Protecting EST payloads with OSCORE (EST-OSCORE)

draft-selander-ace-coap-est-oscore

G. Selander, Ericsson
S. Raza, RISE SICS
M. Furuhed, Nexus
M. Vučinić, Univ. of Montenegro
Background

- EALS (draft-selander-ace-eals) was discussed at ACE WG virtual interim Oct 19, 2017

- The WG was supportive but proposed changes to align with EST / EST-CoAPs

- EST-OSCORE (this draft) is a rewrite of EALS doing that
Similar to EST-CoAPs

EST-CoAPs (draft-ietf-ace-coap-est):
• EST payloads transported with CoAP protected with DTLS

EST-OSCORE (this draft):
• EST payloads transported with CoAP protected with OSCORE

Most parts of EST-CoAPs apply directly to EST-OSCORE:
• EST message types, message bindings, message fragmentation, CoAP response codes, new Content-Formats, shorter Uri-Path, …
Differences with EST-CoAPs

1. Key establishment
   - EST-CoAPs establishes keys with a DTLS handshake
   - EST-OSCORE allows different ways to establish keys
     - Pre-shared keys
     - OSCORE profile of ACE (draft-ietf-ace-oscore-profile)
     - Key exchange

2. Discovery
   - Discovery is the same, but support for OSCORE is indicated by an attribute

3. Proxying (next slide)
CoAP-HTTP proxying

EST-CoAPs:

EST-OSCORE:

ESTcoaps-to-HTTPS proxy at the CoAP boundary.

CoAP-to-HTTP proxy at the CoAP boundary.
Questions for the WG

• Was this the change you requested?

• Other comments?

• Still supportive of the draft?