draft-friel-acme-subdomains-05

Friel, Barnes  Cisco
Hollebeek   DigiCert
Richardson  Sandelman Software Works
• Specifies how a client can perform a single authorization against an Authorized Domain Name, and then request multiple certificates for identifiers in the Domain Namespace subordinate to that ADN without having to perform any authorizations per subordinate identifier
Changes in draft-05 since IETF110 / draft-04

• Reordered some sections and clarified examples
• Closer terminology alignment with CA/B
  • Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System (and maybe we could go further with terminology alignment in the draft..)
• Pre-Authorization Handling
  • Mechanism for client to specify it wants to preauthorize for the Domain Namespace subordinate to an identifier
• New Order Handling
  • Mechanism for client to specify the Domain Namespace it controls that contains the identifier it wants a certificate for
Protocol Enhancements

newAuthz Payload

The client wants to pre-authorize the Domain Namespace under the specified identifier “example.org”

```
"payload": base64url({
  "identifier": {
    "type": "dns",
    "value": "example.org",
    "domainNamespace": true
  }
})
```

newOrder Payload

The client wants a cert for the identifier “foo.bar.example.org” and indicates that it has DNS control over the Domain Namespace “example.org”

```
"payload": base64url({
  "identifiers": [
    {
      "type": "dns",
      "value": "foo.bar.example.org",
      "domainNamespace": "example.org"
    }
  ],
  "notBefore": "2015-01-01T00:00:00+00:00",
  "notAfter": "2016-01-01T00:00:00+00:00"
})
```

Authorization Object

Similar to the “wildcard” field, “domainNamespace” indicates if this authorization covers the full Domain Namespace subordinate to the identifier
### Step 1: Pre-Authorization of parent domain

**POST /acme/new-authz HTTP/1.1**

* Host: example.com
* Content-Type: application/jose+json

```json
{
  "protected": base64url{
    "alg": "ES256",
    "kid": "https://example.com/acme/acct/evOfKhNU60wg",
    "nonce": "uQp5j1Rb4vQVC3VYযyUnWg",
    "url": "https://example.com/acme/new-authz"
  },
  "payload": base64url{
    "identifier": {
      "type": "dns",
      "value": "example.org",
      "domainNamespace": true
    }
  },
  "signature": "nuS1ISlWQ8mGgE7H...QyVUL68yf3Zawps"
}
```

### Step 2: Place order for sub1.example.org

**POST /acme/new-order HTTP/1.1**

* Host: example.com
* Content-Type: application/jose+json

```json
{
  "protected": base64url{
    "alg": "ES256",
    "kid": "https://example.com/acme/acct/evOfKhNU60wg",
    "nonce": "5x11t1EKKaGtR6Pa0c1A",
    "url": "https://example.com/acme/new-order"
  },
  "payload": base64url{
    "identifiers": [
      { "type": "dns", "value": "sub1.example.org" }
    ],
    "notBefore": "2016-01-01T00:00:04:04+00:00",
    "notAfter": "2016-01-01T00:04:04+00:00"
  },
  "signature": "H6ZXT6jTZyUnPeKn...wEA4Tk1Bdh3e45Ag"
}
```

**HTTP/1.1 201 Created**

* Link: <https://example.com/acme/directory>;rel="index"
* Location: https://example.com/acme/order/T01oc8BfRgo

```json
{
  "status": "ready",
  "expires": "2016-01-01T14:09:07.992",
  "identifiers": [
    { "type": "dns", "value": "sub1.example.org" }
  ],
  "authorizations": [
    "https://example.com/acme/authz/PA1nVnsZciz"
  ],
  "finalize": "https://example.com/acme/order/T01oc8BfRgo.finalize"
}
```
Next steps

• draft-05 review of newAuthz, newOrder handling
• Adoption?