# 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 -02 since IETF108

- Added Security Considerations
  - ACME integration service could be configured with keys for  DNS updates
    - Consider restricting blast radius / DNS zone of these keys
  - ACME integration service could be authorised to write to HTTP servers
    - Consider restricting blast radius of these server accesses
  - ACME Infrastructure DoS
    - Integration service cert caches
- Minor editorial changes
  - Fixup some broken references
  - Nits with call flows

# Discussion Item: BRSKI Integration

- EST: 3.6.1. Client Use of Explicit TA Database

  the client MUST check either the configured URI or the most recent HTTP redirection URI against the server's identity according to the rules specified in [RFC6125], Section 6.4, **or** the EST server certificate MUST contain the **id-kp-cmcRA** [RFC6402] extended key usage extension.

- BRSKI: 5.5.4. MASA verification of domain registrar

  The MASA MUST verify that the registrar voucher-request is signed by a registrar. This is confirmed by verifying that the **id-kp-cmcRA** extended key usage extension field (as detailed in EST RFC7030 section 3.6.1) exists in the certificate of the entity that signed the registrar voucher-request.

- BRSKI:5.6.2. Pledge authentication of provisional TLS connection

  The pinned-domain-cert MAY be installed as a trust anchor for future operations such as enrollment (e.g. [RFC7030] as recommended) or trust anchor management or raw protocols that do not need full PKI based key management. It **can** be used to authenticate any dynamically discovered EST server that contain the **id-kp-cmcRA** extended key usage extension as detailed in EST RFC7030 section 3.6.1;

- ACME:

  Nothing to say about EKUs. Currently, ACME server policy decision what EKUs to accept and include in CSRs.

# Next Steps

- Reviewers please
- Feedback please