EAP-based Authentication Service for CoAP

Changes for draft-ietf-ace-wg-coap-eap-04

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

ACE Interim Meeting, September 14th, 2021

Summary of main items

- Flow Independent of CON and NON
- Piggybacking
- Discovery
- OSCORE vs COSE for Last Exchange

- Other changes for v04
  - Tagged CBOR structure

Flow Independent of CON and NON

Context

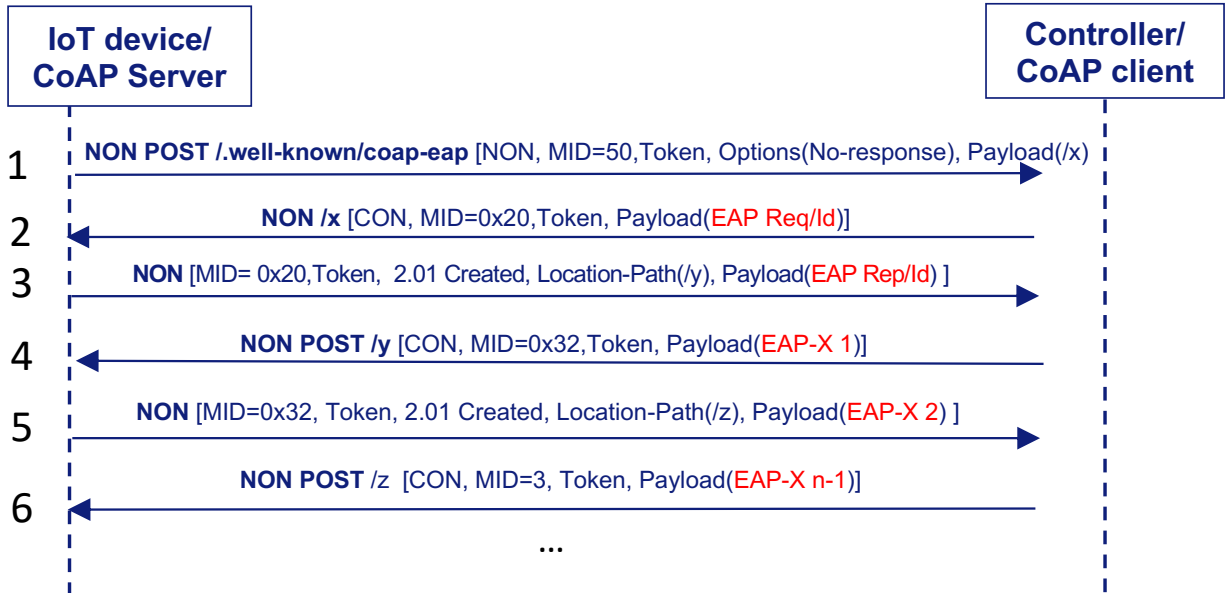
Some CoAP implementations may only support NON

Approach

Add needed support at CoAP-EAP application level → Retransmissions at EAP level

Resources	
URI	EAP processed
/y	✓
/z	x

Keep track of last and current resources in case of retransmission



Resources	
URI	EAP processed
/x	✓
/y	✓
/z	x

Keep track of ALL resources in case of retransmission

Piggybacking

Context

Some CoAP implementations may not support Piggybacking

Approach

Piggybacking is recommended, to save exchanges. In any case, if its not used, it should not be a problem from CoAP-EAP perspective.

Discovery

Context

Mechanisms to discover the IPv6 of the Controller

Approach

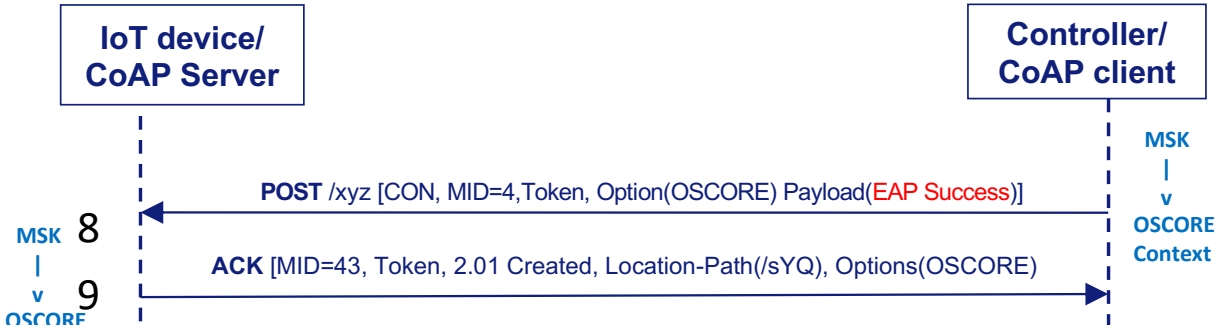
A first approach was to receive the IPv6 of the Border Router (e.g., IPv6 RA) and send there the initial message.

Other approaches:

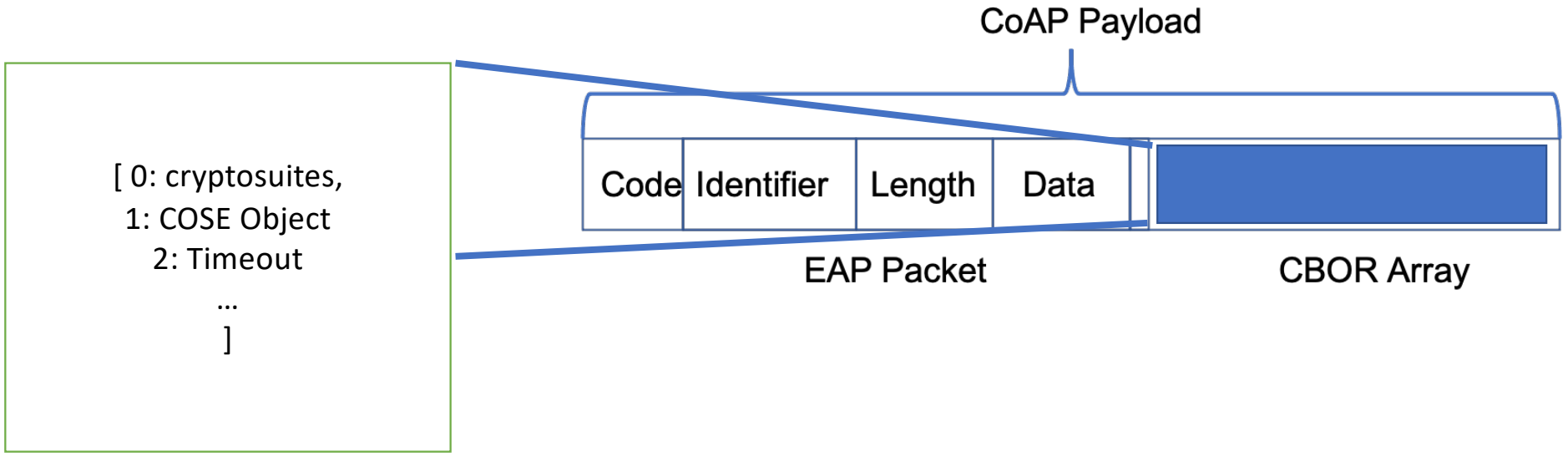
- DHCPv6 [RFC8415]
- mDNS [RFC6762]

OSCORE vs COSE for Last Exchange

- MSK is used to generate the OSCORE security context
- The EAP peer (IoT device) needs the EAP success to make the MSK available to work with OSCORE
  - The resource cannot be associated with an OSCORE context
  - OSCORE ciphers the Payload and URI-Path, hence cannot be directed to the Application
- ALTERNATIVE: Use COSE with only integrity for key confirmation.



Tagged CBOR structure



Extensible CBOR structure

THANK YOU