Applying Generate Random Extensions And Sustain Extensibility (GREASE) to EDHOC Extensibility

draft-amsuess-core-edhoc-grease

Christian Amsüss

IETF121 Dublin, LAKE, 2024-11-04

Long time ago in London...

"EDHOC will start small and then add all things in TLS back in."

Let's be selective – and then mindfully take good parts (e. g. RFC 8701).

GREASE

- “Only by using the extension capabilities of a protocol is the availability of that capability assured.” RFC 9170[1]
- This draft just does that.

[1] Also `edm-protocol-greasing`.

Concrete extension points

- ✔ EAD items: 1× “1+1”, 3× “1+2”; all optional
- ✔ Cipher suites: 1× “1+1”, 3× “1+2”; responder can’t select them
- ✖ Methods: Not negotiated – out of scope
- ✖ COSE headers: Not negotiated – out of scope

…exercising the extension points we *can* keep utilized.

Advancing GREASE for EDHOC

- All is done that can be done in an individual draft.

Advancing GREASE for EDHOC

- All is done that can be done in an individual draft.

Chairs?

Backup slide: Caveats

- We're message size constrained.
  → Apply it in applications where the added size will be tolerable.
- It can be a covert channel (cf. INTDIR on padding).
  → Yes. As can the use of any other EAD.
- The distribution and values of options reveal some data about the implementation.
  → Concrete recommendation available on size and choice – large anonymity set.