Discovery of Designated Resolvers

draft-ietf-add-ddr

Tommy Pauly, Tommy Jensen,
Eric Kinnear, Patrick McManus, Chris Wood
ADD
IETF 112, November 2021, Virtual

Status

-03 draft published October 1

Updates to align with SVCB/DNS draft

Explain that clients can use the documented methods to validate resolvers, but that clients MAY use other methods as extensions

Changed "Authenticated Mode" to "Verified Mode"

1 open issue (#41) with PR (#43)

What is verified?
PR #43

If you discover based on a known IP address...

    ...that IP address must be covered by the certificate

If you discover based on a known hostname...

    ...that hostname must be covered by the certificate

Server name handling
PR #43

Clarify that resolver.arpa MUST NOT be used for SNI or DoH requests

Allow clients to either use IP addresses or SVCB TargetNames in DoH requests

  Why this, and not require only the IP address?

Example

Client issues query to 8.8.8.8, receives the following answer:

```
_dns.resolver.arpa 7200 IN SVCB 1 dns.google. ( alpn=h2 dohpath=/dns-query{?dns} )
```

Client resolves dns.google to 8.8.8.8, 8.8.4.4, 2001:4860::8844, 2001:4860::8888

If the client connects to dns.google / 2001:4860::8888, which should it send?

```
:method = GET
:scheme = https
:authority = dns.google
:path = /dns-query?dns=AAABAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAQAB
accept = application/dns-message

:method = GET
:scheme = https
:authority = 8.8.8.8
:path = /dns-query?dns=AAABAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAQAB
accept = application/dns-message
```

Server name handling
PR #43

If we allow both IP addresses and TargetNames, how are aliases handled?

Current PR uses the ServiceMode TargetName (which is the name that is used for IP address resolution)

Alternative is to use the initial TargetName, even if it is AliasMode

Next steps

Resolve #43

WGLC