ICANN Registry Services Technical Evaluation Panel

Report on Internet Security and Stability Implications

of the

Public Interest Registry (PIR)

DNSSEC Proposal

June 4, 2008

Preface

This report presents the findings of a technical evaluation of the proposal[1] by Public Interest Registry (PIR) to amend their registry agreement with ICANN in order to facilitate the introduction and use of Security Extensions for the Domain Name System (DNSSEC) in the .org zone.

On 8 November 2005 ICANN adopted[2] a consensus policy developed by its Generic Names Supporting Organization (GNSO) concerning the review and approval of requests by gTLD registry operators for new registry services.[3] This policy was implemented on 25 July 2006[4] as the Registry Services Evaluation Policy.[5] The policy provides for the evaluation of a proposed registry service by a team of experts selected from a standing Registry Services Technical Evaluation Panel (RSTEP)[6] when ICANN determines that the service could raise significant security or stability issues.

The process begins with a preliminary determination by ICANN that an RSTEP review is or is not required for a particular proposed registry service.[7] If ICANN determines that a review is required, an RSTEP review team investigates and evaluates the proposed service with respect to its potential impact on security or stability, as defined by the consensus policy:

> **Security**—An effect on security by the proposed Registry Service shall mean (a) the unauthorized disclosure, alteration, insertion, or destruction of Registry Data, or (b) the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards.
>
> **Stability**—An effect on stability shall mean that the proposed Registry Service (a) is not compliant with applicable relevant standards that are authoritative and published by a well-established, recognized, and authoritative standards body, such as relevant Standards-Track or Best Current Practice RFCs sponsored by the IETF, or (b) creates a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems operating in accordance with applicable relevant standards that are authoritative and published by a well-established, recognized, and authoritative standards body, such as relevant Standards-Track or Best Current Practice RFCs and relying on Registry Operator's delegation information or provisioning services.

---

[1] http://icann.org/registries/rsep/pir-request-03apr08.pdf

[2] http://www.icann.org/minutes/resolutions-08nov05.htm

[3] The ICANN Board resolution adopting the GNSO consensus policy (see footnote 2) specifies that implementation of the policy in contractual terms should be guided by the provisions of the .NET registry agreement (http://www.icann.org/tlds/agreements/net/net-agreement-new.html), which includes a precise definition of "Registry Services."

[4] http://www.icann.org/announcements/rsep-advisory-25jul06.htm

[5] http://www.icann.org/registries/rsep/rsep.html

[6] http://www.icann.org/registries/rsep/rstep.html

[7] The consensus policy also provides for the separate review of potential competition issues, which lie outside the scope of the RSTEP review.

The review team completes its evaluation within 45 days, and prepares a written report of its findings, containing:

> (a) a detailed description of the technical issue(s) raised by the proposed registry service, and the assumptions, information,[8] analysis, and reasoning upon which the review team's evaluation is based;
>
> (b) the team's expert assessment of the potential impact of the proposed registry service on security or stability; and
>
> (c) a response to any specific questions from ICANN that were included in the referral from ICANN staff in its request for the RSTEP review.

The review team's report is delivered to the ICANN Board as input to the Board's consideration of the proposed registry service and action on the registry operator's request to deploy the service within the context of its contract with ICANN.

It is important to recognize that the RSTEP review is a technical evaluation of a proposed registry service with respect to the likelihood and materiality of effects on security and stability, including whether the proposed registry service creates a reasonable risk of a meaningful adverse effect on security or stability. Because many other questions and issues may be relevant to the overall assessment of a proposed registry service, it is not a recommendation to the ICANN Board concerning whether or not the Board should approve or reject the registry operator's proposal.

[8] RSTEP review teams are expected to gather information from as many sources as necessary in order to conduct a thorough and comprehensive evaluation, including, but not limited to, information provided by the registry operator, by ICANN, and by contributors to the ICANN public comment forum that is associated with each registry service request.

Table of Contents

1. Introduction

1.1 Summary of the Proposal

PIR's proposal is to introduce DNSSEC (as specified in RFCs 4033, 4034, 4035, and the NSEC3 and opt-out portions of RFC 5155) to the .org zone. Should the proposal be approved, PIR would:

- Provide DS records for domains in the .org zone
- Make changes to the .org registry's EPP server to allow registrars to add, change, and remove DS records for their customers
- Show information in WHOIS about the DNSSEC status of an .org sub-domain

PIR does not propose to charge an additional fee for these changes.

1.2 RSTEP Process Summary

1.2.1 Activities

The RSTEP review team evaluated the PIR proposal with respect to its potential impact on Internet security and stability. In order to inform its work, the review team took advantage of previous analyses of DNSSEC deployment in TLD zones, consulted with outside experts, and engaged PIR in clarifying discussion.

The review team took the following actions during the 45-day period beginning with the referral from ICANN to the Chair of the Registry Services Technical Evaluation Panel on April 21, 2008:

- Participated in regular conference calls attended by the review team and the Chair of the Registry Services Technical Evaluation Panel
- Exchanged email with PIR to get clarification of their proposal (see Appendix A for their clarifications)
- Reviewed the small amount of feedback from the open public comment process initiated by ICANN on April 23, 2008
- Consulted with external experts in registry services related to security, stability, and DNSSEC implementation and operations

1.2.2 Public Comments

ICANN opened a public comment forum for the PIR proposal on April 23, 2008. The comment period closed on May 24, 2008. A total of four comments were made in the forum. The comments talked about different aspects of the PIR proposal, and the review team read and considered each of the comments.

1.2.3 Gathering of Supporting Material and Data

In the early part of the review team's work, a great deal of supporting material related to DNSSEC operations was gathered and reviewed. This included the relevant RFCs and archives of discussions on DNSSEC deployment mailing lists. In addition, many team members had direct experience with deploying DNSSEC, and that experience was shared during discussion. The review team also reviewed documents from ICANN's Security and Stability Advisory Committee relating to DNSSEC.

1.2.4 Discussions with PIR

After reading PIR's proposal, the review team had questions concerning the proposal. The team sent multiple rounds of questions to PIR by email; PIR replied in a timely fashion. The team's questions and the responses that were used are collected in Appendix A of this report. PIR also sent two confidential documents, but the review team did not need the information in either of them in order to reach or support the conclusions found in this report.

1.3 Key Definitions

An overview of DNSSEC and definitions of many of the terms used in this report can be found in RFC 4033.

1.3.1 Security

An effect on security by the proposed Registry Service shall mean (A) the unauthorized disclosure, alteration, insertion or destruction of Registry Data, or (B) the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards. (Definition comes from GNSO Recommendation, located at http://gnso.icann.org/issues/registry-services/final-rpt-registry-approval-10july05.htm#5.)

1.3.2 Stability

An effect on stability shall mean that the proposed Registry Service (A) is not compliant with applicable relevant standards that are authoritative and published by a well-established, recognized and authoritative standards body, such as relevant Standards-Track or Best Current Practice RFCs sponsored by the IETF or (B) creates a condition that adversely affects the throughput, response time, consistency or coherence of responses to Internet servers or end systems, operating in accordance with applicable relevant standards that are authoritative and published by a well-established, recognized and authoritative standards body, such as relevant Standards-Track or Best Current Practice RFCs and relying on Registry Operator's delegation information or provisioning services. (Definition comes from GNSO Recommendation, located at http://gnso.icann.org/issues/registry-services/final-rpt-registry-approval-10july05.htm#5.)

1.3.3 Starting, Running, and Stopping DNSSEC

This document talks about running DNSSEC in many places. Currently, PIR is not running DNSSEC, and they propose to start. They also say that they might have to stop running DNSSEC for a long period of time, such as if there are too few registrars; they might even restart after stopping. The general definitions used in DNSSEC appear in RFCs 4033, 4034, and 4035; other definitions for particular DNSSEC features appear in other RFCs.

In the context of this document, a registry "starting DNSSEC" means taking the following steps:

- Create a zone signing key (ZSK). If the key signing key (KSK) for the zone is different than the ZSK, create one or more KSK. (Throughout this document, we assume that the ZSK is different from the KSK, which is the common practice.)
- Create and sign DNSKEY records for the zone that contain all the existing ZSK and KSK for the zone.
- Create and sign the initial NSEC or NSEC3 records for the zone.
- Create the initial RRSIG records for the resource record sets in the zone.
- Publish in the DNS the DNSKEY, RRSIG, and NSEC/NSEC3 records.
- Distribute the KSK of the zone, either by having it signed by a parent zone (if that zone is running DNSSEC), or by publishing it outside of the DNS so that other systems that are verifying DNSSEC signed responses can use it as a trust anchor for the zone.

In the context of this document, a registry "running DNSSEC" means first starting DNSSEC then taking the following steps:

- Receive authenticated copies of the keying material of child zones of the registry (there are many different ways in which the keying material can be authenticated)
- Sign, and publish in the DNS a DS record (or record set) for all keying material received.
- Update the NSEC or NSEC3 records for the zone based on the current state of the database that the registry is running for the zone.
- Maintain the ZSK and KSKs for the zone by publishing replacements for them according to the maintenance policy (also called the *rollover policy*) for the zone.

In the context of this document, a registry "stopping DNSSEC" means taking the following steps:

- Stop publishing in the DNS any DS records of child zones
- Stop publishing the zone's NSEC/NSEC3 records

- Stop receiving authenticated copies of the keying material of child zones of the registry
- Withdraw the KSK for the zone from the parent zone after the current signature lifetimes and TTLs have expired (if the parent zone is running DNSSEC), or continue to publish the KSK and related records in the zone until all systems that had installed it as a trust anchor have stopped using it as a trust anchor.

Note that this definition of "stopping DNSSEC" is meant for long-term stopping, not just a short period that might occur during an emergency.

This document details some of the different ways to start, run, and stop DNSSEC, and the impact on stability that those different ways might cause.

1.3.4 Other DNSSEC-specific Terminology

These definitions are derived from the formal definitions in RFC 4033. In these definitions, "validating resolver" means a DNS resolver that verifies DNSSEC signed responses.

Secure – A domain is secure only if a validating resolver can use its trust anchor to follow a trust chain to validate all the signatures in the response. This allows positive validation by that resolver.

Insecure – A domain is insecure only if a validating resolver can follow a chain chain of trust from a configured trust anchor to prove that there is no DS record for the domain. This is a positive validation that the domain is not secured.

Indeterminate – A domain's security is indeterminate whenever there is no trust anchor or chain of security to follow to that domain. Because the root zone is currently unsigned, validating resolvers treat most unsigned zones this way. For example, .org is "indeterminate" today. There is neither positive nor negative validation of the domain in this case.

Bogus – The validating resolver has a trust anchor and possibly a secure delegation indicating that subsidiary data is signed, but the response fails to validate for some reason: missing signatures, expired signatures, signatures with unsupported algorithms, data missing that the relevant NSEC record says should be present, and so forth. For the end user, this will usually result in a "server failure" error, and the domain will be unavailable.

1.4 Members of the RSTEP Review Team for this Proposal

The five members of the RSTEP review team for the PIR DNSSEC proposal are:

- Patrik Fältström
- Paul Hoffman (chair)
- Mark Kosters
- Frederico A C Neves
- Andrew Sullivan

The members of the review team were assisted in their work by the Chair of the Registry Services Technical Evaluation Panel, Lyman Chapin.

1.5 Support for the Review Team

Staff support was provided by Patrick Jones, ICANN Registry Liaison Manager. The review team thanks ICANN for providing international teleconference capabilities, and thanks Patrik Fältström for hosting the mailing list, Jabber server, and FTP server.

2. Summary of Findings

Public Interest Registry (PIR) proposes to add support for DNS Security Extensions (DNSSEC) to their management and operation of the .org top-level domain. The RSTEP review team evaluated the PIR proposal with respect to its potential impact on Internet security and stability.

With respect to technical feasibility, the review team is satisfied that PIR could implement the service that they have proposed, in conformance with the relevant Internet standards.

The findings of this review should be interpreted in the context of the size and importance of the .org zone. Were this a proposal from a registry operating a substantially smaller TLD, the security and stability issues would be technically the same, but the potentially affected population of Internet users (and therefore the potential systemic effect on the Internet as a whole) would be much smaller. We note the significance of the fact that ICANN's own domain is a child of .org, which is likely to amplify the impact of ICANN's decision on PIR's proposal.

Our findings should also be interpreted in the context of the current situation with respect to DNSSEC at the root of the DNS. If the root zone were signed, it would not be necessary for PIR themselves to distribute and support a trust anchor for the .org zone. Many of the stability issues analyzed in this report would either not exist at all, or would be much more tractable, if the root were already signed. However, the review team concludes that the unsigned root is not, on its own, a sufficient reason to delay or object to PIR's plans.

Our technical evaluation of this proposed registry service with respect to the likelihood and materiality of effects on security and stability concludes that it does create a reasonable risk of a meaningful adverse effect on security and stability, which can be effectively mitigated by policies, decisions, and actions to which PIR either has expressly committed in its proposal or could reasonably be required to commit. The technical issues that we have identified and investigated include (a) those that are inherent in DNSSEC as a new technology; (b) those that arise from the way in which PIR proposes to implement DNSSEC in .org; and (c) those that PIR has not anticipated in its proposal. This report presents a detailed description of these technical issues, and the assumptions, information, and reasoning upon which our evaluation is based.

The principal findings that lead us to this conclusion may be summarized as follows; each is described in detail in Section 3 of this report:

- PIR plans to make the entire .org zone go bogus if there is a compromise of the .org key signing key. The impact on stability would be significantly lower if PIR made different choices for how to create and distribute their trust anchors.
- A new security risk for domains in .org using DNSSEC is associated with a scenario in which (a) a domain publishes its signing key(s), (b) one or more of those keys are later compromised, and (c) the domain holder cannot get its registrar to publish a new key.

- Introducing a major new technology such as DNSSEC in .org raises stability issues regardless of the way in which the deployment is managed.
- PIR plans to require all DNSSEC-enabled resolvers to load a new PIR trust anchor every year. Users that rely on resolvers that fail to load this trust anchor properly every year will see the entire .org zone go bogus. The impact on stability would be significantly lower if PIR made different choices for how to create and distribute their trust anchors.
- PIR proposes to use the NSEC3 method of preventing zone enumeration, as described in RFC 5155. No significant deployment of NSEC3 has occurred yet, so no empirical data were available to inform the review team's review. However, the review team's analytical evaluation suggests that PIR's choice of the NSEC3 protocol does not represent a threat to security or stability.

In order to present a complete analysis of the issues facing all of the parties affected by the PIR proposal – registrants of .org domain names, users of the DNS who look up names in the .org zone, registrars, users of the DNS as a whole, and PIR itself – the review team identified and analyzed many real but less critical potential stability issues in addition to those summarized above. These are included in Section 3 of this report.

3. Analysis of Security and Stability Issues

3.1 Brief Overview of DNSSEC

DNSSEC provides origin authentication and integrity assurance services for DNS data, including mechanisms for authenticated denial of existence of DNS data. One of the main purposes of DNSSEC is to give Internet users cryptographically-assured responses to their DNS queries. Those responses can be trusted only if they are signed by a directly-trusted authority, or an authority that can be trusted through a cryptographically protected chain of trust to a directly-trusted authority. PIR's proposal is to become a directly-trusted authority for the .org zone because ICANN has not signed the DNS root, and therefore cannot delegate trust for the domains in the .org zone to PIR.

A more complete overview of DNSSEC can be found in RFC 4033.

3.2 Security Issues Related to the Proposal

Section 1.3.1 of this report gives the definition of "security" defined by the ICANN GNSO. The review team finds that only part (A) of that definition is relevant to the PIR proposal: "the unauthorized disclosure, alteration, insertion or destruction of Registry Data". The use of DNSSEC by end entities on the Internet allows those entities to be assured that DNS responses that they receive have not been altered in transit or inserted by parties other than the authoritative zone. The review team notes that the use of DNSSEC also prevents that accidental alteration and insertion of Registry Data, and thus extends the GNSO's definition of "security".

Any use of DNSSEC will inherently increase the security of the DNS for clients that use DNSSEC to validate DNS responses. DNSSEC assures the authenticity of responses from a DNSSEC-enabled name server to any DNSSEC-validating client. Of course, it cannot assure the authenticity of responses to clients not using DNSSEC, or from servers not running DNSSEC. PIR's proposal to allow any domain in the .org zone to be able to authoritatively give cryptographically signed responses to DNS queries increases the security of the DNS for users who make DNS queries about those domains; it does not affect the security of the DNS for users who do not use DNSSEC. Note that "using DNSSEC" can mean either using it directly, or using it indirectly through a resolution service such as at an ISP.

The use of authentication in security always has a tradeoff with stability, regardless of where authentication is used. If either side of the authentication transaction (the party relying on authentication, or the authenticating party) has misconfigured its security system, the authentication will fail and the relying party will act as if the authenticating party is not who they say they are. With DNSSEC, a user who asks for DNS data that can be validated will get a response that, in fact, cannot be validated; the user's software will treat the response as bogus because it might have been tampered with. This lack of stability for the user in the face of misconfiguration is the tradeoff for gaining security when the system is properly configured.

A new security risk for domains in .org using DNSSEC is associated with a scenario in which (a) a domain publishes its signing key(s), (b) one or more of those keys are later compromised, and (c) the domain holder cannot get its registrar to publish a new key. In such a situation, two problems might arise. The first is that there is a risk that someone other than the maintainer of the zone is signing false resource records for the zone. In this case, the domain's security is reduced to a similar level to where it was before the domain started using DNSSEC, because an attacker who can inject malicious answers to DNS queries can again impersonate the compromised zone. The second problem is that the trust chain from the registrant through the registry to the trust anchor is broken, but that chain cannot be rebuilt without the registrant being able to publish new keys in its parent zone.

3.3 Introduction to the Stability Issues Related to the Proposal

We note that many of the stability risks listed in this report can have different types of effects on the DNS. There is currently an expectation among many Internet users that deploying DNSSEC much more widely, such as in a significant TLD such as .org, will make the DNS "more secure" and possibly "more stable". If serious stability problems arise due to the introduction of DNSSEC in .org, there will likely be at least an initial reaction in some parts of the community against DNSSEC. As a result of such criticism, the long-term deployment of DNSSEC could be impeded. The review team has not based any of its assessment of the PIR proposal on concern for this type of criticism; in fact, we doubt that PIR (or any TLD, or the root itself) could prevent all stability problems from happening and thus prevent all such criticism.

In this report, we talk about the stability effects of particular operational policies. We have read PIR's statement of its intended policies, and have drawn conclusions based on those. Of course, PIR changing any of those policies could have significant stability ramifications. In some cases, PIR did not state a particular policy. Whatever policy PIR chooses in those cases could also have significant stability ramifications. Some of PIR's decisions are particularly important; if they changed them, much of this report would change. Those important choices include (but are not limited to) the use of opt-out from RFC 5155 and their method for emergency key rollover of their KSK.

The stability issues described in this report are those for parties other than PIR. That is, the report focuses on the impact on stability for domain name registrants in .org, users of the DNS who look up names in the .org zone, registrars for .org, and users of the DNS as a whole. The review team did not consider stability issues that are purely business risks for PIR. Similarly, we have not included hypothetical stability issues that might ensue should PIR do something that would not be expected of a reasonable registry operator during its normal course of business. In order to present a complete analysis of the issues facing all of the parties affected by the PIR proposal, the review team identified and analyzed both the critical issues from the proposal as well as many real, but less critical, potential stability issues.

In order to achieve secure resolution of requests, it must be possible for the client to follow the chain of security from a trust anchor. Because ICANN has not signed the DNS root, PIR needs to deploy DNSSEC in .org with its own key as a trust anchor.

Having PIR's key as a trust anchor (as compared to having the DNS root signed and PIR publishing a DS record in the root zone) raises many different stability issues, the most important of which are described later in this section. Stated differently, if the root zone were signed, PIR's proposal could (and presumably would) be somewhat different. The part of the proposal that deals with signing domains in the .org zone would be the same. However, PIR would not need to publish its key to be used as a trust anchor, and the procedure for rolling over its KSK would be quite different because the rollover would be done through the root, not through an out-of-band procedure. The review team finds that it is very likely that there would be significantly fewer stability issues for such a proposal than there are in the current proposal. However, because PIR does not currently have that option, the review team has evaluated PIR's proposal based on the current environment.

3.4 Issues among Registrants, Registrars, and the Registry

When a registry uses DNSSEC, it publishes DS information in its zone. That DS information is created by the holder of the private part of the KSK of the child zone. The registry signs the DS information of the child zone before the registry publishes it. This creates the chain of trust between the parent and child zones.

The DS information is passed from the child zone (in the case of this proposal, a SLD under .org) to the registry (PIR) through a registrar using EPP. The use of registrars is mandated by PIR's contract with ICANN. The registrar therefore has to ensure that the DS information is coming from an authoritative source (the registrant); otherwise, there is a risk that someone is injecting false data into the DNS. This requirement is exactly the same as it is today for other information from the child zone, most notably a child zone's NS records. The stability implications of a registrar not using sufficient authentication for receiving and updating DS records from registrants are nearly identical to the implications of the same registrar not using sufficient authentication for updating NS records, namely that a zone could be hijacked by a malicious party.

The private key of the delegated (child) zone is normally managed by the DNS's technical contact or contacts, and in many cases the technical contacts are not the same entity as the holder of the domain (the registrant). Because of this, the registrar must ensure that the technical contacts of the domain are doing the operational tasks on behalf of the domain holder.

There are many things that can go wrong in the communication among the parties involved when provisioning and updating DNSSEC information for registrants. This section lists the ones that the review team has found to be of most concern.

3.4.1 Requirement for Stable Storage of DS Information

The DS records that are submitted by the registrant must be stored in a way that minimizes the risk that a backup has to be restored. The DS record creates a single link between the parent and child zones. This can be compared to NS records that have a level of redundancy because they each represent a different nameserver. The registrant sends its DS record through the registrar to the registry. A failure in the registrar before the domain's DS record

is sent to the registry can lose the DS record. A failure in the registry before the registry has signed and published the domain's DS record can lose the DS record.

In either case, the loss would have a significant stability impact on the registrant, similar to a registrar or registry losing the information for all of a registrant's NS records. Also, because a domain's DS information could be updated much more often than its NS records, there is a higher risk that restoration from a backup will create problems than when restoring NS data from a backup. PIR's registrars can reduce the impact on stability by reducing the chance that DS records will get lost between the registrant and the registry (although it is not clear that PIR can mandate this for its registrars). PIR can reduce the impact on stability by reducing the chance that DS records can get lost before they are signed and published in the .org zone.

3.4.2 Policy for Invalidating Existing DS Records when Data Changes

Many people in the security community believe that private keys should stay private and not be transferred between parties, even when ownership of the resource associated with the public part of the key pair changes. Others disagree, believing that transferring private keys is better than forcing a rollover of public keys when the ownership changes. There are many strong proponents for both opinions.

Given this disagreement, a registry should have a policy for whether or not the DS information will be automatically invalidated if there is transfer of a domain, or if there is a change of domain holder. It is important that this policy be known by the registrars so that they can in turn make this information available to the registrants. Without such a known policy, a domain owner could be surprised by the removal of its DS record. PIR has provided such a policy in their responses to the review team: they do not automatically invalidate a domain's keys.

In addition, each registrar that accepts DS information and passes it to the registry should have a policy for whether or not the DS information will be automatically invalidated if there is transfer of a domain, or if there is a change of domain holder. The review team is not aware of any such requirement on registrars. Answer T6 in Appendix A.2 says that PIR leaves this decision with its registrars.

3.4.3 Procedure for Emergency Key Rollover for a Child Zone

The signing and publication of the parent zone (in this case, .org) should cause no unnecessary delay between provisioning and publication of DS records created from key material from child zones. If there is a delay, the registry needs to have a special mechanism for emergency key rollover of data in the child zone. PIR has provided such a policy in their responses to the review team, namely that emergency key rollovers are treated the same as normal key rollovers (see answer P7 in Appendix A.2).

3.4.5 Impact of Too Few Registrars Willing to Handle DNSSEC

In order to publish and update their DS keys in the .org zone, registrants need to go through their registrar. From PIR's proposal, it is clear that only a subset (possibly a very small subset) of registrars plan on supporting DNSSEC records.

If a registrant wants to publish its DS record, and the registrant's registrar does not support DNSSEC records, the registrant needs to change registrars. This should be a seamless task, but history has shown that it is not always painless. Thus, some registrants who want to use DNSSEC will have to balance the stability of staying with their current registrar against the advantages of using DNSSEC. The impact on stability for registrants wanting to start using DNSSEC would be lower if most or all registrars support DNSSEC records.

If a registrant is using DNSSEC and its registrar stops supporting DNSSEC records, the registrant will have to move to a new registrar. There could be a great deal of impact on stability for the registrant if there are only a small number of registrars supporting DNSSEC. For example, the registrant might be forced to change to a registrar that has a noticeably worse record of care and/or customer service and/or a much higher price for the services. The impact on stability for registrants wanting to continue to use DNSSEC would be lower if most or all registrars supported DNSSEC records.

It is in the interest of PIR to have as many of its registrars supporting DNSSEC records as possible. PIR can reduce the impact on stability by helping registrars to support handling DNSSEC records; PIR can do this both technically and with additional education.

3.4.6 Registrar Failure to Publish New Keys

There is a significant stability risk for domains that publish their signing keys, then try to update their keys for normal key rollover, but cannot get their registrar to publish their new keys. In such a situation, the domain becomes bogus. This situation is similar to an unsigned domain having its nameservers go away but not being able to update its NS records because of problems with its registrar. There is nothing that PIR can do about this stability concern other than to emphasize to the registrars how important it is for the registrar's business to handle the DNSSEC information correctly.

3.5 Issues with Stability Due to Signing and Distributing DNSSEC Data

3.5.1 Normal Rollover of ZSK and KSK Keys in the .org Zone

When a new ZSK is introduced and used for signing the DS from the child zones, the new ZSK must be introduced with a timing overlap of the old ZSK to permit the execution of a pre-publishing procedure, as described in RFC 4641 (an informational RFC). Both keys are used to sign the DS during the time interval when cached signatures and DS RRs might exist on the Internet. PIR has said that it will change ZSKs every three months, with multiple ZSKs generated at one time (see answer P4 in Appendix A.2).

PIR has said that it will change KSKs once a year, with new keys generated and publicized three months in advance (see answer P4 in Appendix A.2). Every DNSSEC resolver on the Internet that is using the PIR KSKs as a trust anchor must add the new KSK before the old KSK is removed from the zone; otherwise, the zone will go bogus for those resolvers. PIR has said that they will use methods such as posting the new KSKs on their web site and using a mailing list to announce the availability of new KSK.

There is a very real stability concern that some DNSSEC resolvers will fail to get the new KSK before the old KSK expires; for example, the administrators of those resolvers could simply forget to check for new KSK trust anchors. There is nothing PIR can do to prevent this other than making even more aggressive announcements of the availability of their new KSK.

The review team finds that there are different stability considerations for different lengths of time for the scheduled rollover of a trust anchor KSK. The are at least five different scenarios with different stability considerations.

Short – A typical short rollover period would be one year. This is the recommendation in RFC 4641. The negative stability impact is that DNS administrators all over the Internet need to update their copy of the trust anchor every year in order to avoid having the .org zone go bogus for their users. PIR has chosen this option, as have other zones such as .se and .br.

Long – A longer rollover period, such as three years, might be chosen in order to reduce the number of times that DNS administrators would need to manually roll over the trust anchor key. The stability impact of this choice is both better and worse than for the "short" choice. This scenario would lead to better stability because it allows for tools to be developed that will remind administrators to roll over keys when they are needed; such tools do not exist now. It would also lead to better stability because it increases the chances that there will be many trust anchors for other zones that must be maintained, increasing the chance that administrators will get in the habit of scheduling rollovers. On the other hand, it could lead to worse stability because it lengthens the amount of time an administrator needs to remember to watch for rollovers. It also makes it more likely that IT staff will change, and the new staff might not be trained in the importance of the rollover.

Long enough for the root to become signed – The rollover period might be selected in order to be long enough that a rollover would likely never need to happen because the DNS root will be signed before the rollover is needed. This scenario adds the large stability gain of making a manual trust anchor rollover completely unneeded because, after the root is signed, it should be possible to perform all rollover automatically.

Two keys with mixed periods – One key, which would be used by the registry for most signing, would have a short rollover period. The second key would have a very long rollover period (possibly decades), but would not be used; it would just be published as a trust anchor stand-by. The second key would be kept offline in order to decrease the chance that it could be compromised through some online attack. This scenario increases the stability of either the "short" or "long" scenarios because it essentially makes rollovers automatic as long as the second (long) key is never rolled over.

RFC 5011 – This is the new IETF standard method for handling trust anchor rollovers. It uses two or more keys with special flags set in the keys. There are no widely-used implementations of this, so at the present time it is essentially like having multiple keys with short or long rollover times.

3.5.2 Emergency Rollover of ZSK and KSK Keys in the .org Zone

If any of the ZSK or KSK keys for a registry becomes compromised, the procedure to retire this key and related activities (such as re-signing the registry's new keys) should be started as soon as possible. A long delay would allow the party that has access to a compromised key to forge zone data and make it look like it came from PIR. If that data is injected into the DNS (through man-in-the-middle attacks or timing attacks, for example), someone requesting a secure response from .org could be fooled into believing the forged response. The most important property of the system during this event is the maintenance of the chain of trust. PIR has provided its policy for this situation in their responses to the review team (see answer P5 in Appendix A.2).

PIR being its own trust anchor presents special problems in case of the need for an emergency KSK rollover. It is impossible to evaluate with any confidence the plan PIR has for emergency KSK rollover, both because PIR's plan is not complete and because there is no real operational experience in the DNSSEC community with a similar deployment. However, at least one of PIR's plans could have a large negative impact on the stability of the DNS for systems that are running DNSSEC.

There are many alternatives for trust anchor rollover. Two are described in PIR's response to questions from the review team. Another is described in RFC 5011. Others were considered in the IETF during the discussion that led to the adoption of RFC 5011 as a standard. The review team notes that there is little operational experience with RFC 5011, although it appears that RFC 5011 has a lower impact on stability than at least one of the plans that PIR has proposed.

The outline of the plan in PIR's proposal and their response to questions from the review team suggest that one alternative under consideration for their emergency KSK rollover plan will remove all DNSKEY records from the zone. This means that resolvers that have a trust anchor configured for .org will treat the zone as bogus. This will probably mean that, to end users of the validating resolvers, the zone will stop working, resulting in error messages such as "server failure". It would be very bad for the stability of the .org zone if it were completely broken to some users. Note that this catastrophic failure will happen for all lookups by validating resolvers on all domain names in .org, not just for domain names that are signed.

3.5.3 Signing the .org Zone and Failure of Zone Generation

The actual signing of zone data happens after the data is accepted into the repository, but before the data is published. According to PIR, there are two possible approaches to the signing under consideration (see answer T3 in Appendix A.2):

- Make a modification to existing code to use a system module that prepares the signed data at the time the rest of the zone data is being prepared.
- Introduce an additional component to sign the data after the data is prepared, on the way through to zone data publication.

It is difficult to evaluate the stability effects of the approach to be implemented, because it is not clear exactly what the approach will be. PIR lists two competing architectures for their

zone signing setup in their response to the review team (see answer T3 of Appendix A.2). The review team notes with concern the fact that the details of implementation were not settled before PIR asked ICANN to review its proposal. Each of the alternatives represents a trade-off, and each may present impacts on stability particular to that alternative. Given the lack of real-world operational experience with signing and constantly re-signing large zones, the review team could not prepare a definitive analysis of the stability implications of each of the architectures, or of other competing architectures.

Because the zone signing step happens between gathering the data that should be in the zone and publishing the zone, it is possible that the signing step alone will fail. Four failure modes can be described:

- *Complete failure with publication*. A valid zone is not generated and an empty zone is published.
- *Complete failure without publication*. A valid zone is not generated but the error is discovered, leading to a failure to publish DNS changes at all, leaving the old zone data in place.
- *Partial failure*. A valid zone is generated, but some or all of the data is not correctly signed. This could result in previously-signed data ceasing to be signed, if a previous signing event did not have the same effects, or in signed data no longer being able to be verified (for example, if the NSEC or NSEC3 chain is no longer complete).
- *Corrupting failure*. The signing step introduces errors into the zone data.

Some failure modes appear to be more likely than others, and depending on the way in which the failure is expressed, some will have more serious stability effects than others. A completely empty zone generated and actually published as the result of a complete failure would be catastrophic for users and domains because all user lookups would fail. By contrast, suspension of changes to the zone during the period where a discovered complete failure was being repaired would be inconvenient, but would probably not be as serious (assuming that the repair time was suitably short).

It might be possible to introduce certain kinds of "failure" on purpose, in order to mitigate effects of deployment. In particular, for insecure zone data that has changed, it might be desirable to continue to publish the insecure data even though the signing mechanism is not working correctly for secure zone data. This would represent a "partial failure" in the above taxonomy of failure modes. PIR has not indicated whether this sort of action is one they would be willing to contemplate, or whether their implementation is capable of operating this way.

It is worth noting that any failure that results in a published zone may cause secured delegations to become bogus. For users with properly-working DNSSEC clients, the target zone will become unavailable for those users on the Internet who are validating DNS entries.

PIR did not describe any procedures for checking whether or not each signing operation completed successfully and, if not, what level of failure had occurred. The impact on stability would be lower if such checking was part of the signing process that happens before new zone data is published.

3.5.4 Signing Intervals of the DS

When a DS is added, or when an existing DS is updated or removed, the DS itself and adjacent NSEC records have to be updated and signed by the registry. The registry's signature has a specific lifetime, and it is important that the registry is re-signing its zone with an interval that assures that there is no risk of publishing signatures that are not valid. This includes ensuring that the signature interval and the TTL of the DS are chosen such that the records are signed before the signature expires by at least the length of the major TTL.

RFC 4641 (an informational RFC) gives detailed information on signing intervals, and their relationship with TTL for the various records. PIR has not stated whether or not it will follow all of the recommendations in RFC 4641.

3.5.5 Signature Maintenance May Be Neglected by Registrants

A DNS signature has a validity period, and a new signature needs to be created before the old signature expires. This means that registrants (or their DNS operators) will need to perform more maintenance on the DNS than they have been used to doing. Also, the recommended lifetime of a KSK is one year. Because the DS in the .org registry is most likely to be derived from the KSK of a .org domain, domain registrants or their registrars will have to alter the registry DNS data more often than they may have been used to doing in the past. It is quite likely that some (maybe even many) registrants and DNS operators will fail to perform the maintenance diligently, and as a result zones that can be validated at one time will eventually become bogus.

There is nothing that PIR can do to correct the problem of domains in the .org zone not being diligent with their zone RRSIG lifetimes, but the results may be surprising for both registrants and users. Even if PIR's educational activities about DNSSEC cover this issue in depth, the mistakes are likely to happen often.

3.5.6 Key Disclosure Due to Weaknesses in the Signing System

PIR's response to the review team says that the private signing keys are never exposed because they are always either stored inside an HSM or else stored only in an encrypted form (see answer P1 in Appendix A.2). There could be an important effect on security and stability if there is an implementation problem with the cryptographic portion of the HSM or encryption on disk, or if there is a disastrous failure of the cryptographic algorithms (which would be a serious issue for everyone, not just PIR). Frequent key rollovers reduce the risk of the need for key recovery from the encrypted key.

3.5.7 Zone Signing May Be Impractical

It is possible that the computational overhead of signing the zone in real time will be significantly higher than anticipated, or that the signing will be susceptible to denial of service due to load. Such a scenario could occur if, for example, DNSSEC rapidly becomes popular for domains in the .org zone. This possibility is especially worrisome for cases such as emergency key rollover (where a complete re-signing is necessary and time is of the

essence). Such a failure could lead to any of the scenarios listed in section 3.5.3 of this report.

The review team notes that, if signing the .org zone adds a delay to publishing all zone data, there is a risk that the time for publication will be longer than the delay in PIR's contractual commitment with ICANN. In such a case, this delay will be felt by every domain in .org, not just those choosing to sign their domain data. Some current users of .org domains may be depending on the contractual time to publication of .org zone data.

3.6 Issues with Operational Impacts

3.6.1 Transition Plan for Starting and Stopping DNSSEC

Ideally, of course, DNSSEC would only need to be turned on once and never turned off. However, PIR has noted situations where DNSSEC might need to be turned off; in such a situation, PIR might later turn DNSSEC on again.

Turning DNSSEC off and on for the .org zone in the current environment where the DNS root is not signed is quite different than it is expected to be in the future when the root is signed. In the current environment, PIR needs to distribute its trust anchor out of band each time it turns DNSSEC on. If PIR turns off DNSSEC, PIR might want to encourage resolvers to remove the PIR trust anchor in order to reduce the operational burden of sending and receiving DNSSEC requests.

Much of the existing infrastructure for the .org zone needs to be changed before DNSSEC can be started. For example:

- EPP needs to be upgraded, and database elements need to be added
- Cryptographic signing devices need to be procured and tested
- The transfer of zones from the distribution master to the various authoritative sites needs to be refactored and tested
- DNS server software on each authoritative server needs to be verified (and possibly upgraded) to handle DNSSEC
- The authoritative server constellation of .org needs to have additional monitoring to watch for issues related to DNSSEC

These infrastructure elements will need to be reconfigured each time DNSSEC is started and stopped in the .org zone. PIR's plan for adding these elements to the .org zone infrastructure was given in its responses to the review team (many answers in Appendix A.2).

PIR's response to the review team lists a small number of business reasons why they might need to turn off DNSSEC, such as fewer than the minimum number of registrars supporting DNSSEC provisioning (answer P10 in Appendix A.2).

The review team concludes that there are many more possible contingencies that could cause PIR to want to turn off DNSSEC, and many possible contingencies that could cause PIR to

want to turn DNSSEC on again after shutting it off. It is impossible to assess the stability concerns of all of these contingencies without a full list of them.

Alternatives for PIR publicizing a shutoff of DNSSEC include:

- PIR can wait until there is a need to turn off DNSSEC (if that ever comes to pass) before devising a plan for publicizing the shutoff
- PIR can form a plan in advance of needing to turn off DNSSEC. Such a plan could include different announcement mechanisms such as mailing lists, pre-established web pages, cryptographic authentication of announcements, communication with and/or through ICANN, and so on.

If PIR decides to shut off DNSSEC, there are two scenarios for how they might do it. Each scenario has different stability implications.

- PIR could simply stop signing the .org zone. This is the easiest for PIR, but it has the very serious stability issue of making every domain in the .org zone bogus for any resolver that still had the PIR trust anchor installed.
- PIR could continue to sign just the apex of the zone after removing all the DS and NSEC3 records. This would be more stable for two reasons. First, the zone would not go bogus for resolvers with the PIR trust anchor installed. Second, it would allow PIR to later start up DNSSEC without having to distribute a new trust anchor.

3.6.2 Reporting of DNSSEC Problems

The .org zone is one of the original TLDs. As an older TLD, there may be many legacy applications that are reliant on the existing architecture; these applications may have unknown behaviors with the advent of DNSSEC. The SiteFinder incident a few years ago illustrated that there were many applications that relied on the DNS working in a very specific way. Therefore, if this behavior changes, some infrastructurally-deficient applications may break. This is not true with new TLDs such as .nu where SiteFinder-like behavior has worked for years without widely-reported incidents. Thus, the introduction of DNSSEC in smaller ccTLDs such as .se and .br may not be a very reliable indicator of the success of adding DNSSEC in .org.

With respect to DNSSEC, a “middlebox” is any system that performs intermediate DNS operations in between a client requesting resolution of a domain name and the authoritative server for the domain name that is queried. This can be almost any type of system on the Internet, including small office and home routers that do recursive DNS, the caching servers run by large ISPs, and many types of systems of varying size. Given that it is not clear how DNSSEC will work with these middleboxes, it would be a very good idea for PIR to create a system in which people in the DNS operations community can report DNSSEC-related issues that are occurring within the Internet. This will allow middlebox vendors to fix reported issues quickly and in an open manner. Such a reporting system has the added benefit of allowing PIR management to measure the success of DNSSEC within the community. PIR has said that they would have a reporting system (answer O3 in Appendix A.2).

3.6.3 Multiple Operators for Nameservers

PIR has historically pursued a policy of having multiple operators of its nameservers. This policy of operator diversity presents some additional stability challenges in the context of DNSSEC. It also offers some benefits.

The first stability concern is the simple problem of server convergence because of the larger amounts of data to be transferred between servers due to the presence of new (and large) resource records. Another challenge is emergency reaction time. Because responses to emergencies will need to be coordinated across different organizations, the reaction time to an emergency may be longer. Different organizations also have different policies about responsiveness, and it may not be possible to ensure complete harmonization across all operators. Yet another challenge is the potential for different technology employed by different operators to behave differently; this is more problematic in the case of a protocol like NSEC3, with which there is very little experience in the general DNS community.

It is nevertheless worth observing that operator diversity adds some additional resilience to the zone operation. The information provided by PIR indicates that zone data generation and signing will happen in a central system, so operator diversity does not protect the .org zone from failures during the signing procedure. It does, on the other hand, protect the zone from failures attributable to a single operator's procedures. Because different operators are likely to have different procedures (even if the differences are slight), this additional protection may be a good trade-off against the challenges noted above. Similarly, to the extent that different operators may use different technologies, multiple operators may provide protection against some failure mode of a single technology.

3.6.4 Greater Demands Placed on the Servers and Infrastructure

DNSSEC adds a number of greater demands on the authoritative servers. The traffic could be so much greater that the zone's nameservers could be overwhelmed.

DNSSEC will require additional memory and storage. These demands may be as high as six times the existing space. This is not a showstopper in today's environment because both disk and memory are relatively cheap. The zone administrator needs to keep this potential increase in the size of the zone in mind when planning the amount of headroom needed for each computer used for name service.

DNSSEC requires more CPU for serving the same number of domains. This is particularly true if the zone must process a large number of queries for which the name does not exist, or if opt-out is deployed (PIR has said that they will use opt-out). In both of those cases, there needs to be a search for the appropriate NSEC RR when a request for the domain is handled. The search-based algorithm is not as efficient as the hash-based algorithms that are typically used in looking up non-DNSSEC records. Consequently, DNSSEC responses require additional tuning as CPU utilization increases. DNSSEC also creates a new way for miscreants to perform a denial-of-service attack because they would have a way of creating queries that cause greater drain on the CPU of the nameserver.

With NSEC3, the number of hash iterations needs to be chosen carefully, because a large number of iterations can impose much larger CPU demands on authoritative servers. In responding to queries for nonexistent names, those servers hash the queried name according to the hash iteration parameter before they can find the covering NSEC3 record. The trade-off being made is between an operator wanting a low number of iterations to avoid CPU-based denial-of-service attacks and a higher number of iterations increasing resistance to dictionary attacks.

If a load balancer is used in zones with DNSSEC, the larger responses can cause the load balancer to be less efficient. Further, the load balancers may be forced to deal with UDP fragments, and this would cause the load balancer to need to keep more state.

If there are many changes to secure delegations, there will be a substantial increase in the amount of bandwidth needed for updates to be propagated to authoritative nameservers. When some of the authoritative nameservers have very limited connectivity back to the distribution masters for the secure zones, this problem is particularly important. In such a case, there is a possibility that the remote nameservers will be out of date.

3.6.5 Denial-of-Service (DOS) Potential

DNSSEC responses are necessarily larger than non-DNSSEC responses, so a DNSSEC-aware nameserver may be requested to send much larger responses than a DNSSEC-unaware nameserver. An attacker can create bogus DNSSEC queries that may saturate the outbound links from the authoritative nameserver and/or saturate the incoming bandwidth at a victim site. Currently, these attacks happen only occasionally on gTLD nameservers; they happen much more frequently on nameservers that are compromised at third level domains or deeper.

The review team finds that the issue of attempts to saturate its outbound links can be dealt with following PIR's normal business procedures. The team does not find that there is anything significant that PIR can do to prevent attacks that saturate the incoming bandwidth of a victim site.

3.6.6 WHOIS Information

WHOIS is the standard interface for verification of current data at a registry and is used as an alternate path to verify the correctness of DNS published data. Without this alternate path, there is no way for a third party to verify that the information being provided in DNS responses matches what was put in the zone during registration and update.

PIR's response to the review team says that they will show in the WHOIS data the signing status (signed or not signed), the time the record was created, and the maximum signature lifetime. They do not propose to show the key tag, signing algorithm, digest type, or digest of the DS record. (See answer P12 in Appendix A.2.) Without the additional information, WHOIS will be less useful as an alternate path for registrants to validate the information stored by their registrars in the registry.

3.6.7 Getting Validators to Remove the PIR Trust Anchor after the DNS Root Is Signed

During its investigation, the review team discovered that the behavior of two widely-available DNSSEC validating resolvers (one of which is also widely-deployed) does not match the review team's interpretation of RFC 4035. The validating resolvers' behavior results in incorrect validation results when the resolver has both a trust anchor for one zone and an expired trust anchor for a zone that is subordinate to the first zone. When the DNS root is signed, some operators of DNS resolvers may install the trust anchors for the root but leave PIR's trust anchor for .org in place. The next time that PIR does a key rollover in the root zone, the problem will immediately appear for anyone using such a resolver: they will treat signed responses from the .org zone as bogus even if PIR has done everything correctly.

A similar problem will appear for those domains in .org that have published trust anchors that are installed in validating resolvers exhibiting this behavior. If ICANN agrees to PIR's proposal to allow PIR to distribute the trust anchor for .org, these domains will have the same problem as described above at the time that those domain holders roll over their keys.

To avoid this serious impact on the stability of the DNS, all organizations running DNSSEC resolvers will need to do one of the following:

- update their software to software that treats both the domain authenticated by the parent zone and the rolled-over trust anchor as valid
- when adding a new trust anchor to a broken resolver, remove all trust anchors for zones subordinate to the new trust anchor

PIR could mitigate these impacts by incorporating this information into their communication and education campaigns both when they do key rollovers before the root zone is signed and when they add a DS to the root zone for the first time.

Separately, the review team has contacted the developers of the implementations in question to alert them of the problems that were found.

4. References

The members of the RSTEP review team that carried out the Security and Stability implications analysis reviewed many resources that helped in their analysis of the PIR proposal. These resources include the proposal from PIR in addition to a great deal of material about DNSSEC operations and deployment.

The PIR proposal and related communications are listed at (http://icann.org/registries/rsep/) under "Proposal 2008004". That material includes:

- The original proposal from PIR (http://icann.org/registries/rsep/pir-request-03apr08.pdf)
- The SSAC endorsement of the proposal (http://icann.org/committees/security/sac029.pdf)
- ICANN's request that an RSTEP review team be formed (http://icann.org/registries/rsep/rstep-letter-21apr08.pdf)
- ICANN's request for comments from the public (http://icann.org/announcements/announcement-23apr08.htm)

Because this was a proposal to modify PIR's agreement with ICANN to operate the registry for the .org zone, the review team also reviewed the contract between ICANN and PIR (http://www.icann.org/tlds/agreements/org/).

The members of the review team were already familiar with the RFCs that are referenced in the proposal: RFC 4033, 4034, 4035, 4641, 5011, and 5155 (http://www.rfc-editor.org/). Most of them were active in many of the DNSSEC protocol and operations discussions over the past decade, and used that perspective to help frame their views of the security and stability concerns with the PIR proposal.

The review team reviewed all of the responses to the request for comments (http://forum.icann.org/lists/pir-dnssec-proposal/).

Appendix A. Additional Material Supplied by PIR

During the course of the review team's deliberations, the review team asked PIR for additional information concerning its proposal. This appendix shows a condensed version of the requests that the review team made and a condensed version of PIR's responses.

A.1 Requests from the RSTEP Review Team

Please describe your policies on the following topics. If you have formal policy documents, please supply them; otherwise, please list whatever informal information you have on the PIR policies for the topics listed.

P1 - KSK key generation and storage

P2 - ZSK key generation and storage

P3 - Zone signing - signature generation, RRSIG validity period, and resigning strategies

P4 - Normal key rollover

P5 - Emergency key rollover

P6 - Normal flow of data from child zone for creation of DS records

P7 - Emergency flow of data from child zone for creation of DS records

P8 - Distribution of signed zone to authoritative servers

P9 - DNSSEC procedures for change of registry if the .org TLD itself is changed to another organization

P10 - Turning off DNSSEC if there are failures (and what thresholds would trigger such an action)

P11 - Use of the secDNS:maxSigLife element in DS creation through EPP: is it required for registration; will it be honored for expiration; etc.

P12 - Listing DNSSEC data from whois requests (show an example)

P13 - Domain owners with keys wanting to move to a registrar that does not support 4310

P14 - Specifying the RFC 5155 opt-out policy

P15 - Salt size and hash iterations policy for RFC 5155

P16 - Changing PIR's implementation of RFC 5155 based on different resolver interactions

P17 - The minimum number of registrars required to have passed OT&E before any registrar will be permitted to put DS records in the registry

P18 - The minimum number of registrars required to have passed OT&E that would cause PIR to stop offering DNSSEC resolution

Please supply information on any operational planning that PIR has done with respect to the DNSSEC addition. In specific, we would like to hear about:

O1 - Testing to show that the DNS server components can handle the additional overhead of DNSSEC resolution

O2 - Testing to show how the increased size of the zone will affect synchronization across the DNS server components

O3 - Ways to report on failure modes such as clock drift on validators, DNSSEC-challenged CPE equipment, and so on

O4 - Interoperability testing with RFC 5155 resolvers

O5 - When the KSK compromise plan will be complete

O6 - Whether the ability to add DS records to the registry be disabled for registrars who have not passed OT&E

Please supply any information that PIR has on the following topics:

T1 - List all the DNSSEC operations that are associated with a domain record

T2 - Which SHOULDs in RFC 4033, 4034, 4035, 4310, and 5155 does PIR *not* intend to do, and why

T3 - Architecture of the DNS provisioning system (DNS Distributor) with the changes for DNSSEC highlighted; maybe this could be fulfilled with the document listed in Section 1.3 of the DNS Distributor test plan

T4 - Details of the DNS server(s) that will be used in support of the deployment of RFC 5155 (given that there is a dearth of publicly- deployed software for this)

T5 - Details of the OT&E testing that PIR will perform with its registrars

T6 - There are different views about whether or not a change in the holder of a domain, the tech contact for a domain, or the registrar of a domain should cause the keys published in the zone to change; please comment on how PIR views this

T7 - List any DNSSEC operation that is automatically triggered by changing the registered name holder of a domain

T8 - List any DNSSEC operation that is automatically triggered by changing the technical contact of a domain

T9 - List any DNSSEC operation that is automatically triggered by changing the registrar of a domain

A.2 Responses from PIR

P1. KSK key generation and storage

Key generation will be performed using a FIPS-140-2 compliant hardware security module (HSM).

Evaluation of the specific HSM device to be used is under way. The key storage implementation will depend on the general category of HSM selected. There are two general approaches to key storage. Either the HSM provides no persistent storage and an encrypted version of the key is stored external to the HSM in the solution layer or the HSM provides key storage and the keys are used only by reference. In either case, a non-encrypted key will never be available external to the HSM.

P2. ZSK key generation and storage

The comments made in section P1 apply here, as well.

P3. Zone signing - signature generation, RRSIG validity period, and resigning strategies

Signatures will be generated entirely by the HSM specified in section P1.

The system is highly configurable and it is expected that tuning of the RRSIG validity period will be required. It is expected that the initial RRSIG lifetime will be ten (10) days.

Due to the high rate of change, signing will be performed and published continuously as part of the solution that generates zone data changes based on administrative updates and EPP transactions.

Introducing new keys and/or expiring old keys can be configured to be performed automatically and may also be triggered at an explicit point in time by an administrator.

Resigning the entire zone (with current, additional, or different keys) is supported as an administrator triggered operation.

P4. Normal key rollover

Normal ZSK rollover will occur on a regular basis (currently planned for once a month). PIR plans to have multiple ZSKs generated at any given time. When new ZSKs are generated, the oldest set of ZSKs will no longer be used to sign the zone, and will be dropped from the set.

KSK rollover will occur once per year. New keys will be generated 3 months in advance. ZSKs will then be generated from these KSKs as well.

As soon as these are generated, the public keys will be posted on both PIR and Afilias websites. Additionally, PIR will implement an email service that is open to the public. This service will inform the list anytime there is a KSK change. PIR will also send in new DS information to IANA once their repository is operational, or the root is signed.

P5. Emergency key rollover

If a ZSK is compromised, PIR will generate a new ZSK, and stop signing the zone with the 'bad' key immediately. This will follow the same basic principles as a normal key rollover – it simply will be unscheduled.

If multiple ZSKs are compromised, PIR will either perform this same function for the affected ZSKs.

If all ZSKs have been compromised, or a KSK has been compromised, then PIR currently plans to do the following:

1. Render the zone unsigned

2. Determine the source of the compromise and rectify it.

3. Regenerate new KSK and ZSK sets

4. Publish the new public data as above

5. Sign the .ORG zone.

This however, may not be the most optimal way of eliminating the possibility of someone injecting incorrect data while the zone is compromised. PIR is working with the DNSSEC deployment community to determine if this can be done without “un-signing” the zone.

P6. Normal flow of data from child zone for creation of DS records

DS records are introduced to the registry, and thus the zone, via the EPP protocol per RFC 4310, Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol and are reflected automatically in the zone as for other EPP initiated changes.

P7. Emergency flow of data from child zone for creation of DS records

Emergency update of DS records is as described in P6, Normal flow of data from child zone for creation of DS records.

P8. Distribution of signed zone to authoritative servers

Signed zones will be distributed in precisely the same manner as unsigned zones, that is using IXFR [RFC 1995], NOTIFY [RFC 1996] and TSIG [RFC 2845]. The DNS interface to the registry (the "distributor") implements these protocols in order to propagate zone changes out to distribution masters in each nameserver cluster.

P9. DNSSEC procedures for change of registry if the .org TLD itself is changed to another organization

Nearly all of the burden of transitioning the .ORG TLD to another organization would fall on the new registry provider. Since the KSK and ZSK information will not be escrowed, the new provider would need to generate keysets for both the KSK and ZSKs. PIR would then add these keys, without signing the zone with them, prior to cut-over. At cut-over, the new organization would need to invoke a KSK key rollover per their procedures.

All DS data sent by the registrars would be transitioned over to the new organization, as well as the zone data.

P10. Turning off DNSSEC if there are failures (and what thresholds would trigger such an action)

One example of when PIR might decide to turn off DNSSEC is outlined in P5. PIR would also consider turning off DNSSEC in the event that providing DNSSEC service threatened the stability of the ORG zone as a whole, or the operational aspects of its maintenance and publication.

P11. Use of the secDNS:maxSigLife element in DS creation through EPP: is it required for registration; will it be honored for expiration; etc.

The system policy regarding the interpretation of maxSigLife is configurable with a minimum, maximum, and default value in the registry. These values will very likely need to be tuned in the production system.

maxSigLife is optional.

The initial values are (forcing a non-configurable 10 day maxSigLife):

• Minimum = 10 days
• Maximum = 10 days
• Default = 10 days

The general system policy regarding maxSigLife is as follows:

• If a maxSigLife is not provided, the default value will be used.

• If a value is provided and is within the range [minimum life, maximum life], then the value specified will be used.

• If the value is outside of the range [minimum life, maximum life], then the default value will be used.

P12. Listing DNSSEC data from whois requests (show an example)

The following are fields that will be appended to the WHOIS output for a domain name with DS records:

• DNSSEC - To denote if the domain name is signed (output can be Signed or Unsigned).

• DS Created - The timestamp that the record was created in UTC

• DS Maximum Signature Life - Maximum signature life associated with the DS record

Example:

DNSSEC: Signed
DS Created : 03-oct-1996 04:00:00 UTC
DS Maximum Signature Life 1: 84000 seconds

DS Created : 04-oct-1996 01:00:00 UTC
DS Maximum Signature Life 2: 1000 seconds

P13. Domain owners with keys wanting to move to a registrar that does not support 4310

Registrants with DS information in the registry will be prohibited from transferring domains to a registrar that has not implemented RFC 4310 AND has passed the DNSSEC OT&E process.

Registrants that wish to transfer their domain name to another registrar must either choose a registrar that meets these requirements, or remove the DS information from their domain name.

P14. Specifying the RFC 5155 opt-out policy

RFC 5155 opt-out will be used for all insecure delegations.

P15. Salt size and hash iterations policy for RFC 5155

Salt and hash iteration policy may need to be tuned based on testing.

The initially selected salt size will be 8 octets.

The initially selected number of iterations is 10.

Resigning with a new randomly selected salt will be triggered in the event of a hash collision.

P16. Changing PIR's implementation of RFC 5155 based on different resolver interactions

Interoperability testing between BIND9 and unbound resolvers and BIND9 and NSD authority-only severs is planned. This testing is being carried out in conjunction with vendors. If interoperability is best served by DNSSEC policy changes, those changes will be made.

P17. The minimum number of registrars required to have passed OT&E before any registrar will be permitted to put DS records in the registry

There should be at least two (2) registrars required to have passed OT&E before any registrar will be permitted to put DS records in the registry. This is due to the contingency in the event of bulk transfer.

P18. The minimum number of registrars required to have passed OT&E that would cause PIR to stop offering DNSSEC resolution

As long as at least two registrars have passed OT&E, we can continue to offer DNSSEC resolution.

P17 and P18. Additional information

PIR will require two registrars upon initial deployment. Once registrars are allowed in, then that registrar will be able to execute DNSSEC transactions with the registry - even if the number of registrars falls to one. This ensures that our registrars can continue to conduct business without being impacted by a competitor.

Regarding transfers, if the number of registrars falls to one, then any registrant that wants to transfer their domain must either remove their DS information, or wait until another registrar becomes available that uses DNSSEC.

O1. Testing to show that the DNS server components can handle the additional overhead of DNSSEC resolution

All individual nameserver hosts within clusters have been equipped with sufficient RAM to accommodate a four-fold increase in the size of the ORG zone. Since ORG will be signed with NSEC3 and opt-in, the practical impact on memory footprint is expected to be well within deployed limits.

The size of the ORG zone is expected to increase as DNSSEC deployment proceeds, and regular capacity planning (including monitoring the memory footprint of in-service nameservers) will continue. Infrastructure will be augmented where appropriate.

All clusters are provisioned with sufficient individual nameservers that the additional CPU load involved in responding to DO=1 queries should be well within available processing capabilities.

Afilias maintains a "lab" nameserver cluster which is never used for production traffic, and which is equipped with an array of load generating hosts precisely to accommodate performance testing. Tests involving various mixes of DO set/unset query streams will be completed in order to confirm our expectation that existing clusters are sufficiently equipped to handle requests from validators.

O2. Testing to show how the increased size of the zone will affect synchronization across the DNS server components

The ORG zone signed with NSEC3/opt-in is expected to grow linearly in size with DNSSEC adoption. Distribution of zone changes takes place over network paths which are provisioned with 80% or more headroom, and which are independent of those paths used for query traffic. Short-term spikes in update traffic due to (e.g.) registry or registrar promotions are routinely accommodated.

Testing in the "lab" nameserver cluster will be carried out to confirm that the over-provisioning described above is sufficient to accommodate update traffic resulting from (e.g.) high DS churn and low signature expiration (with corresponding re-signing impact on update load).

O3. Ways to report on failure modes such as clock drift on validators, DNSSEC-challenged CPE equipment, and so on

Afilias maintains active involvement in forums such as OARC, NANOG, RIPE and IETF/dnsop where operational challenges such as these are routinely discussed. Failures that are raised on those venues will be noted and evaluated.

PIR will publish an e-mail address that can be used by end-users to report problems relating to a signed ORG zone.

Any substantial corrective action taken in response to such reports will be made public on Afilias and PIR web pages.

O4. Interoperability testing with RFC 5155 resolvers

As alluded to in the response to P16, interoperability testing between BIND9 and unbound validators and BIND9 and NSD authority-only servers is underway in conjunction with vendors.

O5. When the KSK compromise plan will be complete

We expect the KSK compromise plan to be finalized in Q3 of 2008.

O6. Whether the ability to add DS records to the registry be disabled for registrars who have not passed OT&E

By default, registrars do not have the ability to add DS records into the registry until they have passed OT&E.

T1. List all the DNSSEC operations that are associated with a domain record

Regarding the domain update command, the following operations are supports:

• Add DNSSEC data of a domain

• Remove DNSSEC data of domain

• Modify existing DNSSEC data of a domain

Regarding the domain info command:

• List details of all DNSSEC data associated to the domain

Regarding the domain create command:

• Add DNSSEC data associated to the domain at creation

*T2. Which SHOULDs in RFC 4033, 4034, 4035, 4310, and 5155 does PIR *not* intend to do, and why*

Note that the implementation will be based on RFC5155 (NSEC3) and therefore elements of the protocol referenced in the earlier RFC's that deal with NSEC will not be implemented at all.

RFC 4033 (DNS Security Introduction and Requirements):

> "Section 9. Name Server Considerations … the private half of each DNSSEC key pair should be kept offline" – The zone will be signed continuously in an automated fashion and so the private key is required online. The risk of this is mitigated by the use of an HSM.

RFC 4034 (Resource Records for the DNS Security Extensions):

All SHOULDs will be implemented

RFC 4035 (Protocol Modifications for the DNS Security Extensions):

"Section 2.4, Including DS RRs in a Zone … A DS RRset SHOULD be present at a delegation point when the child zone is signed." – PIR is not in control of whether the administrator of a delegated zone injects a DS record into the registry and thus the .org zone. Any DS records that are provided will be injected into the zone, however. The root zone is currently not signed and thus DS records for the org. zone will not be present in the root.

Section 2.4. Including DS RRs in a Zone … A DS RR SHOULD point to a DNSKEY RR that is present in the child's apex DNSKEY RRset, and the child's apex DNSKEY RRset SHOULD be signed by the corresponding private key" – PIR will perform no validation of the DS records that are added to the registry. Performing an online check inline during addition of the DS record is impractical. It is left to the delegated zone administrator to manage timing of introduction of DS records against actual use of the associated key.

RFC 4310 (DNS Security Extensions Mapping for the EPP):

Section 2. Object Attributes … The key data SHOULD have the Secure Entry Point (SEP) bit set as described in RFC 3757" – PIR has no control over signed sub-zones. The SEP bit will be set for the keys in the org. zone.

RFC 5155 (DNSSEC Hashed Authenticated Denial of Existence):

All SHOULDs will be implemented

T3. Architecture of the DNS provisioning system (DNS Distributor) with the changes for DNSSEC highlighted; maybe this could be fulfilled with the document listed in Section 1.3 of the DNS Distributor test plan

The current architecture for the DNS Distributor was designed to accommodate introducing DNSSEC data inline with the processing of changes to the zone that result from registry changes. We have since introduced HSM hardware into the solution.

There are two competing architectures that we are currently evaluating.

The first architecture uses the HSM to replace the DNSSEC signing code currently implemented in the DNS Distributor. This requires no architectural changes and simply replaces the Openssl signing with HSM based signing.

The second architecture places the HSM and DNSSEC management code in a system module that sits between the DNS Distributor and the production name server infrastructure. This module performs the zone signing based on zone changes and RRSIG expiry and performs all data transfer using the IXFR and AXFR standards.

T4. Details of the DNS server(s) that will be used in support of the deployment of RFC 5155 (given that there is a dearth of publicly-deployed software for this)

The signed ORG zone will be hosted by NSD 3 and BIND9 authority-only servers. Afilias is in close contact with both NLNet Labs and ISC with regard to this goal, and is well-synchronized with those vendors with respect to software readiness, testing and timelines for delivery.

Early candidate releases incorporating NSEC3 functionality are already deployed in the "lab" cluster.

T5. Details of the OT&E testing that PIR will perform with its registrars

A DNSSEC criteria document has been drafted however it's still under review.

DNSSEC OT&E testing will be a standard OT&E test for existing ORG-accredited registrars who have modified their clients for DNSSEC. Registrars will be provided with an OT&E environment to test their modified clients. Once ready, registrars will need to contact PIR Technical Support to schedule a DNSSEC OT&E test. Once successfully completed, the registrar will be flagged as DNSSEC enabled in the SRS.

The OT&E test will cover domain operations only (validating only the RFC4310):

• Creating a DNSSEC signed domain (with and without optional key data)

• Querying a DNSSEC signed domain (with and without optional key data)

• Updating a DNSSEC signed domain (adding, changing and removing DS data)

T6. There are different views about whether or not a change in the holder of a domain, the tech contact for a domain, or the registrar of a domain should cause the keys published in the zone to change; please comment on how PIR views this

For the domain contacts, it is left up to the discretion of the registrar. It is not required to submit new DS information via EPP if any or all of the contacts change, as it is assumed that the DS information relates to the owner of the domain, not the individual contacts.

Since PIR has no way of establishing if DS information was created by the registrant or the registrar, the registry should not enforce changing the DS information when a transfer occurs. The losing registrar will not be able to change the DS information once the Auth-Info code has been changed as part of the transfer process.

T7. List any DNSSEC operation that is automatically triggered by changing the registered name holder of a domain

No DNSSEC operations are automatically triggered for this case.

T8. List any DNSSEC operation that is automatically triggered by changing the technical contact of a domain

No DNSSEC operations are automatically triggered for this case.

T9. List any DNSSEC operation that is automatically triggered by changing the registrar of a domain

No DNSSEC operations are automatically triggered for this case. An additional comment here is that based on the registry policy, it is prohibited to change the registrar of a domain with DNSSEC data if the targeted registrar is not DNSSEC accredited.