IKEv2 Configuration for Encrypted DNS

draft-btw-add-ipsecme-ike-02

Mohamed Boucadair (Orange)
Tirumaleswar Reddy (McAfee, Inc.)
Dan Wing (Citrix Systems, Inc.)
Valery Smyslov (ELVIS-PLUS)

March 2021, IETF#110
Status

• Presented at IETF#109
  – adoption of the draft was discussed

• Comments raised
  – wait for ADD WG to progress before adoption
    • ADD WG has progressed far enough to reconsider adoption of this draft
    • ADD WG adopted insecure discovery mechanisms: DHCP/RA (draft-ietf-add-dnr) and DNS (draft-ietf-add-ddr)
  • No conflict with the work in ADD WG
  • Commit to cross-review the document in ADD WG
Changes from -01

• New Attribute `ENCDNS_URI_TEMPLATE` is added for conveying DOH URI Templates

• Clarification on authentication of a private encrypted DNS server
  – the encrypted DNS server hosted by VPN provider can get a domain-validate certificate from a public CA but it is only accessible to clients connected to the VPN
ENCDNS_URI_TEMPLATE
Attribute Format

<table>
<thead>
<tr>
<th>R</th>
<th>ENCDNS_URI_TEMPLATE</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Each instance of the uri-template-data is formatted as follows:

<table>
<thead>
<tr>
<th>uri-template-len</th>
<th>URI Template</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DoH Specifics

- DoH servers may support more than one URI Template
- If DoH is requested, the initiator includes an empty ENCDNS_URI_TEMPLATE attribute (in addition to ENCDNS_IP*_DOH attributes) in the CFG_REQUEST
- If the responder includes ENCDNS_IP4_DOH or ENCDNS_IP6_DOH in the response, it MUST also include ENCDNS_URI_TEMPLATE carrying one or more URI Templates
- Avoids the need to rely on insecure discovery mechanisms (DHCP/RA), and on Do53 (which requires additional RTT and is not always secure, since using DNSSEC is not mandatory)
  - draft-schwartz-svcb-dns-01, Section 9.1
Next Steps

• Comments?
• Questions?
• Consider WG adoption

Thank you