TDS

draft-wkumari-dnsop-trust-management

What's the problem?!

- **Sometime** we will have to roll the root key
  - Dunno when, dunno why…
- When this happens, some set of folk likely to break
  - Old resolvers, `trusted-keys` / `managed-keys`
  - Sure would be nice to be able to predict how many and who will break
  - We've worked hard to get DNSSEC out there, would suck if people turn it off because it bites them again….
  - … and the PR issues…

Proposal

- Do something like CDS, but for Trust Anchors
- Resolvers query the ~~root~~ TA location for a special name, made up of the key tags that it knows about
- This exposes to the root who has what TA
- Can monitor the population, predict % breakage
  - …and who will break.
- Also allows key rollover - **if that is what the TA maintainer wants to do**….
- … or 5011 if not

Example

Resolver has key with tag: 19036

Q: `_19036 IN TDS`

R: *`_19036 IN TDS 8 2 49AAC11D7B6…`*

Keyroll starts, new DNSKEY, new tag: 56123

Q: `_19036 IN TDS`

R: `_19036 IN TDS 8 2 49AAC11D7B6…`
`IN TDS 8 2 32AB43123C2…`

Resolver installs new key, now has 2 (19036, 56123)

Q: `_19036-56123 IN TDS`

R: `_19036-56123 IN TDS 8 2 49AAC11D7B6…`
`IN TDS 8 2 32AB43123C2…`

Issues

- Doesn't fix the currently broken people
  - Yup, but it does tell you who **isn't** broken…

- We will roll the root soon, this doesn't exist…
  - Have to start sometime, why not now?
  - Many upgraded BIND on 2015-02-18, 2015-07-08
  - … and unbound on 2014-10-12

- The top 2000 resolvers service 94% of people
  - Sure, but the remaining LOT service 6%

- Gah, we already have 5011, you want to replace it!?
  - This works with 5011 if you want.

Questions?

Cute kitten picture to distract you…

Picture: Andy Rifkin, https://www.flickr.com/photos/ifindkarma/17129805130