Incremental Delegation

Tim, Philip, Willem, Jesse

DELEG

18 March 2025

Where Things Stand

After feedback of previous versions, changed from SVCB to utilizing the new DELEG RR Type.

The -03 version of the draft refers to it as IDELEG for clarity in discussions.

Included a detailed section on the delegation point and motivation on using a different delegation point.

Provided comparison with I-D.wesplaap-deleg and requirements.

But DNS Can Not Change The Delegation Point!

DELEG is a Fundamental change in how zones are managed.

With software and processes changing, it is a good time to rethink things.

The Zone cut has always been problematic

It has just been in recent years where many of the edge cases have been worked through

But Changing The Delegation...

Placing the delegation to the side *ensures* there is no disruption of the existing legacy delegation points. (hard requirement).

The DNS community still has heavy discussions over this.

See draft-ietf-dnsop-ns-revalidation and the discussion around draft-fujiwara-dnsop-ranking-data.

_deleg Globally Scoped DNS Node Name

Currently, using these _underscore labels is a best practice for applications and services.

It still allows a safe transition from legacy delegations

Does the DNS community doesn't see this?

Is using an out of band label such as _deleg it make it more or less obvious looking at DNS from the outside ?

Basic *(real world)* Example

```
;; AUTHORITY SECTION:
customer1.ideleg.net.         3600 IN   NS   supporting.ideleg.net.
customer1._deleg.ideleg.net.  3600 IN   IDELEG   10 (
                                        supporting.ideleg.net.
                                        ipv4hint=188.245.247.219
                                        ipv6hint=2a01:4f8:c2c:99d7::1 )
customer1._deleg.ideleg.net.  3600 IN   RRSIG    IDELEG 13 4 3600 (
        20250403135716 20250306135716 60397 ideleg.net. 4UuzgvStSu... )
customer1.ideleg.net.         3600 IN   NSEC customer2.ideleg.net. NS (
                                                          RRSIG NSEC )
customer1.ideleg.net.         3600 IN   RRSIG    NSEC 13 3 3600 (
        20250403135716 ( 20250306135716 60397 ideleg.net. TeMDps2J... )

;; ADDITIONAL SECTION:
supporting.ideleg.net.        3600 IN   A    188.245.247.219
supporting.ideleg.net.        3600 IN   RRSIG    A 13 3 3600 (
        20250403135716 20250306135716 60397 ideleg.net. RNWvNn/HsO... )
supporting.ideleg.net.        3600 IN   AAAA 2a01:4f8:c2c:99d7::1
supporting.ideleg.net.        3600 IN   RRSIG    AAAA 13 3 3600 (
        20250403135716 20250306135716 60397 ideleg.net. QxDs43bLqX... )
```

Test against the IDELEG testbed

Instructions are at https://ideleg.net/

We're trying to cover every edge case for IDELEG that have been raised in discussions,

Commands like this work!

$ drill/drill -Dord @ www.customer1.ideleg.net.

Working IDELEG test bed

Incrementally Deployable Ex

https://ideleg.net

dns ietf icann ripe nluug oarc os3 labs sa fam wh

- IDELEG testbed
- Software support
  - Idns
  - NSD
  - Unbound
- Internet draft
  - Latest
  - Editors copy
  - Incr. DNSSEC

Incrementally Deployable Extensible Delegation testbed

This website hosts information on the domains we have deployed for evaluating and testing the draft-homburg-deleg-incremental-deleg protocol proposal, as well as draft-wesplaap-deleg.

Zones and name servers

The ideleg.net zone has been provisioned with several incremental delegations (using 65280 as the value for the IDELEG RR type), and is served by two incremental deleg supporting authoritative name servers (ideleg.net and ideleg.nlnetlabs.nl) and one legacy, non incremental deleg supporting, authoritative name server (legacy.ideleg.net) as hidden secondary:

name	IPv4	IPv6	location
ideleg.net	128.199.252.158	2400:6180:0:d2:0:1:ac7b:9000	Singapore
ideleg.nlnetlabs.nl	152.42.143.10	2a03:b0c0:2:f0::5b3e:f001	Amsterdam
legacy.ideleg.net	134.122.39.99	2604:a880:cad:d0::a417:1001	Toronto

https://ideleg.net/nsd.html

- Including resolver to test **your** incremental delegations right now!

Testbed includes resources for wesplaap-deleg

Provisioned machines and software for wesplaap deleg in the testbed.

Testbed has a resolver which can be used to test incremental delegations on the internet.

People can add it to their own zones.

wesplaap-deleg will not work - needs special authoritative software.

How do the two proposals line up

Differences between IDELEG and DELEG documents on the next slide.

Please let us know if are incorrect!

[I-D.wesplaap-deleg]	[I-D.homburg-deleg-incremental-deleg]
Requires implementation in both authoritative name server as well as in the resolver, DNSSEC signers and validators	Only implementation required for functionalities following the delegations (like in resolvers). No support from the authoritative name server, DNSSEC signers or validators are needed. But optimized with updated authoritative software.
DELEG resolvers need to contact DELEG authoritatives directly	IDELEG resolvers can query for the incremental delegation data, therefore direct contact with IDELEG supporting authoritatives is not necessary. All legacy infrastructure (including forwarders etc.) is supported.
DNSKEY flag needed to signal DELEG support with all authoritative name servers that serve the parent (delegating) domain. Special requirements for the child domain.	No DNSKEY flag needed. Separation of concerns.
Authoritative name servers need to be updated all at once	Authoritative name servers may be updated gradually for optimization
New semantics about what is authoritative (BOGUS with current DNSSEC validators)	Works with current DNS and DNSSEC semantics. Easier to implement.

Problem Areas

Registry/Registrar are totally out scope.

But in any proposal this could be an issue. ††

There still exists possibilities of old delegation information being left behind.

Similar to A/AAAA deployed in parent zones

Questions for the WG

With the rise of very large consumer focused Authoritative DNS Services, will the deployment time be quicker or slower?

Will the Geoff Huston AI in 30 years be presenting papers on the demise of DELEG?

One author (tim) feels in 30 years large enterprises will still be running Active Directory DNS platforms, and still not signing zones (until a plugin for excel).

Next Steps?

Let the people speak