Pre-Delegation Testing

Documentation Test Plan

Version D

File name: PDT_Documentation_TP.docx
Last saved: 2013-05-23

Document control

Document information and security

Made by	Responsible for fact	Responsible for document
Björn Sjöholm	Björn Sjöholm	Björn Sjöholm

Security class	File name
External	PDT_Documentation_TP.docx

Revisions

Date	Version	Name	Description
2013-01-06	PA1	Staffan Hagnell	Initial document
2013-01-09	PA2	Rickard Bellgrim	Rearrange text
2013-01-22	PA3	Björn Sjöholm	Test Traceability Matrix added
2013-01-24	PA4	Björn Sjöholm	Test conditions, Test deliverables, Features to be tested, Suspension criteria
2013-01-24	PA5	Rickard Bellgrim	Update text after review
2013-02-07	PA6	Björn Sjöholm	Change in test cases, SL new from DNS, EPP and whois
2013-02-07	PA7	Rickard Bellgrim	Add Document Hierarchy and final chapters
2013-03-01	PA8	Rickard Bellgrim	"key changes" to "key rollovers" "DNSSEC Policy Statement" to "DNSSEC Practice Statement" "KSK/ZSK keys" to "cryptographic keys"
2013-03-06	PA9	Björn Sjöholm	Matrix over Test Cases updated
2013-03-26	PA10	Björn Sjöholm	Matrix over Test Cases updated. Consolidation of testcases.
2013-04-18	PA11	Lennart Beckman	Matrix of Test Cases updated. DocDNS06 withdrawn. DocDNS07-09 renumbered.
2013-04-19	B	Mats Dufberg	Released.
2013-05-03	C	Amar Andersson	Released
2013-05-23	D	Lennart Beckman	Matrix of Test Cases updated. DocDPS Test Cases consolidated to the new DocDPS01, DocDPS02.

LIST OF CONTENTS

1. Introduction

This Level Test Plan focuses on the documents that have been submitted as part of the new gTLD application.

1.1 Scope

A number of documents and attachments are to be reviewed during the testing process. The documents cover multiple areas such as DNS, Whois, EPP, IDN, Data Escrow, and DPS. They have all been gathered into this test level in order to establish a common structure for reviewing the submitted documents.

1.2 References

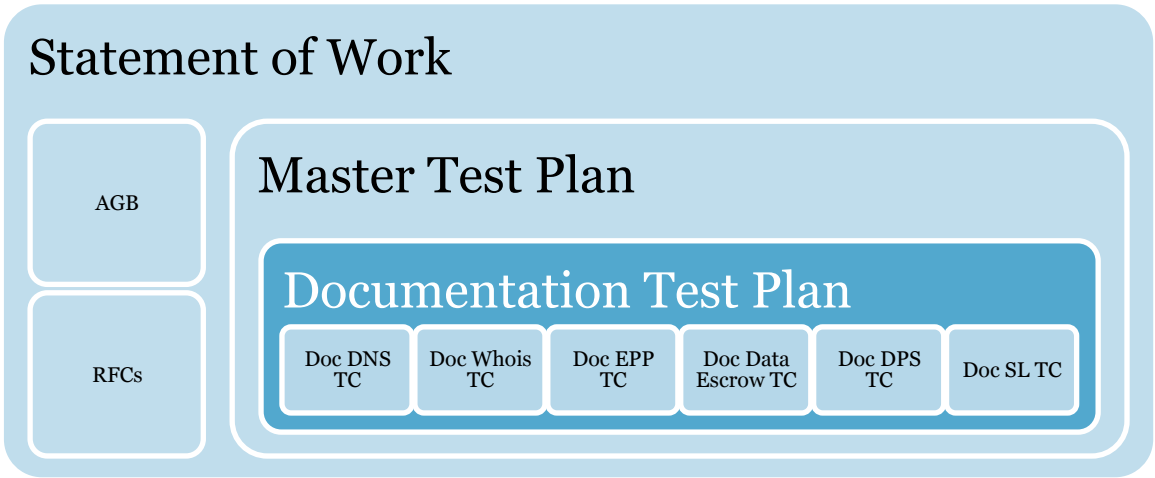
1.2.1 External

- 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

1.2.3 Document Hierarchy



1.3 Level in the overall sequence

This Test Plan and the associated Test Cases can be run in parallel with the other Level Test Plans.

1.4 Test classes and overall test conditions

The test cases cover verification of content in applicant documents such as self-certification documents. The test conditions are limited to the existence of the correct documents.

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 reviewing the documents are found in the Statement of Work:

[R10] **Review** the self-certification documents relating to the DNS infrastructure and verify compliance with the assertions made in the gTLD application in relation to system performance as described in specification 10 of the new gTLD registry agreement set forth in Module 5 of the AGB.

[R11] Test the applicant's Whois interface for compliance with the requirements described in the Section 5.2 of the AGB, including response format and **review** of the data mining detection and mitigation control functions.

[R12] **Review** the self-certification documents relating to the Whois interface and verify compliance with the assertions made in the gTLD application in relation to system performance as described in specification 10 of the new gTLD registry agreement set forth in Module 5 of the AGB.

[R17] **Review** the self-certification documents relating to the EPP interface and verify compliance with the assertions made in the gTLD application in relation to system performance as described in specification 10 of the new gTLD registry agreement set forth in Module 5 of the AGB.

[R18] **Review** applicant's EPP extensions documentation and verify standards compliance with RFC 3735, and verify that any extensions are consistent with the new gTLD registry agreement set forth in Module 5 of the AGB.

[R23] **Review** the submitted escrow provider agreement and any self-certification documents related to data escrow, and verify compliance with the requirements stated by the New gTLD Regisry Agreement Specification 2 – *Data Escrow Requirements* set forth in Module 5 of the AGB.

[R24] For each Data Escrow Service Provider contracted by gTLD applicants, **verify** that data can be released within 24 hours as stated by the New gTLD Registry Agreement Specification 2 – *Data Escrow Requirements* set forth in Module 5 of the AGB.

[R25] **Review** the submitted DNSSEC Practices Statement (DPS) and verify that it is describing critical security controls and procedures for key material storage, access and usage for its own keys and secure acceptance of registrants' public-key material, and that the DPS is following the format described in the IETF DPS Framework (currently in draft format, see http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework).

2.1.2 DNS

On top of the main requirements in the Statement of Work, a set of requirements has been identified in Section 5.2 of the AGB:

[DNS1] The documentation provided by the applicant must include the results from a system performance test indicating available network and server capacity and an estimate of expected capacity during normal operation to ensure stable service as well as to adequately address Distributed Denial of Service (DDoS) attacks.

[DNS2] Self-certification documentation for UDP support MUST include data on load capacity, latency and network reachability.

[DNS2.1] Load capacity MUST be reported using a table, and a corresponding graph, showing percentage of queries responded against an increasing number of queries per second generated from local (to the servers) traffic generators.

[DNS2.2] The load capacity table MUST include at least 20 data points and loads of UDP-based queries that will cause up to 10% query loss against a randomly selected subset of servers within the applicant's DNS infrastructure.

[DNS2.3] The load capacity responses MUST either contain zone data or be NXDOMAIN or NODATA responses to be considered valid.

[DNS2.4] Query latency MUST be reported in milliseconds as measured by DNS probes located just outside the border routers of the physical network hosting the name servers, from a network topology point of view.

[DNS2.5] Reachability MUST be documented by providing information on the transit and peering arrangements for the DNS server locations, listing the AS numbers of the transit providers or peers at each point of presence and available bandwidth at those points of presence.

[DNS3] Self-certification documentation for TCP support MUST include data on load capacity, latency and external network reachability.

[DNS3.1] Load capacity MUST be reported using a table, and a corresponding graph, showing percentage of queries that generated a valid (zone data, NODATA, or NXDOMAIN) response against an increasing number of queries per second generated from local (to the name servers) traffic generators.

[DNS3.2] The load capacity table MUST include at least 20 data points and loads that will cause up to 10% query loss (either due to connection timeout or connection reset) against a randomly selected subset of servers within the applicant's DNS infrastructure.

[DNS3.3] Query latency MUST be reported in milliseconds as measured by DNS probes located just outside the border routers of the physical network hosting the name servers, from a network topology point of view.

[DNS3.4] Reachability MUST be documented by providing records of TCP-based DNS queries from nodes external to the network hosting the servers. These locations may be the same as those used for measuring latency above.

[DNS4] 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.

[DNS4.1] In particular, the applicant MUST demonstrate its ability to support the full life cycle of cryptographic keys.

[DNS5] DNSSEC load capacity, query latency, and reachability MUST be documented as for UDP and TCP in [DNS2] and [DNS3].

[DNS6] Specification 10 of the registry agreement state that the following system performance MUST be met:

Parameter	SLR (monthly basis)
DNS service availability	0 min downtime = 100% availability
DNS name server availability	< 432 min of downtime (≈ 99%)
TCP DNS resolution RTT	< 1500 ms, for at least 95% of the queries
UDP DNS resolution RTT	< 500 ms, for at least 95% of the queries
DNS update time	< 60 min, for at least 95% of the probes

2.1.3 Whois

On top of the main requirements in the Statement of Work, a set of requirements has been identified in Section 5.2 of the AGB:

[WHOIS1] Self-certification documents MUST describe the maximum number of queries per second successfully handled by both the port 43 servers as well as the web interface, together with an applicant-provided load expectation.

[WHOIS2] Additionally, a description of deployed control functions to detect and mitigate data mining of the Whois database MUST be documented.

[WHOIS3] Specification 10 of the registry agreement state that the following system performance MUST be met:

Parameter	SLR (monthly basis)
RDDS availability	≤ 864 min of downtime (≈ 98%)
RDDS query RTT	≤ 2000 ms, for at least 95% of the queries
RDDS update time	≤ 60 min, for at least 95% of the probes

2.1.4 EPP

On top of the main requirements in the Statement of Work, a set of requirements has been identified in Section 5.2 of the AGB:

[EPP1] As part of a shared registration service, applicant MUST provision EPP services for the anticipated load.

[EPP2] Documentation MUST provide a maximum Transactions per Second rate for the EPP interface with 10 data points corresponding to registry database sizes from 0 (empty) to the expected size after one year of operation, as determined by applicant.

[EPP3] Documentation MUST also describe measures taken to handle load during initial registry operations, such as a land-rush period.

[EPP4] Specification 10 of the registry agreement state that the following system performance MUST be met:

Parameter	SLR (monthly basis)
EPP service availability	≤ 864 min of downtime (≈ 98%)
EPP session-command RTT	≤ 4000 ms, for at least 90% of the commands
EPP query-command RTT	≤ 2000 ms, for at least 90% of the commands
EPP transform-command RTT	≤ 4000 ms, for at least 90% of the commands

2.1.5 Data Escrow

On top of the main requirements in the Statement of Work, one requirement has been identified in Section 5.2 of the AGB:

[DATA1] Special attention will be given to the agreement with the escrow provider to ensure that escrowed data can be released within 24 hours should it be necessary.

Specification 2 of the registry agreement states the following requirements which need to be reviewed:

[DATA2] The Technical Specifications set forth in Part A must be included in any data escrow agreement between Registry Operator and the Escrow Agent

[DATA3] The Legal Requirements set forth in Part B must be included in any data escrow agreement between Registry Operator and the Escrow Agent

[DATA4] ICANN must be named a third-party beneficiary

[DATA5] The data escrow agreement may contain other provisions that are not contradictory or intended to subvert the required terms.

Note that requirements on escrow format, processing of deposit files, and file naming convention are tested as part of the Data Escrow Test Plan.

2.1.6 DPS

On top of the main requirements in the Statement of Work, a set of requirements has been identified in Section 5.2 of the AGB:

[DPS1] The ability to accept and publish DS resource records from second-level domain administrators MUST be demonstrated.

[DPS2] The applicant MUST demonstrate its ability to support the full life cycle of cryptographic keys.

[DPS3] The applicant MUST demonstrate its ability to support the full life cycle of key rollovers for child domains.

[DPS4] The document (also known as the DNSSEC Practice Statement or DPS), describing key material storage, access and usage for its own keys MUST also be reviewed as part of this step.

2.2 Test Traceability Matrix

This table describes the different test cases and their mapping to the requirements. They will be documented in six different test case documents: Doc DNS, Doc Whois, Doc EPP, Doc Escrow, Doc DPS, and Doc SL. The tests are performed by reviewing the self-certification documents to verify compliance with the requirements *and* the assertions made by the applicant in the gTLD application.

Test ID	Description	Requirement Point
Doc DNS 01	Identify relevant documentation. Verify that network availability and server capacity is included. Verify that expected capacity is included. Verify that DDoS attacks are addressed.	R10, DNS1
Doc DNS 02	Identify relevant documentation on UDP and TCP support and the corresponding for DNSSEC. Verify that load capacity, latency and network reachability is included.	R10, DNS2, DNS3, DNS5,
Doc DNS 03	Identify relevant documentation on UDP and TCP support and the corresponding for DNSSEC. Verify that load capacity is reported using a table and a corresponding graph, showing percentage of queries responded mapped to number of queries per second.	R10, DNS2.1, DNS3.1, DNS5
Doc DNS 04	Identify relevant documentation on UDP and TCP support and the corresponding for DNSSEC. Verify that the load capacity table includes at least 20 data points and include loads causing up to 10% query loss. Verify load capacity response either contains zone data or are NXDOMAIN or NODATA responses.	R10, DNS2.2, DNS2.3, DNS3.2, DNS5
Doc DNS 05	Identify relevant documentation on UDP and TCP support and the corresponding for DNSSEC. Verify that query latency is reported in milliseconds and adequately measured.	R10, DNS2.4, DNS3.3, DNS5
Doc DNS 06	Identify relevant documentation on TCP support. Verify that documentation includes documentation of reachability by providing records of TCP-based queries from relevant nodes.	R10, DNS3.4

Test ID	Description	Requirement Point
Doc DNS 07	Identify relevant documentation. Verify that the documentation shows support of EDNS(0) and handling of DNSSEC related resource records. Verify that the documentation shows support of full life cycle of cryptographic keys.	R10, DNS4
Doc DNS 08	Identify relevant information on TCP support for DNSSEC in the AS. Verify that the authoritative nameservers declared in the AS are those that were stated in the application.	R10
Doc Whois 01	Identify relevant documentation. Verify that the documentation describes the maximum rate of successfully handled questions on port 43 and the web interface.	R11, R12, WHOIS1
Doc Whois 02	Identify relevant documentation. Verify that this demonstrates data mining detection and mitigation control functions.	R11, R12, WHOIS2
Doc Whois 03	Identify relevant documentation. Verify that the provision made for searchable Whois lookup services comply with assertions made in the application.	R11, R12
Doc EPP 01	Identify relevant documentation. Verify that this demonstrates the provision of EPP services at the anticipated load.	R17, EPP1
Doc EPP 02	Identify relevant documentation. Verify that this provides transaction rate for ten datapoints between an empty registry database and at the size after one year of operation.	R17, EPP2
Doc EPP 03	Identify relevant documentation. Verify that the documentation describes measures to handle high peak load.	R17, EPP3
Doc EPP 04	Identify relevant documentation. Verify EPP extensions and compliance with specification 6 of the Registrar Agreement and RFC 3735	R18
Doc EPP 05	Identify relevant documentation. Verifiy that EPP services over IPv6 comply with assertions given in the gTLD application.	R18
Doc Escr 01	Identify relevant documentation. Verify that the escrow agreement includes the text in Specification 2. Verify that the agreement does not include provision contradicting this text.	R24, DATA1, DATA2, DATA3, DATA4, DATA5

Test ID	Description	Requirement Point
Doc DPS 01	Identify relevant documentation. Verify that the structure of the DPS is compliant with RFC 6841.	R25, DPS4
Doc DPS 02	Identify relevant documentation. Verify that the contents of the DPS is compliant with RFC 6841.	R25, DPS1, DPS2, DPS3, DPS4
Doc SL 01	Identify relevant documentation. Verify that the documentation shows that service levels meet applicable Service Level Requirements for DNS.	R10, DNS6
Doc SL 02	Identify relevant documentation. Verify that the documentation shows that service levels meet applicable Service Level Requirements for Whois.	R10, R12, Whois3
Doc SL 03	Identify relevant documentation. Verify that the documentation shows that service levels meet applicable Service Level Requirements for EPP.	R10, EPP4
Doc SL 04	Identify relevant documentation. Verify that the documentation shows that service levels meet Applicant assertions for DNS.	R10
Doc SL 05	Identify relevant documentation. Verify that the documentation shows that service levels meet Applicant assertions for Whois.	R10
Doc SL 06	Identify relevant documentation. Verify that the documentation shows that service levels meet Applicant assertions for EPP.	R10

2.3 Features to be tested

Not applicable. Test plan only applies to document testing.

2.4 Features not to be tested

Not applicable. Test plan only applies to document testing.

2.5 Approach

Review of submitted documents and attachments shall follow a structured approach. The goal of the review is to assess whether the documents show that the requirements stated in 2.1 are fulfilled.

Assessment shall be based on distinct testing criteria and motivations for judgments shall be supplied.

The review shall consist of the following steps:

1. Brief reading through of the submitted material. Categorization of the material.
2. Overall assessment of documents regarding inconsistency and unambiguity.
3. Finding evidence of fulfillment of requirements. This shall, in general, be based on the order of the requirements. A checklist shall be used. This is found in "Pre-Delegation Testing, Document Test Report Template". The template includes also Testing Procedures and Reporting Instructions for each requirement, which shall be followed.
4. Report.
    a. If all requirements are fulfilled, a brief report shall be compiled to the Applicant. A detailed report shall be compiled for the Pre-Delegation Testing Provider. This report shall state how each requirement is fulfilled, and where in the documents this is shown.
    b. If one or more requirements fail to be fulfilled, the report to the Applicant shall show in detail why the requirement is considered not fulfilled and what is missing in the documentation.

2.6 Item pass/fail criteria

The result of a review of requirements shall be treated uniformly regardless of Applicant and reviewer. The following guidelines shall be followed:

- The required property is found in the documentation. **Pass**.
- The required property is not found in the documentation. **Fail**.
- The required property is not found explicitly in the documentation, but can be inferred from other properties. **Pass**.
- The required property is not found explicitly in the documentation, but can be clearly motivated from other circumstances or facts shown in the documentation. **Pass**. A motivation must be stated.
- It is unclear whether the required property is part of the documentation. **Fail**. A motivation must be stated.
- Ambiguous or inconsistent statements in the documentation. **Fail**.

2.7 Suspension criteria and resumption requirements

Suspension of document testing should occur if:

- Applicant documentation is missing or incomplete for most parts
- Applicant documentation is ambiguous

Suspension of specific test cases can occur if:

- Applicant documentation for the specific test case is missing or ambiguous

If documentation is in place but the test for a specific test case results in a **Fail**, the test should be completed and documented in Documentation Test Log.

The test should restart after suspension if and when:

- Identified missing documentation are delivered by the applicant
- Identified ambiguities are corrected by the applicant

2.8 Test deliverables

The deliverables from the tests are the following reports:

- Pre-Delegation Testing, Document Test Log
- Pre-Delegation Testing, Document Test Report
- Pre-Delegation Testing, Document Anomaly Report, if applicable

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.