Why DNS Cookies

- DNS Native Protection Mechanism against Amplification Attacks
- To be helpful it needs to be enabled everywhere
- Multi-vendor cooperation desirable
DNS Cookies Operation

- Valid Server Cookie? Large answers
- Valid Server Cookie? RRL Disabled!
DNS Cookies in Anycast
Hackthon @IETF104 Results

- draft-sury-toorop-dns-cookies-algorithms-00
- Witold Krecicki, Pieter Lexis, Willem Toorop
- Interoperable Server Cookies for:
  - BIND
  - 9
  - POWERDNS
  - NSD
  - KNOT DNS
  - unbound
Donald & Mark joined

- Merge with: draft-eastlake-dnsop-server-cookies-00
- Use only SipHash2.4 with this Version
- IANA sub-registry “DNS Server Cookie versions”:

<table>
<thead>
<tr>
<th>Version</th>
<th>Algorithm</th>
<th>Server Cookie Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>SipHash24</td>
<td>16</td>
</tr>
<tr>
<td>2-240</td>
<td>Unassigned</td>
<td>-</td>
</tr>
<tr>
<td>240-254</td>
<td>Private use</td>
<td>-</td>
</tr>
<tr>
<td>255</td>
<td>Reserved</td>
<td>-</td>
</tr>
</tbody>
</table>
Still TODO’s

- Operator advise on Server Secret roll-over
- Implementation advise for smooth roll-over
- Appendix with Test vectors

https://github.com/NLnetLabs/draft-sury-toorop-dns-cookies-algorithms

Questions?