Domain Control Validation (DCV) using DNS

draft-ietf-dnsop-domain-verification-techniques-07

Shivan Kaul Sahib, **Shumon Huque**, Paul Wouters, Erik Nygren, Tim Wicinski

IETF 122, Bangkok, Thailand

March 17th 2025

Updates in -07

In response to some critiques (including self critiques), we revamped & re-organized the draft to slim it down and make it more comprehensible to its intended readers (application service providers who are typically not DNS protocol experts):

- Relegate some of the DNS esoterica to the appendix.
- Remove the Appendix of Survey of Existing methods.
- Start upfront with the recommended ways to do Domain Control Validation.
  - TXT based DCV record with a random challenge token in the record data.
  - Record name has underscored application specific label.

Updates in -07

Only mention CNAME for Delegated DCV

- Where a CNAME points to a TXT DCV record in a zone under the control of the delegated party

Support for Multiple Intermediaries

- Account and Provider specific challenges, with an additional account/provider specific label prepended to the record name.

Remove “Scope Indication” mechanism (for now).

Planned

More readability improvements.

More recent comments

Paul Hoffman would like additional changes that we are discussing on list and in-person:

- Remove many of the MUST/SHOULDs
- Remove “time bound” validation (more specifically the draft actually suggests not reusing a previous validation challenge for subsequent revalidations)
- Too much focus on certificate issuance use case.
    - My response: we mention certs a few times, but see the previous survey for an extensive list of other apps that use the basic DCV approach described in the draft.
- Accommodate other approaches besides nonce based domain validation
    - My response: many of those use persistent identifiers to associate domain names with application services (e.g. decentralized social media identifiers) - arguably this is a different class of application than DCV, and we’ve tried to avoid treatment of that in this draft so far.
    - Note that there is another draft in the pipeline (Swapneel Sheth) that is proposing to cover this use case in detail.

Comments/Questions?