ACME Renewal Information

draft-ietf-acme-ari-06

Aaron Gable, Let’s Encrypt
IETF 121, 2024-11-06

Since IETF 120

- Draft -05
  - Introduce “alreadyReplaced” error
  - Advice to clients re: when to supply “replaces” field

- Draft -06
  - Spelling typo fix
  - Advice to servers re: Retry-After header

- Working Group Last Call started and finished!
  - One additional typo found

What's Next

- Referred to IESG

- Advice to clients re: respecting Retry-After
  - Jacob Hoffman-Andrews has a good proposal

ACME Profiles

draft-aaron-acme-profiles-00

Aaron Gable, Let’s Encrypt
IETF 121, 2024-11-06

Since IETF 120

- Published as draft-aaron-acme-profiles-00
  - Adds “profiles” map field to Directory “meta” object
  - Adds “profile” field to Order objects
  - Adds “invalidProfile” error

- Fully implemented in Boulder and Pebble
- Not yet enabled in Let’s Encrypt’s staging environment
- Not yet implemented in public clients

Concrete Proposal

- Augment the directory:

```
Content-Type: application/json

{
  "newNonce": "https://example.com/acme/new-nonce",
  ...,
  "meta": {
    ...,
    "profiles": {
      "profile1": "https://example.com/docs/profiles#profile1",
      "profile2": "https://example.com/docs/profiles#profile2",
    }
  }
}
```

Concrete Proposal

- Augment the order request:

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

{
  "protected": base64url({...}),
  "payload": base64url({
    "profile": "profile1",
    "identifiers": [{"type": "dns", "value": "example.org"}],
  }),
  "signature": "H6ZXtGjTZyUnPeKn...wEA4TklBdh3e454g"
}
```

Concrete Proposal

- Augment the order response:

```
Content-Type: application/json

{
  "status": "valid",
  "expires": "2025-01-01T12:00:00Z",
  "profile": "profile1",
  "identifiers": [{"type": "dns", "value": "example.org"}],
  "authorizations": ["https://example.com/acme/authz/PAniVnsZcis"],
  "finalize": "https://example.com/acme/order/E8rfgo/finalize",
}
```

Concrete Proposal

- Client must only request a profile if one or more are advertised
- Client must not request a profile name that is not advertised
- Server must respond with “invalidProfile” if Client does

- Server should choose a (default) profile for requests that don’t specify one