draft-friel-acme-subdomains-05

Friel, Barnes	Cisco
Hollebeek	DigiCert
Richardson	Sandelman Software Works

TL;DR

- 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

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

newAuthz Payload

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

```
"payload": base64url({
       "identifiers": [
         { "type": "dns",
           "value": "foo.bar.example.org",
           "domainNamespace": "example.org"  }
       ],
       "notBefore": "2016-01-01T00:04:00+04:00",
       "notAfter": "2016-01-08T00:04:00+04:00"
     })
```

newOrder Payload

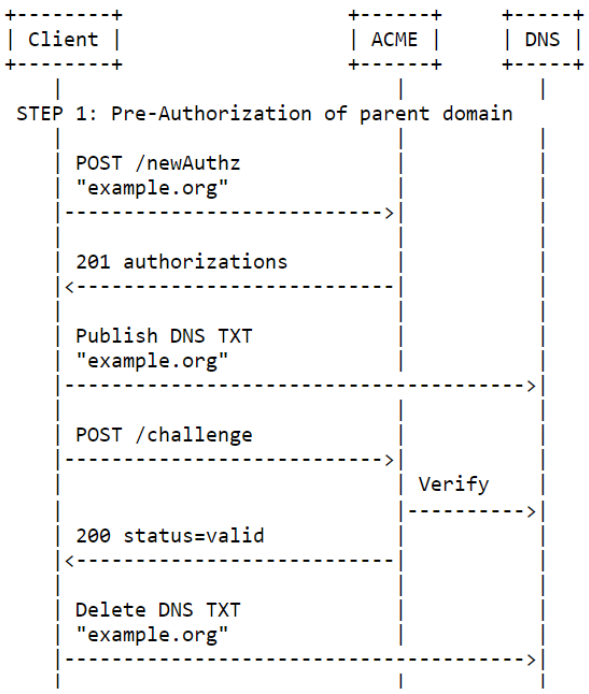
The client wants a cert for the identifier “foo.bar.example.org” and indicates that it has DNS control over the Domain Namespace “example.org”

The server may issue a challenge for any identifier between “foo.bar.example.org” and “example.org”

```
{
  "status": "valid",
  "expires": "2015-03-01T14:09:07.99Z",

  "identifier": {
    "type": "dns",
    "value": "example.org"
  },

  "challenges": [
    {
      "url": "https://example.com/acme/chall/prV_B7yEyA4",
      "type": "http-01",
      "status": "valid",
      "token": "DGyRejmCefe7v4NfDGDKfA",
      "validated": "2014-12-01T12:05:58.16Z"
    }
  ],

  "domainNamespace": true
}
```

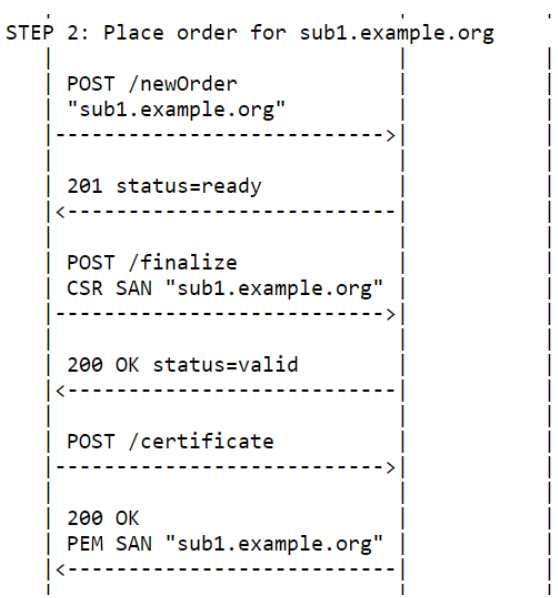
Authorization Object

Similar to the “wildcard” field, “domainNamespace” indicates if this authorization covers the full Domain Namespace subordinate to the identifier




```
POST /acme/new-authz HTTP/1.1
Host: example.com
Content-Type: application/jose+json

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://example.com/acme/acct/evOfKhNU60wg",
    "nonce": "uQpSjlRb4vQVCjVYAyyUWg",
    "url": "https://example.com/acme/new-authz"
  }),
  "payload": base64url({
    "identifier": {
      "type": "dns",
      "value": "example.org",
      "domainNamespace": true
    }
  }),
  "signature": "nuSDISbWG8mMgE7H...QyVUL68yzf3Zawps"
}
```

```
{
  "status": "pending",
  "expires": "2015-03-01T14:09:07.99Z",

  "identifier": {
    "type": "dns",
    "value": "example.org"
  },

  "challenges": [
    {
      "url": "https://example.com/acme/chall/prV_B7yEyA4",
      "type": "http-01",
      "status": "pending",
      "token": "DGyRejmCefe7v4NfDGDKfA",
      "validated": "2014-12-01T12:05:58.16Z"
    }
  ],

  "domainNamespace": true
}
```




```
POST /acme/new-order HTTP/1.1
Host: example.com
Content-Type: application/jose+json

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://example.com/acme/acct/evOfKhNU60wg",
    "nonce": "5XJ1L3lEkMG7tR6pA00clA",
    "url": "https://example.com/acme/new-order"
  }),
  "payload": base64url({
    "identifiers": [
      { "type": "dns", "value": "sub1.example.org" }
    ],
    "notBefore": "2016-01-01T00:04:00+04:00",
    "notAfter": "2016-01-08T00:04:00+04:00"
  }),
  "signature": "H6ZXtGjTZyUnPeKn...wEA4TklBdh3e454g"
}
```

```
HTTP/1.1 201 Created
Replay-Nonce: MYAuvOpaoIiywTezizk5vw
Link: <https://example.com/acme/directory>;rel="index"
Location: https://example.com/acme/order/TOlocE8rfgo

{
  "status": "ready",
  "expires": "2016-01-05T14:09:07.99Z",

  "notBefore": "2016-01-01T00:00:00Z",
  "notAfter": "2016-01-08T00:00:00Z",

  "identifiers": [
    { "type": "dns", "value": "sub1.example.org" }
  ],

  "authorizations": [
    "https://example.com/acme/authz/PAniVnsZcis"
  ],

  "finalize": "https://example.com/acme/order/TOlocrfgo/finalize"
}
```

Next steps

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