Domain Control Validation with DNS

Shivan Sahib, **Shumon Huque**, Paul Wouters, Erik Nygren

November 7th 2023

DNS Operations Working Group

Internet Engineering Task Force (IETF) 118 Meeting

Prague, Czechia

Current version: 03

- Versioned draft:
  - https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-domain-verification-techniques-03
  - Put out mid October
  - No comments on list yet
- Datatracker link:
  - https://datatracker.ietf.org/doc/draft-ietf-dnsop-domain-verification-techniques/

Summary of Changes since -02

- Added Erik Nygren as co-author.
- Tighten up requirements for token generation (encoding alphabets).
- Expanded treatment of delegated domain control validation.
- New section on Domain Boundaries and Public Suffixes.
- Extend validation record format to support:
  - account specific validation
  - multiple CDNs/application service providers
  - scope of validation

Random token Generation additions; Section 5.1.3

base64url ([RFC4648], Section 5) encoded, **base32** ([RFC4648], Section 6) encoded, or **base16** ([RFC4648], Section 8) encoded.

Base32 encoding or hexadecimal base16 encoding are RECOMMENDED to be specified when the random token would exist in a DNS label such as in a CNAME target. This is because base64 relies mixed case (and DNS is case-insensitive as clarified in [RFC4343]) and because some base64 characters ("/", "+", and "=") may not be permitted by implementations that **limit allowed characters to those allowed in hostnames.** If base32 is used, it SHOULD be specified in way that safely omits the trailing padding ("="). Note that **DNS labels are limited to 63** octets which limits how large such a token may be.

5.3.2 Delegated Domain Control Validation

The intermediary gives the user a CNAME record to add for the domain and provider being validated that points to the intermediary's DNS, where the actual validation TXT record is placed.

**_foo-challenge.example.com. IN CNAME **
"<intermediary-random-token>.dcv.intermediary.example."

The intermediary then adds the actual validation record in a domain they control:

<intermediary-random-token>.dcv.intermediary.example. TXT "<provider-random-token>"

CNAMEs allow automating the renewal process by letting the intermediary place the random token in their DNS instead of needing continuous write access to the user's DNS.

Importantly, the CNAME record target also contains a random token issued by the intermediary to the user (preferably over a secure channel) which proves to the intermediary that example.com is controlled by the user. The intermediary must keep an association of users and domain names to the associated intermediary-random-tokens. Without a linkage validated by the intermediary during provisioning and renewal there is the risk that an attacker could leverage a "dangling CNAME" to perform a "subdomain takeover" attack

4.1 & 6.1 Domain Boundaries and Public Suffixes

Whether or not it is appropriate to allow domain verification on a public suffix will depend on the application. In the general case:

- Providers **SHOULD NOT** allow verification of ownership for domains which are public suffixes in the "**ICANN**" division of the PSL. For example, **"_foo-challenge.co.uk" would not be allowed**.
- Providers **MAY allow** verification of ownership for domains which are public suffixes in the "**PRIVATE**" division, although it would be preferable to apply additional safety checks in this case.
  - (e.g. public suffix owner may want a wildcard certificate for all customer names under the suffix)

Expanded Validation Record Format

- Support different scopes (single domain name, entire domain tree rooted at domain, wildcard names).
- Support multiple intermediaries (e.g. multiple accounts, multiple CDNs or providers that each need to be validated separately).

Scope Indication

For applications that may apply more broadly than to a single host name, the RECOMMENDED approach is to differentiate the application-specific underscore prefix labels to also include the scope (see #scope). In particular:

"**_<PROVIDER_RELEVANT_NAME>-host-challenge.example.com**" applies only to the specific host name of "example.com" and not to anything underneath it.

"**_<PROVIDER_RELEVANT_NAME>-wildcard-challenge.example.com**" applies to all host names at the level immediately underneath "example.com". For example, it would apply to "foo.example.com" but not "example.com" nor "quux.bar.example.com"

"**_<PROVIDER_RELEVANT_NAME>-domain-challenge.example.com**" applies to the entire domain "example.com" as well as its subdomains. For example, it would apply to all of "example.com", "foo.example.com", and "quux.bar.example.com"

Multiple Accounts or Intermediaries

There are use-cases where a user may wish to simultaneously use multiple intermediaries or multiple independent accounts with a provider. For example, a hostname may be using a "multi-CDN" where the hostname simultaneously uses multiple Content Delivery Network (CDN) providers.

To support this, **providers may support prefixing the challenge with a label containing an unique account identifier of the form _<identifier-token>**

_<identifier-token>._foo-challenge.example.com. TXT "3419...3d206c4"

or

**_<identifier-token>._foo-challenge.example.com. CNAME **

<intermediary-random-token>.dcv.intermediary.example.

Account specific validation in Acme

- ACME's current proposal (from July): https://datatracker.ietf.org/doc/draft-ietf-acme-dns-account-challenge/
- Subsequent discussion with us has lead them to re-design the format to be consistent with our recommendations (unmerged PR)
  - account specific string should be an distinct label to the left of the application label
- Will require CAB Forum rule changes though (discussions under way)

```
OLD: _acme-challenge_ujmmovf2vn55tgye.www.example.org

NEW: _ujmmovf2vn55tgye._acme-challenge.www.example.org
```