New gTLD Program
Explanatory Memorandum

Pre-delegation Testing for new gTLDs

(Update for Applicant Guidebook v2 – Module 5 Pre-delegation testing)

Date of Publication: 8 June 2009

Background - New gTLD Program

Since ICANN was founded ten years ago as a not-for-profit, multi-stakeholder organization dedicated to coordinating the Internet's addressing system, one of its foundational principles, recognized by the United States and other governments, has been to promote competition in the domain-name marketplace while ensuring Internet security and stability. The expansion will allow for more innovation, choice and change to the Internet's addressing system, now constrained by only 21 generic top-level domain names. In a world with 1.5 billion Internet users—and growing—diversity, choice and competition are key to the continued success and reach of the global network.

The decision to launch these coming new gTLD application rounds followed a detailed and lengthy consultation process with all constituencies of the global Internet community. Representatives from a wide variety of stakeholders—governments, individuals, civil society, business and intellectual property constituencies, and the technology community—were engaged in discussions for more than 18 months. In October 2007, the Generic Names Supporting Organization (GNSO)—one of the groups that coordinate global Internet policy at ICANN—completed its policy development work on new gTLDs and approved a set of recommendations. The culmination of this policy development process was a decision by the ICANN Board of Directors to adopt the community-developed policy in June 2008 at the ICANN meeting in Paris. A thorough brief to the policy process and outcomes can be found at http://gnso.icann.org/issues/new-gtlds/.

This paper is part of a series of papers that will serve as explanatory memoranda published by ICANN to assist the Internet community to better understand the Applicant Guidebook. A public comment period for the Applicant Guidebook will allow for detailed review and input to be made by the Internet community. Those comments will then be used to revise the documents in preparation of a final Applicant Guidebook. ICANN will release the final Applicant Guidebook and open the application process in the first half of 2010. For current information, timelines and activities related to the New gTLD Program, please go to http://www.icann.org/en/topics/new-gtld-program.htm.

Please note that this is a discussion draft only. Potential applicants should not rely on any of the proposed details of the new gTLD program as the program remains subject to further consultation and revision.

Summary of Key Points in this Paper

- After passing financial and technical evaluations, each new gTLD application will be required to successfully complete a series of pre-delegation tests, within the period specified, as a pre-requisite for delegation into the root zone.
- The purpose of the pre-delegation technical test is to verify the applicant has met its commitment to establish registry operations in accordance with the technical and operational criteria described.
- There are three sets of tests or verification: DNS infrastructure testing and prerequisites, registry system testing and prerequisites, and an additional requirement to provide for continuity of basic registry operations.

Preface

Following is the draft text for the pre-delegation testing section of the New gTLD Applicant Guidebook. This section appears in Module 5 of the Applicant Guidebook; see the full module at http://www.icann.org/en/topics/new-gtlds/draft-transition-clean-18feb09-en.pdf.

Module 5 describes procedures applicable at the concluding stages of the gTLD application process, including completion of a pre-delegation test and the execution of a Registry Agreement between the applicant and ICANN. The pre-delegation test includes technical and other requirements.

The purpose of the pre-delegation technical test is to verify the applicant has met its commitment to establish registry operations in accordance with the technical and operational criteria described. (Refer to http://www.icann.org/en/topics/new-tlds/draftevaluation-criteria-clean-18feb09-en.pdf.)

The checks are also intended to ensure that the applicant can operate the gTLD in a stable and secure manner.

ICANN encourages comment on the language provided here. This language is for discussion only, and has not yet been incorporated into the Applicant Guidebook. Comments will be considered for version 3 of the full draft Applicant Guidebook, scheduled to be published in September 2009.

Table of Contents

Draft 2.0 on
Pre-delegation Testing for new gTLDs

Introduction

After passing financial and technical evaluations, each new gTLD application will be required to successfully complete a series of pre-delegation tests, within the period specified, as a pre-requisite for delegation into the root zone.

Technical testing

This section outlines the pre-delegation technical tests that will be performed by ICANN prior to a new gTLD being delegated in the root zone. It is meant as a guide to applicants on their way to a successful bid.

The purpose of the pre-delegation technical tests is to ensure that the applicant is meeting its commitment to establish services according to the criteria described in the Applicant Guidebook.

It is also intended as a way to ensure that the applicant can operate many technical aspects of the new gTLD in a stable manner as well as provide adequate universal access to all involved parties (registrars, end users, etc.).

Tests are comprised both registry operations and the DNS server operational infrastructure. These are detailed separately below.

Additional requirements

At the time of the application, the applicant is required to provide information regarding a financial instrument to provide for continuity of basic registry operations for a period of 3 – 5 years. The information provided by the applicant is validated by ICANN during the pre-delegation testing, to ensure that the financial instrument is in place and the applicant can meet the commitments made in the application.

DNS infrastructure testing and prerequisites

System performance requirements

The DNS infrastructure to which these tests apply comprises the complete set of server and network infrastructure to be used by potential provider to provide DNS service for the new gTLD to the Internet.

The applicant must demonstrate through a system performance test that sufficient network and server capacity is available to ensure stable service as well as to adequately address Distributed Denial of Service (DDoS) attacks according to industry best practices.

Applicant will self-certify adherence to this requirement and provide materials to ICANN that demonstrate adherence. Examples of self-certification documents include but are not limited to performance and availability results that demonstrate DNS availability at stated levels for at least one month. If using anycast to increase performance and/or resilience, applicant shall include a list of locations for current and planned sites.

At ICANN's discretion, aspects of this self-certification documentation can be audited on-site at the service delivery points.

System monitoring

Applicant will self-certify adherence to this requirement and provide materials to ICANN that demonstrate adherence.

Elements of this section shall be comprised of descriptions of the implementation of local (to the registry) and distributed data collection points that indicate global reachability. If anycast routing techniques are used, a description of individual node determination methods must be present as well as information describing how Internet end users may identify specific nodes.

Examples of self-certification documents include but are not limited to: diagrams of existing and in-place monitoring systems (demonstrating correspondence to documentation provided in the application), output of periodic monitoring runs performed by the applicant demonstrating capability claimed in the application, and actual performance of this monitoring set up in use for other registries. Applicant will self-certify adherence to this requirement and provide materials to ICANN that demonstrate adherence.

DNSSEC support

If DNSSEC support is provided in the new gTLD, applicant shall demonstrate support for EDNS(0) in its server infrastructure. Applicant will self-certify adherence to this requirement and provide materials to ICANN that demonstrate adherence.

Elements of this section shall be comprised of documentation demonstrating non-error response to DNS queries that include EDNS(0). At ICANN's discretion, aspects of this self-certification documentation can be audited.

TCP support

TCP transport service for DNS queries and responses must be enabled and provisioned for expected load. Applicant will self-certify adherence to this requirement and provide materials to ICANN that demonstrate adherence.

Elements of this section shall be comprised of documentation demonstrating TCP-based responses to DNS queries as well as information regarding expected TCP query loads and measures taken to support that load. At ICANN's discretion, aspects of this self-certification documentation can be audited.

IPv6 support

Applicant must provision IPv6 service for its DNS infrastructure. The same technical criteria regarding global reachability, bandwidth and network availability that apply to IPv4 network transport apply to IPv6 network transport, including the cases where anycast is in use.

Packet size monitoring

Applicant will describe in-place and existing monitoring and communication mechanisms to registrars for detecting and signaling registry entries resulting in DNS response sizes exceeding the common 512-byte threshold.

If DNSSEC support is provided in the new gTLD applicant must also describe in-place and existing monitoring and communication mechanisms to registrars for detecting and signaling registry entries resulting in DNS response sizes exceeding the RFC 3226-mandated 1220-byte threshold.

Registry system testing and prerequisites

Registry continuity

Applicant will self-certify adherence to this requirement and provide materials such as test results documentation to ICANN that demonstrate adherence. Examples include identification of appropriate contact points and copies of the registry's own continuity plan, and identification of a registry services continuity provider.

An outline of requirements can be found at http://www.icann.org/registries/failover/icann-registry-failover-plan-15jul08.pdf.

System performance

Applicant will self-certify compliance with performance capacities to exceed expected peak registration loads. This comprises server systems used for registry infrastructure as well as their access network.

Applicant will provide materials to ICANN that demonstrate adherence to meeting self-defined capacity requirements. Examples of self-certification documents include but are not limited to performance and availability results that demonstrate WHOIS service availability for at least one month and Domain Name provisioning system availability for the same period. At ICANN's discretion, aspects of this self-certification documentation can be audited on-site at the service delivery points.

Similarly, applicant will self-certify the existence of in-place network access control measures to protect the registry system.

System monitoring

Applicant will self-certify adherence to this requirement and provide materials to ICANN that demonstrate in-place capability for adherence to this requirement. Elements of this requirement include industry best practices such as access control monitoring; load monitoring, availability monitoring and statistics gathering, with record-keeping.

At ICANN's discretion, aspects of this self-certification documentation can be audited on-site at the services delivery point of the registry.

IPv6 support

Applicant's registry system must support IPv6 provisioning for registrants and registrars, allowing IPv6 addresses in any field where an IP address may be used. This provisioning will be tested by ICANN remotely.

DNSSEC support

If DNSSEC is supported in the new gTLD, applicant will be required to establish and publish key rollover procedures for regular and emergency cases, and verify secure communication channels with the IANA for trust anchor material.

Applicant shall describe the in-place provisioning systems allowing the secure communication of trust anchor material from registrants as well as emergency procedures available to registrants.

Applicant must provide a practice and policy document describing key material storage, access and usage for its own keys and the registrants' trust anchor material.

IDN support

If the new gTLD will be supporting IDN, applicant must commit to comply with IDN Guidelines and register with the IANA the complete IDN table used in the registry system. The table must comply with the guidelines in http://iana.org/procedures/idn-repository.html.

Escrow deposit

Escrow deposit of data is aimed at preserving the ability to reconstruct a registry in the case of business or catastrophic technical failure.

The applicant will provide a conforming sample of a dummy data deposit showing correct type and formatting of content. The applicant will also provide evidence of an executed, funded agreement with an escrow provider complying with Part B of the Data Escrow Requirements.

If special applications are necessary to enable registry reconstruction or re-establishment of communications with registrars, these shall also be made part of the escrow deposit.

Escrow specification guidelines are available at http://www.icann.org/en/topics/new-gtlds/draft-escrow-spec-clean-18feb09-en.pdf.

Additional Requirements

Registry operator will submit documented evidence or detailed plan for ability to fund on-going basic registry operations for registrants for a period of 3-5 years in the event of registry failure, default or until a successor operator can be designated and evidence of financial wherewithal to fund this requirement prior to delegation.

The basic functions of a registry which must be supported even if an applicant's business and/or funding fails include:

a. Maintenance of name servers and DNS for registered domain names
b. Shared Registration System
c. Whois service
d. Registrar billing and accounting
e. Data security and data escrow
f. IDN Tables (if IDNs are offered by the registry)
g. DNSSEC Keys (if DNSSEC is offered by the registry)

Applicants must provide evidence of how the funds required for performing these basic functions are ensured, so as to protect registrants. Evidence can be in the form of financial instruments or contracts such as:

- **Contracting with Other Registries**: A contract can be entered into whereby a more established and secure Registry agrees to operate the applicant's Registry should a future need arise
- **Restricted Cash**: Cash held by a third party trustee or held in an account with specific restrictions.
- **Other Collateral**: Assets such as stocks, bonds, negotiable paper, or real estate pledged.
- **Third Party Guaranty**: A financially secure organization provides a guaranty for the applicant or pledges assets.
- **Letters of Credit (LOC), Bonds**: Standby Letters of Credit, irrevocable letters of credit, or "evergreen" letters of credit, performance bonds, surety bonds are financial instruments issued by a bank to ensure payments are made if the applicant fails. The forms, language, and institution backing an LOC determine its strength as collateral.
- **Sinking Fund**: Funds are set aside, over time, by the Registry building up to an amount sufficient to cover the potential obligation.
- **Pooled Sinking Fund**: Applicants may be able to pool together their risks and pay into a collective sinking fund to cover any registry that may fail belonging to the pool.