draft-ietf-acme-integrations

Friel, Barnes	Cisco
Shekh-Yusef	Auth0
Richardson	Sandelman Software Works

TL;DR

- Describes how ACME RFC 8555 can be integrated with multiple existing client / device certificate enrolment mechanisms without requiring any changes 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 (with Updates)
   - RFC 7170 and draft-lear-eap-teap-brski : Tunnel Extensible Authentication Protocol

What has changed since IETF 106

- TEAP and TEAP-BRSKI sections collapsed into single section “ACME Integration with TEAP” section
- Baseline TEAP (RFC 7170) is missing some important certificate enrolment capabilities that are introduced in draft-lear-eap-teap-brski
  - CSR Attributes TLV: Allows a server to tell a client what list of attributes to include in the CSR request, similar to EST (RFC 7030)
  - Retry-After TLV: Allows a server to indicate to a client that the CSR request has been accepted for processing but a response is not yet available, similar to EST /simpleenroll 202 response code

Todo: Security Considerations

- No changes to referenced specification security considerations
  - EST (RFC 7030)
  - BRSKI (draft-ietf-anima-bootstrapping-keyinfra)
  - TEAP (RFC 7170)
- Security considerations still not reviewed and / or complete for
  - draft-lear-eap-teap-brski
  - draft-friel-anima-brski-cloud
- As this document is informational and does not change any of the referenced specifications, we expect the security considerations to be a summary of the referenced documents

Next Steps

- Reviewers please
- Feedback please