Delegated Credentials to Host Encrypted DNS Forwarders on CPEs

draft-reddy-add-delegated-credentials-01
IETF 117, July 2023

Tiru Reddy (Nokia)
M. Boucadair (Orange)
Dan Wing (Citrix)
Shashank Jain (McAfee)
The Problem

• **Goal:** Deploy encrypted DNS on local managed CPEs
  – Improve privacy: local network, query aggregation
  – Improve security: malware filtering, MUD [RFC8520]
  – Improve performance: Local DNS caching

• **However,**
  – Encrypted DNS requires CA-signed certificates
  – Difficult to obtain CA-signed certificates for CPEs
  – Managed CPEs ease user burden, but creates scale burden
DDR and DNR

• DDR’s scope is restricted to public IP addresses
  – Prefix re-numbering induces issues
    • DNS service delayed until new certificate acquired
  – ACME IP Identifier Validation Extension (RFC 8738) not supported

• DNR requires proving possession of an FQDN
  – Unique FQDNs are viable (cpe-1234.example.net)
  – ACME approach: CPE hosts Internet-facing HTTP or DNS server
    • Struggle with CGN (mobile networks)
  – An Alternative approach: CPE obtains certificate signature from Internet-facing server
Issuing CPE certificates from CA

• Could trigger DoS mitigation (throttling) by CA
• Ongoing traffic to renew short-lived certificates (STAR, RFC8739)
• CPE are often unavailable (unplugged)
Solution: Avoid High Traffic to CAs

- Send traffic to Managed CPE service (rather than CA)
- Use *subcerts* [RFC9345] or *name constraints* [RFC8280]

<table>
<thead>
<tr>
<th><strong>subcerts</strong></th>
<th><strong>name constraints</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Con: TLS client &amp; server need subcert support</td>
<td>Standardized 2008</td>
</tr>
<tr>
<td>Pro: Some client support (Firefox)</td>
<td>Con: Little/none CA support</td>
</tr>
</tbody>
</table>
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
• Comments and suggestions are welcome
Modern Managed CPE

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

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