draft-friel-acme-subdomains

Friel, Barnes  Cisco
Hollebeek    DigiCert
Sub-domain certificates

- ACME (RFC 8555) 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
- 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"
3 Changes from RFC 8555

1 x Substantive

1 x Errata

1 x Minor Addition
Substantive Change: newAuthz handling

• RFC 8555 section “7.4.1 Pre-authorization” states:

  If the server is willing to proceed, it builds a pending authorization object from the inputs submitted by the client:
  o "identifier" the identifier submitted by the client

  • i.e. the identifier in the authorization object MUST match that in the newAuthz request

• draft-friel-acme-subdomains states:

  If the client submits a newAuthz request for a subdomain: The server MUST return a status 201 (Created) response. The response body is a newly created authorization object for the parent domain with status set to "pending"

  • i.e. the identifier in the authorization object matches that of the parent domain, even if a subdomain is specified in the newAuthz request
Errata 5861: 200 OK response where appropriate

- RFC 8555 mandates a 201 response to all newAuthz requests
- Errata 5861 proposes additional text in section “7.4.1 Pre-authorization”

If a server receives a newAuthz request for an identifier where the authorization object already exists, whether created by CA provisioning on the ACME server or by the ACME server handling a previous newAuthz request from a client, the server returns a 200 (OK) response with the existing authorization URL in the Location header field and the existing JSON authorization object in the body.

- i.e. return a 200 OK if the authorization object already exists
- draft-friel-acme-subdomains documents using a 200 OK where appropriate, which is a deviation from current RFC 8555
Minor Addition: New ACME Directory Metadata Field

- Directory field to advertise support for subdomains
- No field entry == no assumed default value

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Type</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>implicitSubdomainAuthorization</td>
<td>boolean</td>
<td>RFC XXXX</td>
</tr>
</tbody>
</table>
Next steps

• Missing security considerations

• Adoption?