message_1)),
```

```
* H_12 is H(H(message_1), message_2),
```

Next steps

- WG last call?

thanks!

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

geovane.fedrecheski@inria.fr