Pre-Delegation Testing

DNS Test Plan

Version F

File name: PDT_DNS_TP.docx
Last saved: 2013-07-01

Document control

Document information and security

Made by	Responsible for fact	Responsible for document
Patrik Wallström	Patrik Wallström	Patrik Wallström

Security class	File name
External	PDT_DNS_TP.docx

Revisions

Date	Version	Name	Description
2013-01-15	PA1	Patrik Wallström	Initial document
2013-01-24	PA2	Rickard Bellgrim	Update text after review
2013-02-06	PA3	Rickard Bellgrim	Add Document Hierarchy and final chapters
2013-02-25	PA4	Patrik Wallström	Updated to conform to new requirements (R27b)
2013-03-06	PA5	Patrik Wallström	Updated with new tests based on feedback
2013-04-08	B	Staffan Hagnell	Delivery D2 for production
2013-04-18	C	Patrik Wallström	Updated DNS31
2013-05-03	D	Amar Andersson	Released
2013-05-24	(P)E1	Patrik Wallström	Added the new requirements and test cases for Distributed testing Removed the requirements and test cases for Anycast testing
2013-06-04	E	Mats Dufberg	Released
2013-06-14	(P)F1	Patrik Wallström	Re-numbered the ADD requirements to match amendments to SOW
2013-07-01	PF2	Mats Dufberg	Added reference to Test Case document in Test Case table.
2013-07-01	F	Mats Dufberg	Released.

LIST OF CONTENTS

1. Introduction

This Level Test Plan focuses on the DNS service of the new gTLDs.

1.1 Scope

The Pre-Delegation Testing Provider will test the DNS infrastructure.

1.2 References

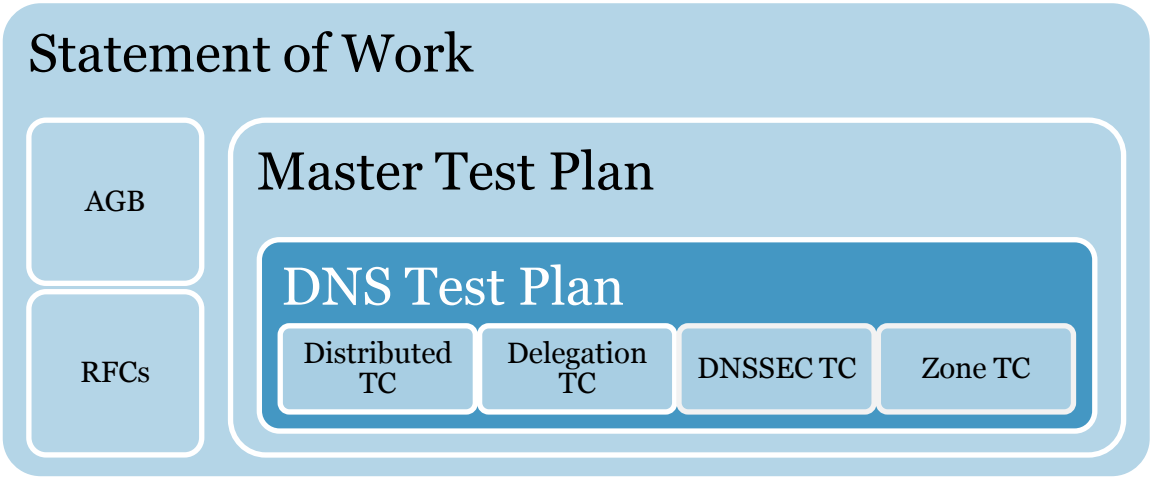
1.2.1 External

- IEEE 829-2008
- ICANN gTLD Applicant Guidebook, Version 2012-06-04

1.2.2 Internal

- Pre-Delegation Testing, Statement of Work
- Pre-Delegation Testing, Master Test Plan
- Pre-Delegation Testing, DNS Delegation Test Cases
- Pre-Delegation Testing, DNS DNSSEC Test Cases
- Pre-Delegation Testing, DNS Distributed Test Cases
- Pre-Delegation Testing, DNS Zone Test Cases

1.2.3 Document Hierarchy



1.3 Level in the overall sequence

The DNS test plan can be executed independently of other tests.

1.4 Test classes and overall test conditions

The DNS service for the gTLD is available over IPv4 and IPv6 via UDP and TCP on port 53. The DNS infrastructure must be open and available for testing, and be configured with the designated zone for authoritative answers. The applicant provides valid test data.

2. Details for this level of test plan

2.1 Test items and their identifiers

2.1.1 Statement of Work

The main requirements for testing the DNS infrastructure are found in the Statement of Work:

[R9] Test the applicant's DNS infrastructure for compliance with the requirements described in section 5.2 of the AGB.

[R25] Verify that the provided DNSSEC trust anchor can be used to validate DNSSEC signatures in the test zone.

[R27] Verify that all authoritative name servers complies with the IANA Technical Requirements – http://www.iana.org/procedures/nameserver-requirements.html

[R28] Verify that the submitted DNSSEC Trust Anchors (DS records) complies with the IANA Technical Requirements – http://www.iana.org/procedures/root-dnssec-records.html

2.1.2 Additions to Statement of Work

[ADD3] Check invalid syntax for SOA RNAME

[ADD4] SOA Minimum must be more than 300 seconds

[ADD5] Check for too many (150) NSEC3 iterations

[ADD6] Check for too short (12 hours) or too long (180 days) RRSIG lifetimes

[ADD7] Check for invalid DNSKEY algorithms

[ADD8] Check for Too long (>172800) TTL for DS records

[ADD9] Wildcards must not exist in the TLD zone ("site finder")

[ADD10] Check for use of zone as "dotless domain"

[ADD11] nic.<TLD> or whois.nic.<TLD> must be delegated

2.1.3 Additions to Statement of Work, Distributed testing

[ADD13] Name server must be able to provide referral to known subdomains, from many distributed measurement nodes

[ADD14] The following AGB requirements must also be tested over IPv4, IPv6, UDP and TCP, from many distributed measurement nodes:

- AGB1, Name server reachability
- AGB2, Return correct DNSKEY
- AGB3, Return NSEC/NSEC3 records

The following test cases must be tested over IPv4, IPv6, UDP and TCP:

- DEL3, Name server reachability
- DEL4, Answer authoritatively
- DEL6, Consistency between glue and authoritative data
- DEL7, Consistency between delegation and zone
- DEL8a, SOA record consistency between authoritative name servers
- DEL8b, Name server consistency between authoritative name servers
- DEL11, No open recursive name service

2.1.4 Technical requirements for authoritative name servers

These requirements are derived from the tests that IANA performs for all name server changes to the root zone. The test cases are mostly collected in the Delegation test case document. This is an overview of the described requirements:

{DEL1}	Minimum number of name servers
{DEL2}	Valid hostnames
{DEL3}	Name server reachability
{DEL4}	Answer authoritatively
{DEL5}	Network diversity
{DEL6}	Consistency between glue and authoritative data
{DEL7}	Consistency between delegation and zone
{DEL8a}	SOA record consistency between authoritative name servers
{DEL8b}	Name server consistency between authoritative name servers
{DEL9}	No truncation of referrals
{DEL10}	Prohibited networks
{DEL11}	No open recursive name service
{DEL12}	Same source address

2.1.5 Placing TLD delegation signer information in the root zone

This IANA document is describing the IANA requirements for publishing a DS record in the root zone. This is an overview of the described requirements:

{DS1}	Valid digest algorithm for the DS hash digest
{DS2}	A DS record must match a DNSKEY that is present in the child zone

2.1.6 Applicant Guidebook

Section 5.2 of the AGB states the following requirements:

> **UDP Support --** The DNS infrastructure to which these tests apply comprises the complete set of servers and network infrastructure to be used by the chosen providers to deliver DNS service for the new gTLD to the Internet.
>
> **TCP support --** TCP transport service for DNS queries and responses must be enabled and provisioned for expected load. ICANN will review the capacity self-certification documentation provided by the applicant and will perform TCP reachability and transaction capability tests across a randomly selected subset of the name servers within the applicant's DNS infrastructure. In case of use of anycast, each individual server in each anycast set will be tested.
>
> **DNSSEC support --** Applicant must demonstrate support for EDNS(0) in its server infrastructure, the ability to return correct DNSSEC-related resource records such as DNSKEY, RRSIG, and NSEC/NSEC3 for the signed zone, and the ability to accept and publish DS resource records from second-level domain administrators. In particular, the applicant must demonstrate its ability to support the full life cycle of KSK and ZSK keys. ICANN will review the self- certification materials as well as test the reachability, response sizes, and DNS transaction capacity for DNS queries using the EDNS(0) protocol extension with the "DNSSEC OK" bit set for a randomly selected subset of all name servers within the applicant's DNS infrastructure. In case of use of anycast, each individual server in each anycast set will be tested.

The test cases described in the Applicant Guidebook section 5.2 are also covered by R27 and R28. So there will be a minimal set of requirements derived from the Applicant Guidebook. Name server reachability over UDP and TCP, DNSSEC and EDNS(0) and anycast support will be covered by these requirements:

[AGB1] Name server reachability

[AGB2] Return correct DNSKEY

[AGB3] Return NSEC/NSEC3 records

2.2 Test Traceability Matrix

Test ID	In Test Case document	Description	Requirement Point
DNS01 Minimum number of name servers	Delegation	There must be at least two NS records listed in a delegation, and the hosts must not resolve to the same IP address.	R27, DEL1, DEL2
DNS02 Name server reachability	Delegation	The name servers must answer DNS queries over both the UDP and TCP protocols on port 53.	R27, DEL3
DNS03 Answer authoritatively	Delegation	The name servers must answer authoritatively for the designated zone. Responses to queries to the name servers for the designated zone must have the "AA"-bit set.	R27, DEL4
DNS04 Network diversity	Delegation	The name servers must be in at least two topologically separate networks.	R27, DEL5
DNS05 Consistency between glue and authoritative data	Delegation	For name servers that have IP addresses listed as glue, the IP addresses must match the authoritative A and AAAA records for that host.	R27, DEL6
DNS06 Consistency between delegation and zone	Delegation	The set of NS records served by the authoritative name servers must match those proposed for the delegation in the parent zone.	R27, DEL7
DNS07 SOA record consistency between authoritative name servers	Delegation	The data served by the authoritative name servers for the designated zone must be consistent. [..] All authoritative name servers must serve the same SOA record for the designated domain.	R27, DEL8a
DNS08 NS record consistency between authoritative name servers	Delegation	The data served by the authoritative name servers for the designated zone must be consistent. All authoritative name servers must serve the same NS record set for the designated domain.	R27, DEL8b
DNS09 No truncation of referrals	Delegation	Referrals from the parent zone's name servers must fit into a non-EDNS0 UDP DNS packet and therefore the DNS payload must not exceed 512 octets.	R27, DEL9
DNS10 Prohibited networks	Delegation	The authoritative name server IP addresses must not be in specially designated networks that are either not globally routable, or are otherwise unsuited for authoritative name service.	R27, DEL10
DNS11 No open recursive name service	Delegation	The authoritative name servers must not provide recursive name service.	R27, DEL11
DNS12 Same source address	Delegation	Responses from the authoritative name servers must contain the same source IP address as the destination IP address of the initial query.	R27, DEL12
(DNS13 Removed)	N/A	(Removed)	
DNS14 Legal values for the DS hash digest algorithm	DNSSEC	For the hash digest, ICANN supports two types — SHA1 (value 1), and SHA256 (value 2). The DnsKeyDigestType for the supplied DS records must match those type values.	R25, R28, DS1

Test ID	In Test Case document	Description	Requirement Point
DNS15 DS must match a DNSKEY in the designated zone	DNSSEC	There must be a DNSKEY that matches the DS record present in the child zone.	R25, R28, DS2, AGB2, AGB5
DNS16 Signatures in the designated zone must validate	Distributed	Verify that the provided DNSSEC trust anchor can be used to validate DNSSEC signatures (RRSIG) in the test zone.	R25, R28, AGB2, ADD14
DNS17 Zone contains NSEC or NSEC3 records	Distributed	The zone must contain NSEC or NSEC3 records with valid signatures.	R9, AGB3, ADD14
DNS18 Consistency between glue and authoritative data	Distributed	For name servers that have IP addresses listed as glue, the IP addresses must match the authoritative A and AAAA records for that host.	R27, ADD14, DEL6
DNS19 SOA record consistency between authoritative name servers	Distributed	The data served by the authoritative name servers for the designated zone must be consistent. [..] All authoritative name servers must serve the same SOA record for the designated domain.	R27, ADD14, DEL8a
DNS20 NS record consistency between authoritative name servers	Distributed	The data served by the authoritative name servers for the designated zone must be consistent. All authoritative name servers must serve the same NS record set for the designated domain.	R27, ADD14, DEL8b
DNS21 No open recursive name service	Distributed	The authoritative name servers must not provide recursive name service.	R27, ADD14, DEL11
(DNS22 Removed)	N/A	(Removed)	
DNS23 Syntax for SOA RNAME	Delegation	Check invalid syntax for SOA RNAME	ADD3
DNS24 SOA Minimum	Delegation	SOA Minimum must be more than 300 seconds	ADD4
DNS25 NSEC3 Iterations	DNSSEC	Check for too many (150) NSEC3 iterations	ADD5
DNS26 RRSIG Lifetimes	DNSSEC	Check for too short (12 hours) or too long (180 days) RRSIG lifetimes	ADD6
DNS27 DNSKEY Algorithms	DNSSEC	Check for invalid DNSKEY algorithms	ADD7
DNS28 DS TTL	Zone	Check for Too long (>172800) TTL for DS records	ADD8
DNS29 Wildcards	Zone	Wildcards must not exist in the TLD zone (“site finder”)	ADD9
DNS30 Dotless domain	Zone	Check for use of zone as “dotless domain”	ADD10
DNS31 nic.<TLD> or whois.nic.<TLD> must be delegated	Zone	nic.<TLD> or whois.nic.<TLD> must be delegated	ADD11
DNS32 Name server reachability	Distributed	The name servers must answer DNS queries over both the UDP and TCP protocols on port 53.	R27, DEL3, ADD14
DNS33 Answer authoritatively	Distributed	The name servers must answer authoritatively for the designated zone. Responses to queries to the name servers for the designated zone must have the “AA”-bit set.	R27, DEL4, ADD14
DNS34 Consistency between delegation and zone	Distributed	The set of NS records served by the authoritative name servers must match those proposed for the delegation in the parent zone.	R27, DEL7, ADD14

Test ID	In Test Case document	Description	Requirement Point
DNS35 Name server must be able to provide referral to known subdomains	Distributed	All name servers must provide a referral with NS, DS and optional glue for the delegated subdomain.	ADD13

2.3 Features to be tested

- DNS infrastructure
- A sub-set of records present in the zone
- Reachability and connectivity to all specified name servers
- UDP and TCP support
- IPv4 and IPv6 connectivity
- DNSSEC with DNSKEY, NSEC/NSEC3 and valid RRSIGs
- Network diversity
- No open resolvers
- DNSKEY algorithms and signature lifetimes
- Legal or correct values in the SOA record

2.4 Features not to be tested

- Load capacity
- PTR records
- DNSKEY key lengths
- AXFR availability
- The internal anycast structure

2.5 Approach

The overall input parameters for the different DNS test cases we consider to be the same set of parameters as those sent to IANA for publication in the root. We follow the same structure as the web form and the e-mail form that is used for communication with IANA.[1]

All DNS tests that are performed using the DNS protocol on the applicants DNS infrastructure is done from all five Internet locations over IPv4 and IPv6. Some tests are not dependent on network connectivity but only applied using rules using the input parameters.

In case of any temporary network failures, all DNS test cases can be repeated if necessary without any external interaction needed.

In the test case document DNS TC Distributed; the measurement criteria for those tests are described in section 1.5 in that document.

2.6 Item pass/fail criteria

The test will pass if an expected response was received from the DNS service. It will however fail if it is not following the requirements.

There are some special procedural requirements that give a "notify" message in the report. The result of the test is ok, but there is some information about the tests result that ICANN should be aware of.

The Service Level Requirement in Specification 10 of the registry agreement states that "If the RTT is 5 times greater than the time specified in the relevant SLR, the RTT will be considered undefined". The requirement for UDP is 500ms and TCP is 1500ms. A test can thus be failed if it takes longer than 2.5 seconds to get an answer over UDP or longer than 7.5 seconds for TCP.

2.7 Suspension criteria and resumption requirements

The only suspension criteria for the test would be if there are external network problems outside the control of the applicant or the PDT tester.

2.8 Test deliverables

The DNS test level will produce:

- Level Test Logs (LTL)
- Anomaly Report (AR) in case of error
- Level Test Report (LTR)

[1] http://www.iana.org/domains/root/tld-change-template.txt

3. Test management

The goal of these documents is to describe the test cases and how the new gTLDs are tested. This is just a part of a larger project and defining test management is not part of this subproject. However, some information can be found in the Master Test Plan.

4. General

4.1 Glossary

The glossary is available in the Master Test Plan.

4.2 Document change procedures

Document change procedures are documented in the Master Test Plan.