Domain Control Validation (DCV) using DNS

draft-ietf-dnsop-domain-verification-techniques-09

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

IETF 123, Madrid
July 21, 2025

Updates in -09

Added a section on "Purpose of Domain Control Validation"

- Introduces distinction of “one-off” vs “persistent” validations

Removed section on "Supporting Multiple Intermediates"

- Still too new, complicated

Added Security Considerations on Unintentional Persistence

Took previously removed Appendix Survey of Existing Methods as file in git repo

Open Issues - how tokens are defined

Open question on how tokens are defined.

- Current doc talks about “random tokens”
- Proposal to switch to "unique tokens" (with random being one option)

https://mailarchive.ietf.org/arch/msg/dnsop/S11G3RU0c7dXwcCjcLib4NI3uF0/

https://github.com/ietf-wg-dnsop/draft-ietf-dnsop-domain-verification-techniques/issues/161

Open Issue - "DNSSEC Validation Language

#1. DNSSEC validation as a “SHOULD” (current) or upgrade to a “MUST”?

#2. Should we clarify anything about how the ASP validator should be handling response four states from RFC4033?

```
DNSSEC validation (SHOULD/MUST?) be performed by Application Service Providers that verify
Validation Records they have requested to be deployed. A "Bogus" or "Indeterminate" result
(as defined in [[RFC4033]]) MUST NOT be accepted. A "Secure" or "Insecure" result SHOULD be
accepted.
```

https://github.com/ietf-wg-dnsop/draft-ietf-dnsop-domain-verification-techniques/issues/182

Open Pull Requests

Marking these PRs as "won't fix" (as alternate approaches taken

- PR 160 "Add a section on the purpose of DCV"
- PR 169 "Removed everything about intermediaries"
- PR 170 "Remove hints about continuous use of the record"
- Due to merged the portions agreed upon in PR 172 included in -09

Any Other Issues

Comments?

Ready for WGLC?

Fin