draft-friel-acme-integrations

ACME BRSKI integration

Friel, Barnes cisco

Summary

- EST (which BRSKI leverages) defines the protocol that clients use to enrol with an EST Registration Authority (RA) using PKCS#10 / PKCS#7 payloads
- EST does not define the mechanism that the RA uses to talk to the CA
- ACME “describes a protocol that a CA and an applicant can use to automate the process of … certificate issuance.”
- draft-friel-acme-integrations describes how an EST RA can leverage ACME to integrate with a CA for automated certificate issuance
  - No changes required to existing ACME, EST or BRSKI drafts (probably)

draft-friel-acme-integrations Use Cases

- ACME issuance of sub-domain certificates
- Multiple client / device certificate integrations
  1. EST
     - RFC 7030 - Enrollment over Secure Transport
  2. **BRSKI**
     - **draft-ietf-anima-bootstrapping-keyinfra - Bootstrapping Remote Key Infrastructures**
  3. TEAP
     - RFC 7170 – Tunnel Extensible Authentication Protocol
  4. TEAP-BRSKI
     - draft-lear-eap-teap-brski - Bootstrapping Key Infrastructure over EAP

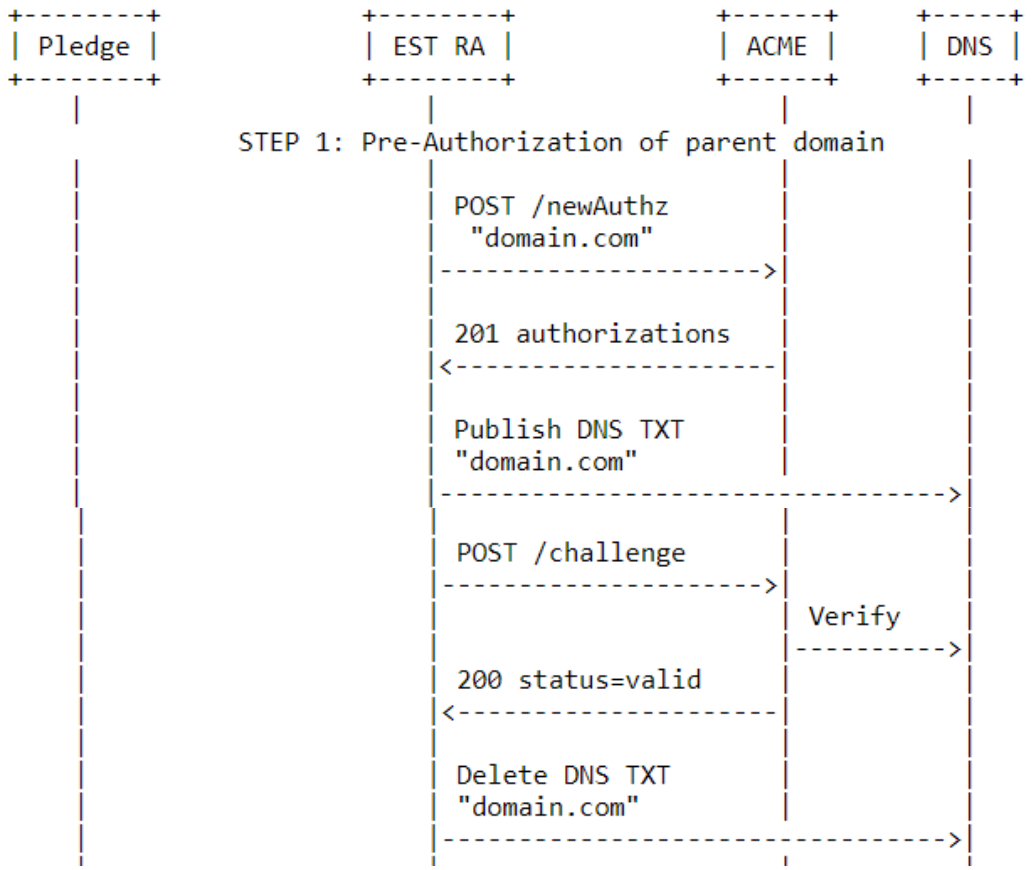
Related Drafts

- draft-yusef-acme-3rd-party-device-attestation
- draft-moriarty-acme-client

- Preliminary discussions about alignment have taken place
- Side meeting scheduled
  - Coller meeting room
  - 9am Wednesday morning

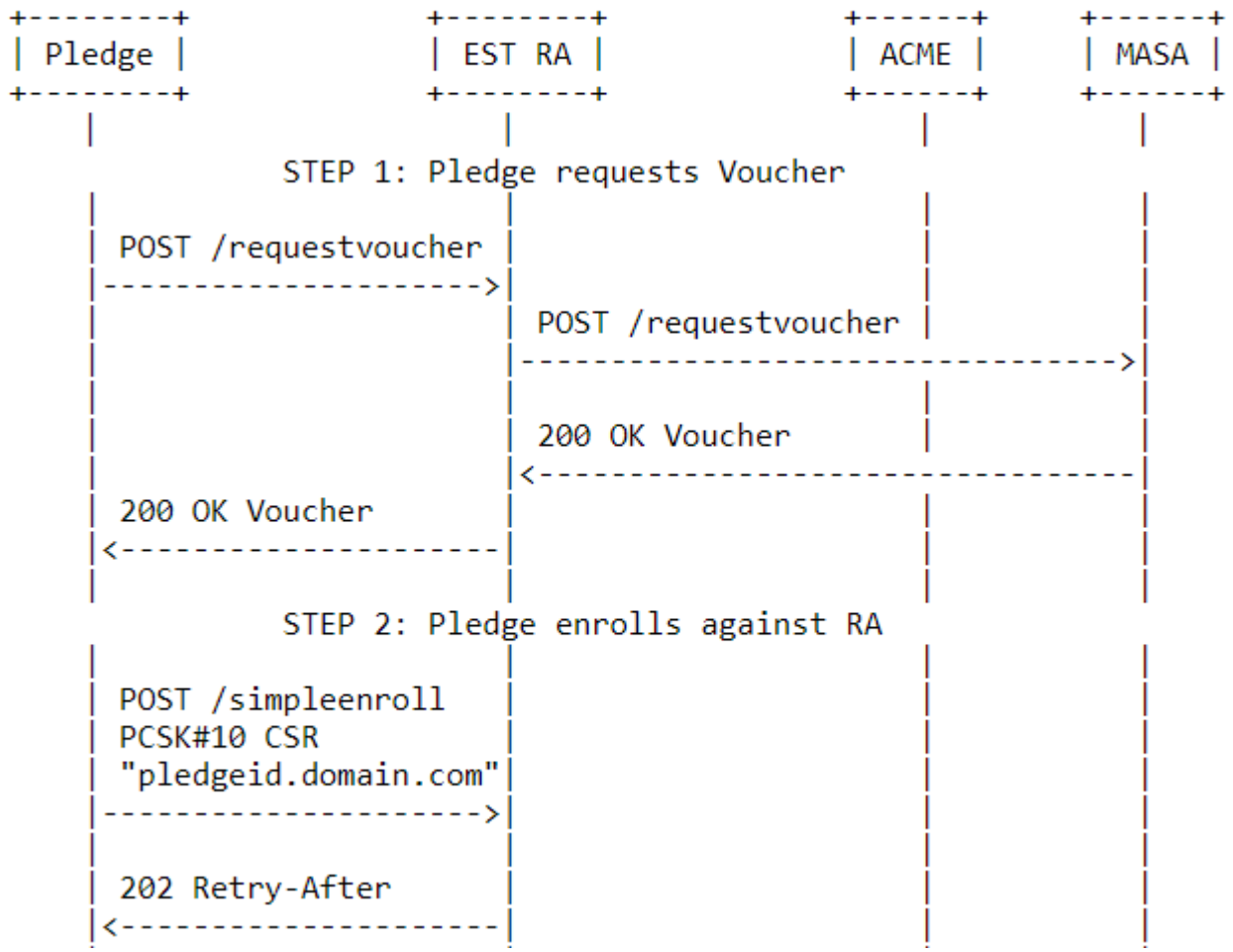
BRSKI -> ACME 1 of 4

- ACME domain authorization



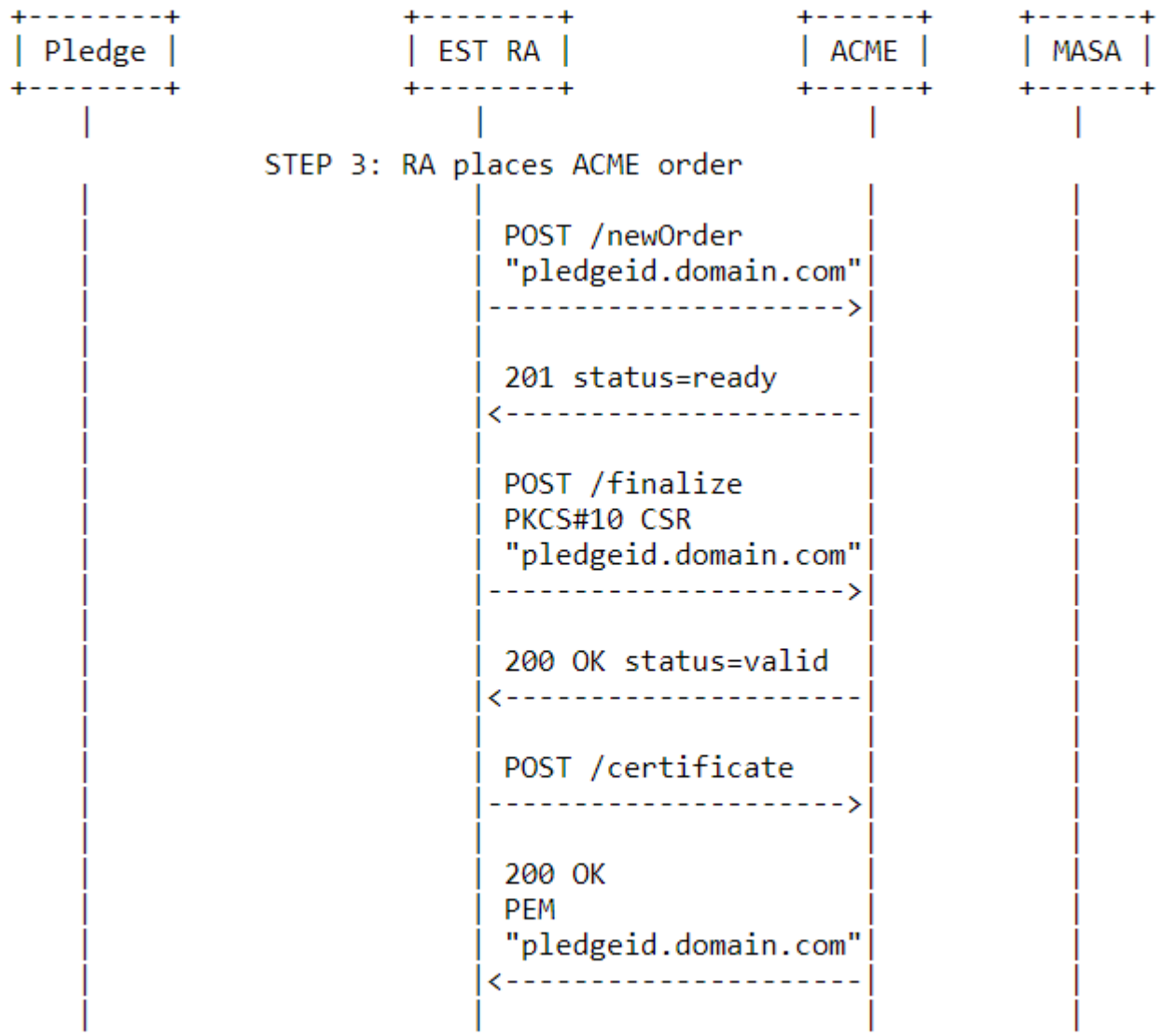
BRSKI -> ACME 2 of 4

- Pledge requests voucher
- Pledge starts enrol process



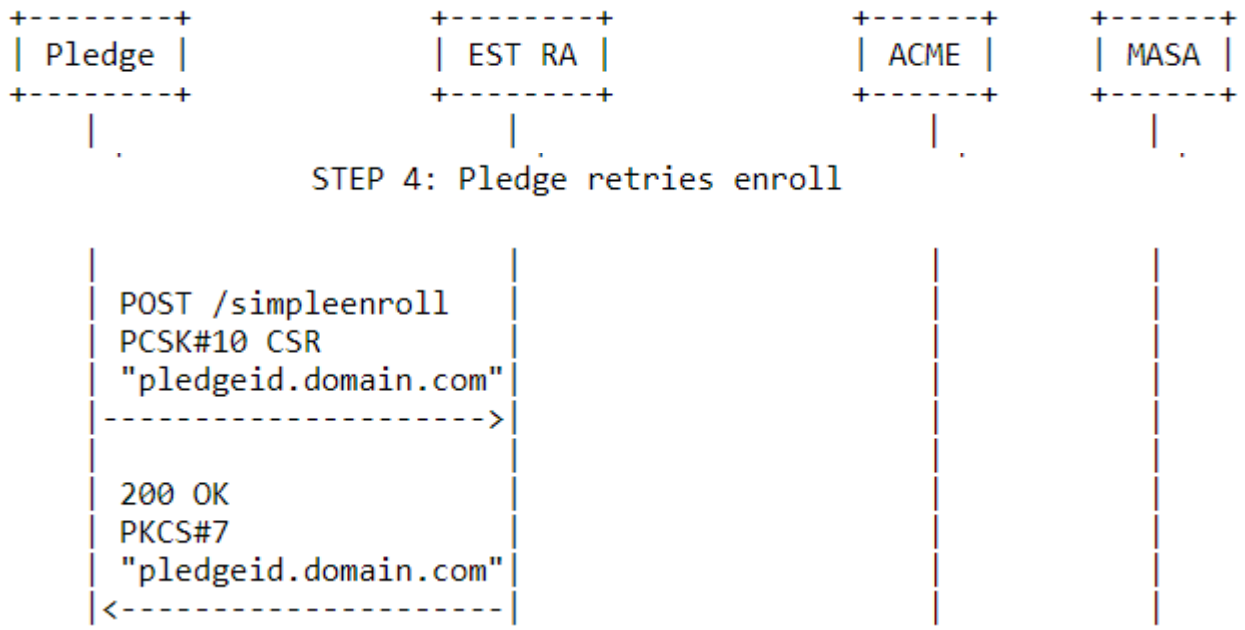
BRSKI -> ACME 3 of 4

- RA completes ACME order



BRSKI -> ACME 4 of 4

- Pledge retries and completes enrol



Discussion

- Is this of broader interest?
- Note: this short presentation will be given at ACME, ANIMA and EMU sessions
- Side meeting reminder: Coller, 9am Wednesday