DNS Server Selection: DNS server Information with Assertion Token

draft-reddy-add-server-policy-selection-04
IETF 108
July 2020

T. Reddy (McAfee)
D. Wing (Citrix)
M. Richardson (Sandelman Software Works)
M. Boucadair (Orange)
Agenda

• Updates from 00 to 04
• Next Steps
Overview

1. DNS server identity and resolver information attestation.

2. Determine resolver information (e.g., DNS filtering) to feed server selection

3. Easily find DNS server privacy statement URL and audit URL

4. Change notification of privacy/audit URL and resolver information

This draft does not discuss policy claims.
Identity and resolver info attestation

• It is particularly useful when the DoH/DoT server is insecurely discovered.
  ▪ Prevents the client from connecting to the attacker’s server.
  ▪ Cryptographically assert the DoT/DoH server hosted by a specific organization

• OV/EV certificates registered organizations to cryptographically attest
  ▪ the DNS server identity (ADN or URI)
  ▪ Resolver information (e.g., filtering)
  ▪ privacy statement URL and audit URL
Privacy assertion token (PAT)

- CA that issued the OV/EV certificate does not attest the DNS server identity and resolver information.
- PAT object is created by the organization hosting the DoT/DoH server.
  - Optionally by a third party (privacy and security auditor) of the DoT/DoH server.
- PAT uses JSON Web Token (JWT) and JSON Web Signature (JWS)
- Client retrieves PAT per draft-pp-add-resinfo using RESINFO RRTYPE
Filtering capabilities

• DNS-based Filtering Capabilities
  ▪ Malware Blocking
  ▪ Phishing Blocking
  ▪ Policy Blocking
  ▪ Censored Blocking

• Indicate whether the server supports QNAME minimization.

• Indicate whether the server requires client authentication.

Extended error codes in [ietf-dnsop-extended-error](https://datatracker.ietf.org/doc/html/rfc6890)
PAT object example

{
    "server": {
        "adn": ["example.com"]
    },
    "iat": 1443208345,
    "exp": 1443640345,
    "policyinfo": {
        "filtering": {
            "malwareblocking": true,
            "policyblocking": false
        },
        "privacyurl": "https://example.com/privacy/",
        "auditurl": "https://audit-example.com/privacyaudit"
    }
}
• Consider for WG adoption
• Comments and suggestions are welcome