Using the Extensible Authentication Protocol with Ephemeral Diffie-Hellman over COSE (EDHOC)

draft-ietf-emu-eap-edhoc-04

Dan García-Carrillo, University of Oviedo
Rafael Marín-López, University of Murcia
Göran Selander, Ericsson
John Preuß Mattsson, Ericsson
Francisco López Gómez, University of Murcia

IETF 123

Summary

- Situation since IETF 122
  - From version 03 to 04.
  - WGLC
  - Feedback received.

- Questions/comments?

Situation since IETF 122

- Only editorial changes between draft versions -03 and -04. Stable version achieved.
- WGLC initiated last month.
- Received a lot of feedback. Thank you all!
  - 6 persons commented that it is ready / want to see it progress.
  - No objections

Detailed reviews

- Reviews from *Marco Tiloca* and *Christian Amsüss*. Very positive feedback, mostly editorial changes.

- **Thank you! We will address them before the next submission.**

EAP Channel Binding

- Input from Alan:
  - https://mailarchive.ietf.org/arch/msg/emu/MEJ2PC9pIyQrnMPNqzMOPTpzc1Q
  - “The implicit consensus of EMU and implementors is that channel bindings aren't needed. This should be brought up at the next WG meeting, and perhaps needs a larger discussion with the ADs.”

- Channel binding support in EAP-EDHOC
  - The document defines Channel Binding info as an opaque blob of data – CBOR byte string – in an EDHOC EAD field
  - EAD fields in EDHOC are optional and so will be the Channel Binding info.
  - Clarification about the defined EAD item for compliance with RFC9528:
    - Critical. Multiple occurrences of the EAD item within one EAD field are not allowed.
  - Which data is sent in channel binding is up to the endpoints
  - Error cases will also be clarified.

Interest in EAP-EDHOC

- Published an open-source implementation of the method (with support for fragmentation):
  https://gitlab.com/franciscolopezg/eap-edhoc-testbed.git

- Also a paper about EAP-EDHOC, including performance results in a Wi-Fi environment.
  https://doi.org/10.1016/j.csi.2025.104037

- Interest from companies in the automotive industry to use EAP-EDHOC reported on the EMU mailing list.

Questions/comments ?

THANK YOU!