GoDaddy DNSSEC Signing and DS Updates

How We Do DNSSEC for DNS and Registrar Customers

GoDaddy Registrar Customers

- DS Added via EPP
- Enabling Managed DNSSEC triggers automated updates to DS
- Customer UI always available to change DS records at Registry
- Customers can disable Managed DNSSEC and submit DS
- GoDaddy as Secondary DNS for DNSSEC signed zones
  - Signed elsewhere and zone transferred in (AXFR)
- GoDaddy as Primary DNS for DNSSEC signed zones
  - Signed by GoDaddy and zone transferred out (AXFR)

GoDaddy Managed DNSSEC

- Regardless of parent (TLD), CDS and CDNSKEY are always published
- That is all
- We encourage all Registries to poll CDS and/or CDNSKEY, and accept Notify for domains using CDS/CDNSKEY
- It would be nice if Registries had a way to publish which they use (CDS or CDNSKEY), and Registrars to flag Registrant domains as using said thing
- Registrars: Please understand that DS records are “use once” in nature, and there should never be a need to obtain a DS if updated via CDS or CDNSKEY
  - In particular: No need for Registrars to track current value of DS
- Registries/Registrars: Notification for non-CDS/CDNSKEY DS updates would really be a good thing. Ideally exclude CDS/CDNSKEY changes from the notification scheme. Flag for domains using CDS/CDNSKEY?

GoDaddy DNSSEC Cross-Signing

- We don’t do dynamic (in-line) signing, so it isn’t a technical requirement for us
- We are interested in working on this to support multi-provider DNSSEC
- Suggest use of DNS mechanisms for widest interoperability and security (vs any actual APIs), e.g.:
  - CDNSKEY (overload), or similar RRTYPE ZDNSKEY?
  - Sign with ZSK, hidden master queries for this, merge into DNSKEY RRSet
  - Sign DNSKEY RRSet with KSK, providers do XFR and sign zone
  - Hidden master does CDS and CDNSKEY exclusively

Initial DS from DNS to Registry Idea

- Assumption/Requirement: DNS hosting provider, supports DNSSEC
- DNS provider: Use DNSSEC for zone(s) containing names used as NS records by customers
- Add TLSA records for those NS names, and Certificates on those name servers for those NS names
- Registry can poll via DNS-over-TLS to Authority (DoTA) to obtain initial DS using CDS/CDNSKEY records
- Validate DoT using DANE-TLSA
- Registry already has NS names and if necessary, glue for A/AAAA