Afilias℠

Deploying DNSSEC: Lessons Learned

Jim Galvin
Director

ICANN Brussels Meeting
DNSSEC Workshop

23 June 2010

Who is Afilias?

- **10 years of experience** in critical Internet infrastructure
- Best known for domain name registry services in **support of 15 million domains** across 15 TLDs
- Diverse DNS Network handling **billions of queries** daily
- Launched Managed DNS services in Feb 2009

DNSSEC Best Practices

- Must support the import and export of the public key
- Must provide a mechanism to unsign a domain
- Must functionally separate DNS services from registration services
  - Must support the import of a new NS resource record set without discontinuing existing DNS services
  - Must continue DNS services until explicitly told to stop
  - Must setup new DNS services in advance of transfer
  - Must support export of domain's zone file

Import/Export of Public Key

- Must support the import of a public key created by a third party
  - Must always be published in the domain's zone, which will be at the registrar if DNS services are bundled with registration services, otherwise at the DNS operator
  - Must optionally be published in the parent's zone; "on deck" keys will not be published in the parent zone
- Must support the export of a public key created locally
  - Gaining DNS operators need their new key information published in the zone file of the Losing DNS operator as an "on deck" key

Unsigning

- Functionally, to unsign a domain name what is required is to remove the public key information (DS record) from the parent zone
  - Registrars must support this feature

Import of NS Resource Records

- When DNS services are being transferred the registrar must import and publish to the registry the new NS resource record glue set
- Most registrars already do this except that importing a third party set of NS resource records results in existing DNS services being discontinued if the registrar is providing both DNS services and registration services; this must not happen

Continue DNS Services

- When executing the transfer of DNS services, the Losing DNS operator must continue to provide DNS services until explicitly told to stop
- When DNS services are bundled with registration services, it is essential that Losing registrars continue providing DNS services after the registration has transferred until explicitly told the services are no longer needed

Provide New DNS Service First

- When executing a transfer of DNS services, the Gaining DNS operator must configure and deploy the new zone prior to initiating the transfer at the Losing DNS operator
- When DNS services are bundled with registration services, a Gaining registrar must do this before initiating the transfer of registration services, including signing the zone if required

Zone File View

- DNS operators should provide a mechanism for the export of a zone's contents to a human readable format
  - This facilitates the transfer of a domain's zone from one DNS operator to another

More Information

- http://afilias.info/dnssec

- Jim Galvin
  - jgalvin@afilias.info
  - +1 215-706-5715