Generalized Notifications

John Levine, IETF 120 dnsop

The general idea

- Server A has changed something and wants server B to notice
  - Server B polls, but may not poll for a long time
- Thirty years ago: primary NS tells secondary to AXFR/IXFR
- Now: more kinds of updates, child to parent
  - CSYNC to update NS and glue
  - CDS to update DNSSEC keys
Changes to existing NOTIFY

● The record already has an RRTYPE field for the kind of notification
● We just add to the list of RRTYPEs
● No changes in record format
● No new security issues, parent does the same checks it would do anyway
Where to send them

- RFC 1996 didn’t say
  - Primary notifies the rest of the NS for the zone
  - Often hand-configured due to more complex configs
- Child to parent is much more complicated
  - Domain registries all have hidden masters
  - Updates usually through registrars that use EPP to update registry
- New DSYNC RRTYPE in parent
  - Only scheme is NOTIFY, allows expansion for APIs

*._dsync.example. IN DSYNC CDS scheme port target
child._dsync.example. IN DSYNC CSYNC scheme port target
Open questions

- Use SVCB rather than DSYNC?
  - AliasMode or CNAME can point to registrar’s SVCB
  - Use port, ipv4hint, ipv6hint, mandatory
  - Add notifyrrrtype, notifyscheme
- Will registries adopt DSYNC?
  - Is the wildcard OK? Or use two queries for child._dsync and plain _dsync
  - Delegate _dsync.tld to stunt server?
- Add notifications for new RFC 9615 DNSSEC bootstrap
  - Use the same CDS notify, parent knows if it’s bootstrap or rotate
- Further clarifications?
  - DNSDIR review suggested changes, new version posted
- Other issues?