EST over coaps

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

IETF 102 - ACE Working Group

EST over coaps

Enrollment over Secure Transport (EST) [RFC7030]
uses HTTP and TLS

This draft proposes CoAP and DTLS
to support constrained devices

Application areas:

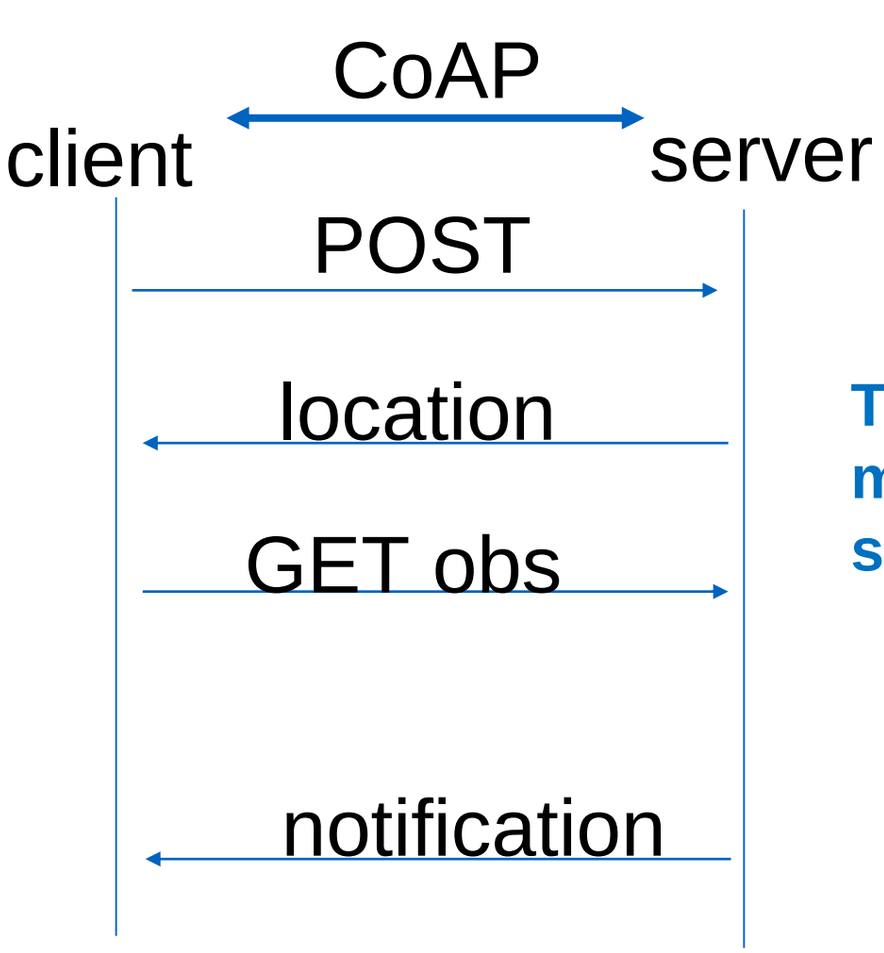
- Secure bootstrapping devices
- Distribution of identity (certificates)

Major updates

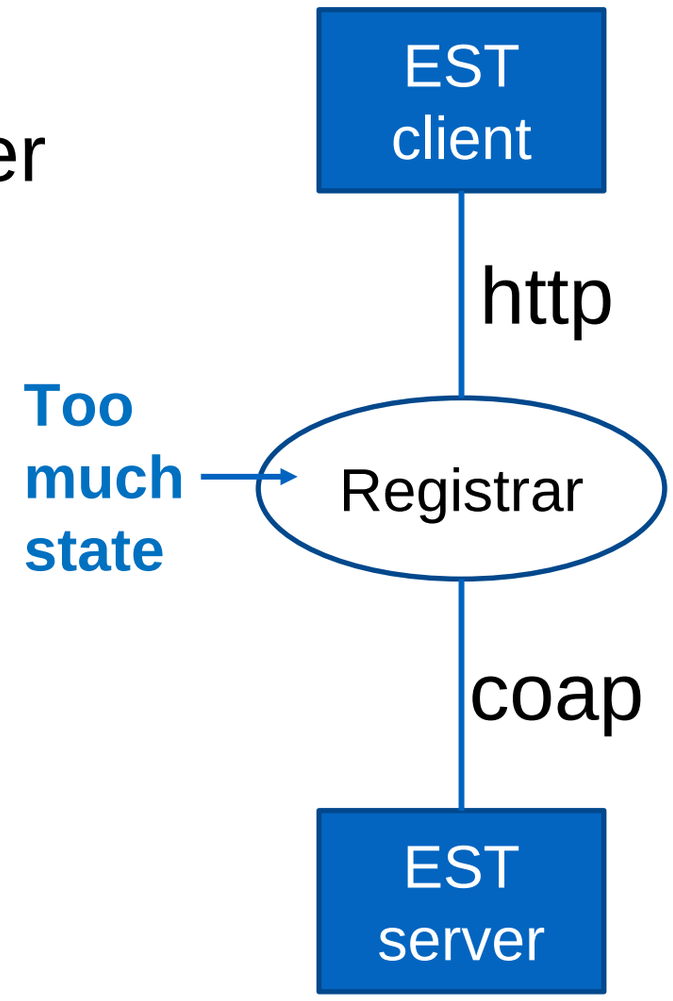
- **Long delay handling**
- **Multipart payload**
- Examples improved
- Parameter section included
- https/coaps Registrar instead of “proxy”
- Server key generation improved and motivated

Long delay handling

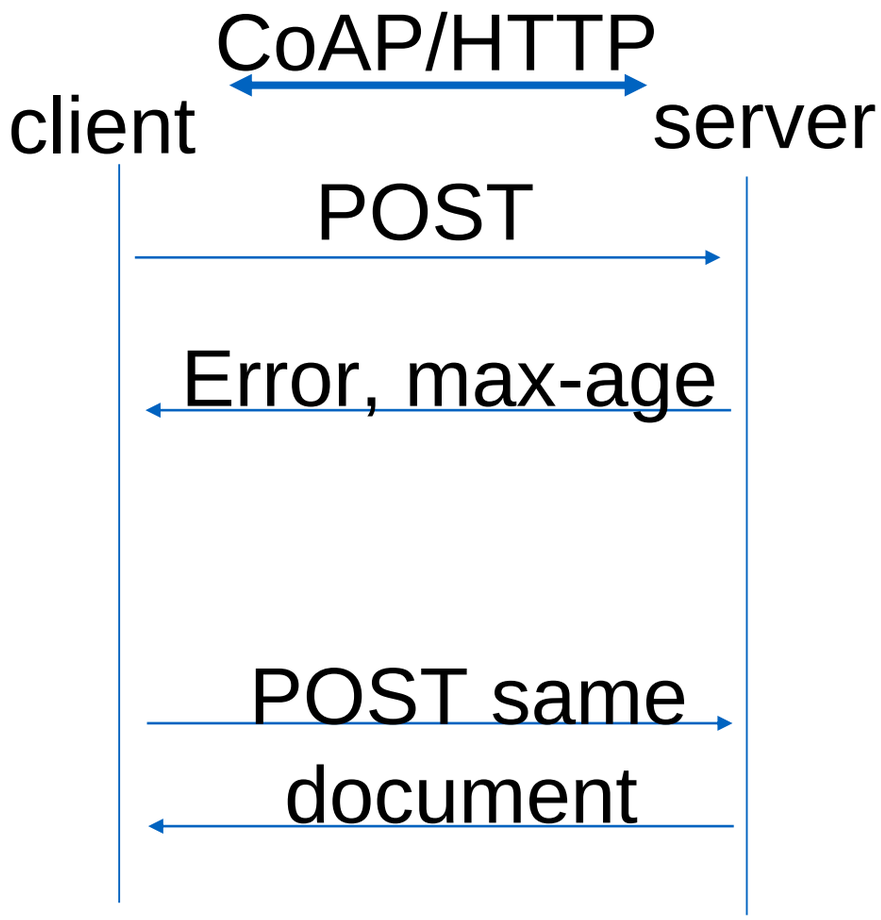
ORIGINAL text



Problem



CURRENT text



Two shorter delay examples in draft

Multipart payload

In serverkeygen (EST and EST-coaps) ,
the returned payload is composed of two parts featuring different Media types

Currently, this was not possible in CoAP, specifying only one content-format

The draft ietf-core-multipart-ct specifies a media type containing multiple ones.
Uses CBOR array: [CF-1, payload-1, CF-2, payload-2,…….]

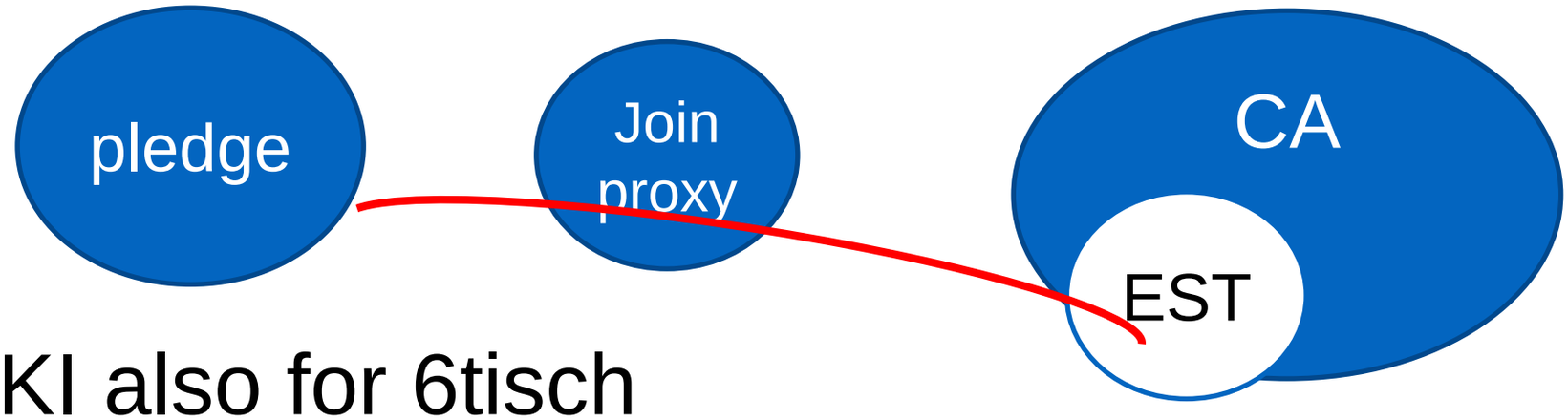
For example, a payload containing two separate media format parts looks:
[42, h’0123456789abcdef’, 0, h’fedcba9876543210’]

Going on

- Early Content-Formats assignment requested
- Update example payloads
- Prepare interop
- RISE, Nexus, Cisco, ARM, Sandelman

REMINDER

Application areas



BRSKI also for 6tisch

Pledge and EST server exchange Certificates and Vouchers

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