Enrollment with Application Layer Security (EALS)

Göran Selander, Ericsson
Shahid Raza, RISE SICS
Mališa Vučinić, Inria
Martin Furuhed, Nexus
Michael Richardson, Sandelman Software Works

IETF 98, ACE WG, March 27, 2017

Application Layer Security

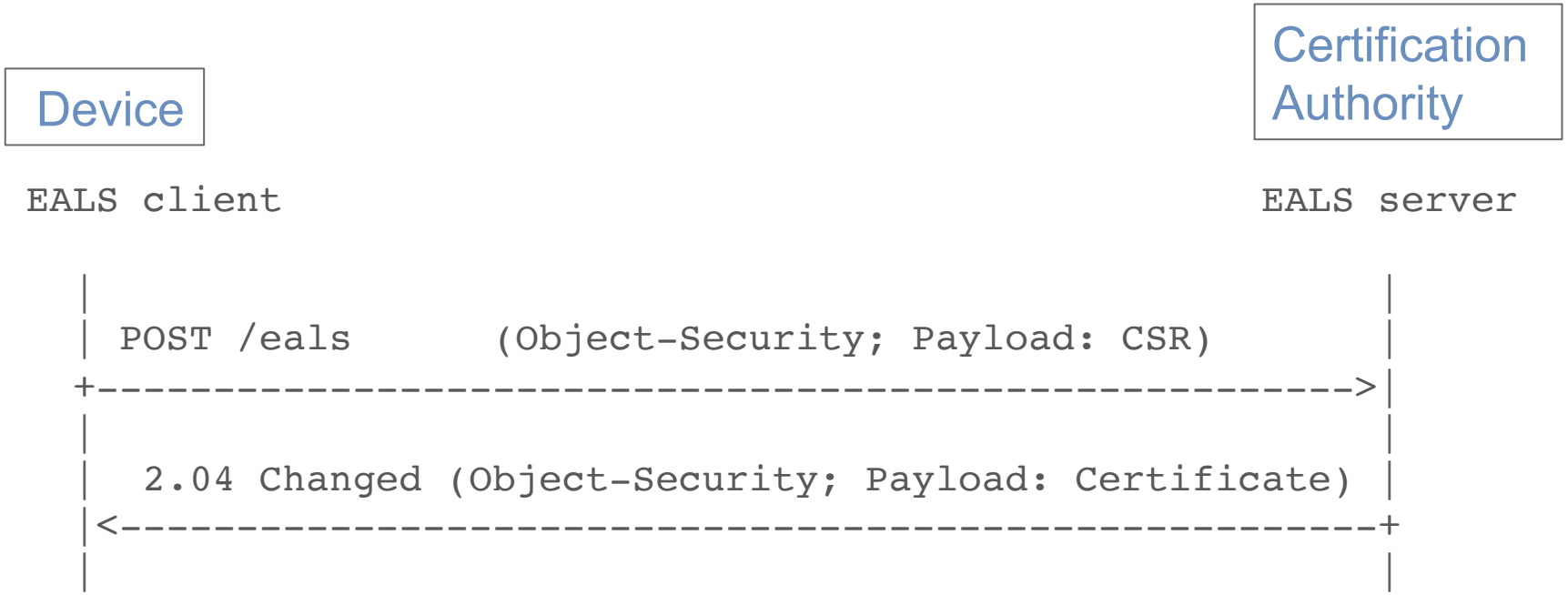
- Ongoing work in CoRE and ACE on application layer security protocols suitable for IoT:
  - OSCOAP (confidentiality, integrity and replay protection)
  - Secure Group Communication for CoAP (e.g. secure multicast)
    - Extension to OSCOAP
  - EDHOC (key exchange)
  - OSCOAP/EDHOC profile for ACE (authorization and access control)
- OSCOAP/EDHOC uses CoAP, CBOR, and COSE
- Can we also do certificate enrollment based on application layer primitives?

Application layer analogy of EST

- EST: Certificate Management over CMS (CMC) authenticated with transport layer security
- EALS: CMC authenticated with application layer security

Transport layer	**Application layer**
TLS/DTLS handshake	EDHOC
TLS/DTLS record layer	OSCOAP
EST	EALS

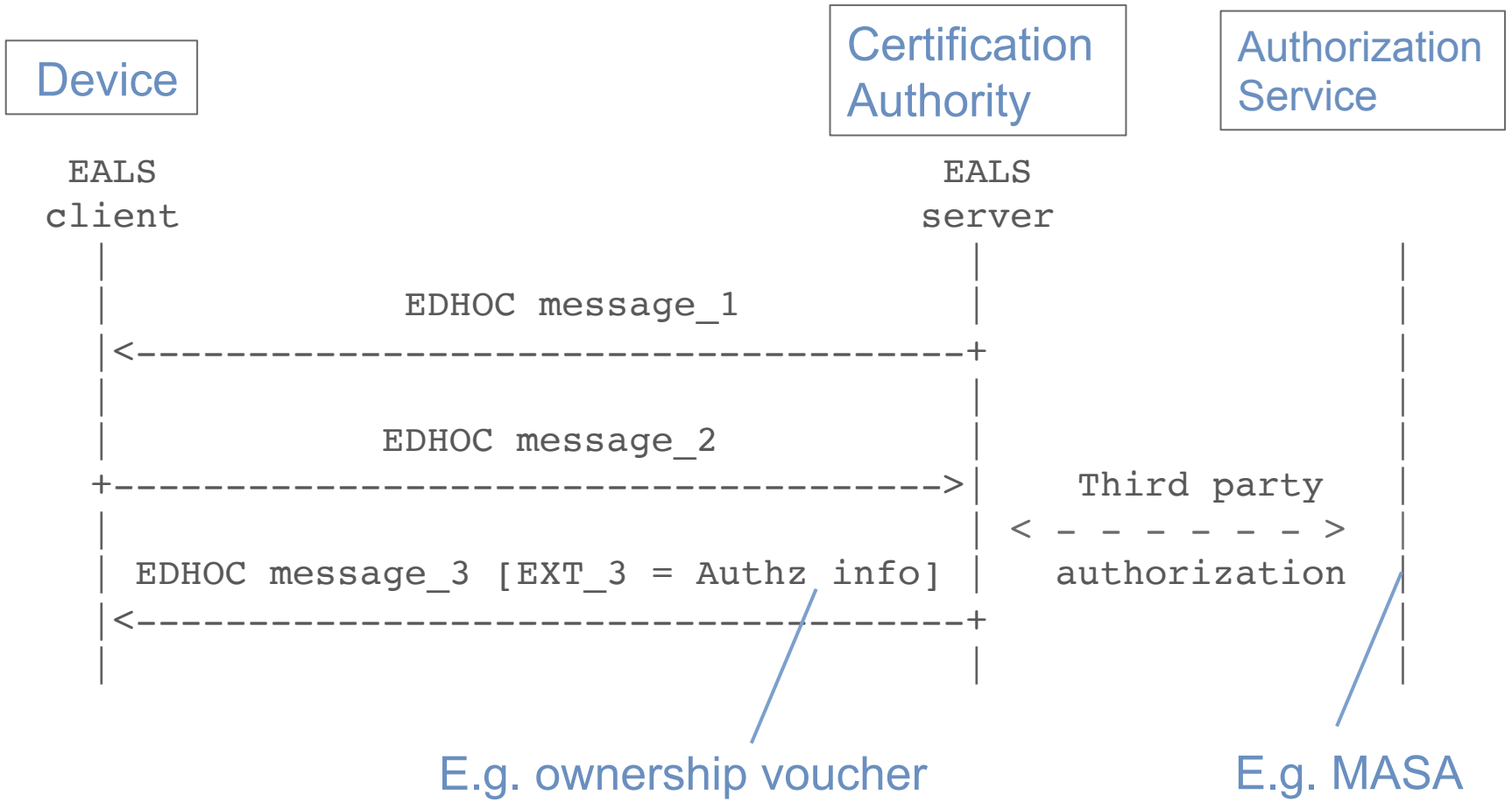
Phase 2: Enrollment



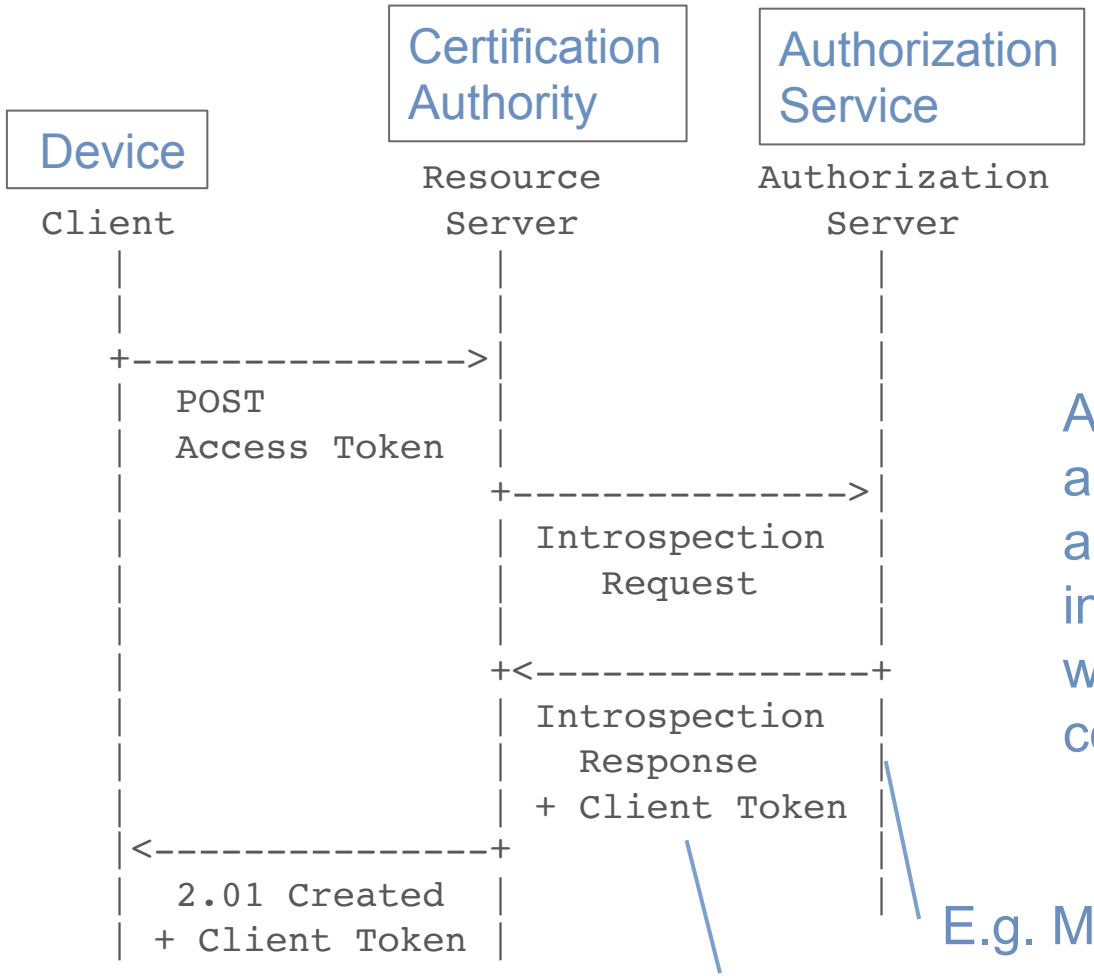
Simple CMC protected with OSCOAP
CSR = Certification Signing Request

The figure is a simplification, e.g. the EALS server may be Registration Authority/Registrar which in turn communicates with the CA

Phase 1: EDHOC



Phase 1 (alt.): ACE Client Token



ACE establishes authorization information and keys in Client and RS, which may have never communicated before.

Thank you!

Comments/questions?

https://tools.ietf.org/html/draft-selander-ace-eals