Lightweight Authorization for EDHOC

draft-selander-lake-authz-00

Göran Selander, John Preuß Mattsson, Ericsson
Michael Richardson, SSW
Mališa Vučinić, INRIA
Aurelio Schellenbaum, ZHAW

IETF 115, LAKE WG, November 08, 2022

Authorization support in EDHOC

- The External Authorization Data (EAD) fields in EDHOC provides integration points
  - Support for authorization of peers running EDHOC
  - Typically involving trusted third parties (TTPs)

- **This draft:**
  - **Initiator retrieves voucher from an Authorization Server authorizing the Responder**

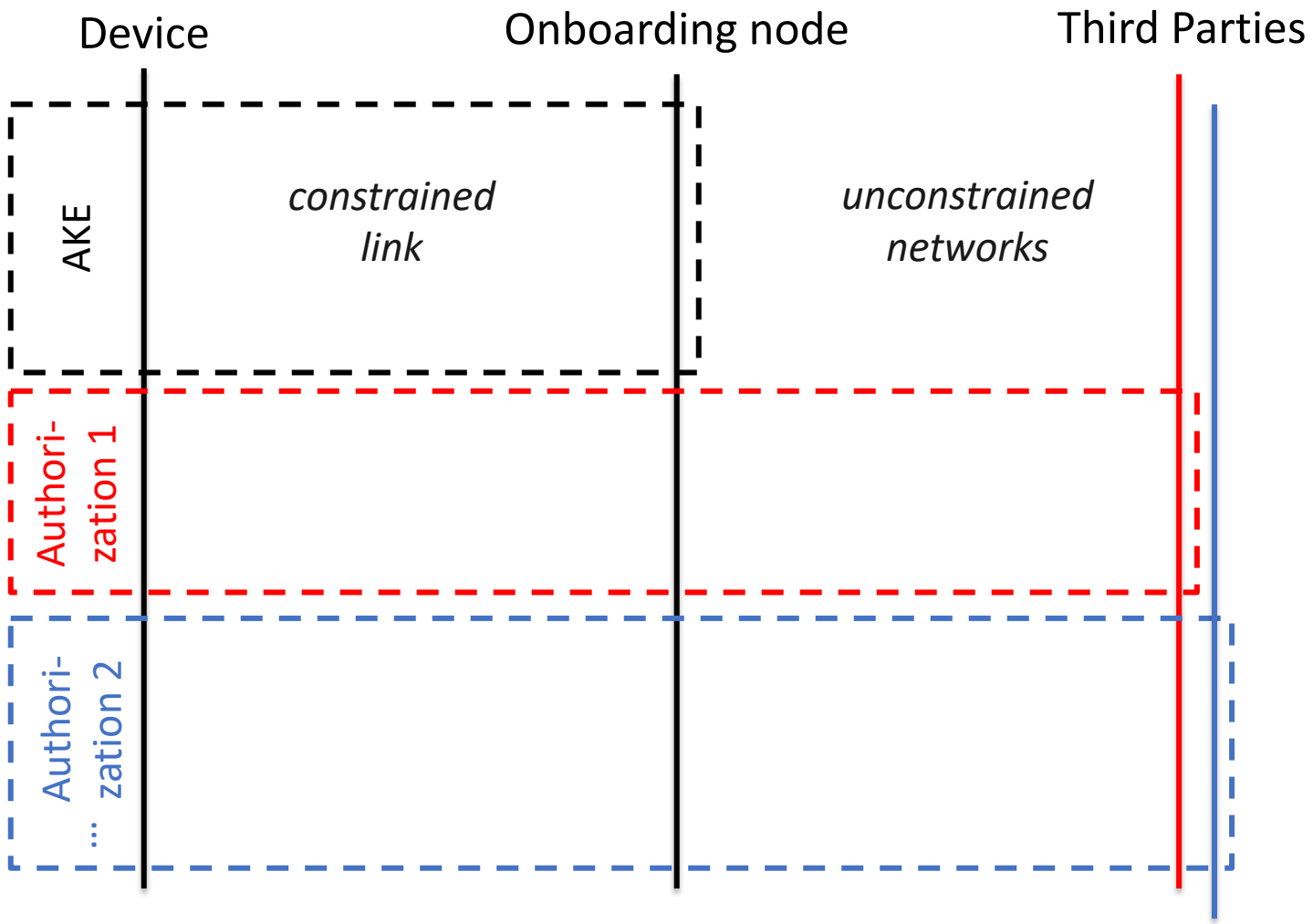
- Other examples: remote attestation, revocation checking

EAD in draft-ietf-lake-edhoc

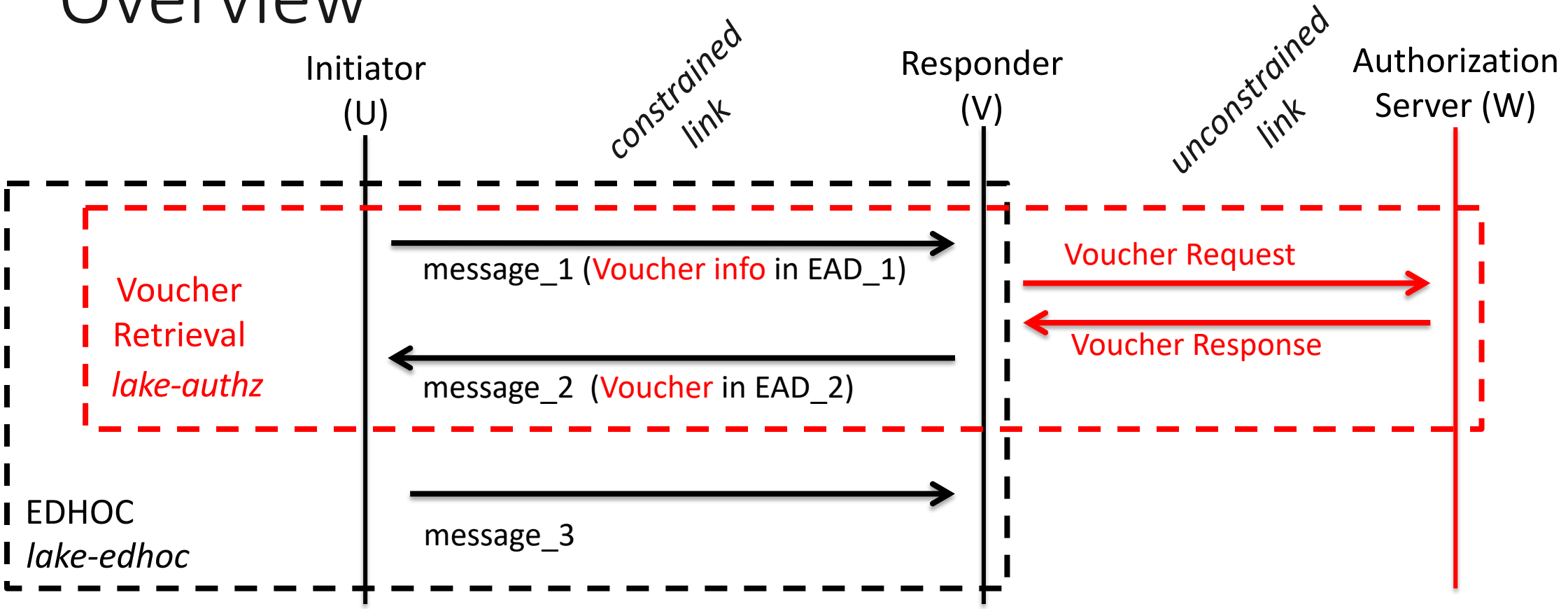
- Format and basic use in Section 3.8
  - *"must not be used for generic application data"*
- Appendix E: Use of External Authorization Data
  - *"Security applications … must perform the necessary security analysis."*
- Caveat in the security considerations (Section 8.1)
  - *"Any new uses of EAD should be subject to careful review"*
- IANA registration procedure is "Specification Required"

Example: Device Onboarding

- **Device onboarding setting**
  - AKE
  - Authorize onboarding node
  - …
- **Involving third parties**
  - Authorization Server
  - …
- **Potential inefficiencies**
  - Sequential processing
  - Same data in different phases, e.g. public key of the peer
  - Data sent over constrained link can be accessed over unconstrained network



Overview



- Data in EDHOC also used for authorization
- Transport credentials etc. over unconstrained instead of constrained links
- In parallel instead of in sequence

- Reuse of data
- Lower overhead
- Reduced latency
- Early abort

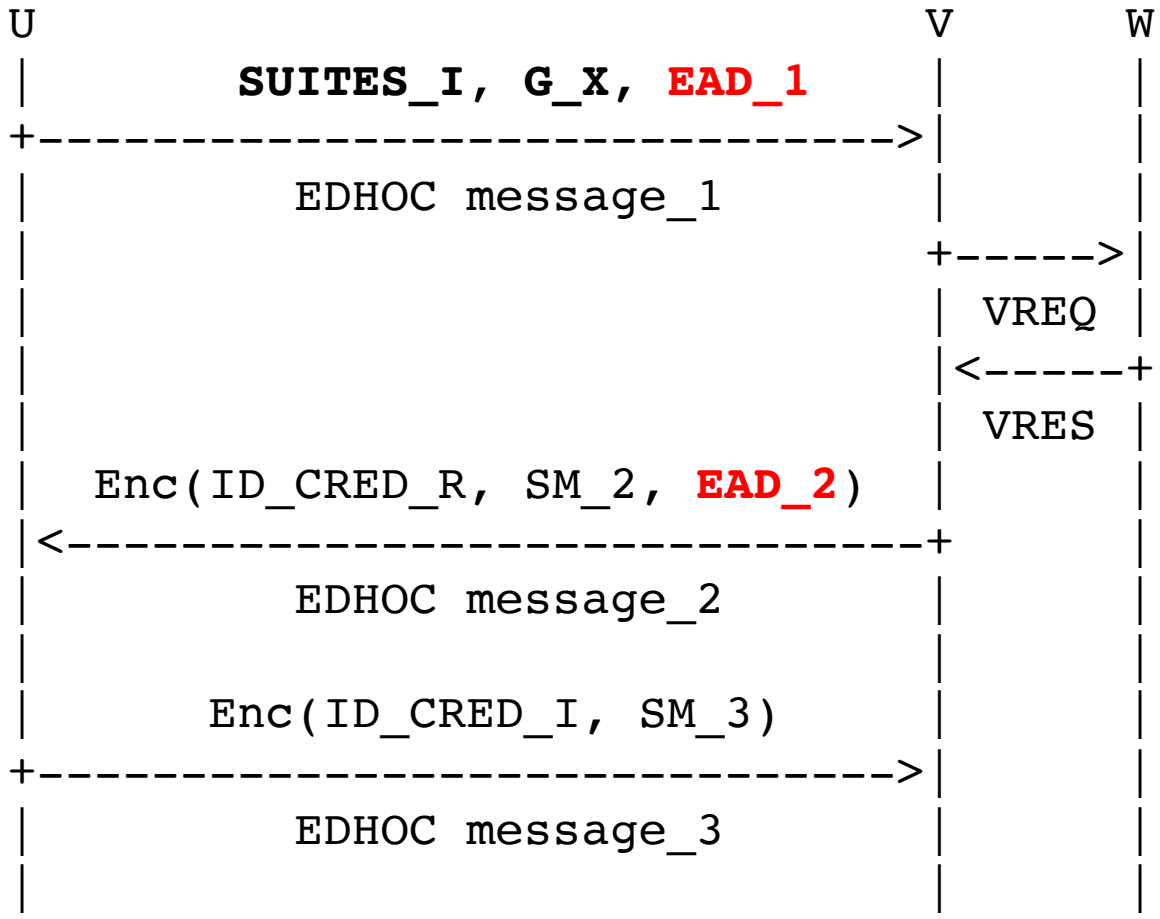
Protocol U-V

Assumptions

U ←→V
- No prior trust relation
- U provide location of W to V

V ←→W
- Web based trust
- Proof of Possession of PK of V
  - PK of V is in CRED_R

U ←→W
- U trusts g^W (PK of W) to issue vouchers
- g^W pre-provisioned



where
EAD_1 contains **LOC_W**, **ENC_ID**
EAD_2 contains **Voucher**: MAC(H(message_1), CRED_R)

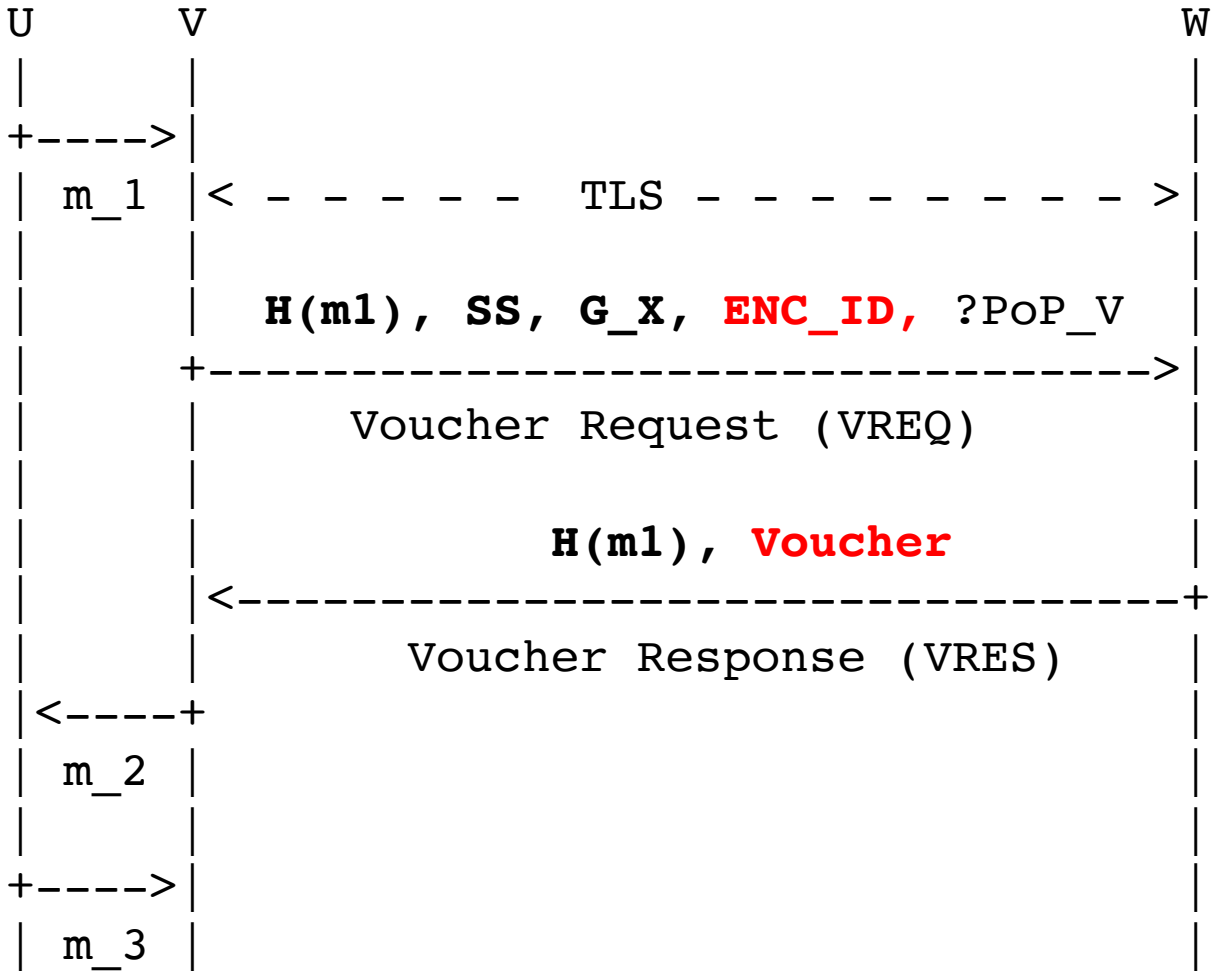
Protocol V-W

Assumptions

U ←→V
- No prior trust relation
- U provide location of W to V

V ←→W
- Web based trust
- Proof of Possession of PK of V
  - PK of V is in CRED_R

U ←→W
- U trusts g^W (PK of W) to issue vouchers
- g^W pre-provisioned



where
H(m1) = H(message_1)
SS = Selected EDHOC ciphersuite
Voucher: MAC(H(message_1), CRED_R)

Next steps

- Review updates
  - Marco's review: https://mailarchive.ietf.org/arch/msg/lake/5fR1AitD4XRuWf18OgGbtwge40U/
- Implementation