Proposed Service

Name of Proposed Service

Security Extensions for the DNS – DNSSEC

Technical Description of the Proposed Service

This is a request by the Public Interest Registry (PIR) for an amendment to the .ORG registry agreement (the "Agreement").

This request is to change the function of the registry and the corresponding WHOIS and DNS systems for the .ORG gTLD to facilitate the use of DNSSEC as specified in RFCs 4033, 4034, 4035, and 5155 (NSEC3).

PIR anticipates a backwards-compatible change to our customers' EPP client. The change will include modifications to allow manipulation of the DNSSEC DS records by the registrar. PIR expects these changes to be in compliance with RFC 4310. Some registrars may modify their own software to reflect these changes.

PIR anticipates changes to the WHOIS subsystem that will reflect some of the DNSSEC data in the registry.

PIR will make the production changes in the OT&E environment in advance of the production system changes. Registrars that wish to utilize DNSSEC will be required to complete a DNSSEC OT&E test prior to use in the production environment.

PIR anticipates changes to the .ORG name servers to answer queries that request DNSSEC data for validation of the response.

PIR anticipates changes to the .ORG zone. PIR will self-sign the .ORG zone initially. Once the root zone is signed, PIR will deliver DS records for proper DNSSEC delegation in the root.

PIR anticipates no changes in rate-limiting and add storm limiting policies and practices.

PIR anticipates additional reports to be delivered to registrars that enumerates which domain names are signed, along with their expiration time stamp. Other reports may become available later. PIR anticipates no other changes to billing software and registrar invoices.

PIR does not intend to charge an additional fee for this service.

Consultation

Please describe with specificity your consultations with the community, experts and or others. What were the quantity, nature and content of the consultations?

PIR has formed the .ORG DNSSEC Deployment group, whose membership consists of several business and technical leaders in the industry, including individuals that are on the SSAC committee, the GNSO, the DNSEXT Working Group, and administrators of the .SE zone (which is already using DNSSEC).

This group has convened several times over the past 18 months. The group was originally tasked with weighing the pros and cons of DNSSEC deployment in general, to determine if this would be beneficial to the .ORG community at large. Once this was decided, the group made suggestions on policy and procedures regarding the deployment of DNSSEC.

a. If the registry is a sponsored TLD, what were the nature and content of these consultations with the sponsored TLD community?

N/A

b. Were consultations with gTLD registrars or the registrar constituency appropriate? Which registrars were consulted? What were the nature and consent of the consultation?

The results of a survey of registrars completed on March 11, 2008 are attached.

c. Were consultations with other constituency groups appropriate? Which groups were consulted? What were the nature and content of these consultations?

No other formal consultations were made.

d. Were consultations with end users appropriate? Which groups were consulted? What were the nature and content of these consultations?

No formal consultations with end users were made.

e. Who would endorse the introduction of this service? What were the nature and content of these consultations?

The endorsements of the DNSSec Deployment Working Group and the SSAC are attached.

f. Who would object the introduction of this service? What were the nature and content of these consultations?

Because DNSSEC has been accepted as the standard for securing the DNS against man-in-the-middle attacks, PIR does not believe that there would be objection to this service.

Timeline

Please describe the timeline for implementation of the proposed new registry service:

PIR plans to give immediate notification to registrars upon receipt of ICANN approval, and plans to sign the .ORG zone in the 4thquarter of 2008. Registrars will be allowed to enter DNSSEC information shortly thereafter.

Business Description

Describe how the Proposed Service will be offered:

Adding DNSSEC security will be offered by the registrars to their customers. Once registrars have the relevant information, they will be able to manipulate the DS Resource Records in the registry using EPP (as described in RFC 4310).

Once in the registry, the appropriate records will be signed on an on-going basis. This information will then be disseminated to all .ORG name servers continuously.

The Public key portions of DNSSEC will be announced to the public by PIR, and, at a minimum, will be made available on the PIR website. Name server administrators that want to use DNSSEC with .ORG query / responses will need to retrieve these keys and load them into their DNSSEC-aware name server systems.

End user applications that are DNSSEC-aware will ask queries of the DNS with a flag set for a signed response. The registry name servers will then respond with the correct response, including the signatures for the requested records. It is up to the end user to validate the signatures returned.

Describe quality assurance plan or testing of Proposed Service:

The test plans of the Proposed Services are attached.

Contractual Provisions

List the relevant contractual provisions impacted by the Proposed Service

Section 3.1(c)(i) Data Escrow of the Registry Agreement (8 December 2006) between ICANN and Public Interest Registry.

What effect, if any, will the Proposed Service have on the reporting data to ICANN?

PIR does not expect to add any additional reports to ICANN for this service.

What effect, if any, will the Proposed Service have on the WHOIS?

The WHOIS will now include data to show that the domain name is signed. It will not include any DNSSEC data that would compromise the security of the domain name, such as a private key.

What effect, if any, will the Proposed Service have on the price of a domain name registration?

PIR does not plan to charge for this service.

Contract Amendments

Please describe or provide the necessary contractual amendments for the proposed service:

Amend Section 3.1(c)(i) Data Escrow of the Registry Agreement (8 December 2006) between ICANN and Public Interest Registry to read as follows:

3.1(c)(i) Data Escrow. Registry Operator shall establish at its expense a data escrow or mirror site policy for the Registry Data compiled by Registry Operator. Registry Data, as used in this Agreement, shall mean the following: (1) data for domains sponsored by all registrars, consisting of domain name, server name for each nameserver, registrar id, updated date, creation date, expiration date, status information, and DNSSEC DS data (if Registry Operator implements DNSSEC); (2) data for nameservers sponsored by all registrars consisting of server name, each IP address, registrar id, updated date, creation date, expiration date, and status information; (3) data for registrars sponsoring registered domains and nameservers, consisting of registrar id, registrar address, registrar telephone number, registrar e-mail address, whois server, referral URL, updated date and the name, telephone number, and e-mail address of all the registrar's administrative, billing, and technical contacts; (4) domain name registrant data collected by the Registry Operator from registrars as part of or following registration of a domain name; and (5) DNSSEC resource records in the zone (if Registry Operator implements DNSSEC).

Benefits of Service

Please describe the benefits of the Proposed Service:

PIR believes that the Internet user community will be better able to conduct secure transactions on the Internet with .ORG websites, because DNSEC validates the URLs that are entered by users.

How would you define the markets in which your proposed Registry Service would compete?

This service will be available to every .ORG domain name holder.

What companies / entities provide services or products that are similar in substance or effect to your proposed registry service?

There are no similar services that can provide this service for the .ORG domain.

In view of your status as a registry operator, would the introduction of your proposed Registry Service potentially impair the ability of other companies / entities that provide similar products or services to compete?

No

Do you propose to work with a vendor or contractor to provide the proposed Registry Service? If so, what is the name of the vendor / contractor, and describe the nature of the services the vendor / contractor would provide.

PIR is working with its back end service provider, Afilias Limited.

Have you communicated with any of the entities whose products or services might be affected by the introduction of your proposed Registry Service? If so, please describe the communications.

Please see the results of the survey attached in response to the prior question re: Consultation.

Do you have any documents that address the possible side effects on competition of your proposed Registry Service? If so, please submit them with your application (ICANN will keep the documents confidential).

N / A

Security and Stability

Does the proposed service alter the storage and input of Registry Data?

Yes. As specified by RFC 4310, registrars will now have the ability to enter and manipulate additional EPP records that correspond to DNSSEC DS records.

Please explain how the proposed service will affect the throughput, response time, consistency or coherence of responses to Internet servers of end systems?

DNSSEC requires proper configuration, as well as periodic maintenance, in order to work correctly. Once properly installed and configured, the resolvers must perform the additional step of signature validation. This will cause resolution of signed Resource Records to take slightly longer. It will not impact the resolution of names that are not signed.

Have technical concerns been raised about the proposed service, and if so, how do you intend to address those concerns?

There is some concern regarding the ability of routers that have poor DNS implementations to send and receive correct DNSSEC related query/response pairs.

Research is under way within the DNS community to automate the rollover of keys for DNSSEC. PIR will announce key changes, and, at a minimum, publish the public key on the PIR website.

Other Issues

Are there any Intellectual Property considerations raised by the proposed service?

PIR is not aware of any.

Does the proposed service contain intellectual property exclusive to your gTLD registry?

No.

List Disclaimers provided to potential customers regarding the proposed service:

N/A

Any other relevant information to include with this request?

1. For more information on the deployment of DNSSEC, please see http://www.dnssec-deployment.org/, and for more information on NSEC3, please see http://www.nsec3.org/

2. Responses to additional questions:

1. What plan does PIR have to recover from .ORG KSK and ZSK private?

The following is a high-level summary of a draft plan which has not yet been subject to expert review.

PIR acknowledges the importance of having a robust procedure established for reacting to a KSK compromise.

Once the KSK compromise plan is complete and has completed satisfactory peer review, it will be made public. PIR will not publish a signed .ORG zone before a satisfactory KSK compromise plan has been published.

Draft KSK Compromise Plan Summary

1. Remove all DNSKEY, RRSIG and NSEC3 records from .ORG, rendering it insecure.
2. Repositories of trust anchors (e.g. a future signed root zone, DLV repositories) are updated using appropriate mechanisms to indicate that the .ORG delegation is insecure.
3. Execute an emergency communications plan by which the actions of steps (1) and (2) are publicised widely. The need to be able to authenticate such communications is acknowledged.
4. The attack vector by which the KSK was compromised is identified.
5. The security infrastructure is reviewed to confirm that the known attack vectors are eliminated.
6. A new KSK is generated.
7. Repositories referred to in (2) are updated with the new trust anchor.
8. .ORG is re-signed and published. The re-signing procedure will include the generation of new ZSKs, which will be signed with the new KSK.

The elapsed time between the execution of step 1 and the execution of step 6 will exceed the validity of the compromised KSK's signatures of the active ZSKs at the time of compromise.

2. The request points out that Registrars will be able to manipulate customer DS records in the registry using EPP. Can you provide additional clarity regarding Registrar control and/or ownership of DS record information?

The Registry will treat the DS data in the same manner that other DNS and WHOIS information provided by the registrar is treated. It is the responsibility of the registrar to ensure that all data sent into the registry is factual and correct.

3. What plan does PIR have to respond to Registrar failures relating to DNSSEC issues?

In the event of a failed Registrar that runs DNSSEC, the Registry will require that the Gaining Registrar be able to run DNSSEC as well. It will be the responsibility of the Gaining Registrar to determine which DS records were generated by the Registrant, which were generated by the Losing Registrar, and which were generated by third parties. The Gaining Registrar will need to submit new DS data for those domain names signed by the Losing Registrar. The Gaining Registrar should also then develop a secure method for receiving DS data from those third parties identified above (although those will not need to be re-submitted to the Registry).

In the best interest of the Registrant community as a whole, the Registry will not delete any DS, RRSIG, or other information from the Registry or the zone. Doing so would cause inconsistencies between the Gaining Registrar's data and the Registry, as well as having the potential for a large number of validly signed zones to become unusable to DNSSEC-aware resolvers.

4. What plan, if any, does PIR have to educate the public regarding DNSSEC usage on .ORG?

The following are examples of PIR plans to assist in the education of the public regarding DNSSEC:

- Public presentations to the technical community who run DNS resolvers, such as ISPs.
- Provide DNSSEC marketing/training materials to our registrars that they can present to their customers.
- Post DNSSEC informational materials on the public area of the PIR website.
- Provide workshops & surveys to the end user community through forums such as NTEN, The Webby Awards .ORG holders, and Union of International Associations.

Registrar Survey for DNSSec Deployment in .ORG

Public Interest Registry (PIR) sent this survey to contacts for all ICANN accredited .ORG registrars that were currently in ramp up or production status.

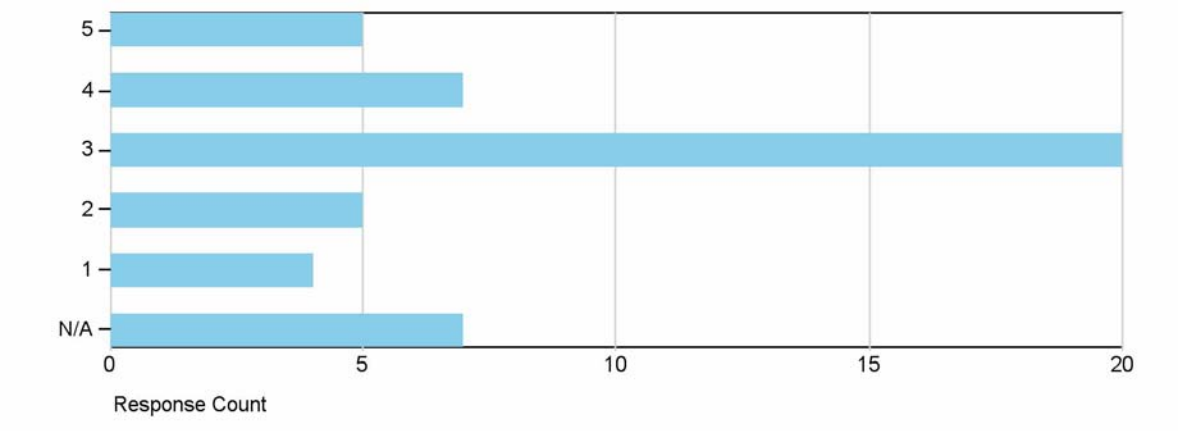
The survey was open for registrar responses from February 22, 2008 through March 11, 2008.

Registrars were asked two questions relating to DNSSec deployment:

1. How important is it that we offer DNSSEC? (Scale of 1 to 5 - 5 being most important)
2. If DNSSec were deployed in .ORG, how likely would you be to offer this feature to your registrants? (Scale 1 to 5 - 5 being most likely to offer)

The results of the survey are summarized in the following pages.

1. How important is it that we offer DNSSEC? (Scale of 1 to 5 - 5 being most important)

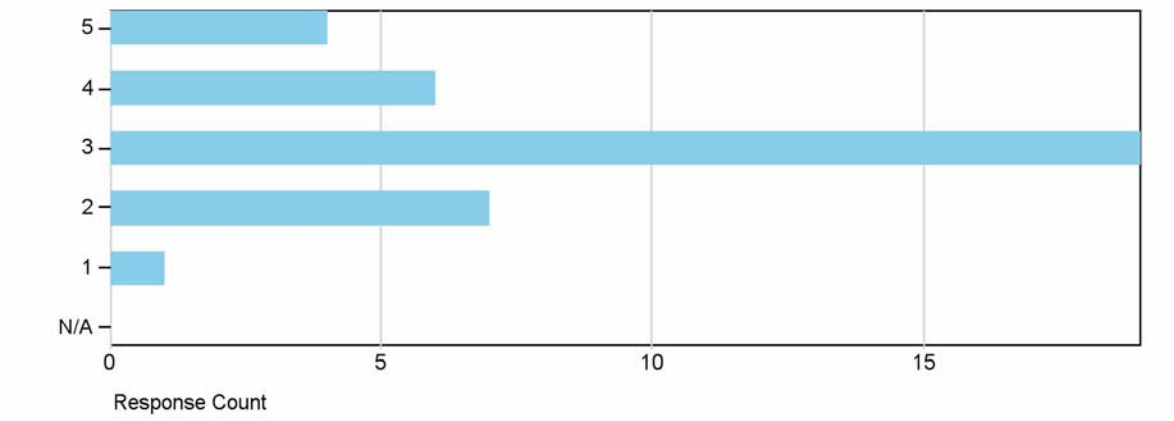


Total Respondents: 48
Total Skipped: 0

	Choice	Response Percent	Response Total
1	N/A	14.58%	7
2	1	8.33%	4
3	2	10.42%	5
4	3	41.67%	20
5	4	14.58%	7
6	5	10.42%	5

Analytics	
Mean	3.646
Standard Deviation	1.479
Standard Error	0.213
Variance	2.187

2. If DNSSec were deployed in .ORG, how likely would you be to offer this feature to your registrants? (Scale 1 to 5 - 5 being most likely to offer)



Total Respondents: 37
Total Skipped: 0

	Choice	Response Percent	Response Total
1	N/A	0.00%	0
2	1	2.70%	1
3	2	18.92%	7
4	3	51.35%	19
5	4	16.22%	6
6	5	10.81%	4

Analytics	
Mean	4.135
Standard Deviation	0.935
Standard Error	0.154
Variance	0.874

ENDORSEMENTS:

From: Steve Crocker [mailto:steve@shinkuro.com]
Sent: Friday, March 07, 2008 4:01 PM
To: Pamela Miller
Cc: Steve Crocker
Subject: Re: DNSSec Endorsement

Pamela,

Thanks for your request. SSAC has been strongly supportive of DNSSEC from the beginning of SSAC's formation and has viewed deployment of DNSSEC as one the most important security initiatives in the domain name system. We heartily endorse your application to ICANN for approval to offer DNSSEC service for the .ORG domain. We recently published SAC 026, SSAC Statement to ICANN and Community on Deployment of DNSSEC (30 January 2008) (http://www.icann.org/committees/security/sac026.pdf), so we are delighted to see PIR proceeding with such a request. We note that Sweden, Bulgaria, Puerto Rico and Brazil have already begun DNSSEC service, so there is ample precedence. In fact, Sweden initiated full scale commercial service more than a year ago after an extensive test period, so this technology is now well understood and past its initial shake down period.

We hope the example you are setting will serve as a positive signal to others, and we further hope that ICANN expedites your request and makes it clear to others that similar requests are welcome and will be processed expeditiously.

Please let us know if SSAC can assist you in any way.

Sincerely,

Steve Crocker, Chair

ICANN Security and Stability Advisory Committee

From: Russ Mundy [mailto:mundy@sparta.com]
Sent: Wednesday, March 12, 2008 5:56 PM
To: Pamela Miller
Cc: Russ Mundy; steve@shinkuro.com
Subject: Re: Fwd: DNSSec Endorsement

Pam,

Steve Crocker and I have discussed the PIR request for endorsement by

the DNSSEC Deployment WG of the plans for DNSSEC deployment in the .org registry. As co-chairs of the DNSSEC Deployment WG, Steve and I fully support moving forward with deploying DNSSEC in .org. I applaud this effort as an important step in improving the security and stability for the Internet.

Regards,

Russ Mundy
Co-Chair, DNSSEC Deployment Working Group
http://www.dnssec-deployment.org/

DNS Distributor with DNSSEC support
Test Plan

Project Name: ORG Release 1.0

Author: Name

Revision Number: **1.0**

Date: **11/13/07**

Revision History

Revision Number	Date	Who	Comments
1.0	11/13/07	AC	Initial Draft
1.1	11/13/07	AC	Added items 2.4.6,3.3; corrections

1 Introduction

This Test Plan document outlines the scope, approach, resources, and schedule of the testing activities for the DNS Distributor v.3.
DNS Distributor v.3 implements support for DNS Security Extensions (DNSSEC): a collection of new resource records and protocol modifications that add data origin authentication and data integrity to the DNS.
DNS Distributor v.3 is part of the larger project, ORG Release 1.0.

1.1 Scope

The scope of the testing will be to cover the new features introduced by DNSSEC support and performance testing to measures response times, transaction rates, and other time sensitive requirements.

The testing will include, also, a new procedure for externally manage zone signing keys and key signing keys (based on the key rollover policy).

1.2 Objective

The tests will ensure that each feature of DNS Distributor and the new command line tool (for administrative DNSSEC operations) meets the function specification requirements.

The key rollover process will be tested to meet the established policies .

1.3 Applicable Documents

This document is based upon on the technical requirements and design specifications as defined in “DNS Distributor DNSSEC Technical Specification and Design v2”.

2 Test Approach and Execution

Functionality testing will mainly use Execution and Analysis as the testing method. **E**xecution, **A**nalysis or **I**nspection will be used as indicated in the following test matrix. The results will be provided in text file format to facilitate the analysis.

Requirement	*Estimated Test Duration*	*Verification Method*
2.1 Installation Test 2.1.1 Verification of successful software installation process in accordance with installation notes. 2.1.2 Verification that the software runs and satisfies all hardware and software dependencies. 2.1.3 Installation/Upgrade documentation verification.	2 days	I, E, A
2.2 Configuration Test 2.2.1 Application configuration -- show utility -- service_admin utility -- service_config.xml 2.2.3 Adapters utilities & configuration -- dnssec_admin utility -- adapter_admin utility -- nus_admin utility -- cert utility -- xfr_admin utility -- notify_admin utility -- tsig_admin utility	5 days	I, E, A
2.3 Integration Test 2.3.1 Validate DNS Distributor integration with OXRS system (upstream) and bind/nsd system (downstream).	5 days	I,E,A
2.4 Functionality Test (with DNSSEC enabled/disabled) 2.4.1 DNSSEC Management Tools -- enable/disable DNSSEC -- add, remove, employ KSK -- add, remove, employ ZSK 2.4.2 Signing/re-signing the zone -- verify DNSKEY, NSEC, RRSIG records, and DS extension generated in each component. -- generate axfr/ixfr files. -- dig DNSKEY, NSEC, RRSIG resource records	15 days	I, E, A

Requirement	*Estimated Test Duration*	*Verification Method*
-- dig NS, A resource records 2.4.3 Query DNSSEC information: -- list / history 2.4.5 Adapters functionality: Domain Creation Domain Modification Domain Deletion Host within TLD Creation Host within TLD Modification Host within TLD Deletion -- generate zone file/dig on each component box 2.4.6 Validate the key managment procedure.		
2.5 Performance Test Validate System Response time for designated transactions or business functions under a the following two conditions: - normal anticipated volume - anticipated worse case volume	10 days	I,E,A
2.6 Load Test Verify System Response time for designated transactions under varying workload conditions.	10 days	E,A
2.7 Documentation Documentation of the Test Plan, Test Cases, results of performance and other tests, problems identified and their status.	5 days	I, E

3 Resources

3.1 Environment

Three application servers for DNS Distributor adapters (AIX/Linux)
Two application (OXRS) servers (load-balanced):
- 4 x PowerPC_POWER5 1.5 Ghz 64-bit processors

- 8GB RAM

Two database servers:

- 4 x PowerPC_POWER5 1.5 Ghz 64-bit processors
- 8GB RAM

One x86 Linux client.

DNS name server(s) with BIND, NSD.

3.2 Software

Application Servers
- AIX 3.5 / Linux
- Java 1.5
- Perl 5.8.2

Database Servers
- AIX 3.5
- PostgreSQL 8.1.8

- OXRS system
- epptt client

3.3 Personnel

The Afilias QA department will perform all the testing.

4 Schedule

Scheduled project time based on test duration and resources allocated.

5 Assumptions

3.1 OXRS system will support DNSSEC.
3.2 EPPTT will support DNSSEC.
3.3 Key rollover policy and procedures will be available when the QA cycle starts.
3.4 No significant system setup difficulties are encountered.

3.5 QA staff has unfettered access to the hardware resources mentioned above.

TEST PLAN
.ORG DNSSEC Implementation

Version: 1.4 :: Date: 2007-10-29 :: Authors: Radha Murthi, Paul Wojcik

1. Scope and Objectives

1.1 Scope

1.1.1. This test plan covers the testing of the implementation of RFC 4310 in the .ORG registry and dropzone. It also includes testing of the modified web administration tool, RTK and the .ORG WHOIS display to verify their ability to support the implementation of RFC 4310 in the .ORG registry. The new weekly reports for registrars and the registry operator will be tested as well. The functional specifications, business requirements and design documents provide the basis for this document.

1.2 Out of Scope

1.2.1. Downstream business intelligence applications.

1.3 Objective

1.3.1. To ensure that the implementation of RFC 4310 in the .ORG registry matches the business requirements and functional specification.

2. Test Approach

Functionality testing will mainly use demonstration as the testing method. When necessary, **E**xecution, **A**nalysis or **I**nspection will be used as indicated in the following test matrix.

Test Requirement	***Verification Method***	***Estimated Duration***
2.1. Installation	I, E,A	1 day
2.1.1. Verification of successful software installation process in accordance with installation notes.		
2.1.2. Verification that the software runs and satisfies all hardware and software dependencies.		

2.2. Configuration 2.2.1. Verification that the system is configurable as described in the installation notes to allow for the functionality described in the Functional Specification. This includes: • Verification of property default values. • Verification of successful handling of parameter data boundaries as specified in supporting documentation. • Verification of negative scenarios such as missing data, or illegal characters.	I, E,A	4 days
2.3. Functionality 2.3.1. Verification that the functionality of EPP and Web Interface is as described in the Functional Specification.	I, E, A	25 days
2.4. Integration 2.4.1. Verification of the OXRS system's integration with parallel and downstream components of the registry. This includes: • DNS Distributor • Whois server and cache management • Drop Zone	I, E, A	4 days
2.5. Performance 2.5.1. Benchmark • Generate load of domain create and update operations based on normal usage patterns. Measure system stability and performance levels. 2.5.2. Capacity • Generate stress-focused load by performing domain create and update operations beyond normal usage patterns with maximum allowable data injection limits from multiple clients and multiple accounts. Measure system stability and level of performance degradation while incrementally increasing transaction volumes.	E, A	12 days

2.6. Concurrency 2.6.1. Repeat performance tests where all the functions the system is expected to handle are performed simultaneously. Measure system stability and performance level in relation to benchmark results.	I, E, A	2 days
2.7. Longevity 2.7.1. Ensure system stability over at least a one week period where the system will be subject to varied states of activity. Moderate and heavy loads will be intersected by periods of idle states in an effort to simulate possible real system usage and measure its response.	E, A	7 days
2.8. Documentation 2.8.1. Documentation of the Test Plan, Test Cases, results of performance and other tests, problems identified and their status.	I, E	5 days

3. Resources

3.1 Environment

QA hardware allocated for testing:

Two application servers (load-balanced):
- 4 x PowerPC_POWER5 1.5 Ghz 64-bit processors
- 8GB RAM

One database server:

- 4 x PowerPC_POWER5 1.5 Ghz 64-bit processors
- 8GB RAM

One or more x86 linux clients.

3.2 Software

Application Servers
- AIX 3.5
- J2RE 1.4.2 IBM AIX 5L for PowerPC (64 bit JVM) build caix64142-20060421
- Perl 5.8.2

Database Servers
- AIX 3.5
- PostgreSQL 8.1.8

The Afilias EPP Test Tool (EPPTT) will be modified to support the DSSEC extensions and will be the primary test client used. Other clients may be used where required.

3.3 Personnel

The Afilias QA department will perform all the testing. Two people from the QA department will be assigned full time for the duration of the testing.

4. Schedule

4.1 Scheduled project time based on test duration and resources allocated.

5. Assumptions

5.1 All prices are in USD and all times are in UTC.

5.2 The DNSSEC Hashed Authenticated Denial of Existence draft at http://www.ietf.org/internet-drafts/draft-ietf-dnsext-nsec3-12.txt will be implemented for the .ORG registry. Implementation follows the requirements laid out in the functional specifications and no additional functionality is added or significant changes made.

5.3 No significant system setup difficulties are encountered.

5.4 QA staff has unfettered access to the hardware resources mentioned above.