Not at the Zone Cut!
What is this about?

- Where to put the new extensible delegation info?
- **Fundamental design choice** -- with consequences
  - Affected software
  - Ease to deploy
  - May impact requirements
What design choice?

- At the parent side of the zone cut
- Elsewhere in the zone
- For the sake of example we reference
- Both originate from IETF 118 Hackathon
- Both based on SVCB (irrelevant for this talk)

draft-wesplaap-deleg-00
draft-homburg-deleg-incremental-deleg-00

example.com. 3600 IN NS ...
example.com. 3600 IN DS ...
example.com. 3600 IN DELEG ...
example.com. 3600 IN NS ...
example.com. 3600 IN DS ...
example._deleg.com. 3600 IN SVCB ...
The zone cut makes child authoritative

- example.com. 3600 IN NS ...
- Everything at or below example.com. is not authoritative in the com. zone (except DS & NSEC)
- It will not be signed by unmodified signers
- It will not be returned by unmodified name servers
  - Instead the delegation is returned
- If it is signed by com. DNSKEY, then unmodified validating resolvers will consider it BOGUS
... thus ...

- example.com. 3600 IN DELEG ...

- ... new authoritative in the parent RRs require:
  - Modified DNSSEC signers
  - Modified name servers
    - For returning it in referral response
    - For returning it when queried for it
  - Modified DNSSEC validators

- Apart from new delegation mechanism (modified resolver)
... on the other hand

- example._deleg.com. 3600 IN SVCB ...
- Semantics with respect to what is authoritative remain
- Is authoritative in the com. zone
- It will be signed by unmodified signers
- It will be returned by unmodified name servers
- unmodified DNSSEC validators will validate it
- implementation in the resolver only, already makes it work
... on the other hand

- Semantics with respect to what is authoritative remain
- The conventional methods to alias remain functional
  - Outsource delegation to one operator:
  - Outsource the operation of delegations to an operator:
Downgrade protection

- New authoritative in the parent RRs will **not** be returned by **unmodified name servers**
- They cannot be queried for by the resolver
- [draft-wesplaap-deleg-00](https://example.com) uses a DNSKEY flag to signal support by **all** authoritative servers serving the zone
  - No separation of concern

- Authoritatively provisioned extensible delegations supports incremental deployment on authoritative servers
But, but, but,

- Every non extensible delegation zone will get two queries!?
  - NSEC(3) RRs shows that _deleg.com. does not exist
  - Cost: 1 query per zone
  - Or else require DNSKEY flag

- What about unsigned zones?
  - Needs explicit _deleg.com. query
  - Cost: 1 more query per zone
  - Or else require authoritative support for unsigned zones
<table>
<thead>
<tr>
<th>At the zone cut</th>
<th>Not at the zone cut</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Name servers, signers, resolvers all need to change</td>
<td>● Can work with resolver implementation only</td>
</tr>
<tr>
<td>● New aliasing mechanisms</td>
<td>● CNAME and DNAME</td>
</tr>
<tr>
<td>● All name servers serving a zone need to be upgraded</td>
<td>● None, mixed or full deployment on name servers all work fine</td>
</tr>
<tr>
<td>● 0 extra queries</td>
<td>● Can work with 0 extra queries</td>
</tr>
</tbody>
</table>
Not a new notion!  ●  DELEG Panel Discussion at https://419.consulting/encrypted-dns/f/deleg-the-hairy-dns-camel

We can generalize. Back to some mistakes that I think DNSSEC has made. And one is to put the DS record at the delegation point.
Questions

Comments