/delivers/

CDS, CDNSKEY

Mechanisms for in-band provisioning of registry metadata for DNSSEC

Joe Ableyjoe

@ableyjoe

ICANN 49, Singapore, March 2014

“I have never been able to properly explain myself in this climate.” Hunter S. Thompson

“If you get off the plane and see satellite dishes pointing straight up, get back on the plane.” Randy Bush

DNSSEC for Zone Administrators

Toolchains exist to make life easy!

- BIND9, OpenDNS, others
- Key generation, RRSet signing
- KSK rollover and initial signing require interaction with a registrar
  - need, ultimately, to publish a DS RRSet in the parent zone
  - there is no standard protocol or mechanism for this

DS RRSets in the Parent Zone

Straightforward and Simple!

- Figure out whether your parent wants a DS RRSet, or a DNSKEY RRSet (most want DS, some want DNSKEY)
- Cut and paste multi-line base64 data from a terminal window into a web form
  - keep doing it until it works, or
  - call the registrar helpdesk, or
  - give up

Clearly this is not a support nightmare

57217 5 2
AEC44D5748449950D77C7B2C36ECEF8E30A497DB7EE726
21375ACE1139FE3151

57217 5 1
2BF1EE54C7B17D104BA2F55A46A3889644C893FD

Enter CDS, CDNSKEY

draft-kumari-ogud-dnsop-cds-05

- Instead of trying to paste obscurely-formatted nonsense into a web form, publish it in the child zone instead
- Instead of doing that manually, have your excellent DNSSEC tools do it for you
- Reduce the registrant/registrar interaction to click-and-confirm

About Warren's Draft

draft-kumari-ogud-dnsop-cds-05

- Goes to great lengths to specify exactly what is and isn't appropriate
  - it would defeat the whole point of DNSSEC not to do this carefully
- Accommodates a wide range of relationships between child and parent

Information Retrieval

Two Potential Approaches

- If practical, you could walk all your registrants' zones looking for CDS/CDNSKEY changes, and take action where necessary
  - trigger communication with the registrant
  - trigger registry interaction, if secure
- Or, poll the zone only when a registrant triggers the retrieval
  - no cut-and-paste required

Related Work

draft-hardaker-dnsop-csync-02

- Similar mechanism intended to allow a child zone operator to signal desired NS, A and AAAA RRSets in the parent
  - also potentially interesting
  - specifically not intended for use with DS/DNSKEY

Recommendations!

Registrars that are doing DNSSEC:

- Point your developers at draft-kumari-ogud-dnsop-cds-05
  - you can Google it *(Warren, Google is a verb!)*
  - feedback on dnsop (IETF) mailing list, or to authors
- Consider whether implementing a mechanism like this (or, exactly this) could make your customers' lives easier
  - a happy customer is a higher-margin customer