# DNS DELEG

John Levine | ICANN 85 Mumbai | 

# What’s the problem?

- DNS delegation is complicated and fragile
- Path authentication would be nice for
  ADoT / ADoQ
- Clean up part of the camel

# Delegation today

```
examp1e.com. DS 34909 8 2 1aebbf52...0ee5e2a9743c9
```

```
examp1e.com. NS ns1.examp1e.com.
ns1.examp1e.com. A 12.34.56.78
```

Parent only signs DS

Child signs everything else

```
examp1e.com. SOA ns1.examp1e.com dns.examp1e.com. 2026030102 ...
  DNSKEY 256 3 8 AwEAA...I= ;{id = 18111 (zsk), size = 1024b}
  DNSKEY 257 3 8 AwEAA...8= ;{id = 34909 (ksk), size = 2048b}
  NS ns1.examp1e.com.
ns1.examp1e.com. A 12.34.56.78
```

# Delegation today

```
examp1e.com. DS 34909 8 2 1ae1dfe818bbf52...0ee5e2a9743c9
```

```
examp1e.com. NS ns1.examp1e.com.
ns1.examp1e.com. A 12.34.56.78
```

- Parent NS and glue are only hints
- Child zone can be served from anywhere so long as DS matches DNSKEY

```
examp1e.com. DNSKEY 257 3 8 AwEAA...8= ;{id = 34909 (ksk), size = 2048b}
```

# Delegation today

```
examp1e.com. DS 34909 8 2 1ae1dfe818bbf52...0ee5e2a9743c9
```

```
examp1e.com. NS ns1.examp1e.com.
ns1.examp1e.com. A 12.34.56.78
```

```
examp1e.com. SOA ns1.examp1e.com dns.examp1e.com. ...
  DNSKEY 257 3 8 AwEAA...8= ;{id = 34909 (ksk)}
  NS ns1.examp1e.com.
  NS ns2.examp1e.com.
ns1.examp1e.com. A 22.33.44.55
ns2.examp1e.com. A 12.34.56.78
```

- Child NS and A/AAAA are definitive
- Need not agree with parent
- Which usually works

  except when it doesn't

# Surely we can do better

# DELEG

```
examp1e.com. DS 34909 8 2 1ae1dfe2…0ee5e2a9743c9
  DELEG server-ipv4=11.22.33.44,23.45.56.67
  DELEG server-ipv6=2001:db8::123
  DELEG server-name=ns1.bigisp.com
```

- Authoritative DELEG in parent

- No DELEG in child

```
examp1e.com. SOA ns1.examp1e.com dns.examp1e.com. 2026030102 …
  DNSKEY 258 3 8 AwEAA...I= ;{id = 18111 (zsk)}
  DNSKEY 257 3 8 AwEAA...8= ;{id = 34909 (ksk)}
```

# DELEG

```
examp1e.com. DS 34909 8 2 1ae1dfe2…0ee5e2a9743c9
  DELEG server-ipv4=11.22.33.44,23.45.56.67
  DELEG server-ipv6=2001:db8::123
  DELEG server-name=ns1.bigisp.com
```

- Parent has name and/or address of child server
- That’s authoritative, child can’t change it

# No more glue

```
examp1e.com. DS 34909 8 2 1ae1dfe2…0ee5e2a9743c9
  DELEG server-ipv4=11.22.33.44
  DELEG server-name=ns1.examp1e.com.
```

- Parent has name and/or address of child server
- Name cannot be in child zone, use address instead

# DELEGPARAM

```
examp1e.com. DS 34909 8 2 1ae1dfe2…0ee5e2a9743c9
  DELEG include-delegparam=ns.myreg.com
```

```
ns.myreg.com. DELEGPARAM server-ipv4=11.22.33.44
   DELEGPARAM server-ipv6=2001:db8::123
```

- CNAME-like redirection (can also include CNAMEs)
- DELEGPARAM has same format as DELEG, but no zone cut or special processing

# How do we get there from here

```
examp1e.com. DS 34909 8 2 1aebbf52...0ee5e2a9743c9
  NS ns1.examp1e.com.
  NS ns2.examp1e.com.
  DELEG server-ipv4=22.33.44.55,66.77.88.99
ns1.examp1e.com. A 22.33.44.55
ns2.examp1e.com. A 66.77.88.99
```

- New DE EDNS0 bit in queries
- “I understand DELEG”
- Referral response contains DELEG
- Or NS and glue if not

# Anti-downgrade

- Authoritative Delegation Types (ADT) flag in DNSKEY ( 002)
- This server understands DELEG, check in NSEC in referrals it sends
- Prevents stripping DELEG, malicious fallback to NS
- Enforces DELEG chain of servers

```
examp1e.com. SOA ns1.examp1e.com dns.examp1e.com. 2026030102 ...
  DNSKEY 258 3 8 AwEAA...I= ;{id = 18111 (zsk)
  DNSKEY 257 3 8 AwEAA...8= ;{id = 34909 (ksk)
```

# Open issues

- DELEG-only zone cut and non-DE client
  - You lose? If so with what code
  - Synthetic NS? How hard to try? What about NS that don’t have names?
- Early implementations
  - Seem to work, but hasn’t been tested very hard
- Hope to publish later this year

# Toward a new security model

- DELEG chain lets you say exactly which servers have your DNS data
  - Strictly top down now, no zone-level redo's
- Extensions to DELEG to require ADoT/ADoQ
  - Entire chain of lookups can be encrypted
- DELEG IP or name is authoritative
  - So can and should check for matching TLS certificate from child server
- If server is trustworthy
  - Maybe someday you can believe unsigned things it says?

# DNS DELEG

John Levine | ICANN 85 Mumbai |