

draft-friel-acme-integrations

Friel, Barnes

Cisco

Shekh-Yusef

Avaya

TL;DR

- Describes how ACME RFC 8555 can be integrated with multiple existing client / device certificate enrolment mechanisms without requiring any changes required to ACME

Multiple Client / Device Integration Use Cases

1. EST

- RFC 7030: Enrollment over Secure Transport

2. BRSKI

- draft-ietf-anima-bootstrapping-keyinfra: Bootstrapping Remote Key Infrastructures

3. BRSKI Cloud Registrar

- draft-friel-anima-brski-cloud: Specifies BRSKI behaviour with default cloud registrar

4. TEAP

- RFC 7170: Tunnel Extensible Authentication Protocol

5. TEAP Update and Extensions for Bootstrapping

- draft-lear-eap-teap-brski: PKCS#10 / PKCS#7 Updates and BRSKI Extensions

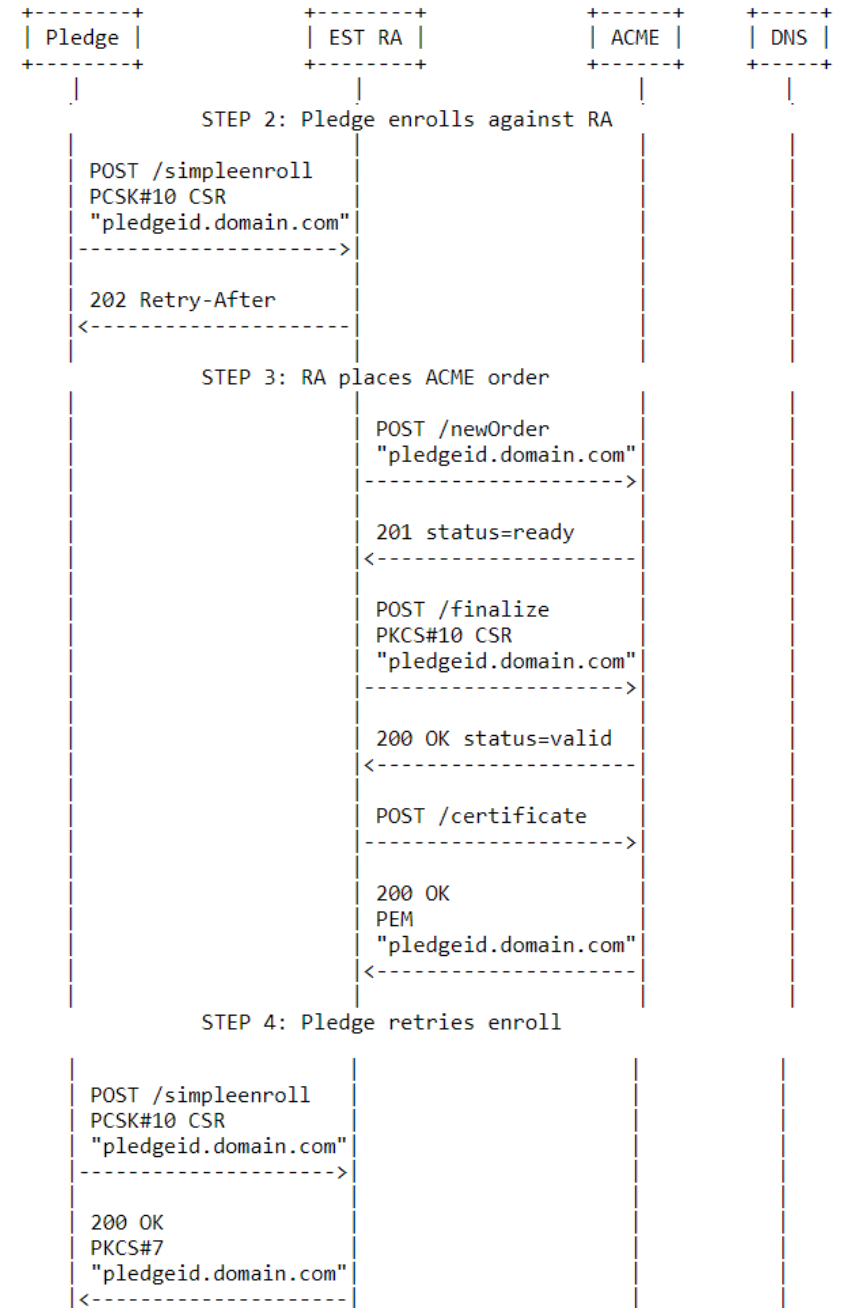
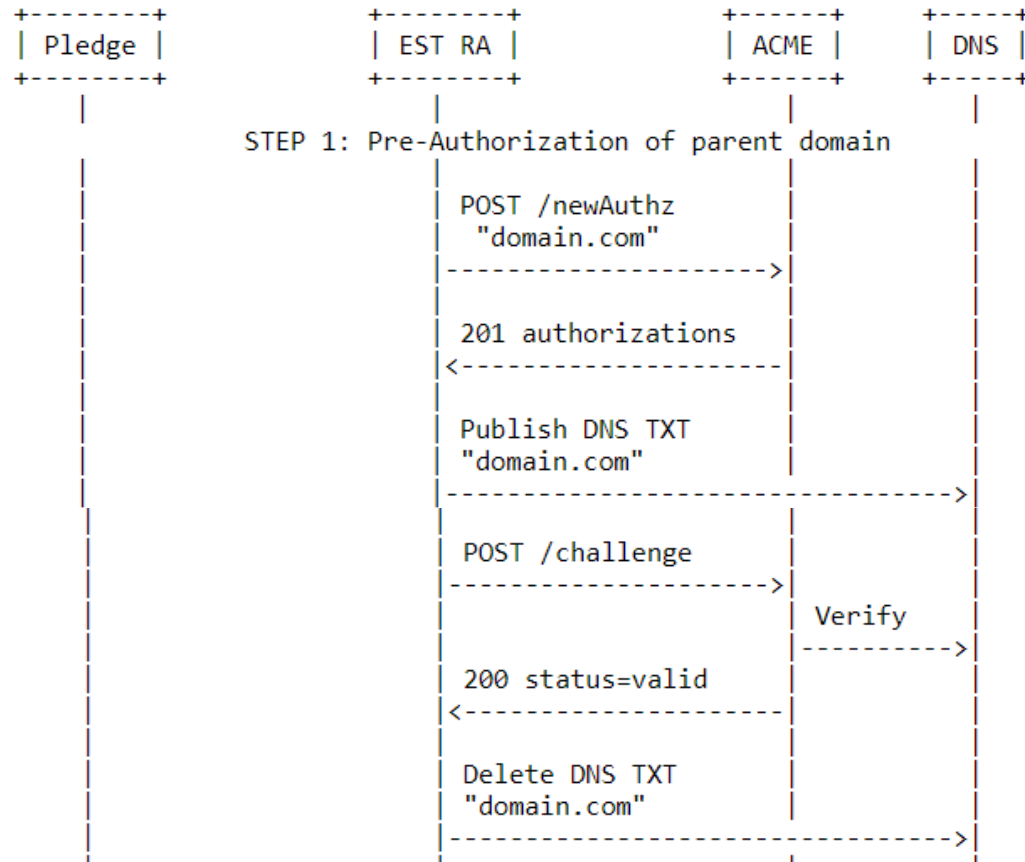
What has changed since IETF 105

- ACME subdomain use case split out into separate document
 - draft-friel-acme-subdomains
- BRSKI Cloud Registrar use case added
 - draft-friel-anima-brski-cloud

Client / device certificate integrations

- EST
 - 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
- BRSKI certificate enrolment leverages EST
 - EST<->ACME Integrations are equally applicable to BRSKI
- TEAP
 - Defines the protocol that clients use to enrol with a TEAP server using PKCS#10 / PKCS#7 payloads
 - TEAP does not define the mechanism that the TEAP server uses to talk to the CA

EST -> ACME



Discussion

- To do: Security considerations
- Integrations span across ACME, ANIMA, EMU WGs
- Where does this belong?
- Is there interest in continuing this work?
- Next Steps?