

# Generalized DNS Notifications

... or: how to beg for your parent's attention

ICANN 82 – DNSSEC Workshop  
March 12, 2025

Johan Stenstam  
John Levine  
Peter Thomassen

# Problem Statement

---

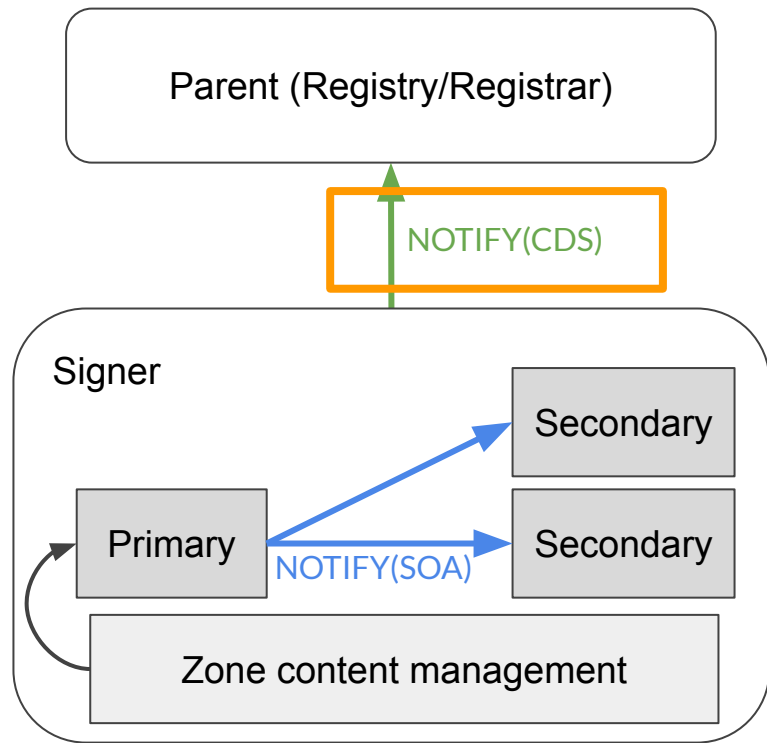
How to tell parent to ...

- create **DS RRset** (bootstrap, RFC 9615)
- update **DS RRset** (RFC 7344)
- update **NS RRset** (CSYNC, RFC 7477)

Delegation management relies on parent **scanning** for CDS/CDNSKEY/CSYNC.

- Slow scanning **delays convergence**
  - Fast scanning is **costly**
- **inefficient**

# Solution Approach



# Endpoint Discovery for Sending Notifications

— — —

- Operator of **child.parent** wants to inform parent of delegation update
- Look for locator in parent zone (and validate if parent has DNSSEC):

`child._dsync.parent. IN DSYNC ...`

- DSYNC record has the following contents (e.g.):

`... IN DSYNC CDS NOTIFY 5301 notifications.parent.`

|                |                                                                                    |
|----------------|------------------------------------------------------------------------------------|
| <b>RRtype:</b> | notification type, e.g. to signal CDS, CSYNC, ... changes                          |
| <b>Scheme:</b> | 1: NOTIFY message;<br>2: DDNS update (draft-johani-dnsop-delegation-mgmt-via-ddns) |
| <b>Port:</b>   | Destination port: recipient is a maintenance service, <b>likely ≠ 53</b>           |
| <b>Target:</b> | Destination hostname; may be a proxy (e.g., registry → registrar)                  |

# Operational Flexibility

— — —

- Different publication approaches
  - Some operators may want to **synthesize DSYNC** at `child._dsync.parent.`
  - ... or put a **wildcard DSYNC** at `*._dsync.parent.`
- Deep delegations (e.g. **city.ise.mie.jp**) require sequence of queries:
  1. Start by assuming the parent is one level up: `DSYNC city._dsync.ise.mie.jp`
  2. Negative response identifies parent, so retry there: `DSYNC city.ise.mie._dsync.jp`
  3. For parents with no-wildcard policy, final try: `DSYNC _dsync.jp`

Much of this is cacheable → parent hit with less queries in practice

- NOTIFY may include EDNS0 Report-Channel option (RFC 9567)
  - Provides feedback channel in case parent encounters a processing problem

# Status

— — —

- [draft-ietf-dnsop-generalized-notify](#) passed DNSOP Last Call & IETF Last Call
  - Sorting out final nits with IESG → publication
- Implementation at child DNS operators:
  - IronDNS implementation under way
  - deSEC implementation under way
- Parent-side:
  - SWITCH (.CH/.LI) implementation under way
  - .SE/.NU planning implementation

# Thank you!

Questions?

[peter@desec.io](mailto:peter@desec.io)

— — —