Remote attestation over EDHOC

draft-ietf-lake-ra

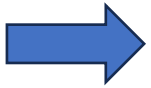
Yuxuan SONG, Inria

Göran Selander, Ericsson

Issue #40, #22 Complete 4 examples in Section6

Version 04

6. Instantiation of Remote Attestation Protocol
   - 6.1. (IoT, BG, Fwd): IoT Device Attestation
   - 6.2. (Net, PP, Fwd): Network Service Attestation
7. Mutual Attestation in EDHOC
   - 7.1. (IoT, BG, Fwd) - (Net, PP, Fwd)

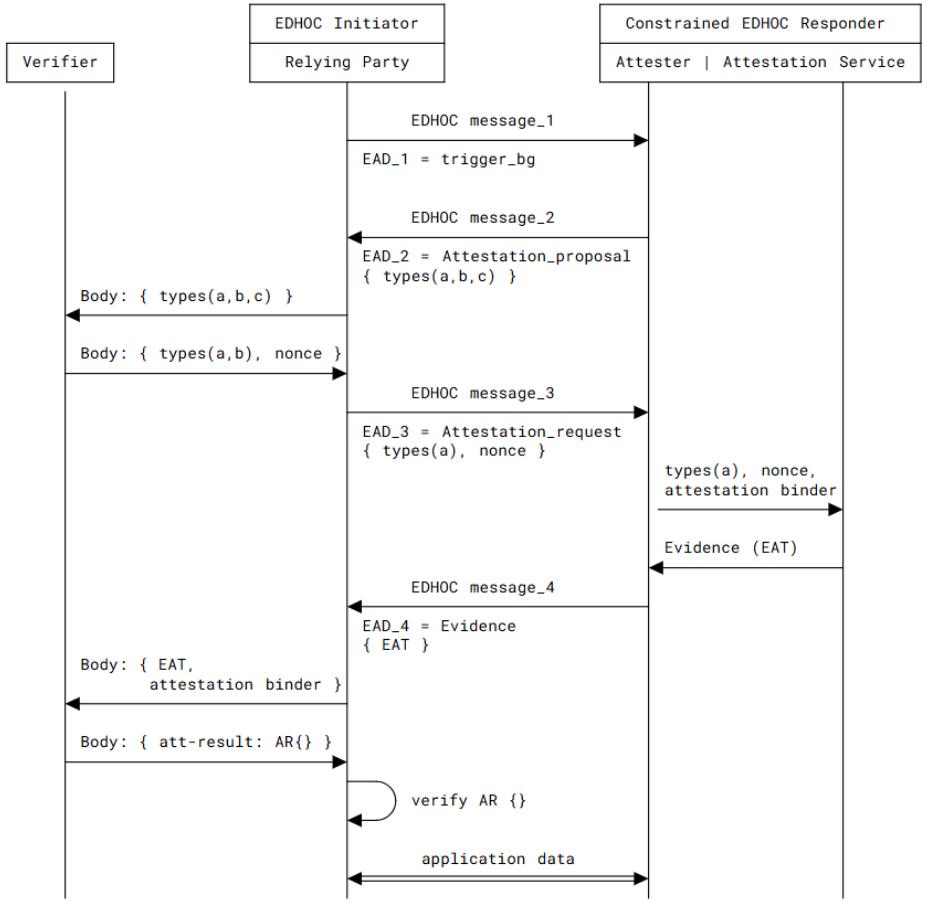


Version 05

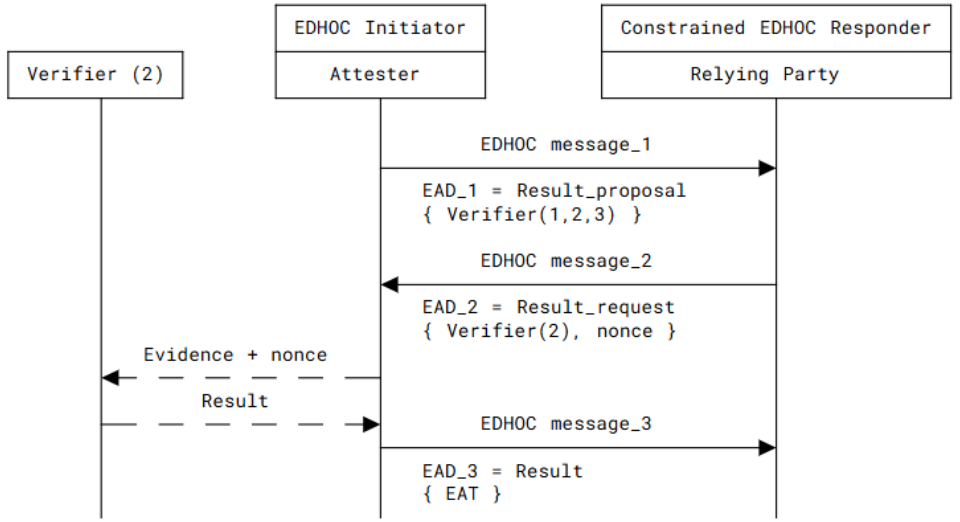
6. Instantiation of Remote Attestation Protocol
   - 6.1. (I, BG): EDHOC Initiator Attestation in the Background-check Model
   - 6.2. (R, PP): EDHOC Responder Attestation in the Passport Model
   - 6.3. (R, BG): EDHOC Responder Attestation in the Background-check Model
   - 6.4. (I, PP): EDHOC Initiator Attestation in the Passport Model
7. Mutual Attestation in EDHOC
   - 7.1. (I, BG) - (R, PP)

New subsections 6.3, 6.4

Section 6.3: (R, BG) Respnder as Attester in Background-check model

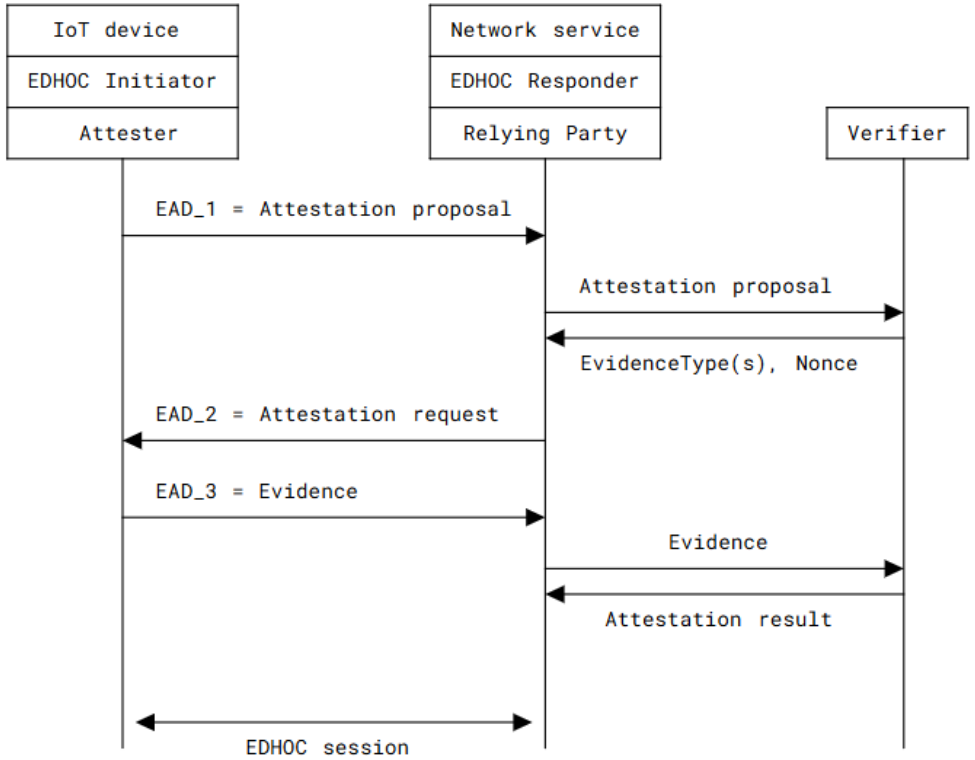


Section 6.4: (I,PP) Initiator as Attester in Passport model

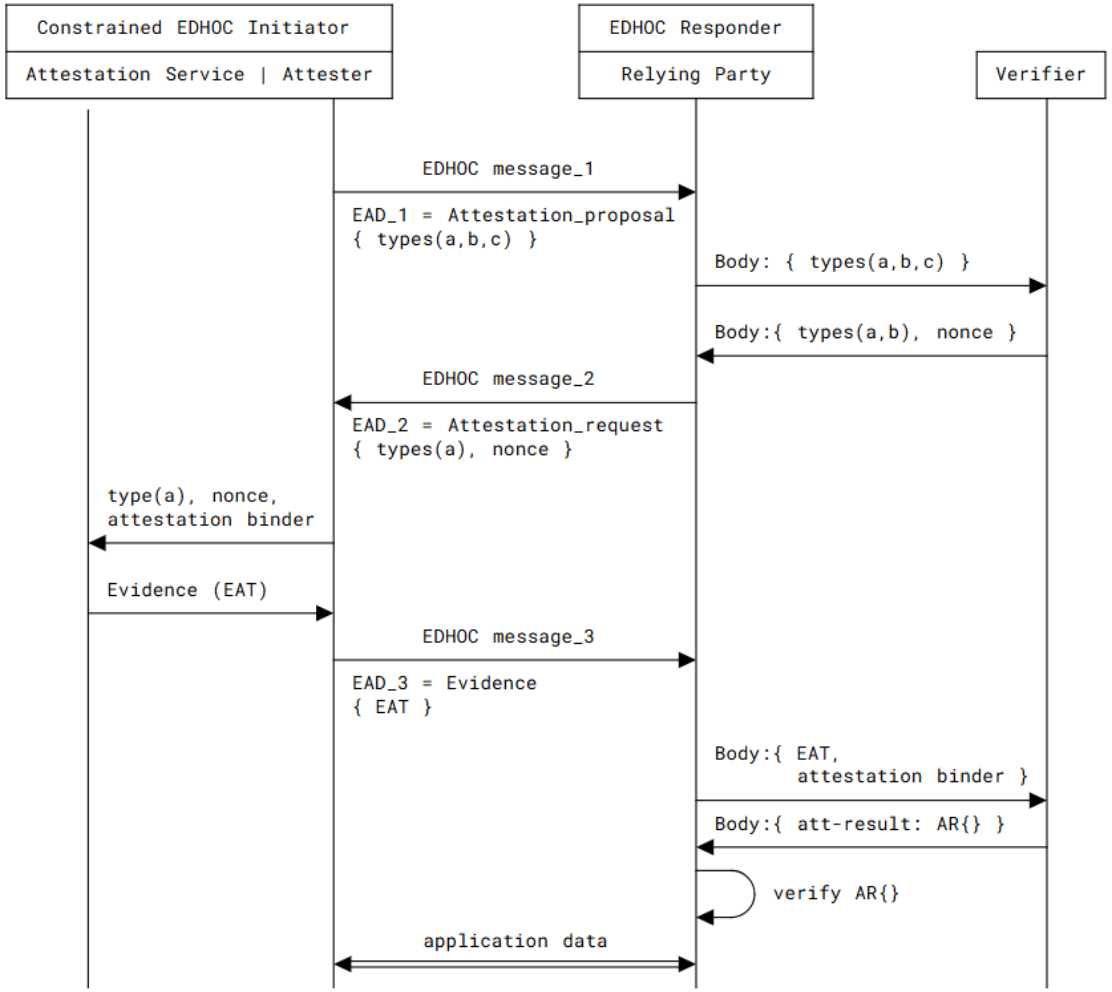


Issue #38: Combine Appendix A with Figure1 in section 6.1

Version 04



Version 05



Issue #38: Improve attestation binder

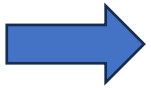
Version 04

Intra-handshake attestation

```
attestation_binder = H(message_1, message_2)
```

Post-handshake attestation

```
attestation_binder = EDHOC_Exporter (exporter_label, context, length)
```



Version 05

```
attestation_binder_m3 = HKDF-Expand(0, attest_info, hash_length)
attest_info = [ H_12, "attestation", ID_CRED_I ]
H_12 = H(H(message_1), message_2)
```

```
attestation_binder_m4 = EDHOC_Exporter (exporter_label, context, length)
```

Issue #38: new subsection 4.1: Reuse of EDHOC

4.1. Reuse of EDHOC

This specification reuses several components of EDHOC.

- EAD is the External Authorization Data message field of EDHOC messages, see Section 3.8 of [RFC9528]. This specification specifies four new EAD items in background-check model, and four new EAD items in passport model (see Section 5).¶
- ID_CRED_I is used to identify the authentication credential of the Initiator in the authentication session.
- EDHOC hash algorithm of the selected cipher suite is used to generate the attestation_binder_m3 (see Section 5.3.3.1) when Evidence is sent in EDHOC message_3.
- EDHOC_Exporter is used to generate the attestation_binder_m4 (see Section 5.3.3.1) when Evidence is sent in EDHOC message_4.

Issue #41: Sanity check by Marco

- Add references and move several informative references to normative references
- Rephrase unclear text for better readability
- Assign names to EAD items and fix the related Figure 6
- Revise the CDDL grammar
- Clarifications and editorials
- Clarify that the protocol is not required to be CoAP-based, although both forward and reverse message flows are supported
- Improve the messages shown in the figures

Thank you!

https://github.com/lake-wg/ra