draft-ietf-acme-subdomains-02

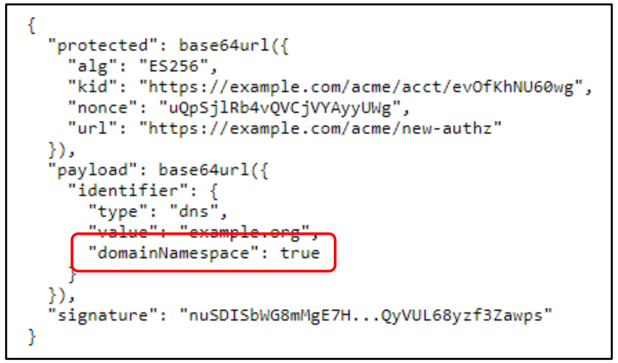
Friel, Barnes	Cisco
Hollebeek	DigiCert
Richardson	Sandelman Software Works

Changes since draft-ietf-acme-subdomains-00

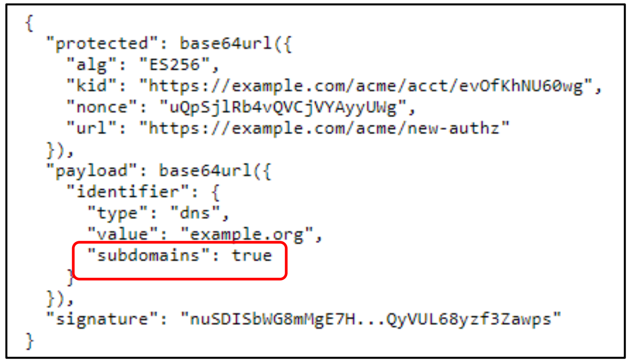
- Use RFC 8499 “DNS Terminology” consistently
  - Removed CA/Browser Terminology definitions as this is not limited to Web PKI use cases
- Updated JSON field names to use RFC 8499 aligned names
- Added additional clarifying text to examples

RFC8499 JSON Terminology Alignment

newAuthz

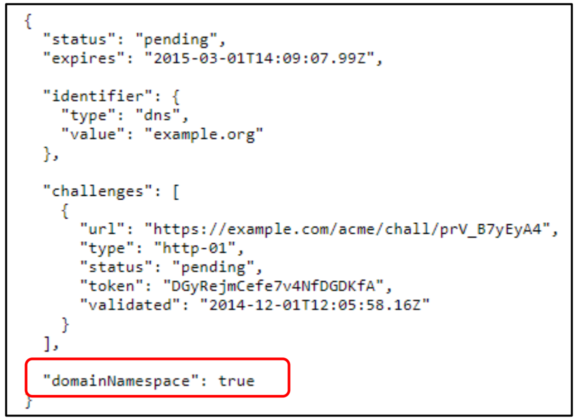


```
{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://example.com/acme/acct/evOfKhNU60wg",
    "nonce": "uQpSjlRb4vQVCjVYAyyUWg",
    "url": "https://example.com/acme/new-authz"
  }),
  "payload": base64url({
    "identifier": {
      "type": "dns",
      "value": "example.org",
 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



```
{
  "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",
      "subdomains": true
    }
  }),
  "signature": "nuSDISbWG8mMgE7H...QyVUL68yzf3Zawps"
}
```

Authorization Object

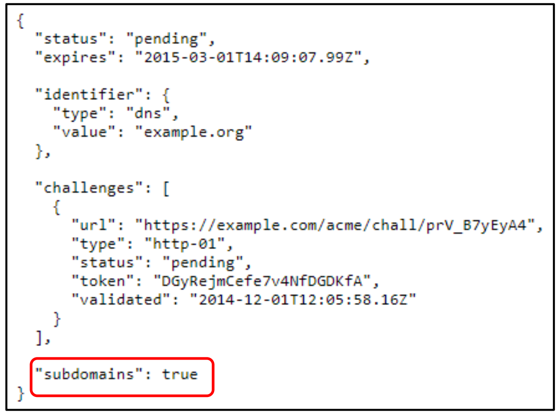


```
{
  "status": "pending",
  "expires": "2015-03-01T14:09:07.99Z",

  "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
}
```



```
{
  "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"
    }
  ],

  "subdomains": true
}
```

draft-00

draft-02

Next Steps

- Some minor editorial nits are fixed in github but not published as draft-03 yet
- Document ready for WGLC