Proposal: ACME Profiles

draft-aaron-acme-profiles-00 eventually

Aaron Gable, Let’s Encrypt
IETF 120, 2024-07-26
The Problem

- new-order has few knobs:
  - notBefore
  - notAfter
  - identifiers
- finalize CSR is unwieldy
  - Too late
  - Too untrusted
  - Too fine-grained
  - Difficult for clients to manipulate
The Solution

● “Profiles” – CA-curated collections of certificate attributes

● Pros:
  ○ Simple for clients to implement
  ○ Simple for site operators to configure

● Cons:
  ○ No dynamic profile negotiation
Augment the directory:

```
GET /directory HTTP/1.1

{
    "newAccount": "https://api.example.ca/acme/new-account",
    "meta": {
        "profiles": {
            "legacy": "The same profile you know and love",
            "modern": "https://example.ca/profiles#tls-server"
        }
    },
    ...
}
```
Augment the order object:

POST /acme/new-order HTTP/1.1

{
    "protected": base64url(...),
    "payload": base64url(
        "profile": "modern",
        "identifiers": [{"type": "dns", "value": "example.org"}],
    ),
    "signature": "H6ZXtGjTZyUnPeKn...wEA4Tk1Bdh3e454g"
}
Status

- Already implemented by Let’s Encrypt / Boulder
- Profile controls:
  - Validity period
  - Inclusion of Common Name
  - Inclusion of Subject Key ID
  - Inclusion of TLS Client Auth EKU
  - Inclusion of keyEncipherment KU (for RSA certs)
- Next steps:
  - Control lifetime of ACME order / authorization objects
  - Client implementations
  - Standardization