Automating DNSSEC delegation

draft-kumari-ogud-dnsop-cds-01

Olafur Gudmundsson
Warren Kumari
Goal

- Automate DNSSEC KSK rollover in-band.
Relationship Examples

A large (internal) enterprise

Owner/operator and RRR

Owner, outsourced operator & RRR

Registrar as DNS Host
Childs view: State of delegation information flow

- Childs/Publishing DNS operator interacts with parent via one of these types of channels
  - **API**  First class
  - **GUI**  Second class
  - **Email to intermediary**  Third class
Why DS first?

- Its different
- Requires DNSSEC
CDS: Child DS

• Idea: Child publishes what it wants parent to reflect
  • simple concept easy for child to express
  • only difference between CDS and DS is the type code

• Consequence: "`parent" scans for CDS
CDS protocol 101

- Child publishes CDS signed by KSK
- Parental Agent queries for CDS validates and translates into changes in DS set
- Child checks for changes in DS
  - Child moves to next step in rollover
  - --> Child updates/removes CDS
- repeat
CDS: Reactions

• This is good; just what we want

• As a parent I want instructions that I can log

• I, the parent, want your public key because you kids can not be trusted to do this right

• This is a bad idea
Path forward

- Warren and I hosted a F2F discussing CDS
  - Overall positive but some concerns
- What next:
  - Publish updated version or drop?
Backup slides
Who is my parent?

- When Joe Public registers joe-public.<tld> from registrar X then from his point of view
  - X is <tld>
  - Backend registry/DNS operator is immaterial
  - relationship between X and backend is not visible to child