Afilias℠

Registry Failover and DNSSEC

Jim Galvin, Ph.D.

ICANN Toronto
DNSSEC Workshop
17 October 2012

Describe The Situation

- DNS operator is failing
  - Explicit separation from the registry
  - May or may not be related to a registry failure
- Significant and irreparable impact on existing registrants because DNS resolution is at risk
- DNS resolution affects all services and applications available through the registered domain name
- DNS services (and thus DNSSEC) must be transitioned to a new operator

Transition Requirement

- **Minimize if not eliminate validation failures**
  - Includes DNS resolution more generally
- Transitioning DNS and DNSSEC services is still getting a lot of attention in various technical fora
- I want to focus on one specific technical requirement and put it in a registry discovery recovery context
- Note, this is not a complete technical solution; I am calling out a technical issue that a registry operator should consider in their risk management assessment

Pre-Publication of Next Key

- The essential technical principle is that in order for validation to succeed the appropriate public key must be available at the time it is needed
- For this to remain true during a key rollover the “next” key must be published in advance, which is simple when there is no DNS operator change
- The essential action when the DNS operator changes is to get the new key included in the key set published by the “losing” DNS operator
- Again, simple when the transition is planned

Unplanned Transition

- During an unplanned transition the fundamental question is whether or not the "losing" DNS operator is capable of continuing services
- If so, the procedures for an unplanned transition would be the same as for a planned transition
  - Coordinate the pre-publication of the "next" key or DS
- If not, there is no way to avoid validation failures
  - It might be necessary to be "unsigned" before "resigning"

EBERO and DNSSEC

- The essential characteristic of a solution to the problem is to have an active key relationship with an emergency backup DNS service provider
- Active means the key is available on hot-standby and can be placed in service in near-real-time

THANK YOU!