draft-friel-acme-subdomains-04

Friel, Barnes         Cisco
Hollebeek            DigiCert
Richardson           Sandelman Software Works
Sub-domain certificates

• ACME (RFC 8555) 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.

• For example, an ACME server could issue a certificate for `foo.bar.example.com` where the ACME client has only fulfilled a challenge for `bar.example.com` or `example.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.
  • Scale benefits when issuing a large number of end entity certificates.

• ACME for subdomains may optionally be used with pre-authorizations but pre-authorizations are not required.
Changes in -04 since IETF109

• Incorporates mailer feedback on -03
• Restricts challenge type to “dns-01” for subdomains
  • i.e. “dns-01” challenge must be fulfilled against a parent Authorized Domain Name in order to issue certs for a subdomain identifier
• Incorporates proposals to address 2 Open Items
Open Items 1

Open Item: Does the client need a mechanism to indicate that they want to authorize a parent domain and not the explicit subdomain identifier? Or a mechanism to indicate that they are happy to authorize against a choice of identifiers?

E.g. for foo.bar.example.com, should the client be able to specify anywhere from 1 to 3 identifiers they are willing to fulfill challenges for?

Mailer discussion: Want to avoid server issuing challenges that the client is unable to fulfil e.g. client does not have DNT TXT control over parent ADN.

Proposal: Include an optional “parentDomainAuthorization” boolean flag with newOrder/newAuthz “identifiers” indicating if the client has control over all parent ADNs.

If true: the server may issue a challenge against the identifier FQDN or any parent ADN
If false: the server must only issue a challenge against the identifier FQDN

```
{
  "identifiers": [
    {
      "type": "dns", "value": "foo.bar.example.org", "parentDomainAuthorization": true }
  ],
  "notBefore": "2016-01-01T00:04:00+04:00",
  "notAfter": "2016-01-08T00:04:00+04:00"
}
```

In this example, client indicates it can fulfill challenges against foo.bar.example.com, bar.example.com and example.com
Follow on to Open Item 1 Proposal

• Is “parentDomainAuthorization” boolean flag granular enough? Is there any need for a client to be able to specify a subset of parent ADNs it has control over?
  • e.g. if a client wants a cert for "foo.bar.example.org" and has control over "bar.example.org" but not "example.org"
  • Could include an array of ADNs that client has control over in newAuthz/newOrder requests
• Is this necessary? Draft -04 says “parentDomainAuthorization” is sufficient...

```
{  "identifiers": [    {      "type": "dns",      "value": "foo.bar.example.org",      "parentDomainAuthorization": true    },    {      "notBefore": "2016-01-01T00:04:00+04:00",      "notAfter": "2016-01-08T00:04:00+04:00"    }  ],  "identifiers": [    {      "type": "dns",      "value": "foo.bar.example.org"    },    {      "adns": [        {          "value": "bar.example.org"        },        {          "value": "example.org"        }      ]    },    {      "notBefore": "2016-01-01T00:04:00+04:00",      "notAfter": "2016-01-08T00:04:00+04:00"    }  ]
```
vs.

```
{  "identifiers": [    {      "type": "dns",      "value": "foo.bar.example.org",      "adns": [        {          "value": "bar.example.org"        },        {          "value": "example.org"        }      ]    },    {      "notBefore": "2016-01-01T00:04:00+04:00",      "notAfter": "2016-01-08T00:04:00+04:00"    }  ],  "identifiers": [    {      "type": "dns",      "value": "foo.bar.example.org"    },    {      "adns": [        {          "value": "bar.example.org"        }      ]    },    {      "notBefore": "2016-01-01T00:04:00+04:00",      "notAfter": "2016-01-08T00:04:00+04:00"    }  ]
```
Open Items 2

**Open Item:** Does the server need a mechanism to provide a choice of identifiers to the client and let the client choose which challenge to fulfil?

E.g. for foo1.foo2.bar.example.com, should the server be able to specify anywhere from 1 to 4 identifiers that the client can pick from to fulfil?

**Mailer Discussion:** Not needed and makes server state machine and tracking too complex. It is sufficient for client to be able to signal the identifiers that it can fulfill challenges against.

**Proposal:** No provision in draft for this. Clarifying statements added that if client indicates “parentDomainAuthorization” true, then server policy controls which identifier to issue challenge against.
Next steps

• Open item proposals review
• Draft -04 review
• Adoption?