

From Formal Analysis of Attested TLS to Attested EDHOC

Muhammad Usama Sardar^{1,2}, Viacheslav Dubeyko³,
and Jean-Marie Jacquet⁴
(ACK: Yuxuan Song, Marco Tiloca, Göran Selander)

¹TU Dresden, Germany

²Co-chair, Trusted Research Environment (TRE) Open Suite,
Global Alliance for Genomics and Health (GA4GH)

³IBM, San Jose, CA, USA

⁴Nadi Research Institute, University of Namur, Belgium

March 16, 2026

Motivation: our brand new charter¹

Within each protocol message, EDHOC provides External Authorization Data (EAD) fields. These fields may be used by external security applications to reduce the number of messages and round trips, or to simplify processing. The working group will specify Standards Track documents with the following uses of EAD fields to augment the EDHOC key exchange:

- 3rd party-assisted authorization of EDHOC peers.
- Remote attestation of EDHOC peers, reusing as much as possible available work from the RATS and TLS working groups.

The working group will also work on a Standard Track means for coordinating the use and discovery of EDHOC application profiles, the definition of well-known application profiles and processing extensions through EDHOC's defined extension points, such as registering new schemes and new EAD registrations.

In addition, the working group will work on an Informational document gathering implementation considerations and guidance for the base protocol specification.

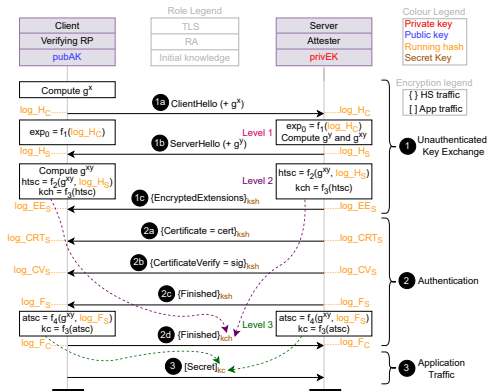
Liaisons and Formal Analysis

The working group will work closely with other related working groups in the IETF. This includes for example CoRE, ACE, IOTOPS, PQUIP, COSE, CBOR, RATS, EMU, TLS, SEAT and 6LO. The group welcomes formal analysis to be performed on the documents that introduce cryptographically-relevant changes or additions to the EDHOC protocol.

- draft-ietf-lake-ra has been religiously following [draft-fossati-tls-attestation](#).
- Remote attestation is a **subtle** addition \Rightarrow **Formal analysis** is required for high assurance.

¹<https://datatracker.ietf.org/doc/charter-ietf-lake/03/>

From Attested TLS: Devil is in the Details!



- htsc : used for encryption of clientFinished message (2d).
 - Irrelevant for security goals
 - Server **not yet authenticated** at this point
- atsc : used for encryption of application data (client's secret, e.g., decryption key)
 - Relevant for security goals

To Attested EDHOC (draft-ietf-lake-ra-03)

Thanks to charter, devil is easier to find!

- **Approach**²: we use modularity, abstraction and analogies with TLS.
- **Results**: Correlation properties fail \Rightarrow Relay attacks³

Security level	draft-ietf-lake-ra-03
L_1	×
L_2	×
L_3	×

- **Root cause**: No cryptographic binding of Evidence to the connection
- **Proposed fix**: Post-handshake attestation

²<https://mailarchive.ietf.org/arch/msg/lake/FhB68GT1qSZuRILN7gMPQdn6SEc/>

³<https://mailarchive.ietf.org/arch/msg/lake/Tovt17wgvzwJWT2I2ZwnhoIOnYQ/>