draft-ietf-acme-integrations

Friel, Barnes   Cisco

Shekh-Yusef   Auth0

Richardson   Sandelman Software Works

TL;DR

- Informational draft
- Describes how ACME RFC 8555 can be integrated with multiple existing client / device certificate enrolment mechanisms without requiring any changes to ACME
  - EST
  - BRSKI / BRSKI Cloud
  - TEAP

Changes in -03 since IETF109

- BRSKI Integration id-kp-cmcRA Open Item addressed
- BRSKI RA end entity certificate must have id-kp-cmcRA set when signing voucher requests sent to MASA
- Some ACME servers (e.g. Public CAs like Let's Encrypt) may be unwilling to issue an end entity certificate with id-kp-cmcRA set
- Therefore the BRSKI RA may use ACME as a CA for issuing Pledge certificates, but may need to get its own end entity certificate from a different CA e.g. an operator private CA

Next Steps

- Reviewers please
- Feedback please