Generalized DNS Notifications

Simplifying DS Automation in the Presence of Automatic Key Rollovers

ICANN 77 – DNSSEC Workshop
June 12, 2023

Johan Stenstam
Peter Thomassen

Problem Statement

– – –

CDS/CDNSKEY relies on scanning.

- Slow scanning **delays convergence**.
- Fast scanning is **resource consuming and costly**.

→ **Scanning is inefficient** (casting millions of nets return small number of fish)

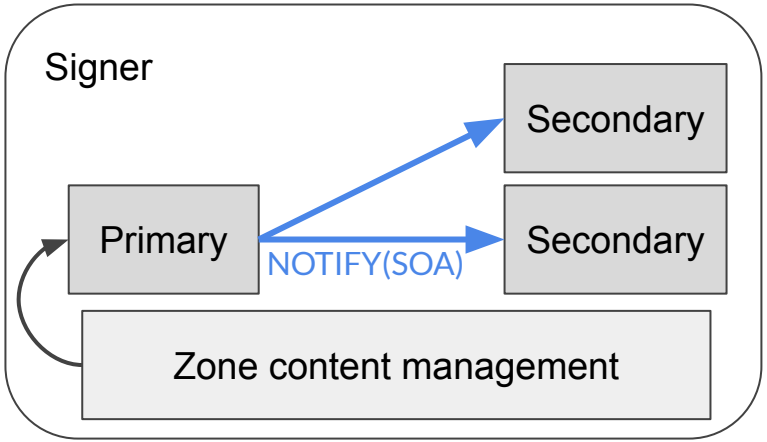
Related Problems:

- **CSYNC:** relies on scanning as well (exactly same situation)
- **Multi-signer** (RFC 8901): signers import each other's DNSKEYs ("union")
  - How to learn about key rolls?

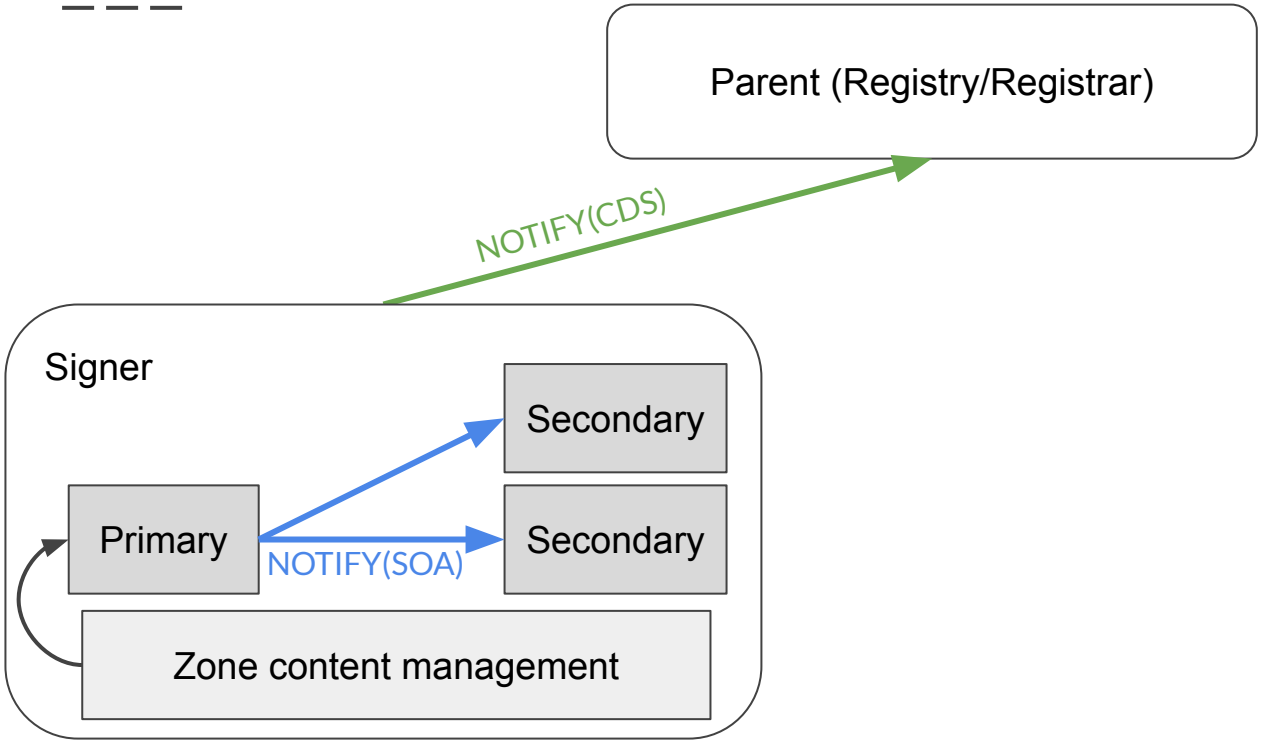
RFC 1996 To the Rescue

- **Recall:** Zone replication suffers from same issue
  - Secondaries check primary for updates every *N* seconds, with *N* given by SOA REFRESH field
- Solution (RFC 1996):
  - Make primary send hint to secondary: DNS NOTIFY message of type SOA
  - **Upon receipt, secondary behaves as if refresh timer had expired**
- **NOTIFY specification allows for notification types beyond NOTIFY(SOA)!**
  - Not a protocol change
- Proposal: Extend with **NOTIFY(CDS)** and similar
  - Intent: Optimize the inefficient scanning done by an increasing number of TLD Registries
  - draft-thomassen-dnsop-generalized-dns-notify

NOTIFY: Internal



NOTIFY: Internal, Vertical



Where to Send NOTIFY(CDS)?

- Look for locator in parent zone. Proposal from draft:

```
parent.   IN SOA …
parent.   IN NOTIFY  CDS     1 5301 notifications.parent.
parent.   IN NOTIFY  CDNSKEY 1 5302 notifications.parent.
```

- Alternative:

```
_notify.[child]._signal.parent.  IN NOTIFY  CDS 1 5301 notifications.parent.
```

- NOTIFY record fields:

Type:	notification type, e.g. to signal CDS, CSYNC, … changes
Scheme:	always 1 for scheme described here. (Others in the future?)
Port:	Destination port: recipient is a (scanning) service, **likely ≠ 53**
Destination:	Destination hostname: **may be a proxy!** e.g. Registry → Registrar

So far, so good!

Enter Multi-Signer

– – –

- Multi-signer workflow (when signers don't share keys):
  1. Zone owner sends zone to all signers
  2. All signers sign with their own key
- **Who coordinates sync** (addition/removal) of delegation-related records?
  DNSKEY/CDS/CDNSKEY/NS/CSYNC?
- One multi-signer implementation uses a **MU**lti-**SI**gner **C**ontroller ("MuSiC")
  → https://github.com/DNSSEC-Provisioning/music
  1. Sync DNSSEC state: (1) fetch all signers' DNSKEY, CDS, CDNSKEY; (2) pass values around
  2. Sync NS state: (1) adds/removes NS records accordingly; (2) set CSYNC
- Controller can run centrally (MuSiC), or decentrally (service runs at each signer)
  decentralized: draft-thomassen-dnsop-mske

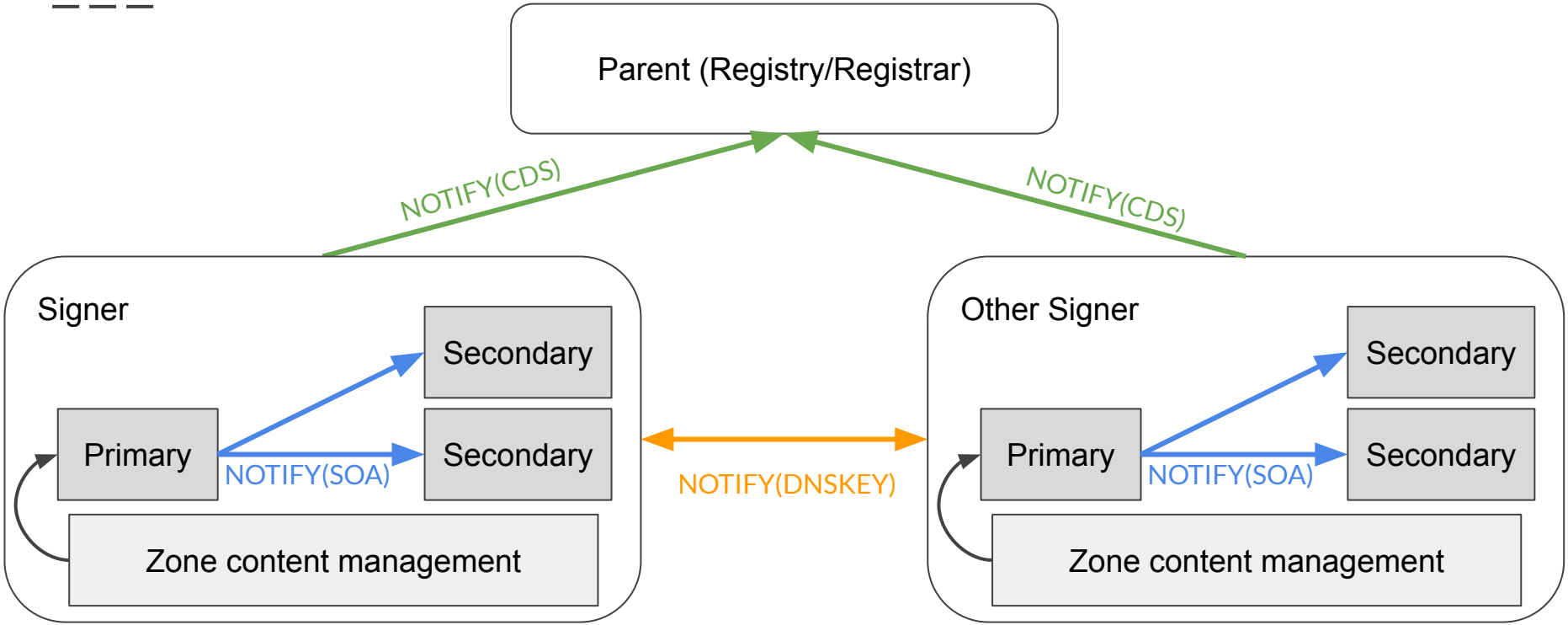
Multi-Signer Key Rollovers

- DNS signers typically consider **ZSK rollovers a completely internal operation**
- **But:** any ZSK rollover requires DNSKEY sync to other signers
  - Similar for KSK rollover (requires CDS/CDNSKEY sync)

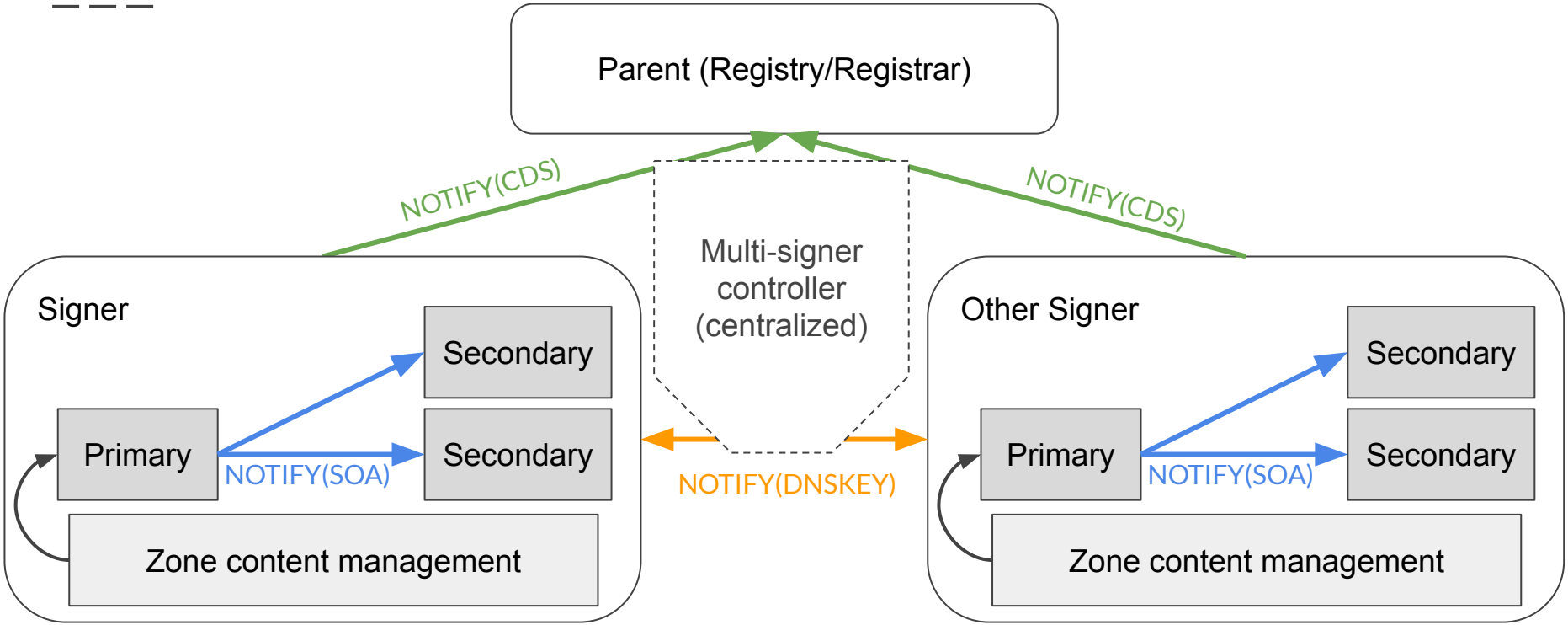
Q: When **Signer A rolls their key**, how does Signer B learn about it?

- **Solution:** Enable Signer A to somehow notify Signer B → **NOTIFY(DNSKEY)**
  - Use `NOTIFY` record type to indicate destination (in the child zone, or per NS)

NOTIFY: Internal, Vertical, and Horizontal



NOTIFY: Internal, Vertical, and Horizontal, with Controller



Summary / Next Steps

- Concept and usefulness of Generalized DNS notifications are beginning to become understood

- Extension of **NOTIFY(SOA)** to **NOTIFY(CDS)**, **NOTIFY(DNSKEY)** may
  - … unlock efficiency gains in automated DNSSEC delegation management
  - … also solve an almost-showstopper for multi-signer models
- This is not a protocol change
  - Unlike the new record type, needed for specifying the notification destination
- Draft presented at IETF 116 (Yokohama, March 2023)
  - Asked for adoption in DNSOP WG
- Working code: https://github.com/johanix/gen-notify-test

Thank you!

Questions?

johan.stenstam@internetstiftelsen.se
peter@desec.io