Registry System Testing

Documentation Test Area Specification

Version A

File name: Test Area Documentation.docx
Last saved: 2017-07-27

Document control

Document information and security

Made by	Responsible for fact	Responsible for document
Lennart Bonnevier	Mats Dufberg	Mats Dufberg

Security class	File name
External	Test Area Documentation.docx

Revisions

Date	Version	Name	Description
2017-07-27	A	Mats Dufberg	First release version.

LIST OF CONTENTS

1. Introduction

This document describes the Documentation Level Tests within the Registry System Testing framework.

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 area in order to establish a common structure for reviewing the submitted documents.

1.2 References

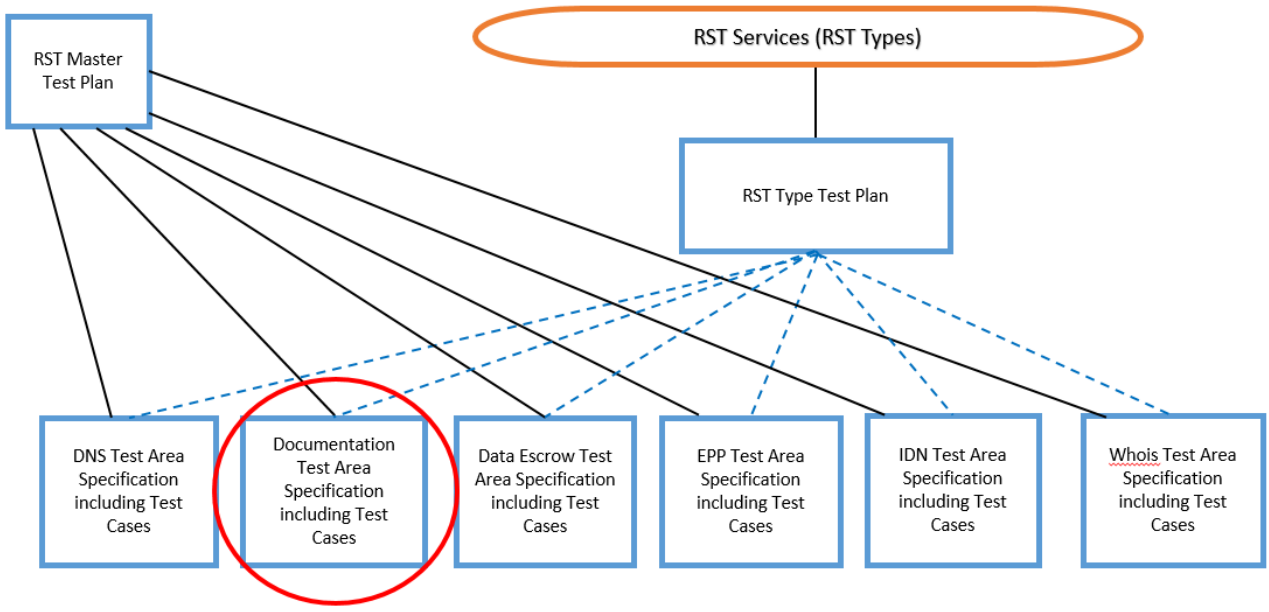
1.2.1 External

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

1.2.2 Internal

- Pre-Delegation Testing, Statement of Work
- Registry System Testing, Master Test Plan

1.2.3 Document Hierarchy



This document is one of many Test Area Specifications for RST (circled in red in the above graphic). It defines the Test Cases for its Test Area.

1.3 Earlier documents

This document replaces, in contents, the following documents that were part of PDT (Pre-Delegation Testing):

- Pre-Delegation Testing: Documentation Test Plan (version J)

- Pre-Delegation Testing: Documentation Data Escrow Test Cases (version G)
- Pre-Delegation Testing: Documentation DNS Test Cases (version H)
- Pre-Delegation Testing: Documentation DPS Test Cases (version G)
- Pre-Delegation Testing: Documentation EPP Test Cases (version G)
- Pre-Delegation Testing: Documentation Service Level Test Cases (version G)
- Pre-Delegation Testing: Documentation Whois Test Cases (version F)

1.4 Level in the overall sequence

This Test Area and the associated Test Cases can be run in parallel with the other Test Areas.

1.5 Test classes and overall test conditions

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

2. Test Requirements

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 [Registry Operator'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** [Registry Operator'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 [Registry Operators], **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 [Registry Operator] 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 [Registry Operator'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 [Registry Operator'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] [Registry Operator] 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 [Registry Operator] 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 [a] load expectation [provided by the Registry Operator].

[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, [Registry Operator] 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 the Registry Operator.

[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 Test Area Data Escrow.

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 Registry Operator MUST demonstrate its ability to support the full life cycle of cryptographic keys.

[DPS3] The Registry Operator 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.

In addition to the above, the requirement below has been identified in 'Section 4.8 – Legal Matters' in RFC 6841:

[DPS5] The Registry Operator MUST indicate under what jurisdiction the registry is operated.

2.2 Features to be tested

Not applicable. This Test Area only applies to document reviewing.

2.3 Features not to be tested

Not applicable. This Test Area only applies to document reviewing.

2.4 Approach

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

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

The review consists 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. The template for this checklist 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 Registry Operator. A detailed report shall be compiled for the Registry System 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 Registry Operator shall show in detail why the requirement is considered not fulfilled and what is missing in the documentation.

2.5 Item pass/fail criteria

The result of a review of requirements shall be treated uniformly regardless of Registry Operator 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**.

2.6 Suspension criteria and resumption requirements

Suspension of document testing should occur if:
- Submitted documentation is missing or incomplete for most parts
- Submitted documentation is ambiguous

Suspension of specific test cases can occur if:
- Submitted 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 is delivered by the Registry Operator
- Identified ambiguities are corrected by the Registry Operator

2.7 Test deliverables

The deliverables from the tests are the following reports:

- Registry System Testing, Document Test Log
- Registry System Testing, Document Test Report
- Registry System Testing, Document Anomaly Report, if applicable

3. Test Traceability Matrix

This table describes the different test cases and their mapping to the requirements. The tests are performed by reviewing the self-certification documents to verify compliance with the requirements *and* any assertions made by the Registry Operator in the Registry Agreement.

Test ID	Description	Requirement Point
DocDNS01	Identify relevant documentation. Verify that network availability and server capacity is included. Verify that expected capacity is included. Verify that DNS server and network availability capacity is equal to or greater than 2 times the expexted load. Verify that DDoS attacks are addressed.	R10, DNS1
DocDNS02	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,
DocDNS03	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
DocDNS04	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.	R10, DNS2.2, DNS3.2, DNS5
DocDNS05	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
DocDNS06	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
DocDNS07	Identify relevant documentation. Verify that the documentation on DNSSEC states support of EDNS(0) and handling of DNSSEC related resource records. Verify that the documentation states support of full life cycle of cryptographic keys.	R10, DNS4
DocDNS08	Identify relevant information on nameservers in the documentation. Verify that the there is no conflict between nameservers declared for the technical tests and those declared in the self-certification documents.	R10
DocWhois01	Identify relevant documentation. Verify that the documentation describes the maximum rate of successfully handled questions on port 43 and the web interface. Verify that an expected load is provided. Verify that the Whois service capacity is equal to or greater than 2 times the expected load.	R11, R12, WHOIS1
DocWhois02	Identify relevant documentation. Verify that this demonstrates data mining detection and mitigation control functions.	R11, R12, WHOIS2
DocEPP01	Identify relevant documentation. Verify that this demonstrates the provision of EPP services at the anticipated load. Verify that the EPP service capacity is equal to or greater than 2 times the expected load.	R17, EPP1
DocEPP02	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
DocEPP03	Identify relevant documentation. Verify that the documentation describes measures to handle high peak load.	R17, EPP3
DocEPP04	Identify relevant documentation. Verify EPP extensions compliance with the Registry Agreement and RFC 3735	R18
DocEscr01	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
DocDPS01	Identify relevant documentation. Verify that the structure of the DPS is compliant with RFC 6841.	R25, DPS4
DocDPS02	Identify relevant documentation. Verify that the contents of the DPS is compliant with RFC 6841.	R25, DPS1, DPS2, DPS3, DPS4, DPS5

Test ID	Description	Requirement Point
DocSL01	Identify relevant documentation. Verify that the documentation shows that service levels meet applicable Service Level Requirements for DNS in Specification 10 of the Registry Agreement.	R10, DNS6
DocSL02	Identify relevant documentation. Verify that the documentation shows that service levels meet applicable Service Level Requirements for Whois in Specification 10 of the Registry Agreement.	R10, R12, Whois3
DocSL03	Identify relevant documentation. Verify that the documentation shows that service levels meet applicable Service Level Requirements for EPP in Specification 10 of the Registry Agreement.	R10, EPP4

4. 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.

5. Test Case Document DNS 01: Capacity and DDOS Mitigation

5.1 Test case identifier

DocDNS01

5.2 Objective

The test verifies that the self-certification documents include

- results from system performance tests indicating available network and server capacity.
- an estimate of expected capacity during normal operation.
- mitigation of DDoS attacks.

5.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

5.4 Outcome(s)

The self-certification documents MUST include the required information.

5.5 Environmental needs

N/A

5.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

5.7 Intercase dependencies

This test has no intercase dependencies.

5.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents that contain system performance test including available network and server capacity. Expected part is: document gTLDSelfCert section 1.1.5.
2. Verify the following results from a system performance test are included
    a. available network and
    b. server capacity.
3. Identify the parts in the self-certification documents that contain an estimation of expected capacity during normal operation. Expected part is: document gTLDSelfCert section 1.1.2, 1.1.5.
4. Verify that an estimate of expected capacity during normal operation is included.
5. Verify that the self-certification documents demonstrate that the DNS server and network availability capacity is equal to or greater than 2 times the expected load.
6. Identify the parts in the self-certification documents that cover DDoS attacks. Expected part is: document gTLDSelfCert section 1.1.4.

7. Verify that Distributed Denial of Service attacks are adequately addressed.
   While it is difficult to give definite criteria for adequate mitigation of DDoS attacks, the self-certification should address at least the following points for automatic or semi-automatic as well as manual countermeasures:
   a. Describe the strategy for dealing with DDoS attacks.
   b. Describe the controls used in dealing with DDoS attacks.
   c. The extent to which the chosen countermeasures suppress DDoS traffic.
   d. The extent to which the chosen countermeasures affect legitimate DNS queries.
   e. The time that elapses before countermeasures reach full effect.
   f. The time that elapses before normal operation is reestablished after a DDos attack has ended.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- Results regarding available network and server capacity are included (step 2).
- An estimate of expected capacity is included. The documentation must show that the DNS server and network availability capacity exceeds the anticipated load by at least 2 times as stated in the self-certification documents (step 5).
- An adequate description of the handling of DDOS attacks is included (step 7).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

6. Test Case Document DNS 02: Load Capacity, Latency and Network Reachablility

6.1 Test case identifier

DocDNS02

6.2 Objective

The test verifies that the self-certification documents include data on load capacity, latency and network reachability, for UDP and TCP support, and the corresponding for DNSSEC.

6.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

6.4 Outcome(s)

The self-certification documents MUST include the required information.

6.5 Environmental needs

N/A

6.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

6.7 Intercase dependencies

This test has no intercase dependencies.

6.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents that cover load capacity, latency and network reachability for UDP and TCP support, and the corresponding with DNSSEC. Expected part is: document gTLDSelfCert section 1.1, 1.1.5, 1.2, 1.3.
2. Verify the following are included
    a. load capacity,
    b. latency and
    c. network reachability with ASN's of transit providers or peers.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- Values for load capacity & latency MUST be provided.
- Network reachability information MUST be provided.

Criteria for FAIL:

- Some of the requested information is unclear or missing.

7. Test Case Document DNS 03: Load Capacity Tables and Graphs

7.1 Test case identifier

DocDNS03

7.2 Objective

The test verifies that the self-certification documents include a report of load capacity both using a tables and corresponding graphs, for UDP and TCP support, and the corresponding for DNSSEC. The graphs shall show the percentage of queries responded against an increasing number of queries per second, generated from local traffic generators.

7.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

7.4 Outcome(s)

The self-certification documents MUST include the required information.

7.5 Environmental needs

N/A

7.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

7.7 Intercase dependencies

This test has no intercase dependencies.

7.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents that contain report on load capacity for UDP and TCP support, and the corresponding with DNSSEC. Expected part is: document gTLDSelfCert section 1.1.3, 1.1.5.
2. Verify that the load capacity is reported both using
    a. a table, and
    b. a corresponding graph.
3. Verify the data provided reflects percentage of queries responded against an increasing number of queries per second generated from local (to the servers) traffic generators.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- Load capacity is reported in a table (step 2 a).
- Load capacity is reported in a graph (step 2 b).

- The table and graph shows the percentage of queries successfully responded to against an increasing number of queries per second (step 3).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

8. Test Case Document DNS 04: 20 Data Points

8.1 Test case identifier

DocDNS04

8.2 Objective

The test verifies that the report on load capacity for UDP and TCP support, and the corresponding with DNSSEC, in the self-certification documents includes at least 20 data points, and loads of queries that will cause up to 10% query loss against a randomly selected subset of servers within the Registry Operator's DNS infrastructure.

8.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

8.4 Outcome(s)

The self-certification documents MUST include the required information.

8.5 Environmental needs

N/A

8.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

8.7 Intercase dependencies

This test has no intercase dependencies.

8.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents that contain report on load capacity for UDP and TCP support, and the corresponding with DNSSEC. Expected part is: document gTLDSelfCert section 1.1.3, 1.1.5.
2. Verify that the reported table includes:
    a. at least 20 data points and
    b. loads that will cause up to 10% query loss against a randomly selected subset of servers within the Registry Operator's DNS infrastructure.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- The table on load capacity contains at least 20 data points (step 2 a).
- The table on load capacity contains data points for loads causing up to 10% query loss or contains load up to 100 000 queries per second (step 2 b).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

9. Test Case Document DNS 05: Query Latency

9.1 Test case identifier

DocDNS05

9.2 Objective

The test verifies that the self-certification documents for UDP and TCP support, and the corresponding with DNSSEC include a report on query latency in milliseconds, measured by DNS probes located just outside the border routers.

9.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

9.4 Outcome(s)

The self-certification documents MUST include the required information.

9.5 Environmental needs

N/A

9.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

9.7 Intercase dependencies

This test has no intercase dependencies.

9.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents that contain report on latency for UDP and TCP support, and the corresponding with DNSSEC. Expected part is: document gTLDSelfCert section 1.2.1, 1.2.2.
2. Verify that query latency is
    a. reported in milliseconds,
    b. 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.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- Query latency is reported in milliseconds (step 2 a).
- Query latency is measured outside the border routers of the network hosting the name servers (step 2 b).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

10. Test Case Document DNS 06: TCP Reachability

10.1 Test case identifier

DocDNS06

10.2 Objective

The test verifies that the self-certification documents for TCP support include documentation on reachability by providing records of TCP-based DNS queries from nodes external to the network hosting the servers.

10.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

10.4 Outcome(s)

The self-certification documents MUST include the required information.

10.5 Environmental needs

N/A

10.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

10.7 Intercase dependencies

This test has no intercase dependencies.

10.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents that contain report on reachability for TCP support. Expected part is: document gTLDSelfCert section 1.3.1.
2. Verify that reachability is documented by providing records of TCP-based DNS queries from nodes external to the network hosting the servers. These nodes may be the same as those used for measuring latency for TCP support, TC DocDNS05.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- Records of TCP-based queries are included (step 2).
- It is stated that these are sent from external nodes (step 2).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

11. Test Case Document DNS 07: Basic DNSSEC Support

11.1 Test case identifier

DocDNS07

11.2 Objective

The test verifies that the self-certification documents for DNSSEC support state support for EDNS(0) in Registry Operator's 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.

The test also verifies that the documents state support for the full life cycle of cryptographic keys.

11.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

11.4 Outcome(s)

The self-certification documents MUST include the required information.

11.5 Environmental needs

N/A

11.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

11.7 Intercase dependencies

This test has no intercase dependencies.

11.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents that cover DNSSEC support. Expected part is: document gTLDSelfCert section 1.4.
2. Verify that it states
    a. support for EDNS(0) in its server infrastructure,
    b. the ability to return correct DNSSEC-related resource records such as DNSKEY, RRSIG, and NSEC/NSEC3 for the signed zone, and
    c. the ability to accept and publish DS resource records from second-level domain administrators.
3. Verify that it states the ability to support the full life cycle of cryptographic keys.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- It is stated that support for EDNS(0) is included (step 2 a).
- It is stated that correct DNSSEC-related resource records can be returned. Examples are DNSKEY, RRSIG and NSEC/NSEC3 (step 2 b).
- It is stated that DS resource records from second-level domain administrators can be accepted and published (step 2 c).
- It is stated that the full life cycle of cryptographic keys is supported (step 3).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

12. Test Case Document DNS 08: Nameserver Consistency

12.1 Test case identifier

DocDNS08

12.2 Objective

The test verifies that there is no conflict between the authoritative nameservers (anycast nodes, unicast nodes and DNS operators) declared in the self-certification documents and those defined for the technical tests.

12.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents
XMLFile	Description of Registry Operator's DNS environment in XML format	Files

12.4 Outcome(s)

The self-certification documents MUST include the required information.

12.5 Environmental needs

N/A

12.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

12.7 Intercase dependencies

This test has no intercase dependencies.

12.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents that states nameservers. Expected part is: document gTLDSelfCert section 1.1.5.
2. Identify the authoritative nameservers declared in the submitted XML-file.
3. Verify that there is no conflict between the authoritative nameservers (anycast nodes, unicast nodes and DNS operators) defined for the technical test and those declared in the self-certification documents.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- No differences may be present between the name servers provided for the DNS tests & those declared in the self-certification documents (step 2).

Criteria for FAIL:

- One or more of the PASS criteria is not fulfilled.
- Part of the requested information is unclear or missing.

13. Test Case Document Whois 01: Maximum QPS

13.1 Test case identifier

DocWhois01

13.2 Objective

The test verifies that the self-certification documents

- describe the maximum number of queries per second successfully handled, both on port 43 and web interface
- include a load expectation provided by the Registry Operator

13.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

13.4 Outcome(s)

The self-certification documents MUST include the required information.

13.5 Environmental needs

N/A

13.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

13.7 Intercase dependencies

This test has no intercase dependencies.

13.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents concerning Whois transaction capacity, including both TCP port 43 and via a web interface. Expected part is: document gTLDSelfCert section 2.1.
2. Verify that the self-certification documents include a description of the maximum number of queries successfully handled on TCP port 43.
3. Verify that the self-certification documents include a description of the maximum number of queries successfully handled on a web interface.
4. Verify that the self-certification documents demonstrate that the Whois service capacity is equal to or greater than 2 times the expected load.
5. Verify that the self-certification documents include an estimate of expected load.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- The maximum number of queries per second successfully handled on TCP port 43 is included (step 2).
- The maximum number of queries per second successfully handled on a web interface is included (step 3).
- The capacity is equal to or greater than 2 times the expected load (step 4).
- A load expectation is stated (step 5).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

14. Test Case Document Whois 02: Data Mining

14.1 Test case identifier

DocWhois02 Data Mining

14.2 Objective

The test verifies that the self-certification documents

- Include a description of deployed control functions to detect data mining of the Whois database.
- Include a description of deployed control functions to mitigate data mining of the Whois database.

14.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

14.4 Outcome(s)

The self-certification documents MUST include the required information.

14.5 Environmental needs

N/A

14.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

14.7 Intercase dependencies

This test has no intercase dependencies.

14.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents describing detection and mitigation of data mining of the Whois service. Expected part is: document gTLDSelfCert section 2.2.
2. Verify that the self-certification documents include a description of deployed control functions for detecting data mining of the Whois service.
3. Verify that the self-certification documents include a description of deployed control functions for mitigating data mining of the Whois service.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- A description of a deployed control function for the detection of data-mining attempts of the Whois service is included (step 2).
- A description of a deployed control function for the mitigation of data-mining attempts of the Whois service is included (step 3).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

15. Test Case Document EPP 01: EPP Capacity

15.1 Test case identifier

DocEPP01

15.2 Objective

The test verifies that the self-certification documents demonstrate that the EPP service capacity exceeds the anticipated load.

15.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

15.4 Outcome(s)

The self-certification documents MUST include the required information.

15.5 Environmental needs

N/A

15.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

15.7 Intercase dependencies

This test has no intercase dependencies.

15.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents concerning EPP service capacity. Expected part is: document gTLDSelfCert section 3.1.
2. Verify that the self-certification documents demonstrate that the EPP service capacity is equal to or greater than 2 times the expected load.

The outcome of the testcase is PASS if the criteria for PASS and no criteria for FAIL is fulfilled.

Criteria for PASS:

- The anticipated load on the EPP service is stated, as well as the capacity of the service. The documentation must show that the EPP service capacity exceeds the expected load by at least 2 times as stated in the self-certification documents (step 2).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

16. Test Case Document EPP 02: EPP TPS

16.1 Test case identifier

DocEPP02 EPP TPS

16.2 Objective

The test verifies that the self-certification documents

- provide the expected transactions per second rate for the EPP interface.
- provide this rate with 10 data points ranging from empty registry database to the expected size after one year of operations.

16.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

16.4 Outcome(s)

The self-certification documents MUST include the required information.

16.5 Environmental needs

N/A

16.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

16.7 Intercase dependencies

This test has no intercase dependencies.

16.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents concerning EPP transaction rate. Expected part is: document gTLDSelfCert section 3.1.
2. Verify that the self-certification documents provides expected transactions rate for the EPP interface.
3. Verify that the documentation states the expected size of the registry database after one year of operations, as determined by the Registry Operator.
4. Verify that the expected transaction rate is given in 10 data points ranging from an empty registry database to the expected size after one year of operations.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- Expected transaction rate for the EPP interface is provided (step 2).

- An estimate of the registry database after one year of operation is provided (step 3).
- The expected transaction rate is provided for 10 data points ranging from an empty database to the above mentioned estimated size (step 4).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

17. Test Case Document EPP 03: EPP Land-rush

17.1 Test case identifier

DocEPP03

17.2 Objective

The test verifies that the self-certification documents describe measures taken to handle EPP services during initial registry operations, e.g. a land-rush period.

17.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

17.4 Outcome(s)

The self-certification documents MUST include the required information.

17.5 Environmental needs

N/A

17.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

17.7 Intercase dependencies

This test has no intercase dependencies.

17.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents concerning EPP service capacity. Expected part is: document gTLDSelfCert section 3.2.
2. Verify that the self-certification documents describe measure taken to handle EPP services during initial registry operations, e.g. a land-rush period.

The outcome of the testcase is PASS if the criteria for PASS and no criteria for FAIL is fulfilled.

Criteria for PASS:

- A brief description is included of reasonable measures for handling EPP services during initial registry operations (step 2).

Criteria for FAIL:

- Part of the requested information is unclear or missing.

18. Test Case Document EPP 04: EPP Extensions

18.1 Test case identifier

DocEPP04

18.2 Objective

The test verifies that the Registry Operator attests the EPP extensions are documented in accordance with RFC 3735 in their self certification document.

18.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents

18.4 Outcome(s)

A pass will be awarded if statement in the self certification claims the EPP extensions are documented in accordance with the guidelines of RFC 3735, otherwise the test case will fail.

18.5 Environmental needs

N/A

18.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

18.7 Intercase dependencies

This test has no intercase dependencies.

18.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents concerning EPP extensions. Expected part is: document gTLDSelfCert section 3.3.
2. Verify that the self-certification documents demonstrate that the EPP extensions
    a. complies with RFC 3735
    b. are documented in Internet-Draft format following the guidelines described in RFC 3735

The outcome of the testcase is PASS if the criteria for PASS and no criteria for FAIL are fulfilled.

19. Test Case Document Escr 01: Data Escrow Agreement

19.1 Test case identifier

DocEscr01

19.2 Objective

The test verifies that the Registry Operator's data escrow agreement complies with specification 2 of the Registry Agreement.

19.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents
DataEscrowAgreement	The data escrow agreement between Registry Operator and data escrow agent	Document
LetterOfCompliance	A letter of compliance from either the data escrow agent or ICANN	Document

19.4 Outcome(s)

The data escrow agreement is found valid.

19.5 Environmental needs

N/A

19.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

19.7 Intercase dependencies

This test has no intercase dependencies.

19.8 Ordered description of steps to be taken to execute the test case

1. Identify the uploaded data escrow agreement and written letter of compliance from either escrow agent or ICANN, as relevant. Expected part is: document gTLDSelfCert section 4.
2. Verify that the data escrow agent is an ICANN approved data escrow agent, according to list https://newgtlds.icann.org/en/applicants/data-escrow
3. Verify that the submitted letter of compliance is issued by the correct party (data escrow agent or ICANN). Registry Operators requiring letter of compliance from ICANN are separately identified by ICANN, all other shall provide letters of compliance from the data escrow agents.
4. Verify that the data escrow agreement is duly executed (signed by the Registry Operator and the approved data escrow agent)
5. Verify that the relevant letter of compliance is duly executed, i.e. signed by either;
    a. the data escrow agent; or
    b. by ICANN representative
6. Verify that the effective date of the data escrow agreement is not in the future.

7. Verify that the date in the letter of compliance is not in the future.
8. Verify that the TLD referred to in the data escrow agreement and the relevant letter of compliance is the same and that the TLD is attributable to the relevant Registry Operator.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- The data escrow agent is an ICANN approved data escrow agent.
- The data escrow agreement is signed by both parties.
- The gTLD-string is correctly stated in the data escrow agreement and in the letter of compliance.
- The effective date of the agreement and the date in the letter of compliance are not in the future.
- The data escrow agreement is shown to be approved by
    - a cover letter, signed by the data escrow agent, certifying that both Part A and Part B of Specification 2 are fulfilled, or by
    - an ICANN approval letter for non standard escrow agreements, signed by ICANN representative.

Criteria for FAIL:

- Some of the requested information is unclear or missing.

20. Test Case Document SL 01: DNS SLA

20.1 Test case identifier

DocSL01

20.2 Objective

The test verifies that the self-certification documents concerning DNS service levels comply with with the SLA given in Specification 10 of the Registry Agreement.

20.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents
Specification 10	Specification 10 of the Registry Agreement	Documents

20.4 Outcome(s)

The self-certification documents MUST include the required information.

20.5 Environmental needs

N/A

20.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

20.7 Intercase dependencies

This test has no intercase dependencies.

20.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents that contain service levels for DNS support. Expected part is: document gTLDSelfCert section 1.5.
2. Verify that DNS service availability
    a. is stated in the self-certification documents and
    b. that it complies with the SLA in Specification 10.
3. Verify that DNS name server availability
    a. is stated in the self-certification documents and
    b. that it complies with the SLA in Specification 10.
4. Verify that TCP DNS resolution RTT
    a. is stated in the self-certification documents and
    b. that it complies with the SLA in Specification 10.
5. Verify that UDP DNS resolution RTT
    a. is stated in the self-certification documents and
    b. that it complies with the SLA in Specification 10.
6. Verify that DNS update time
    a. is stated in the self-certification documents and
    b. that it complies with the SLA in Specification 10.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- All service levels comply with what is stated in Specification 10 of the Registry Agreement.

Criteria for FAIL:

- One or more service levels does not fulfill what is stated in the Registry Agreement.
- Part of the requested information is unclear or missing.

21. Test Case Document SL 02: Whois SLA

21.1 Test case identifier

DocSL02

21.2 Objective

The test verifies that the self-certification documents concerning Whois service levels comply with with the SLA given in Specification 10 of the Registry Agreement.

21.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents
Specification 10	Specification 10 of the Registry Agreement	Documents

21.4 Outcome(s)

The self-certification documents MUST include the required information.

21.5 Environmental needs

N/A

21.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

21.7 Intercase dependencies

This test has no intercase dependencies.

21.8 Ordered description of steps to be taken to execute the test case

1. Identify the parts in the self-certification documents that contain service levels for Whois services. Expected part is: document gTLDSelfCert section 2.3.
2. Verify that the availability of Whois services
    a. is stated in the self-certification documents and
    b. that it complies with the SLA in Specification 10.
3. Verify that the query Round-Trip Time for Whois services
    a. is stated in the self-certification documents and
    b. that it complies with the SLA in Specification 10.
4. Verify that the update time for Whois services
    a. is stated in the self-certification documents and
    b. that it complies with the SLA in Specification 10.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- All service levels comply with what is stated in Specification 10 of the Registry Agreement.

Criteria for FAIL:

- One or more service levels does not fulfill what is stated in the Registry Agreement.
- Part of the requested information is unclear or missing.

22. Test Case Document SL 03: EPP SLA

22.1 Test case identifier

DocSL03

22.2 Objective

The test verifies that the self-certification documents concerning EPP service levels comply with with the SLA given in Specification 10 of the Registry Agreement.

22.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDSelfCert	The submitted self-certification documentation	Documents
Specification 10	Specification 10 of the Registry Agreement	Documents

22.4 Outcome(s)

The self-certification documents MUST include the required information.

22.5 Environmental needs

N/A

22.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

22.7 Intercase dependencies

This test has no intercase dependencies.

23. Test Case Document DPS 01: DPS Structure

23.1 Test case identifier

DocDPS01

23.2 Objective

The test verifies that the structure of the DNSSEC Practice Statement (DPS) is compliant with RFC 6841.

23.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDDPS	The submitted DNSSEC Practice Statement	Document

23.4 Outcome(s)

The documents MUST include the required information.

23.5 Environmental needs

N/A

23.6 Special procedural requirements

Suspend test if documentation is missing or incomplete for most parts.

23.7 Intercase dependencies

This test has no intercase dependencies.

23.8 Ordered description of steps to be taken to execute the test case

1. Identify the DNSSEC Practice Statement, DPS. Expected document is: document gTLDDPS.
2. Verify that the DPS essentially follows the structure described in the IETF A Framework for DNSSEC Policies and DNSSEC Practice Statements, RFC 6841.
3. Verify that the DPS essentially includes the 8 main sections and all applicable second level subsections of these, stated in RFC 6841, section 5 "Contents of a Set of Provisions".

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- The DPS follows the structure given in RFC 6841 with only minor deviations (step 2).
- The DPS includes all 8 main sections and all applicable second level subsections stated in RFC 6841 section 5, with only minor deviations (step 3).

Criteria for FAIL:

- Greater than minor deviations from RFC 6841 exists in the DPS, e.g. missing sections.
- Part of the requested information is unclear or missing.

24. Test Case Document DPS 02: DPS Contents

24.1 Test case identifier

DocDPS02

24.2 Objective

The test verifies that the contents of the DNSSEC Practice Statement (DPS) is compliant with RFC 6841.

24.3 Inputs

The following information will be needed as input for this test case:

Id	Description	Type
gTLDDPS	The submitted DNSSEC Practice Statement	Document

24.4 Outcome(s)

The documents MUST include the required information.

24.5 Environmental needs

N/A

24.6 Special procedural requirements

Suspend test if documentation is incomplete for most parts or missing completely.

24.7 Intercase dependencies

This test has no intercase dependencies.

24.8 Ordered description of steps to be taken to execute the test case

1. Identify the DNSSEC Practice Statement, DPS. Expected document is: document gTLDDPS.
2. Verify that the DPS essentially follows the contents described in the IETF A Framework for DNSSEC Policies and DNSSEC Practice Statements, RFC 6841.
3. Verify that the DPS essentially follows the guidelines given in RFC 6841, section 4 "Contents of a Set of Provisions".
4. Verify specifically that the DPS includes the following content:
    a. "Section 1 Introduction", including Document identification and Version.
    b. "Section 2 Publication and Repositories".
    c. "Section 5 Technical Security Controls" including:
        i. What keys are going to be used
        ii. Key pair generation and installation
        iii. Private key protection
        iv. Life cycle technical controls
    d. "Section 6 Zone Signing" including:
        i. Key lengths and algorithms
        ii. Authenticated denial of existence (NSEC/NSEC3)
        iii. Signature format
        iv. Key rollover (for each present key type)
        v. Signature lifetime and re-signing frequency
    e. "Section 8 Legal Matters", must include information about under what jurisdiction the registry is operated.

The outcome of the testcase is PASS if all criteria for PASS and no criteria for FAIL are fulfilled.

Criteria for PASS:

- The DPS contains the contents given in RFC 6841 section 4, with only minor deviations (step 2 and 3).
- The DPS contain all of the contents stated above (step 4).

Criteria for FAIL:

- Greater than minor deviations from RFC 6841 section 4 exists in the DPS, e.g. more than one missing information.
- One or more of the information requested in step 4 is missing or unclear.
- Part of the otherwise requested information is unclear or missing.
- Information about under what jurisdiction the registry is operated is not specified.

25. General

25.1 Glossary

The glossary is available in the Master Test Plan.

25.2 Document change procedures

Document change procedures are documented in the Master Test Plan.