draft-friel-acme-subdomains-03

Friel, Barnes	Cisco
Hollebeek	DigiCert
Richardson	Sandelman Software Works

Sub-domain certificates

- ACME (RFC 8555) allows an ACME server to issue certificates for a given identifier (e.g. a subdomain) without requiring a challenge to be explicitly fulfilled against that identifier
- For example, an ACME server could issue a certificate for **foo1.foo2.bar.example.com** where the ACME client has only fulfilled a challenge for **bar.example.com** or **example.com**
- An ACME server could issue certificates for a number of sub-domain certificates and only require a single challenge to be fulfilled against the parent domain
  - Scale benefits when issuing a large number of end entity certificates
- ACME for subdomains may optionally be used with pre-authorizations but pre-authorizations are not required

Relevant ACME RFC8555 Text

- Section 7.1.3 Order Objects

authorizations (required, array of string): For pending orders, the authorizations that the client needs to complete before the requested certificate can be issued (see Section 7.5), including unexpired authorizations that the client has completed in the past for identifiers specified in the order. **The authorizations required are dictated by server policy; there may not be a 1:1 relationship between the order identifiers and the authorizations required.** For final orders (in the "valid" or "invalid" state), the authorizations that were completed. Each entry is a URL from which an authorization can be fetched with a POST-as-GET request.

Changes in -03 since IETF108

- Incorporates mailer feedback on -02
- Terminology updated
- Security Considerations added
- Open Items

Terminology Clarification

- CA/Browser Forum Baseline Requirements definitions referenced
  - Base Domain Name
  - Domain Name
  - Domain Namespace
- Subdomain is defined as
  - a Domain Name that is in the Domain Namespace of a given Parent Domain

Security Considerations

- ACME for Subdomains has the same two security goals as ACME:
  - Only an entity that controls an identifier can get an authorization for that identifier
  - Once authorized, an account key's authorizations cannot be improperly used by another account
- ACME for Subdomains makes no changes to
  - Account or key management
  - ACME channel establishment, security mechanisms or threat model
  - Validation channel establishment, security mechanisms or threat model
- ACME Server Policy Considerations
  - Document may be applicable to Public CAs, Private CAs, Issuance of IoT certificates, etc.
  - CA/Browser Forum Baseline requirements may not necessarily be applicable
  - Specific server policies are out of scope of this document

Open Items

1. Does the **client** need a mechanism to indicate that they want to authorize a parent domain and not the explicit subdomain identifier? Or a mechanism to indicate that they are happy to authorize against a choice of identifiers?

   E.g. for foo1.foo2.bar.example.com, should the client be able to specify anywhere from 1 to 4 identifiers they are willing to fulfil challenges for?

2. Does the **server** need a mechanism to provide a choice of identifiers to the client and let the client chose which challenge to fulfil?

   E.g. for foo1.foo2.bar.example.com, should the server be able to specify anywhere from 1 to 4 identifiers that the client can pick from to fulfil?

- Both 1 and 2 require JSON object definition changes
- Currently, the document only defines how a client can submit a newOrder / newAuthz for a subdomain, and the server can chose any one parent identifier that it requires a challenge fulfilment on

Next steps

- Open items
- Adoption?