

# *draft-ietf-ace-wg-coap-eap*

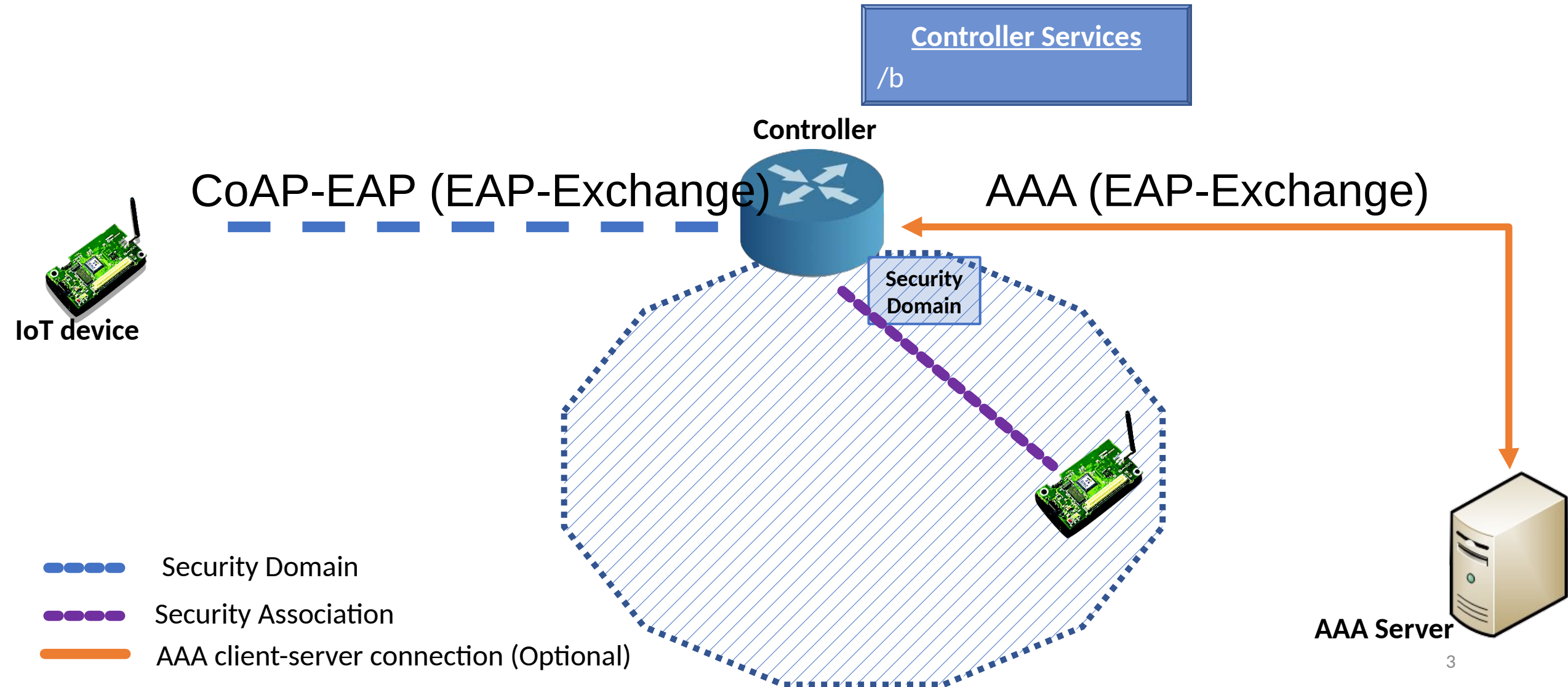
Rafael Marín López

Presenter: Dan García Carrillo

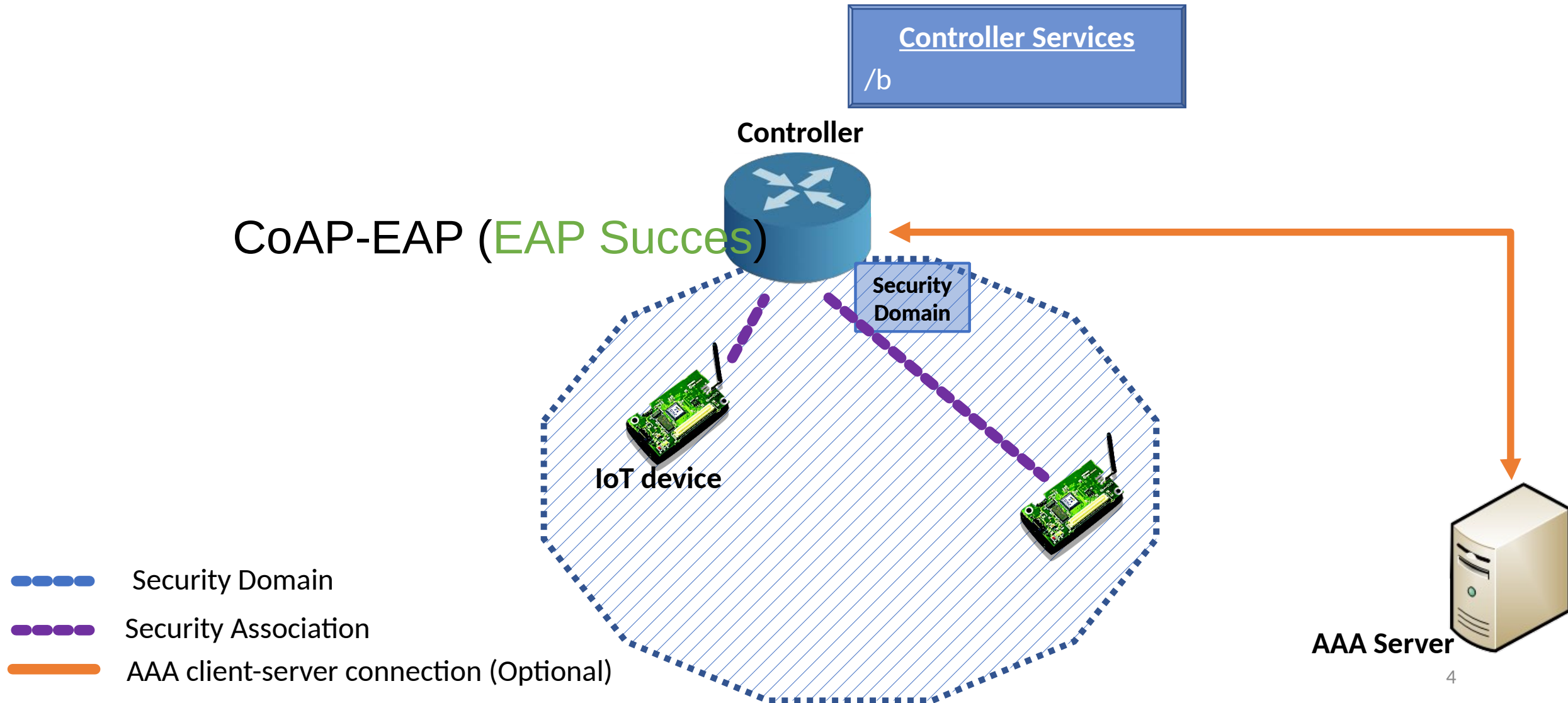
# Outline

- CoAP-EAP: The Concept
- Use cases
- Current state
- How to move forward from last version -00

# CoAP-EAP: The main idea

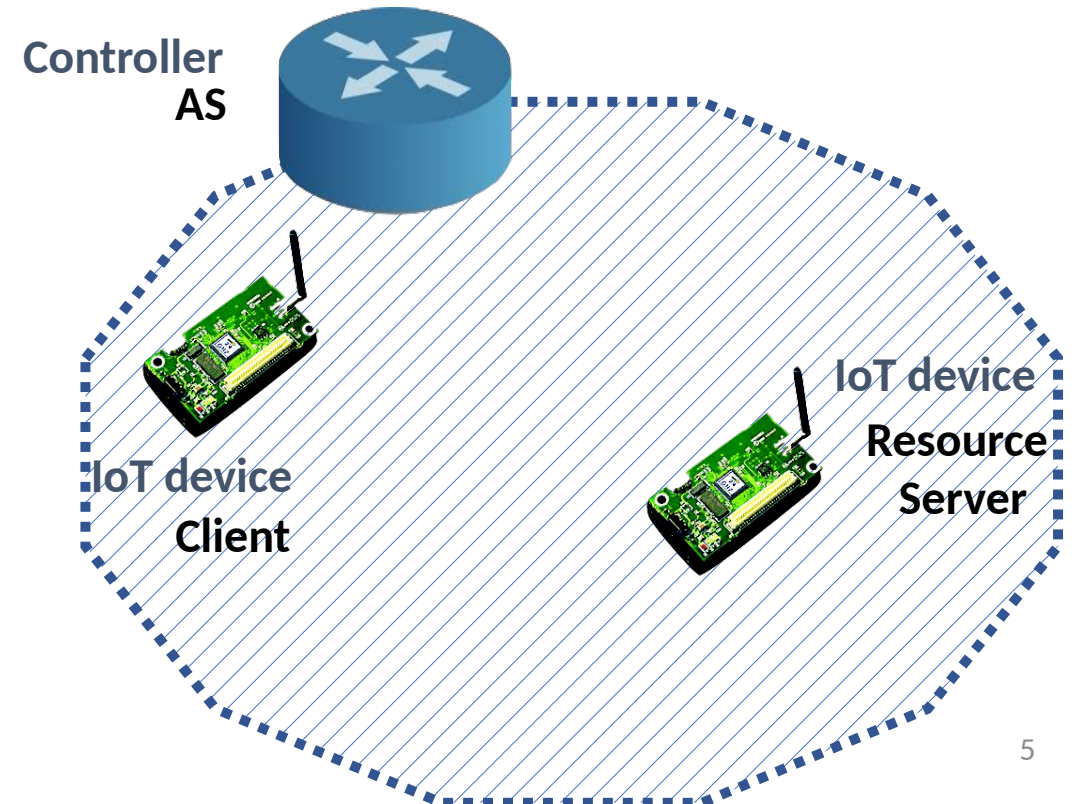
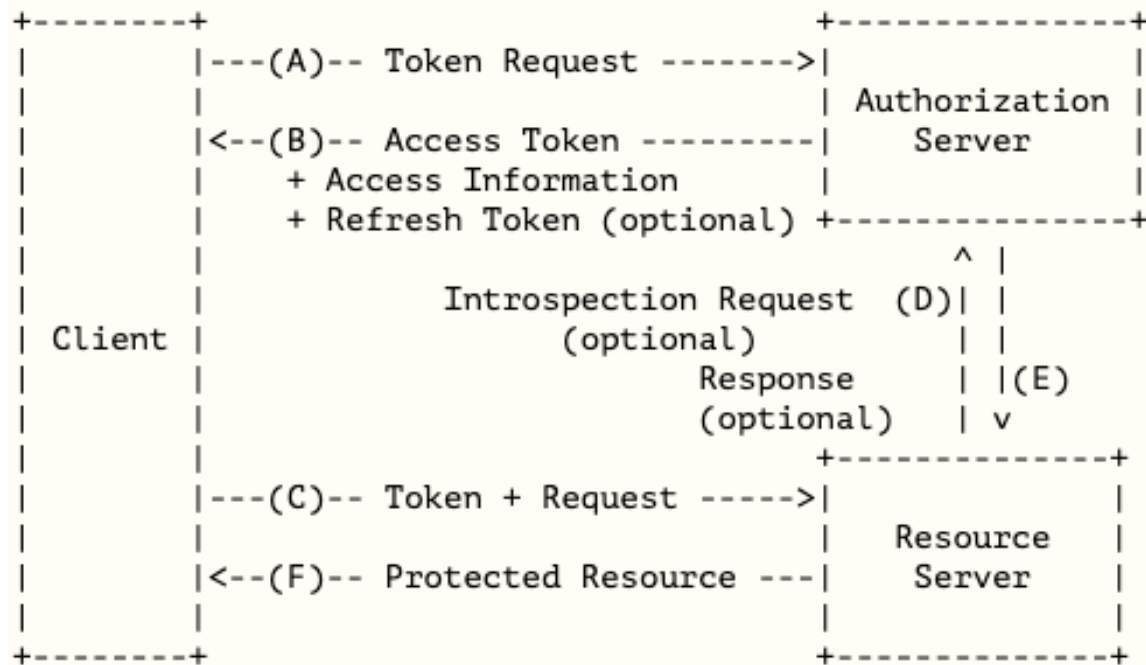


# CoAP-EAP: The main idea



# Use cases

- CoAP-EAP in ACE
  - CoAP-EAP can be used to perform the Client registration, and derive key material to establish different Security Associations (SA)



# Use cases

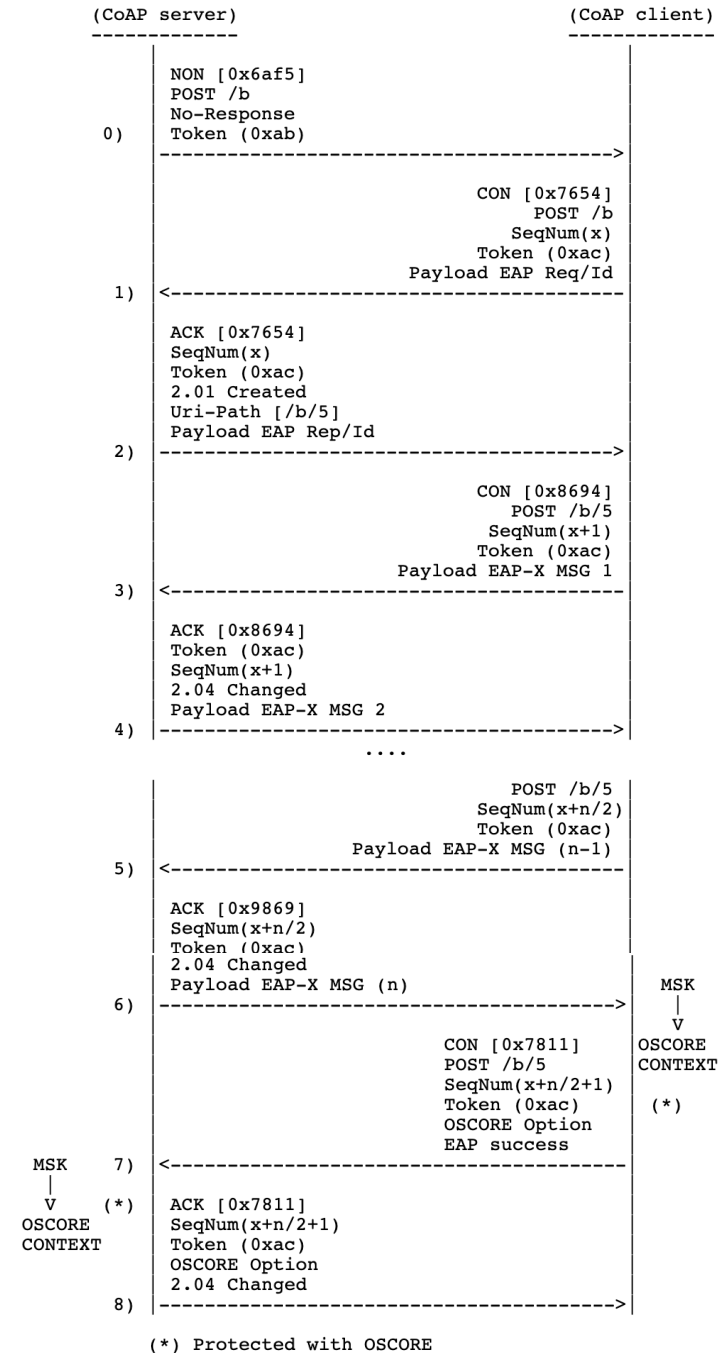
- CoAP-EAP for network access
  - As a way of allowing traffic through an network entity for packet forwarding.
- CoAP-EAP for service authentication
  - Additional authentications other services beside Network Access can be needed, and can be also managed using CoAP-EAP. (Infrastructure and network is managed by one organization, services by other)

# Different ways to operate in the use cases

- Multi-domain case with AAA infrastructures
  - Devices from different organizations can join the same security domain
- Single-domain with AAA infrastructures
  - Within an organization, different buildings can be managed with AAA infrastructures and any device will be able to operate within the domain.
- Single-domain without AAA infrastructures
  - Using EAP in standalone mode we can also manage the devices deployed co-locating the EAP server with the EAP authenticator.

# Current state

- CoAP-based EAP lower layer
- Independent of CoAP engine
- AAA support
- OSCORE security association





# How to move forward from last version - 00

- CoAP engine independent vs optimized solution
  - Can we (do we want to) modify the way the CoAP engine chooses
    - Tokens
    - MSG-IDs
- Possible optimizations
  - Empty Token
  - No additional SeqNum Option
  - Monotonically increasing MSG-ID after initial value