Domain Verification Techniques

DNSOP WG, IETF 114

Shivan Kaul Sahib
Shumon Huque
Paul Wouters
What is domain verification?

Many providers on the internet need users to prove that they control a particular domain before granting them some sort of privilege associated with that domain.

For e.g. ACME has a DNS-based challenge for a user to prove that they control a particular domain (and hence should be issued a cert for it)
Survey

1. TXT
2. CNAME
TXT-based

- “Please add this DNS TXT record with random value at the domain being verified to prove that you own this domain”
- Typically expires in a few days
- In practice, wide variation
Pattern: RDATA

```
bbc.com. 3599 IN TXT "atlassian-domain-verification=SQsgJ5h/FqwMTXuSG/G4Nd1Gx6uX2keRE0sZSa22D5XT46EsEuyaic8Aej4cR4Tr"

bbc.com. 3599 IN TXT "google-site-verification=yTRDtkD0tgHXSaJL0EtVrYGv1moNR-QkK8BAvjTv2Q8"
```
Pattern: name

ACME DNS TXT example

_acme-challenge.example.com. IN TXT "cE3A8qQpEzAIYq-T9DWNdLJ1_YRXamdxcjGTbzrOH5L"

GitHub DNS TXT example

_github-challenge-octocat.octocat.com IN TXT "9a6c10f4c4"
No pattern

```
bbc.com. 3599 IN TXT "1884df5221d841f294fd942e3e95a01f"
```
CNAME-based

- Fallback option

- Might be used if the domain name already has a CNAME
  
  - Since CNAMEs can’t coexist with other records (e.g. TXT) at the same domain name

- Point to a service provider property
Google Workspace CNAME example

3IBW7URVCRWY.example.com. IN CNAME
gv-LtgM1Qg1w0JCE7mBVgLvM1DwuLGnuzwPCbsmXh3zjs4h6EWb8gy6.domainverify.googlehosted.com."
Recommendations

1. Targeted to service
2. Time-bound
Targeted Domain Verification

1. Similar to what ACME and GitHub do

2. Allows a service provider to get only the records they need

3. Putting all TXT records at the same name causes bloating
   a. Causing retries over TCP
Time-bound checking

1. When can the records be removed?

2. Should they exist in perpetuity?
Feedback and Changes

1. Removed mention of specific companies
   a. Move to Appendix (#25)

2. Removed use of normative language
   a. Purely informational

3. Summarize recommendations in the intro

4. Adopted by WG
TODO

1. Move examples to Appendix (#25)
2. Move to WG GitHub
Thanks!