EST over coaps

Peter van der Stok, Sandeep Kumar, Panos Kampanakis
Martin Furuhed, Shahid Raza, Michael Richardson

IETF 101 - ACE Working Group
Enrollment over Secure Transport (EST) [RFC7030] uses HTTP and TLS

This draft proposes CoAP and DTLS to support constrained devices

Application areas:
• Secure bootstrapping devices
• Distribution of identity (certificates) and keying material
Major progress

- Removed all BRSKI extensions to EST moved to draft-richardson-anima-ace-constrained-voucher-03 such as:
  request-voucher
  voucherstatus
  CBOR serialization of voucher

- Michael produced diagram to show relations between bootstrapping drafts as function of deployment environment
  https://trac.ietf.org/trac/int/wiki/EnrollmentRoadmap

Many thanks to Benjamin, Jim, and Hannes for ietf-0 comments
Current issues

• Proxying section to be clarified, role of RA
• DTLS 1.2 vs DTLS 1.3 forward compatibility
• Long wait (draft-hartke-core-pending-02 )
• Server key generation only COSE ?
• Use MAY and MUST for
  • long names .well-known/est/ArbitraryLabel/est-name
  • short names: .well-known/est/est-short-name
TODO

• Operational parameter values
• Server side key generation using simple multipart encoding
• Explain trust relations for http/coap proxying
BRSKI modes

- generic (YANG) voucher semantics
- constrained voucher (CBOR) (xxxx?)
- constrained signature (COSE)
- constrained security (EDHOC)
- constrained object security (OSCORE)
- ultral-constrained bootstrap
- stateless, CoAP proxy
- 6tisch minimal security
- one-touch pre-shared auth keys
- constrained object security (OSCORE)
- constrained signature (COSE)
- constrained security (EDHOC)
- constrained bootstrap
- stateless, CoAP proxy
- 6tisch zero touch
- UDP (EST-COAP) based security (DTLS) [est-coaps]
- slightly-constrained bootstrap
- stateless, IPIP proxy
- stateless, DTLS proxy?
- circuit-level proxy
- unconstrained bootstrap
- other: netconf call home, USB key
- BRSKI
- JSON format voucher
- standard signature (CMS) (RFCxxx)
- TCP (EST) based security (TLS)
- NETCONF
- ultra-constrained bootstrap
- constrained bootstrap
- MASA
REMINDER
Application areas

BRSKI also for 6tisch
Pledge and EST server exchange Certificates and Vouchers

BRSKI [anima]: Bootstrapping Remote Secure Key Infrastructures

Authenticated/authorized endpoint cert enrollment (and optionally key provisioning) through a CA or Registration Authority.