EAP method based on EDHOC Authentication

draft-ingles-eap-edhoc-00
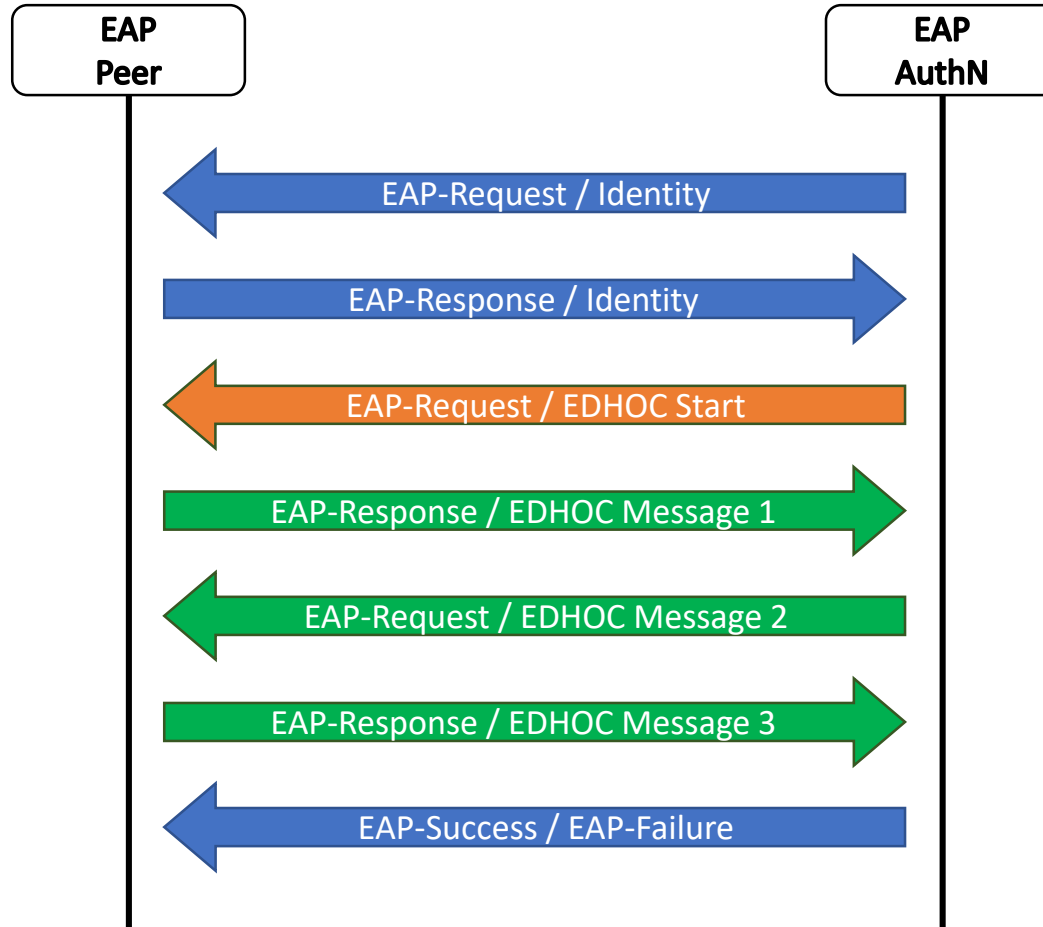
Eduardo Ingles / Dan Garcia / Rafael Marin

109th IETF EMU WG

Connecting IoT devices with EAP

- Goals

  - Alternative EAP solution for IoT appliances

  - Take advantage of CoAP-based protocols

  - End-to-end security

  - Lightweight solution by design

- EDHOC: Ephemeral Diffie-Hellman Over COSE

  - Lightweight Authenticated Key Exchange

    LAKE WG: https://datatracker.ietf.org/wg/lake/

Message Exchange

EAP Peer

EAP AuthN

EAP-Request / Identity

EAP-Response / Identity

EAP-Request / EDHOC Start

EAP-Response / EDHOC Message 1

EAP-Request / EDHOC Message 2

EAP-Response / EDHOC Message 3

EAP-Success / EAP-Failure

Transport & message correlation

- Lock-step procedure in EAP

- EAP manages message correlation

METHOD_CORR = 4 * method + corr

Where:

corr = 3

Ongoing work

- Present the idea to the community

- Extend the writing of draft sections

- Detail the composition of EAP-EDHOC messages 1 to 3

- Complement the solution presented in

  draft-ingles-radex-radius-edhoc-00

Question

- Does it make sense as a WG item?