DNSSEC Industry Coalition
DNSSEC Readiness:
Risk Analysis

Prepared by: Afilias Limited & Shinkuro, Inc.
For: .ORG, Public Interest Registry

April 2010
1. Introduction

Public Interest Registry (PIR) is the registry for the .ORG top level domain (TLD). Afilias Limited (Afilias) is the registry service provider for the .ORG TLD.

On 2 June 2009 PIR launched the signing of the .ORG top-level domain (TLD). Since that time PIR and Afilias have been working together to conduct testing of the DNSSEC operation and with registrars to test the deployment of signed delegations.

In preparation for launching signed delegations, i.e., permitting certified registrars to offer DNSSEC services to registrants, PIR requested Afilias to conduct a risk analysis of our readiness to launch signed delegations in the .ORG TLD. We engaged the services of Shinkuro, Inc., to assist in the risk analysis.

1.1. Scope

The analysis includes a review of all operations and activities related to DNSSEC beginning at the registrar through and including DNS resolution of DNSSEC related information. It expressly does not include actions taken by a registrant, although it does include the actions taken by a registrar that may result from the registrant actions. It further does not include any activities related to the signing of the .ORG zone unless those activities are directly affected by an in scope action. Finally, it does not include a review of any operations or activities that are a direct result of policies or contractual obligations set forth by PIR or ICANN.

1.2. Method

The analysis was conducted as a tabletop exercise. A list of questions was created, Afilias answered the questions, and Shinkuro based their assessment on our responses to those questions.

The list of questions was created from two sources. Shinkuro created an initial list of questions and Afilias reviewed the RSTEP response to the PIR DNSSEC proposal and extracted a list of the open questions and suggestions made at that time. These preliminary lists were reviewed together by both Shinkuro and Afilias. We agreed by consensus the questions that were in scope and to be answered by Afilias.

The answers to the questions were prepared through an iterative process. Afilias provided drafts of this analysis to Shinkuro who responded with comments and additional clarifying questions until a mutual understanding of the response was reached. Shinkuro prepared their assessment after a final version of the document was prepared.
2. Questions

1) Questions related to key roll overs.

   a) What are the key rollover plans? Include planned, unplanned, and emergency procedures for both KSK and ZSK.

   b) Will you be compliant with RFC 5011, Automated Updates of DNS Security (DNSSEC) Trust Anchors?

   c) With what aspects of RFC 4641, DNSSEC Operational Practices, will you be compliant? For the aspects for which you will not be compliant, what is the alternative and what is the impact?

2) Questions related to a DS record.

   a) What is the process for publishing a DS record in the zone, from receipt of the EPP transaction to its presence in an authoritative name server?

   b) Does the registry perform any checking of DS data when it is sent to the registry (either for internal validity, e.g. algorithm-signature compatibility, for agreement with a supplied DNSKEY, or for agreement with child zone data)?

      i) If so, what is the effect if there is found to be a problem? If not, is this policy clear to registrars?

      ii) What happens if the registry is apprised of a mismatch that is causing a validation failure?

   c) What prevents a registrar who has not passed the DNSSEC portion of the OT&E test from adding DS data to a domain?

   d) Is there any ability for a registrar that has not passed OT&E test to pass through a DS for customer via any other channel than EPP?

3) Questions related to signing the zone.

   a) What are the procedures for checking whether or not each signing operation completes successfully? If it does not complete what level of failure is raised?

   b) What is the plan if signing the .ORG zone adds a delay to publishing that is longer than the delay in PIR’s contractual commitment to ICANN?

   c) How does the registry ensure it never publishes a bogus signature?
d) What happens if a name server loses contact with the master and its signatures are about to expire?

e) Can the registry drop TTLs if it is aware that a transfer is taking place?

f) Are timers (signature times, TTLs) appropriate and consistent?

4) Is there a way to test the quality of the data that gets into the registry before it makes it to the cloud?

5) Are there circumstances during which DNSSEC might be stopped? If so, how will this be implemented?

6) What are you doing, if anything, in response to the expected problems with middleboxes?

7) What changes are you making to Whois responses in support of DNSSEC?

8) Is there an architecture/flow diagram of the DNSSEC update process?

9) Is there a rollback process in place to deal with problem zones, including those where the problems are DNSSEC-related?
   a) Is it exercised?
   b) Can it be exercised?
   c) On demand?

10) Questions related to algorithms.
   a) Is there a standard process for adding support for new algorithms?
      i) For DS records?
      ii) At some time in the future should .ORG roll algorithms?
   b) Is there a standard test that the registry will apply when new algorithms are approved?

11) Is there monitoring of TCP statistics based on the addition of DNSSEC?

12) Will Afilias provide toolkits to registrars to in order to help transition to DNSSEC? If so what tool kits?

13) What are the technical requirements for a registrar to be able to add DS data to a domain? How are those requirements tested? Is there any monitoring of the
capability once a registrar has passed the initial test? Under what conditions will registrars have their DNSSEC capabilities revoked?

14) Questions related to technical support.
   
   a) What is the training regimen for Tech Support reps in DNSSEC?
   
   b) How are Tech Support agents tested on their DNSSEC understanding?
   
   c) What tools are available to Tech Support agents to perform DNSSEC troubleshooting?
   
   d) Do the tools have the ability to be run from a remote vantage point?
   
   e) Is there a standard "troubleshooting script" for DNS troubleshooting? How has it been modified in the face of DNSSEC?
   
   f) Does the script take into account difference in visibility of anycast instances?
   
   g) Is the Tech Support staffing level expected to change during DNSSEC turn-up? If so, how? For how long?
   
   h) What do Tech Support reps do when they are not successful in isolating the source of a DNS problem?

15) Is there any provision for emergency rollover of child key (DS) data?

16) Is there any mechanism for registrars to control the TTL on DS or any other RR at a delegation in the registry?

17) Does the registry accept the maxSigLife parameter on DS data in EPP commands? If so, what are the limits on that acceptance? What is the effect if a registrar sends a maxSigLife parameter outside the registry's parameters?

18) Are there concerns about the revision to RFC 4310 that is currently in progress? What if anything is planned to address those issues?

19) Questions related to publishing DS records in authoritative name servers.
   
   a) What is the minimum time between the addition of new DS data to the registry and it being available from at least one name server?
      
      i) The average time?
      
      ii) The maximum possible time?
      
      iii) Are these figures different in case of removal of DS data?
b) What is the minimum time between the addition of new DS data to the registry and it being available from every name server?

i)  The average time?

ii) The maximum possible time?

iii) Are these figures different in the case of removal?

c) What additional processing time to a domain name update is added as the result of the additional DS data?

20) What are the throughput limits of the signing process?

a) How different are they from the process without any signer in the way?

b) How has this been tested?

21) Do registrations with DS data (i.e. not fitting in an Opt-Out span) get processed along with unsigned registrations, or do they update the zone via separate paths?

a) If the former, what are the possible effects on domain registration/update/delete processing?

b) If the latter, are there any side effects of updating the DNS in a different order than the registry? What are they? How has this been tested?

22) The addition of DS data will increase the size of positive data for non-Opt-Out zones. Is there an anticipated effect on DNS server availability due to bandwidth constraints?

a) How has this been modeled?

b) What happens if the model parameters change?

c) What are the limiting assumptions?

23) Afilias is over provisioned in its DNS systems. Does the addition of DNSSEC alter the percentage by which the systems are over provisioned?

a) How is this determined?

b) How is it monitored?

c) What is the threshold at which additional systems will be added to a site?

d) To the overall cloud?
e) Is there a level that will require a new site to be added?

24) How much TCP traffic can one site handle as a percentage of its total traffic per second? What will this do to the number of queries per second that can be handled?

25) What is being done to keep answers small to fit in a single, un-fragmented UDP packet?
   a) Smaller than 1500 bytes (Ethernet v2)
   b) Smaller than 1492 bytes (PPPoE)
   c) Smaller than 1220 bytes (IPv6 tunnels)

26) How do we monitor capacity and time to update regarding when keys are rolled over? How does rolling a key impact the update time?

27) Is there going to be a way for an unsigned domain to be included in an NSEC3 chain?

28) Have you or do you plan on reviewing additional iterations of NSEC3?

29) Under what conditions would you switch to NSEC?

30) Is any consideration being made for bulk updates of DS records for multiple zones that are signed by a common key (KSK)?
   a) When a registrar signs zones for registrants?
   b) When a third-party (DNS Service Provider) signs zones for registrants?