

Protecting EST payloads with OSCORE (EST-OSCORE)

draft-selander-ace-coap-est-oscore-02

IETF 104, ACE WG
Göran Selander, Ericsson
Shahid Raza, RISE SICS
Martin Furuhed, Nexus
Mališa Vučinić, Inria

Background

- ACE WG virtual interim on certificate enrolment for constrained devices (Oct 2017)
 - Two candidate solutions
 - Protect enrolment with DTLS
→ draft-ietf-ace-coap-est (**EST-coaps**)
 - Protect enrolment with OSCORE
→ draft-selander-ace-coap-est-oscore (**EST-OSCORE**; this draft)
 - Question: *“For the two solutions, which one should we work on?”*
 - Answer: *“Do both, EST-coaps first”*
- EST-coaps is done. We now restart work on EST-OSCORE.

Reminder about EST-OSCORE

- Certificate enrolment for devices implementing OSCORE/EDHOC
 - Reuse OSCORE for protecting enrolment
 - Avoid implementing multiple communication security protocols
- Most parts of EST-coaps apply directly to EST-OSCORE
 - EST message types, message bindings, CoAP response codes, new Content-Formats, shorter Uri-Path, . . .
- EST payloads protected with OSCORE
 - Instead of DTLS record layer

EST request/response messages		
CoAP with OSCORE		HTTP with OSCORE
UDP		DTLS/UDP TLS/TCP

Next Steps

- Detail the mapping to EST-coaps
- Optional EDHOC run
- Other suggestion?