How DELEG and `_deleg` meet the requirements

Philip Homburg philip@nlnetlabs.nl
Petr Špaček pspacek@isc.org

Introduction

- Legacy delegation:

```
customer5          IN  NS     ns.customer5
ns.customer5       IN  A      198.51.100.5
                   IN  AAAA   2001:db8:5::1
```

- Use DELEG as short for draft-wesplaap-deleg-01
  This draft adds:

```
customer5 IN DELEG   1 ns.customer5 alpn=h2,h3 (
                                     ipv4hint=198.51.100.5
                                     ipv6hint=2001:db8:5::1
                                     dohpath=/dns-query{?dns}
                                     )
```

- Use `_deleg` as short for draft-homburg-deleg-incremental-deleg-00
  This draft adds:

```
customer5._deleg IN SVCB   1 ns.customer5 alpn=h2,h3 (
                                     ipv4hint=198.51.100.5
                                     ipv6hint=2001:db8:5::1
                                     dohpath=/dns-query{?dns}
                                     )
```

H1 – H3

- **H1. DELEG must not disrupt the existing registration model of domains.**
  The existing concept of delegations from a parent zone to a child zone is left unchanged. (Both drafts)
- **H2. DELEG must be backwards compatible with the existing ecosystem.**
  The new delegations do not interfere with legacy software.
  The behavior of resolvers includes a fallback to NS records if no DELEG or `_deleg` is present.
- **H3. DELEG must not negatively impact most DNS software.**
  Old software is not confused by new delegations. (Both drafts)

H4 – H6

- **H4. DELEG must be able to secure delegations with DNSSEC.**
  Delegations are automatically secured with DNSSEC (if the parent zone is signed). A separate draft is required to create a replacement for DS records. (Both drafts)
- **H5. DELEG must support updates to delegation information with the same relative ease as currently exists with NS records.**
  Delegations are affected by TTL like any other DNS record. (Both drafts)
- **H6. DELEG must be incrementally deployable and not require any sort of flag day of universal change.**
  For `_deleg`, new zones can be added without upgrading authoritatives. New zones still work with old resolvers and validators. Basically any combination of old and new should work, though with reduced efficiency for some combinations. For DELEG, new zones can be served only by upgraded authoritatives, Putting DNSSEC functionality in DELEG (such as a replacement for DS) will make new validators unable to work behind old recursive resolvers.

H7, S1 – S2

- **H7. DELEG must allow multiple independent operators to simultaneously serve a zone.**
  Both DELEG and `_deleg` allow for multiple DELEG/SVCB records. This allows multiple operators to serve the zone.
  For `_deleg`, because it used SVCB records directly, it requires defining how multiple AliasMode records can exist for a single name.
- **S1. DELEG should facilitate the use of new DNS transport mechanisms**
  New transports are already defined for the DNS mode of SVCB (see RFC 9461). This is enough for `_deleg`.
  We can decide that RFC 9461 applies to DELEG as well.
- **S2. DELEG should make clear all of the necessary details for contacting a service**
  Currently there is no replacement for DS.

S3 – S5

- **S3. DELEG should minimize transaction cost in its usage.**
  DELEG does not require extra queries.
  For `_deleg`, assuming Qname-minimisation, there are no extra queries needed if the authoritative name server has incremental deleg support. The exception is when the parent zone is not signed and has no incremental deleg records. In that case, one extra query is needed when the parent zone is first contacted (and every TTL).
  Additional queries may be needed to deal with aliasing. (Both drafts)
- **S4. DELEG should simplify management of a zone's DNS service.**
  Zone management can be simplified using the alias mode of DELEG/SVCB. This allows the zone operator to change the details of the delegation without involving the parent zone.
- **S5. DELEG should allow for backward compatibility to the conventional NS-based delegation mechanism.**
  NS records and glue can be derived from the DELEG/SVCB record assuming no aliasing is used.

S6 – S7

- **S6. DELEG should be extensible and allow for the easy incremental addition of new delegation features after initial deployment.**
  DELEG/SVCB records are extensible by design.
- **S7. DELEG should be able to convey a security model for delegations stronger than currently exists with DNSSEC.**
  Delegations from these drafts are protected by DNSSEC, unlike NS records at the parent zone.

Non-Requirements

- **Whether NS records must continue to be the primary means by which resolutions happen.**
  NS records are superseded by DELEG/SVCB records if they are present.
- **Whether information for a new delegation mechanism is stored in at the zone name or elsewhere in the domain name hierarchy.**
  DELEG records are stored at the zone name.
  With `_deleg`, delegations are not stored at the zone name. The way lookups at the zone name are handled is unchanged. In the future, when NS and DS records are deprecated, lookups at the zone name are only handled by the child zone.
- **If a new delegation protocol is based on a DNS resource record, that record must not appear in both the parent and child with the same name and type.**
  DELEG introduces a new RR type at the parent side of the zone cut.
  `_deleg` does not introduce new record types. Delegation information is provided in the parent under an Underscored and Globally Scoped DNS Node Name registry label (`_deleg`)