Protecting EST operations with EDHOC/OSCORE

draft-selander-ace-coap-est-oscore-04

Göran Selander, Ericsson
Shahid Raza, RISE
Martin Furuhed, Nexus
Mališa Vučinić, INRIA
Timothy Claeys, INRIA

ACE, IETF 109, November 2020

Background

- CMS = Cryptographic Message Syntax (RFC 5672)
  - Encapsulation syntax for signatures and encryption
- CMC = Certificate Management over CMS (RFC 5272)
  - Certificate management protocol using CMS
- EST = Enrollment over Secure Transport (RFC 7030)
  - Simple PKI messages in CMC protected by TLS and HTTP
- EST-coaps = draft-ietf-ace-coap-est
  - EST payloads protected by DTLS and CoAP
- **EST-oscore = this draft**
  - **EST payloads protected by EDHOC/OSCORE**

Protocol Layering

```
+-------------------------------------------------+
|          EST request/response messages          |
+-------------------------------------------------+
|   CoAP with OSCORE    |   HTTP with OSCORE      |
+-------------------------------------------------+
|   UDP  |  DTLS/UDP    |   TCP    |   TLS/TCP    |
+-------------------------------------------------+
```

— EST builds on EST-coaps, follow EST design

— DTLS record layer is replaced, or complemented, with OSCORE (RFC 8613)

— DTLS handshake is replaced, or complemented, with EDHOC (draft-ietf-lake-edhoc)

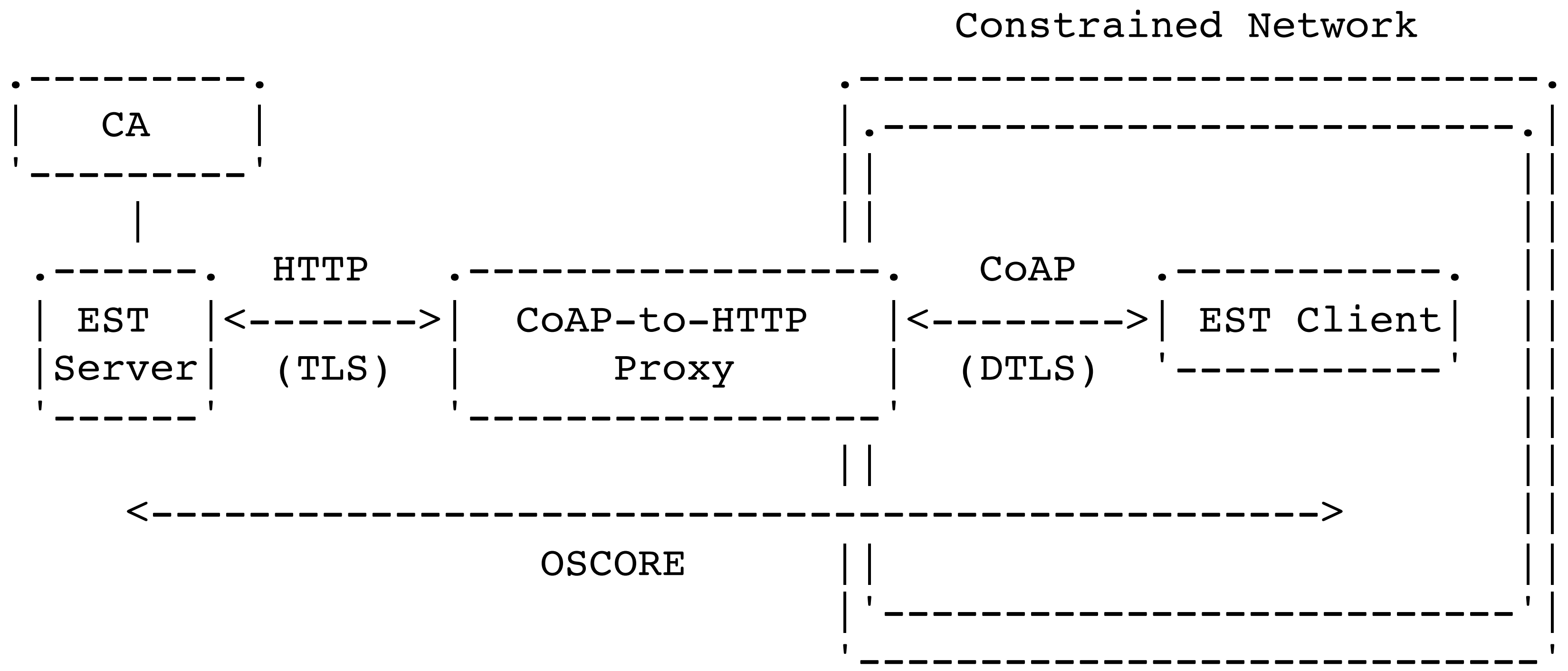
Re-use of EST-coaps

- Discovery
  - .well-known/core
- EST functions
  - /crts, /sen, /sren, /skg, /skc, /att
- Payload formats
- Message bindings
- CoAP response codes
- Delayed responses
- Fragmentation
  - CoAP Block1/2

Additions

- ”osc”: new resource type attribute used in discovery
- /rpks: similar to /crts, but requesting raw public key based trust anchors
- CBOR encoded EST payloads
  - Certificate Signing Request
  - Certificates (CBOR certificates as defined in draft-mattsson-cose-cbor-cert-compress)

CoAP-to-HTTP proxy



- EST server commonly outside the constrained network
  - Supporting HTTP but not CoAP
- OSCORE protects EST payloads over mixed CoAP/HTTP
- **CoAP-to-HTTP proxy need not be trusted**

Next steps

— Complete the additions

— Submit -05

— Reviews?