Delegated Credentials to Host Encrypted DNS Forwarders on CPEs

draft-reddy-add-delegated-credentials-02
IETF#118, Prague, November 2023

Tiru Reddy (Nokia)
M. Boucadair (Orange)
Dan Wing (Citrix)
Shashank Jain (McAfee)
Changes Since IETF#117

• Addressed comments from the WG
• Added “delegation” SvcParamKey
“delegation” SVCB SvcParamKey

• Mandatory:
  – If the server is only accessible using delegation credentials

• Not Mandatory:
  – DNS server that can be optionally authenticated using delegation credentials
Example of “delegation”

SvcParamKey

_dns.example.net. 7200 IN SVCB 1 doh.example.net (alpn=h2 dohpath=/dns-query{?dns} delegation mandatory=delegation)
Scope of the I-D: Reminder

• Managed Modern CPEs
  ✓ Upgraded without end-user intervention
  ✓ Already support encrypted DNS (e.g., PowerDNS DNSdist)

• Deployment of DNS forwarders for Encrypted DNS

https://blog.open-xchange.com/dnsdist-as-a-router-ready-solution
Next Steps

• All raised comments were addressed so far
• The content is more stable
• Request the WG to consider adoption
BACKUP
Encrypted DNS client

(CPE) Encrypted DNS Forwarder

Managed CPE Service

Mutual Authentication

Credential (Key, Time, algorithm)

Delegated Credential

ClientHello + delegated_credential

ServerHello + Certificate + delegated_credential

Validate the delegated credential