# Generalized DNS Notifications

draft-ietf-dnsop-generalized-notify

… and related updates on
draft-johani-dnsop-delegation-mgmt-via-ddns

IETF 119 – DNSOP WG
March 18, 2024

John Levine, Johan Stenstam, Peter Thomassen

# Problem Statement

Delegation management via CDS/CDNSKEY/CSYNC processing today relies on scanning.

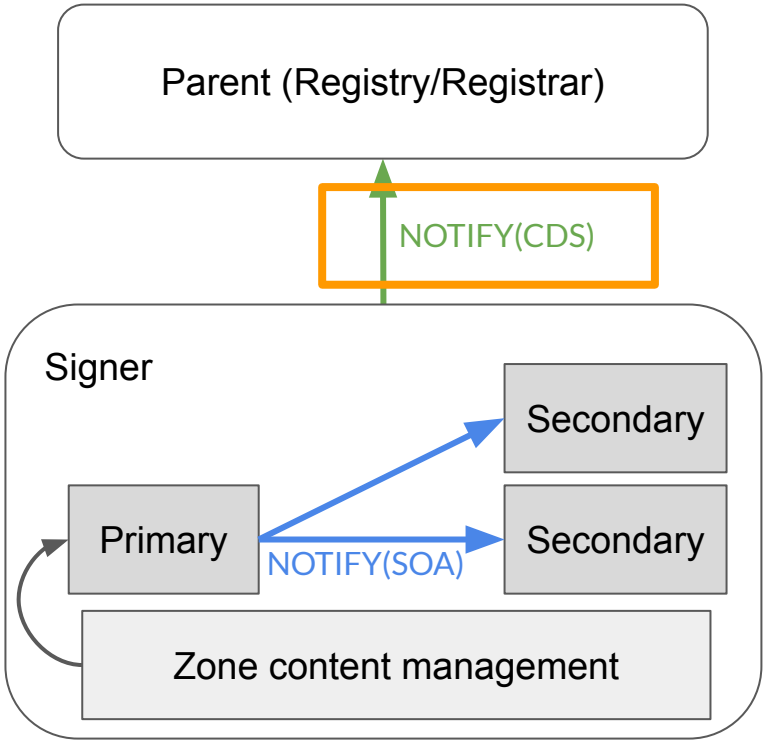
- Slow scanning **delays convergence**
- Fast scanning is **costly**

  → **inefficient**

Related Problems (not treated here):

- Synchronization of DNSKEY RRsets in multi-signer (RFC 8901) setups

# Solution Approach



# News since -00

- Fleshed out mechanism for discovering notification target
  - Uses record published by the parent
  - Record type renamed from NOTIFY to DSYNC (prevent ambiguity with NOTIFY message)
  - Draft says it lives at a `_signal` label, planning to change to `_dsync`
- DSYNC record allows specifying a scheme → reserved some for private use
- Narrowed scope to focus on delegation maintenance
  - Multi-signer scenarios have different requirements for endpoint discovery
- Editorial changes

# Endpoint Discovery for Sending Notifications

- Scenario: 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 1 5301 notifications.parent.
```

**RRtype:** notification type, e.g. to signal CDS, CSYNC, … changes
**Scheme:** 1: NOTIFY message;
2: DDNS update (draft-johani-dnsop-delegation-mgmt-via-ddns)
**Port:** Destination port: recipient is a maintenance service, **likely ≠ 53**
**Target:** 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:
   `city._dsync.ise.mie.jp`
2. A negative response will tell about the parent, so retry there:
   `city.ise.mie._dsync.jp`
3. To facilitate parents with a no-wildcard policy, final try without child labels:
   `_dsync.jp`

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

# Current Status

- Received Dnsdir early review (thanks, Patrick!) → to be processed
- Running code around the corner (thanks to Hackathon!)
- Related draft draft-johani-dnsop-delegation-mgmt-via-ddns (for scheme: 2) updated to reference discovery mechanism