DS Automation: Non-technical Considerations

James Galvin, Ph.D.
Afilias, Inc
ICANN69 - DNSSEC Workshop
21 October 2020

Two Primary Considerations

- Catch-22 within the retail side of domain registration system
  - Lack of “market” for DNSSEC - been around for more than 25 years
  - Investment required to get it done

- Gap in “authority”
  - Registry requirements
  - Registrar requirements
  - Missing Link

Registry Requirements

- Base Registry Agreement – Updated 31 July 2017
  - 2.10(d) Registry Operator shall provide public query-based DNS lookup service for the TLD (that is, operate the Registry TLD zone servers) at its sole expense.
- Specification 6 - Registry Interoperability and Continuity Specifications
- Section 1.3 DNSSEC

  Registry Operator shall sign its TLD zone files implementing Domain Name System Security Extensions (“DNSSEC”).

  Registry Operator shall accept public-key material from child domain names in a secure manner according to industry best practices.

Registrar Requirements

- 2013 Registrar Accreditation Agreement - 27 June 2013
- Additional Technical Specifications
- Section 1

> Registrar must allow its customers to use DNSSEC upon request by relaying orders to add, remove or change public key material (e.g., DNSKEY or DS resource records) on behalf of customers to the Registries that support DNSSEC. Such requests shall be accepted and processed in a secure manner and according to industry best practices.

Missing Link?

- DNS Service Providers do not have a defined role in the registration ecosystem, and yet:
  - DNS is essential to the value of a domain name
  - Have a vested interest in the evolving advancement of DNS
  - Have a vested role in the deployment of DNSSEC
- How does a DNS service provider submit DNSSEC information?
  - Become a registrar to support your customers - not ideal
  - SneakerNet - error prone
- Technology is not the problem