draft-friel-acme-integrations

ACME TEAP integration

Friel, Barnes cisco

Summary

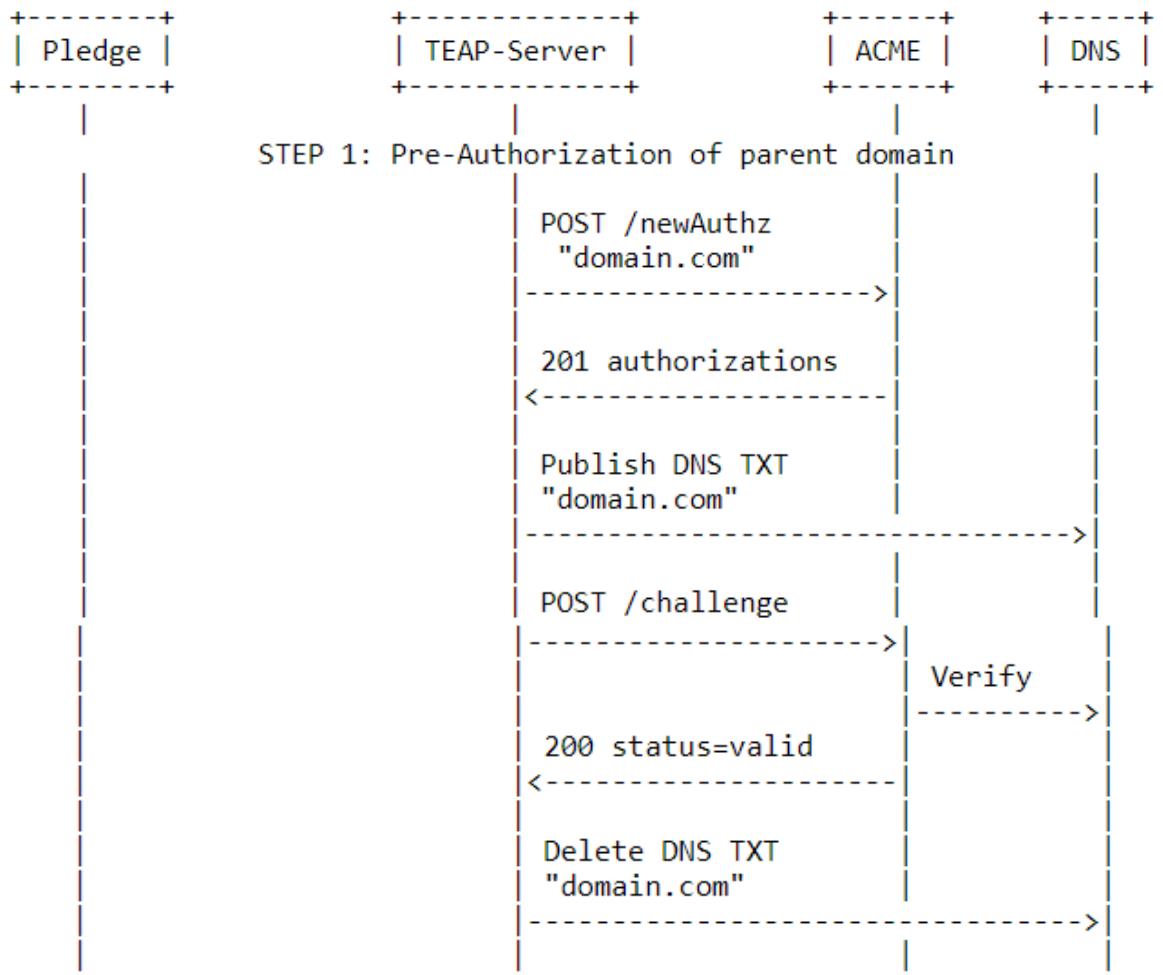
- TEAP (RFC 7170) defines how a Peer can perform certificate enrolment by exchanging PKCS#10 / PKCS#7 payloads with a TEAP server
- TEAP does not define how the TEAP server interacts with the CA
- ACME “describes a protocol that a CA and an applicant can use to automate the process of … certificate issuance.”
- draft-friel-acme-integrations describes how a TEAP server can leverage ACME to integrate with a CA for automated certificate issuance
  - Equally applicable to TEAP-BRKSI (draft-lear-eap-teap-brski)
  - No changes required to existing ACME or TEAP 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

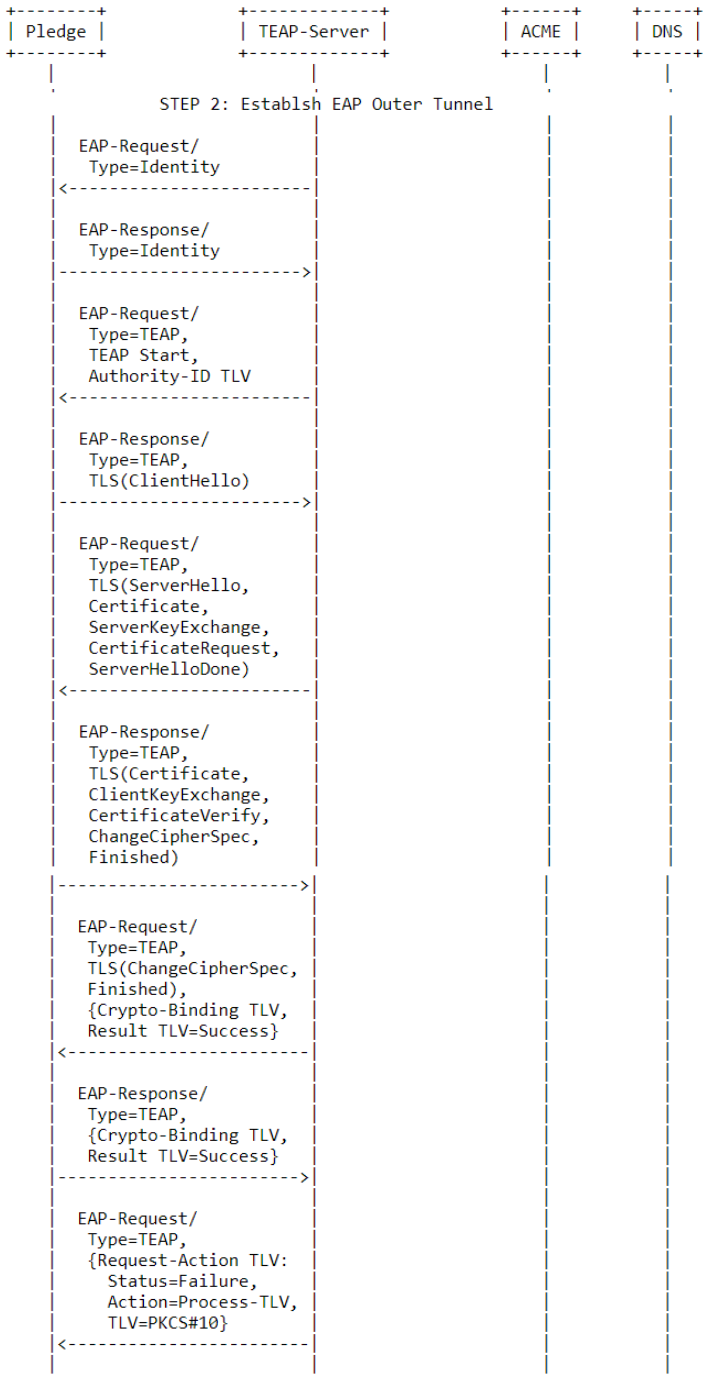
TEAP -> ACME 1 of 3

- ACME domain authorization



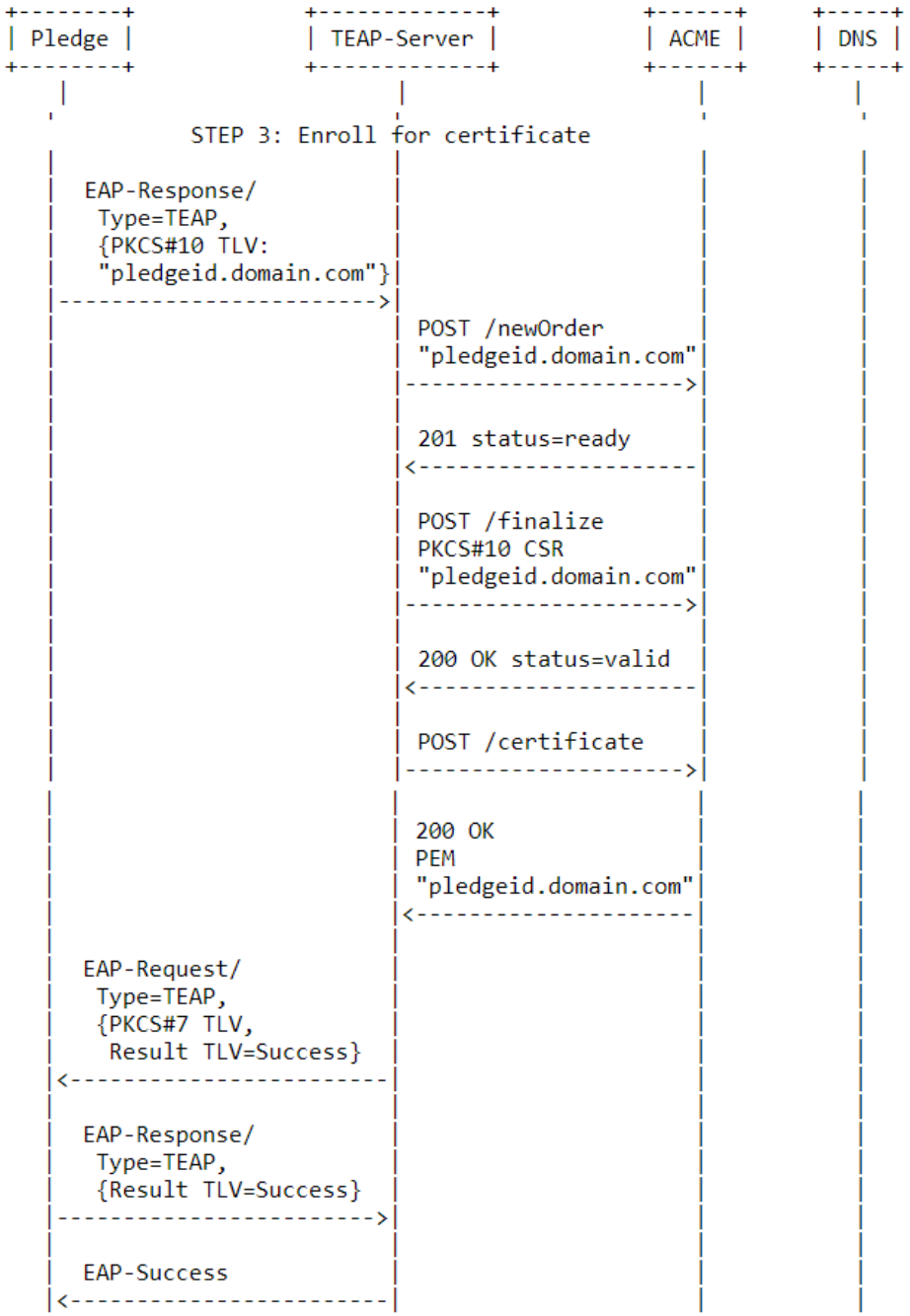
TEAP -> ACME 2 of 3

- Peer establishes TEAP outer TLS tunnel



TEAP -> ACME
3 of 3

- Peer enrols for certificate



Discussion

- Is this of broader interest?
- Do we need a backoff/retry mechanism in response to the Peer's PKCS#10 TLV?
- Are there channel binding issues not covered by https://tools.ietf.org/html/rfc7170#section-3.8.2 "Certificate Provisioning within the Tunnel" ?
- Related drafts
  - draft-yusef-acme-3rd-party-device-attestation
  - draft-moriarty-acme-client