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
Related Drafts

- draft-yusef-acme-3rd-party-device-attestation
- draft-moriarty-acme-client

- Preliminary discussions about alignment have taken place
- Side meeting scheduled
  - Coller meeting room
  - 9am Wednesday morning
Sub-domain certificates

• ACME mandates that
  • The `identifier` in CSR must match `identifier` in `newOrder` request
  • The `identifier` in the `authorization` object must be used when fulfilling challenges via HTTP or DNS

• ACME does not mandate that
  • The `identifier` in a `newOrder` request matches the `identifier` in `authorization` object

• The specification therefore allows an ACME server to issue certificates for a given identifier (e.g. a subdomain) without requiring a challenge to be explicitly fulfilled against that identifier
  • An ACME server could issue a certificate for `sub.domain.com` where the ACME client has only fulfilled a challenge for `domain.com`
  • An ACME server could issue certificates for a number of sub-domain certificates and only require a single challenge to be fulfilled against the parent domain
Sub-domains with pre-authorization

**STEP 1: Pre-Authorization of parent domain**

- POST /newAuthz "domain.com"
- 201 authorizations
- Publish DNS TXT "domain.com"
- POST /challenge
  - Verify
  - 200 status=valid
- Delete DNS TXT "domain.com"

**STEP 2: Place order for subdomain**

- POST /newOrder "sub.domain.com"
- 201 status=ready
- POST /finalize CSR "sub.domain.com"
- 200 OK status=valid
- POST /certificate
  - 200 OK
  - PKI "sub.domain.com"
Client / device certificate integrations

• EST (which BRSKI leverages) 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
• TEAP (which TEAP-BRSKI leverages) 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
• The draft illustrates how ACME can be used to integrate an EST RA or a TEAP server with a CA
  • No changes are required to EST, TEAP or ACME specifications
  • The sub-domain proposal is a nice optimisation to facilitate issuance of large numbers of client / device certificates
EST -> ACME

**STEP 1: Pre-Authorization of parent domain**

- POST /newAuthz "domain.com"
  - 201 authorizations
  - Publish DNS TXT "domain.com"
  - POST /challenge
    - Verify
    - 200 status=valid
  - Delete DNS TXT "domain.com"

**STEP 2: Pledge enrolls against RA**

- POST /simpleenroll
  - PKCS#10 CSR "pledgeid.domain.com"
  - 202 Retry-After

**STEP 3: RA places ACME order**

- POST /newOrder "pledgeid.domain.com"
  - 201 status=ready
  - POST /finalize
    - PKCS#10 CSR "pledgeid.domain.com"
    - 200 OK status=valid
  - POST /certificate
    - 200 OK
    - PEM "pledgeid.domain.com"

**STEP 4: Pledge retries enroll**

- POST /simpleenroll
  - PKCS#10 CSR "pledgeid.domain.com"
  - 200 OK
  - PKCS#7 "pledgeid.domain.com"
Discussion

• Is the sub-domain use case of interest to ACME CAs?
  • Is this worth formally documenting?

• Are the client / device use cases of interest?
  • Note: this short presentation will be given at ACME, ANIMA and EMU sessions
  • Side meeting reminder: Coller, 9am Wednesday