EAP-based Authentication Service for CoAP

Work in progress for:
draft-ietf-ace-wg-coap-eap-02

Rafael Marín-López, University of Murcia
Dan García-Carrillo, University of Oviedo

ACE Interim Meeting, June 08th, 2021
CoAP-EAP – Updates Summary 01 version

• Changed URI to conform to HATEOAS
• Added casuistic when a message is lost
• Added explanation on how the CoAP server and Client processes work.
• Writing and typo review
CoAP-EAP – Ordering guarantee following HATEOAS

• General Service URI /b
• Each step within the authentication creates a new resource with structure
  • /b/x
    • x -> Value representing the current step in the authentication process

x can be set to any value as long as it serves to specify univocally to both entities of the exchange the next step within the authentication process.
CoAP-EAP – Ordering guarantee w/ HATEOAS
CoAP-EAP – Ordering guarantee w/ HATEOAS

- For each CoAP request (which contains an EAP Request) the process is:
  - The CoAP server
    - Receive the EAP payload and process it
    - Send the content to the EAP state machine
    - Receive the response from the EAP state machine
      - If everything goes as expected:
        - A new resource is created, /b/y
        - The previous resource /b/x is deleted
        - A response specifying the new resource is sent back
      - If an error occurs an error message is returned depending on the cause of the error.
CoAP-EAP – Ordering guarantee w/ HATEOAS

- Casuistic when messages are lost
  - If the piggybacked response with a new resource is lost
    - The CoAP client will continue to retransmit until the response arrives
    - The CoAP server will recognize the message as retransmission and resend the message
CoAP-EAP – Ordering guarantee w/ HATEOAS

• Casuistic when an old message arrives

IF managed at CoAP engine
• If the CoAP engine takes care of it, as the server recognizes the old message it can send a stored copy
  Then the client would recognize MSGID < and that he got the response already, dropping it

IF managed at Application
• If the control in the server goes up to the application, it generates a 4.04 not found since its deleted
  Then the client would recognize the MSGID < and that he got the response already, dropping it
THANK YOU