DNS Server Selection:

DNS server Information with Assertion Token

draft-reddy-add-server-policy-selection-00

IETF 107

March 2020

T. Reddy (McAfee)

D.Wing (Citrix)

M. Richardson (Sandelman Software Works)

M.Boucadair (Orange)

v1

Agenda

- Context & Motivation
- Solution Overview
- Privacy Assertion Token (PAT)
- PAT Object
- Next Steps

Context & Motivation

- DNS clients may maintain a list of DNS servers
  - Pre-configured
  - Discovered
- DNS clients may be provided with a set of preferences
  - Pre-configured
  - Instructed by a user
- DNS clients need to implement a selection procedure to select the server

Our Approach

1. Determine relevant resolver information (e.g., DNS filtering) to feed the server selection
2. Policy **attestation**
3. **Change notification** of privacy statement and DNS filtering
4. **Easily Find** DNS server privacy statement URL

This draft does not discuss policy content

Filtering Capabilities

- Current filtering capabilities
  - DNS Filtering
    - Malware blocking
    - Policy blocking (blacklist or objectionable content)
  - QNAME minimization (RFC7816)

Policy Attestation

- Signature by the organization operating the DNS server
  - Optionally signed by another domain ("auditor")

- OV/EV certificates registered organizations to cryptographically attest the privacy statement URL and filtering policy
  - Or DNS client is configured to trust the signer of the PAT object

Privacy Assertion Token (PAT)

- PAT uses JSON Web Token (JWT) and JSON Web Signature (JWS)
- Clients retrieve PAT as per draft-ietf-dnsop-resolver-information
- A PAT object is created by the organization hosting the DoT/DoH server, and optionally by a third party (privacy and security auditor) of the DoT/DoH server

PAT Object Example

```
{
    "server":{
        "adn":["example.com"]
    },
    "iat":1443208345,
    "exp":1443640345,
    "policyinfo": {
      "filtering": {
           "malwareblocking": true,
           "policyblocking": false,
       },
       "privacyurl": "https://example.com/privacy/",
       "auditurl": "https://example.com/privacyaudit"
    }
}
```

Change Notification

- Notify client of changes to privacy statement and filtering
  - DNS push notifications: draft-ietf-dnssd-push

Privacy Statement URL

- **Easily Finds** human readable privacy statement URL
  - User or automata easily finds privacy policy

- Users may review the privacy statement of the DNS server and **assess its filtering capability**

Next Steps

- Additional capabilities for server selection?
- Comments and suggestions