Quick Review

Basic delegation:

example.com. 86400 IN DELEG 1 ns1.example.com. (ipv4hint=192.0.2.1 ipv6hint=2001:DB8::1)

Alias mode:

example.com. 86400 IN DELEG 0 config2.example.net.
config2.example.net 3600 IN SVCB . (ipv4hint=192.0.2.54,192.0.2.56
ipv6hint=2001:db8:2423::3,2001:db8:2423::4)
Motivations

● **Secures the delegation**
  ○ Currently chain-of-trust break is only discovered after talking to rogue nameserver
  ○ DELEG positively secures the next resolution stage

● **Supports recognition of operator role**
  ○ Manages DNSSEC without needing ongoing registrant interaction
  ○ Can more easily change authoritative name servers via configuration sets

● **Transport Usage**
  ○ Effectively a resolver can only trust that a delegation goes to udp/53
  ○ DoT / DoQ / DoH all have no in-bound way to signal use

● **Extensibility**
  ○ Hopefully makes parent-side changes just once
  ○ Many ideas to address from [Prague Hackathon](https://praguehackathon.org)
  ○ Makes a clean off-ramp to a new base protocol ("DNSv2") easier
Positive Initial Results

● Encouraged by interest from multiple sectors of the industry
  ○ Resolver and auth server implementers
  ○ Registries
  ○ Operators
  ○ Paul Mockapetris :) (To be clear: he didn't specifically endorse DELEG but at least the idea of updating how delegations are done.)

● Roy Arends and Shumon Huque tested the basic approach
  ○ Authoritative server configured to return dual-DELEG/NS
  ○ Also tested DNSSEC assertion of DELEG use, to avoid downgrade
  ○ Existing, non-DELEG-aware resolvers handled presence of DELEG gracefully
Open Issues

- How is DELEG used without DNSSEC?
  - Any security-related parameters can't be trusted; eg, certificate references

- Should there be a signal in query indicating DELEG support?
  - Maybe one for getting *only* DELEG if present, to keep response size down?

- DELEG proposes indicating properties of the delegation
  - Can it also signal properties of the zone, like "this is a public suffix"?
  - Maybe use a special server target of "." to indicate zone parameters?
  - How does that work in multi-provider?

- Can any service parameters go on an alias-mode DELEG?
  - Glue? Error reporting channel?

- What should happen in a dual-DELEG/NS delegation?
  - Can a DELEG-aware resolver fall back to NS?

- Anything else? Send it to the list!